SOPHOS

Rapporto sulla sicurezza: 2009

Preparatevi per le nuove minacce di quest'anno

SOPHOS

Rapporto sulla sicurezza: **2009**

Panoramica

Il 2 novembre 1988, Robert Morris, uno studente ventiduenne iscritto alla Cornell University, rilasciò un worm di Internet in grado di sfruttare le vulnerabilità del sistema operativo UNIX. Si stima che infettò il 10% del traffico Internet. Venti anni dopo, l' entità del problema malware è cresciuta esponenzialmente. Gli attacchi odierni sono organizzati e studiati per trafugare informazioni e risorse da clienti e aziende. Anche se vi sono stati dei casi di attacchi spinti da motivazioni politiche e religiose, la motivazione principale resta quella di carattere finanziario.

Ormai Internet è il canale principale attraverso il quale i criminali informatici infettano i computer, principalmente a causa del fatto che un numero sempre maggiore di organizzazioni ha messo in sicurezza i propri gateway e-mail. Di conseguenza, i criminali informatici stanno disseminando codice malevolo in siti Web "innocenti". Dopodiché, il codice resta semplicemente in attesa e infetta silenziosamente i computer che li visitano.

La scala di questa operazione criminale ha raggiunto proporzioni tali che Sophos scopre una nuova pagina Web infetta ogni 4,5 secondi, 24 ore su 24, 365 giorni l'anno. Inoltre, SophosLabs, la nostra rete globale di centri di analisi delle minacce, riceve circa 20.000 nuovi campioni di codice sospetto al giorno.

Il 2008 ha dimostrato che il malware non è un problema che riguarda solo Microsoft. Anche se il numero puro e semplice di minacce Windows è di gran lunga superiore agli attacchi contro qualsiasi altra piattaforma, i criminali informatici stanno rivolgendo la loro attenzione a sistemi operativi come quelli Apple Macintosh e a software multipiattaforma vulnerabile. È probabile che questa tendenza continui anche nel 2009, di pari passo con la crescente popolarità di dispositivi portatili come iPhone, iPod Touch, telefoni con sistema operativo Google Android e notebook portatili.

Uno sguardo al 2008

Minacce malware più gravi: attacchi contro i siti Web tramite iniezione di codice SQL; aumento dello scareware

Nuove infezioni Web: ogni 4,5 secondi Sophos scopre una nuova pagina Web infettata

Allegati e-mail malevoli: alla fine del 2008, quintuplicati rispetto all'inizio dell'anno

Pagine Web con spam: ogni 15 secondi Sophos scopre una nuova pagina Web

Nuovi siti Web scareware: cinque siti identificati al giorno

Principale Paese che ospita malware: U.S.A., con il 37%

Paese che invia più messaggi spam: Asia con il 36,6%

Quantità di e-mail aziendali costituita da spam: 97%

Per le organizzazioni, resta di fondamentale importanza difendersi in tutte le fasi della loro attività, non soltanto a livello di gateway e-mail e Web. Le reti, i desktop, i laptop e i dispositivi mobili vanno messi in sicurezza nella loro totalità, per difenderli contro la miriade di minacce diffuse dai cybercriminali.

Sfruttamento di siti Web legittimi

Negli ultimi due anni, Internet è diventato un grande vettore di attacchi da parte dei criminali informatici, prendendo il posto dei sistemi e-mail, che in passato erano quelli presi maggiormente di mira. Sfruttando i siti Internet legittimi scarsamente protetti, gli hacker sono riusciti a impiantare codice malevolo al loro interno, con l'obiettivo di infettare ogni visitatore. Uno dei motivi per cui Internet è tanto diffusa è che i siti Web legittimi possono attrarre un gran numero di visitatori, i quali sono tutti delle potenziali vittime.

Nel corso del 2008, molte organizzazioni e marchi conosciuti sono caduti vittima di questo tipo di attacco. Sono state prese di mira sia le organizzazioni grandi che quelle piccole, a testimoniare l'importanza di un'adeguata sicurezza in Internet.

- **Gennaio 2008**: Migliaia di siti Web appartenenti a società incluse nella classifica Fortune 500, enti statali e istituti d'istruzione sono stati infettati da codice malevolo.
- **Febbraio 2008:** ITV, una rete televisiva del Regno Unito, è stata vittima di una campagna pubblicitaria infetta diffusa via Web, studiata per introdurre scareware nei computer degli utenti Windows e Mac[1].
- **Marzo 2008:** È stato attaccato un sito per la vendita di biglietti per i Campionati europei di calcio 2008[2], mentre Trend Micro, l'azienda produttrice di software antivirus si è vista violare alcune delle pagine del suo sito[3].
- **Aprile 2008:** Il sito Web della Cambridge University Press è stato violato e i visitatori del suo dizionario online hanno subito tentativi di esecuzione di script non autorizzato nei loro computer[4].
- **Giugno 2008:** Subito dopo l'inizio del torneo di tennis di Wimbledon, il sito dell'ATP (Association of Tennis Professionals) è stato infettato[5].
- **Luglio 2008:** Il sito Web della US PlayStation di Sony ha subito un assalto con iniezione di codice SQL che ha fatto correre ai visitatori il rischio di subire un attacco scareware[6].
- **Settembre 2008:** La rivista ***BusinessWeek*** è stata infettata tramite un attacco con iniezione di codice SQL, il quale ha tentato di scaricare malware da un server con sede in Russia[7].
- **Ottobre 2008:** Un'area del sito Web Adobe, progettata per fornire assistenza ai blogger video, è stata compromessa da un attacco con iniezione di codice SQL[8].

Attacchi con iniezione di codice SQL

Una delle notizie che ha fatto maggiore scalpore nel 2008 è stata l'attacco con iniezione di codice SQL. Attacchi di questo genere sfruttano le vulnerabilità del sistema di sicurezza e inseriscono codice malevolo (in questo caso, tag di script) nel database che gestisce un sito. Quando i dati immessi dall'utente, come ad esempio quelli relativi a un modulo Internet, non vengono filtrati o controllati correttamente, il codice prende di mira il database mediante istruzioni di codice malevole. Il ripristino può risultare difficile ed esistono numerosi casi di proprietari di siti Web che ripuliscono il loro database per poi subire nuovi attacchi dopo qualche ora.

Sistemi automatici

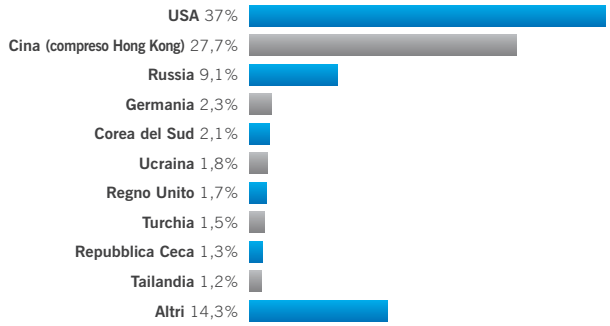
Gli hacker hanno sviluppato degli strumenti automatici che utilizzano motori di ricerca come Google per identificare i siti Web potenzialmente vulnerabili e iniettare codice nei loro server. I siti Web vengono raramente presi di mira appositamente e spesso subiscono soltanto la cattiva sorte di venire scoperti dallo strumento di distribuzione di malware dei criminali informatici.

Inoltre, i criminali informatici stanno realizzando i propri siti Web infettati da malware, utilizzando spesso dei servizi di web-hosting gratuiti, i quali non richiedono agli utenti di sottoporsi a una rigorosa procedura di identificazione. Dopodiché, utilizzano sistemi automatici per inserire collegamenti malevoli nei blog e nei forum legittimi, i quali puntano a questi siti infetti.

Ad esempio, nel 2008, Sophos ha riscontrato numerosi esempi di blog e bacheche di messaggi legittimi, i quali contenevano commenti con collegamenti a siti Web che avrebbero dovuto offrire video per adulti, ma la cui visione rendeva invece necessario un aggiornamento del plug-in del browser. Il codec finto aggiornato o il software Flash Player fasullo che l'utente scaricava era in realtà scareware che tentava di impaurire l'utente per indurlo ad acquistare falso software per la sicurezza.

