



G DATA

Rapporto sui malware

Rapporto semestrale luglio-dicembre 2008

Ralf Benz Müller

Go safe. Go safer. **G DATA.**

Rapporto sui malware di G DATA Luglio-Dicembre 2008

Ralf Benzmüller

Panoramica

Cifre e dati

- 894.250 nuovi virus nel 2008 sono ca. 6,7 volte in più rispetto al 2007.
- 576.002 nuovi virus nel 2° semestre del 2008 implicano un incremento di 1,8 volte rispetto al primo semestre.
- Le più frequenti categorie di virus sono i cavalli di Troia, i backdoor ed i downloader. Ulteriori categorie sono costituite da spyware, adware e worm.
- Le famiglie di virus più attive comprendono i backdoor, i ladri di account dei giochi online e i componenti per l'installazione di adware e scareware. Per diffondersi, il worm più attivo denominato "Autorun" utilizza le funzioni di autostart per CD e chiavette USB.
- Il 99,2% di tutti i malware del secondo semestre viene eseguito in Windows. Gli autori di malware si concentrano maggiormente sui leader di mercato. I codici dannosi destinati piattaforme mobili, Unix ed Apple anche nel 2008 hanno rappresentato per lo più un'eccezione.
- I malware per JavaScript sono diminuiti di oltre un quarto, mentre il numero dei virus basati su Flash è cresciuto del 38%. La tendenza quindi tende ad abbandonare JavaScript e a concentrarsi sui malware Flash.

Eventi e tendenze

- La generazione di exploit, ovvero codici dannosi che sfruttano le lacune della protezione per attaccare i computer, avviene in tempi sempre più rapidi. Nel mese di ottobre e dicembre Microsoft ha dovuto fornire patch aggiuntive.
- I più importanti trucchi sfruttati per indurre gli utenti di Internet a installare malware sono stati 1. Esortazioni a scaricare Codec o software, 2. Antivirus contraffatti e scareware e 3. E-Mail su ordini, pacchi e consegne.
- Le guerre del mondo vengono disputate sempre più spesso su e tramite Internet. I siti Web dell'avversario vengono attaccati con overload di dati e le fonti di informazione sono sottoposte a crack e manipolate a scopo propagandistico.
- Numerosi guasti nei dati rendono accessibili i dati personali anche di personaggi noti e rivelano informazioni militari strettamente riservate. La protezione dei dati non è presa sul serio.
- Il carding forum online "Dark Market", considerato un importante punto di scambio per le informazioni sulle carte di credito, è stato smantellato. In tutto il mondo sono state arrestate 56 persone.
- Intercage e McColo sono stati rimossi dalla rete. Il flusso di spam si è ridotto per un periodo ma il mercato della rete Bot si riorganizza.
- Sempre più spesso per diffondere spam e malware si utilizzano i social network.
- Grandi eventi quali le Olimpiadi e le elezioni presidenziali negli USA sono utilizzati da spammer e autori di malware.

Previsioni

- Internet è sempre più pericoloso. Applicazioni Web 2.0, social network, forum e blog offrono molte possibilità di attacco che nei prossimi mesi saranno sempre più sfruttate.
- Flash come mezzo di diffusione per i malware vedrà un incremento nei prossimi mesi. Finora la visualizzazione di filmati Flash non era considerata un pericolo.
- Il flusso di malware continuerà a crescere, ma con dei tassi di crescita ridotti

Contenuto

Eventi e tendenze del secondo semestre 2008

Lacune di protezione sfruttate rapidamente	4
Microsoft Patch-Day: Data fissa nel calendario dei cybercriminali	4
Vulnerabilità in Internet.....	5
Cyber-War: Internet come arma	7
Dati: fallimenti, ladri e guasti.....	8

Calendario

Luglio 2008	13
Agosto 2008	14
Settembre 2008.....	15
Ottobre 2008.....	15
Novembre 2008.....	15
Dicembre 2008	16

Malware: Cifre e dati

Il flusso di malware continua a crescere.....	17
Reti Bot, spyware e adware determinano il futuro.....	19
Attenzione ad Autorun	20
Malware Flash in ascesa.....	21

Prospettive per il 2009

Più pagine Web dannose	22
Più malware Flash	22
Allontanamento da Windows?	22
La caccia ai dati continua	22
Ancora più malware?	22

Eventi e tendenze del secondo semestre 2008

Nella seconda metà dell'anno 2008 i criminali online sono stati attivi su vasta scala. Nei G DATA Security Labs sono stati trattati talmente spesso i seguenti temi da richiedere un paragrafo dedicato a ciascuno. I temi più importanti sono forniti dagli exploit, dai trucchi più comuni, dalla guerra su Internet, dai guasti nei dati, dalla protezione dei dati e dalla lotta alla cybercriminalità.

Lacune di protezione sfruttate rapidamente

Gli esperti di protezione non mancano mai di sottolineare l'importanza di tenere aggiornati il sistema operativo ed il software. Molti produttori di software pubblicano, ad intervalli più o meno regolari, le patch aggiornate. Ogni secondo martedì del mese, Microsoft rilascia nuove patch relative a nuove lacune di protezione del sistema operativo o del software Microsoft (da qui deriva il nome "Patch-Day"). Col tempo si sommano svariate mini-installazioni. Il Service Pack 3 di Windows XP include le patch del Service Pack 2. Dal 9 luglio il Service Pack 3 di Windows XP viene rilasciato automaticamente tramite aggiornamento.

Microsoft Patch-Day: Data fissa nel calendario dei cybercriminali

Anche nel secondo semestre del 2008 gli hacker e i criminali online hanno reagito al "Patch-Day". Spesso le lacune di protezione vengono sfruttate anche subito dopo il rilascio delle patch di Microsoft. Gli hacker analizzano infatti i file modificati del sistema operativo e sviluppano dei codici Exploit sulla base delle informazioni acquisite. In molti casi il tutto richiede solo poche ore. Questi codici Exploit vengono quindi integrati da criminali online nei malware oppure, peggio ancora, negli strumenti per la creazione e la diffusione di malware.

Sempre più spesso, subito dopo il "Patch-Day" di Microsoft, sono state pubblicate anche lacune di protezione per le quali non esiste ancora alcuna patch. I criminali online attendono il Patch-Day e, se verificano che la lacuna non è stata ancora risolta, potranno continuare a infettare per un altro mese i computer, a meno che Microsoft non pubblichi una patch speciale. E proprio ciò si è verificato per due volte nel secondo semestre:

- Dopo che il 23 ottobre sono stati resi noti dei rapporti su attacchi mirati a computer Windows basati sulla vulnerabilità critica nel servizio RPC di Windows, Microsoft ha pubblicato un aggiornamento della protezione oltre i termini consueti (MS-08-067). Due giorni dopo Gimmiv.A utilizzava questa vulnerabilità per introdursi nei computer e rubare dati. Nonostante la rapida reazione di Microsoft, all'inizio del 2009 i computer del Governo locale della Carinzia e della società di gestione degli ospedali regionali della Carinzia KABEG sono stati infettati da un worm denominato Conficker (alias Downadup).
- Il 17 dicembre in un aggiornamento speciale (MS08-078) è stata chiusa una lacuna di protezione di Internet Explorer (versioni da 5 a 8). Su diversi siti web, non solo di quelli pornografici, è stato trovato il codice Exploit che sfruttava la lacuna per infettare i computer con un codice dannoso.

In particolare il primo esempio dimostra quanto sia diventato importante l'aggiornamento del software e dei sistemi operativi.

Vulnerabilità in Internet

Con dei trucchi perfidi, i criminali online tentano di convincere le loro vittime a installare malware durante la navigazione. I trucchi più efficaci per ingannare gli utenti sono

1. Esortazione a installare Codec o software che vengono indicati come mancanti sul sistema
2. Contraffazioni di scareware e antivirus
3. Consegne, ordini e pacchi

Nel primo caso si viene attirati su un sito web, tramite E-Mail o Instant Messaging, ma anche attraverso altri siti web o forum e newsgroup, che si ritiene contenga un video interessante o altri file multimediali. Durante la riproduzione viene constatato che non si è in possesso del Codec o software necessario. L'utente viene invitato a installare il componente presumibilmente mancante. Chi segue questo invito, infetta il proprio computer.

