

Minacce informatiche

dalla A alla Z



SOPHOS

Minacce informatiche

dalla **A** alla **Z**

Questo opuscolo si rivolge a chi amministra le reti informatiche, utilizza il computer per lavoro o semplicemente naviga in Internet. Descrive con un linguaggio chiaro e comprensibile le minacce informatiche, come virus, worm, spyware, spam.

Sophos è leader mondiale nella fornitura di soluzioni per la gestione integrata dei pericoli informatici per aziende, pubblica amministrazione e settore education. I suoi prodotti neutralizzano minacce conosciute e sconosciute come malware, spyware, intrusioni, applicazioni indesiderate, spam e violazioni delle politiche di sicurezza aziendali. Le soluzioni di Sophos, altamente affidabili e facili da utilizzare, proteggono oltre 35 milioni di utenti in più di 150 Paesi. Con 20 anni di esperienza e una rete globale di centri di analisi delle minacce, l'azienda è in grado di rispondere velocemente ai pericoli emergenti, indipendentemente dalla complessità, raggiungendo i massimi livelli di soddisfazione del cliente nel settore.

Sommario

Introduzione	4
Minacce dalla A alla Z	6
Software di protezione	75
Consigli generali	83
La “cronologia” dei virus	96

Copyright 2006 Sophos Group. Tutti i diritti riservati.
Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la registrazione o altri mezzi, senza previa autorizzazione scritta del titolare dei diritti d'autore.

Sophos e Sophos Anti-Virus sono marchi commerciali o registrati di Sophos Plc e Sophos Group. Tutti i nomi di marchi, prodotti e aziende sono marchi registrati appartenenti ai rispettivi detentori.

ISBN 0-9553212-0-4

ISBN 978-0-9553212-0-7

Introduzione

Tutti conosciamo i virus informatici... o meglio, pensiamo di conoscerli.

Il primo virus informatico è stato scritto circa vent'anni fa apparentemente con lo scopo di evitare la duplicazione illegale di un software salvato su floppy disk. A partire da quel momento, si sono diffuse centinaia di migliaia di virus e di malware - software inviati per e-mail, via Internet, Trojan, keystroke logger - alcuni con effetti devastanti in tutto il mondo. Molti hanno sentito parlare di virus che fanno apparire messaggi fastidiosi sullo schermo oppure cancellano i documenti salvati sul disco rigido. Nell'immaginario collettivo, il termine virus è ancora associato allo scherzo o al sabotaggio. Gli anni Novanta sono stati caratterizzati da un'ondata di panico scatenata dal virus Michelangelo, ormai dimenticato da tempo. I primi anni del 2000 hanno visto protagonista il virus SoBig-F programmato per far scaricare a milioni di computer, automaticamente e contemporaneamente dalla rete, programmi sconosciuti. Per scongiurare scenari apocalittici le aziende produttrici di software antivirus hanno cercato in tutti i modi di convincere gli internet provider a spegnere i server. Film come Independence Day e The Net - Intrappolata Nella Rete hanno contribuito a rafforzare questa convinzione di attacchi informatici rappresentati da schermi e allarmi lampeggianti.

Questo non è quello che accade nella realtà quotidiana. Le minacce sono comunque reali, ma mantengono un basso profilo e vengono utilizzate soprattutto per scopi di lucro, non per generare confusione.

Oggi è difficile che i malware cancellino il vostro hard disk, danneggino i vostri fogli elettronici o facciano apparire un messaggio. Questo tipo di "cyber-vandalismo" ha dato vita a minacce più proficue. I virus sviluppati oggi potrebbero codificare i vostri file e poi chiedervi un "riscatto" per poterli riaprire. Oppure un hacker potrebbe minacciare una grande azienda con un attacco di tipo DoS ("denial of service" ovvero "negazione di servizio") che impedirebbe ai clienti di accedere al sito Web.

Di solito i virus non provocano danni evidenti o addirittura non si manifestano in alcun modo. Invece, potrebbero installare, a vostra insaputa, un programma in grado di registrare le digitazioni dell'utente (keystroke logger) per memorizzare dati personali e password. Queste informazioni, spesso utilizzate per accedere ai siti delle banche, vengono inoltrate all'hacker sempre via Internet. Lo scopo ultimo di questa azione è quello di clonare carte di credito o appropriarsi del denaro depositato sul conto. Spesso, la vittima non sa nemmeno che il proprio computer è stato infettato. Una volta che il virus ha raggiunto il suo obiettivo, potrebbe autodistruggersi per evitare di essere individuato.

Un'altra tendenza è quella di utilizzare un mix di tipologie diverse di malware o metodi di hacking. Un creatore di virus potrebbe utilizzare la lista di indirizzi mail di uno spammer per inviare un programma Trojan ed essere sicuro della diffusione rapida della sua minaccia. Questo tipo di tecnica può favorire anche gli spammer. Virus e Trojan sono in grado di controllare a distanza numerosi computer, trasformandoli in "zombie" per distribuire posta commerciale non richiesta (spam).

Gli hacker non puntano più a colpire un grande numero di persone. Gli attacchi spettacolari suscitano grande clamore e richiamano l'attenzione delle aziende che producono software antivirus, che riescono a neutralizzare velocemente eventuali malware diffusi in massa. Inoltre una minaccia su larga scala metterebbe a disposizione degli hacker più dati di quelli che in realtà sono in grado di gestire. Per questo motivo le minacce informatiche hanno un obiettivo sempre più preciso. Lo "spear phishing" è un esempio. Il "phishing" è l'uso di e-mail e di siti falsificati per indurre il maggior numero di persone a fornire, con l'inganno, informazioni confidenziali o personali che vengono poi utilizzate per altri scopi. Il messaggio contiene generalmente un link al sito web di una banca. Lo "spear phishing", nuova versione di questo tipo di frode, consiste in un attacco tramite posta elettronica inviato soltanto a un gruppo ristretto di persone, di solito appartenenti alla medesima organizzazione. La struttura del messaggio potrebbe lasciare intendere che sia stato inviato da un collega a tutti gli altri componenti della società, con la richiesta di fornire nomi utente e password. Il principio è lo stesso, ma in questo caso sussistono maggiori probabilità di successo, dato che la vittima è portata a pensare che si tratti di un messaggio interno all'azienda e quindi il suo livello di attenzione diminuisce.

Insidiose, su piccola scala, con obiettivi mirati: sembrano essere queste le caratteristiche delle minacce informatiche moderne.

E in futuro che cosa accadrà? Cercare di capire in quale modo si evolveranno le minacce nei prossimi anni è quasi impossibile. Alcuni esperti hanno affermato che ci saranno solo poche centinaia di virus e Bill Gates, fondatore e presidente di Microsoft, ha dichiarato che entro il 2006 lo spam non sarà più un problema. Ad ogni modo non è chiaro prevedere la gravità e la provenienza delle minacce del futuro. Se esiste un'opportunità di guadagno, i pirati informatici cercheranno sempre di coglierla, provando a impossessarsi di dati privati. Questa è l'unica certezza.

A

=

Z



Adware

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

L'adware (in inglese, contrazione di “advertising-supported software”, ovvero “software sovvenzionato da pubblicità”) mostra messaggi pubblicitari (banner o finestre pop-up) direttamente sullo schermo dell'utente quando viene utilizzata l'applicazione. Non si tratta necessariamente di un'azione dannosa. Queste pubblicità possono finanziare lo sviluppo di programmi utili che vengono poi distribuiti gratuitamente (ad esempio, il browser Opera).

In ogni caso, l'adware può rappresentare una minaccia se:

- si installa direttamente sul computer senza il consenso dell'utente.
- si installa in applicazioni diverse da quelle di origine e fa apparire messaggi pubblicitari durante l'utilizzo di tali applicazioni.
- cambia le impostazioni del browser per scopi pubblicitari (vedi **Browser hijacker**).
- raccoglie informazioni riservate riguardanti l'attività online di un utente senza il suo consenso, trasmettendole via Internet ad altri utenti (vedi **Spyware**).
- è difficile da disinstallare.

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

Inoltre le finestre pop-up distraggono l'utente, facendogli sprecare tempo visto che è costretto a chiuderle tutte prima di proseguire la navigazione.

Alcuni software antivirus sono in grado di individuare gli adware e classificarli come “applicazioni potenzialmente indesiderate”. Sta all'utente decidere se autorizzare la presenza dell'adware oppure rimuoverlo dal proprio computer. Esistono anche programmi specifici per la rimozione degli adware.



Backdoor Trojans

Un backdoor Trojan è un programma che consente di prendere il controllo del computer di un utente senza il suo consenso tramite una connessione internet.

Un backdoor Trojan può sembrare un software apparentemente innocuo, come gli altri Trojan, in modo che venga eseguito senza alcun sospetto. Sempre più spesso, gli utenti possono diventare vittime di un Trojan semplicemente cliccando sul link contenuto in una spam.

Una volta eseguito, il Trojan si aggiunge alla routine di avvio del computer. Quindi può monitorare il PC finché l'utente non si collega a Internet. Una volta eseguita la connessione Internet, la persona che ha inviato il Trojan può eseguire programmi sul computer infetto, accedere ai file personali, modificare e caricare file, registrare le digitazioni dell'utente sulla tastiera oppure inviare spam.

Tra i backdoor Trojan più noti figurano **Subseven**, **BackOrifice** e **Graybird**, che si spacciava come rimedio contro il famigerato worm **Blaster**.

Per evitare i backdoor Trojan dovrete tenere sempre aggiornato il vostro sistema operativo con le ultime patch disponibili (per ridurre le vulnerabilità del sistema) e utilizzare software antivirus e antispam. Dovreste attivare anche un firewall, che impedisce ai Trojan di accedere a Internet per mettersi in contatto con il loro hacker.

Bluejacking

Il bluejacking consiste nell'invio di messaggi anonimi e indesiderati a utenti che utilizzano cellulari o computer portatili dotati di tecnologia Bluetooth.

Il Bluejacking sfrutta la tecnologia Bluetooth per individuare ed entrare in contatto con altri dispositivi nelle vicinanze. L'hacker utilizza una funzionalità originariamente sviluppata per scambiare le informazioni sui contatti in forma di "biglietti da visita elettronici". Il pirata aggiunge un nuovo contatto nella rubrica, digita un messaggio e sceglie di inviarlo via Bluetooth. Il telefono cellulare cerca altri dispositivi Bluetooth disponibili e, appena ne individua uno, invia il messaggio.

Il Bluejacking non è particolarmente pericoloso. Non vengono infatti sottratti dati personali e non si perde il controllo del proprio telefono.

Il Bluejacking può essere fastidioso se viene utilizzato per inviare messaggi osceni e minacce, o per scopi pubblicitari. Per evitare questo tipo di messaggi, è sufficiente disattivare il Bluetooth oppure utilizzarlo in modalità "invisibile".

I dispositivi attivi possono essere esposti a minacce molto più serie come il Bluesnarfing.



Bluesnarfing

Il Bluesnarfing consiste nella sottrazione dei dati presenti su un telefono cellulare provvisto di tecnologia Bluetooth.

Proprio come il Bluejacking, il Bluesnarfing sfrutta la tecnologia Bluetooth per individuare ed entrare in contatto con altri dispositivi nelle vicinanze.

In linea teorica, un pirata provvisto di un computer portatile con il software adatto è in grado di individuare un cellulare nelle vicinanze e, senza il consenso dell'utente, scaricare informazioni riservate come la rubrica, le immagini dei contatti e l'agenda.

Anche il numero seriale del telefono cellulare può essere letto e utilizzato per operazioni di clonazione.

Si raccomanda pertanto di disattivare il dispositivo Bluetooth oppure utilizzarlo in modalità "invisibile". La modalità "invisibile" permette infatti di continuare a utilizzare dispositivi Bluetooth come l'auricolare senza che il telefono risulti visibile ad altri.



Boot virus o virus del settore di avvio

I boot virus si diffondono modificando il programma di avvio del computer.

All'accensione del computer, l'hardware cerca il boot sector, o settore di avvio, sull'hard disk (ma può anche trattarsi di un floppy o un CD), ed esegue il programma di avvio del sistema. Questo programma carica l'intero sistema operativo in memoria.

Un boot virus sostituisce il boot sector originale con una versione modificata (e normalmente nasconde l'originale in un'altra sezione del disco rigido). All'avvio viene così utilizzato il boot sector modificato e il virus diventa attivo.

Il computer può essere infettato solo se viene avviato da un disco infetto, ad esempio un floppy disk con boot sector infetto.

I boot virus sono stati i primi virus utilizzati e sono ormai superati, tanto che oggi si incontrano molto raramente.



Browser hijacking o “dirottamento” del browser

I browser hijacker modificano la pagina iniziale e le pagine di ricerca del programma di navigazione.