I primi 10 Paesi che ospitano malware in Internet

Il 2008 ha rivelato che USA, Cina e Russia ospitano quasi i tre quarti dei siti Web che diffondono malware. Tuttavia, non sarebbe corretto ritenere che gli altri Paesi non stiano contribuendo anch'essi all'ampliarsi del problema.



I primi 10 Paesi che ospitano malware

Le ricerche Sophos rivelano che esiste un effetto "onda lunga", con oltre 150 Paesi identificati che ospitano malware nelle pagine Web all'interno dei loro confini nazionali. Di queste pagine Web infettate, l'85% si trova in siti Web legittimi che sono stati attaccati dagli hacker.

Classifica del malware

- Gli Stati Uniti guidano la classifica con poco meno di 3 pagine Web infettate su 8. Questi dati mostrano un aumento rispetto al 2007, in cui le pagine infettate erano meno di 1 su 4 (23,4%).
- La Cina, che è stata responsabile di oltre metà (51,4%) di tutto il malware a livello mondiale nel 2007, adesso ha praticamente dimezzato il suo contributo al problema.
- La Repubblica Ceca figura per la prima volta nell'elenco e ospita oltre l'1% di tutto il malware.
- Nel 2007, Polonia, Francia, Canada e Olanda erano rispettivamente in sesta, ottava e nona posizione, ma adesso contano un numero ridotto di siti Web malevoli e non figurano più nell'elenco.

Resistenza degli utenti

Anche se la sicurezza Web è studiata per fornire protezione contro malware e altre minacce, alcuni utenti hanno reagito negativamente e hanno adottato comportamenti che mettono a repentaglio la protezione. Questo è particolarmente vero nei casi in cui le aziende e le organizzazioni filtrano gli URL di siti Web particolari, per motivi legati ai criteri adottati, ad esempio bloccando i siti sociali o in cui è possibile scaricare video.

Proxy anonimi

Alcuni utenti hanno reagito al filtraggio Web utilizzando i proxy anonimi[9], i quali celano la vera natura di un sito per indurre il filtro di un'organizzazione a consentire l'accesso.

Le informazioni sui proxy anonimi pubblici vengono condivise liberamente in migliaia di blog, forum e siti Web ed esiste un numero sconosciuto di proxy anonimi privati realizzati per l'uso da parte di individui o piccoli gruppi. Questo rende estremamente semplice per gli utenti accedere a un proxy anonimo, ma per gli amministratori risulta difficile rilevarli e bloccarli. Se gli utenti stanno navigando mediante proxy anonimi, oltre a oltrepassare il filtraggio URL, eludono anche la scansione del contenuto a livello perimetrale, il che fa aumentare drasticamente la possibilità di infezione.

Sophos ha addirittura identificato proxy anonimi che sono essi stessi infettati da malware. Non è possibile stabilire se i proxy anonimi siano vittime innocenti dell'infezione oppure se siano stati configurati con malware incorporato. Tuttavia, a prescindere dal fatto che l'infezione sia premeditata o meno, chiunque li utilizzi corre effettivamente il rischio di infettare il computer e la rete alla quale è connesso.

I proxy anonimi sembrano essere prevalenti tra gli istituti scolastici, in cui gli studenti con approfondite conoscenze informatiche tentano di sovvertire i criteri di utilizzo accettabili. Sophos controlla attivamente i forum Internet per scoprire nuovi servizi proxy anonimi e incorpora il rilevamento in tempo reale di proxy anonimi privati mediante il controllo del traffico nella relativa Web appliance.

Minacce via e-mail

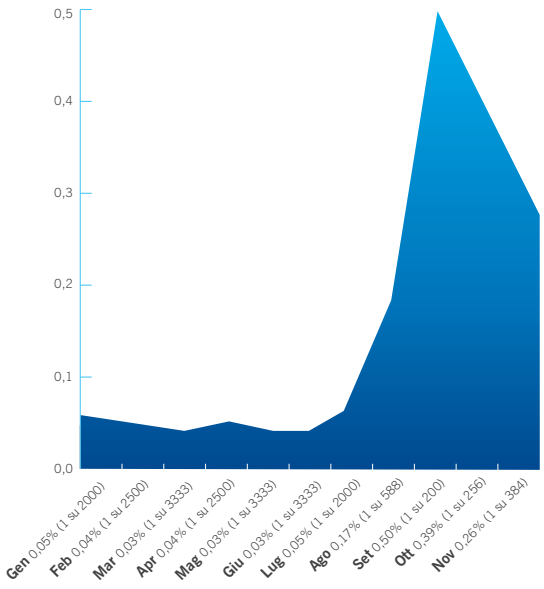
Gli allegati infetti sono in aumento

Negli ultimi anni, il numero di minacce diffuse tramite gli allegati di posta elettronica è diminuito.

Anno	E-mail con allegati infettati (media)
2005	1 su 44
2006	1 su 337
2007	1 su 909
2008	1 su 714

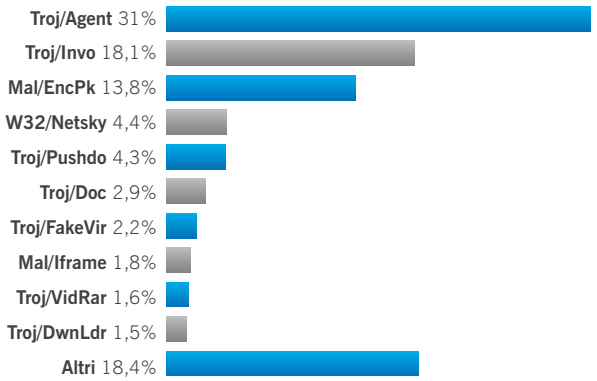
Tuttavia, mentre le minacce Web hanno rivelato la tendenza a dominare l'agenda del malware negli ultimi 12 mesi, alla fine del 2008 è stato riscontrato un numero cinque volte maggiore di allegati e-mail malevoli rispetto all'inizio dell'anno.

L'aumento risulta più evidente se analizzato mese per mese: da appena 1 su 3333 nel primo trimestre dell'anno fino a ben 1 su 200 in settembre.



Percentuale di allegati e-mail infetti nel 2008, mese per mese

Sophos ha appurato che gran parte di questo aumento è attribuibile ai numerosi attacchi su grande scala effettuati dagli spammer dal mese di agosto 2008 in poi. Gli attacchi massicci durante questo periodo includevano il Trojan Invo-Zip, il quale era mascherato da avviso di mancato recapito di un pacchetto da parte di società come FedEx e UPS[10]. Il Trojan Agent-HNY si era diffuso assumendo la forma del gioco Penguin Panic Apple iPhone[11], mentre il Trojan EncPk-CZ era mascherato da patch di protezione Microsoft[12].



I primi 10 malware degli allegati e-mail del 2008

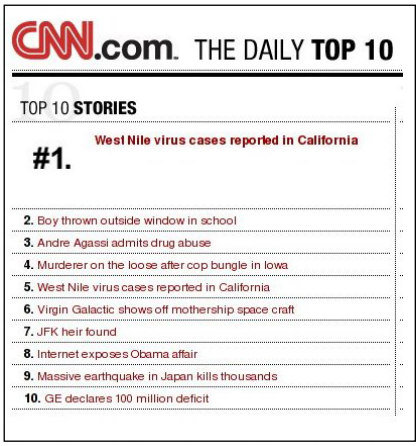
L'entità degli attacchi e-mail nella seconda metà del 2008 è osservabile nel Trojan Pushdo[13] (il quale offriva immagini senza veli di Angelina Jolie e Nicole Kidman), presente nel 31% di tutte le segnalazioni nella prima metà dell'anno.

Il rapido dominio di Troj/Agent e Troj/Invo nel campo del malware degli allegati e-mail, che rappresenta quasi il 50%, è notevole in quanto risulta superiore al worm Netsky, il quale ha costantemente occupato le prime posizioni della classifica sin dal suo rilascio, all'inizio del 2004[14]. Mentre Netsky contiene codice che ha la capacità di autoreplicarsi e diffondersi via Internet, l'agente e i Trojan Invo non possono viaggiare autonomamente, ma si affidano allo spam, usando solitamente un computer violato come base di partenza.