Nel caso di scareware (dall'inglese to scare : spaventarsi), all'utente viene fatto credere che sia in corso una scansione del sistema. Questa scansione termina diagnosticando la presenza (presunta) di malware sul computer. Successivamente all'utente viene suggerito di (o meglio forzato a) scaricare un antivirus contraffatto e spesso non funzionante. Questi prodotti nella maggior parte dei casi non riconoscono alcun malware. Essi fanno più che altro in modo di disattivare i messaggi di avviso inventati. Durante il secondo semestre sono apparsi i primi modelli di simili software antivirus falsi che integrano l'antivirus gratuito ClamAV. Evidentemente i criminali online vogliono sottrarsi all'azione penale.

Con ordini falsificati, messaggi di uffici incassi o comunicazioni su problemi nella consegna del pacco, gli utenti vengono invitati ad aprire il file allegato nella E-Mail oppure a visitare un sito web dannoso. Lì si nasconde un software nocivo che infetta il computer.

Ecco alcuni esempi:

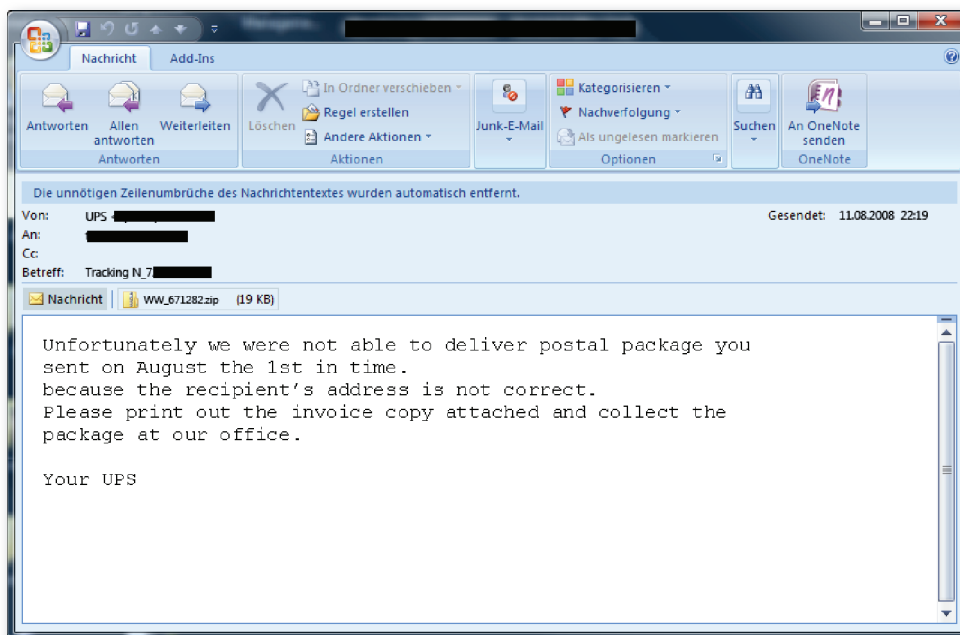


Fig. 1: Messaggio UPS falsificato del 11 agosto. Il file allegato installa spyware.

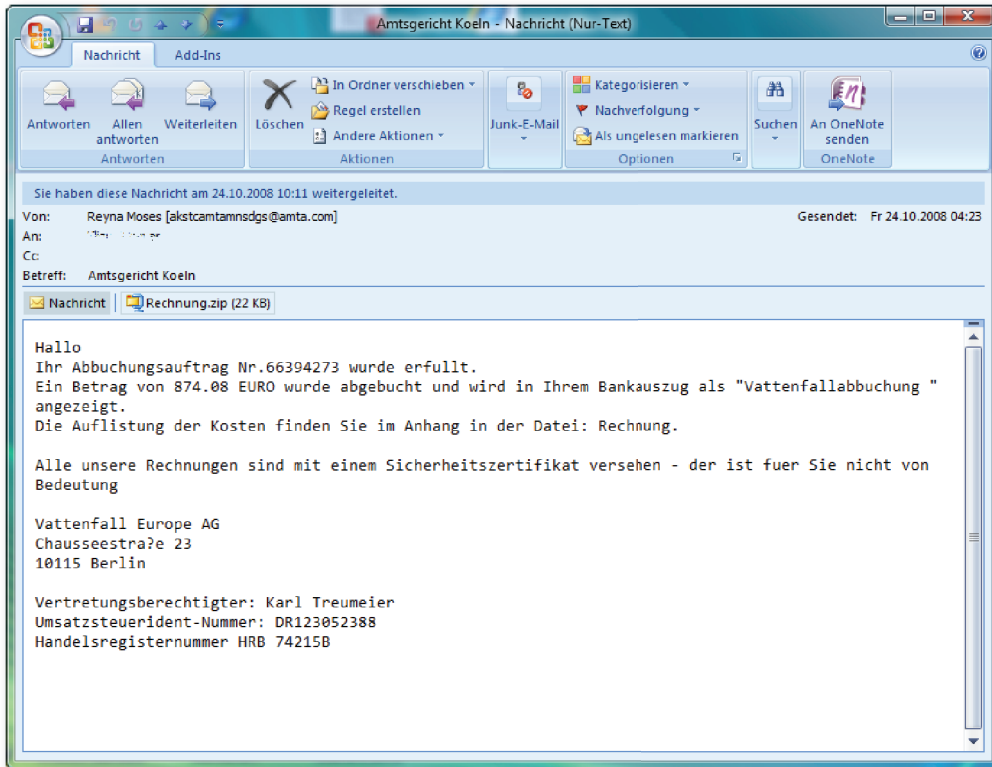


Fig. 2: Presunto ordine di addebito della Pretura di Colonia. Il file allegato „Rechnung.zip“ contiene un link denominato „Rechnung.txt“ ed il codice dannoso „Zertifikat.ssl“. Il link esegue questo codice dannoso come comando dalla riga di comando. (cfr. <http://www.gdata.de/de/virenforschung/news/news-details/article/928-warnung-vor-gefaelschten-rechn.html>)

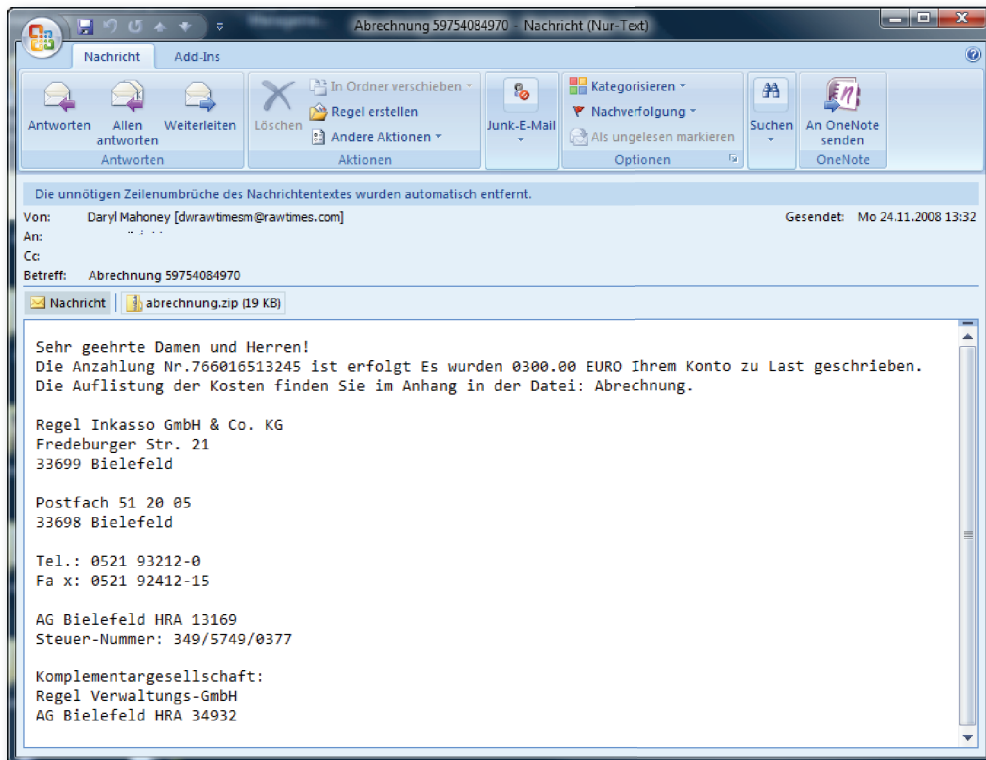


Fig. 3: A nome di Regola Incasso vengono inviati dei "Conteggi" che integrano il computer in una rete Bot.