Alcuni siti web contengono uno script che modifica le impostazioni del browser di navigazione senza il consenso dell'utente. Questi software di “dirottamento” possono aggiungere nuovi collegamenti nella cartella “Preferiti” o, ancora peggio, possono cambiare la pagina iniziale che appare quando si lancia il browser.

In alcuni casi risulta impossibile reimpostare la pagina iniziale su quella prescelta. Alcuni browser hijacker modificano infatti il registro di Windows in modo che le impostazioni di “dirottamento” vengano ripristinate ogni volta che si riavvia il computer. Altri eliminano la voce Opzioni dal menu “Strumenti” del browser, impedendo all'utente di reimpostare la pagina iniziale.

In ogni caso, lo scopo è identico: obbligare l'utente a visitare un determinato sito Internet. Queste procedure “gonfiano” il numero di visite e il sito sale nelle classifiche dei motori di ricerca, aumentando il grado di visibilità e gli introiti pubblicitari.

Questi software di dirottamento possono essere molto resistenti. Alcuni vengono rimossi in maniera automatica dai software di sicurezza, altri invece devono essere eliminati manualmente. In alcuni casi è più semplice reinstallare il sistema operativo o riportarlo a un punto di ripristino precedente all'infezione.



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. Le tipologie principali sono:

- Gli "hoax", ovvero falsi allarmi su potenziali attacchi terroristici, numeri telefonici a tariffa maggiorata, furti ai Bancomat ecc.
- False dichiarazioni di aziende che offrono gratuitamente voli aerei, telefoni cellulari o ricompense in denaro se si inoltra il messaggio in questione.
- Messaggi che sembrano provenire da organizzazioni come la CIA o l'FBI che avvertono della presenza di pericolosi criminali nella vostra zona.
- Petizioni e richieste di carattere umanitario, magari autentiche, ma che continuano a circolare a lungo anche quando viene a cessare la loro utilità.
- Scherzi di vario genere, ad esempio il messaggio che affermava che il servizio Internet sarebbe stato sospeso il primo di Aprile.

Le catene di Sant'Antonio non rappresentano una minaccia alla sicurezza, ma causano sprechi di tempo, diffondono informazioni non corrette e sviano l'attenzione degli utenti.

Possono anche generare traffico inutile, rallentando i server di posta. In alcuni casi invitano le persone a inviare messaggi e-mail a indirizzi precisi, così che questi destinatari vengono sommersi da posta indesiderata.

La soluzione per bloccare le catene di Sant'Antonio è molto semplice: non inoltrate il messaggio.



Cookie

I cookie sono file che permettono a un sito Web di registrare le visite e memorizzare i dati degli utenti.

Quando si visitano alcuni siti internet, viene installato sul computer un piccolo pacchetto dati chiamato cookie. I cookie consentono al sito di memorizzare i dati dell'utente e di tenere traccia delle visite. Questi file non rappresentano una minaccia per i dati, ma possono violare la privacy degli utenti.

I cookie sono stati progettati in origine per facilitare alcune operazioni. Ad esempio, se dovete identificarvi quando visitate un sito, il cookie vi permette di salvare queste informazioni in modo tale da non doverle inserire ogni volta. Possono rappresentare un aiuto per i webmaster, poiché indicano quali pagine vengono utilizzate e quindi forniscono dati utili quando si deve rinnovare un sito.

I cookie sono piccoli file di testo e non danneggiano i dati presenti sul computer. Tuttavia possono violare la privacy. Infatti vengono immagazzinati automaticamente sul computer dell'utente senza il suo consenso e contengono informazioni difficilmente accessibili da parte della vittima. Quando si accede nuovamente al sito interessato, questi dati vengono inviati al web server, sempre senza autorizzazione.

I siti Internet riescono in questo modo a creare un profilo degli utenti e dei loro interessi. Queste informazioni possono essere vendute o condivise con altri siti e permettono a chi fa pubblicità di sponsorizzare prodotti che interessano l'utente, di visualizzare banner mirati e di contare quante volte viene visualizzato un determinato annuncio pubblicitario.

Se preferite restare anonimi, dovete modificare le impostazioni di sicurezza del browser disabilitando i cookie.

Denial-of-service Attacco DoS

Un attacco DoS (Denial-of-service, letteralmente “negazione del servizio”) impedisce agli utenti di accedere a un computer o sito Internet.

In un attacco DoS, un hacker tenta di sovraccaricare o spegnere un computer per impedire l’accesso agli utenti. Solitamente gli attacchi DoS sono diretti ai Web server e hanno lo scopo di rendere inaccessibili i siti Web che girano su questi server. Nessun dato viene sottratto o danneggiato, ma l’interruzione del servizio può infliggere danni considerevoli alle aziende.

La strategia più comune per effettuare un attacco Dos consiste nel generare un traffico più intenso di quello che il computer riesce a gestire. I metodi più rudimentali si basano sull’invio di pacchetti di dati molto pesanti o messaggi di posta elettronica con allegati che hanno nomi più lunghi di quelli gestiti dai programmi di posta.

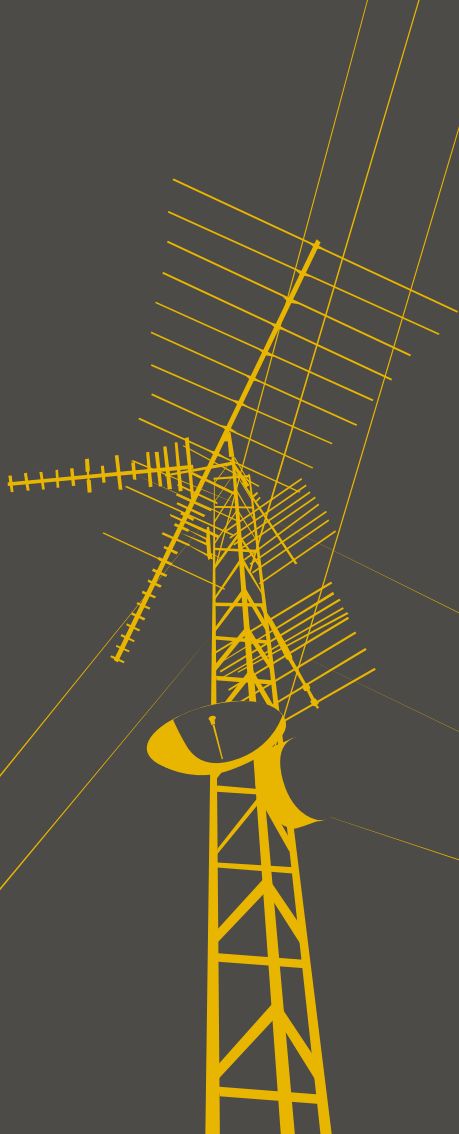
L’attacco può anche sfruttare il modo in cui viene instaurata la “sessione” di comunicazione quando l’utente entra in contatto con il computer. Se l’hacker richiede l’apertura di numerose connessioni e poi ignora la risposta del server, le richieste vengono lasciate nel buffer per un certo periodo. In questo modo le richieste degli utenti “veri” non possono essere elaborate e quindi risulta per loro impossibile contattare il computer.

Un altro metodo consiste nell’inviare un messaggio “IP ping” (messaggi che richiedono una risposta da altri computer) che sembra provenire dal computer della vittima. Il messaggio viene inoltrato a un numero elevato di computer e tutti forniscono la propria risposta. La vittima viene così “inondata” dalle risposte e il computer non è più in grado di gestire il traffico.

Il **DDoS (Distributed Denial of Service)** utilizza molti computer per sferrare l’attacco. Solitamente gli hacker infettano un numero elevato di computer con virus o Trojan che aprono delle “backdoor” attraverso le quali riescono ad assumere il controllo delle macchine. Questi computer “zombie” vengono quindi utilizzati per lanciare un attacco DoS coordinato.

Vedi **Backdoor Trojan, Zombie**.





Dialer

I dialer cambiano il numero telefonico della connessione Internet, sostituendolo con un servizio a pagamento.

I dialer non sono sempre illegali. Alcune aziende richiedono legalmente di scaricare prodotti o giochi collegandosi a un numero di telefono a tariffa maggiorata. Una finestra di pop-up invita l'utente a scaricare il dialer e lo informa del costo della chiamata.

Altri dialer, invece, si installano automaticamente senza alcuna autorizzazione quando cliccate su un pop-up (ad esempio un messaggio che vi avverte della presenza di virus sul vostro computer e che vi offre una soluzione). Questi programmi non offrono nessun servizio: semplicemente cambiano i parametri della connessione Internet, dirottandola su un numero a pagamento.

Chi ha una connessione a banda larga non corre rischi anche se si installa un dialer. Infatti la banda larga non utilizza i normali numeri telefonici e gli utenti, di solito, non sono connessi alla rete tramite un modem tradizionale.

I software antivirus sono in grado di individuare ed eliminare i Trojan che installano i dialer.

hoax

Gli hoax sono falsi allarmi su virus inesistenti.

Solitamente gli hoax sono messaggi di posta elettronica che si comportano, in tutto o in parte, in uno dei seguenti modi.

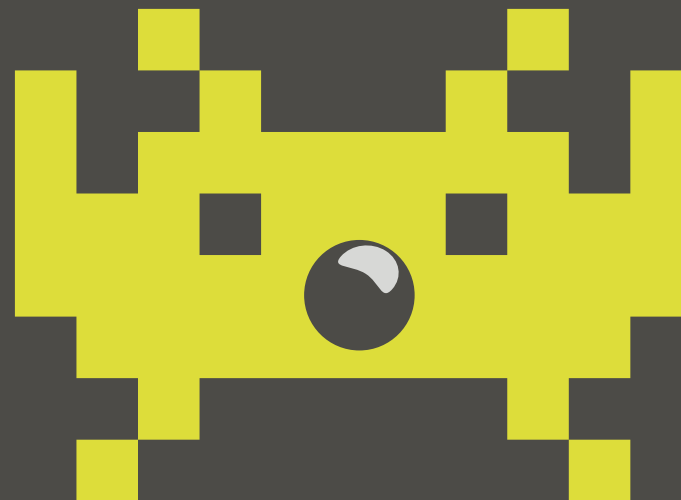
- Segnalano la presenza di un virus altamente distruttivo che non può essere rilevato.
- Chiedono di non leggere messaggi di posta elettronica con un determinato oggetto, ad esempio “Budweiser Frogs”.
- Fanno credere che l’avvertimento provenga da un grande produttore di software, da un Internet Provider o da un’agenzia governativa, ad esempio IBM, Microsoft e AOL.
- Fanno credere che il nuovo virus possa fare qualcosa di assolutamente improbabile. Ad esempio, il falso allarme “A moment of silence” sosteneva che non era necessario alcun trasferimento di file affinché un nuovo computer venisse infettato.
- Usano il gergo tecnologico per descrivere gli effetti del virus. Ad esempio, “Good Times” afferma che il virus può portare il processore in “un ciclo binario infinito di ennesima complessità”.
- Spingono l’utente a inoltrare l’avvertimento.

Se gli utenti inoltrano effettivamente un falso allarme a tutti gli amici e colleghi, può generarsi una valanga di e-mail, con il conseguente sovraccarico e crash dei server di posta. L’effetto è identico al virus Sobig, con la differenza che l’hoaxer non ha avuto bisogno di scrivere neppure una riga di codice.

Tutto nasce solo per un eccesso di reazione da parte degli utenti. Le aziende che ricevono questi falsi allarmi spesso prendono contromisure drastiche, chiudendo ad esempio il server di posta o l’intera rete. Questi attacchi sono ancora più efficaci dei virus veri e propri in termini di danno alle comunicazioni, perché impediscono l’accesso a messaggi che possono essere importanti.

I falsi allarmi distolgono inoltre l’attenzione dai virus veri e propri.

Gli hoax possono avere anche una lunga durata. Poiché non si tratta di virus, il software antivirus non è in grado di individuarli né di neutralizzarli.



Internet worm

I worm sono programmi che si replicano e si diffondono attraverso le connessioni Internet.

I worm si differenziano dai virus perché sono in grado di replicarsi e non hanno bisogno di un programma o di un documento che li ospiti. Creano semplicemente copie esatte di se stessi e utilizzano le connessioni Internet per diffondersi.

Gli internet worm possono propagarsi da un computer all'altro sfruttando le "falle" di sicurezza presenti nel sistema operativo. Il worm Blaster, per esempio, sfrutta una vulnerabilità insita nel servizio di chiamata di procedura remota (RPC - Remote Procedure Call) dei sistemi operativi Windows NT, 2000 e XP e si "autoinvia" ad altri computer.

