G DATA

Rapporto sul malware

Rapporto semestrale gennaio-giugno 2008

Ralf Benzmüller e Thorsten Urbanski

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

G DATA - Rapporto sul malware Gennaio-giugno 2008

Ralf Benzmüller e Thorsten Urbanski

1. Riepilogo: Incremento esplosivo di malware

Nel 2008 la fase di consolidamento delle attività del malware raccoglie i suoi devastanti frutti. Se il 2007 era stato considerato l'anno del malware per eccellenza, con un aumento del 300% rispetto al 2006, il 2008 supera già tutti i record. Soltanto nei primi tre mesi dell'anno in corso è stato messo in circolazione un numero maggiore di virus rispetto all'intero anno precedente (133.253).

Inoltre, nei prossimi mesi non si prevede alcun calo di questa inondazione di malware. Secondo una stima di G DATA Security Labs, già nel 3° trimestre del 2008 verrà superata la soglia di oltre mezzo milione di nuovi virus, ovvero un tasso di crescita nettamente superiore al 400%.

Dall'analisi delle famiglie di codici dannosi, emerge che gli obiettivi primari dei criminali sono il furto di dati e l'integrazione nelle reti Bot dei PC catturati. I downloader (37.546) e i backdoor (44.156) rappresentano in questo contesto la maggior parte dei nuovi arrivi nel primo semestre del 2008.

Codici dannosi	Nuovi arrivi	Quota in percentuale
Backdoors	75.027	23,6 %
Downloader/ Dropper	64.482	20,3 %
Spyware	58.872	18,5 %
Cavalli di Troia	52.087	16,4 %
Adware	32.068	10,1 %

Tabella 1: I primi 5 malware da gennaio a giugno 2008

1.1 Campi minati in rete

La minaccia delle pagine Web preparate è aumentata notevolmente. Il rilascio di codici dannosi in Internet, pronosticato da G DATA nel 2007, è ormai da molto tempo una realtà.

Per questa attività gli autori sfruttano le falle nella protezione del browser o dei plug-in del browser, come Flash, Real Player o Adobe Reader. Diversamente da quanto normalmente si crede, questi pericoli sono in agguato non tanto nei "club a luci rosse" di Internet, bensì soprattutto nelle pagine Web più note e frequentate.

1.2 Smartphone: è esplosa la bolla di sapone del marketing

Il clamore riguardo i virus degli smartphone non trova riscontro nelle cifre attuali: Gli autori di malware hanno distribuito soltanto 41 nuovi elementi dannosi fino alla fine di giugno 2008. Secondo le analisi condotte da G DATA, questi programmi dannosi sono, nella maggior parte dei casi, software di monitoraggio semilegali o studi di fattibilità (Proof of Concept).

Ciò è ancora più evidente se si esaminano le cifre totali dei nuovi elementi dannosi per smartphone a partire dal gennaio 2006: 145 nuovi codici dannosi per tutti i sistemi operativi degli smartphone. Parlare di un reale pericolo per i possessori di questi dispositivi sembra, al momento attuale, alquanto eccessivo.

1.3 Conclusione e previsioni

G DATA non prevede una pausa estiva delle attività di malware nelle prossime settimane e mesi. La produzione di nuovo malware si intensificherà ulteriormente e potrebbe raggiungere dimensioni impreviste.

Le prossime importanti manifestazioni sportive, come le Olimpiadi di Pechino, potrebbero aggravare ancora di più la situazione. I criminali online utilizzano gli eventi globali come occasione per intensificare la caccia ai dati e fare bottino. Va quindi presa in considerazione la probabilità di un aumento della produzione di e-mail nocive a breve termine.

I virus per gli smartphone, invece, anche quest'anno non avranno alcun ruolo determinante, poiché la diffusione di questo tipo di parassiti è sempre associata a un'interazione da parte dell'utente e, in caso di diffusione via Bluetooth, limitata nello spazio. Infine, last but not least, mancano promettenti business model di eCrime. In fondo, la criminalità online è un settore di professionisti che si orienta in base alle tendenze del mercato.