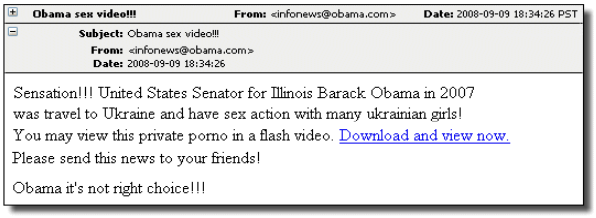
Collegamenti malevoli

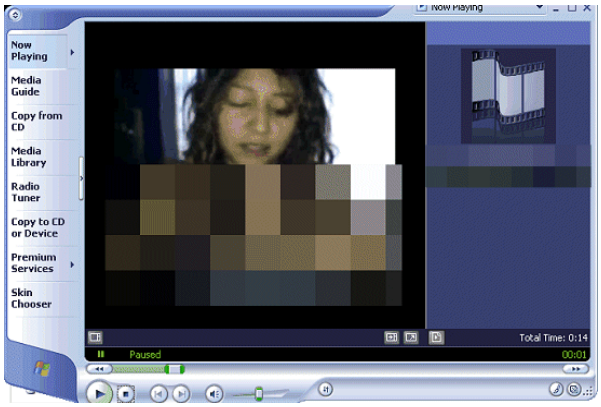
Oltre a utilizzare allegati e-mail malevoli, i criminali informatici continuano a incorporare collegamenti malevoli nelle e-mail e a diffondere attacchi creativi e puntuali miranti a stuzzicare la curiosità degli utenti.

Ad esempio, nel mese di agosto 2008, Sophos ha informato di un'ondata di messaggi spam in cui si annunciava l'offerta delle ultimissime notizie delle reti televisive MSNBC e CNN[15]. Ciascuna e-mail invitava gli utenti a fare clic su un collegamento per leggere le notizie, per poi indirizzarli a una pagina Web malevola che infettava il computer Windows con il Trojan Mal/EncPk-DA.



Nel mese di settembre 2008, ebbe ampia diffusione un'e-mail contenente un collegamento a quello che sembrava essere un video pornografico del candidato alla presidenza USA Barack Obama[16]. In realtà, la relativa pagina Web installava il malware Mal/Hupig-D.





Il giorno della vittoria elettorale di Obama, un'altra campagna di malware invitava i destinatari a fare clic su un collegamento Web per guardare un video del candidato democratico vincitore delle elezioni[17]. In realtà, visitando il sito Web i dati personali sarebbero stati trafugati dal computer della vittima e inviati a un server ubicato a Kiev, in Ucraina.

Paura dell'infezione

Un metodo ampiamente utilizzato dai criminali informatici per fare soldi durante il 2008 consisteva nell'utilizzo di finto software antivirus, noto anche come scareware o rogueware. Questo tipo di attacchi sfrutta i timori degli utenti nel campo della sicurezza IT e li induce a ritenere che il loro computer abbia un problema, mentre in realtà non è assolutamente vero.

Di solito, lo scareware viene installato nei siti Web sotto forma di inserzioni pubblicitarie a comparsa o file scaricabili camuffati. Tuttavia, vi sono anche dei casi in cui gli hacker hanno messo in circolazione scareware, o collegamenti ad esso, utilizzando le tradizionali tecniche di ingegneria sociale per ingannare gli utenti e indurli a fare clic sull'allegato o sul collegamento. Solo in una delle sue trappole spam, Sophos rileva circa 5000 e-mail di questo tipo ogni giorno.

I siti Web collegati allo scareware spesso contengono programmi di sicurezza che sembrano non creare alcun tipo di problema, con tanto di recensioni fasulle relative alla loro efficacia nell'eliminare i virus. Talvolta i siti Web trafugano i dettagli della carta di credito degli utenti.

Le bande di hacker si sono specializzate nella rapida creazione di siti Web fasulli dall'aspetto professionale, che sembrano offrire soluzioni di sicurezza legittime. Mediamente, Sophos identifica 5 nuovi siti scareware al giorno, ma talvolta il numero è superiore a 20 al giorno. Anche le aziende ben affermate che producono Norton AntiVirus[18] e AVG sono state prese di mira.

Alcune società produttrici di software legittimo sono state vittime di raggiri, tramite false campagne pubblicitarie miranti ad aumentare le vendite di prodotti legittimi.

Le motivazioni dei responsabili del problema dello scareware risultano evidenti analizzando il caso di Lee Shin-ja, ex amministratore delegato di una società coreana produttrice di antivirus. Si dice che Lee abbia guadagnato oltre 9,8 milioni di dollari, dal 2005, grazie a un programma anti-spyware gratuito che visualizzava avvisi di sicurezza fasulli e invitava gli utenti ad acquistare la soluzione antivirus Doctor Virus della sua azienda[19].

Inutile dire che il problema dello scareware non è limitato ai computer Windows. Nel febbraio 2008, Sophos ha rilevato campagne di scareware che avevano preso di mira sia gli utenti Windows che Apple Mac[20].

Malware in movimento

È in aumento anche il malware trasferito tramite USB memory stick. Forse la storia più strana relativa al malware USB, di cui si è venuto a sapere durante il 2008, è stata quella degli astronauti che avevano infettato i computer della stazione spaziale internazionale a causa delle misure di sicurezza insufficienti[21].

Attacchi malware tramite le reti sociali

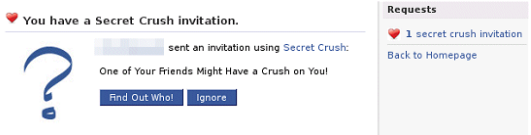
Il 2008 ha visto un notevole aumento della diffusione del malware tramite i siti di reti sociali. In agosto, Facebook ha ammesso che i profili di circa 1800 utenti erano stati manomessi da un attacco che aveva segretamente installato un Trojan che mostrava l'animazione di un buffone di corte che faceva una pernacchia[22 e 23].

Inoltre, i membri di Facebook stanno ricevendo messaggi dagli account colpiti dagli hacker degli amici, tramite la rete sociale, e vengono indirizzati a siti Web di terzi appositamente studiati per infettare il computer del destinatario[24]. Gli hacker hanno trovato conveniente violare gli account Facebook, trafugando nomi utente e password per poi utilizzarne i profili come trampolino di lancio per attacchi malware e spam su vasta scala[25].

Vi sono inoltre delle applicazioni Facebook di terzi studiate per visualizzare annunci irritanti[26]. Tuttavia, sembra che queste siano diventate meno pericolose da quando Facebook ha cambiato l'interfaccia utente, relegando a un ruolo di importanza secondaria le applicazioni di terzi.

Sfruttamento di programmi più ampi

Invece di cercare semplicemente le vulnerabilità del sistema operativo e del browser, gli hacker stanno anche analizzando le falle di sicurezza in altri programmi e strumenti di largo uso, come Adobe Flash e i file PDF.



L'aumento di file malevoli Flash e PDF può essere in parte spiegabile con l'utilizzo di kit di costruzione di malware che consentono di creare pagine Web in cui è incorporato codice-trappola. L'inclusione del contenuto Flash e PDF prende di mira le vulnerabilità che sono state riscontrate nei plugin del browser Adobe, sottolineando l'importanza di tenere aggiornati questi strumenti.

Inoltre, nel 2008 c'è stato un aumento del 46% nella quantità di rootkit della modalità kernel. Questi rootkit tentano di eludere il rilevamento da parte dei tradizionali prodotti per la sicurezza camuffandoli mediante sofisticate tecniche del sistema operativo di basso livello.

Il malware per aree geografiche

Le ricerche SophosLabs hanno identificato malware scritto in un totale di 44 lingue diverse, anche se non è stato possibile estrarre informazioni sull'area geografica nel 47,9% dei campioni di malware esaminati.

