SOPHOS

Rapporto di Sophos sulla sicurezza

Versione luglio 2006

Rapporto di Sophos sulla sicurezza

Versione aggiornata: luglio 2006

Sguardo retrospettivo al primo semestre 2006

Questa versione aggiornata del rapporto annuale di Sophos sulla sicurezza pubblicato a dicembre 2005 presenta il nuovo scenario delle minacce alla sicurezza, con i cambiamenti avvenuti durante il primo semestre del 2006, e le tendenze previste per la seconda parte dell'anno.

Ancora una volta, i responsabili della sicurezza delle reti aziendali sono stati messi duramente alla prova in modi nuovi ed ingegnosi. I reparti IT hanno continuato a fronteggiare sfide sempre più ardue, in quanto i criminali informatici escogitano ogni giorno nuovi metodi per sfruttare le vulnerabilità umane e dei sistemi informatici, con l'obiettivo di rubare ed estocere denaro agli utenti e alle aziende.

Le cifre del malware hanno registrato un aumento e l'enfasi crescente posta sulla segretezza nell'ultima parte dello scorso anno ha raggiunto il parossismo. Lo spyware e il phishing rimangono due delle minacce più preoccupanti tra quelle che insidiano la sicurezza delle imprese, e gli attacchi di malware, contrariamente ai worm che venivano inviati in massa nel passato, prendono quasi sempre di mira un ristretto gruppo di vittime. In questo modo, i criminali informatici tentano di distogliere da sé l'attenzione.

Secondo il Global Security Survey, condotto da Deloitte Touche Tohmatsu e pubblicato a giugno 2006 dalla Financial Services Industry, più di tre quarti (il 78%, rispetto al 26% del 2005) degli intervistati hanno confermato che la propria organizzazione ha subito una violazione della sicurezza dall'esterno.[1] Il sondaggio ha definito il furto d'identità come "il crimine del 21mo secolo".

Il primo semestre 2006 in breve

Sophos ha rilevato oltre 180.000 minacce

Le e-mail contenenti virus sono scese a 1 su 91

Il rapporto nuovi Trojan/virus e worm è stato di 4:1

È nato il ransomware, il ricatto in formato elettronico

Percentuali di aumento

Il numero delle minacce fa registrare un aumento costante. Alla fine di giugno 2005, il numero dei vari programmi, denominati collettivamente malware, da cui Sophos era in grado di proteggere era di 140.118*. A distanza di un anno, alla fine di giugno 2006, Sophos era in grado di identificare e proteggere da 180.292* virus, spyware, worm, Trojan e altro malware, adware e altre applicazioni potenzialmente indesiderate.

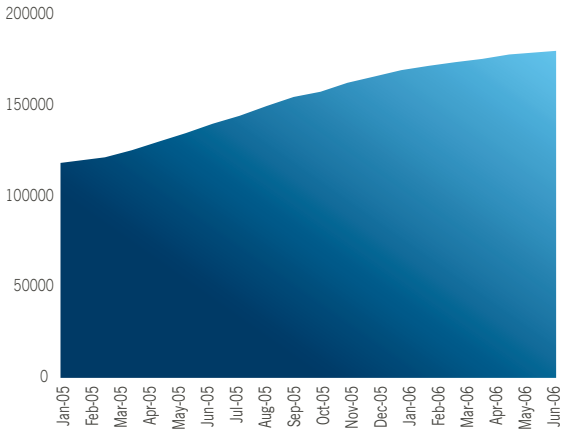

Figura 1: aumento del malware

Sempre alla ricerca di vittime sacrificali, gli autori di malware stanno gradualmente spostando il baricentro del proprio interesse dai worm diffusi utilizzando la posta elettronica verso altri metodi di infezione. Spinti dalla sete di guadagno, gli hacker non intendono infettare milioni di computer, per non attirare l'attenzione su di sé e per non aumentare le probabilità che gli utenti si adoperino per proteggersi adeguatamente.