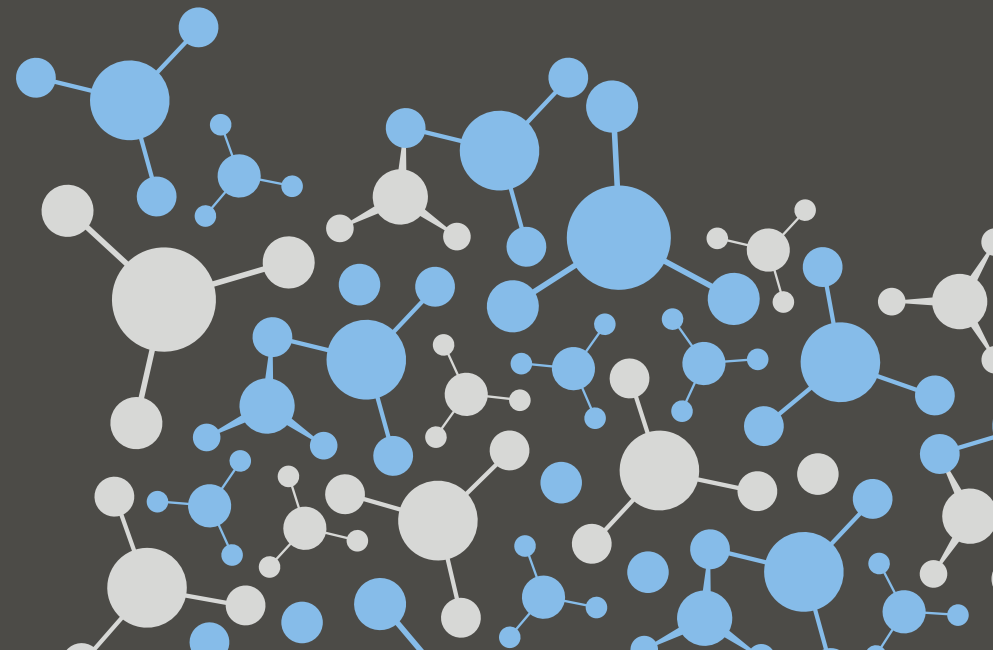
Molti virus odierni come MyDoom o Bagle si comportano esattamente come i worm e utilizzano la posta elettronica per propagarsi.

I worm possono produrre effetti negativi. Ad esempio, possono utilizzare i computer infetti per creare un enorme volume di traffico attraverso un attacco di tipo DoS (Denial-of-service) e danneggiare specifici siti Web sommergendoli di richieste o di dati. Oppure potrebbero codificare i file dell'utente in modo tale da renderli inutilizzabili. Entrambe le procedure permettono di ricattare le aziende colpite.

Diversi worm aprono una "backdoor" che consente agli hacker di assumere il controllo dei computer. Le macchine infette possono quindi essere utilizzate per distribuire spam (vedi Zombie).

Oltre a questi effetti, i worm sono in grado di rallentare le comunicazioni generando un enorme volume di traffico su Internet. E' il caso del worm Blaster che si diffonde sulla rete e intensifica il traffico, rallentando le comunicazioni e causando il crash dei computer. Questa particolare minaccia, inoltre, usa il computer infetto per sommergere di dati un sito Web di Microsoft allo scopo di renderlo inaccessibile.

Microsoft, così come altre aziende che forniscono sistemi operativi, rilascia delle patch per correggere le vulnerabilità presenti nel sistema di sicurezza. Ogni utente dovrebbe visitare regolarmente i siti dei produttori di software per aggiornare il proprio PC con le ultime patch disponibili.





“Mousetrapping”

Il “mouse-trapping” impedisce all’utente di uscire da un determinato sito Internet.

Se venite indirizzati su un falso sito Web, vi potrebbe capitare di non essere più in grado di uscire utilizzando il pulsante Indietro del browser o Chiudi della finestra. In alcuni casi, anche se si digita un nuovo indirizzo Internet nell’apposita barra, non si riesce comunque a uscire dalla “trappola”.

Il sito che vi cattura potrebbe impedirvi di visitare altri indirizzi oppure aprire un’altra finestra nella quale viene visualizzata la stessa pagina. In alcuni casi l’utente, dopo molti tentativi, riesce a uscire, ma a volte non c’è via di scampo.

Per sfuggire alla trappola, selezionate un indirizzo dall’elenco “Preferiti” (o Segnalibri) oppure aprite la Cronologia e cliccate sul penultimo indirizzo visitato. Potete anche digitare Ctrl+Alt+Canc e utilizzare Task Manager per terminare il browser oppure, in caso non fosse possibile, riavviare il computer.

Per evitare i pericoli del “mouse-trapping” è consigliabile disattivare l’esecuzione dei Javascript nel browser Internet. Questo accorgimento permette di aumentare la sicurezza evitando l’esecuzione di questi script, ma influisce anche sulla visualizzazione e sulla funzionalità dei siti Internet.



“Page-jacking”

Con il termine “page-jacking” si intende l’uso di repliche di pagine Web molto visitate per “dirottare” gli utenti su altri siti Internet.

I “page-jacker” copiano le pagine da un sito Web noto e le inseriscono in un nuovo sito che sembra essere autentico, quindi registrano questo nuovo sito sui principali motori di ricerca in modo che gli utenti vengano indirizzati sul sito creato ad hoc. Quando l’utente accede al sito Web, viene automaticamente indirizzato su un altro sito che contiene pubblicità od offerte di servizi diversi da quelli ricercati. Alcuni siti potrebbero addirittura impedire all’utente di uscire dal sito senza prima riavviare il computer (vedi “**Mouse-trapping**”).

Il “page-jacking” viene utilizzato per aumentare il numero di visitatori di un sito. In questo modo il sito acquisisce maggiori introiti pubblicitari e assume più valore nel caso dovesse essere venduto. Oppure, il pirata informatico può reindirizzare i visitatori su un determinato sito e chiedere un compenso per averli “dirottati”.

Il fenomeno del “page-jacking” è molto fastidioso e, a volte, pone l’utente davanti a materiale e immagini sgradevoli. Inoltre riduce il fatturato dei siti originali e ridimensiona l’utilità dei motori di ricerca.

In alcuni casi, il “page-jacking” può essere utilizzato per il **phishing**.

Per evitare il fenomeno del “page-jacking” si consiglia di utilizzare i link nella lista dei “Preferiti” (o segnalibri), ma bisogna essere certi di non aver salvato il sito incriminato all’interno della lista. In alternativa, potete digitare l’indirizzo del sito Web direttamente nell’apposita barra (URL).

“Pharming” (manipolazione di indirizzi web)

Il termine “pharming” indica il reindirizzamento del traffico su Internet da un sito Web a un altro del tutto identico, ma creato per frodare gli utenti e persuaderli a inserire dati sensibili nel database del sito falsificato.

Il “pharming” manipola la struttura degli indirizzi internet.

Ogni computer collegato alla rete internet ha un indirizzo IP numerico, ad esempio 127.0.0.1. Tuttavia non è semplice ricordarlo. Per questo motivo gli indirizzi Web dispongono anche di una sigla alfanumerica, il dominio, come sophos.com. Ogni volta che un utente digita nel proprio browser l'indirizzo di una pagina web, questo viene tradotto automaticamente in un indirizzo IP. Il server DNS (Domain Name Server) gestisce tale conversione, a meno che un “file host” nel computer dell'utente non abbia già effettuato l'operazione.

Gli hacker possono sconvolgere questo processo seguendo due metodologie di attacco. Possono utilizzare programmi Trojan che modificano i file host direttamente nel computer dell'utente, in modo tale che associno il nome del dominio con il sito web falsificato. In questo modo l'utente viene indirizzato sul sito clonato anche se digita correttamente l'indirizzo. In alternativa gli hacker possono operare delle variazioni nelle directory dei server DNS, modificando gli abbinamenti. Gli utenti connessi, pur digitando il corretto indirizzo, verranno inconsapevolmente rindirizzati a un sito trappola.

Per evitare il fenomeno del “pharming”, assicuratevi che la connessione sia protetta. Ovviamente prima di inserire dati sensibili. Basta controllare il prefisso `https://` nell'indirizzo Web. Se un hacker clona un sito protetto, un messaggio vi avvertirà che il certificato del sito non corrisponde all'indirizzo che state visitando.

Se i messaggi indicano che il certificato non è valido oppure non è rilasciato da fonte affidabile, non dovrete accedere al sito.

Esistono anche soluzioni software. Alcuni programmi avvertono l'utente nel caso in cui inserisca informazioni personali rispondendo a un messaggio di posta sconosciuto. Altre utility sono in grado di verificare se i siti internet o gli indirizzi IP sono validi o potenzialmente pericolosi.



“Phishing”

Il “phishing” consiste nell’uso di e-mail e di falsi siti Web per indurre gli utenti con l’inganno a fornire informazioni confidenziali o personali.

Solitamente l’utente riceve una e-mail che sembra provenire da una società rispettabile, ad esempio una banca. Il messaggio contiene quello che pare essere il link al sito Internet dell’azienda. Tuttavia, se si seleziona il collegamento, l’utente viene reindirizzato su un sito fittizio. Tutti i dati inseriti, come numeri di conto, PIN o password, possono essere sottratti e utilizzati dagli hacker che hanno creato la replica del sito.

A volte il collegamento è diretto al sito originale, ma viene nascosto da una finestra di popup sovrapposta.

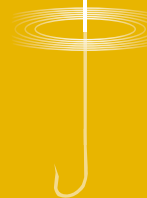
In questo modo l’utente visualizza l’indirizzo del sito originale sullo sfondo, ma le informazioni vengono inserite nella finestra di popup e quindi vengono rubate.

Talvolta gli hacker utilizzano una tecnica chiamata “cross-site scripting”: Il collegamento porta al sito autentico, ma i contenuti vengono gestiti da fonti inaffidabili. Ancora una volta, la parte del sito nella quale vengono inserite le informazioni viene gestita dagli hacker.

Il fenomeno del “phishing” è iniziato negli anni Novanta. I truffatori utilizzavano questa tecnica per rilevare le informazioni relative agli utenti di AOL al fine di accedere ai servizi Internet gratuitamente. Le informazioni sottratte erano chiamate “phish” perché venivano “pescate” in seguito alla digitazione dell’utente (“fish” in inglese significa “pesce”). La grafia “ph” rimanda alla parola “phreaker”, termine utilizzato per indicare coloro che compiono operazioni illecite sulla rete telefonica.

Bisogna prestare sempre attenzione ai messaggi di posta che utilizzano formule generiche, ad esempio “Gentile cliente” ed evitare di cliccare sui link contenuti nella mail. E’ consigliabile digitare l’indirizzo del sito nell’apposita barra per navigare all’interno della pagina autentica, oppure utilizzare un collegamento della lista “Preferiti” (o Segnalibri). Anche digitando l’indirizzo corretto, vi è il pericolo di essere indirizzati nuovamente sul sito fantasma (vedi **Pharming**), quindi è necessario prestare la massima attenzione.

I software antispam sono in grado di bloccare i tentativi di phishing tramite e-mail. Alcuni programmi riescono a individuare il contenuto potenzialmente pericoloso delle pagine Web o delle e-mail e forniscono una barra strumenti grazie alla quale è possibile verificare il dominio effettivo a cui si accedrebbe selezionando un determinato link.





Potentially unwanted applications (PUAs)

Applicazioni potenzialmente indesiderate

Potentially unwanted applications are programs that are not malicious but may be unsuitable on company networks.

Alcune applicazioni non rappresentano un pericolo e, in alcuni contesti, possono addirittura risultare utili, ma non nel caso delle reti aziendali. Ad esempio adware, dialer, spyware non malevoli, strumenti per amministrare il PC da remoto e strumenti di hacking.

Alcuni software antivirus sono in grado di rilevare tali applicazioni sul computer dell'utente, presentando un rapporto di scansione. L'amministratore può decidere se autorizzare l'applicazione o rimuoverla completamente dal PC.



“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”. Il Trojan **Archiveus**, ad esempio, 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 verrà comunicata solo dopo aver effettuato un acquisto da una farmacia on-line.

In questo caso, come nella maggior parte dei “ransomware”, la password è nascosta all’interno del codice del Trojan e può essere rilevata dagli analisti di virus. Tuttavia, in futuro, gli hacker potrebbero utilizzare una crittografia asimmetrica o a chiave pubblica che sfrutta codici diversi per codificare e decodificare, in maniera tale che la password non venga salvata sul computer dell’utente.

In alcuni casi è sufficiente la semplice minaccia di negazione dell’accesso. Il Trojan **Ransom-A**, ad esempio, minaccia l’utente comunicandogli che ogni 30 minuti sarà cancellato un file finché non verrà acquistato il “codice di sblocco” tramite Western Union. Se viene digitata una password errata, il Trojan avvisa che il computer andrà in crash dopo tre giorni. Ad ogni modo, le minacce non sono reali, dato che **Ransom-A** non è in grado di effettuare queste operazioni.

