



Security threat report

2007

SOPHOS
secured.

Security threat report 2007

Scenario2006

Nel corso del 2006 i criminali informatici hanno agito in maniera sempre più subdola, escogitando modi di volta in volta più ingegnosi per mascherare le proprie attività illecite. Siti web fasulli riconoscibili come tali solo da un occhio esperto, campagne di spam che cambiano da un secondo all'altro per non essere rilevate, sistemi di posta vocale riprodotti dai "phisher" per simulare i centralini telefonici di società legittime: questi sono solo alcuni esempi della mutevolezza che caratterizza lo scenario delle minacce informatiche.

Lo scorso anno Sophos ha protetto da 207.684 tipologie diverse di malware: a farla da padrone è stata la famiglia di worm Mytob. I vettori più comuni di diffusione sono stati lo spam, i messaggi istantanei, i siti web controllati dagli hacker, la posta elettronica e le condivisioni di rete. Inoltre, Internet è diventato una fonte significativa di minacce, facendo registrare una vera e propria invasione di spyware, adware, applicazioni potenzialmente indesiderate e siti web indesiderati. Come sempre, è stata la sete di guadagni a spingere i malfattori a tentare di sottrarre informazioni confidenziali o di controllare i PC degli utenti.

Si riconferma il trend osservato nel corso del 2005: gli autori di malware sembrano abbandonare gradualmente l'utilizzo della posta elettronica preferendo mascherare i propri codici malevoli per bypassare i sistemi di rilevamento. Dal 2005 al 2006, l'incidenza delle mail infette è notevolmente calata, passando addirittura da una mail su 44 a una mail su 337.

Ai modi sempre più sofisticati per appropriarsi di informazioni confidenziali relative ad aziende e privati hanno fatto riscontro l'evoluzione sempre più rapida delle campagne di spam, complessi metodi operativi e una raffica di nuove truffe on line. Per contrastare questi fenomeni si è provveduto all'introduzione e alla severa applicazione di nuove leggi, ma il panorama delle minacce alla sicurezza per l'anno appena iniziato rimane intricato.

Fatti e misfatti del 2006

- Agli attacchi su vasta scala gli autori di malware hanno continuato a prediligere attacchi più mirati
- Boom dei downloader ospitati sui siti web per spiare gli utenti
- Sophos ha rilevato 41.536 nuovi malware e protetto in totale da 207.684 malware diversi
- Il numero dei Trojan è stato quattro volte superiore a quello dei virus e worm specifici di Windows
- Debutto del worm di tipo mass-mailing denominato Stratio: a novembre ne erano in circolazione oltre 1.000 varianti diverse
- Calo dei messaggi contenenti allegati infetti: segnalata una mail infetta su 337
- La maggior parte dello spam continua ad essere inviato da computer statunitensi non adeguatamente protetti

Solo il 34% delle aziende ritiene che le prospettive per il 2007 in ambito sicurezza siano più promettenti rispetto al 2006.

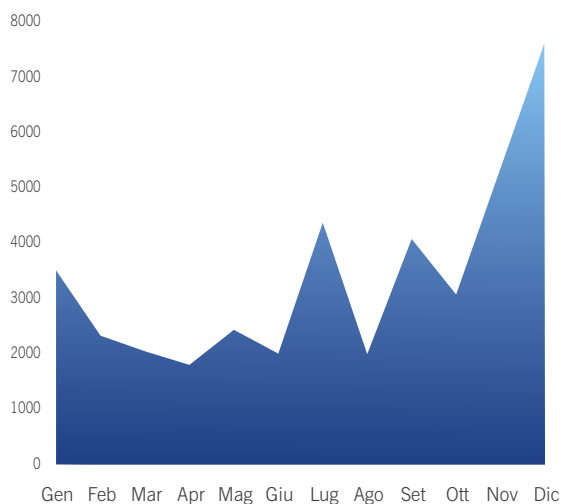
Fonte: Sondaggio on line di Sophos, dicembre 2006

Ritmi di crescita del malware

Nel 2006, Sophos ha rilevato 41.536 nuove minacce. Per tutto l'anno, gli autori di malware hanno dato libero sfogo alla propria creatività nella ricerca di nuovi metodi per attaccare i computer e indurre gli utenti a rivelare informazioni confidenziali. Nel mese di novembre, si è registrata un'impennata delle nuove minacce, che hanno toccato quota 7.612, una cifra quasi quattro volte superiore a quella registrata nello stesso mese del 2005, in cui le nuove minacce erano state 1940.

Secondo le previsioni di Sophos per il 2007, l'aumento del malware non accuserà battute d'arresto, anzi sono previsti tentativi ancora più subdoli di sottrarre informazioni a scopo di lucro.

Il picco raffigurato nel grafico in alto è ascrivibile allo stato di emergenza creato nel 2006 dalla famiglia di worm Stratio, anche noto come Stration o Warezov. Questo worm di tipo mass-mailing ha avuto una crescita così vertiginosa che nel mese di novembre ne era in circolazione oltre un migliaio di varianti diverse (Stratio è descritto più avanti in maniera dettagliata).



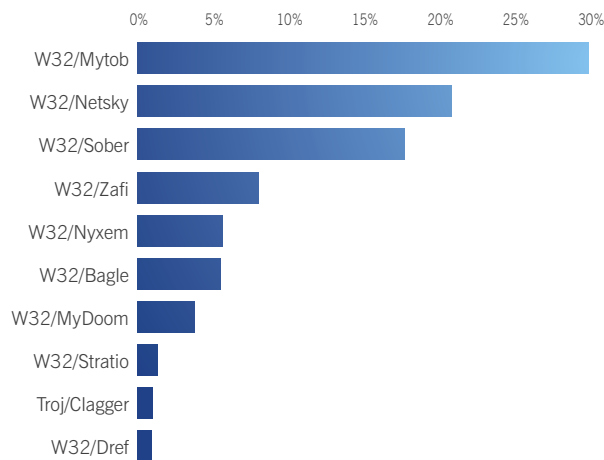
Numero di nuovi malware identificati ogni mese nel 2006

Le dieci minacce più diffuse per posta elettronica

Dai dati raccolti dai centri di monitoraggio di Sophos, dislocati in tutto il mondo, risulta che, malgrado la forte flessione nel volume di mail infette, che sono scese da una mail su 44 nel 2005 a una mail su 337, pari allo 0,3% delle mail in circolazione nel 2006, alcuni malware di alto profilo siano riusciti ugualmente a intrufolarsi nelle caselle di posta degli utenti. Durante l'anno, infatti, i worm Mytob, Netsky e Sober hanno fatto largo uso della posta elettronica come vettore di diffusione.

1 Mytob

La classifica delle dieci famiglie di malware più diffuse rivela che le varianti del worm Mytob restano lo spauracchio degli utenti, in tutto il mondo, sprovvisti di una protezione adeguata. Mytob ha debuttato nel marzo 2005, eppure continua ad infettare gli utenti che lo ricevono come allegato di posta elettronica. Il diciottenne Farid Essebar, un marocchino nato in Russia, meglio conosciuto come "Diablo", è stato condannato a due anni di reclusione per aver messo in circolazione il worm Zotob¹. Inoltre, esistono prove del suo coinvolgimento nella creazione di alcune varianti di Mytob.



Le dieci famiglie di malware più diffuse nel 2006

L'esistenza di migliaia di varianti diverse di Mytob, molte delle quali nascoste all'interno di un codice di compressione creato "su misura", lascia pensare che Mytob continuerà a colpire gli utenti sprovvisti di protezione anche nel 2007.

2 Netsky

L'8 maggio 2004, l'adolescente tedesco Sven Jaschan fu arrestato con l'accusa di aver messo in circolazione i worm Netsky e Sasser. Nel luglio 2005, fu pronunciata la sentenza di condanna a un anno e nove mesi di reclusione con la condizionale e a 30 ore di servizio sociale^{2*}.

Malgrado la condanna di Jaschan, i worm della famiglia Netsky, in particolar modo le varianti Netsky-P e Netsky-D, occupano tuttora posizioni di tutto rispetto nelle classifiche del malware più segnalato.

