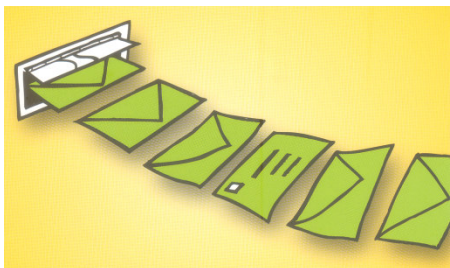


Ransomware

I "ransomware" sono programmi che impediscono l'accesso ai documenti personali finché non viene pagato un "riscatto".

In passato venivano utilizzati per danneggiare o cancellare documenti; oggi questi programmi si impossessano dei dati e li tengono "in ostaggio". Ad esempio, il Trojan Archiveus copia il contenuto della cartella "Documenti" all'interno di un file protetto da password e, in seguito, cancella l'originale. L'utente riceve un messaggio nel quale viene specificato che è necessario digitare una password di 30 caratteri per accedere alla cartella e che tale password gli sarà comunicata solo dopo aver effettuato un acquisto da un negozio online.



Spam

Lo spam è posta commerciale non richiesta, l'equivalente elettronico dei volantini e dei cataloghi che intasano le cassette della posta.

Oltre il 99% dello spam proviene da computer violati, sistemi infettati che fanno parte di una botnet. Spesso lo spam è redditizio; gli spammer sono in grado di inviare milioni di e-mail nel corso di un'unica campagna, ad un costo irrisorio. Se anche un solo destinatario, su migliaia di invii, effettua un acquisto, lo spammer consegue un guadagno.

Catone di Sant'Antonio

Ransomware Hoax

Spam Virus Zombies

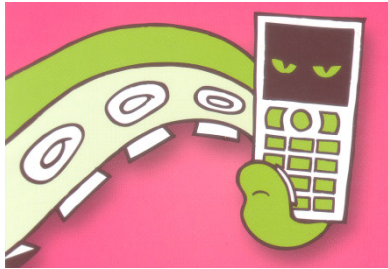
Rootkit Adware

Mobile Phone Malware

E-mail Malware

Spear phishing

www.opificium.it



Mobile phone malware

Il malware dei telefoni cellulari è destinato all'esecuzione sui dispositivi mobili, come ad esempio smartphone o PDA.

Il primo worm per telefoni cellulari è stato scritto nel 2004. Il worm Cabir-A attacca i telefoni cellulari che utilizzano il sistema operativo Symbian e viene trasmesso sotto forma di file di gioco telefonico (come file SIS). Se si avvia il file, sullo schermo compare un messaggio e il worm viene seguito ad ogni successiva accensione del telefono. Cabir-A cerca altri telefoni cellulari che si trovano nelle vicinanze utilizzando la tecnologia Bluetooth e si propaga al primo telefono disponibile che trova.



E-mail Malware

Per e-mail malware si intende il malware distribuito tramite e-mail.

Storicamente, alcune delle famiglie di virus più prolifiche (es.: Netsky e SoBig) si sono diffuse come allegati a messaggi e-mail.

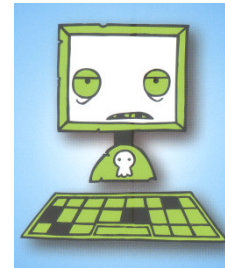
Queste famiglie inducevano gli utenti a effettuare doppio clic su un allegato, provocando l'esecuzione del codice malevolo, l'infezione del sistema e l'invio, con conseguente propagazione ad altri indirizzi e-mail presenti nel computer.



Attacchi Brute Force

Un attacco "brute force" è un attacco in cui gli hacker provano un gran numero di combinazioni di tasti o password per riuscire ad accedere a un sistema o file non autorizzato.

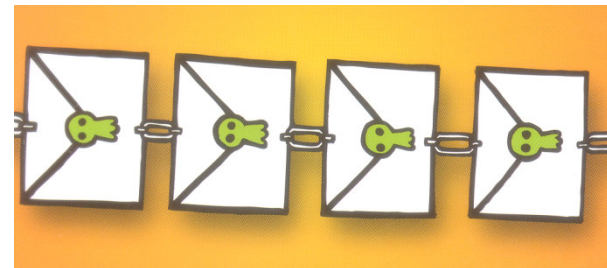
Spesso gli attacchi "brute force" sono utilizzati per violare uno schema crittografico, come ad esempio quelli protetti da password. Gli hacker utilizzano i programmi informatici per creare un gran numero di password, nel tentativo di decifrare un messaggio o accedere al sistema.