In modo analogo, il numero di computer presi di mira da ogni attacco di spam è stato ridotto, affinché la minaccia potesse eludere le tecniche antispam che misurano il volume della posta elettronica.

Dalle ricerche condotte da Sophos emerge che, fino a questo

**Si noti che Sophos ha modificato il sistema utilizzato per calcolare e segnalare le minacce da cui è in grado di proteggere, affinché la cifra ottenuta rispecchi in maniera più precisa le singole minacce rilevate dalla tecnologia Genotype.*

momento, solo 1 mail su 91 tra quelle in circolazione quest'anno conteneva virus. Nello stesso periodo del 2005, invece, si registrava una mail infetta su 35, a riprova che gli attacchi sferrati dai worm contenuti nei messaggi e-mail hanno subito una flessione a favore di altri metodi di attacco.

Le dieci minacce informatiche più diffuse

Sophos dispone di una rete mondiale formata da decine di migliaia di centri di monitoraggio: questi raccolgono i dati sui virus più recenti che si diffondono per e-mail, consentendo a Sophos di monitorare lo stato di salute dei sistemi di posta e di allertare tempestivamente gli utenti in caso di attacco da parte di un virus.

Un aspetto interessante è rappresentato dalla prevalenza nella top ten (vedere figura 2) dei virus già in circolazione da qualche tempo, come rappresentato nel grafico qui sotto.

La minaccia che ha mietuto più vittime da gennaio a giugno 2006 è stato il worm Sober-Z, che, nel momento di massima diffusione, rappresentava una mail infetta su 13.[2] Il worm, che camuffato da messaggio dell'FBI o della CIA accusava il destinatario di aver visitato siti web illegali,[3] la fa da padrone, seppur programmato per cessare di diffondersi il 6 gennaio 2006.

Un solo worm nuovo è riuscito a far breccia nella top ten del malware: Nyxem-D, anche noto come Kama Sutra. Nyxem-D è contenuto all'interno di un messaggio e-mail che offre immagini pornografiche e filmati erotici.[4] Questi dati evidenziano che gli attacchi di data più recente sono stati i più insidiosi, infettando in maniera subdola gruppi ristretti di persone, nel tentativo di creare un diversivo.

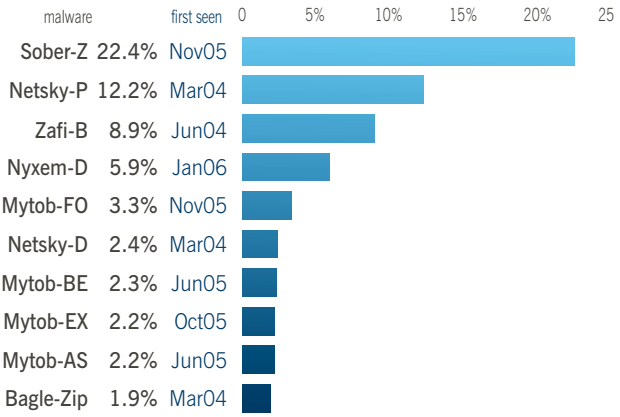

Figura 2: top ten delle minacce e loro ciclo di vita

Trojan

I primi sei mesi del 2006 indicano che il bersaglio prediletto dagli autori di virus continua ad essere il sistema operativo Windows, che viene attaccato da Trojan, virus e worm.

Nel 2005, il numero dei Trojan ha superato quello di virus e worm, con un rapporto di quasi 2:1; oggi è quattro volte più probabile che un utente venga colpito da un Trojan piuttosto che da un virus o worm.

Inoltre, un Trojan su due, nel primo semestre dell'anno, conteneva componenti spyware ed era in grado di eseguire determinate azioni come la registrazione delle battute sulla tastiera, il furto di informazioni confidenziali (nome utente, password, dati della carta di credito), e di consentire a terze parti l'accesso ai computer infetti.