Inoltre, si teme che Netsky-D possa attaccare con successo le installazioni predefinite di Windows Vista, il sistema operativo recentemente rilasciato da Microsoft³. Sebbene Vista sia dotato di funzioni di sicurezza supplementari, che bloccano il computer in caso di attacco, le potenzialità di questo worm confermano l'importanza di aggiornare regolarmente la protezione antivirus.

3 Sober

Avvistato per la prima volta nell'ottobre 2003, Sober è tuttora presente nelle top ten stilate da Sophos. La sua variante più segnalata, Sober Z, identificata per la prima volta alla fine del 2005, si autoinviava come allegato di posta elettronica, spacciandosi per messaggio del FBI, della CIA o delle autorità tedesche, e tentava di disattivare il software di sicurezza sui computer delle vittime. Pur avendo circolato fino al 6 gennaio 2006, in quei pochi giorni di presenza, è riuscito ad assicurare a Sober il terzo posto nella top ten delle famiglie di malware più prolifiche del 2006.**

4 Zafi

Un'altra vecchia conoscenza delle classifiche, il worm Zafi, entrato in scena ad aprile 2004, rastrellava indirizzi e-mail usando tecniche di harvesting, per poi prenderli di mira. La quarta versione del worm, Zafi-D, è la variante più diffusa di questa famiglia⁵. Travestito da cartolina natalizia, il worm utilizzava tecniche di ingegneria sociale per trarre in inganno gli utenti e spingerli a lanciare l'allegato. Al culmine della sua ascesa, il worm era contenuto in una mail su 10 tra tutte quelle che viaggiavano in Rete, e guadagnò quindi la pole position della top ten per l'anno 2005.

* Due anni fa, una società tedesca operante nel campo della sicurezza informatica, forse in cerca di pubblicità, ha assunto Sven Jaschan come programmatore. Con questo gesto, l'azienda ha rischiato di lanciare un messaggio negativo e pericoloso: malgrado il loro comportamento malevolo, gli autori di virus possono facilmente trovare impiego nel settore della sicurezza.

**Un ventenne tedesco, di cui si ignora il nome, che nascondeva sul computer svariate immagini pedopornografiche, si è consegnato a sorpresa alle autorità perché spaventato da un messaggio inviato da Sober-Z. Il messaggio sosteneva, infatti, che il giovane fosse indagato dal Bundeskriminalamt, la Polizia criminale tedesca, per aver visitato siti web illegali.⁴

5 Nyxem

Questo worm di tipo mass-mailing, comunemente noto come worm Kama Sutra poiché utilizza svariati travestimenti a sfondo pornografico, ha scatenato il panico tra le sue vittime agli inizi del 2006⁶. Gli effetti del worm erano infatti disastrosi: il terzo giorno del mese distruggeva i file con estensione DOC, XLS, MDB, MDE, PPT, PPS, ZIP, RAR, PDF, PSD e DMP.

6 Bagle

Il primo avvistamento di Bagle risale al mese di gennaio 2004. Benché la protezione sia stata rilasciata al momento dell'identificazione del worm, e pur trattandosi di una minaccia ormai ben nota, Bagle continua a mietere vittime tra gli utenti. Nel febbraio 2006, nuove varianti del worm sono proliferate a macchia d'olio: Bagle-CM circolava all'interno di un'e-mail che offriva biglietti gratuiti per i Giochi Olimpici invernali di Torino⁷, mentre Bagle-CO era camuffato da cartolina di San Valentino.

Microsoft Windows Vista



A novembre 2006, Microsoft ha lanciato Windows Vista, il successore di Windows XP. Vista vanta numerose funzioni di sicurezza, tra cui Controllo accesso utente, che consente all'utente di scegliere caso per caso le applicazioni che è consentito eseguire e offre una migliore protezione contro il malware. Il client di posta Windows Mail presenta una serie di impostazioni predefinite che servono a bloccare l'esecuzione del malware. Queste novità saranno ben accolte dagli utenti: un sistema operativo che garantisce una migliore protezione contro le minacce informatiche non può che integrare le politiche di sicurezza.

Tuttavia, è importante che gli utenti non facciano affidamento unicamente sulle funzioni di protezione disponibili in Windows Vista per salvaguardare i propri sistemi dagli attacchi del malware. Sophos ha testato la nuova piattaforma Microsoft con le impostazioni predefinite e ha riscontrato che tre worm di alto profilo, Stratio-Zip, Netsky-D e MyDoom-O, diffusi su vasta scala utilizzando la posta elettronica come vettore, sono in grado di attaccare con successo Windows Vista. Queste tre varianti hanno rappresentato quasi il 40% di tutte le minacce in circolazione nel mese di novembre 2006.

Nel 2007 Microsoft si troverà quindi ad affrontare un'ennesima sfida. Gli autori di malware, oltre a bersagliare senza sosta i sistemi operativi precedenti a Windows Vista, saranno altrettanto solerti nel ricercare vulnerabilità nel codice di Vista. Sebbene Microsoft abbia fatto grandi progressi nel rilascio delle patch per correggere note vulnerabilità presenti nei propri sistemi operativi, gli autori di malware scoprono regolarmente il metodo per sfruttare tali vulnerabilità e aggirare la sicurezza dei computer.

Queste minacce devono il proprio successo all'esistenza di un elevato numero di computer ancora sprovvisti di adeguata protezione. Le varianti di Bagle continueranno a far strage di computer, sfruttando la posta elettronica, fino a quando gli utenti non si decideranno a installare un software antivirus a difesa dei propri computer.

7 MyDoom

La famiglia di worm MyDoom è stata alla ribalta per parecchi anni. Identificato per la prima volta nel gennaio 2004, MyDoom ha catalizzato l'attenzione, anche per il fatto che l'azienda informatica SCO si offrì di pagare una ricompensa di 250.000 dollari a chi avrebbe fornito informazioni utili per la cattura dell'autore⁸.

Si teme inoltre che la variante più diffusa, MyDoom-O, possa infettare, come già accennato sopra nel caso di Netsky, i computer con sistema operativo Vista, a riprova dell'importanza di utilizzare una protezione antivirus aggiornata⁹.

8 Stratio

Stratio, nuovo worm di tipo mass-mailing, ha debuttato nel mese di agosto 2006, ed è riuscito ad espugnare la classifica dei dieci malware più diffusi, grazie alla sua massiccia distribuzione, piazzandosi al primo posto¹⁰. Si diffonde per posta elettronica, camuffato in vari modi, per esempio da messaggio in cui si avvisa l'utente che il suo computer è stato infettato da un worm. Alla fine dell'anno si è scoperto che Stratio-Zip è uno dei tre worm di primo piano in grado di infettare il sistema operativo Vista.

Del worm Stratio sono state sguinzagliate migliaia e migliaia di varianti, tanto che in alcuni giorni il worm costituiva oltre il 50% di tutto il malware segnalato. L'obiettivo di Stratio è la diffusione del cosiddetto "image spam", ovvero una tipologia di spam che utilizza immagini anziché testo, al fine di aggirare i filtri antispam in grado di analizzare il solo contenuto testuale. A tal scopo, scarica da Internet una serie di componenti aggiuntivi. Alla fine del 2006, lo spam in circolazione sulla Rete era costituito in gran parte da image-spam, con una netta predominanza dei messaggi che pubblicizzavano farmacie on line.

9 Clagger

Clagger è il solo Trojan presente nella top ten. Poiché i Trojan non sono in grado di diffondersi autonomamente, affinché Clagger potesse entrare in classifica, è stato necessario inviarlo a milioni di indirizzi e-mail. Ciò dimostra quanto possano essere incisive le campagne di spam che si evolvono rapidamente. Sfruttando alcune note vulnerabilità, questo Trojan si installa su un PC e ne disattiva la protezione. Scarica quindi dei programmi spia, con il fine ultimo di rubare informazioni confidenziali. Agli inizi del

2006, per esempio, è stato distribuito come allegato nelle mail che fingevano di provenire da PayPal e Amazon¹¹. L'efficacia di questo Trojan è testimoniata dall'ottava posizione di Clagger nella top ten del malware, inserita nel rapporto sulla sicurezza pubblicato da Sophos a metà del 2006.