2. Introduzione

Lo sviluppo e la diffusione di malware è decisamente un affare per professionisti e provoca ogni anno danni per miliardi. Da tempo gli autori non agiscono più in singoli gruppi di cyber-criminali, bensì collaborano nelle reti mondiali, dividendosi il lavoro. Gli artefici di malware, gli spammer e i ricettatori di dati lavorano fianco a fianco e sono quindi in grado di coprire l'intero ventaglio di prestazioni criminali online.

In questo circolo di eCrime è indispensabile per i criminali, dal punto di vista economico, sviluppare e diffondere nuove creazioni di malware ad intervalli sempre più brevi, in modo da infettare, saccheggiare ed integrare nell'infrastruttura della rete "bot" il maggior numero di computer nel minor tempo possibile.

Ciò che G DATA aveva previsto alla fine del 2007 si è verificato nel 2008: il numero di codici dannosi è aumentato in maniera esponenziale! Soltanto nei primi sei mesi di quest'anno sono stati messi in circolazione 318.000 nuovi virus: un numero 2,4 volte maggiore rispetto all'intero 2007.

La diffusione di malware ha luogo principalmente tramite le pagine Web, che sono piene zeppe di strumenti per infettare i computer tramite il metodo "drive by download". Già l'anno scorso è stato ridimensionato il ruolo, fino ad allora dominante, degli allegati ai messaggi di posta come portatori di programmi nocivi, i quali vengono ora usati principalmente per attirare le vittime su pagine Internet preparate. La maggior parte delle nuove infezioni avviene attualmente tramite le pagine Web. Internet assomiglia quindi a un campo di battaglia con vaste aree minate!

3. Eventi e sviluppi importanti nel primo semestre del 2008

Nei primi sei mesi del 2008 le attività criminali online sono state numerose e incontrastate. I cosiddetti "storm worm", ritenuti da molti definitivamente debellati alla fine del 2007, hanno potuto festeggiare il loro compleanno in maniera molto particolare.

La banda degli storm worm ha suddiviso le reti Bot di modo che i computer dietro a un router inviassero solo spam. I computer senza router vengono utilizzati per ospitare pagine di spam e phishing. La risoluzione di un nome di dominio fa riferimento costantemente ad altri computer della rete Bot (metodo Fast Flux). Pertanto, è molto più difficile individuare in rete le pagine Web che contengono file nocivi.

Tramite le pagine Web compromesse viene diffuso un numero sempre maggiore di codici dannosi. Alcuni toolkit speciali semplificano l'introduzione di malware sui server Web ai criminali online. Inoltre, è stata ritoccata e implementata una vecchia tecnologia: i virus del settore di boot oggi non contengono più agenti infettanti dei file, bensì rootkit nascosti.

3.1 Lo "storm worm"[1] festeggia il suo compleanno

Nel primo semestre di quest'anno, i gestori della rete Bot Storm hanno dimostrato tutta la potenza della propria armata di computer zombie sfruttando anche le occasioni fornite da festività e ricorrenze internazionali, In effetti questi criminali hanno iniziato a sfruttare il giorno di San Valentino (14 febbraio) già da metà gennaio, ma ciò non ha impedito in alcun modo il loro successo. Il programma della banda Storm includeva anche cartoline "divertenti" e pagine Web relative al 1° aprile. In questa occasione sono stati infettati e trasformati in computer zombie una miriade di PC.

Dopo una fase relativamente tranquilla nell'ultimo trimestre del 2007, ora gli storm worm sono tornati attivi e si prevede che lo resteranno ancora per un pò!

Your download will start in 5 seconds.
If your download does not start,
click here and then press "Run".

Your download will start in 5 seconds.
If your download does not start, click here

Your download should begin shortly. If your download does not start in 10-20 seconds, you can click here to launch the download and then press Run. Enjoy!

