

rapporto sulla sicurezza primo trimestre 2008

Uno sguardo ai fatti salienti del 2008

Il rapporto passa in rassegna tendenze ed eventi che hanno scandito il primo trimestre del 2008, informando utenti e aziende sui rischi che attualmente ne insidiano la sicurezza, al fine di aiutarli a tutelarsi meglio contro eventuali attacchi.

In aumento il malware presente in Rete

Sul web si registra una presenza sempre più massiccia di malware: Sophos identifica attualmente una nuova pagina web infetta ogni 5 secondi. In altre parole, una media di oltre 15.000 pagine al giorno, una cifra tre volte superiore al 2007. Sophos ha individuato, inoltre, una nuova pagina web collegata ad attività di spamming quasi ogni 3 secondi.

Cresce il fenomeno della fuga di dati

Spiccano due casi di alto profilo in cui le società nordamericane Hannaford e Advanced Auto Parts hanno subito il furto dei dati sensibili dei propri clienti. Le aziende sono chiamate sempre più pressantemente a conformarsi alle nuove norme PCI (Payment Card Industry). Paradossalmente il caso più eclatante di violazione della sicurezza dei dati segnalato finora ha fatto seguito all'implementazione da parte di Hannaford di tali norme. Ciò dimostra che anche le più guardinghe delle aziende non sono immuni dal rischio di perdita dei dati.

Forte flessione del malware contenuto nei messaggi e-mail

L'incidenza delle mail infette è pari ad appena 1 su 2.500 contro 1 su 909 del 2007.

Arresti eccellenti

A febbraio le autorità canadesi hanno arrestato 17 persone sospettate di gestire la più estesa rete di computer zombie mai scoperta nel Paese. Si ritiene che fosse formata da quasi un milione di computer compromessi sparsi in 100 Paesi.¹ Nel mese di marzo il diciottenne neozelandese Owen Thor Walker è stato riconosciuto colpevole di sei capi d'accusa per aver utilizzato computer per scopi illeciti. Walker ha ammesso di aver svolto un ruolo fondamentale in un'operazione illecita in cui sono stati infettati 1.300.000 computer in tutto il mondo, con l'obiettivo di installarvi adware a scopo di lucro e sottrarre dati per un valore di 20 milioni di dollari.²

Malware in agguato sul web

Internet si riconferma lo strumento prediletto dagli autori di malware per mettere a segno i propri attacchi. La crescente dipendenza degli utenti dal web come fonte di informazioni lo rende il terreno ideale per i criminali informatici a caccia di utenti sprovvisti di adeguata protezione.

Nel 2007 gli esperti di SophosLabs®, la rete mondiale Sophos di ricercatori e analisti, hanno identificato una nuova pagina web infetta ogni 14 secondi. Allo stato attuale viene individuata una pagina ogni 5 secondi. Nel 79% dei casi si tratta di siti web legittimi, e non solo di quelli "a conduzione familiare".

Nel mese di marzo il sito web di un noto rivenditore di biglietti per gli incontri di calcio di Euro 2008 è stato manomesso da criminali informatici intenzionati a infettare i PC di inconsapevoli tifosi.³ A gennaio, invece, migliaia di siti web appartenenti a società presenti nella classifica Fortune 500, enti pubblici e scuole sono stati infettati da malware.⁴ A febbraio il sito web del canale televisivo britannico ITV è caduto nella trappola di una campagna pubblicitaria online finalizzata a colpire gli utenti Windows e Mac servendosi di un cosiddetto scareware, ossia un tipo di software progettato per ingannare gli utenti facendogli credere che il loro computer è infetto o vulnerabile, e spingerli ad acquistare una versione completa del software che lo disinfetterà.⁵

Nel mirino degli hacker sono finiti persino i produttori di software di sicurezza. Agli inizi del 2008 le pagine del sito di Trend Micro contenenti le analisi del malware sono rimaste per alcuni giorni in balia degli hacker.⁶ Non si tratta di un caso isolato tra le aziende del settore della sicurezza informatica. Anche i siti web di Symantec e Computer Associates hanno ambedue subito simili attacchi.⁷ Persino un forum dedicato alla sicurezza di Macintosh è stato bombardato da messaggi di spam contenenti materiale pornografico e malware.⁸

Mal/Iframe e Mal/ObfJS restano i dominatori indiscussi della classifica e gli hacker se ne servono per collocare codici malevoli su siti e server web sfruttandone eventuali vulnerabilità. Gli utenti farebbero quindi bene a navigare in Rete da un computer provvisto di adeguata protezione, mentre le aziende dovrebbero assicurarsi che i propri server web siano protetti da eventuali attacchi. Per maggiori informazioni su come salvaguardare i server web, consultare il documento tecnico dal titolo **Securing websites** redatto da SophosLabs.⁹

Dove si annida il malware?