10 Dref

Le prime versioni di Dref, avvistato per la prima volta a metà del 2005, si propagavano attraverso un canale IRC e come allegato ai messaggi e-mail in uscita. Questo worm di tipo mass-mailing, specifico di Windows, disattiva il software antivirus, si autoinvia agli indirizzi e-mail presenti sul computer infetto e scarica altro malware sui PC degli utenti. Le versioni successive, come Dref-N, tentavano di spingere i destinatari ad aprire il file infetto, spacciandosi per notizia dell'ultima ora, per esempio l'annuncio dello scoppio di una guerra nucleare o della scomparsa del Presidente George W. Bush¹². Questo trucco faceva salire le probabilità di attirare nella trappola anche gli utenti più sensibili ai rischi legati all'apertura degli allegati di posta elettronica.

Mascherato da messaggio di auguri, Dref-V è stato il worm più segnalato nelle ultime 48 ore del 2006, raggiungendo l'incredibile percentuale del 93,7%¹³. Il successo di questo worm va attribuito al fatto che gli utenti, rientrati al lavoro dopo la pausa natalizia e desiderosi di smaltire rapidamente il cumulo di messaggi ricevuti, aprivano inavvertitamente gli allegati.

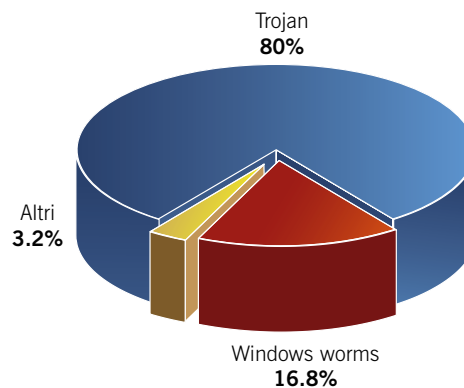
La posta elettronica come principale vettore di diffusione nel 2007

La posta elettronica continuerà ad essere un importante vettore di distribuzione del malware, ma Sophos prevede per il 2007 una lenta e costante diminuzione del numero dei worm inviati come allegato a milioni di indirizzi e-mail. L'accento si sposterà infatti sui messaggi di spam contenenti immagini e link a siti web infetti. La ragione di questo cambiamento di rotta è duplice. Innanzitutto, un messaggio senza allegati ha più probabilità di essere recapitato al destinatario. In secondo luogo, i worm sono difficili da gestire: una volta messi in circolazione, colpiscono in maniera indiscriminata tutti i computer vulnerabili in cui si imbattono. La distribuzione e la diffusione di virus e worm su vasta scala rischiano di porre gli autori di malware al centro dell'attenzione. Piazzando invece dei Trojan sui siti web, per esempio downloader e spyware, gli autori di malware possono prendere di mira un target specifico e il malware può infiltrarsi più facilmente in un computer, senza essere rilevato.

Trojan horses

Sebbene alcuni attacchi, come quelli sferrati da Dref e Stratio, abbiano avuto una portata tale che i relativi worm sono entrati di prepotenza nella top ten del malware per il 2006, in realtà, sono stati di gran lunga superati dagli attacchi dei Trojan, inviati in numero estremamente elevato nell'ambito di piccole campagne mirate.

I Trojan hanno costituito l'80% circa del malware individuato nel 2006. È rimasta quindi invariata la tendenza osservata nel 2005, ossia una netta prevalenza dei Trojan rispetto ai worm specifici di Windows, sebbene la percentuale dei Trojan nel 2005 fosse solo del 62%.



Trojan vs. virus e worm di Windows nel 2006

Spyware e downloader

Lo spyware continua ad affliggere le aziende e ha reso scottante il tema della sicurezza web. Rappresenta attualmente la seconda fonte di preoccupazione per la sicurezza delle società¹⁴: si annida nei computer, memorizzando le battute sulla tastiera, e rubando e inviando a terzi informazioni confidenziali, finanziarie e personali, senza il consenso e all'insaputa dell'utente. Inoltre, espone le reti al rischio di ulteriori attacchi.

Per cercare di ottenere informazioni e dati riservati, gli autori di malware agiscono in maniera sempre più subdola. Non si limitano più a collocare spyware di tipo "tradizionale" su singoli computer, ma si stanno orientando verso un nuovo metodo basato sull'invio di milioni di messaggi contenenti un link da cui scaricare un plug-in per visualizzare video o film pornografici, o persino software di protezione gratuiti. In realtà, il link conduce l'utente raggirato su un sito web infetto, dal quale viene scaricato un Trojan che apre una backdoor o ruba dati. Nel migliore dei casi, non appena la pagina web viene caricata, il malware presente sul sito infetta il computer del visitatore.

In effetti, questo tipo di Trojan non rappresenta una novità, ma i cosiddetti "downloader" stanno assumendo un ruolo sempre più rilevante nella creazione del malware, e i metodi di attacco diventano sempre più sofisticati. I siti web infetti tentano ora di valutare l'efficacia della protezione in uso sul computer, ricercando vulnerabilità da sfruttare, software antivirus non aggiornati o un sistema per aggirare il firewall. L'idea di fondo consiste nel trovare un mezzo per scaricare malware in grado di disabilitare la protezione del computer in visita sul sito, per poi scaricarvi altro malware. Per mascherare il proprio intento, il cybercriminale si serve di una serie di downloader: il primo ne colloca un secondo su un altro sito, il secondo colloca a sua volta un terzo

downloader su un altro sito ancora, e così via. L'ultimo downloader della serie ha il compito di piazzare lo spyware, che sarà utilizzato per rubare informazioni confidenziali o consentire a terzi non autorizzati l'accesso al computer. Poiché la protezione del computer è stata disattivata, lo spyware ha maggiori probabilità di autoinstallarsi senza essere individuato.

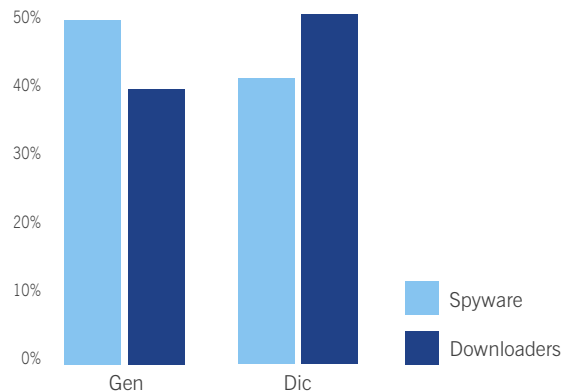
Alcune famiglie di alto profilo come Bagle¹⁵ hanno utilizzato i Trojan downloader con ottimi risultati e molte minacce che si propagano tramite canali IRC sono dotate di backdoor con funzioni di "download ed esecuzione". Un altro esemplare degno di nota è Zlob, noto anche come Popupper o Puper¹⁶. La famiglia dei Trojan Zlob comprende un'ampia gamma di componenti, la cui dannosità è testimoniata dall'enorme volume di messaggi postati sui forum in Rete. Zlob si serve principalmente di siti web per adulti per adescare le proprie vittime. Gli utenti attirati sul sito scaricano ed eseguono il presunto programma di installazione di un video codec, necessario per visualizzare un film pornografico, oppure un presunto strumento per gestire le password di accesso a siti web specifici. In alcuni casi, è possibile sentire l'audio di un film per adulti, ma non si vede alcuna immagine: si tratta di un ulteriore trucco per spingere gli utenti a scaricare file che si presumono necessari.

Poiché i Trojan downloader hanno raggiunto la maturità – la loro versatilità li rende uno strumento interessante determinando un drastico aumento del loro utilizzo – Sophos prevede che continueranno ad essere utilizzati in abbinamento allo spyware. È improbabile, infatti, che le vittime, in particolar modo gli utenti che hanno visitato siti per adulti, abbiano voglia di venire allo scoperto. Inoltre, la complessità del processo che va dall'installazione iniziale del downloader all'installazione finale dello spyware non consente ai piccoli produttori di soluzioni per la sicurezza di proteggere i propri utenti in maniera adeguata. Di

conseguenza, le piccole società vorranno sostituire gli attuali prodotti in uso con la soluzione all-in-one di un grande produttore, che protegga contro malware, spam, spyware, adware e dagli hacker, e che possa essere gestita a livello centrale.