La Cina è responsabile dell'11,6% di tutto il malware. Si tratta di una percentuale più piccola rispetto al 2007, quando gli hacker della Repubblica Popolare erano responsabili del 21% del codice malevolo proveniente da un'area geografica particolare. L'analisi in base alla lingua ha dato i seguenti risultati:

- Paesi di lingua anglosassone – 24,5%
- Cinese – 11,6%
- Tedesco – 3,7%
- Francese – 3,1%
- Russo – 3%
- Portoghese brasiliano – 1,6%
- Altre lingue – 4,6%

Inoltre, l'analisi ha evidenziato alcune differenze interessanti per quanto riguarda le motivazioni e le tattiche utilizzate dai vari gruppi di hacker a livello mondiale.

Gran parte del malware cinese assume la forma di backdoor Trojan, ma vi è anche una certa percentuale di malware cinese il cui obiettivo è rubare le password a chi gioca in Internet.

La maggior parte del codice malevolo scritto in Brasile è costituito da Trojan creati per trafugare informazioni alle banche online. Gli hacker russi, invece, si stanno concentrando in gran parte nella creazione di botnet e nell'apertura di backdoor che consentano ai criminali informatici di accedere ai computer violati.

La storia di tre società Internet

Atrivo
ISP con sede in California (noto anche come Intercage) è stato disconnesso da Internet in settembre, in seguito alla pubblicazione di notizie in base alle quali gran parte della sua rete veniva utilizzata per mettere in giro software anti-virus (o scareware) e malware fasullo[27].

ESTDomains
Furono sollevati dei dubbi su Vladimir Tsastsin, un signore di etnia russa che viveva in Estonia[28], fondatore di EstDomains, un servizio di registrazione di domini e, per coincidenza, cliente di Atrivo. La sua società fu accusata di fornire un riparo sicuro ai criminali che registravano domini per attività malevole, facendo in modo che le loro attività non venissero chiuse quando EstDomains riceveva segnalazioni di abusi.

Dopo che il governo estone ebbe accusato Tsastsin di frode con carte di credito, riciclaggio e altri reati, ICANN gli ritirò la licenza di società autorizzata alla registrazione di domini.

McColo
Un'altra rete di proprietà di un russo, McColo, fu accusata da più parti di ospitare centri di comando e controllo di cinque grandi botnet: Srizbi (Zlob), Mega-D, Rustock, Dedler e Storm.

Quando McColo venne disconnessa da Internet alle 13:23 dell'11 novembre 2008[29], le botnet si disattivarono, determinando un enorme calo dei livelli di spam. I volumi di spam scesero immediatamente del 75%[30] subito dopo la disconnessione di McColo. Da allora gli hacker hanno tentato di riacquisire il controllo di tali botnet, con un certo

successo[31].

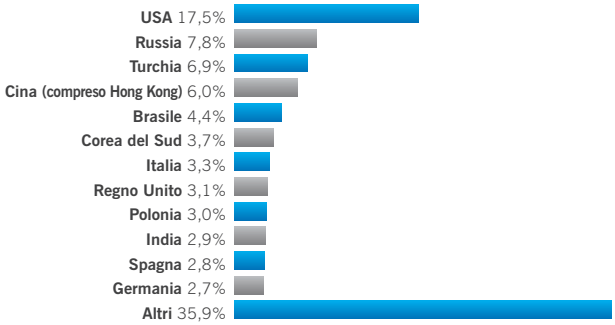
Questi esempi hanno evidenziato che quando c'è collaborazione tra coloro che si occupano di sicurezza, si riesce a ostacolare con successo le attività dei criminali informatici su scala globale. In effetti, la cessazione dell'attività di McColo ha avuto più di una conseguenza sui livelli di spam globali (anche se temporaneamente) di qualsiasi arresto di hacker mai effettuato da parte delle autorità.

Lo spam è ancora popolare

Lo spam resta ancora un grave problema per le aziende: le ricerche Sophos hanno evidenziato che addirittura il 97% delle e-mail delle aziende è costituito da spam. Sophos riceve milioni di nuovi messaggi ogni giorno dalla propria rete di trappole per spam.

Lo spam Paese per Paese

Nel 2008, lo spam è stato inviato da 240 Paesi. Gli Stati Uniti hanno diminuito il loro gestendo il 17,5% di tutto lo spam rispetto al 22,5% nel 2007. Tuttavia, resta ancora molto da fare per risolvere il problema.



I primi 12 Paesi che hanno inviato spam nel 2008

Gli Stati Uniti sono ancora responsabili della maggior parte delle e-mail indesiderate del mondo, ad alcune delle quali è allegato malware. Altre invece contengono dei collegamenti a siti Web malevoli o infetti. La maggior parte di questo spam proviene da utenti domestici inconsapevoli, i cui computer fanno parte di una botnet.

Tuttavia, il problema delle botnet può essere considerato globale. È evidente che un numero maggiore di computer richiede una protezione antivirus aggiornata e le più recenti patch di sicurezza. Inoltre, gli utenti inesperti vanno istruiti adeguatamente su come evitare di mettere a repentaglio i propri dati personali e il computer.

Siete degli spammer?

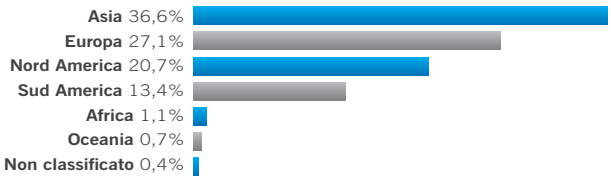
Praticamente tutti i messaggi spam provengono da computer violati (chiamati “bot” o “zombi”) che, all’insaputa dei loro proprietari, vengono usati dagli hacker per inviare grandi volumi di spam, lanciando attacchi Denial-of-Service distribuiti o rubando informazioni riservate.

Disporre di una protezione antivirus aggiornata, installare ed eseguire un firewall e assicurarsi che tutte le patch di sicurezza siano aggiornate sia per il sistema operativo che per le applicazioni installate riduce notevolmente la probabilità di subire attacchi.

Il servizio Sophos ZombieAlert™[32] identifica i computer aziendali che sono stati violati e che stanno inviando e-mail a nome degli spammer.

Spam per continente

L’Asia è responsabile di oltre un terzo di tutto lo spam e insieme all’Europa contribuisce per quasi due terzi alle e-mail indesiderate a livello mondiale.



Spam inviato per continente nel 2008

Spam dei blog

Lo spam non viene inviato soltanto per posta elettronica. I blog Internet, i quali invitano i visitatori a lasciare commenti, vengono utilizzati in misura sempre maggiore da bot automatici alla ricerca di pagine vulnerabili.

Si stima che oltre l'85% di tutti i commenti inviati ai blog siano di fatto costituiti da spam[33], anche se molti blog utilizzano strumenti gratuiti per tentare di filtrare i contenuti prima della pubblicazione.

Spam e reti sociali

Nel 2008 gli spammer si sono rivelati molto intraprendenti nel provare nuovi metodi per distribuire i loro messaggi di marketing e malware. I siti di reti sociali, come Facebook e Twitter, sono stati presi di mira in modo particolare.

Di solito gli hacker rubano i nomi utente e le password dei membri, quindi bombardano gli amici e i familiari delle vittime con messaggi di marketing ben camuffati, indirizzandoli alle pagine Web di terzi.

È inoltre emersa un'interessante tendenza a sfruttare le reti sociali. Gli imbroglioni si intrufolano negli innocui account di Facebook presentandosi come persone normali. Dopodiché, diffondono messaggi spam agli amici delle persone che entrano in contatto con loro, con la scusa che durante una vacanza all'estero sono stati scippati e hanno perso il portafogli e il biglietto aereo. Infine, fanno richieste di denaro da inviare tramite Western Union[34].

Gli utenti di computer che normalmente sarebbero sospettosi nel ricevere e-mail di questo tipo nella loro casella postale, diventano più malleabili nel comunicare tramite Facebook con un contatto che considerano amichevole. I truffatori possono sfruttare ulteriormente la rete conversando con le loro vittime designate e servendosi delle informazioni degli account che hanno violato. Ad esempio, se il proprietario dell'account violato ha raccontato ai suoi amici di Facebook, tramite un messaggio di stato, di essere in viaggio in un determinato Paese, la storia del truffatore risulterà molto più credibile.