Rispetto al "Rapporto Sophos sulla sicurezza 2007" la classifica dei Paesi che ospitano il maggior numero di siti web contenenti malware presenta alcune interessanti novità.

Gli Stati Uniti hanno fatto registrare un aumento senza precedenti, ospitando quasi la metà dei siti web infetti. Dopo aver chiuso il 2007 al secondo posto della top ten con una percentuale inferiore al 25%, nel primo trimestre del 2008 hanno totalizzato il 42% balzando al vertice della classifica.

Nel 2007 oltre la metà delle pagine web infette era targata Cina; per i primi tre mesi del 2008, invece, si è registrata, come già nel 2005, una quota inferiore a un terzo. L'esordiente Thailandia ha contribuito con l'1% dei siti web infetti identificati da Sophos.

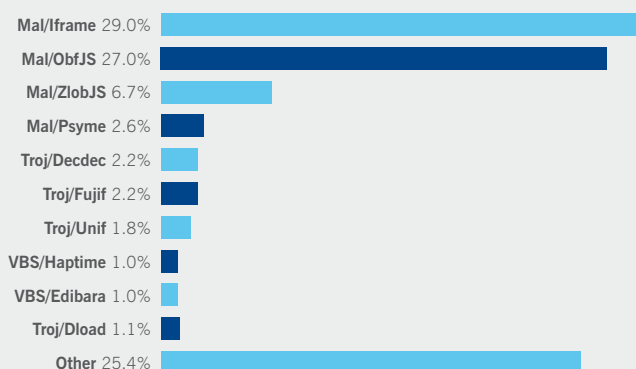
La Polonia e i Paesi Bassi, presenti nella classifica del 2007 rispettivamente in sesta e nona posizione, non figurano nella top ten di questo trimestre.

Malware via e-mail, spam e phishing

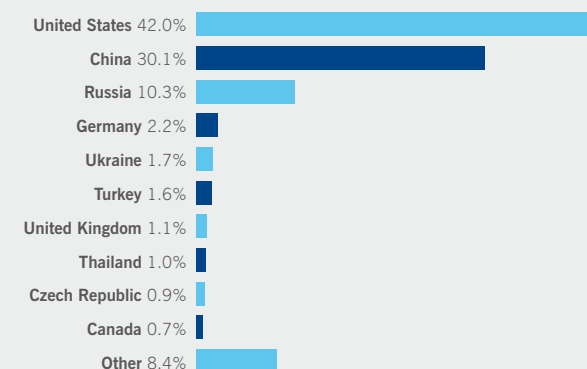
Nel primo trimestre del 2008 l'incidenza delle mail contenenti malware è stata pari ad appena 1 su 2.500, il 40% in meno rispetto al 2007. Invece di inserire il malware nel messaggio e-mail sotto forma di allegato, i cybercriminali inviano messaggi non richiesti contenenti link a siti web compromessi. Eppure è ancora diffusa la credenza che le mail non richieste, ovvero lo spam, siano innocue. Considerato che si tratta sempre di messaggi indesiderati e che un'alta percentuale di essi contiene link a siti web infetti, le aziende farebbero bene ad affrontare il problema prima che accada l'irreparabile.

Durante il primo trimestre del 2008 gli esperti di Sophos hanno identificato numerose campagne che hanno utilizzato il Trojan Pushdo. Alcune delle tecniche adottate sono state affinate allo scopo di eludere i sistemi di rilevamento.¹⁰ Queste tecniche implicano la modifica del tipo di programmi di compressione utilizzati per offuscare il malware. Pur essendo in vetta alla classifica del malware contenuto negli allegati di posta elettronica, Pushdo non si è diffuso su vasta scala come i worm di tipo mass-mailing in auge nel 2003 e 2004, ad es. Netsky, Bagle e Sobig, due dei quali sono ancora presenti nella top ten.

Top ten del malware identificato sul web nel primo trimestre del 2008



Top ten dei Paesi che hanno ospitato il maggior numero di siti web infetti nel primo trimestre del 2008



Spam

Lo spam non smette di agitare i sogni degli utenti. Dalle ricerche svolte da Sophos emerge che il 92,3% di tutte le mail in circolazione nel primo trimestre del 2008 era costituito da messaggi di spam. Milioni di nuovi messaggi vengono sottoposti giornalmente ad analisi automatizzate e utilizzati per affinare e aggiornare le regole per l'identificazione dello spam. Attualmente Sophos rileva oltre il 99% di tutto lo spam in circolazione.