Il grafico sottostante mostra i valori percentuali delle mail contenenti spyware e delle mail contenenti link ai siti web da cui viene scaricato lo spyware, registrati all'inizio e alla fine dell'anno. Da questi dati risulta evidente il cambiamento di tendenza a favore dei downloader.

Il malware ospitato sui siti web, e pronto per essere scaricato dai Trojan downloader, viene frequentemente modificato dagli hacker, nel tentativo di aggirare le soluzioni di sicurezza. In alcuni casi, Sophos ha riscontrato che il malware veniva riprogrammato in media sette volte al giorno. Lo stesso dicasi per alcuni degli adware più comuni.



Percentuale di spyware e downloader registrata nel 2006

Malware: dove nasce e dove si nasconde

Oltre a produrre soluzioni di protezione contro il malware nuovo e sconosciuto, gli esperti dei SophosLabs svolgono ricerche sui Paesi responsabili della creazione del malware, e sugli stati che ospitano i siti web in cui si annidano virus e Trojan.

La fabbrica del malware

Le accurate analisi svolte dai SophosLabs per stabilire la provenienza del malware hanno messo in luce alcune interessanti differenze nelle motivazioni e nelle tattiche utilizzate dai diversi gruppi di hacker che operano in tutto il globo.

Per esempio, il 30% del malware globale prodotto proviene dalla Cina. Si tratta per lo più di backdoor Trojan, ma è sorprendente come il 17% del malware programmato in Cina venga creato con l'obiettivo specifico di rubare le password dei giocatori on line¹⁷.

Al Brasile va attribuita invece la paternità del 14,2% del malware analizzato dai SophosLabs. La maggioranza del malware "carioca" è costituito da Trojan, il cui compito è di sottrarre le informazioni di accesso ai conti bancari on line.

Gli hacker russi e svedesi (responsabili rispettivamente del 4,1% e del 3,8% del malware esistente) si diletano in massima parte nella programmazione di backdoor Trojan, che consentono l'accesso non autorizzato ai computer delle vittime. Ne sono esempio i Trojan della famiglia Bifrose, che costituiscono il 15% di tutto il malware scritto in Svezia.

Anche l'Ucraina, rea di creare il 3,4% di tutto il malware analizzato dai SophosLabs, sembra essere una fucina di backdoor e bot.

Essere a conoscenza che gli hacker cinesi sono interessati alle password dei giocatori on line, e che i loro colleghi brasiliani puntano a mettere le mani sulle informazioni di accesso ai conti bancari on line aiuta gli esperti della sicurezza e le autorità a tracciare l'identikit degli autori di malware. Sophos prevede che nel 2007 gli hacker cinesi, russi e brasiliani proseguiranno sul cammino intrapreso. Sarà quindi interessante vedere quali nuovi Paesi emergeranno e verso quale tipologia di malware propenderanno.

I Paesi che ospitano malware sul Web

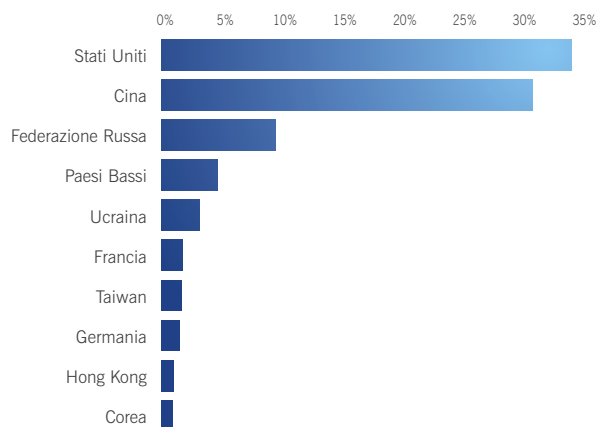
Il grafico sottostante mostra la percentuale degli indirizzi web contenenti il malware individuato dai SophosLabs nel corso del 2006. Gli URL sono raggruppati a seconda del Paese in cui era ospitato il server web.

Considerato l'elevato numero dei computer che si trovano in Nord America, non c'è da sorprendersi che gli Stati Uniti guidino la classifica ed ospitino oltre un terzo di tutti i siti web contenenti malware.

Tuttavia, uno dei Paesi che destano interesse è l'Olanda. La presenza dei Paesi Bassi al quarto posto della classifica con il 4,7% si spiega forse con il fatto che in Olanda operano alcune società di web hosting che chiudono un occhio sulle attività dei propri utenti, in nome della libertà di parola. In realtà, il Paese ospita numerosi siti contenenti informazioni e codici ad uso e consumo di cracker e hacker.

Sophos ritiene che le società di web hosting debbano agire in modo responsabile come membri della comunità globale di Internet, vigilando in maniera più efficace sui contenuti pubblicati negli spazi web dei propri clienti, e collaborando con le autorità per garantire la tempestiva rimozione del malware dai siti di pubblico accesso.

Sarà interessante vedere come si evolveranno queste tendenze nel corso del 2007. È difficile fare pronostici su questo specifico aspetto del rapporto, perché dipende molto dall'impegno profuso dai governi per porre un freno ai siti che ospitano malware. In molti casi, quando i siti web subiscono un attacco, i loro amministratori non dispongono di contromisure atte a impedire l'irruzione degli hacker. Il malware odierno è così subdolo che gli amministratori dei siti web sprovvisti di una protezione adeguata potrebbero addirittura non essere consapevoli delle minacce che si annidano sui loro siti, pronte a infettare i computer dei visitatori.

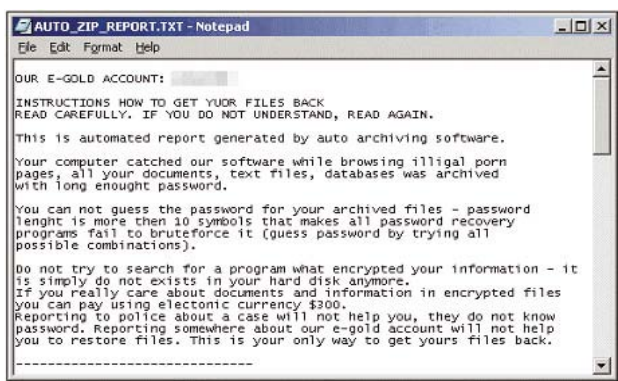


I dieci Paesi che nel 2006 hanno ospitato il maggior numero di siti web infetti

Ransomware

Il ransomware è una tipologia di malware che impedisce agli utenti di accedere ai propri file, per lo più criptandoli, e fornisce la password di accesso solo dopo il pagamento di un riscatto.

Nei casi più gravi, l'hacker minaccia addirittura di cancellare i file in modo irreversibile ogni 30 minuti, fino a quando non sarà pagato il riscatto. Di solito l'hacker richiede che il pagamento venga effettuato mediante e-Gold o Western Union per tentare di nascondere la sua vera identità. Questa tecnica, nata in Russia, viene adottata ora in tutto il mondo¹⁸.



Esempio di ransomware

Tra gli esempi di ransomware osservati durante il 2006 figurano il worm Arhiveus¹⁹ e il Trojan Zippo20.

Tuttavia, malgrado questi esempi di una certa rilevanza, nella top ten del malware per il 2006 non sono presenti casi di ransomware, ed è improbabile che lo saranno nel 2007. Questa forma di ricatto elettronico non è popolare, e richiede molto impegno e molti sforzi da parte dei malfattori. Inoltre, è improbabile che le società legittime siano disposte a pagare un simile riscatto. Poiché la maggior parte di esse è in possesso di copie di backup dei propri dati, è senz'altro più vantaggioso in termini di costo ed eticamente corretto rimuovere le minacce dai computer e ripristinare i dati dalle copie di backup.

Scareware

Sophos sta individuando sempre più spesso le prove della connivenza tra autori di malware e produttori di adware, che si pone l'obiettivo di installare malware e realizzare lauti guadagni, facendo leva sui timori legati alla sicurezza. Nel 2006 si è assistito infatti a un aumento del cosiddetto "scareware", ossia dei software progettati per indurre gli utenti di Internet a credere che il proprio PC sia infetto o vulnerabile, affinché si decidano ad acquistare una versione "perfettamente funzionante" del software con cui disinfettare o proteggere il proprio computer.