Poiché i Trojan non riescono a diffondersi da soli, il loro autore è costretto ad escogitare il modo per istigare gli utenti a scaricare o eseguire il malware. La posta elettronica rappresenta in questo senso un mezzo di comunicazione economico e immediato. Invece di un allegato infetto, i messaggi oggi contengono spesso il link a un sito web. Se il destinatario visita la pagina web, il programma dannoso che si nasconde in essa tenterà di accedere al computer, sfruttando

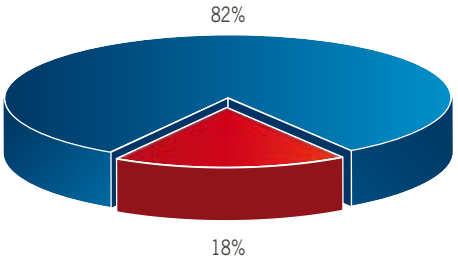

Figura 3: nuovi Trojan (82%) vs. virus (18%)

una vulnerabilità di Windows: un bug nel software o una protezione antivirus o firewall inadeguata. Il programma riesce quindi a scaricarsi da solo nel computer, a insaputa dell'utente.

Nuove tipologie di minaccia

Ransomware

Quest'anno ha debuttato una nuova tipologia di Trojan, una vera e propria forma di ricatto in formato elettronico. Questo nuovo fenomeno conferma più di qualunque altro la propensione degli autori di malware per attacchi mirati contro

specifici gruppi ristretti di persone, anziché per attacchi in massa contro gli utenti di Internet.

Il cosiddetto "ransomware" è una tipologia di malware - spesso un Trojan - che impedisce agli utenti di accedere ai propri file, per lo più cifrandoli, e poi chiede un riscatto per ripristinare l'accesso ai file. I SophosLabs hanno identificato diversi esempi di ransomware: Zippo, entrato in scena nel marzo 2006, cifrava file e dati richiedendo poi un riscatto di $300.[5]

Ransom-A impediva alle vittime di accedere ai loro dati fino a quando non avessero pagato un riscatto di $10,99 tramite la Western Union.[6] Inoltre, minacciava di cancellare un file ogni mezz'ora fino ad avvenuto pagamento del riscatto, mostrava immagini pornografiche e visualizzava un fastidioso messaggio. Se l'utente tentava di utilizzare la combinazione di tasti CTRL+ALT+CANC per interrompere l'esecuzione del Trojan, riceveva un messaggio ingiurioso.

Arhiveus (vedere figura 4) pretendeva che la vittima acquistasse gli articoli di un drugstore online.[7]

Rootkit

"Rootkit" è il nome di una serie di strumenti software collocati da terze parti in un computer e destinati a nascondere processi in esecuzione, file o dati di sistema. L'idea venne alla ribalta alla fine del 2005, quando la Sony utilizzò un rootkit nei suoi CD musicali per proteggere i diritti di copyright. Seppur in buona fede, la Sony diede vita a una vulnerabilità sfruttata in seguito da numerosi Trojan. La Sony ha riconosciuto di aver causato disagi e perdite finanziarie ad utenti e aziende, e ha offerto loro una sorta di risarcimento.[8]

La minaccia, però, esiste tuttora, e Trojan creati ad hoc utilizzano spesso i rootkit per installarsi in un piccolo numero

Figura 4: file e dati "tenuti in ostaggio" dal Trojan Arhiveus

Cosa ci riserba il futuro?

Telefonia mobile

Già alla fine degli anni 90 alcuni produttori di antivirus predissero l'arrivo imminente di un potente virus che avrebbe infettato i telefoni cellulari, ma questo evento non si è ancora verificato. Ad oggi, non si conoscono virus che abbiano colpito cellulari o PDA su vasta scala, e la minaccia da essi rappresentata è alquanto trascurabile se si pensa alla pericolosità dei virus che colpiscono i sistemi operativi Microsoft Windows.

Una delle ragioni per cui non sono ancora stati creati dei virus che infettino i telefoni cellulari è che le bande di criminali organizzati, responsabili di creare la maggior parte del malware oggi in circolazione, non ritengono vantaggioso colpire questi dispositivi. I computer con sistema operativo Windows sono talmente popolari e vulnerabili che i virus li infettano con estrema facilità. Il variegato mercato della telefonia cellulare è caratterizzato invece da troppi sistemi operativi e tecnologie.