Ogni 3 secondi in media, inoltre, Sophos individua una nuova pagina web collegata ad attività di spamming, in altre parole 23.300 pagine al giorno. Questa cifra include le pagine registrate su comunità virtuali come Blogspot, Geocities, ecc. e, secondo le previsioni di Sophos, è destinata ad aumentare fino a quando gli spammer realizzeranno profitti servendosi di questi stratagemmi. Bloccando in quarantena i messaggi di spam per evitare che vengano recapitati ai destinatari, le aziende non solo possono risparmiare tempo e denaro, ma anche proteggere i propri utenti dalle mail contenenti link a siti infetti.

Nel tentativo di aggirare i filtri basati sulla reputazione del mittente, gli spammer che si avvalevano delle botnet, le reti di computer zombie, cercano ora di manomettere i servizi di posta elettronica basata sul web come Hotmail, AOL AIM e Gmail. Di recente questa tecnica è stata adottata in un'importante campagna di spam nota come "Canadian Pharmacy". In alcuni casi le mail provenivano esclusivamente da indirizzi di posta elettronica basata sul web. Gli esperti ritengono che l'aumento dei messaggi di spam inviati da indirizzi di posta elettronica basata sul web potrebbe essere correlato al fatto che gli spammer sono riusciti ad aggirare i test CAPTCHA, usati per stabilire se l'utente sia o meno un essere umano.¹¹

La "sporca dozzina" rivela che gli Stati Uniti hanno ridotto il volume di spam prodotto, passando dal 21,3% dell'ultimo trimestre del 2007 ad appena il 15% del primo trimestre del 2008.¹²

Gli esperti di Sophos sono impegnati inoltre nel monitoraggio di numerosi domini cinesi promossi nell'ambito di campagne di spam. Un dato interessante è rappresentato dall'esistenza di una promozione che invita a registrare domini .cn al costo di un solo Yuan (14 centesimi di dollaro).¹³ Questo prezzo così accessibile risulta allettante per gli hacker, in quanto gli consente di registrare centinaia di nuovi domini e usarli a rotazione ogni cinque minuti per bypassare i filtri antispam che si servono di blacklist degli URL.

Phishing

La piaga del phishing continua a inquietare banche e istituti finanziari, causando problemi anche a grandi società online come eBay e PayPal. Nel primo trimestre del 2007, secondo i dati raccolti da Sophos, il 59% delle e-mail di phishing ha preso di mira almeno una delle due aziende.¹⁴

Per i primi tre mesi del 2008, invece, Sophos ha registrato una forte flessione delle campagne di phishing ai danni di eBay e PayPal. PayPal è stata il bersaglio di poco più del 15% delle truffe online, mentre eBay è stata presa di mira in meno del 4% dei casi. È probabile che l'aumentata consapevolezza degli utenti abbia indotto i phisher a escogitare nuovi espedienti per attirare le loro ignare vittime su siti web fasulli. Gli utenti devono essere prudenti nel fornire dati riservati online e assolutamente certi di operare da un computer munito di adeguata protezione.

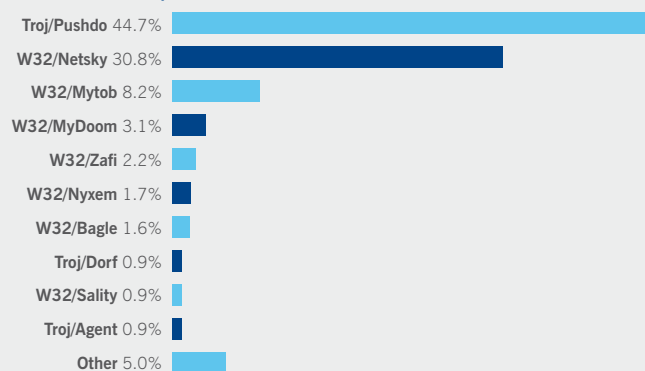
Gli esperti di SophosLabs hanno riscontrato inoltre un aumento delle attività di spear phishing, una strategia molto più mirata del phishing tradizionale, che colpisce obiettivi specifici. Gli attacchi sono stati sferrati contro numerose istituzioni educative nordamericane in possesso di servizi di posta elettronica basata sul web. Sebbene la maggior parte degli utenti abbia imparato a distinguere i tentativi di phishing tradizionale, è comunque incline a credere alle e-mail – e quindi ad esserne ingannata – che sostengono di provenire dal reparto IT o Risorse Umane della propria azienda. Pertanto le aziende sono urgentemente chiamate a vigilare in questo ambito.