Cyber-War: Internet come arma

Oltre al molto diffuso utilizzo commerciale di malware, i programmi dannosi sono impiegati anche per fini politici. Con i malware si spiano gli avversari politici e con essi si diffonde della propaganda. Gli attacchi all'infrastruttura IT avversaria nei conflitti appartengono già da molto tempo dell'arsenale delle forze armate. L'ultimo più importante evento si è verificato nel mese di maggio del 2007 quando dei nazionalisti russi in Estonia hanno sfruttato le reti Bot per decidere a loro favore la controversia politica relativa a un monumento russo dedicato ai caduti in guerra. Anche nel secondo semestre del 2008 su Internet si sono svolte delle controversie belliche.

- Durante la campagna militare di Russia contro Georgia, degli spammer anti-georgiani hanno tentato di costituire una rete Bot con dei presunti messaggi della BBC. Nel mese di agosto del 2008 la Georgia ha accusato la Russia di aver reso inaccessibile il sito Web del Ministero degli esteri tanto che i messaggi del Ministero degli esteri georgiano hanno dovuto essere pubblicati su una pagina Blogspot e sulla pagina del presidente polacco. Diversi attacchi DDoS (Distributed Denial of Service) sono stati perpetrati anche contro altre pagine di distribuzione delle notizie georgiane (apsny.ge, news.ge). Il sito web della banca nazionale georgiana è stato violato pubblicando immagini di dittatori e del presidente georgiano. Anche dalla parte opposta sono stati perpetrati degli attacchi su siti web del governo dell'Ossezia del sud e dell'agenzia di stampa russa RIA Novosti.
- Nel conflitto tra il Pakistan e l'India si verificano sempre delle controversie virtuali. Infatti nel mese di ottobre è stato violato, presumibilmente da aggressori pachistani, il sito web della società ferroviaria indiana Eastern Railway.
- Già poco dopo che Israele ha iniziato a bombardare gli insediamenti nella Striscia di Gaza, più di 300 siti web israeliani sono stati violati con messaggi anti-israeliani ed anti-americani. Come risposta gli israeliani hanno avviato una campagna di propaganda nella sfera dei blog. Hanno inaugurato un canale proprio su Youtube ed organizzato una conferenza stampa tramite Twitter. Anche su Facebook si svolgono delle battaglie. In gruppi quali " Hamas, I don't like them" o "Fxxk Israel" si pronunciano gli appartenenti delle relative fazioni. Alcuni di questi gruppi sono stati resi inaccessibili dalla "Jewish Internet Defense Force". Sul sito Web "help-israel-win" era possibile scaricare un programma che inseriva il computer in una rete Bot. Tale programma eseguiva attacchi su servizi Web nemici. La supremazia israeliana su questo territorio viene rafforzata anche dal fatto che sciiti e sunniti si ostacolano a vicenda con dei cyber-attacchi. Rimane per ora estranea a questa disputa l'Hamas sunnita.

Dati: fallimenti, ladri e guasti

Anche nel 2° semestre del 2008 sono stati resi noti numerosi casi di furti di dati, guasti nei dati e violazioni della protezione dei dati. Ecco una selezione di quanto riscontrato:

Il cittadino trasparente

Presso la sede centrale dei consumatori dello Schleswig-Holstein i cittadini si lamentano di addebiti non autorizzati. Si scopre che poco tempo prima tutti i clienti avevano acquistato tramite conto bancario dei biglietti da lotteria della Süddeutsche Klassenlotterie (SKL). Gli addetti al Call-Center avevano evidentemente a disposizione i dati bancari delle vittime. All'inizio del mese di agosto la centrale dei consumatori riceve anonimamente un CD con i dati di 17.000 cittadini. I dati con cognome, data di nascita, indirizzo, numero di telefono e di conto corrente sono stati venduti da una ditta del Nordreno-Vestfalia. Alcuni dipendenti scorretti del Call-Center sfruttavano evidentemente questi dati per prelevare dei soldi dal conto corrente degli utenti dopo un colloquio breve e probabilmente anche irrilevante. Il settimanale Wirtschaftswoche ha effettuato altre ricerche che alla fine hanno portato all'affare Call-Center. Nel mese di novembre ha rivelato che si trovavano in circolazione i dati bancari di ca. 21 milioni di cittadini. La vicenda riguarda quindi 3 correntisti su 4. Gli autori sono nella maggior parte dei casi dei piccoli Call-Center.

cfr: <http://www.verbraucherzentrale-sh.de/UNI123246437731306/link481821A.html>

<http://www.wiwo.de/unternehmer-maerkte/kontonummern-von-21-millionen-buergern-illegal-im-umlauf-380382/>

Best Western

25 agosto: 8 milioni di dati di clienti della catena alberghiera Best Western, che vi hanno soggiornato l'anno precedente, sono stati sottratti illecitamente da un cracker indiano e venduti tramite un forum underground alla mafia russa.

Guasti nei dati in Inghilterra

Nella seconda metà dell'anno è proseguita la serie di perdite di dati in Inghilterra. Gli eventi dimostrano da un lato la diversità delle condizioni che possono determinare la perdita di dati e dall'altro il modo sprovveduto e avventato con cui si utilizzano i dati personali.

- Luglio: In un treno vengono trovati dei documenti segreti sulla rete terroristica di Al-Kaida.
- 25 agosto: Viene smarrita una chiavetta USB con i dati di 84.000 detenuti britannici, tra cui 33.000 dati di pluripregiudicati. Una società che aveva il compito di realizzare un sistema per la gestione dei dati ha perso questo supporto dati. Complessivamente nel 2008 sono scomparse in Inghilterra 26 chiavette USB contenenti in parte informazioni riservate.
- 27 agosto: Su eBay viene messo all'asta a 45 € un computer contenente i nomi, i numeri di cellulare, i dati bancari e le firme di oltre un milione di clienti della Royal Bank of Scotland (RBS).
- 8 settembre: Scompare un disco rigido contenente nomi, date di nascita, numeri di assistenza sanitaria e residenze di circa 5000 dipendenti di case circondariali del National Offender Management Service (NOMS) britannico. È interessato un impiegato su nove della ditta. Alcuni chiedono il trasferimento ad altro incarico e/o altra sede per proteggere le proprie famiglie da possibili ritorsioni.

- 18 settembre: L'ufficio di insolvenza ammette la perdita di un laptop contenente dati personali di 122 ex-dirigenti aziendali. Nel laptop erano inoltre presenti informazioni su creditori, investitori e dipendenti.
- 30 settembre: Una macchina fotografica digitale, messa all'asta su eBay a 25 €, conteneva dati altamente riservati del servizio segreto britannico MI6 su sospetti terroristi di Al-Kaida con foto e impronte digitali ed informazioni sulla fornitura di armi.
- 10 ottobre: Da un ufficio della società di servizi IT EDS scompare un disco rigido portatile con i nomi, gli indirizzi, la data di nascita e altre informazioni di 100.000 persone appartenenti alle forze armate e di 600.000 candidati.
- 10 novembre: Nella settimana di Natale, la società di servizi di pagamento RBS WorldPay ha ammesso, dopo i primi casi di truffa, che sono stati rubati ca. 1,5 milioni di dati in seguito ad un attacco di hacker. I dati riguardavano informazioni personali di utenti per schede prepagate e schede omaggio e i PIN di tutte le schede a base PIN. È stato rubato il numero di matricola previdenziale (così importante negli USA) di ca. 1,1 milioni di clienti.

Guasti nei dati in Germania

Ma anche in Germania la protezione dei dati è stata calpestata:

- Presso LIDL, Penny, Plus, Norma, Rewe, Edeka, Tegut, Hagebau e in molte altre aziende i dipendenti sono controllati e spiati.
- La Telekom stessa si è impossessata di questo diritto e sfrutta i dati di collegamento esistenti per scoprire le vulnerabilità nella propria comunicazione aziendale.
- Il gruppo Lufthansa analizza illegalmente i dati di volo dei passeggeri (tra cui anche i giornalisti)
- Tramite il sindacato di Polizia erano disponibili liberamente su Internet i numeri di cellulare di 13.500 poliziotti berlinesi.
- Due ex dipendenti della T-Mobile hanno rubato 17 milioni di dati di clienti (indirizzi, numeri di cellulare, data di nascita ed event. indirizzi E-Mail), tra cui personaggi noti del mondo politico, economico e della stampa, e li hanno venduti ad ambigui commercianti di dati.