Zombies

Uno zombie è un computer infettato e controllato in remoto da un hacker. Spesso, fa parte di una botnet, ossia una rete di molti computer zombie, o bot.

Se un hacker'è in grado di controllare il computer in remoto via Internet, significa che esso è uno zombie.



Catene di Sant'Antonio

Le catene di Sant'Antonio sono e-mail che esortano a

inoltrare urgentemente copie del messaggio ad altri utenti.

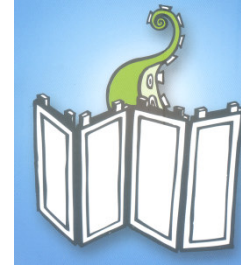
Le catene di Sant'Antonio, come gli hoax, vengono propagate sfruttando gli utenti stessi invece di agire sulla programmazione del computer. Non rappresentano una minaccia alla sicurezza, ma causano sprechi di tempo, diffondono informazioni non corrette e sviano l'attenzione degli utenti. La soluzione per bloccare le catene di Sant'Antonio è molto semplice: non inoltrate il messaggio.



Adware

L'adware è un programma che mostra messaggi pubblicitari sul monitor del computer.

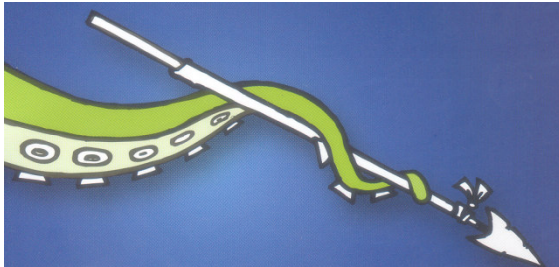
I software adware possono rallentare il PC, così come la navigazione, a causa dell'intasamento dovuto ai messaggi pubblicitari. Talvolta una presenza eccessiva di questi software può rendere il computer instabile.



Rootkit

Un rootkit è un software in grado di nascondere i programmi o i processi in esecuzione sul computer. Viene solitamente utilizzato per sottrarre dati o eseguire operazioni illecite.

Una percentuale significativa dell'attuale malware installa i rootkit dopo l'infezione, per nascondere la propria attività.



Spear phishing

Lo "spear phishing" è un tipo di phishing mirato, che utilizza messaggi di posta elettronica falsificati

apparentemente attendibili che inducono tutti gli appartenenti a una determinata organizzazione a rivelare dati o credenziali sensibili.

A differenza del phishing, che si basa su invii di massa, lo "spear phishing" opera su scala ridotta e in maniera molto mirata. Lo spear phisher prende di mira gli utenti di una singola azienda. I messaggi sembrano provenire da un altro dipendente della stessa azienda e chiedono di confermare nome utente e password. Un trucco diffuso è quello di spacciarsi per un collega di un ufficio che ha motivo e titolo di chiedere tali informazioni, ad esempio sistemi informativi o gestione del personale. A volte il messaggio dirotta l'utente su una versione falsificata del sito o della intranet aziendale.



Virus

I virus sono programmi che si diffondono generando copie di se stessi.

I virus informatici si diffondono sul computer e sulle reti generando copie di se stessi, solitamente all'insaputa dell'utente. I virus possono sortire effetti dannosi, dalla visualizzazione di messaggi fastidiosi sullo schermo alla sottrazione di dati, fino alla cessione del controllo del computer ad altri utenti.



Hoax

Gli hoax sono falsi allarmi su virus inesistenti.

Se gli utenti inoltrano effettivamente un falso allarme, può generarsi una valanga di e-mail, con il conseguente sovraccarico e blocco dei server di posta. I messaggi falsi possono inoltre distrarre l'utente nel corso dei suoi tentativi di fronteggiare le reali minacce del malware. Poiché gli hoax non sono malware, l'antivirus e il software di protezione dei computer non sono in grado né di rilevarli né di disattivarli.



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 applicazione pratica nei primi anni '60, nel gioco ideato da un gruppo di programmatori dei Bell Laboratories di AT&T, chiamato "Core Wars", nel quale più programmi si dovevano sconfiggere, sovrascrivendosi a vicenda. Era l'inizio della storia dei virus informatici.

Il termine "virus" venne usato la prima volta da Fred Cohen (1984 - University of Southern California) nel suo scritto Experiments with Computer Viruses. La definizione era la seguente: "Un virus informatico è un programma che ricorsivamente ed esplicitamente copia una versione possibilmente evoluta di sé stesso".