“Rootkit”

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

Quando un software malevolo, come un worm, riesce ad accedere al computer dell'utente, può installare un rootkit. Questo codice viene utilizzato spesso per nascondere la presenza di applicazioni che permettono all'hacker di aprire delle “backdoor” grazie alle quali viene consentito l'accesso al computer. Le utility nascoste potrebbero addirittura permettere all'hacker di utilizzare funzioni che normalmente vengono eseguite da utenti con privilegi speciali. (Su computer UNIX e Linux, questi utenti vengono chiamati “root” e da questo deriva il nome “rootkit”).

Un rootkit può nascondere cosiddetti keystroke logger o password sniffer, cioè meccanismi che rilevano le digitazioni su tastiera e sottraggono password che inviano agli hacker via Internet. Inoltre permette anche all'hacker di eseguire operazioni illecite, come attacchi di tipo DoS contro altri computer o l'invio di spam: tutto senza il consenso dell'utente.

Anche se un rootkit viene installato senza cattive intenzioni (come nel caso di Digital Rights Management di Sony, un software utilizzato per impedire la copiatura pirata di CD musicali), può rendere il computer più vulnerabile agli attacchi informatici.

Rilevare un rootkit è difficile. Quando il rootkit viene attivato, non è possibile identificare in modo sicuro tutti i processi che vengono eseguiti dal computer o tutti i documenti nelle directory, quindi i software antivirus tradizionali potrebbero non rilevare la sua presenza. Il rootkit potrebbe anche sospendere la sua attività durante l'intera scansione. Un metodo sicuro per individuare la presenza di un rootkit è spegnere il computer, riavviarlo da un CD di ripristino e poi effettuare una scansione del sistema tramite un software antivirus. Il rootkit non è più attivo e quindi non è più in grado di nascondersi.



I software antivirus possono rilevare i Trojan o i worm che installano il rootkit e alcuni riescono a individuare direttamente il rootkit mentre è in funzione.

Spam

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

I tipi di spam più diffusi riguardano:

- farmaci con ricetta, farmaci che ingrandiscono o potenziano alcune parti del corpo, prodotti di erboristeria o cure dimagranti
- proposte di arricchimento facile e veloce
- servizi finanziari, ad esempio offerte di mutuo o proposte per ridurre i debiti
- titoli e qualifiche, ad esempio la possibilità di acquistare diplomi, lauree o titoli professionali
- casinò e gioco d'azzardo online
- software a prezzi stracciati o pirata.

A volte lo spam è “mascherato” da un oggetto con frasi molto personali, ad esempio “Scusa per ieri”, o un messaggio di tipo professionale come “Devi rinnovare il tuo account”, oppure una notifica di messaggio respinto.

Gli spammer spesso “truccano” le proprie mail per evitare i software anti-spam (vedi **Spam offuscato**).

L'invio di spam genera un guadagno per chi le spedisce. Gli spammer possono infatti distribuire milioni di e-mail con un unico invio a un costo trascurabile; se riescono a prendere il controllo di altri computer per la spedizione, il costo è ancora più basso. Se anche un solo destinatario su diecimila fa un acquisto, lo spammer ha ottenuto un guadagno.

Lo spam è un problema?

- Lo spam fa perdere tempo al personale. Gli utenti senza protezione anti-spam devono verificare ogni messaggio e cancellarlo.
- Gli utenti possono facilmente trascurare o cancellare messaggi importanti, scambiandoli per spam.
- Lo spam, come gli “hoax” allarmistici e i virus via mail, occupa larghezza di banda e intasano i database.
- Alcune messaggi spam sono offensivi. Il datore di lavoro può essere ritenuto responsabile, in quanto è tenuto a garantire un ambiente di lavoro equo e sicuro.
- Gli spammer usano spesso computer di altri utenti per inviare spam (vedi **Zombie**).



Spam offuscato

Lo spam offuscato è un messaggio di posta elettronica mascherato per sfuggire ai software antispam.

Gli spammer sono costantemente alla ricerca di nuovi metodi per camuffare i propri messaggi e aggirare i software antispam, arrivando direttamente all'utente.

L'esempio più semplice è costituito dall'aggiunta di alcuni spazi tra le lettere di una parola, nella speranza che il software antispam non legga le lettere come un'unica parola, ad esempio

V I A G R A

Un altro metodo diffuso è quello di utilizzare un'ortografia scorretta oppure caratteri non-standard, ad esempio

V!agra

Questi trucchi sono comunque facili da individuare.

I metodi più avanzati sfruttano il codice HTML (il linguaggio utilizzato per scrivere le pagine web) all'interno delle e-mail. Questo permette agli spammer di creare messaggi che vengono visualizzati in maniera diversa dai software antispam.

Una parola può essere scritta utilizzando uno speciale codice HTML per ogni lettera. Il termine "Viagra", per esempio, può essere scritto digitando

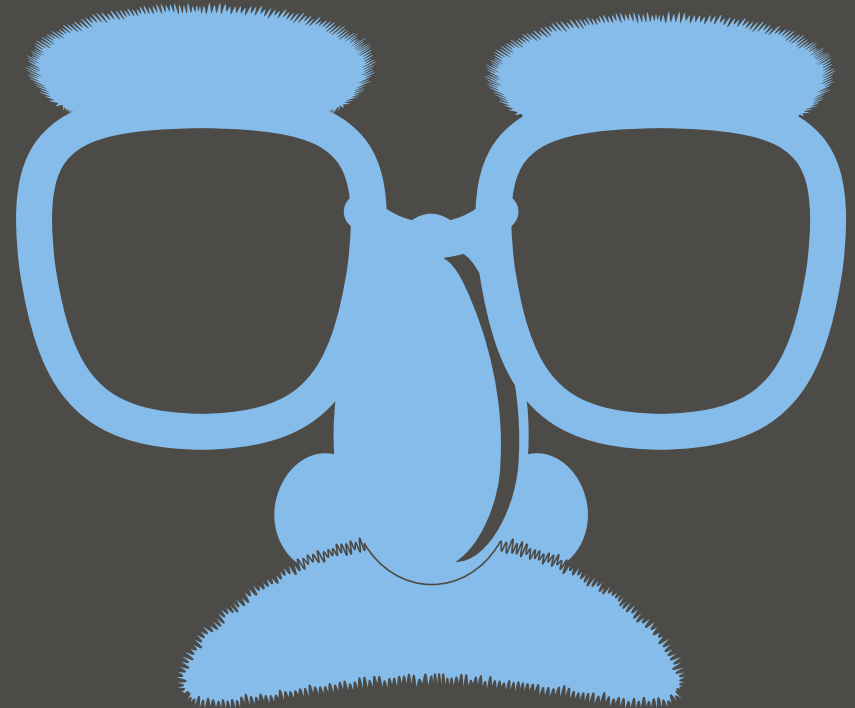
Viagra

Il linguaggio HTML permette all'utente di vedere un determinato messaggio, mentre il programma antispam ne vede un altro che appare innocuo. Il messaggio innocuo è dello stesso colore dello sfondo.

```
<body bgcolor=white> Viagra
```

```
<font color=white>Hi, Johnny! It was nice to have dinner with you. </font></body>
```

Gli spammer a volte inseriscono una porzione consistente di testo nascosto, spesso proveniente da guide on-line, per aggirare i software antispam che analizzano la mail verificando la frequenza di alcune parole chiave.





Spear phishing

Lo “spear phishing” utilizza messaggi di posta elettronica falsificati apparentemente attendibili che inducono tutti gli appartenenti a una determinata organizzazione a rivelare nome utente e password.

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 username 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. Rispondendo al messaggio, il phisher acquisisce le informazioni e le utilizza per i propri scopi.

Lo spear phisher può generare facilmente gli indirizzi delle proprie vittime utilizzando appositi software che generano innumerevoli combinazioni di nomi e cognomi. L'invio può essere effettuato verso un solo dominio, riducendo così la possibilità che i messaggi vengano individuati come spam.

Spoofing

Lo spoofing si basa sulla falsificazione dell'indirizzo del mittente nel messaggio di posta elettronica.

Se il server di posta di un'azienda permette di connettersi alla porta SMTP, chiunque può collegarsi e inviare mail che sembrano così provenire da un indirizzo di quel dominio; l'indirizzo può essere reale o fittizio. Questa pratica viene definita "spoofing".

Lo spoofing può essere utilizzato per diversi scopi fraudolenti.

I phisher, che inducono gli utenti a rivelare informazioni riservate, usano indirizzi falsificati per simulare che il messaggio proviene da una fonte affidabile, ad esempio una banca. L'e-mail può dirottare l'utente su un sito fittizio (ad esempio una replica del sito di una banca online), dove vengono sottratte le informazioni sull'utente e le sue password.

I phisher possono inviare messaggi che sembrano provenire dall'interno dell'organizzazione, ad esempio dall'amministratore di sistema, con la richiesta di modificare la password o confermare le proprie informazioni personali.

I criminali che utilizzano la posta elettronica per truffe o frodi possono sfruttare indirizzi falsificati per coprire le proprie tracce e sfuggire all'identificazione.

Gli spammer possono usare lo spoofing per spacciarsi come un mittente innocuo o una delle tante aziende che mandano spam. Un altro vantaggio è che i veri mittenti non vengono inondati di notifiche di mancato recapito.

Lo spoofing può essere evitato in diversi modi.

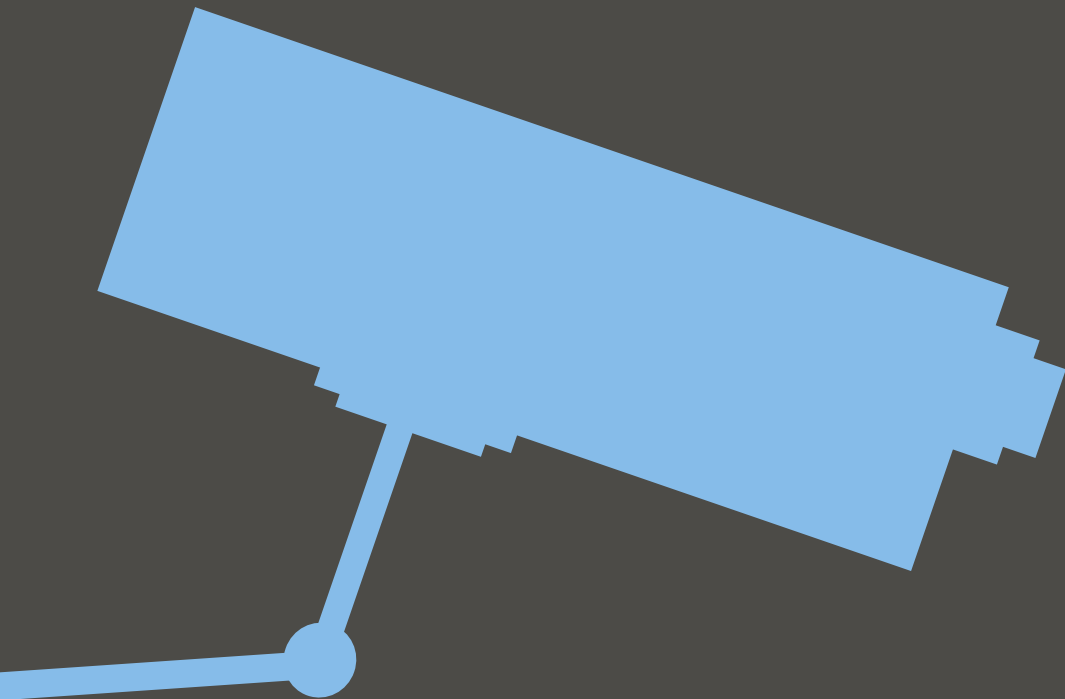
Si può configurare il sistema di posta in modo da impedire a chiunque di collegarsi alla porta SMTP.

Si può anche attivare la codifica per l'invio di messaggi autenticati. Questa procedura garantisce che i messaggi provengano effettivamente dagli utenti visualizzati e che non siano stati modificati.

Assicuratevi che il sistema di invio della posta abbia un registro e che sia configurato per rintracciare la provenienza delle e-mail con indirizzo falsificato.

Valutate l'utilizzo di un unico punto di accesso per le e-mail nel vostro sito. Potete farlo configurando il firewall in modo che le connessioni SMTP dall'esterno del firewall passino attraverso un hub di posta centrale. In questo modo avrete un registro centralizzato che vi permetterà di rintracciare l'origine dei tentativi di spoofing verso il vostro sito.





Spyware

Lo spyware è un software che permette a società commerciali e hacker di raccogliere informazioni a insaputa dell'utente.