Vittime illustri

Anche in questo semestre alcune personalità della vita pubblica sono state vittime di attacchi più o meno mirati:

- Il 18 settembre è stato reso noto che è stato violato l'account di posta elettronica su Yahoo di Sarah Palin. L'aggressore ha risposto alle domande di sicurezza che vengono poste quando si dimentica la propria password. (cfr. <http://blog.wired.com/27bstroke6/2008/09/palin-e-mail-ha.html>)
- Nel mese di settembre da uno dei conti corrente del presidente francese Sarkozy è stato prelevato un piccolo importo. È piuttosto inverosimile che Sarkozy abbia inserito i propri dati in una pagina di Phishing. E non si tratta neanche di un attacco mirato. È molto più probabile che uno dei suoi computer fosse infetto da un Banking-Trojan. Dati simili vengono venduti a centinaia o migliaia di pacchetti. All'acquisto solitamente vengono impiegati pochi account di prova. Gli acquirenti di dati hanno quindi utilizzato i dati di Sarkozy per verificare la validità dell'intero pacchetto di dati. Evidentemente i ladri di dati non sapevano con chi avevano a che fare.

Protezione dati

Molti cittadini non si rendono conto di quanti dati vengono loro estorti e quanto preziosi possono diventare questi dati. Solo lentamente i casi di uso improprio che determinano ad es. malfunzionamenti, limitazioni della sicurezza o perdite finanziarie dimostrano il modo in cui i dati possono essere usati in modo improprio. Oltre ai criminali online che rubano denaro alle loro vittime con questi dati, anche alcuni imprenditori ambigui approfittano dell'uso spensierato dei dati dei clienti e delle informazioni di segnalazione. Con l'affare Call-Center è diventata chiara la vasta portata di queste azioni criminali. I dati della maggior parte di cittadini sono disponibili già da tempo ai commercianti di dati. Il valore dei dati e la loro protezione è tuttora sottovalutata.

In lotta contro l'economia eCrime

Nel mese di ottobre del 2008 le autorità penali, dopo due anni di missione sotto copertura, sono riuscite a chiudere il carding forum online "Dark Market" e ad arrestare 56 persone sparse in tutto in mondo. Dark Market era uno dei luoghi di scambio dei dati relativi a carte di credito e ai codici di accesso bancari.

Ma molto più efficace si è dimostrato un altro aspetto. Anche i siti web, i dati ed i server di controllo dell'industria malware devono essere ospitati su un computer. Il Russian Business Network (RBN) l'anno scorso si è reso tristemente famoso nel campo del "Bullet-Proof-Hosting". Tuttavia la crescente attenzione, suscitata anche presso gli inseguitori, ha avuto dei risvolti negativi per gli affari. La RBN si è divisa in diversi sottogruppi in Cina e nell'Europa dell'est. Pertanto altri Hosting Services, che non agivano in Europa dell'est o in Cina ma negli USA, hanno avuto modo di approfittarne.

Alla fine del mese di agosto del 2008 è stato reso noto che la ditta californiana Intercage, che poco prima si chiamava Atrivo, metteva i suoi servizi di Hosting e di registrazione di domini prevalentemente al servizio di utenti illegali (cfr. <http://hostexploit.com/downloads/Atrivo%20white%20paper%20090308ad.pdf>). Su Spamhaus la Atrivo/Intercage in 3 anni ha colpito con oltre 350 casi di diffusione di malware e Command & Control Server per reti Bot. Due provider di Intercage, in seguito alla pressione dell'opinione pubblica, hanno sciolto i contratti con Intercage e pertanto i server su Internet non erano più raggiungibili. Un provider amico di Intercage, entrato in sostituzione, dopo qualche giorno si è dovuto piegare alla pressione dell'opinione pubblica. Di conseguenza i server carichi di malware e spam di Intercage dal 21 settembre non sono stati più accessibili. Poco dopo Intercage è passata a un provider estone. I risultati sono stati:

- la diffusione di spam si è ridotta per un breve periodo.
- le turbolenze attorno a Intercage hanno fatto sì che le attività delle rete Bot Storm venissero annientate.

In seguito alle indagini su Intercage, agli inizi del mese di settembre il Privacy Protection Service del registratore di domini indiano entra in crisi. Questo tuttavia rapidamente si è estinto. (cfr. <http://www.knujon.com/news.html#09042008>). Nel caso del registratore estone ESTDomains la vicenda ha invece avuto degli sviluppi diversi. Qui continuavano ad essere registrati dei domini coinvolti in affari illegali, spam e phishing. Il 28 ottobre la ICANN ha annullato la collaborazione con ESTDomains e bandito la gestione dei 281.000 nomi di domini gestiti da ESTDomains (cfr. <http://www.icann.org/en/announcements/announcement-2-28oct08-en.htm>)

Gli effetti più forti sulla comunità di Internet tuttavia sono stati l'isolamento dell'Hosting-Provider californiano McColo. Brian Krebs del Washington Post ha reso note le relazioni tra McColo e Pharma Domains e Payment Sites, Scareware, siti web di pedopornografia, servizi di anonimato e last not least controller di reti Bot per le note reti Bot di spam. Quando McColo è stato rimosso dalla rete l'11 novembre, il volume di spam si è ridotto a un terzo del totale da un giorno all'altro (cfr. Fig. 4). Anche il servizio Proxy di Fraudcrew è stato annientato.

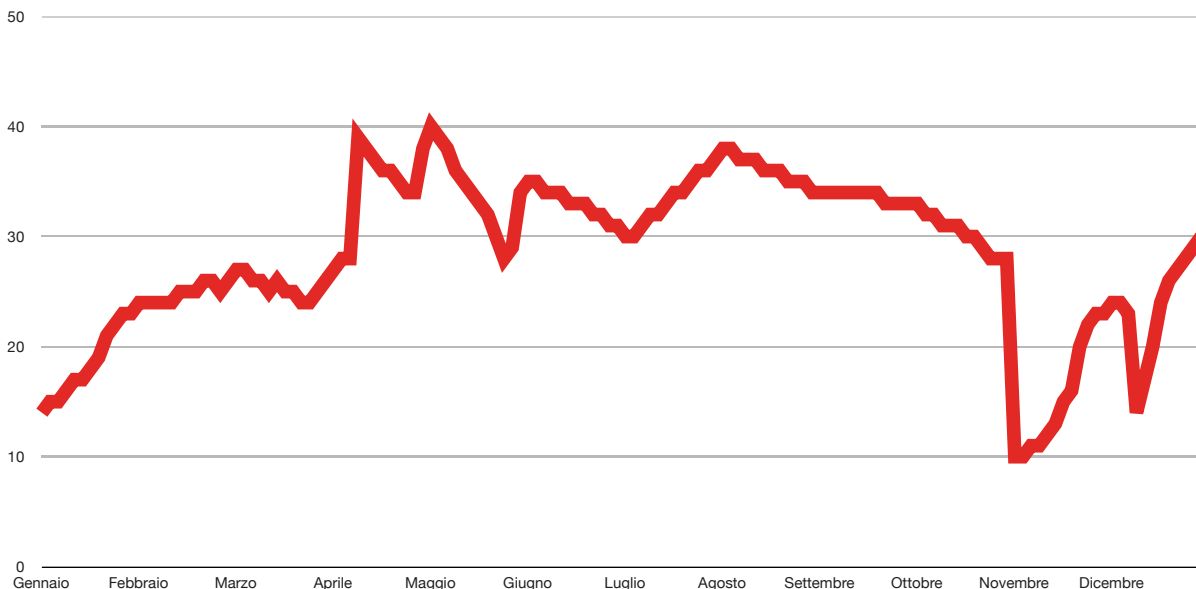


Fig. 4: Numero di Spam-Mail al secondo da gennaio a dicembre 2008.