(1) Lo storm worm è, da un punto di vista tecnico, un cavallo di Troia. Il termine risultante "storm trojan" è tuttavia meno affascinante e non completamente corretto.

Informazioni esplicative sulla rete Bot Storm:

Nel gennaio 2007 l'uragano Kyrill ha imperversato su vaste regioni d'Europa, provocando enormi danni. Il vento si era appena placato quando furono messi in circolazione messaggi e-mail che contenevano nell'allegato readmore.exe ulteriori informazioni sui danni provocati dall'uragano. Ecco spiegata l'origine del nome „storm worm", anche se non si tratta di un worm ma di un cavallo di Troia e anche se dallo stesso gruppo erano state diffuse, già alla fine di dicembre 2006, numerose e-mail con gli auguri per le festività natalizie e per l'anno nuovo.

L'obiettivo delle e-mail è, come in precedenza, integrare nella rete Bot i computer infetti, che verranno poi utilizzati per l'invio di spam e per attacchi DDoS (Distributed Denial of Service). Nei mesi seguenti si sono susseguite ondate di messaggi falsi („Saddam Hussein è vivo!" oppure „Fidel Castro è morto") e avvisi sulla presenza di virus. Anche queste e-mail contenevano un codice dannoso come file allegato.

Nel giugno 2007 la strategia è cambiata: eCard e cartoline di auguri attiravano gli utenti su pagine Web dove per visionare la cartolina occorreva installare un file (dannoso). Nel frattempo, i criminali cercavano di sfruttare in background le falle presenti nella protezione del browser o dei componenti del browser. L'infezione si verificava quindi durante la visione della cartolina. Venivano usati altri trucchi, come il download di codec per visionare video o di software per proteggere la trasmissione dei dati e la privacy. Come trucco è stato usato anche il reclutamento di utenti per testare programmi beta.

Per attirare le vittime su pagine Web nocive, nel settembre dell'anno scorso sono stati sfruttati ancora degli eventi di attualità. Si è cominciato con la „Festa dei lavoratori", seguita dall'inizio del nuovo Campionato Nazionale di Football Americano (NFL). In questo caso i download pericolosi sono stati presentati come „Free NFL Game tracker" (rilevatori gratuiti delle partite NFL). Altri trucchi usati facevano riferimento a giochi online, software di „cracking", festa di Halloween e nuovamente auguri di Buon Natale e Felice Anno Nuovo.

In autunno la rete Bot Storm è rimasta relativamente tranquilla. Evidentemente gli autori hanno trasferito le loro attività da San Pietroburgo alla Cina e alla Turchia per poter agire in maniera più massiccia.

3.2 Rootkit nel settore di boot

È sin dall'avvio del computer che la competizione tra malware e software di protezione ha inizio. Prima riesce il software di protezione ad assumere il controllo sul sistema e meglio sarà in grado di proteggere il computer, altrimenti il malware riuscirà a sfuggire alle funzioni di protezione.

Rivisitazione di una vecchia strategia

Con il Backdoor.Win32.Sinowal all'inizio di gennaio è apparso un virus "in the wild" che sovrascrive il record di avvio principale per ancorare alcune funzioni mimetiche nel kernel di Windows XP. Questa nuova tecnologia di mimetismo viene utilizzata per occultare le funzioni che realizzano furti nei siti di online banking. Nel primo semestre del 2008 sono apparse 97 varianti di questo virus. L'introduzione clandestina di codici dannosi nel settore di boot è tuttavia un modulo a sé stante, indipendente dalla funzione nociva e quindi può essere integrato rapidamente in altri malware. Il malware ha gioco facile, in XP perfino un normale utente è in grado di sovrascrivere il record di avvio principale, mentre in Vista l'operazione è un po' più complicata.