È bene che gli utenti di Internet diventino più scettici e cinici in merito a tali messaggi, se in futuro non vogliono incorrere negli stessi errori di eccessiva fiducia.

Nel novembre 2008, Facebook è stato risarcito con 873 milioni di dollari grazie alla sentenza di un tribunale che ha condannato uno spammer con sede a Montreal per avere inviato oltre quattro milioni di messaggi agli utenti tramite account violati[35]. Sophos ha assistito al repentino aumento dello spam inviato tramite i siti di reti sociali e prevede che questa tendenza continuerà.

Altre tendenze dello spam

Lo spam tramite "newsletter" sta diventando un metodo di diffusione molto utilizzato; gli spammer copiano modelli e struttura delle newsletter legittime. Anche gli hacker utilizzano account di posta elettronica come Gmail, Hotmail e Yahoo per diffondere lo spam in tutto il mondo, dopo aver violato il sistema CAPTCHA (Completely Automated Procedure for Telling Computer and Humans Apart, procedura completamente automatica per distinguere computer e umani).

Utenti Mac, un bersaglio facile

Il problema rappresentato dal malware per Apple è limitato rispetto alla situazione per gli utenti Windows. Tuttavia, dopo la comparsa dei primi casi di malware animati da motivazioni finanziarie per Mac OS X alla fine del 2007, ci sono stati più tentativi da parte degli hacker di infettare i computer Mac.

Nel febbraio 2008, un nuovo Trojan basato su Flash, Troj/Gida-B[36], fu progettato per indurre gli utenti ad acquistare software di sicurezza fasullo. Lo scareware utilizzava inserzioni pubblicitarie dannose che funzionavano bene sia su computer Mac che Windows.

Il Trojan OSX/Hovdy-A[37], scoperto nel giugno 2008, è in grado di infettare anche i computer Mac OS X e tenta di rubare le password, aprire i firewall e disattivare le impostazioni di sicurezza. Sfrutta la vulnerabilità segnalata di recente in Mac OS X, ARDAgent, per accedere alla cartella principale. Dopo che un computer è stato infettato l'hacker può assumere il controllo completo e coprire le sue tracce mediante la disattivazione del registro di sistema.

Nell'agosto 2008, fu scoperto Troj/RKOSX-A[38], uno strumento Mac OS X che consentiva agli hacker di creare backdoor Trojans. Tre mesi dopo, Sophos annunciava la scoperta di un nuovo malware Mac che si installava nei siti Web: OSX/Jahlav-A[39]. Questo Trojan finge di essere un'applicazione legittima, ma una volta installato scarica componenti aggiuntivi da un server in Olanda.

Anche se nel mondo la diffusione di Malware Mac è più limitata, vi sono numerosi fattori di cui gli utenti Mac dovrebbero tenere conto.

- Un elevato livello di sottovalutazione nella comunità Mac significa che molti utenti credono erroneamente di essere immuni alle minacce della sicurezza in Internet. Questo li rende un bersaglio facile per i futuri attacchi.
- L'utilizzo di chip basati su Intel nell'hardware Apple Mac ha contribuito alla diffusione di Windows sui Mac. Pertanto, adesso i Mac hanno maggiori probabilità di ospitare e diffondere malware Windows.
- Il 2008 ha visto vendite record di computer Apple Mac[40], con alcuni utenti che hanno abbandonato i PC a causa della delusione di Windows Vista. Con la crescita della quota di mercato di Apple Mac, gli utenti Mac probabilmente sono destinati a subire un maggior numero di attacchi.

Con così tanti utenti domestici Windows non in grado di difendersi adeguatamente contro malware e spyware, sembra essere plausibile ritenere che alcuni di essi decideranno di passare alla piattaforma Apple Mac. Questa ipotesi prende campo non perché Mac OS X sia superiore, ma semplicemente perché attualmente per esso viene scritto molto meno malware. Nel prossimo futuro, i criminali informatici che cercano di ottenere il massimo dalle loro azioni probabilmente continueranno ad attaccare principalmente i computer Windows.

Tuttavia, il malware mirato ai sistemi Mac continuerà a essere scritto ed è bene che gli utenti continuino ad adottare le migliori pratiche IT che garantiscono la sicurezza, come ad esempio l'esecuzione di un prodotto antivirus e l'aggiornamento delle patch di protezione.

Falle nella sicurezza degli smartphone

Accompagnato da un grande clamore, il 2008 è stato l'anno del lancio della versione 3G dell'Apple iPhone, il primo telefono a utilizzare il sistema operativo per cellulari Google Android.

Apple iPhone

Non vi è alcun dubbio che la versione 3G dell'iPhone sia più allettante per le aziende e gli utenti di Internet rispetto alla versione precedente, grazie alla sua maggiore connettività e al prezzo più competitivo. Analizzando i suoi risultati finanziari più recenti, Apple ha reso noto che l'iPhone stava vendendo di più del noto concorrente Blackberry di RIM[41].

Tuttavia, l'aumento della quota di mercato di Apple potrebbe a sua volta favorire ulteriori tentativi di attacco concertati dai criminali, che in futuro tenteranno di violare i dispositivi.

Anche se da sempre si scopre malware semplice, l'iPhone non è ancora stato preso di mira dagli hacker con motivazioni finanziarie. Tuttavia, nell'applicazione e-mail mobile e nel browser Safari di Apple sono state riscontrate delle falle nella sicurezza e l'azienda è stata criticata per non aver creato delle patch per questi punti deboli, come invece è avvenuto per gli altri computer in cui è installato Mac OS X.

Gli utenti dell'iPhone devono essere consapevoli che potrebbero essere più vulnerabili agli attacchi di phishing rispetto ai computer desktop, in quanto:

- Dovendo immettere gli URL tramite lo schermo tattile potrebbero venire maggiormente tentati di fare semplicemente clic sui collegamenti indicati nelle e-mail.
- La versione iPhone di Safari non visualizza gli URL incorporati nelle e-mail prima che vi si faccia clic sopra. Pertanto, per gli utenti è più difficile stabilire se il collegamento indirizza, ad esempio, al sito fasullo di una banca online.
- Il browser dell'iPhone visualizza solo URL parziali nella sua barra degli indirizzi e pertanto per i criminali informatici è più semplice indurre gli utenti a credere che stanno visitando un sito Web legittimo.

Google Android

Al momento della pubblicazione del presente documento, l'unico telefono cellulare sul mercato a utilizzare il sistema operativo Google Android è il T-Mobile G1, che gli hacker hanno appena iniziato a prendere di mira. Anche se le prime versioni evidenziavano principalmente le differenze "estetiche" rispetto all'Apple iPhone (come la tastiera estraibile e lo schermo tattile meno flessibile), è stata ben presto scoperta una vulnerabilità del browser G1[42].

Sono stati inoltre sollevati dei dubbi sull'apertura di Google verso le applicazioni, il che potrebbe facilitare la distribuzione di programmi malevoli tra gli utenti del telefono.

Sophos ritiene che probabilmente i primi esempi di malware per questi sistemi operativi saranno scritti da appassionati desiderosi di far parlare di sé, piuttosto che da criminali con motivazioni di carattere finanziario. Tuttavia, quando il numero di acquirenti avrà raggiunto qualche milione, la creazione di malware per i cellulari diventerà sempre più allettante per i malintenzionati. Un esempio in merito potrebbe essere la creazione di un attacco generico per Mac OS X, in grado di minacciare le funzionalità più comuni e la tecnologia dei computer Mac e dell'iPhone[43].

Allo stesso modo, ci sarebbe poco da sorprendersi se venissero lanciati degli attacchi sperimentali contro gli utenti di Google Android.