Lo shutdown di McColo è stato così sorprendente per i gestori di reti Bot che in un solo colpo diverse centinaia di migliaia di PC zombie si sono trovati senza gestore. Ogni 72 ore gli zombie calcolano 4 domini di emergenza e qui cercano nuovi master. Ma gli specialisti della ditta FireEye sono riusciti a impossessarsi dell'algoritmo e a registrare per sé i domini risultanti. Poiché FireEye non era in grado di sostenere ulteriormente le spese di registrazione, pari a ca. 4000 \$ a settimana, alla fine del mese di novembre la registrazione è stata interrotta. In questo modo i "Bot-Herder" hanno avuto modo di accedere alla sua rete Bot. Per motivi legali FireEye ha rinunciato ad eseguire la disinfezione eseguibile dal punto di vista tecnico dei computer infetti. Poiché sui server McColo erano ospitati i server di comando di numerose reti Bot, successivamente la scena delle reti Bot è cambiata fortemente (cfr. Fig. 5). L'effetto sulla rete Bot Srizbi è stato profondo. Srizbi era fino ad allora la più grande rete Bot (ca. 450.000 zombi) attraverso la quale venivano inviate la maggior parte delle E-Mail di spam. Nel mese di novembre la quota della rete Bot Srizbi è scesa praticamente a zero. Evidentemente i "clienti" non intendevano aspettare la ripresa di Srizbi. In poco tempo subentrarono Pushdo (alias Cutwail) e Bobax. Dagli inizi del mese di dicembre Mega-D è la più forte rete Bot, ma da quest'anno Rustock e la

nuova rete Bot Xarvester sono in ripresa. Con Waledec e Cimbot sono in fase ascendente altre due reti Bot. Queste nuove reti Bot sono realizzate in modo tale da imparare dalle esperienze passate. La comunicazione è crittografata e i meccanismi Fall-Back sono escogitati in modo tale da evitare intoppi simili a quelli del caso di McColo. Ci sarebbe da augurarsi di poter rinunciare per il 2009 a simili successi. Ma non bisogna sottovalutare i gestori di reti Bot e crearsi troppe aspettative.

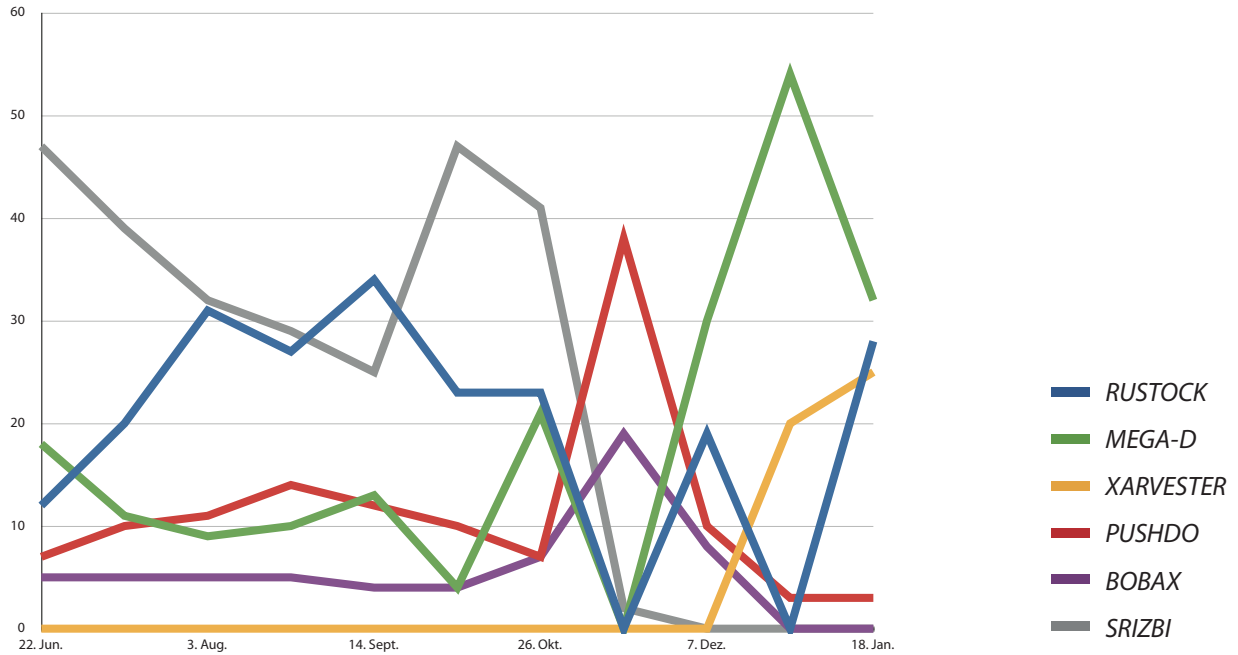


Fig. 5: Quota di reti Bot per l'invio di spam

Calendario

Oltre agli eventi raggruppati tematicamente nei capitoli precedenti, vi sono state anche alcune interessanti novità ed eventi che desideriamo elencare per data.

Luglio 2008

Il worm GetCodec sfrutta i file audio e video per diffondersi

Il 9 luglio compare un nuovo worm dal nome "GetCodec" che si diffonde attraverso i file multimediali del tipo WMA/WMV. In questo formato di file è presente molto di più di una semplice traccia audio o video, esso contiene anche informazioni sui Codec necessari. GetCodec modifica queste informazioni in modo tale che MediaPlayer non trovi questi Codec e cerchi di scaricarli da Internet. Finora simili richieste per l'installazione di Codec arrivavano solo dal browser. GetCodec estende la zona di pericolo a Media Player stesso. Nel caso in cui l'utente chiuda con OK la finestra di dialogo di conferma, al posto del Codec viene installato un cavallo di Troia che a sua volta carica altri software dannosi (tra questi anche un worm che infetta altri file WMA/WMV). Varianti successive possono infettare anche file MP2 ed MP3. I file vengono trasformati in formato WMA/WMV, mentre l'estensione del file non si modifica.

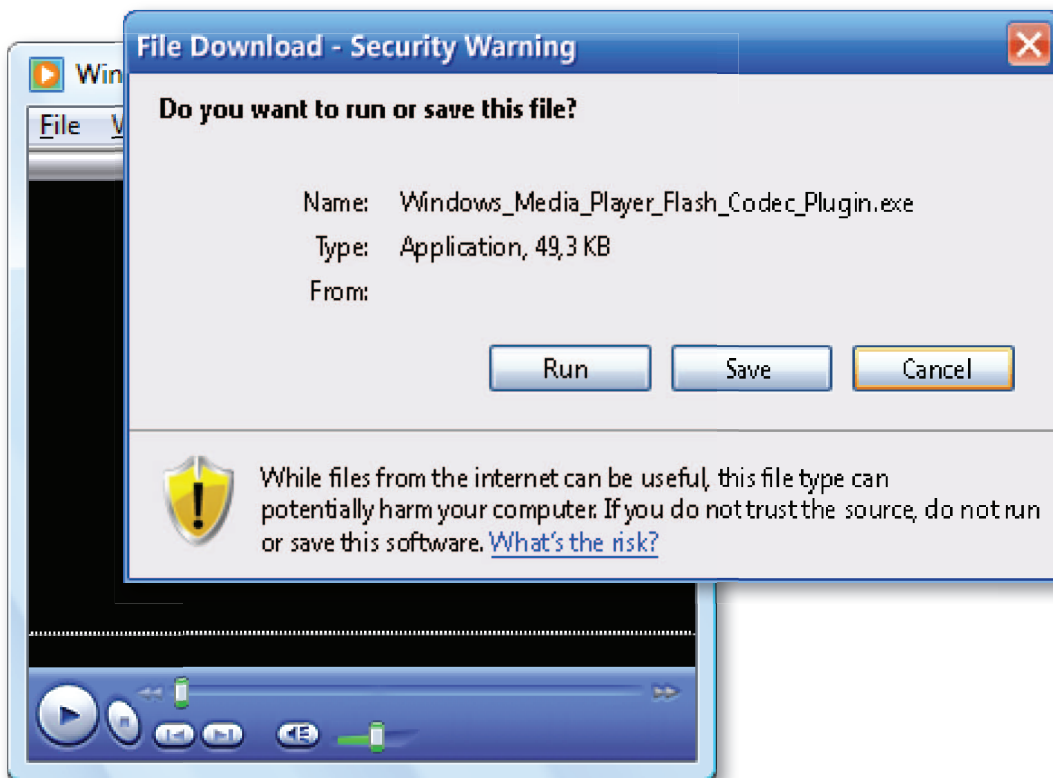


Fig. 6: GetCodec chiede l'installazione di un Codec da Media Player

3. Guerra mondiale

Il 10 luglio nelle E-Mail della rete Bot Storm viene preannunciata la 3° guerra mondiale. I video, presumibilmente girati da soldati, richiedono l'installazione di un Codec che è in effetti un cavallo di Troia. Altrimenti le attività della rete Bot Storm nei mesi successivi si esaurirebbero del tutto.