Fuga di dati

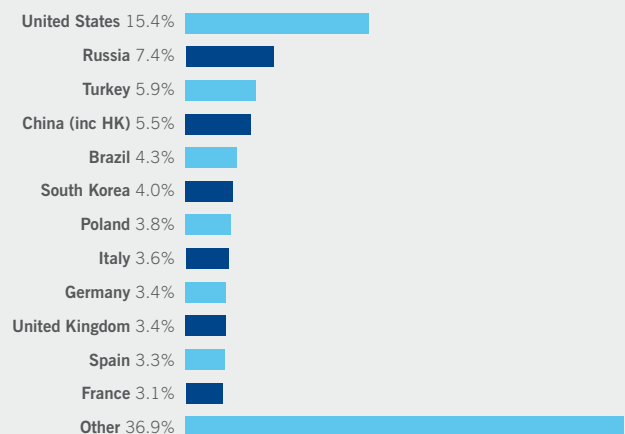
I casi di furto di dati sensibili che coinvolgono aziende ed enti pubblici continuano a fare notizia.

Nel mese di marzo 2008 si è appreso che i numeri della carta di credito di oltre 4 milioni di clienti della catena di supermercati Hannaford Bros erano stati rubati per mezzo di un malware installato sui server delle filiali della catena in New England e Florida.¹⁵ Tali dati sono poi stati inviati oltreoceano. Secondo quanto riportato dai media nel periodo in cui è stato stilato il presente rapporto, i Servizi Segreti continuano a investigare e hanno già scoperto circa 1.800 casi di truffa risultanti da questa violazione. Hannaford si è scusata con una lettera firmata Ron Hodge, CEO della società, che i clienti hanno trovato in ogni busta della spesa.

Top ten del malware diffuso mediante allegati di posta elettronica nel primo trimestre del 2008



La "sporca dozzina": i maggiori produttori di spam nel primo trimestre del 2008



Sempre a marzo Advance Auto Parts, rivenditore statunitense di ricambi e accessori per auto, ha reso noto che 14 delle proprie filiali in tutto il mondo avevano subito un attacco, in cui i dati sensibili di 56.000 clienti della società sono finiti nelle mani di criminali informatici.¹⁶

I particolari riguardanti le modalità con cui è stato perpetrato il furto non sono stati resi noti, e l'identità degli hacker resta tuttora sconosciuta. Advance Auto Parts ha dichiarato che sta collaborando con gli inquirenti.

Permane il dubbio su come gli hacker siano riusciti a infiltrare malware anche nelle reti di aziende che sono conformi alle norme PCI. Gli esperti di Sophos rammentano alle aziende che il raggiungimento della conformità non deve spingerle ad abbassare la guardia. Nessun sistema di sicurezza è inespugnabile, ma vale la pena ricordare che quanto maggiore è lo sforzo compiuto per sottrarre i dati di un'azienda, tanto minore sarà l'attrattiva dell'obiettivo in questione.

Nel corso del 2008 assisteremo senz'altro ad altri episodi di alto profilo, in cui rinomate società saranno costrette ad ammettere con imbarazzo di aver subito il furto dei dati dei propri clienti ad opera di criminali informatici.

Malware e vulnerabilità sui sistemi Macintosh: un trend in ascesa

Per quanto di portata trascurabile rispetto al problema che affligge la piattaforma Windows, il fenomeno del malware non risparmia nemmeno gli utenti Macintosh.¹⁷ Nel corso del primo trimestre di quest'anno, Sophos ha identificato un nuovo Trojan programmato per impaurire gli utenti inducendoli ad acquistare un finto software di sicurezza, una campagna pubblicitaria online in grado di infettare sia computer Macintosh che Windows e vulnerabilità che mettevano a rischio la sicurezza sia degli utenti Macintosh che Windows.¹⁸

Come diretta conseguenza della crescente quota di mercato detenuta da Apple, sembra probabile che gli hacker tenteranno con sempre maggior frequenza di farla in barba agli utenti di Internet, spesso erroneamente convinti di essere immuni da molti rischi che insidiano la sicurezza della Rete.