Esistono tuttavia alcuni meccanismi di protezione: spesso il BIOS offre la possibilità di dotare il record di avvio principale con una protezione anti-scrittura. Probabilmente ora è il momento giusto per adottare questa precauzione. In passato i virus del settore di boot sono stati rilevati avviando il computer tramite un dischetto pulito.

Il CD di boot con le soluzioni antivirus di G DATA è in grado di rilevare in modo affidabile gli attuali rootkit del record di avvio principale.

Secondo G DATA Security Labs è solo una questione di tempo prima che i nuovi virus imparino a sfruttare questa tecnologia per nascondersi.

Funzionamento

La prima posizione nel processo di avvio in cui il controllo viene assunto dal software modificabile è il record di avvio principale (Master Boot Record: MBR) di un disco rigido o il settore di boot di un altro supporto di avvio, ad esempio un dischetto. Il record di avvio principale (MBR) è il primo settore di un disco rigido. Qui è memorizzato il caricatore di avvio e la tabella di partizione del disco rigido. Il caricatore di avvio contiene il codice eseguibile, identifica la partizione di boot e carica le parti importanti del sistema operativo, ad es. il kernel.

Mentre il settore di boot è la prima posizione in cui un codice estraneo può infiltrarsi nel sistema, già i primi virus come Brain, Stoned e Michelangelo erano dei cosiddetti virus del settore di boot. Non è dunque una novità che i codici nocivi sovrascrivano il settore di boot per assumere il controllo.

Purtroppo in Windows XP è sempre possibile sovrascrivere il record di avvio principale. Tuttavia l'anno scorso questa falla è stata sfruttata solo da pochi virus. Nel 2005 Derek Soeder di eEye Digital Security ha illustrato la possibilità con BootRoot che un rootkit possa venire attivato nel record di avvio principale. In questo caso le funzioni mimetiche si attivano prima ancora che venga caricato il sistema operativo. Nel 2007 Nitin e Vipin Kumar di NVLabs hanno pubblicato VBootkit, nel quale sono state implementate le funzioni mimetiche per Vista. Sia BootRoot che VBootkit erano studi tecnici di fattibilità, i cosiddetti Proof of Concept, senza reali funzioni dannose e non sono mai comparsi associati a un malware. Ora con Sinowal la situazione è cambiata.

3.3 Internet come un campo minato: fare clic, infettare, derubare

Nel primo semestre del 2008 la minaccia delle pagine Web infette e preparate ad arte è aumentata notevolmente ed Internet assomiglia sempre di più a un campo di battaglia.

Attualmente più del 70% di tutte le infezioni provocate da codici dannosi avvengono visitando le offerte via Internet. Occorre aspettarsi un ulteriore incremento in concomitanza con eventi sportivi, come le Olimpiadi di Pechino. I portali dei fan, mal protetti e già infetti, rappresentano per i cybercriminali le piattaforme ideali.

Metodo adottato dalle gang online:

Solo poche e-mail con le quali si diffondo gli attuali virus contengono ancora allegati di file. La maggior parte rimanda direttamente a un file dannoso oppure offre il file dannoso in una pagina Web di download. Spesso l'inganno è camuffato da notizie di attualità, cartoline elettroniche, presunti addebiti e codec per film interessanti.

Il codice nocivo, infiltrato nelle pagine Web, tenta di sfruttare i punti deboli nel browser o nei componenti del browser (come Adobe Reader o Flash) per infettare subdolamente il computer quando questo richiama la pagina. Contrariamente a quanto credono molti utenti, questi "**drive by download**" raramente si nascondono nei club a luci rosse di Internet.

Il maggior numero di infezioni proviene da normali pagine Web molto frequentate, in cui vengono usati i banner pubblicitari in maniera fraudolenta o vengono crackati gli stessi server Web. Ciò può accadere, ad esempio, a causa di password degli FTP inefficaci o rubate oppure sfruttando le falle nella protezione di comuni applicazioni Web, come sistemi per la gestione dei contenuti o Bulletin Board.