Fig. 7: Annuncio video della 3° guerra mondiale

Monster-Phisher

Gli utenti della borsa lavoro Monster il 14 luglio diventano obbiettivi di E-mail di phishing. Nelle E-Mail avente come oggetto "Monster customer service: new security measures." ai destinatari viene fatto credere che in seguito a delle modifiche tecniche è necessario effettuare una nuova registrazione. Coloro che seguono il link presente nella E-Mail vengono indirizzati ad una pagina contraffatta, ma molto simile a quella originale. Chi in questa pagina inserisce i propri dati di accesso fornisce ai phisher il proprio curriculum ed i dati personali.

Agosto 08

Social Network nel mirino

I Social Network sono sempre più amati e diffusi... anche presso i cybergangster. Gli account rubati vengono utilizzati per ospitare e diffondere messaggi di spam. Il 2 agosto un virus dal nome "Koobface" invia messaggi ad amici di MySpace e Facebook nei quali si invita a visionare un video interessante su Youtube. Sull'imitazione russa di Youtube viene richiesto un aggiornamento di Flash-Player che risulta essere invece un downloader.

Anche su Twitter agli inizi di agosto si verificano i primi casi di diffusione di malware. Alcuni profili realizzati appositamente rimandano a siti web con video contenenti immagini e testi allettanti. Qui si viene invitati ad installare Flash Player che si rivela essere un downloader che scarica dei cavalli di Troia di tipo banking. La visita dei profili preparati può essere richiesta tramite spam o Instant Message. Twitter offre in questo caso un'ulteriore possibilità. Attraverso una lacuna della protezione, con un clic sconsiderato su un link si può diventare "Follower" di un determinato profilo (cfr. <http://blogs.zdnet.com/security/?p=1611>).

Cavalli di Troia nello spazio

Sulla stazione spaziale ISS è stato trovato un cavallo di Troia del tipo Online-Gaming. Presumibilmente è riuscito ad infiltrarsi tramite una chiavetta USB o tramite un laptop infetto. I computer della ISS non sono collegati a Internet. (cfr. <http://blog.wired.com/27bstroke6/2008/08/virus-infects-s.html>)

Olimpiadi anche per i malware

I grandi eventi sportivi quali ad es. la finale del Superbowl negli USA anche l'anno scorso sono stati sfruttati dagli autori di malware. Puntuali, anche in occasione dei Giochi Olimpici in Cina, si sono verificate numerose attività di spam e malware. Ecco alcuni esempi:

- l'imitazione di una presentazione PowerPoint mostra delle immagini della cerimonia di inaugurazione e installa una backdoor.
- documenti Word e PDF promettono informazioni sui Giochi olimpici
- Screensaver con nomi quali "2008BeijingOlympics.scr" o "100Olymp.scr" infettano il PC con downloader e backdoor.
- Diverse centinaia di siti web che dovrebbero contenere informazioni sui Giochi olimpici sono utilizzati per la diffusione di malware. Nella maggior parte dei casi sono stati colpiti utenti asiatici.

Settembre 2008

Google Chrome Beta

La maggior parte di attacchi ai computer avviene attraverso il browser. La scelta del browser per gli utenti è pertanto una questione di fiducia. Agli inizi di settembre del 2008 con "Chrome" Google offriva una prima versione Beta di un browser. La struttura interna avrebbe dovuto tutelare da attacchi quali Cross Site Request Forgery. Ma la maggior parte delle preoccupazioni si è indirizzata contro l'enorme raccolta di dati di Google.

Ottobre 2008

ClickJacking

Il 15 ottobre è stato presentato un nuovo metodo per la modifica delle impostazioni nel browser nel quale i clic eseguiti in specifici giochi online possono essere utilizzati per modificare ad es. le impostazioni di Flash in modo tale da attivare la Webcam. (cfr. <http://video.google.com/videoplay?docid=-1023253423246814538&hl=en>)

Novembre 2008

Come nel caso dei Giochi olimpici, anche le elezioni presidenziali sono state utilizzate per diffondere malware. Obama e McCain erano presenti sempre più spesso nelle righe degli oggetti di E-Mail di spam che rimandavano a pagine di prodotti farmaceutici o a pagine malware.

Anche alcuni nomi di file contenevano il nome Obama:

- „Beat_Obama_NNN.exe" (NNN sta per una sequenza numerica casuale) installava backdoor della famiglia PcClient.
- Un altro nome di file suggeriva attività sessuali di Obama con una 17enne.

Come testare i software antivirus?

10 novembre: AMTSO pubblica delle direttive per testare gli anti-malware. L'organizzazione Anti-Malware Testing Standards Organization è un'unione di istituti di test di malware, giornalisti, accademici e produttori di soluzioni antivirus. Dopo lunghe discussioni il 10 novembre vengono pubblicate delle direttive per l'esecuzione di test di confronto espressivi e neutrali. Le direttive devono consentire test aperti, trasparenti e neutrali, eseguiti con metodi adeguati e devono condurre a risultati utili e sensati. (cfr. <http://www.amtso.org>)

Dicembre 2008

Malware-Fox

5 dicembre

ChromInject è un cavallo di Troia che si è integrato usando il nome GreaseMonkey-Add-Ons in Firefox e che successivamente ha letto i dati immessi su oltre 100 pagine di banche e li ha inviati a un server in Russia.

Scareware viene vietato

11 dicembre

L'americana Federal Trade Commission (FTC) vince in tribunale contro due produttori di scareware. Viene loro vietata la vendita dei presunti programmi di protezione di loro proprietà. Questi spesso sono „offerti“ su siti web in cui una scansione contraffatta infetta il computer. “offerti su siti web in cui una scansione contraffatta infetta il computer. Prodotti come WinFixer, WinAntivirus, DriveCleaner, ErrorSafe ed XP Antivirus tuttavia non proteggono da malware. Inoltre è stato sequestrato il patrimonio delle due società imputate (Innovative Marketing, Inc. e ByteHosting Internet Services, LLC).

Curse of Silence

In occasione del 25° Chaos Computer Congress di Berlino, Tobias Engel ha presentato una lacuna di protezione degli smartphone Symbian S60 di Nokia e di Sony Ericsson. Con un SMS appositamente formattato, viene interrotto il servizio SMS senza alcun avviso o avvertenza dello smartphone ricevente. Successivamente non sarà più possibile ricevere alcun SMS/MMS.

Malware: Cifre e dati

Il flusso di malware continua a crescere

Nel secondo semestre del 2008 è continuato a crescere il numero dei nuovi virus. Nel primo semestre i nuovi virus erano 318.248, nel secondo 576.002. Pertanto sono state superate quasi del doppio le cifre record dell'anno precedente. In tutto il 2008 sono stati rilevati 894.250 nuovi virus; 6,7 volte in più rispetto al 2007. Il numero delle famiglie di virus per l'intero 2008 è stato di 3069 rispetto ai 2313 del 2007, quindi solo poco più alto rispetto al 2007. Nel secondo semestre il numero delle famiglie di virus rispetto al primo semestre si è ridotto passando da 2395 a 2094. Il numero maggiore di malware non deriva invece da un numero fortemente in crescita di nuovi autori di malware.