Basti citare come esempio il raggio architettato da Zhijian Chen, residente a Portland, nello stato dell'Oregon. Dopo aver terrorizzato gli utenti con messaggi allarmanti che avvertivano della presenza di spyware sul loro computer, Chen offriva alle vittime l'unica scappatoia possibile per risolvere il problema: l'acquisto e il download immediato del "poderoso" software Spyware Cleaner. Chen ha dapprima guadagnato soldi a palate, ma, nell'aprile 2006, è stato colto nel sacco e condannato a pagare una multa di 84.000 dollari²¹.

È necessario che i produttori di software prendano seri provvedimenti nei confronti dei propri partner e rivenditori che violano la legge installando malware sui computer di vittime innocenti a scopo di lucro.

Malware sui dispositivi mobili

Il malware creato ad hoc per i dispositivi mobili costituisce un problema di scarsa entità, se confrontato con il volume molto più consistente di malware che prende di mira il sistema operativo Windows. Tuttavia, questa minaccia diventa ogni giorno più concreta.

Alcuni produttori sono rei di averne amplificato l'entità: questo è quanto emerge da un sondaggio on line condotto da Sophos nel giugno 2005. Secondo il 70% dei partecipanti, alcuni produttori di soluzioni per la sicurezza hanno contribuito ad enfatizzare il problema²².

Tuttavia, in occasione di un sondaggio on line svoltosi a novembre 2006, l'81% dei partecipanti si è detto preoccupato che in futuro i telefoni cellulari possano diventare un bersaglio più frequente per gli autori di malware²³, anche se il 64% delle aziende ha ammesso di non aver ancora implementato alcuna protezione sui propri smartphone e PDA²⁴.

È evidente che la protezione dei dispositivi mobili assumerà nel 2007 un ruolo più importante: molte aziende non saranno disposte ad acquistare dispositivi per i quali non esistono sistemi di sicurezza affidabili. Sarà necessario che i produttori di dispositivi mobili ed esperti della sicurezza collaborino più strettamente per garantire una migliore protezione contro il furto dei dati, il malware e altre violazioni della sicurezza.

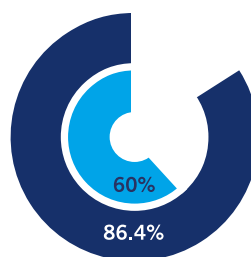
Minacce interne

I reparti IT saranno chiamati in causa non solo per proteggere le reti aziendali contro le minacce dirette alla sicurezza, ma anche per salvaguardare la produttività aziendale e preservare la larghezza di banda, limitando l'utilizzo di applicazioni indesiderate o non autorizzate, e garantendo un utilizzo di Internet sicuro ed efficiente.

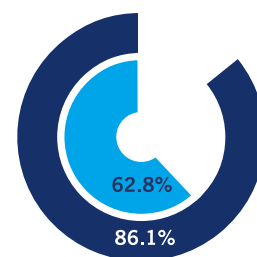
Controllo delle applicazioni

Un sondaggio condotto da Sophos a settembre 2006 rispecchia la seria preoccupazione degli amministratori di sistema per l'utilizzo incontrollato di determinate applicazioni sulle reti aziendali²⁵. Per esempio, l'86,1% dei partecipanti si è espresso a favore della possibilità di bloccare le applicazioni per la telefonia Internet. Di questa percentuale, il 62,8% si è spinto oltre, dichiarando che è indispensabile bloccare tali applicazioni.

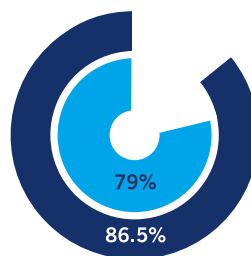
Le società saranno sempre più propense a controllare la propria rete aziendale. Poiché la sicurezza pone sfide sempre più ardue, la formazione degli utenti alla protezione è un compito complesso e difficile. Le aziende non saranno disposte a rischiare l'integrità della rete facendo affidamento unicamente sul buon senso dei propri utenti, quindi opteranno per il rafforzamento del proprio sistema di protezione contro ogni potenziale minaccia. Un elemento chiave di questa strategia sarà la riduzione delle fonti di distrazione per i dipendenti: regolamentando l'utilizzo in rete delle applicazioni non essenziali, i reparti IT contribuiranno a incrementare la produttività sul posto di lavoro.



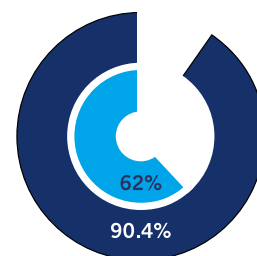
Instant messaging



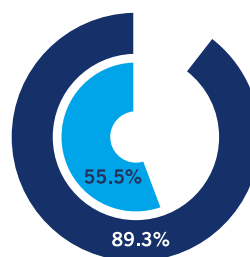
VoIP



Peer-to-peer



Games



Applicazioni informatiche distribuite

■ want to block ■ essential to block

Web surfing

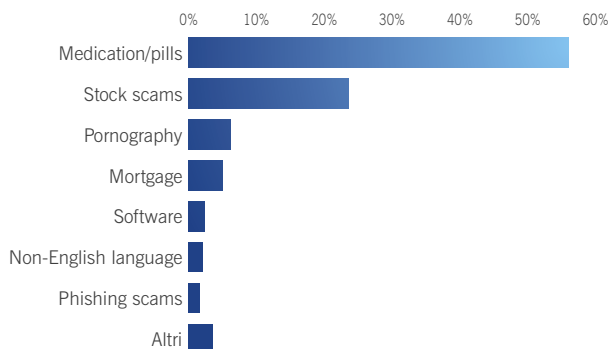
Durante il 2006, è diventato evidente che i siti web possono contenere insidie per la sicurezza delle aziende e che le abitudini Internet del personale aziendale possono incidere pesantemente sulla produttività e sulla larghezza di banda. Secondo un sondaggio, i lavoratori destinano il 20% circa del tempo di navigazione su Internet a fini personali o ricreativi²⁶.

Gli autori di malware sono alla continua ricerca di facili vie di accesso alla rete. Oggi, la via più facile è Internet. L'emergere del Web 2.0 ha ridefinito le modalità di interazione degli utenti con Internet, alzando il livello di esposizione alle minacce provenienti dalla Rete. Oltre ad accedere a siti web non regolamentati, gli utenti esperti scaricano con sempre maggior frequenza applicazioni e streaming audio/video. Le aziende sono attualmente sprovviste di una protezione adeguata contro i rischi legati al comportamento on line dei propri utenti. Si avverte quindi l'esigenza pressante di una soluzione che renda sicura la navigazione web.

Categorie di spam: vincenti e perdenti

Lo spam legato al settore medico (che riguarda principalmente presunti farmaci per migliorare le prestazioni sessuali o perdere peso, oppure gli ormoni della crescita) non solo resta la tipologia predominante di spam, ma, nel corso dell'anno, ha fatto registrare un aumento. Questa tipologia di spam è sempre stata popolare tra gli imbonitori elettronici, sia perché i consumatori si sentono più a proprio agio acquistando certi prodotti in forma anonima su Internet, sia perché è difficile ottenerli per vie legali in un regolare negozio. Verso la fine del 2006, lo spam legato al settore medico rappresentava oltre la metà di tutto lo spam in circolazione.

In crescita, del 10% circa, anche lo spam di tipo azionario, pari grossomodo a un quarto del totale delle e-mail "spazzatura". Gli spammer si sono serviti soprattutto del cosiddetto "image spam" (v. sotto) nell'ambito di campagne che tentavano operazioni di tipo "pump-and-dump", cioè con l'obiettivo di gonfiare ad arte il prezzo di un titolo di scarso valore e poco negoziato per realizzare enormi guadagni.