Probabilmente tali attacchi sarebbero basati sull'ingegneria sociale, piuttosto che sulle vulnerabilità del software, per ingannare gli utenti e indurli a eseguire codice pericoloso. Di conseguenza, i proprietari di telefoni cellulari che hanno l'abitudine di aggiungere applicazioni di terzi senza prestare attenzione vedranno aumentare le possibilità che il loro dispositivo venga infettato.

Fuga di dati

Dati non sicuri

Nel 2008 si è parlato molto di fuga di dati, in quanto le aziende e gli enti statali hanno adottato criteri più ampi per la protezione dei loro dati riservati[44].

Le organizzazioni di tutte le dimensioni si sono rese conto che oggi i lavoratori mobili e i collaboratori devono poter accedere alle informazioni sia dall'ufficio che dal di fuori e devono poter avere la possibilità di condividerle con i colleghi e i partner.

Gli utenti utilizzano e condividono regolarmente i dati senza preoccuparsi troppo della riservatezza e delle leggi sulla protezione dei dati stessi. Quasi il 30% di essi archivia su supporti rimovibili dati relativi a contratti e aspetti finanziari, informazioni su clienti, obiettivi di vendita, contatti e account personali[45]. Questo ha provocato numerosi casi di perdita di dati, più spesso accidentali che malevoli.

Hardware utilizzato

Sono stati segnalati vari casi di dati riservati diventati di dominio pubblico in seguito alla vendita all'asta su eBay di vecchi computer, nei quali i dati sul disco rigido non erano stati cancellati[46].

Questo ha indotto alcuni osservatori a ritenere che su eBay vi sia una maggiore domanda (con conseguente aumento dei prezzi) di unità disco usate rispetto a quelle nuove. C'è poco da sorprendersi, vista la quantità di dati riservati potenzialmente recuperabile[47].

Cifratura

La procedura più importante per bloccare la fuga di dati consiste nella cifratura di dati sensibili archiviati nei laptop, nei dispositivi di memorizzazione rimovibili e nelle e-mail. Se i dati vengono cifrati con una password, non possono venire decifrati né utilizzati, a meno che la password non sia conosciuta. Ciò significa che anche se tutte le altre misure di sicurezza non riescono a impedire che un hacker acceda ai dati più sensibili, egli non riuscirà a leggerle e quindi a comprometterne l'integrità.

Perdere dati significa perdere denaro

Nell'agosto 2008, le autorità USA accusarono 11 persone di aver partecipato a un atto di pirateria informatica legato al furto di oltre 40 milioni di numeri di carta di credito e di debito. I negozi vittime degli attacchi comprendevano OfficeMax, Barnes & Noble, Boston Market e TJX, che gestisce i negozi al dettaglio TJ Maxx (noto come TK Maxx nel Regno Unito) e Marshalls.

Secondo i servizi segreti e il Ministero Giustizia, la banda di "piloti criminali" (che perlustrava una determinata zona alla ricerca di reti aziendali wireless non protette da violare) aveva installato programmi malevoli e venduto le informazioni rubate ad altri criminali negli Stati Uniti e in Europa dell'est. Decine di migliaia di dollari furono ritirati illegalmente dagli sportelli Bancomat utilizzando carte di credito clonate.

Il Ministero dell'Interno britannico ha reso noto il caso dello smarrimento di un dispositivo USB contenente i dati personali non cifrati di circa 130.000 criminali condannati. Le informazioni comprendevano i nomi, gli indirizzi, le date di nascita e in alcuni casi le date di rilascio dei prigionieri. Il dispositivo USB veniva utilizzato dalla società di consulenza PA Consulting, la quale di conseguenza perse un contratto da 1,5 milioni di sterline con il governo britannico.

La seconda procedura consiste nel controllare il modo in cui gli utenti trattano le informazioni. È opportuno non adottare comportamenti a rischio, come ad esempio il trasferimento di dati non cifrati su dispositivi USB. Le organizzazioni dovrebbero estendere la loro infrastruttura anti-malware al fine di:

- Controllare l'utilizzo delle informazioni.
- Garantire un funzionamento efficace.
- Assicurarsi che vengano rispettate le norme vigenti.

Considerando la possibilità dell'aumento di licenziamenti nel 2009, le organizzazioni dovrebbero inoltre adottare gli accorgimenti necessari affinché i dati contenuti nei dispositivi utilizzati dai dipendenti che lasciano l'azienda vengano adeguatamente cifrati o correttamente cancellati. Inoltre, è bene prendere in considerazione anche i rischi potenziali legati al sentimento di rancore provato da alcuni dipendenti licenziati, i quali potrebbero lasciare l'azienda portando con sé dati riservati o intraprendere un'attività di spionaggio industriale.

Crimini informatici sponsorizzati dagli stati

Lo spionaggio digitale è in crescita

I Paesi di tutto il mondo si spiano per ottenere vantaggi politici, commerciali e militari e sarebbe ingenuo pensare che non sfruttino computer e Internet per svolgere al meglio le loro attività.

Nel 2007, molti Paesi si accusarono reciprocamente e apertamente di condurre attività di spionaggio via Internet. Ad esempio, nel mese di settembre, l'esercito cinese fu accusato di un attacco al sistema informatico del Pentagono[48]. Le preoccupazioni legate ai crimini informatici sponsorizzati dagli Stati raggiunsero il culmine alla fine del 2007, con la scoperta che l'MI5, il servizio di sicurezza britannico, aveva scritto a 300 dirigenti e responsabili della sicurezza di aziende del Regno Unito avvertendole di un "attacco di spionaggio elettronico".

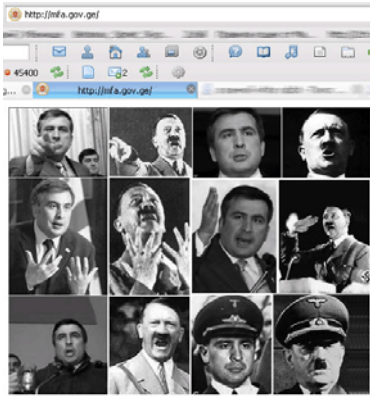
Nel 2008 il numero di presunti crimini informatici promossi dai governi nazionali è stato ancora maggiore. Anche se risulta estremamente difficile provare che un attacco è stato ordinato da uno Stato, probabilmente nel 2009 assisteremo a un maggiore numero di scambi di accuse tra Paesi che si attaccano e si spiano tramite Internet.

- **Aprile 2008.** ***Der Spiegel*** rese noto che il BND – i servizi segreti tedeschi – si è servito di spyware per monitorare il Ministero del commercio e dell'industria in Afghanistan[49]. Secondo il settimanale, documenti riservati, password e comunicazioni e-mail erano state violate dalle spie tedesche e inviati al quartier generale del BND. La notizia seguì le rivelazioni che il BND aveva intercettato le e-mail tra la giornalista dello ***Spiegel*** Susanne Koelbl e il ministro del commercio afgano Amin Farhang, provocando un incidente diplomatico tra i due Paesi.

- **Maggio 2008** Dei funzionari indiani di Nuova Delhi confermarono che gli hacker cinesi avevano preso di mira il Ministero degli esteri e il Centro informatico nazionale[50], che costituisce la dorsale della rete per il governo centrale e la pubblica amministrazione, oltre che per gli altri enti amministrativi indiani. I funzionari, di cui non furono rese note le generalità, avrebbero detto che questo era il modo in cui i cinesi intendevano acquisire un "vantaggio asimmetrico" sui potenziali avversari.

- **Maggio 2008.** Anche il Belgio accusò il governo cinese di spionaggio informatico, affermando che gli attacchi contro il governo federale belga erano partiti dalla Cina e probabilmente erano stati ordinati dal governo di Pechino[51]. In un'altra sede, il ministro degli esteri belga riferì al parlamento che il suo ministero era stato oggetto di spionaggio informatico da parte dei cinesi alcune settimane prima.

- **Agosto 2008.** Con l'aumentare della tensione, gli hacker di Ossezia del sud, Russia e Georgia si lanciarono degli attacchi reciproci[52]. Degni di nota furono un attacco "Denial of Service" contro il sito del governo dell'Ossezia del sud e l'oscuramento del sito del Ministero degli esterni georgiano,



sostituito con una serie di immagini del presidente georgiano Mikheil Saakashvili e di Adolf Hitler[53].