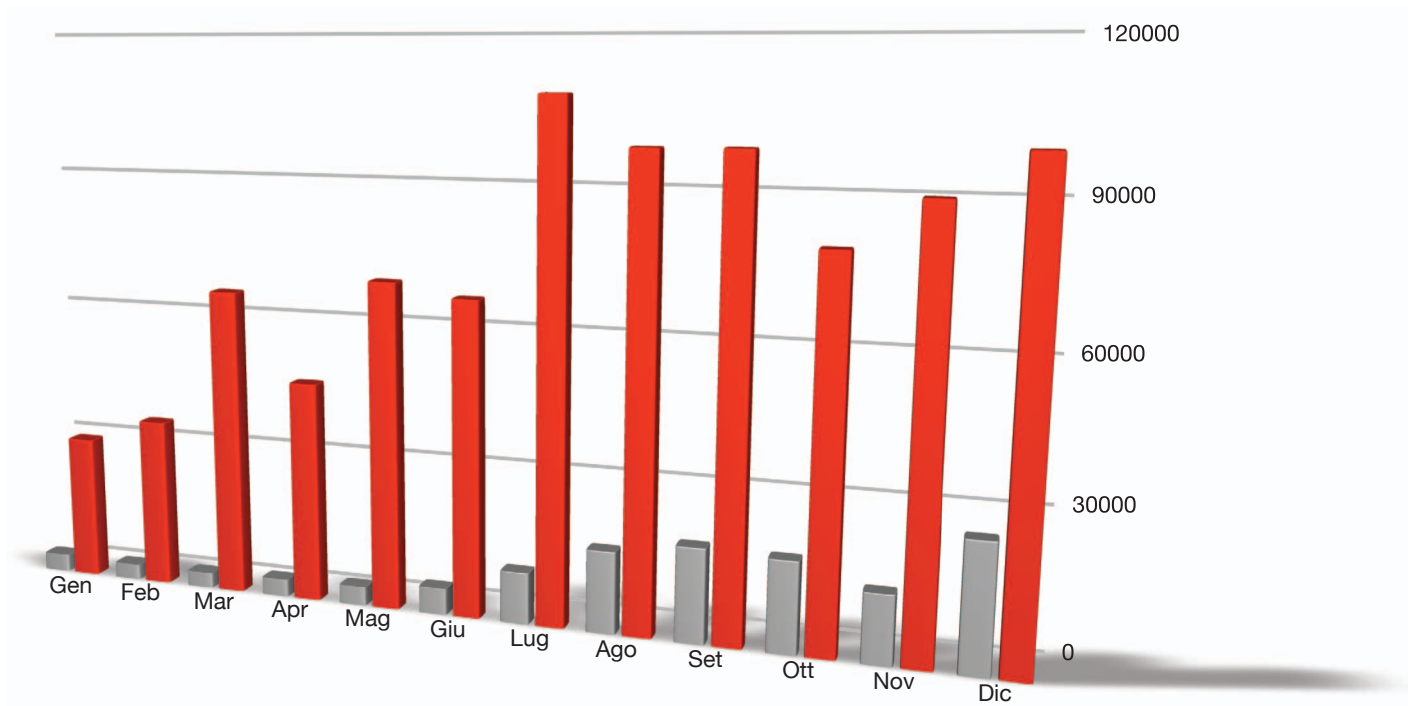


Grafico 1: Numero mensile dei nuovi malware per il 2007 (grigio) e il 2008 (rosso)

Le cause per questo nuovo incremento sono tra l'altro

- **Modularizzazione:** Il malware non si presenta più come un grande blocco monolitico. Tutte le funzioni vengono invece ripartite in specifici sottoprogrammi.
- **Utilizzo multiplo:** Per aggirare l'individuazione tramite delle firme, i file malware possono essere modificati con diverse tecniche di camuffamento e/o runtime packer, in modo tale da non poter essere più riconosciuti dai programmi antivirus. La funzionalità dei malware in questo caso resta (ampiamente) invariata
- **Cavalli di Troia usa e getta:** Molti downloader e numerosi cavalli di Troia sono pensati come elementi "monouso". Dopo aver fatto il loro servizio vengono eliminati dai sistemi infettati e non riutilizzati in questa forma dagli autori di malware

- Aggiornamento come meccanismo di mimetizzazione: Alcuni gestori di reti Bot eseguono spesso degli aggiornamenti dei componenti di backdoor. Tale operazione serve da un lato per la cura del software, ma è utilizzata anche per installare nuove versioni prima che gli aggiornamenti delle firme dei produttori AV riconoscano i malware.
- Lavoro su commissione: I PC zombie in reti Bot sono i complici dei mittenti di spam, phisher, estorsori e distributori di malware. I gestori di reti Bot affittano le loro reti per un determinato periodo o per eseguire determinati compiti. A tal fine ogni zombie riceve un pacchetto di software e di dati da elaborare. Terminato il lavoro il software e i dati vengono cancellati dal computer interessato. Quanto più versatile è l'utilizzo di una rete Bot tanto più malware specifici vengono diffusi.
- Polimorfia dal lato server: Sempre più malware vengono diffusi tramite siti web. Quando una vittima accede a una pagina infetta sono rilevati, sulla base dell'indirizzo IP, l'area di provenienza del visitatore, il browser, il sistema operativo e la relativa versione. Sulla base di queste informazioni ogni visitatore riceve un malware su misura. Teoricamente basandosi su queste informazioni si potrebbe creare sul server una cifratura del file ed ogni visitatore di un sito web potrebbe ricevere una versione diversa del malware. In questo modo è possibile diffondere migliaia di varianti dello stesso malware.

Per continuare a mantenere sotto controllo il flusso di malware diventa sempre più importante il riconoscimento proattivo. Le firme euristiche riconoscono i malware in base a determinate caratteristiche che interessano anche nuovi malware. Il riconoscimento fondato sul comportamento è un'ulteriore possibilità per riconoscere codici dannosi presenti sul computer. La generazione G DATA del 2009 ha migliorato ulteriormente il riconoscimento proattivo e, nonostante l'elevatissimo numero di malware, è in grado di garantire alti tassi di riconoscimento in poco tempo, anche nel caso di malware finora sconosciuti.

Reti Bot, spyware e adware determinano il futuro

Osservando le categorie di malware e il loro sviluppo, il quadro risultante è simile a quello del primo semestre. Esistono tuttavia alcune novità. Come in passato spyware e adware fanno parte delle categorie più frequenti. I primi posti sono occupati anche dai downloader, impiegati per infettare i computer, e dai backdoor, che consentono di controllare un computer a distanza e di integrarlo in reti Bot. Le percentuali di crescita in questi settori presentano un valore medio del 181%.

Categoria	#2008 S2	Percentuale	# 2008 S1	Percentuale	Diff 2008 S1 e 2008 S2
Cavalli di Troia	155.167	26,9%	52.087	16,40%	321%
Backdoor	125.086	21,7%	75.027	23,60%	166%
Downloader/ Dropper	115.358	20,0%	64.482	20,30%	172%
Spyware	96.081	16,7%	58.872	18,50%	162%
Adware	40.680	7,1%	32.068	10,10%	127%
Worm	17.504	3,0%	10.227	3,20%	171%
Tool	7.727	1,3%	12.203	3,80%	60%
Rootkit	6.959	1,2%	1.425	0,40%	487%
Exploit	1.841	0,3%	1.613	0,50%	114%
Dialer	1013	0,2%	4.760	1,50%	21%
Virus	167	0,0%	327	0,10%	51%
Altro	8.419	1,5%	5.170	1,60%	163%
Totale	576.002	100,0%	318.248	100,00%	181%

Tabella 1: Numero e percentuale delle nuove categorie di malware nel primo semestre e nel secondo semestre del 2008 e loro modifica

La categoria dei cavalli di Troia nel secondo semestre è purtroppo cresciuta di oltre tre volte ed è passata dal quarto al primo posto. Questa crescita deve essere spiegata con l'impiego dei cavalli di Troia precedentemente citati. Testimoniano l'utilizzo attivo di reti Bot per l'invio di spam, per l'esecuzione di attacchi di overload distribuiti e della maggiore modularizzazione di malware.

Il numero degli exploit è cresciuto. Ma qui non si tratta della massa. È importante che gli exploit disponibili vengano sfruttati rapidamente ed efficacemente come illustrato precedentemente.

L'incremento più si è registrato nel campo dei rootkit. Ciò dimostra come si sono affermati ed attestati come meccanismo di camuffamento per malware. La riduzione maggiore si è riscontrata sul numero dei virus (vale a dire agenti infettanti ed autoreplicanti del settore boot o di file) e dei dialer. La rilevanza dei dialer è sempre minore a causa dello scarso utilizzo di modem.