Gli spyware non sono virus (non si diffondono ad altri computer) ma possono avere effetti indesiderati.

Uno spyware può inserirsi nel computer quando si visitano determinati siti Web. Un messaggio di popup può invitare l'utente a scaricare un software "necessario", oppure il software può essere scaricato automaticamente a vostra insaputa.

Lo spyware si autoesegue sul computer e tiene traccia dell'attività (ad esempio le visite ai siti Web), riferendo tutto a soggetti interessati, ad esempio che fa pubblicità. Il software può anche cambiare la pagina iniziale che viene visualizzata quando si apre il browser, oppure attivare una connessione telefonica diretta verso numeri a pagamento. Gli spyware assorbono inoltre memoria e potenza di calcolo, rallentando o bloccando il computer.

Un buon programma antivirus è in grado di individuare ed eliminare gli spyware, che vengono gestiti come una tipologia di Trojan.



Trojan

I Trojan sono programmi che vengono spacciati per software legittimi ma in realtà nascondono funzionalità dannose.

Un Trojan “finge” di avere una funzione (e può persino simulare di svolgerla), ma in realtà fa altro, normalmente a insaputa dell’utente. Ad esempio, **DLoader-L** arriva in allegato a un’e-mail che sembra essere un aggiornamento importante, spedito da Microsoft per proteggere i sistemi operativi Windows XP. Eseguendo l’allegato si scarica un programma che utilizza il computer per connettersi a certi siti Web, nel tentativo di sovraccaricarli, causando un cosiddetto “Denial of Service”, ovvero la negazione del servizio.

I Trojan non possono diffondersi con la stessa rapidità del virus, perché non creano copie di se stessi. Tuttavia la loro azione viene combinata spesso a quella dei virus. I virus possono scaricare Trojan che registrano le digitazioni sulla tastiera o sottraggono informazioni riservate. Altri Trojan possono essere utilizzati per infettare un computer con un virus.

Vedi anche [Backdoor Trojans](#).



Truffe azionarie

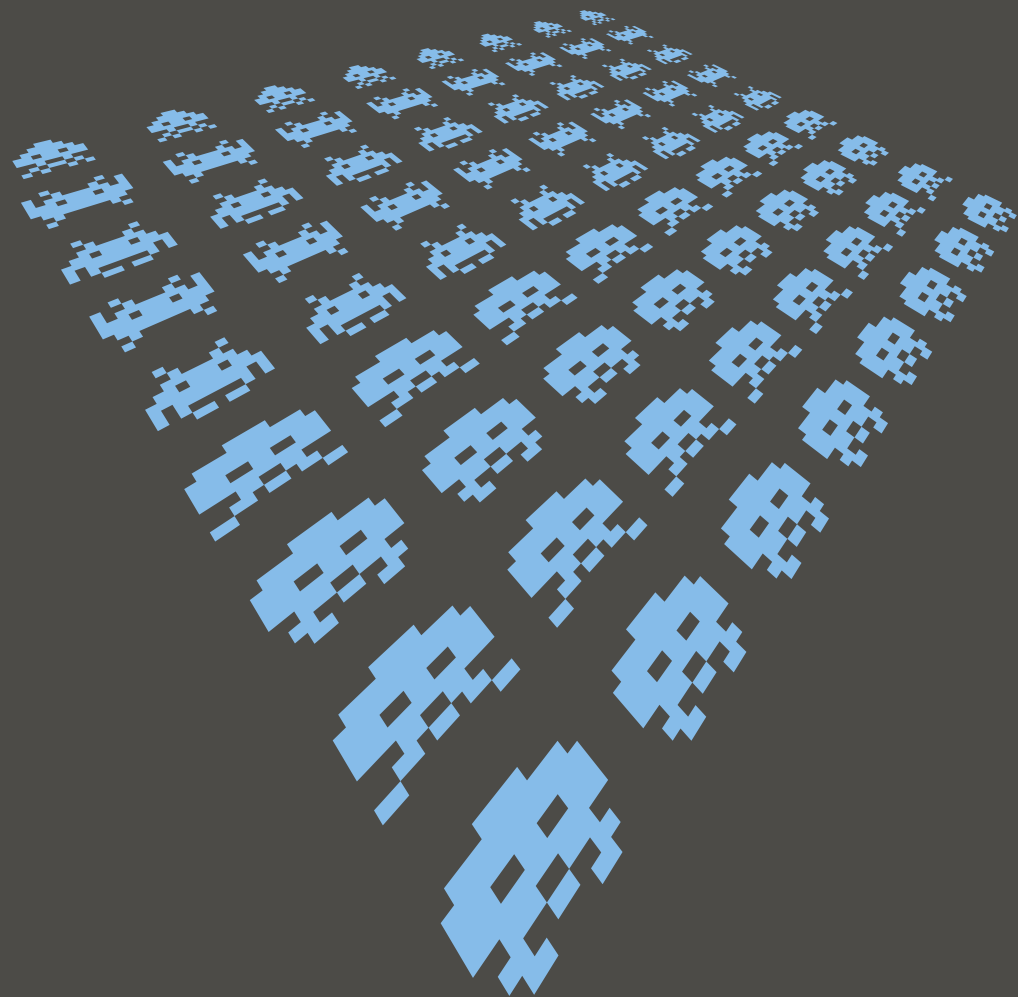
Gli spammer inviano messaggi per consigliare l'acquisto di azioni che poi possono essere vendute con profitto.

Le truffe sull'acquisto di azioni, conosciute anche come frodi "pump-and-dump", consistono nell'invio di mail che consigliano l'acquisto di azioni di aziende apparentemente "in crescita". Le vittime vengono incoraggiate a investire acquistando azioni, il cui prezzo risulta così appositamente "gonfiato"; i truffatori riescono in questo modo a vendere i titoli con profitto, prima che le quotazioni crollino nuovamente.

Le truffe azionarie hanno tutte le caratteristiche dei messaggi spam. Si tratta di posta commerciale non richiesta, solitamente distribuita utilizzando PC "zombie" controllati dagli hacker, che sfrutta tecniche di offuscamento per evitare i software anti-spam (ad esempio l'oggetto potrebbe utilizzare la grafia "st0ck" invece del termine "stock", cioè "azioni"). Queste mail contengono anche dichiarazioni non veritiere, nonostante possano includere dati reali per aumentare la credibilità del messaggio.

Queste truffe danneggiano sia gli investitori sia le piccole imprese. Quando la truffa viene scoperta e le azioni precipitano, gli investitori perdono i propri soldi. La perdita di valore può essere devastante per le aziende che dispongono di risorse limitate.

Il consiglio per evitare questo tipo di truffa è sempre lo stesso, come per i messaggi spam: non acquistare, non provare, non rispondere.



Virus

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

I virus si diffondono sui computer e sulle reti generando copie di se stessi, solitamente a 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.

Trattandosi di un programma, un virus deve essere eseguito prima di poter infettare un computer. I virus sono concepiti in modo tale che ciò avvenga. Possono attaccarsi ad altri programmi o nascondersi nel codice che viene eseguito automaticamente all'apertura di certi tipi di file. Talvolta, per essere eseguiti e diffondersi automaticamente sulla rete, possono sfruttare delle "falle" nella sicurezza del sistema operativo del computer.

L'utente può ricevere un file infetto in diversi modi: come allegato a un messaggio di posta, in un download da Internet oppure semplicemente su un dischetto. Non appena il file viene lanciato, il codice del virus viene eseguito. Il virus può così copiarsi in altri file o dischetti e apportare modifiche al computer.



Virus di documento o macrovirus

Questi virus sfruttano le macro, ovvero sequenze di comandi contenuti all'interno di file che vengono eseguite automaticamente.

Molte applicazioni, soprattutto la videoscrittura e i fogli elettronici, utilizzano le macro. Un macrovirus è un programma che si copia automaticamente e si diffonde da un file all'altro. Se si apre un documento che contiene un macrovirus, il virus si copia nei file di avvio dell'applicazione. Il computer viene così infettato.

Tutti i documenti aperti con quell'applicazione vengono infettati dal virus. Se il computer è connesso a una rete, il virus può diffondersi con estrema rapidità: il file danneggiato potrebbe essere aperto da altri utenti e infettare anche le loro applicazioni. Un macrovirus può persino apportare modifiche ai documenti e alle impostazioni predefinite.

Questi virus infettano i file utilizzati nella maggior parte degli uffici, colpendo applicazioni come Word ed Excel. Si diffondono su qualsiasi piattaforma che ospita l'applicazione danneggiata.

I macrovirus sono nati attorno alla metà degli anni Novanta, diventando subito la minaccia più seria di quel periodo. Oggi circolano ancora pochissimi virus di questo tipo.

Virus nelle e-mail

Molti dei virus più diffusi si distribuiscono automaticamente tramite i messaggi di posta elettronica.

Solitamente l'effetto dei virus contenuti nelle e-mail dipende dal comportamento dell'utente. Se l'utente clicca due volte sull'allegato, viene eseguito uno script che inoltra il documento infetto ad altri computer. Il virus Netsky, ad esempio, ricerca sul computer i file che possono contenere indirizzi e-mail e poi utilizza il programma di posta per autoinviarsi a questi indirizzi. Alcuni virus, come **Sobig-F**, non hanno nemmeno bisogno di utilizzare il client di posta; infatti dispongono di un proprio motore SMTP integrato per l'elaborazione e l'invio dei messaggi.

Ogni allegato ricevuto per posta elettronica potrebbe contenere un virus: aprendolo si corre il rischio di infettare il proprio computer.

Anche se l'estensione del file potrebbe farci pensare a un documento innocuo, ad esempio .txt, è meglio essere sempre diffidenti. Potrebbe trattarsi di uno script VBS la cui vera estensione è nascosta.

Alcuni virus, come **Kakworm** e **Bubbleboy**, sfruttano le vulnerabilità del sistema operativo o del programma di posta per colpire gli utenti non appena leggono l'e-mail. Si presentano come normali messaggi, ma contengono uno script nascosto che viene eseguito non appena si apre il messaggio di posta o lo si visualizza nel riquadro di anteprima (se si utilizza Outlook con la versione corretta di Internet Explorer). Questo script può modificare le impostazioni del sistema e inviare il virus ad altri utenti tramite posta elettronica.

I virus contenuti nei messaggi e-mail possono compromettere la sicurezza del computer o sottrarre informazioni riservate, ma la loro funzione principale è quella di generare un traffico di posta intenso e creare problemi ai server.

Per difendersi da questo tipo di virus è necessario installare un software antivirus ed evitare di aprire allegati sospetti, inattesi o non richiesti. E' opportuno anche installare le patch rilasciate dai produttori di software per eliminare le vulnerabilità del sistema sfruttate dai virus.





Virus parassiti

I virus che infettano i file, detti virus parassiti, si infiltrano all'interno di applicazioni e programmi.

Quando viene avviato un programma che contiene un virus parassita, viene eseguito il codice maligno. Per nascondersi, il virus restituisce poi il controllo dell'applicazione al programma originale.

Il sistema operativo considera il virus parte del programma e gli conferisce le stesse priorità. Queste priorità permettono al virus di copiarsi e installarsi nella memoria oppure di apportare modifiche sul computer dell'utente.

I virus parassiti sono stati tra i primi a colpire e, ancora oggi, rappresentano una minaccia.



Virus per cellulari

I cellulari possono essere colpiti da worm che si diffondono attraverso la rete di telefonia mobile.

Nel 2004 è stato creato il primo virus per cellulari. Il worm **Cabir-A** colpisce i cellulari che utilizzano il sistema operativo Symbian e viene trasmesso sotto forma di gioco (file SIS). Se il file viene eseguito, appare un messaggio sul display e il worm viene attivato ogni volta che si accende il cellulare. **Cabir-A** ricerca altri dispositivi attraverso la tecnologia Bluetooth e si invia automaticamente al primo telefono disponibile.

Esistono anche virus convenzionali che inviano i messaggi ai telefoni cellulari. **Timo-A**, ad esempio, utilizza i modem dei computer per inviare messaggi di testo (SMS) a numeri di telefono specifici, ma in questo caso il virus non può colpire o danneggiare il dispositivo mobile.

Finora le minacce per i telefoni cellulari hanno avuto un'incidenza limitata, probabilmente perché si utilizzano diversi sistemi operativi e le caratteristiche del software e dei dispositivi variano rapidamente.



Virus per palmari

I palmari o PDA costituiscono un nuovo bersaglio per i virus, ma finora gli hacker hanno dimostrato scarso interesse nei loro confronti.

I palmari o PDA hanno sistemi operativi speciali, come Palm e Microsoft PocketPC. Questi sistemi operativi sono vulnerabili ai codici malevoli, ma ad oggi i rischi sono irrilevanti.