Data la crescente diffusione dei cellulari e l'utilizzo di sistemi operativi comuni, è probabile che in un prossimo futuro si dovrà fare i conti anche con il malware creato specificamente per tali piattaforme.

Sebbene allo stato attuale la minaccia rappresentata dal malware per i telefoni cellulari non desti preoccupazioni, i produttori di soluzioni di sicurezza stanno lavorando a una tecnologia di protezione dei cellulari, e si prevede che nel corso del 2006 saranno preannunciate soluzioni di sicurezza progettate ad hoc.

Windows Vista

Nel marzo 2006 Microsoft ha annunciato che il rilascio di Windows Vista, il suo sistema operativo di ultima generazione, è stato posticipato a non prima del 2007.

Il rinvio del lancio di Vista è una cattiva notizia per gli utenti sensibili al problema della sicurezza, poiché Vista include una serie di nuove funzioni che dovrebbero ottimizzare la protezione del sistema operativo contro gli attacchi del malware: per esempio, il tool contro lo spyware chiamato Defender, destinato agli utenti domestici. Gli attacchi diretti contro tali utenti utilizzando i computer zombie hanno permesso agli hacker di realizzare notevoli guadagni.

È probabile che Windows Vista costringerà gli autori di malware a rivedere le tecniche utilizzate sia per il malware che per i rootkit. I rootkit esistenti potrebbero non funzionare più a causa delle modifiche apportate da Microsoft al sistema operativo di base. Tuttavia, potrebbe trattarsi solo di una questione di tempo: prima o poi i creatori di malware conosceranno Vista tanto quanto basta per progettare rootkit o altro malware con eguale capacità di dissimulazione.

Macintosh

Sebbene il primo malware per Mac OS X sia stato identificato a febbraio 2006, non si è realmente diffuso sul campo ("in the wild") e non è stato foriero di una valanga di nuovo malware per il sistema operativo di Apple. Gli hacker continuano a prediligere gli attacchi diretti contro gli utenti di Microsoft Windows, disinteressandosi delle altre piattaforme. Sembra probabile che anche in futuro i Mac saranno un rifugio sicuro per gli utenti.

di sistemi senza attirare l'attenzione. È probabile che questa tattica diventi sempre più sofisticata nei prossimi mesi. Tuttavia, i rootkit sono difficili da creare, quindi vedremo in circolazione varianti di quelli esistenti piuttosto che nuove versioni. Resta ancora da vedere se funzioneranno su Vista, il nuovo sistema operativo di Microsoft, il cui rilascio è previsto per il 2007.

Spammer

Lo spam legato al settore medico (che riguarda principalmente presunti farmaci per migliorare le prestazioni sessuali o perdere peso, oppure gli ormoni della crescita) e lo spam contenente materiale pornografico restano le due tipologie più prolifiche. Inoltre, lo spam legato al settore azionario continua ad essere fonte di enormi guadagni per spammer senza scrupoli.

Alla metà di giugno 2006, gli esperti di Sophos hanno identificato una vasta campagna di spam che incoraggiava gli utenti ad acquistare azioni di una società chiamata Southern Cosmetics[9], al fine di gonfiarne il prezzo di mercato delle azioni. I messaggi di spam, che utilizzavano una grafica incorporata per bypassare i filtri antispam, sostenevano che fosse saggio investire in azioni della società, poiché questa era in affari con la Naomi LLC, azienda cosmetica cofondata dalla cantante country Naomi Judd.

Come diretta conseguenza di questa campagna di spam, il prezzo delle azioni della Southern Cosmetics ha subito un'impennata. Dall'analisi del prezzo risulta un forte incremento nella negoziazione del titolo, da meno di un centesimo di dollaro nel periodo precedente alla campagna di spam ai 6,6 centesimi del periodo successivo.