- **Settembre 2008.** Seoul accusò i suoi avversari della Corea del nord di aver trafugato i documenti di ufficiali militari ricorrendo a spyware e a un agente segreto[54]. L'attacco spyware assunse la forma di un allegato e-mail malevolo progettato per trafugare documenti da computer infettati. Gli indirizzi e-mail erano stati forniti dal trentacinquenne Won Jeong Hwa.

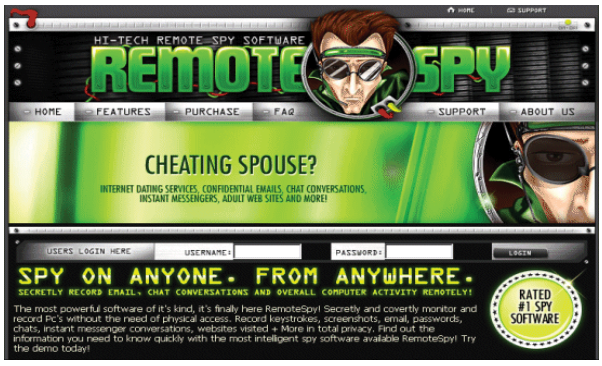
Dietro le sbarre

Le autorità internazionali per la lotta contro i crimini informatici hanno collaborato per contrastare i criminali informatici e negli ultimi dodici mesi il numero di arresti e dure sentenze contro quanti erano coinvolti in crimini di alto profilo finanziario è aumentato sensibilmente.

Ecco alcuni dei casi più famosi del 2008.

- **Gennaio 2008**. Tre uomini che avevano elaborato una sofisticata truffa via e-mail si dichiararono colpevoli di fronte a un tribunale di New York di aver rubato oltre 1,2 milioni di dollari[55]. Gli uomini misero in circolazione delle e-mail in cui l'autore affermava di essere affetto da un tumore maligno alla faringe e di avere intenzione di dare in beneficienza 55 milioni di dollari. Un membro della banda, Nnamdi Chizuba Ainsiobi, telefonava ai destinatari delle e-mail, contraffacendo la voce per fingere di essere affetto dalla malattia.
- **Febbraio 2008**. Un adolescente americano si dichiarò colpevole di aver preso il controllo di centinaia di migliaia di computer zombi e di averli utilizzati per visualizzare inserzioni pubblicitarie truffaldine[56]. Alcuni dei computer violati erano quelli della "Divisione armamenti" del Comando aereo delle forze navali USA e del Ministero della Difesa USA.

- **Marzo 2008** Un tribunale cinese condannò al carcere da sei a otto anni e mezzo quattro uomini che avevano utilizzato un Trojan per rubare i dati di conti bancari in Internet.[57]
- **Aprile 2008** Un tribunale israeliano condannò al carcere tre membri della società investigativa privata Modi'in Ezrahi dopo essere risultati colpevoli di aver utilizzato un Trojan per rubare informazioni commerciali.[58]
- **Maggio 2008**. Le autorità di U.S.A. e Romania incriminarono 38 persone sospettate di aver gestito un'organizzazione criminale internazionale che aveva preso di mira centinaia di istituti finanziari mediante e-mail di phishing e SMS[59].
- **Giugno 2008**. Il diciannovenne Jason Michael Milmont ammise di essere il programmatore del malware Nugache, che aveva infettato i computer Windows[60] trasformandoli in una sofisticata botnet controllata mediante un sistema peer-to-peer (P2P) e costituita da circa 5.000-15.000 PC violati contemporaneamente. Milmont utilizzava le informazioni bancarie rubate per accedere ai conti e acquistare merci.
- **Luglio 2008.** Una corte federale di Manhattan condannò il diciassettenne Adam Vitale a 30 mesi di reclusione per aver inviato oltre 1,2 milioni di messaggi spam in meno di una settimana[61]. Vitale aveva tentato di prendersi una quota dei profitti generati dalle vendita di merci tramite i messaggi.
- **Agosto 2008.**Le autorità olandesi arrestarono Leni de Abreu Neto, in seguito alla segnalazione dell'FBI e della polizia federale brasiliana[62]. Il trentacinquenne brasiliano aveva gestito e consentito l'accesso a una botnet comprendente 100.000 computer.
- **Settembre 2008**. Una banda di ladri di carte di credito, accusata di aver rubato 1,8 milioni di dollari canadesi a un'azienda di Calgary, fu sgominata dalla polizia canadese[63]. Uno degli arrestati era Ehud Tenenbaum, detto "l'analizzatore", che 10 anni prima era stato sorpreso nel tentativo di accedere illegalmente ai computer del Pentagono.
- **Ottobre 2008**. La FTC (Federal Trade Commission, commissione federale per il commercio) convinse un tribunale a bloc- care l'attività di un importante gruppo di persone dedite allo spam[64]. L'FTC affermò di aver ricevuto oltre tre milioni di proteste da parte di utenti di computer che avevano ricevuto e-mail relative alla campagna di spam, molte delle quali offrivano ciò che veniva descritto come una pillola per il miglioramento delle prestazioni sessuali maschili "sicura al 100% e a base di erbe naturali".
- **Novembre 2008**. Un tribunale USA ordinò alla CyberSpy Software LLC di cessare la vendita del software keylogger RemoteSpy in seguito alle indagini della FTC, la quale sospettava che esso venisse utilizzato per infrangere la legge[65]. Nel mese di dicembre il divieto fu sospeso[66].



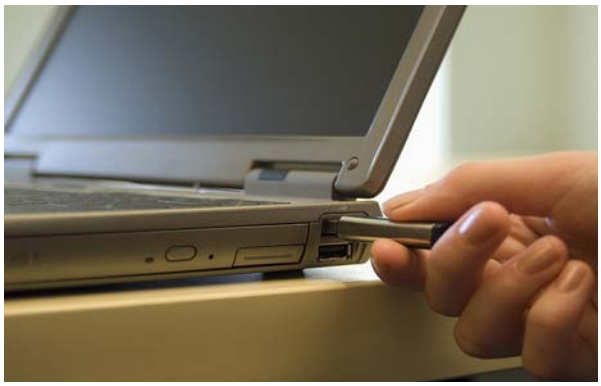
Il futuro

Maggiore complessità degli attacchi

Prevedere il futuro in un ambiente in così rapida evoluzione è praticamente impossibile. Per rendersi conto di quanto la minaccia sia diventata più grave è sufficiente osservare la frequenza con la quale il malware compare oggi rispetto a cinque anni fa.

Tuttavia, alcune cose sembrano certe:

- **La varietà degli attacchi** e il loro numero continueranno ad aumentare, dietro la spinta del crimine organizzato che mira a violare i computer per trafugare informazioni, identità e risorse.
- **La fuga di dati** diventerà un problema sempre più grande, specialmente con l'aumento dell'utilizzo delle tecnologie mobili. Molti Paesi hanno introdotto delle normative molto severe sulla divulgazione dei dati sensibili, o si accingono a farlo. Tali norme mirano a impedire alle aziende di ignorare le questioni legate alla sicurezza. Anche una fuga di dati di modesta entità ha le potenzialità per influire negativamente sulla reputazione dei prodotti e i servizi di un'azienda.



- **I PC violati**, sia nelle abitazioni private che negli uffici, continueranno a costituire la principale fonte di spam. Molte botnet stanno adottando un sistema di funzionamento tipo P2P decentralizzato e di conseguenza sarà sempre più difficile riuscire a riscuotere successi come la disattivazione del provider McColo, il quale fungeva da centro di comando e controllo delle botnet.
- **L'insicurezza di Internet**, in particolare la sua vulnerabilità agli attacchi remoti, come le iniezioni di codice SQL, continuerà a favorire la distribuzione di malware nato sul Web. I criminali informatici potranno continuare a inviare messaggi spam apparentemente innocenti contenenti collegamenti a pagine Web legittime, ma violate. Questi siti violati contengono collegamenti invisibili a contenuti malevoli.
- **Le e-mail malevole** includeranno una percentuale crescente di allegati o collegamenti via Internet a file non riconducibili a programmi (non eseguibili). Si tratterà di file di dati dall'aspetto legittimo, come ad esempio documenti di Word e file PDF, contenenti codice-trappola che sfrutta le vulnerabilità del software. La visualizzazione di questi file, che in un computer munito di patch risulterebbe innocua, potrebbe provocare un disastro invisibile su un computer che ne fosse sprovvisto.
- **Il furto di identità** continuerà ad avere effetti negativi sulla lealtà dei clienti. L'anno prossimo, le aziende dovranno garantire ai clienti di aver adottato misure di sicurezza adeguate e complete in modo da ridurre al minimo il rischio di violazione.