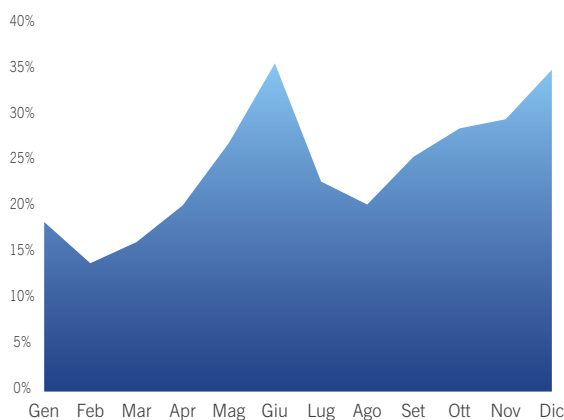
Le categorie di spam più diffuse nel 2006

Di contro, lo spam pornografico ha subito una forte flessione, passando dal 17% del 2005 al 6% del 2006. Normative più severe volte a contrastare questa tipologia di spam possono aver spinto alcuni spammer a commercializzare beni e servizi di altro genere.

Anche lo spam legato al settore creditizio ha perso posizioni in classifica, rappresentando solo il 5% dello spam in circolazione contro il 12% del 2005.

Image spam

Una delle tendenze chiave del 2006 è stata la crescita dello spam contenente immagini, la cui percentuale è lievitata dal 18,5% di gennaio al 35,1% di dicembre. Il trucco delle immagini fa aumentare le probabilità che i messaggi di spam vengano letti, perché gli consente di sfuggire ai filtri antispyam in grado di analizzare il solo contenuto testuale. A tal scopo, vengono spesso inserite nel messaggio animazioni GIF. Gli strati multipli di immagini caricati l'uno sull'altro creano confusione, rendendo unico ogni singolo messaggio.



Percentuale di image spam rispetto al totale dello spam in circolazione

L'immagine spam viene utilizzato in massima parte nelle campagne di spam che tentano frodi azionarie di tipo "pump-and-dump", come quella raffigurata in basso, in cui gli spammer pompano il valore delle azioni di una data società per realizzare facili guadagni.

BullsEye Financial Weekly Report Septe Issue:

Make no mistake, our mission at BullsEye Financial is to sift the thousands of underperforming companies out there to find the golden needle in the haystack.

The micro-cap diamond that can make you a fortune. More or not, the stocks we profile show a significant increase in stock prices sometimes in days or hours, not months or years.

We have come across what we feel is one of those rare deals public has not heard about yet.

Trade Date: Tuesday, September 5, 2006
Company: TRIMAX CORPORATION
Ticker: TMXO
Current Price: \$0.38
Short Term Target Price: \$1.50
Long Term Target Price: \$2.50
Recommendation: STRONG BUY

BUY!!!

Buy!

BUY!

Messaggio di spam di tipo pump-and-dump che visualizza ogni 15 secondi circa il messaggio subliminale "ACQUISTA!"

Altro image spam

Verso la fine dell'anno, i creatori di image spam hanno tentato di lucrare sul rilascio di Windows Vista, il nuovo sistema operativo di Microsoft, offrendone una versione a prezzo ridotto. Resta da chiarire se, rispondendo al messaggio, l'utente avrebbe ricevuto una versione pirata di Windows Vista, oppure avrebbe subito il furto dei dati della propria carta di credito²⁷.

In altri casi, l'immagine adatta la nuova tecnica a un vecchio stratagemma, usando la pornografia come esca. È il caso di una campagna che inviava a utenti australiani messaggi e-mail che sostenevano di provenire da una giovane donna in visita nel Paese²⁸. Le e-mail non contenevano testo, ma un'immagine grafica che invitava gli utenti a visitare un sito web contenente immagini soft-core e un link al Trojan Dloadr-AMA.

Phishing

Dalle ricerche condotte dai SophosLabs nel corso del 2006 risulta che oltre il 75% di tutte le e-mail fraudolente bersagliano gli utenti di PayPal o di eBay²⁹, ma queste non sono le uniche società on line i cui clienti sono stati al centro dell'attenzione dei ladri di identità.

Nel 2006 si sono verificati i primi casi di voice phishing (altrimenti detto "vishing") organizzato: i phisher chiedevano ai destinatari delle e-mail di chiamare un numero telefonico, anziché rispondere via e-mail o visitare un sito web. Poiché gli hacker diventano ogni giorno più scaltri, è probabile che si indurranno sempre più non solo per creare siti web fasulli, ma anche per raccogliere con tecniche di harvesting i messaggi provenienti dai centralini telefonici di grandi aziende, simulando ancora meglio le società legittime³⁰.

Sembra probabile che nel corso del 2007 molti hacker tenteranno di sfruttare la tecnologia VoIP per gli attacchi di vishing.

Nel frattempo, il phishing tradizionale ha continuato a colpire molti utenti di posta elettronica.

In uno dei casi più vergognosi di sfruttamento della generosità pubblica, un ventenne di Miami è stato accusato, nell'agosto 2006, in relazione a un sito di phishing che sosteneva di raccogliere fondi a favore delle vittime dell'uragano Katrina³¹.

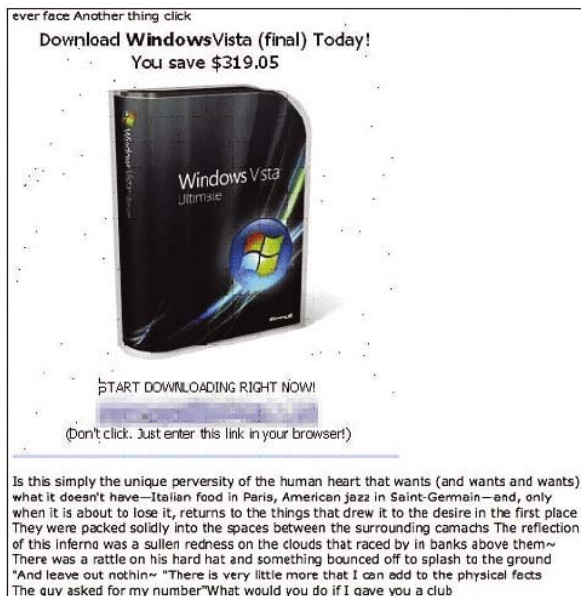


Image spam che offre Windows Vista a un prezzo affare

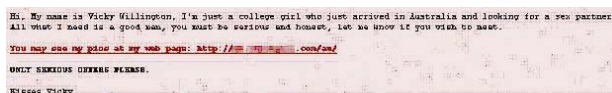


Image spam che usa la pornografia come esca

È probabile che nel 2007 il phishing seguirà nuove direzioni. Sebbene gli utenti siano molto più diffidenti verso le e-mail che sostengono di provenire da aziende legittime, i phisher impiegano alcuni trucchi ingegnosi per indurre le proprie vittime a credere che un messaggio sia autentico. Poiché le autorità sono diventate più abili nel rintracciare le frodi on line internazionali, i phisher propenderanno forse per attacchi indiretti come le frodi azionarie.

La sporca dozzina dei produttori di spam

Sophos analizza tutti i messaggi di spam intercettati dalla propria rete globale di trappole per lo spam. In questo modo, gli esperti dei SophosLabs hanno constatato che gli Stati Uniti, pur avendo compiuto passi da gigante nella riduzione del volume di spam inviato, restano saldamente al comando della classifica dei principali produttori di e-mail “spazzatura”.

Nel complesso, tranne alcune eccezioni, i risultati dell'analisi sono più o meno in linea con quanto osservato nel 2005.

La Cina e la Corea del Sud hanno perso posizioni in classifica: il drastico calo nella quantità di spam prodotto dalla Corea del Sud si spiega forse con i consistenti investimenti del Paese nell'infrastruttura Internet e con l'impiego costante di sistemi operativi più resilienti. Gli utenti sono più sensibili alle problematiche della sicurezza e proteggono i propri computer in maniera adeguata, quindi è meno probabile che i loro PC vengano infettati dal malware o utilizzati per l'invio di spam.

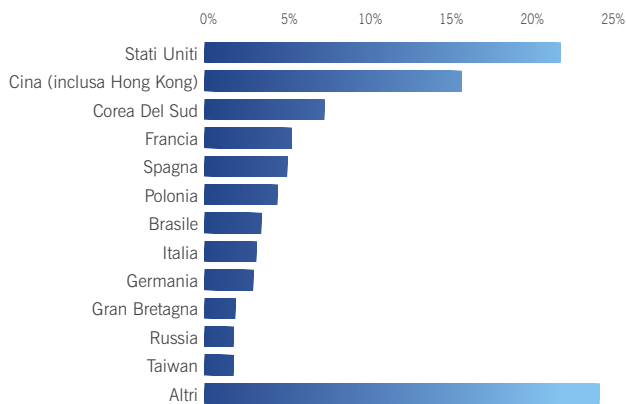
Anche grazie agli sforzi compiuti dalle autorità per garantire che gli Internet Service Provider adottino best practice in ambito sicurezza, il Canada, che nel 2005 occupava la 5ta posizione in classifica, è sceso nel 2006 al 17mo posto.