Il futuro

Il concetto di protezione dei dati, rispolverato e reintrodotta nel mercato da molti operatori del settore della sicurezza informatica, non rappresenta una novità. Da 15 anni a questa parte le problematiche inerenti la sicurezza ruotano intorno alla protezione delle informazioni: dai virus delle macro nei primi anni 90, che manomettevano e cancellavano le informazioni, all'odierno fenomeno del furto di dati su vasta scala.

Da un lato, i progressi tecnologici aiutano gli operatori commerciali a concentrare i propri sforzi su specifici mercati in modo rapido, efficace ed economicamente vantaggioso, ma dall'altro hanno semplificato la vita agli hacker. L'evoluzione della tecnologia favorisce sia buoni che cattivi, traducendosi in un migliore rendimento del capitale investito.

Non è tempo per le aziende di nascondere la testa sotto la sabbia nella speranza che nessuno si accorga dell'eventuale presenza di vulnerabilità nella sicurezza delle proprie reti. Gli attacchi odierni sono sofisticati, poggiano su solide basi e vengono sferrati su vasta scala. L'adozione di criteri di sicurezza aggiornati che salvaguardano il gateway web e di posta, proteggono in maniera proattiva gli endpoint e i dispositivi mobili e contribuiscono a sensibilizzare gli utenti ad un uso responsabile e appropriato del computer su Internet può rendere un'azienda un bersaglio tutt'altro che allettante.

Fonti

- 1 <http://www.sophos.com/news/2008/02/botnet-busted.html>
- 2 <http://www.sophos.com/news/2008/04/owen-walker.html>
- 3 <http://www.sophos.com/news/2008/03/euro2008.html>
- 4 http://www.theregister.co.uk/201/08/08/malicious_website_redirectors/
- 5 <http://www.sophos.com/news/2008/02/poisoned-adverts.html>
- 6 <http://www.sophos.com/security/blog/203/08/86.html>
- 7 <http://news.bbc.co.uk/1/hi/sci/tech/409980.stm>
- 8 <http://sunbeltblog.blogspot.com/2008/03/oops-macvirusorg-hosting-porno-malware.html>
- 9 <http://www.sophos.com/security/technical-papers/>
- 10 <http://www.sophos.com/security/blog/2008/03/1233.html>
- 11 <http://www.scmagazine.com/uk/news/article/789445/cybercrooks-beating-captcha-send-spam/>
- 12 <http://www.sophos.com/news/2008/02/dirtydozfeb08.html>
- 13 <http://www.cnnic.cn/html/Dir/2007/12/27/4953.htm>
- 14 <http://www.sophos.com/news/2007/10/paypal.html>
- 15 <http://www.sophos.com/news/2008/03/hannaford.html>
- 16 <http://www.sophos.com/news/2008/04/advance.html>
- 17 <http://www.sophos.com/news/2008/03/imunizator.html>
- 18 <http://www.sophos.com/news/2008/02/poisoned-adverts.html>

Informazioni su Sophos

Sophos offre soluzioni che consentono alle imprese di tutto il mondo di proteggere e controllare la propria infrastruttura informatica. Le soluzioni Sophos per il Network Access Control e l'ambiente endpoint semplificano la sicurezza, offrendo una protezione integrata contro malware, spyware, intrusioni, applicazioni indesiderate e violazioni delle politiche di sicurezza aziendale. Questa gamma di soluzioni è arricchita e completata da prodotti innovativi per la sicurezza della posta elettronica e della navigazione web, che filtrano il traffico di dati ricercando malware, spam e violazioni delle politiche di sicurezza aziendale. Sophos vanta un'esperienza ventennale nel settore della sicurezza informatica. Le soluzioni e i servizi Sophos, ingegnerizzati per ottenere la massima affidabilità, proteggono oltre 100 milioni di utenti in più di 140 Paesi. Rinomata per l'alto livello di soddisfazione dei clienti e per le sue soluzioni potenti e di facile uso, Sophos ha ricevuto numerosi premi, certificazioni e recensioni positive. Sophos è una multinazionale con sede centrale a Boston, USA e ad Oxford, UK. Per maggiori informazioni visitare www.sophos.it.

Per maggiori informazioni su Sophos e i suoi prodotti, visitare www.sophos.it

© Copyright 2008. Sophos Plc.

Tutti i marchi registrati e i copyright sono proprietà dei rispettivi titolari.

Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero dati o trasmessa, in qualsiasi forma o con qualsiasi mezzo, senza previa autorizzazione scritta degli autori.

SOPHOS
secured.