Esistono solo pochi malware scritti appositamente per i palmari.

L'obiettivo prediletto dagli autori di virus sono i desktop, probabilmente perché sono più diffusi e consentono ai virus di propagarsi rapidamente tramite Internet e la posta elettronica.

L'unico rischio, per il momento, è che il palmare possa diventare un mezzo di diffusione. Quando lo si collega a un PC, a casa o in ufficio, per sincronizzare i dati, un virus innocuo sul palmare potrebbe diventare pericoloso nel momento in cui viene trasferito al computer. Per evitare questo rischio, vi raccomandiamo di seguire i consigli contenuti nella sezione **Come evitare virus, Trojan, worm e spyware** e di utilizzare un software antivirus sempre aggiornato.



Voice phishing

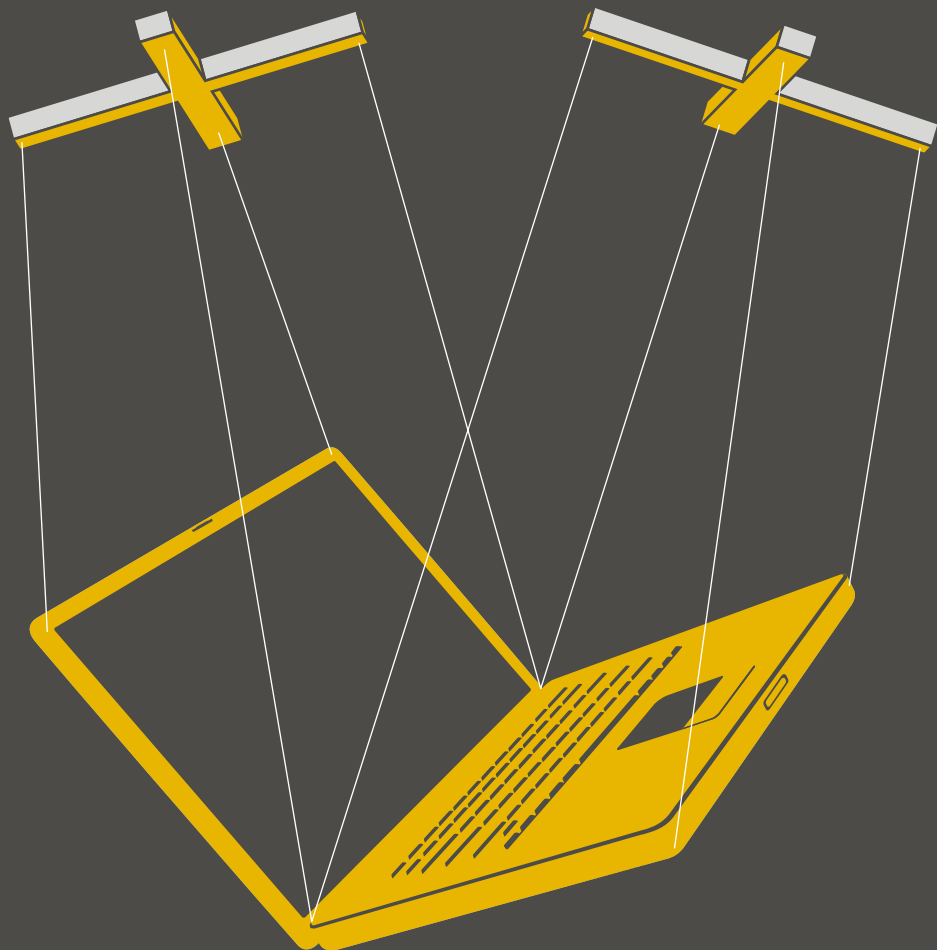
Il “voice phishing” usa falsi numeri telefonici per indurre gli utenti a rivelare informazioni personali o riservate.

In origine, il **Phishing** comportava l’invio di e-mail con link a siti fittizi, dove le vittime venivano indotte a immettere i dati del proprio account o altre informazioni riservate. Il voice phishing (noto anche come vishing, v-phishing o phone phishing) chiede all’utente di chiamare un numero di telefono, invece di visitare un sito Web, ma lo scopo finale è identico: sottrarre informazioni a scopo di lucro.

Un esempio è l’e-mail di voice phishing che sfrutta la notorietà di PayPal. Il messaggio sembra provenire da PayPal, il servizio di pagamento elettronico, e fa credere che l’account dell’utente possa essere stato utilizzato in maniera fraudolenta. L’utente viene avvertito che l’account verrà sospeso se l’utente non chiama un numero telefonico per “verificare” le informazioni. Quando l’utente chiama, un risponditore automatico chiede il numero di carta di credito, che viene successivamente utilizzato dai truffatori a scopo di lucro.

Gli utenti possono essere sospettosi verso i link in un’e-mail inattesa e possono fare attenzione ad accedere al sito Web corretto quando utilizzano un servizio finanziario. Ma più difficilmente conosceranno il numero di telefono dell’azienda.

Per tutelarsi contro il phishing telefonico, è opportuno usare un software antispam capace di individuare le mail di phishing e gestire con la dovuta attenzione i messaggi non richiesti.



Zombie

Uno zombie è un computer che viene controllato da remoto e utilizzato per scopi malevoli a insaputa del legittimo proprietario.

Un virus o un Trojan possono infettare un computer e aprire una “back door” che consente l’accesso ad altri utenti. Non appena ciò accade, il virus invia un messaggio al suo creatore, che può così assumere il controllo del computer via Internet. Da questo momento il computer è uno “zombie” al servizio di altri senza che l’utente ne sia consapevole. L’insieme di questi computer viene definito “botnet”.

Il creatore del virus può condividere o vendere l’accesso alla sua lista di computer controllati, in modo che altri possano utilizzarli per scopi fraudolenti.

Ad esempio, uno spammer può sfruttare computer zombie per inviare spam. Attualmente l’80% di tutto lo spam viene distribuito con questa tecnica. Gli spammer possono in questo modo evitare di essere individuati e aggirare l’eventuale blocco dell’indirizzo applicato al loro server. Possono inoltre ridurre i costi, in quanto è il proprietario del computer che paga per la connessione a Internet.

Gli hacker possono anche usare gli zombie per lanciare un attacco Denial of Service. Migliaia di computer vengono predisposti per tentare l’accesso simultaneamente allo stesso sito, in modo che il Web server non riesca a gestire tutte le richieste che riceve. Il sito Web attaccato diventa così inaccessibile.

Vedi anche **Attacco DoS (Denial of Service)**, **Spam**, **Backdoor Trojan**.

Software di protezione

Software antivirus

Il software antivirus protegge da virus, Trojan, worm e – a seconda dei prodotti – anche da spyware e altri tipi di malware.

- **Virus conosciuti** – Lo scanner confronta i file del computer con una libreria di “identità” di virus conosciuti. Se trova una corrispondenza, manda un avvertimento e blocca l’accesso al file.
- **Virus sconosciuti** – Lo scanner analizza il comportamento probabile di un programma. Se ha le caratteristiche di un virus, l’accesso viene bloccato anche se il file non corrisponde ad alcun virus noto.
- **File sospetti** – Lo scanner analizza il comportamento probabile di un programma. Se il comportamento rivela caratteristiche indesiderabili, lo scanner segnala che potrebbe trattarsi di un virus.

Il rilevamento di virus conosciuti dipende dalla frequenza di aggiornamento del software con le ultime identità dei virus.

Esistono scanner in accesso e su richiesta. La maggior parte dei software antivirus offrono entrambe le possibilità.

Gli scanner in accesso rimangono attivi sul computer tutte le volte che lo si accende. I file vengono controllati in modo automatico non appena si tenta di aprirli o di eseguirli. In questo modo viene impedito agli utenti di utilizzare i file infetti.

Gli scanner su richiesta consentono di avviare o di pianificare la scansione di determinati file o unità.

Anti-spam software

I programmi antispam possono individuare le e-mail indesiderate evitando che raggiungano la casella della posta in arrivo.

Questi programmi utilizzano una combinazione di metodi per stabilire se un messaggio è spam. Ad esempio:

- Bloccano la posta in arrivo da indirizzi presenti nell'elenco di indirizzi vietati. Si può trattare di una lista generale disponibile in commercio oppure di una lista locale di indirizzi dai quali in passato è stato spedito spam all'azienda.
- Bloccano le e-mail che contengono determinati indirizzi Web.
- Verificano se la posta proviene da un dominio o un indirizzo Web accettabili. Gli spammer usano spesso indirizzi fasulli per tentare di eludere i programmi antispam.
- Ricercano parole o espressioni chiave che ricorrono nei messaggi spam (ad esempio "carta di credito" o "dieta dimagrante").
- Ricercano alcuni trucchi utilizzati dagli spammer per mascherare le parole chiave all'interno del messaggio (ad esempio, "hardc*re p0rn").
- Ricercano codici HTML superflui utilizzati dagli spammer per nascondere i messaggi e confondere i programmi antispam.

Il programma utilizza tutte le informazioni raccolte per stabilire la probabilità che un'e-mail sia spam. Se la probabilità è abbastanza alta, blocca l'e-mail o la cancella, a seconda delle impostazioni prescelte.

Il software antispam deve essere aggiornato frequentemente con nuove "regole" per poter riconoscere le tecniche più avanzate usate dagli spammer.

Come vengono protette le e-mail legittime

Molti utenti temono che il software antispam cancelli la posta privata o utile. In realtà, la posta è al sicuro e, se si vuole, è possibile visualizzare lo spam bloccato.

I programmi antispam possono essere molto precisi. Di solito bloccano meno di un'e-mail legittima su diecimila o addirittura centomila.

Anche se il programma identifica erroneamente un'e-mail legittima come spam, può essere configurato per metterla in "quarantena" anziché cancellarla. L'amministratore può quindi decidere se consegnare o cancellare il messaggio. Alcuni programmi consentono a ogni singolo utente di decidere le sorti di ogni messaggio messo in quarantena.

Il software "adattivo"

Alcuni programmi antispam sono "adattivi", ossia apprendono quali argomenti sono da considerare accettabili e quali no.

Supponiamo che un'azienda farmaceutica installi un software antispam. All'inizio il software tenta di rilevare lo spam cercando le seguenti parole chiave: credito, gratis, debito, ipoteca, farmaci, ricetta, medicina, dottore. Il software blocca i messaggi che contengono un numero elevato di queste parole, ma consente ai singoli utenti di recuperare i messaggi che desiderano leggere.

Qualcuno nel reparto ricerca scopre che la posta legittima sui nuovi farmaci è stata bloccata e richiede che ne venga autorizzata la consegna. Il software apprende che l'utente riceve spesso messaggi sui farmaci e assegna quindi un peso minore alle parole correlate ai farmaci quando analizza le probabilità che i messaggi siano spam.

Nel reparto finanze, gli utenti reclamano la posta contenente termini finanziari, quindi il software impara ad assegnare un peso minore a questo tipo di parole, continuando però a bloccare per questi utenti la posta relativa ai farmaci.

Firewall

Un firewall impedisce l'accesso non autorizzato a un computer o una rete.

Come suggerisce il nome (letteralmente “parete tagliafuoco”) funge da barriera fra diverse reti o diverse parti di una rete, bloccando il traffico pericoloso o respingendo gli attacchi degli hacker.

Un **firewall di rete** viene installato in corrispondenza del confine fra due reti, solitamente fra Internet e la rete aziendale. Può essersi un'apparecchiatura hardware o un software installato su un computer che funge da gateway per la rete aziendale.

Un **client firewall** è un software che gira sul PC di un utente finale e protegge solo quel computer.

In entrambi i casi, il firewall sorveglia il traffico, sia in entrata sia in uscita, per stabilire se soddisfa determinati criteri.

In caso affermativo, il traffico viene autorizzato, altrimenti il firewall lo blocca. Il firewall può filtrare il traffico in base a

- indirizzi di provenienza e destinazione e numeri di porta (filtro indirizzi)
- tipo di traffico di rete, ad es. HTTP o FTP (filtro protocollo)
- attributi o stato dei pacchetti di informazioni inviati.

Un firewall client può inoltre avvertire l'utente ogni qualvolta un programma tenta di stabilire una connessione e chiede se la connessione deve essere autorizzata o bloccata. Il software è in grado di apprendere gradualmente in base alle risposte dell'utente, imparando a conoscere il tipo di traffico consentito dall'utente.

Resource shielding

La tecnica di “resource shielding” (letteralmente “schermatura delle risorse”) protegge dai tentativi di accesso alle parti vulnerabili del computer.

Il “resource shielding” analizza il comportamento di tutti i programmi già attivi sul computer e blocca qualsiasi attività che viene giudicata dannosa. Ad esempio, verifica tutte le modifiche apportate al registro di Windows, che possono indicare che un malware si sta autoinstallando per avviarsi automaticamente ogni volta che si accende il computer.