La figura 5 mostra un'altra società che è oggetto di monitoraggio da parte di Sophos. La campagna di spam è partita il 21 aprile, proiettando il volume delle azioni vendute alla quota di quasi 400.000 e gonfiando il prezzo delle azioni del 74%. Una settimana più tardi, una seconda ondata di spam ha causato un'ulteriore impennata dei prezzi.

Questo genere di spam viene inviato di solito nel fine settimana, perché in quei giorni la maggior parte dei produttori di soluzioni antispam, contrariamente a Sophos, non dispone di ricercatori che analizzino le nuove campagne di spam e distribuiscano le nuove regole per bloccarle.

Questa tipologia di spam utilizza esattamente le stesse tecniche di una truffa vecchio stampo. Lo spammer (che appartiene spesso a un gruppo di criminali organizzati) acquista le azioni a basso prezzo, le promuove tramite messaggi di spam e, quando il prezzo sale, comincia a venderle. Lo spammer ne ricava soldi a palate, l'acquirente si ritrova con un titolo sovraquotato e la società nel caos finanziario.

Ingegneria sociale

La maggior parte delle persone ha ormai compreso quanto sia rischioso cliccare su un allegato che dovrebbe contenere immagini o altro materiale relativo a un celebre personaggio senza veli. Di conseguenza, l'ingegneria sociale ha perfezionato le proprie tecniche rendendole più subdole. Temi politici, notizie di attualità o strappalacrime hanno reso l'inganno più difficile da riconoscere per gli utenti, e ribadito la necessità per le organizzazioni di mettere in opera un sistema di sicurezza inespugnabile.

Sophos ha continuato a intercettare numerose e-mail

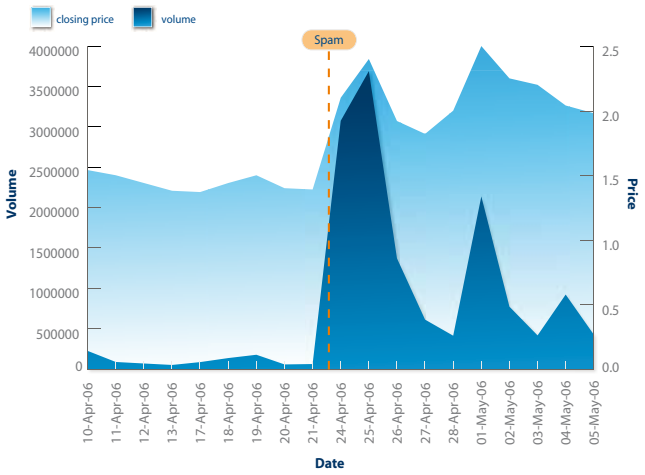

Figura 5: effetto pump & dump sulle azioni

fraudolente di questo genere. Nel giugno 2006, una versione del Trojan Stinx sosteneva che George W Bush e Tony Blair si fossero incontrati segretamente per concertare il prezzo del greggio proveniente dal Medioriente;[10] il worm Sixem, invece, adescava le proprie vittime nella fase preliminare della Coppa del Mondo di calcio, sostenendo di contenere immagini di tifosi nudi impegnati in un incontro di calcio.[11]

Classifica dei Paesi da cui viene inviato lo spam

Lo spam sta diventando sempre più un problema di portata mondiale. Presenta, infatti, un enorme vantaggio: qualunque sia la sede operativa dello spammer, questi può sfruttare agevolmente connessioni domestiche a banda larga non adeguatamente protette, in qualunque parte del globo, al fine di inviare messaggi commerciali indesiderati.

Gli Stati Uniti continuano a detenere il record negativo guidando la "sporca dozzina" dei Paesi da cui proviene il maggior volume di spam (23,4%). Rispetto al 2004, però, la

quantità di spam inviato è diminuita. Questa flessione è dovuta alla concomitanza di più fattori: sentenze di condanna per gli spammer, normative più severe e la migliorata sicurezza dei sistemi.