Nel 1972 David Gerrold scrisse un romanzo di fantascienza, "La macchina di D.I.O.", in cui è presente la descrizione di un programma per computer chiamato "VIRUS", che fa esattamente le stesse cose di un virus informatico. Nel 1975 John Brunner nel romanzo "Codice 4GH" descrive programmi chiamati "tapeworms", che attaccano la rete con lo scopo di cancellare tutti i dati. Nel 1973 la frase "virus del computer" è usata nel film "Il mondo dei robot". 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.

Un programma chiamato "Elk Cloner" è accreditato come il primo virus per computer al mondo. Fu creato nel 1982 da Rich Skrenta sul DOS 3.3 della Apple e l'infezione era propagata mediante lo scambio di floppy disk, che rappresentò, nel corso degli anni ottanta, la modalità prevalente del contagio da virus informatici. Dalla metà degli anni novanta, con la diffusione di internet, virus e malware presero a diffondersi più velocemente, usando la rete e lo scambio di e-mail come mezzo per nuove infezioni. Il bersaglio preferito di questi software sono prevalentemente le varie versioni di Microsoft Windows.

Il primo virus informatico di fama mondiale fu creato nel 1986 da due fratelli pakistani, per punire chi copiava illegalmente il loro software. Il virus si chiamava Brain, ebbe diffusione planetaria, e fu il primo esempio di virus che infettava il settore di avvio.

Il primo file infector apparve nel 1987. Si chiamava Lehigh ed infettava solo il file COMMAND.COM. Nel 1988 Robert Morris Jr. creò il primo worm della storia. L'anno seguente fecero la loro comparsa i primi virus polimorfi, tra i più famosi Vienna, e venne diffuso il trojan AIDS (conosciuto come Cyborg), molto simile a PGPCoder, un trojan dei giorni nostri (2005): entrambi codificano i dati del disco fisso chiedendo poi un riscatto all'utente per poter recuperare i dati.



Nel 1995 compaiono i macro virus, virus scritti nel linguaggio di scripting di Microsoft che infettano, soprattutto, le varie versioni dei programmi Microsoft attraverso lo scambio di documenti. Concept fu il primo macro virus della storia. Nel 1998 nasce un altro virus storico: 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 Internet alla fine degli anni 90 determina la modifica delle tecniche di propagazione virale mediante 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. Nel 2000 il famoso I Love You inaugura il periodo degli script virus, i più insidiosi tra i virus diffusi attraverso la posta elettronica, perché sfruttano la possibilità, offerta da diversi client di posta, di eseguire istruzioni attive (dette script), contenute nelle email scritte in HTML, per svolgere azioni potenzialmente pericolose sul computer del destinatario. Gli script virus sono tra i più pericolosi perché possono attivarsi autonomamente non appena il messaggio viene aperto per la lettura. I Love You si diffuse in milioni di computer di tutto il mondo; per l'arresto del suo creatore, un ragazzo Filipino, intervenne una squadra speciale dell'FBI: si trattava di un messaggio email contenente un piccolo programma che istruiva il computer a inoltrare il messaggio appena arrivato a tutti gli indirizzi contenuti nella rubrica della vittima, generando, in tal modo, una catena di Sant'Antonio automatica che mandava in tilt i server di posta.

Dal 2001 un incremento di worm che si diffondono senza bisogno dell'intervento dell'utente, sfruttando le falle di programmi o sistemi operativi. Nel 2003 SQL/Slammer si rivela il più rapido worm della storia. In quindici minuti dopo il primo attacco, Slammer aveva già fatto infettare metà dei server che tenevano in piedi internet, mandando in tilt i bancomat della Bank of America e spegnendo il servizio di emergenza 911 a Seattle. Nel 2004 fanno la loro comparsa i due worm più famosi della storia: Blaster e Sasser.

Ogni sistema operativo che permette l'esecuzione di programmi scritti da terzi è un potenziale sistema attaccabile da virus, bisogna, tuttavia, riconoscere che ci sono sistemi operativi meno sicuri di altri. I sistemi operativi Microsoft risultano i più colpiti dai virus (anche a causa della loro diffusione tra un pubblico di "non addetti ai lavori"), anche se esistono virus per altre piattaforme. Si deve, inoltre, sottolineare che sui sistemi basati sul progetto GNU e su MacOSX la diffusione di un virus è molto improbabile, se il sistema è gestito correttamente dal proprietario; inoltre, su questi sistemi un virus molto difficilmente può riuscire a causare danni al sistema operativo.