I prodotti di resource shielding consentono solitamente di impostare regole proprie sulle risorse da proteggere.

Consigli di protezione

Come evitare virus, Trojan, worm e spyware

Usate un software antivirus

Installate un software antivirus su tutti i desktop e i server e tenetelo sempre aggiornato. I nuovi virus possono diffondersi molto velocemente, quindi è bene prevedere un sistema per l'aggiornamento automatico, frequente e immediato di tutti i computer dell'azienda.

Usate un software di filtraggio della posta anche sul gateway di posta elettronica, per proteggere l'azienda dalle minacce di virus contenuti nelle e-mail, spam e spyware.

E non dimenticate di proteggere i computer portatili e i desktop utilizzati da chi lavora a casa. Virus, worm e spyware possono sfruttare facilmente questi veicoli per insinuarsi in azienda.

Bloccate i tipi di file che portano virus

Tipicamente sono i file EXE, COM, PIF, SCR, VBS, SHS, CHM e BAT. È quanto mai improbabile che la vostra azienda debba ricevere questi tipi di file dall'esterno.

Bloccate i file con più estensioni

Alcuni virus "nascondono" il fatto di essere programmi utilizzando una doppia estensione, ad esempio TXT.VBS. A una prima occhiata, file come LOVE-LETTER-FORYOU.TXT.VBS o ANNAKOURNIKOVA.JPG.VBS possono apparire come innocui file di testo o immagine. Bloccate qualsiasi file con doppia estensione al gateway di posta.

Assicuratevi che tutti i programmi vengano controllati dal reparto IT

Assicuratevi che tutti i programmi provenienti dall'esterno via e-mail vengano sottoposti direttamente al reparto sistemi informativi o, nelle piccole aziende, al responsabile IT, per verifica e approvazione. Gli addetti potranno confermare che si tratta di software esente da virus, con le necessarie licenze, che difficilmente provocherà conflitti con il software esistente.

Abbonatevi a un servizio di allarme via e-mail

Un servizio di allarme può informarvi su nuovi virus e fornirvi le relative identità affinché il vostro software antivirus riesca a individuare i pericoli. Sophos offre un servizio gratuito. Per maggiori informazioni, visitate il sito <http://www.sophos.it/security/notifications> Valutate anche la distribuzione in diretta di informazioni sui virus sul vostro sito Web o sulla Intranet aziendale per assicurarvi che gli utenti siano a conoscenza degli ultimi virus informatici.

Usate un firewall sui computer collegati a Internet

Dovete usare un firewall per proteggere i computer collegati con il mondo esterno. Anche chi utilizza un portatile e/o lavora da casa ha bisogno di una protezione firewall.

Aggiornate il sistema con le patch di sicurezza

Prestate attenzione alle informazioni di sicurezza e scaricate le patch. Le patch correggono le vulnerabilità del sistema e riducono la vulnerabilità a virus e worm. I responsabili dei sistemi informativi dovrebbero iscriversi alle mailing list delle principali aziende produttrici di software, ad esempio Microsoft (www.microsoft.com/technet/security/bulletin/notify.mspx). Gli utenti privati in possesso di computer con sistema operativo Windows possono visitare la pagina windowsupdate.microsoft.com, dalla quale è possibile effettuare una scansione che permette di verificare la presenza di vulnerabilità e di installare le patch per correggere i problemi rilevati.

Effettuate backup regolari dei programmi e dei dati

Effettuate backup regolari dei lavori e dei dati più importanti e verificate che le copie siano state effettivamente create. E' consigliabile conservare i file di backup in un posto sicuro, possibilmente in un luogo diverso dalla sede di lavoro per tutelarsi anche in caso di incendio. Se il computer viene infettato da un virus, sarete in grado di ripristinare tutti i programmi e i dati persi.

Disabilitate l'avvio da floppy disk

Oggi i Boot virus o virus del settore di avvio sono rari, ma è sempre meglio proteggersi da eventuali attacchi. Modificate la sequenza di avvio affinché il computer carichi sempre il sistema operativo dal disco rigido, invece di utilizzare il floppy disk (unità A:). In questo modo, anche se un floppy disk infetto viene dimenticato all'interno del lettore, non può essere infettato da un virus del settore di avvio. Qualora abbiate bisogno di riavviare il sistema da floppy disk, le impostazioni possono essere modificate facilmente.

Adottate una politica aziendale contro i virus

Stabilire regole precise utili a garantire un ambiente di lavoro sicuro e comunicatele a tutto il personale. La politica di sicurezza può prevedere diversi accorgimenti:

- Non scaricare file eseguibili e/o documenti direttamente da Internet.
- Non aprire programmi, documenti o fogli elettronici non richiesti.
- Non utilizzare giochi o salvaschermi che non sono stati forniti con il sistema operativo.
- Sottoporre all'attenzione dell'ufficio sistemi informativi gli allegati delle mail e attendere una conferma della loro innocuità.
- Salvare tutti i documenti Word come file RTF (Rich Text Format), dato che i documenti con estensione .doc possono contenere virus macro.
- Diffidare di qualsiasi messaggio di posta inatteso.
- Inoltrare direttamente ai sistemi informativi (e a nessun altro) i messaggi che avvertono della presenza di virus o gli hoax, per verificare se si tratti di minacce reali o fittizie.
- Informare subito il reparto IT se si ritiene che il computer possa essere infetto.

Come evitare gli “hoax”

Adottate una politica aziendale sugli allarmi virus

Implementate una politica aziendale sugli allarmi virus, dando ad esempio disposizioni come “non inviare allarmi virus di alcun genere a NESSUNA altra persona diversa del responsabile per la gestione dei virus. Non importa se gli allarmi provengono da un produttore di software antivirus o se sono stati confermati da una grande azienda informatica, da un amico di fiducia. TUTTI gli allarmi virus devono essere inviati esclusivamente al responsabile informatico, il cui compito sarà quello di avvertire gli utenti dell’azienda nel caso in cui la minaccia sia concreta. Gli allarmi provenienti da altre fonti devono essere ignorati.”

Tenetevi informati sugli “hoax”

Tenetevi aggiornati sugli “hoax”, visitando la pagina dedicata ai falsi allarmi sul nostro sito Web: www.sophos.com/security/hoaxes/

Non inoltrate le Catene di Sant’Antonio

Non inoltrate messaggi a catena, anche se offrono ricompense o fanno credere di distribuire informazioni utili.

Come prevenire lo spam

Utilizzate un software di filtraggio per proteggere il vostro server di posta

Usate un software di filtraggio sul server di posta elettronica per proteggere la vostra azienda dallo spam e dalle minacce di virus, spyware e worm contenuti nelle e-mail.

Non effettuate mai acquisti da un’e-mail non richiesta

Effettuando un acquisto di questo tipo, finanziate le attività di spamming. Il vostro indirizzo di posta elettronica potrebbe anche essere aggiunto alle liste che vengono vendute agli spammer, quindi rischiate di ricevere molti più messaggi “spazzatura”. E, cosa ancor più grave, potreste essere vittima di una frode.

Se non conoscete il mittente, cancellate il messaggio

La maggior parte dei messaggi spam non rappresenta una minaccia, ma causa solo fastidio. Tuttavia tali messaggi possono contenere virus in grado di danneggiare il computer all’apertura dell’e-mail.

Non rispondete mai ai messaggi spam e ignorate i link al loro interno

Se rispondete allo spam, anche solo per cancellarli dalla mailing list, confermate che l’indirizzo di posta è valido e incoraggiate gli spammer a spedire una maggiore quantità di messaggi.

Non utilizzate la modalità “anteprima” nel programma di posta elettronica

Molti spammer sono in grado di sapere quando viene visualizzato il messaggio, anche se non si seleziona direttamente l'e-mail. La modalità “anteprima”, in realtà, apre il messaggio consentendo agli spammer di capire se le loro e-mail sono arrivate a destinazione. Quando controllate la posta cercate di stabilire, solo in base all'oggetto, se si tratta di un messaggio di posta indesiderata.

Usate il campo “bcc” o “ccn” se inviate l'e-mail a più persone

Il campo “Bcc” (“Ccn” per i programmi di posta in italiano) permette di nascondere agli utenti la lista dei destinatari. Se gli indirizzi vengono inseriti nel campo “To” (“A” in italiano), gli spammer potrebbero utilizzarli e aggiungerli alle proprie mailing list.

Non pubblicate mai il vostro indirizzo e-mail su Internet

Non pubblicate mai il vostro indirizzo e-mail sui siti Web, sui newsgroup o sui forum online di dominio pubblico. Gli spammer utilizzano programmi che raccolgono indirizzi e-mail da Internet.

Date il vostro indirizzo di posta elettronica solo a persone fidate

Comunicare il vostro indirizzo e-mail principale solamente ad amici e colleghi.

Utilizzate uno o due indirizzi e-mail secondari

Se compilate moduli di registrazione o partecipate a sondaggi su siti Web dai quali non desiderate ricevere ulteriori informazioni, utilizzate un indirizzo e-mail secondario. In questo modo eviterete di ricevere messaggi di posta indesiderata sul vostro indirizzo principale.

Non accettate di ricevere ulteriori informazioni o promozioni

Quando compilate un modulo elettronico on-line, controllate, nell'apposito riquadro, la voce con la quale si autorizza il sito a utilizzare il vostro indirizzo mail per spedirvi ulteriori informazioni o offerte speciali. Decidete se è il caso di selezionarla oppure no.

Come evitare il “phishing”

Non rispondete mai ai messaggi che richiedono informazioni finanziarie personali

Diffidate dalle e-mail che richiedono di inserire password e dettagli relativi a conti bancari o che includono link per effettuare tali operazioni. Le banche e le società di e-commerce di solito non spediscono messaggi di questo genere.

Individuate i particolari che vi aiutano a capire se il messaggio ha un intento fraudolento

Le mail di “phishing” di solito usano un'intestazione generica, come “Gentile cliente” perché non dispongono di dati precisi, visto che sono a tutti gli effetti messaggi spam. Possono anche riportare dichiarazioni allarmanti, segnalandovi, ad esempio, che i dettagli del vostro conto sono stati persi o rubati. Il messaggio spesso può contenere errori di ortografia o parole scritte con caratteri diversi, come “1nformaziOne”, per evitare di essere eliminato dal software antispam.

Visitate i siti Internet delle banche digitando l'indirizzo nell'apposita barra

Non selezionate i link presenti nei messaggi di posta indesiderata. I “phisher” possono utilizzare questi collegamenti per reindirizzare l'utente su un sito Web fantasma. Meglio digitare l'indirizzo del sito nell'apposita barra per navigare all'interno della pagina autentica.

Controllate regolarmente i vostri conti on-line

Accedete regolarmente ai vostri conti on-line e controllate le varie operazioni effettuate. Se notate qualcosa di strano, avvisate subito la banca o il fornitore dei servizi di credito.

Verificate che la connessione sia protetta

Controllate la dicitura nella barra degli indirizzi. Se il sito che state visitando si trova su un server protetto, il collegamento dovrebbe iniziare con “https://” (la “s” sta per “secure”, cioè “protetto”) invece di “http://”. Inoltre accertatevi che vi sia l'icona del lucchetto nella barra di stato del browser. Questo significa che il sito Web utilizza una connessione crittografata, ma non garantisce sempre che il sito sia autentico.

State attenti a gestire e-mail e dati personali

Leggete le istruzioni della vostra banca per effettuare transazioni sicure. Non rivelate a nessuno e non riscrivete il codice PIN o la password, non utilizzate la stessa password per tutti i vostri conti on-line. Non aprite i messaggi di spam e non rispondete per nessun motivo. Il rischio è quello di confermare che il vostro indirizzo di posta è valido e, in seguito, potreste essere vittima di truffe on-line.

Protegete il vostro computer

I software antispam riducono drasticamente i tentativi di “phishing”. L'utilizzo di un firewall permette di proteggere le informazioni personali e di bloccare le comunicazioni non autorizzate. E' molto importante disporre di un software antivirus per rilevare ed eliminare i programmi potenzialmente dannosi, come spyware o backdoor Trojan, che potrebbero essere contenuti nelle e-mail. Aggiornate il browser Internet installando le ultime patch di sicurezza disponibili.

Segnalate ogni attività sospetta

Se ricevete una e-mail sospetta, inoltratela all'organizzazione direttamente coinvolta (molte aziende hanno un indirizzo di posta creato appositamente per le segnalazioni di questo tipo).

Come navigare sicuri in Internet

Questa sezione fornisce consigli generali per utilizzare in maniera sicura e-mail e connessioni Internet. Vedi anche [Come evitare il “phishing”](#).