Gli USA sono seguiti dalla Cina (20,5%) e dalla Corea del Sud (8,7%). Tuttavia, come illustrato nella figura 6, gli stati asiatici nel loro insieme sono responsabili di una quantità di spam superiore a quella proveniente dagli Stati Uniti.

Esigenza di protezione

I computer non adeguatamente protetti continuano ad essere bersagliati in tempi sempre più brevi. Il malware che sfrutta le vulnerabilità presenti nei software è in grado di diffondersi senza l'intervento degli utenti. Gli hacker sguinzagliano i loro programmi dannosi, prima ancora che gli utenti abbiano potuto applicare le patch di sicurezza rilasciate da Microsoft

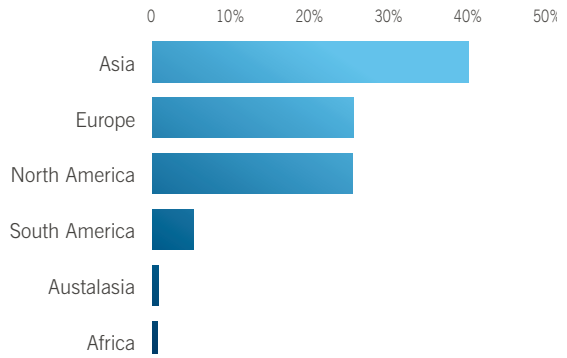

Figura 6: distribuzione geografica dello spam

o, addirittura in qualche caso, prima del rilascio stesso delle patch. Il Trojan Oscor-B, per esempio, sfrutta una vulnerabilità cosiddetta "del giorno zero" (day-zero) presente in Microsoft Word, che gli consente di infettare i computer all'apertura di documenti Word infetti.[12]

Riepilogo

La quantità crescente di nuove minacce, la rapidità con cui si diffondono e l'arduo compito di proteggere le reti avranno implicazioni significative per le imprese durante il secondo semestre del 2006. I criminali informatici diventano sempre più scaltri e utilizzano metodi sempre più ingegnosi per mascherare il malware, quindi le aziende saranno sempre più inclini a rivolgersi a un singolo produttore, con esperienza a 360 gradi nel campo della sicurezza informatica, e a soluzioni integrate in grado di proteggere i sistemi, i dati e la continuità del business da tutte le tipologie di minaccia informatica.

Bibliografia

1 Global Security Survey, Financial Services Industry and Deloitte Touche Tohmatsu, giugno 2006

2 The latest news on the Sober-Z worm outbreak, 1 in 13 emails are now infected by the Sober worm
www.sophos.com/pressoffice/news/articles/2005/11/soberz.html

3 Sober-Z worm poses as bogus messages from FBI or CIA
www.sophos.com/pressoffice/news/articles/2005/11/soberfbi.html

4 Obscene Kama Sutra worm spreads via email
www.sophos.com/pressoffice/news/articles/2006/01/nyxemd.html

5 Zippo Trojan horse demands $300 ransom for victims' encrypted data
www.sophos.com/pressoffice/news/articles/2006/03/zippo.html

6 Ransom Trojan horse demands money with menaces
www.sophos.com/pressoffice/news/articles/2006/04/ransom.html

7 Devious Arhiveus ransomware kidnaps data from victims' computers
www.sophos.com/pressoffice/news/articles/2006/06/arhiveus.html

8 Refunds for music fans hit by Sony DRM rootkit
www.sophos.com/pressoffice/news/articles/2006/05/sonysettlement.html

9 Cosmetics company's stock price rises sharply following spam campaign
www.sophos.com/pressoffice/news/articles/2006/06/stockspam.html

10 Spammed Trojan claims Bush/Blair Middle East oil cover-up
www.sophos.com/pressoffice/news/articles/2006/06/stinxw.html

11 Nude World Cup worm spreads via email
www.sophos.com/pressoffice/news/articles/2006/06/sixem.html

12 Trojan horse exploits zero day Microsoft Word vulnerability
www.sophos.com/pressoffice/news/articles/2006/05/oscorb.html