Gli utenti dei computer continueranno a doversi occupare dei problemi di sicurezza del controllo dei sistemi,in quanto i criminali tenteranno di sfruttare le nuove tecnologie per fare soldi e provocare danni. Inoltre, minacce quali il furto d'identità e le frodi informatiche continueranno a verificarsi anche in futuro, a causa degli errori umani.

Tuttavia, se gestito correttamente, il problema non dovrebbe rivelarsi insormontabile. Solide pratiche di sicurezza, aggiornamenti alla protezione e un impegno attivo per tenersi informati nel corso dell'anno aiuteranno le imprese a difendere le proprie reti.

La buona notizia è che il software di protezione migliora in continuazione. Il rilevamento proattivo delle minacce malware nuove e sconosciute funziona ottimamente e gli utenti sensibili al problema e adeguatamente difesi possono ridurre notevolmente i rischi.

Fonti

1. www.sophos.com/pressoffice/news/articles/2008/02/poisoned-adverts.html
2. www.sophos.com/pressoffice/news/articles/2008/03/euro2008.html
3. www.sophos.com/security/blog/2008/03/1186.html
4. www.sophos.com/security/blog/2008/04/1292.html
5. www.sophos.com/pressoffice/news/articles/2008/06/infected-tennis-sites.html
6. www.sophos.com/pressoffice/news/articles/2008/07/playstation.html
7. www.sophos.com/blogs/gc/g/2008/09/15/hackers-infect-businessweek-website-via-sql-injection-attack/
8. www.sophos.com/pressoffice/news/articles/2008/10/adobe-infection.html
9. www.sophos.com/security/sophoslabs/anonymizing-proxies.html
10. www.sophos.com/security/blog/2008/08/1685.html
11. www.sophos.com/blogs/gc/g/2008/09/17/hackers-distribute-trojan-as-iphone-game/
12. www.sophos.com/blogs/gc/g/2008/10/13/malicious-microsoft-security-patch-spammed-out-before-patch-tuesday/
13. www.sophos.com/pressoffice/news/articles/2008/07/security-report.html
14. www.sophos.com/pressoffice/news/articles/2004/03/va.html
15. www.sophos.com/blogs/gc/g/2008/08/07/exposed-cnn-top-ten-video-malware/
16. www.sophos.com/blogs/gc/g/2008/11/05/the-president-elects-first-malware-campaign/
17. www.sophos.com/blogs/gc/g/2008/09/10/barack-obama-sex-video-malware-campaign/
18. www.sophos.com/blogs/gc/g/2008/09/23/free-norton-antivirus-hackers-disguise-fake-product-to-spread-trojan/
19. www.sophos.com/pressoffice/news/articles/2008/03/lee-shin-ja.html
20. www.sophos.com/pressoffice/news/articles/2008/02/poisoned-adverts.html
21. www.sophos.com/blogs/gc/g/2008/08/27/computer-worm-strikes-international-space-station/
22. www.sophos.com/blogs/gc/g/2008/08/08/up-to-1800-profiles-hit-by-malware-attack-says-facebook/
23. www.sophos.com/blogs/gc/g/2008/08/07/more-malicious-links-seen-on-facebook/
24. www.sophos.com/blogs/gc/g/2008/08/04/facebook-and-myspace-malware/
25. www.sophos.com/blogs/gc/g/2008/09/17/facebook-malware-is-a-real-threat/
26. www.sophos.com/pressoffice/news/articles/2008/01/facebook-adware.html
27. voices.washingtonpost.com/securityfix/2008/09/internet_shuns_us_based_isp_am.html
28. voices.washingtonpost.com/securityfix/2008/10/icann_de-accredits_estdomains.html
29. www.sophos.com/security/blog/2008/11/1970.html
30. voices.washingtonpost.com/securityfix/2008/11/the_badness_that_was_mccolo.html
31. www.sophos.com/security/blog/2008/11/2028.html
32. www.sophos.com/products/enterprise/alert-services/zombiealert.html
33. akismet.com/stats
34. www.sophos.com/blogs/gc/g/2008/11/10/facebook-friend-stranded-in-nigeria-would-you-rescue-them/
35. www.sophos.com/blogs/gc/g/2008/11/25/facebook-takes-on-spammer-and-wins-873-million/
36. www.sophos.com/pressoffice/news/articles/2008/02/poisoned-adverts.html
37. www.sophos.com/pressoffice/news/articles/2008/06/machovdyA.html
38. www.sophos.com/security/blog/2008/11/2028.html
39. www.sophos.com/security/blog/2008/11/2024.html
40. www.apple.com/pr/library/2008/10/21results.html
41. www.apple.com/pr/library/2008/10/21results.html
42. www.macworld.com/article/2008/10/25/technology/internet/25phone.html
43. www.sophos.com/blogs/gc/g/2008/11/03/guest-blog-will-hackers-make-the-iphone-an-iph0wn/
44. www.sophos.com/blogs/gc/g/category/data-leakage/
45. Indagine sui supporti rimovibili Utimaco, 2007.
46. www.sophos.com/blogs/gc/g/2008/09/30/who-needs-to-steal-data-when-you-can-buy-it-on-ebay/
47. www.sophos.com/blogs/gc/g/208/08/26/are-your-bank-details-being-sold-on-ebay/
48. www.sophos.com/pressoffice/news/articles/2007/09/chinese-hack.html

49. www.sophos.com/blogs/gc/g/2008/04/28/german-spooks-deploy-spyware-against-afghan-ministry/
50. www.sophos.com/blogs/gc/g/205/08/09/china-crisis-now-india-claims-hackers-are-attacking-it-from-behind-the-bamboo-curtain/
51. www.sophos.com/pressoffice/news/articles/2008/05/belgium.html
52. www.sophos.com/blogs/gc/g/2008/08/12/update-on-website-attacks-in-georgia-and-russia/
53. www.sophos.com/blogs/gc/g/2008/08/12/conflict-between-russia-and-georgia-turns-to-cyber-warfare/
54. www.sophos.com/blogs/gc/g/2008/09/02/sex-spyware-and-north-and-south-korea/
55. www.sophos.com/news/2008/01/nigerian-scam.html
56. www.sophos.com/news/2008/02/sobe.html
57. www.sophos.com/news/2008/03/zhang.html
58. www.sophos.com/blogs/gc/g/2008/04/29/i-spy-with-my-private-eye
59. www.sophos.com/news/2008/05/phishing-gang.html
60. www.sophos.com/news/2008/06/milmont.html
61. www.sophos.com/blogs/gc/g/2008/16/07/30-months-of-bread-and-water-for-spammer/
62. www.sophos.com/blogs/gc/g/2008/08/22/brazilian-charged-with-selling-access-to-100000-pc-botnet/
63. www.sophos.com/blogs/gc/g/2008/09/05/gang-arrested-in-canada-for-alleged-credit-card-data-heist/
64. www.sophos.com/blogs/gc/g/2008/10/14/ftc-shuts-down-major-international-spam-operation/
65. www.sophos.com/blogs/gc/g/2008/11/18/court-orders-company-to-stop-selling-spyware/
66. www.prweb.com/releases/spy/software/prweb1706254.htm

Per maggiori informazioni sui prodotti Sophos, visitate il sito www.sophos.it.

Boston, USA | Oxford, Regno Unito

tr/081208

SOPHOS
WWW.SOPHOS.COM