Non cliccate sui popup

Se appaiono popup inattesi, come quelli che avvertono della presenza di virus sul computer e che offrono una soluzione, non selezionate il link e non autorizzate nessun download. Potreste scaricare e installare software potenzialmente dannosi.

Non cliccate sui link presenti all'interno dei messaggi di posta indesiderata

Tali collegamenti potrebbero indirizzare l'utente su un sito fittizio, utilizzato per sottrarre informazioni personali, come dettagli bancari e password. Digitate sempre l'indirizzo Internet che volete visitare direttamente nella barra del browser.

Utilizzate una password diversa per ogni sito

Usate una password diversa per ogni sito sul quale vi registrate. Così, se una password viene scoperta, il pericolo riguarderà un solo account.

Configurate il browser Internet per garantire la massima sicurezza

Potete disabilitare i controlli Java o Active X, oppure chiedere di essere avvisati prima dell'esecuzione di tali codici. Per esempio, in Microsoft Internet Explorer, selezionate Strumenti/ Opzioni Internet/ Protezione/ Livello personalizzato e impostate i valori che desiderate.

Impedite l'accesso ad alcuni siti Internet o a certi contenuti on-line

In un ambiente di lavoro, potrebbe essere necessario impedire l'accesso degli utenti ai siti Internet che risultano inappropriati, che hanno contenuti offensivi o che potrebbero rappresentare delle minacce (ad esempio siti che installano spyware). Tutto questo è possibile grazie a software di filtraggio Web o "applicazioni" hardware.

Utilizzate le tecnologie di filtraggio basate sulla reputazione

I sistemi di filtraggio Web basati sulla reputazione verificano l'attendibilità del mittente di una mail utilizzando un database grazie al quale è possibile determinare quanti messaggi spam, virus, worm vengono inviati da un particolare indirizzo. Il software assegna all'e-mail un "punteggio basato sulla reputazione" che serve per capire se bloccare il messaggio o se posticipare la ricezione, dando la priorità ad altre e-mail.

Munitevi di firewall

La vostra azienda può installare un firewall di rete per autorizzare solo una certa tipologia di traffico. Su tutti i computer della rete viene installato un firewall client che accetta solo il traffico autorizzato e quindi blocca gli attacchi degli hacker e dei worm di Internet. Inoltre, impedisce al computer di comunicare via Internet con programmi non autorizzati.

Utilizzate un router

Potete servirvi di un router per limitare la connessione fra Internet e determinati computer. Molti router integrano anche un firewall di rete.

Come scegliere le password

Le password permettono di proteggersi contro le frodi e le sottrazioni di informazioni riservate, ma poche persone scelgono password davvero sicure.

Scegliete una password lunga

Più la password è lunga, più è difficile da decifrare o indovinare utilizzando tutte le possibili combinazioni (metodo "forza bruta"). Deve essere composta da almeno otto caratteri.

Usate caratteri diversi

Usate una password che contenga numeri, segni di punteggiatura, lettere maiuscole e minuscole.

Non usate parole contenute nei dizionari

Non usate parole, sostantivi, nomi propri o geografici che sono contenuti nei dizionari. Gli hacker possono sferrare un "dictionary attack", provando a inserire, in maniera automatica, tutte le parole contenute nel dizionario al fine di decifrare la password corretta.

Non inserite informazioni personali

E' probabile che altre persone siano a conoscenza di informazioni come la vostra data di nascita, il nome del vostro partner o del vostro bambino, il vostro numero di telefono e queste potrebbero indovinare la password.

Non usate il vostro username

Non scegliete una password uguale al vostro username o al numero di conto.

Scegliete una password difficile da identificare durante la digitazione

Assicuratevi di non usare caratteri ripetuti o tasti vicini sulla tastiera.

Valutate l'uso di una "passphrase" ("frase chiave")

Una "passphrase" è composta da un insieme di parole o di stringhe alfanumeriche. Abbinamenti insoliti di parole sono difficili da decifrare.

Cercate di memorizzare la password

Memorizzate le vostre password invece di scriverle. Scegliete una combinazione significativa per voi oppure servitevi di sistemi mnemonici per ricordare le password.

Non salvate le password sul computer o su dispositivi on-line

Gli hacker potrebbero essere in grado di accedere al vostro computer e trovare le password.

Se decidete di scrivere le password, conservatele in un posto sicuro

Non tenete le password vicino al computer o in un posto facilmente accessibile.

Utilizzate password diverse per ogni account

Se un hacker riesce a decifrare una delle vostre password, solo un account viene compromesso.

Non rivelate a nessuno le vostre password

Se ricevete un modulo che vi richiede di "confermare" le vostre password, evitate di compilarlo anche se la fonte sembra attendibile. (vedi "Phishing").

Non inserite nessuna password su computer di pubblica utenza

Non inserite le vostre password se usate computer di pubblica utenza, come quelli disponibili negli hotel o negli internet point. Questi computer potrebbero non essere sicuri e nascondere "keystroke loggers".

Cambiate le vostre password con regolarità

Se la vostra password è corta o semplice da indovinare, dovrete cambiarla frequentemente.

La “cronologia” dei virus

Quando virus, Trojan e worm hanno iniziato a rappresentare una minaccia? Molti considerano come punto di partenza Brain, il primo virus per il sistema operativo Microsoft, scritto nel 1986. Tuttavia programmi con tutte le caratteristiche di un virus sono stati introdotti ben prima. Ecco una sezione che illustra i momenti chiave nella storia dei virus.

1949 Macchine e programmi in grado di replicarsi

John von Neumann, il padre della cibernetica, dimostra matematicamente la possibilità di costruire una macchina o un programma in grado di replicarsi autonomamente.

1959 Il gioco “Core Wars”

H Douglas McIlroy, Victor Vysotsky e Robert P Morris, programmatori dei Bell Laboratories, sviluppano il gioco “Core Wars”, nel quale alcuni programmi chiamati “organismi” fanno a gara per assorbire le capacità di calcolo del computer.

1960 Programmi “Rabbit”

I programmatori iniziano a scrivere “segnaposto” per i mainframe. Quando non ci sono più lavori in attesa, questi programmi aggiungono una copia di se stessi alla coda. Sono chiamati “rabbit” (“conigli” in italiano) perché si moltiplicano rapidamente, assorbendo tutte le risorse disponibili sul sistema.

1971 Il primo worm

Bob Thomas, un programmatore che lavorava al sistema ARPANET - precursore della rete Internet - scrive **Creeper**, il primo worm in grado di passare da computer a computer e di visualizzare un messaggio.

1975 Codice replicabile

A K Dewdney scrive Pervade, una subroutine informatica per un gioco che sfrutta il sistema UNIVAC 1100. Quando il gioco viene avviato, la funzione copia la versione più recente di se stessa all’interno di ogni directory accessibile, incluse le cartelle condivise, e, in seguito, si diffonde sulla rete.

1978 Il worm Vampire

John Shoch e Jon Hupp di Xerox PARC iniziano a sperimentare worm che consentono di effettuare operazioni utili. Il worm **Vampire** non è attivo durante il giorno, ma la notte assegna incarichi ai computer sottoutilizzati.

1981 Virus Apple

Joe Dellinger, studente della Texas A&M University, modifica il sistema operativo nei floppy disk Apple II in modo tale che si comporti come un virus. Questo virus non ha avuto particolari effetti collaterali e non è stato mai pubblicato. Tuttavia sono state scritte e diffuse ulteriori versioni.

1982 Virus Apple con effetti collaterali

Rich Skrenta, un ragazzo di quindici anni, scrive Elk Cloner, un virus per il sistema operativo Apple II. Elk Cloner si attiva quando il computer viene avviato da un floppy infetto e si diffonde su tutti i floppy-disk inseriti nel lettore. Viene visualizzato un messaggio ogni 50 avvisi del computer.

1985 Trojan via e-mail

Viene distribuito via e-mail il Trojan **EGABTR**, che si spaccia per un programma in grado di migliorare la grafica. Tuttavia, una volta in azione, cancella tutti i file sull’hard disk e visualizza un messaggio sullo schermo.

1986 Il primo virus per PC

Il primo virus per PC IBM, **Brain**, viene scritto presumibilmente da due fratelli pakistani per proteggere il loro software da copie pirata. Il virus si replica su tutti i dischetti su cui viene copiato, aggiungendo anche un messaggio di copyright.

1987 Il worm Christmas tree

Si tratta di un biglietto di auguri natalizi elettronico che contiene un codice di programma. Se eseguito, il codice disegna l'albero di Natale come promesso, ma si inoltra a tutti gli indirizzi contenuti nella rubrica. Il traffico generato paralizza l'intera rete mondiale di IBM.

1988 Internet Worm

Robert Morris, uno studente di 23 anni, diffonde un worm sulla rete statunitense DARPA. Il virus si diffonde a migliaia di computer e, a causa di un errore, li re-infecta continuamente fino a causare il crash del sistema.

1989 Trojan ricattatore

Il Trojan AIDS viene diffuso su un dischetto che fornisce informazioni su AIDS e HIV. Il virus codifica l'hard disk del computer e chiede un riscatto in denaro per rilasciare la password.

1991 Il primo virus polimorfico

Tequila è il primo virus polimorfico. Questo tipo di virus rende più difficile il rilevamento da parte degli scanner perché cambia aspetto a ogni nuova infezione.

1992 Il panico da Michelangelo

Il virus Michelangelo è stato ideato per cancellare gli hard disk ogni anno il 6 marzo (data di nascita di Michelangelo). Quando due aziende distribuirono accidentalmente dischi e PC infetti, si scatenò il panico in tutto il mondo, ma l'infezione restò limitata a pochi computer.

1994 Il primo hoax via mail

Il primo falso allarme distribuito via posta elettronica segnala un virus malevolo che dovrebbe cancellare l'intero hard disk in seguito all'apertura di una semplice mail con oggetto "Good Times".

1995 Il primo virus macro

Appare il primo virus contenuto in un documento o "macro", Concept, che si diffonde sfruttando le macro di Microsoft Word.

1998 Il primo virus che colpisce l'hardware

Melissa, un virus che si autoinvia per e-mail, si diffonde in tutto il mondo. Fa la sua comparsa **Bubbleboy**, il primo virus che riesce a infettare un computer con la sola lettura di un'e-mail.

2000 Virus Palm

Appare il primo virus per il sistema operativo Palm, sebbene nessun utente venga colpito.

2000 Attacchi Denial-of-service

Attacchi "distributed denial-of-service" contro Yahoo, eBay, Amazon e altri siti molto popolari mettono i sistemi fuori uso per diverse ore.

Love Bug si afferma come il virus di maggior successo fra quelli che si trasmettono tramite posta elettronica.

2001 Virus diffusi tramite siti Internet o reti condivise

I programmi malevoli cominciano a sfruttare le falle dei software per potersi diffondere senza alcun intervento da parte dell'utente. **Nimda** infetta gli utenti che entrano semplicemente in un sito Web. Sircam utilizza un proprio motore di posta elettronica per diffondersi, anche attraverso condivisioni di rete.

2003 Zombie, Phishing

Il worm Sobig permette agli hacker di acquisire il controllo dei PC e trasformarli in "zombie" per la diffusione di spam. Il worm Mimail si spaccia per una e-mail di Paypal che chiede agli utenti di confermare i dati della loro carta di credito.

2004 Bot IRC

Vengono sviluppati bot IRC (Internet Relay Chat) malevoli. I bot vengono piazzati su un computer tramite un Trojan e da lì si connettono a un canale IRC a insaputa dell'utente, permettendo agli hacker di assumere il controllo del computer.

2005 Rootkit

Il sistema di protezione DRM di Sony contro le copie pirata installa un “rootkit” sul PC, nascondendo i file in modo che non possano essere duplicati. Gli hacker scrivono Trojan che sfruttano questa debolezza e installano una “backdoor” nascosta.

2006 Truffe sull'acquisto di azioni

Si diffondono i messaggi spam che invitano ad acquistare azioni di piccole società (dette “pump-and- dump”, cioè “pompa e scarica”).

2006 Ransomware

I Trojan Zippo e Archiveus, che codificano i file degli utenti e chiedono un riscatto in denaro per ottenere la password, sono i primi esempi di ransomware.

Questo opuscolo si rivolge a chi amministra reti informatiche, utilizza il computer per lavoro o semplicemente naviga in Internet. Vengono descritte le minacce alla sicurezza e vengono illustrate le contromisure che si possono adottare per proteggere i computer.

Sophos

Via Senigallia 18/2, 20161 Milano

tel: +39 02 66 28 10 0

fax: +39 02 66 28 10 99

Via Krekich 25,00143 Roma

tel: +39 06 50 52 44 66

Fax: +39 06 50 99 02 24

www.sophos.it

SOPHOS
secured.