Attenzione ad Autorun

La Top 10 delle famiglie di virus mostra uno spaccato tra le più attive modalità di gioco di malware. La famiglia di virus più attiva continua ad essere il backdoor Hupigon. Al secondo posto rimangono le varianti di "OnlineGames" che per lo più ruba i dati di accesso ai giochi online tramite keylogger. Magania, l'altra famiglia che si impossessa dei dati di accesso a giochi online, nonostante l'accresciuta attività ha perso tre posti. Nuove sono le famiglie Monder e MonderB. Servono per installare i programmi scareware dalla famiglia Virtumonde che con messaggi falsi e snervanti di virus tentano di installare programmi quali WinFixer o AntiVirus XP. Con questa modularizzazione non è stato più necessario aggiornare così frequentemente i componenti principali di Virtumonde che scende dal 3° al 10° posto. Gli autori di Adware Cinmus, che si integra in Internet Explorer e visualizza PopUp pubblicitari, nel secondo semestre dell'anno sono stati molto più efficaci e hanno creato il doppio di varianti rispetto al primo semestre. Lo spyware Buzus si è piazzato invece al 6° posto. Unica nuova entrata nella Top 10 è il backdoor PcClient entrato al posto dei backdoor della famiglia Bifrose.

	#2008 S2	Famiglia di virus	# 2008 S1	Famiglia di virus
1	45.407	Hupigon	32.383	Hupigon
2	35.361	OnlineGames	19.415	OnLineGames
3	20.708	Monder	13.922	Virtumonde
4	18.718	MonderB	11.933	Magania
5	15.937	Cinmus	7.370	FenomenGame
6	13.133	Buzus	7.151	Buzus
7	13.104	Magania	6.779	Zlob
8	12.805	PcClient	6.247	Cinmus
9	11.530	Zlob	6.194	Banload
10	10.412	Virtumonde	5.433	Bifrose

Tabella 2: Le 10 famiglie di virus più attive nel primo e secondo semestre del 2008

Un'altra famiglia merita di essere citata. La famiglia di worm più attiva è Autorun che riesce, con 7256 nuove varianti rispetto alle 2756 del primo semestre, a classificarsi al 14° posto. Questa famiglia per diffondersi sfrutta anche le funzioni di Autorun del sistema operativo. A tal fine scrive informazioni nel file autorun.inf. Questo viene ad es. analizzato quando si inserisce o si collega un CD/DVD, un supporto dati USB o una scheda di memoria. In questo modo Autorun non ha riscosso grande attenzione, ma ha provocato ciononostante numerose infezioni.

Malware Flash in ascesa

Il 99,2% di tutti i malware mira ad attaccare il sistema operativo di Windows. La percentuale nel secondo semestre è cresciuta di un altro punto e, anche in assoluto, la percentuale di malware non Windows è scesa di ca. un quinto. Da un lato potrebbe essere dovuto al fatto che i difficili processi di camuffamento non sono necessari su altre piattaforme. Ciò dimostra tuttavia anche che gli autori di malware scelgono la strada con meno ostacoli e che si concentrano su utenti del sistema operativo leader di mercato. Raramente si presentano malware per altri sistemi operativi quali UNIX (16) o Apple (6). J2ME, la versione Java per dispositivi mobili e smartphone, spicca per i 59 nuovi modelli di malware. Complessivamente per le piattaforme mobili (J2ME, Windows CE e SymbianOS) sono stati rilevati 70 nuovi virus. Finora non si è registrata alcuna grande onda di attacchi su smartphone e dispositivi mobili.

	Piattaforma	#2008 S2	% 2008 S2	# 2008 S1	% 2008 S1
1	Win32	571.568	99,2%	312.656	98,2%
2	WebScripts	2.961	0,5%	3.849	1,4%
3	Scripts	1.062	0,2%	1.155	0,3%
4	MSIL	318	0,1%	252	0,1%
5	Macro	93	0,0%	164	0,0%

Tabella 3: Prime 5 piattaforme nel primo semestre del 2008. WebScripts si riferisce a malware a base JavaScript, HTML, Flash/Shockwave, PHP o ASP e solitamente sfrutta i punti deboli tramite browser. "Scripts" sono script Batch o Shell o programmi scritti nelle lingue di script VBS, Perl, Python o Ruby. MSIL è un malware presente nel codice intermedio dei programmi .NET. Le macro sono scritte in linguaggio macro per applicazioni quali Word, Excel, AutoCAD, PowerPoint ecc.

Anche gli autori di malware nella programmazione sfruttano le possibilità del framework .NET. Le applicazioni .NET, come le applicazioni Java, funzionano su diversi hardware. .NET offre inoltre la possibilità di assemblare le applicazioni di diversi progetti che sfruttano diversi linguaggi di programmazione. Per poter raggiungere questo risultato, tali applicazioni sono tradotte nel linguaggio MSIL (Microsoft Intermediate Language). Il numero di malware, creato in questo linguaggio intermedio dalle applicazioni .NET, nel secondo semestre è cresciuto in controtendenza e supera di molto il numero di malware Java.

Nonostante si verifichino sempre più attacchi tramite siti web, il numero di malware su base web con i linguaggi script quali JavaScript, ASP, PHP o ActionScript per Shockwave e Flash complessivamente si è ridotto. In particolare nel campo dei malware JavaScript, nel secondo semestre sono stati rilevati molti meno virus (1910 vs. 2650 nel primo semestre). Tuttavia in questo gruppo si è evidenziato il malware in formato SWF che ha segnato la crescita percentuale più alta (321 vs. 231 nel primo semestre). Il formato SWF sfrutta il linguaggio script ActionScript di Flash-Player. Questa nuova strada è ancora poco nota e solo pochi utenti temono che il loro computer possa essere infettato visualizzando dei video Flash.

Prospettive per il 2009

Sulla base degli eventi illustrati, delle cifre e delle tendenze è possibile fare alcune supposizioni sullo sviluppo della scena malware per il prossimo futuro.

Più pagine Web dannose

Il browser diventa sempre più importante come porta di ingresso per malware e gli attacchi al browser e ai suoi componenti sono sfruttati non appena sono resi noti. Ma anche molti servizi presenti su Internet vengono sfruttati molto per diffondere messaggi pubblicitari indesiderati e malware. In particolare gli utenti di social network, forum, blog, giochi online e applicazioni Web 2.0 dovrebbero agire in modo prudente. Server web compromessi, risultati di ricerca manipolati ed errori di battitura nell'inserimento dell'indirizzo URL possono condurre a pagine sulle quale il computer del visitatore viene infettato inavvertitamente in background (Drive-by-Download).

Più malware Flash

Il numero di malware che sfrutta le ActionScript Flash per la diffusione di malware nell'ultimo semestre è cresciuto notevolmente e presumibilmente continuerà a crescere. Finora i video Flash non erano visti come minaccia e questi sono i migliori presupposti per uno sfruttamento massiccio da parte dei cyber-criminali.

Allontanamento da Windows?

Negli ultimi anni i malware si sono concentrati sul sistema operativo di Windows. Il maggior numero di infezioni avviene su computer con Windows XP. Probabilmente questa situazione cambierà quando un maggior numero di utenti passerà a Vista o, verso la metà dell'anno, a Windows 7. Nel semestre in arrivo tuttavia non prevediamo che Windows scompaia dalla linea di tiro. È comunque probabile che gli utenti di OS X di Apple si debbano occupare molto di malware. I malware per smartphone avranno un ruolo secondario anche nei prossimi mesi.

La caccia ai dati continua

Il rapporto sui guasti nei dati e furti di dati nell'ultimo semestre ha reso più incisivo il valore attribuito ai dati personali. Tuttavia c'è ancora molto da fare e i criminali continueranno a tentare di accedere a dati bancari e delle carte di credito. Lo spyware anche in futuro costituirà una percentuale rilevante di malware. e continueremo a sentir parlare di guasti nei dati.

Ancora più malware?

In media nel 2° semestre del 2008 è stato scoperto un virus al minuto. È possibile prevedere che questo valore possa continuare a crescere. È chiaro che l'economia del cybercrimine non scomparirà e anzi diventerà più produttiva. La questione è tuttavia se i criminali online debbano produrre più file. Prevediamo ulteriori incrementi, ma con un tasso di crescita ridotto.

Go safe. Go safer. **G DATA.**