Sebbene Stati Uniti, Cina e Corea del Sud siano rei di produrre oltre il 45% di tutto lo spam in circolazione, dal confronto tra i continenti emerge il predominio dell'Europa sul Nord America: dal Vecchio Continente proviene infatti quasi un terzo del volume totale di spam. A ciò contribuiscono numerosi fattori: condanne degli spammer alla reclusione, normative più severe e una migliore protezione dei sistemi.

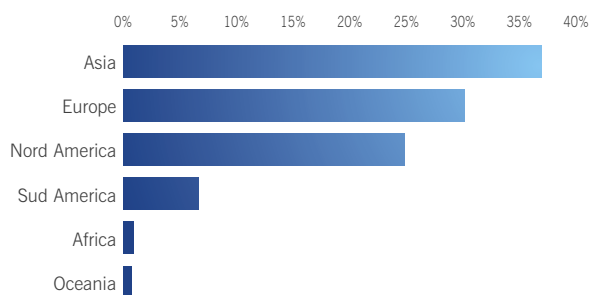
Il 90% di tutto lo spam in circolazione proviene attualmente da computer zombie, anche noti come botnet, controllati a distanza dagli hacker per mezzo di Trojan, worm e virus. Per assumere il controllo di un PC e sfruttarlo per inviare spam, non è necessario infatti che un hacker risieda nello stesso Paese in cui si trova il suddetto computer.

Una rete di computer zombie è in grado di inviare centinaia di milioni di messaggi di spam nell'arco di poche ore, quindi il problema dei botnet si presenta ostico per coloro che sono impegnati a vigilare sulla Rete e a renderla sicura.

Qualunque sia la propria sede operativa, lo spammer può sfruttare connessioni a banda larga insicure, in qualunque parte del globo, per inviare messaggi commerciali indesiderati.



La sporca dozzina dei produttori di spam nel 2006



Distribuzione geografica dello spam nel 2006

Frodi on line

I truffatori hanno continuato a usare Internet per raggirare gli utenti e sottrargli denaro o informazioni confidenziali. Nella cosiddetta truffa nigeriana o truffa 419 (in riferimento all'articolo del Codice penale della Nigeria, dove sono state ideate molte delle truffe on line) viene offerta solitamente una congrua somma di denaro. Dopo aver irretito la vittima, il truffatore richiede informazioni personali, che possono essere utilizzate poi per estorsioni, furti di identità e sottrazione di informazioni bancarie.

Negli ultimi 12 mesi i truffatori informatici si sono camuffati nei modi più svariati. Ecco alcuni esempi:

- Un agente del KGB in punto di morte sosteneva di essere in possesso di informazioni segrete sull'assassinio di John F. Kennedy³²
- Un diciannovenne sosteneva di aver trovato una cura per l'AIDS³³ a base di erbe
- Un sergente statunitense con sede a Baghdad³⁴ proponeva una transazione finanziaria fasulla
- Presunti avvocati rappresentavano i diritti delle vittime del disastro aereo del Concorde³⁵
- Presunti medici assistevano le persone ferite nel disastro minerario della West Virginia³⁶
- Segretaria di un magnate russo del petrolio in galera³⁷
- Agenzia di moda australiana alla ricerca di persone interessate a lavorare in TV e al cinema³⁸
- Il Ministro scozzese per la Cultura, il Turismo e lo Sport³⁹

Il 2007 non segnerà certo la fine delle frodi on line, e gli imbonitori informatici persevereranno nei loro tentativi di carpire la fiducia degli utenti di Internet.

Delitto e castigo

Il denaro è oggi il movente principale della maggior parte degli autori di virus e spammer. Mentre, in passato, il malware era opera di esibizionisti e megalomani, oggi non è che uno strumento per generare profitti attraverso il furto di identità, il phishing, l'adware, gli attacchi DoS distribuiti, e persino il ransomware.

Come logica conseguenza di questa evoluzione, le autorità hanno iniziato a punire più severamente i reati informatici.

Nel 2006 sono state intraprese alcune azioni legali di alto profilo contro spammer, truffatori, phisher e autori di malware. Ma, ovviamente, il crimine informatico è un fenomeno globale, quindi è necessario intervenire a livello internazionale con severe misure nei confronti di coloro che delincono sulla Rete. Le normative vengono continuamente aggiornate in tutto il mondo per rispecchiare le tipologie più recenti di reato informatico⁴⁰. La Gran Bretagna, per esempio, ha cominciato ad affrontare il problema degli attacchi DoS distribuiti: iniziativa che merita un elogio, visto che le reti formate da computer zombie e i ricatti in formato elettronico stanno assumendo un ruolo di primo piano nel panorama della criminalità informatica.

Con l'aiuto di leggi come la CAN-SPAM, e grazie allo scambio di informazioni tra Internet Service Provider, gli USA sono stati i pionieri nel comminare pene e multe severe agli spammer più prolifici. Durante il primo trimestre del 2006, diverse persone hanno ammesso di far parte di una rete criminale organizzata dedicata alla distribuzione di massicce quantità di materiale pornografico: Jennifer Clason, residente nello stato del New Hampshire, Andrew Ellifson, originario dell'Arizona e Kirk Rogers, californiano, appartenevano a una banda che inviava milioni di e-mail in cui venivano pubblicizzati siti per adulti⁴¹.

A maggio 2006⁴², il ventunenne hacker californiano Jeanson James Ancheta, che aveva assunto il controllo di 400.000 PC creando una rete di computer zombie, è stato condannato a 57 mesi di reclusione. Ancheta, che ha ammesso di aver pubblicizzato su Internet le sue reti di computer infetti ("botnet"), vendeva l'accesso a un software in grado di controllare i computer da remoto per inviare spam e lanciare attacchi DoS distribuiti contro i siti web. I siti colpiti dall'attacco DDoS potevano poi essere costretti, con l'arma del ricatto, a pagare cifre consistenti per far ripristinare l'accesso al sito. L'operazione più redditizia per Ancheta è stata l'installazione di adware sui computer zombie: i proventi gli hanno consentito di acquistare server per sferrare ulteriori attacchi, un nuovo guardaroba e una

lussuosa BMW. Oltre alla condanna alla reclusione, Ancheta si è visto infliggere una multa di 15.000 dollari da versare alle organizzazioni militari vittime dei suoi attacchi.

A settembre 2006, le autorità marocchine hanno fermato il diciannovenne Farid Essebar, studente di scienze, e il ventiduenne Achraf Bahloul con l'accusa di aver creato e diffuso il worm Zotob, che ad agosto 2005 sfruttò una vulnerabilità critica nel servizio Plug and Play di alcuni sistemi operativi di Microsoft, mandando in tilt i computer della CNN, della ABC, del Financial Times e del New York Times⁴³. I due baby-autori sono stati condannati, rispettivamente, a due e a un anno di reclusione.

Non è inconsueto che gli autori di malware lascino la propria "firma" all'interno del codice creato, accompagnata a volte da altri messaggi. Si ritiene che Essebar, un marocchino nato in Russia, abbia utilizzato il soprannome "Diablo", inserendolo all'interno del worm W32/Zotob-A. Poiché lo stesso nickname compare in oltre venti varianti del worm Mytob, la minaccia più prolifica del 2006, i ricercatori Sophos ipotizzano che "Diablo" sia coinvolto anche nella loro creazione.

Nel mese di agosto 2006, un altro hacker californiano di 21 anni, Christopher Maxwell, è stato condannato a un periodo detentivo di tre anni, dopo aver ammesso di aver infettato 50.000 computer presso basi militari e scuole statunitensi, e in un ospedale di Seattle⁴⁴. I suoi attacchi avrebbero paralizzato le attività ospedaliere e fruttato a Maxwell e alla sua banda, grazie all'installazione di adware sui PC infetti, oltre 100.000 dollari.

Nel mese di settembre 2006, l'ACMA, l'Autorità Australiana per le Comunicazioni, ha avviato un'inchiesta sulle attività di un uomo sospettato di aver inviato più di due miliardi di messaggi di spam che offrivano il Viagra⁴⁵, mentre negli USA è stato avviato un procedimento contro due società accusate di aver inviato e-mail non richieste sulle scommesse e sugli alcolici ai bambini⁴⁶.

Sempre negli USA, William Bailey Jr., residente nella Carolina del Nord, accusato di aver scaricato illegalmente i dati personali di 80.000 membri dell'American College of Physicians, ha rischiato una condanna a 55 anni di reclusione e una multa di 2.750.000 dollari.

Le autorità russe hanno posto fine alle attività malavitose di una banda specializzata in attacchi DDoS⁴⁷ contro società che gestiscono casinò e scommesse on line. La gang formata da Ivan Maksakov, Alexander Petrov e Denis Stepanov era riuscita ad estorcere più di 4 milioni di dollari ai bookmaker inglesi sotto la minaccia di attaccarne i siti web, rendendoli inaccessibili al mondo esterno. I tre hacker, che utilizzavano computer zombie per lanciare gli attacchi DDoS, sono stati condannati a un periodo detentivo di 8 anni e a una sanzione pecuniaria di 3.700 dollari.

A dicembre, un tribunale tedesco ha condannato un uomo a quattro anni di reclusione, e un'altra persona a 39 mesi, per il loro coinvolgimento in un piano criminale che ha messo KO i computer di numerosi utenti di Internet con un Trojan che componeva numeri telefonici a tariffa maggiorata (con prefisso 0190) per contattare un sito web per adulti⁴⁸. La banda ha rastrellato 12 milioni di euro infettando oltre 100.000 PC.

Riepilogo

Sebbene il sondaggio condotto da Sophos, e riportato a pagina 1, riveli che molte aziende temono un acuirsi delle minacce alla sicurezza informatica nel 2007, il problema, se gestito correttamente, non dovrebbe essere insormontabile. I criminali informatici escogiteranno modi sempre più subdoli di infettare i computer e sottrarre informazioni confidenziali, ma le aziende potranno difendere le proprie reti attuando norme di sicurezza efficaci, utilizzando una protezione aggiornata e impegnandosi attivamente nella formazione degli utenti. Per ridurre al minimo le probabilità di attacco, infatti, è necessario che le aziende mettano in atto criteri e procedure incisivi, e proteggano tutte le vie di accesso alla propria rete e ai computer desktop

Per maggiori informazioni sui prodotti Sophos e su come richiederne la valutazione gratuita, visitare www.sophos.it

Sources

- 1 www.sophos.com/pressoffice/news/articles/2005/08/va_diablo.html
- 2 www.sophos.com/pressoffice/news/articles/2005/07/va_sasserfree.html
- 3 www.sophos.com/pressoffice/news/articles/2006/11/toptennov.html
- 4 www.sophos.com/pressoffice/news/articles/2005/12/soberzcrim.html
- 5 www.sophos.com/pressoffice/news/articles/2005/12/toptensummary05.html
- 6 www.sophos.com/pressoffice/news/articles/2006/02/nyxempanic.html
- 7 www.sophos.com/pressoffice/news/articles/2006/02/baglecm.html
- 8 www.sophos.com/pressoffice/news/articles/2004/01/va_mydoombounty.html
- 9 www.sophos.com/pressoffice/news/articles/2006/11/toptennov.html
- 10 www.sophos.com/pressoffice/news/articles/2006/09/stration-worm.html
- 11 www.sophos.com/pressoffice/news/articles/2006/02/claggerh.html
- 12 www.sophos.com/pressoffice/news/articles/2006/11/drefn.html
- 13 www.sophos.com/pressoffice/news/articles/2007/01/drefv.html
- 14 Worldwide Secure Content Management 2005-2009 forecast update and 2004 vendor shares: spyware, spam, and malicious code continue to wreak havoc. IDC. September 2005
- 15 www.sophos.com/pressoffice/news/articles/2004/03/va_baglegraphic.html
- 16 www.sophos.com/virusinfo/analyses/trojzloba.html
- 17 www.sophos.com/pressoffice/news/articles/2006/11/chinamalware.html
- 18 www.sophos.com/pressoffice/news/articles/2006/04/ransom.html
- 19 www.sophos.com/pressoffice/news/articles/2006/06/arhiveus.html
- 20 www.sophos.com/pressoffice/news/articles/2006/03/zippo.html
- 21 www.sophos.com/pressoffice/news/articles/2006/04/spywarechen.html
- 22 Sophos web poll, June 2005
- 23 Sophos web poll, November 2006
- 24 Sophos web poll, January 2007
- 25 Sophos web poll, September 2006
- 26 Burstek releases 2005 internet usage study.
www.findarticles.com/p/articles/mi_m0EIN/is_2006_March_20/ai_n16109780
- 27 www.sophos.com/pressoffice/news/articles/2006/12/vistaspam.html
- 28 www.sophos.com/pressoffice/news/articles/2006/08/vicky-image-trojan.html
- 29 www.sophos.com/pressoffice/news/articles/2006/07/top-phishing-targets.html
- 30 www.sophos.com/pressoffice/news/articles/2006/07/paypalvox.html
- 31 www.sophos.com/pressoffice/news/articles/2006/08/hurricane-phisher.html
- 32 www.sophos.com/pressoffice/news/articles/2006/08/kennedy-scam.html
- 33 www.sophos.com/pressoffice/news/articles/2006/07/aids cure.html
- 34 www.sophos.com/pressoffice/news/articles/2006/01/iraq419.html
- 35 www.sophos.com/pressoffice/news/articles/2006/04/concorde419.html
- 36 www.sophos.com/pressoffice/news/articles/2006/01/sago.html
- 37 www.sophos.com/pressoffice/news/articles/2006/01/yukos.html
- 38 www.sophos.com/pressoffice/news/articles/2006/09/model-scam.html
- 39 www.sophos.com/pressoffice/news/articles/2006/06/scottishmp419.html
- 40 www.cybercrimelaw.net
- 41 www.sophos.com/pressoffice/news/articles/2006/03/clason.html
- 42 www.sophos.com/pressoffice/news/articles/2006/05/anchetasentence.html
- 43 www.sophos.com/pressoffice/news/articles/2006/09/zotob-jail.html
- 44 www.sophos.com/pressoffice/news/articles/2006/08/maxwell-sentence.html
- 45 www.sophos.com/pressoffice/news/articles/2006/09/viagra-spammer.html
- 46 www.sophos.com/pressoffice/news/articles/2006/08/kid-spam-lawsuit.html
- 47 www.sophos.com/pressoffice/news/articles/2006/10/extort-ddos-blackmail.html
- 48 www.sophos.com/pressoffice/news/articles/2006/12/dialgang.html

A proposito di Sophos

Sophos è società leader a livello mondiale nella sicurezza informatica e nella tecnologia di controllo dell'accesso alla rete. Sophos garantisce una protezione completa, sia a livello gateway che endpoint, contro minacce complesse quali malware noto e sconosciuto, spyware, intrusioni, applicazioni indesiderate, spam, violazioni delle politiche di sicurezza aziendale e accesso non controllato alla rete. Le soluzioni Sophos, affidabili e facili da utilizzare, sono progettate su misura per le aziende, il settore education e la Pubblica Amministrazione, e proteggono oltre 35 milioni di utenti in più di 150 Paesi. Sophos dispone di una rete mondiale di centri per l'analisi delle minacce informatiche, in cui operano esperti altamente qualificati. Forte della propria esperienza ventennale nel settore e della competenza dei propri centri di ricerca e analisi, Sophos risponde tempestivamente alle nuove minacce alla sicurezza e vanta un livello invidiabile di soddisfazione dei clienti. Sophos è una multinazionale con sede centrale a Oxford, Gran Bretagna. Per maggiori informazioni su Sophos, visitare www.sophos.it.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2007. Sophos Plc.

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted
by any form or by any means without the prior written permission of the publishers.*

SOPHOS
secured.