Software per i forum: una porta per le invasioni

Nel primo trimestre del 2008 si sono verificati attacchi di massa ai punti deboli di applicazioni Web. Ad esempio, un errore nel software per forum phpBB ha generato da febbraio migliaia di pagine Web infette. Ad aprile centinaia di migliaia di pagine Web sono state attaccate tramite SQL Injection e hanno fornito un IFRAME nocivo ai visitatori delle pagine Web. Anche il numero di virus basati su Flash è aumentato notevolmente.

Per i server coinvolti in questa trappola sono stati diffusi strumenti ancora più efficaci, con i quali vengono introdotti in una pagina Web i codici nocivi che si infiltreranno poi inosservati nei computer degli utenti che visitano tale pagina.

All'inizio dell'anno è apparso FirePack, attualmente presente anche in versione cinese. A febbraio si è palesato all'improvviso un nuovo toolkit Multi-Exploit. Ma anche MPack, IcePack, TrafficPro, Nuclear Malware Kit, Web-Attacker, SmartPack ed altri sono venduti in Internet a prezzi che oscillano tra 40 e 3000 dollari.

È evidente che in ogni pagina Web può esserci un codice dannoso in agguato. La protezione antivirus dovrebbe quindi essere configurata in modo da verificare il flusso di dati HTTP prima che questo venga elaborato dal browser.

Per verificare questo fatto, provate a scaricare la versione testuale del file di test EICAR. Si tratta di un programma per DOS che emette il testo „EICAR-STANDARD-ANTIVIRUS-TEST-FILE!“. Questo programma, in sé innocuo, viene rilevato da tutti i software antivirus come codice dannoso.

Se provate a scaricare la versione testuale di questo file dal sito http://www.eicar.org/download/eicar.com.txt, riceverete un messaggio di avviso che impedisce l'accesso alla pagina oppure nel browser verrà visualizzata una riga con un testo criptico, incluso il testo sopra citato. Se si verifica quest'ultimo caso, il vostro computer non è assolutamente protetto da attacchi provenienti da Internet. Come accade per questo testo, nel browser possono essere caricati codici di script. Il codice viene inizialmente eseguito e solo quando il browser salva i file nella cartella dei file Internet temporanei il programma antivirus si accorge che un virus è attivo ed emette un avviso, ma a questo punto è troppo tardi.

4. Cifre e tendenze del malware nel primo semestre del 2008

Il numero di nuovi malware è cresciuto notevolmente, anche con la corresponsabilità dei runtime packer. Come in precedenza, lo scenario è dominato da reti Bot, spyware e adware. La percentuale di spam si è consolidata a livelli elevati e gli spammer hanno sempre pronti un paio di nuovi trucchi. Nei paragrafi che seguono sono riportati i dettagli.

4.1 L'inondazione di malware nel 2008

Il 2008 potrebbe essere citato sin d'ora nella storia del malware. Ricorrendo a metodi davvero originali, gli autori sono riusciti in soli tre mesi a battere il record del 2007. Già alla fine di marzo 2008 gli esperti di G DATA Security Labs hanno registrato un numero maggiore di nuovi virus rispetto all'intero anno precedente.

G DATA calcola che entro la fine dell'anno il numero di nuovi elementi dannosi sarà quantomeno quadruplicato. Ciò è dovuto al fatto che i programmi di scansione dei virus sono in grado di rilevare solo i codici malware conosciuti e gli artefici del malware traggono vantaggio da questa caratteristica. Come descritto nell'ultimo rapporto sul malware "Riciclaggio del malware", un codice nocivo viene trasformato in modo tale che i database antivirus non sono in grado di rilevarlo, anche a causa dei packer e di altri strumenti di occultamento. La funzionalità del codice dannoso resta comunque intatta. Il codice così modificato e non più riconoscibile viene diffuso immediatamente.

Un ulteriore meccanismo che produce numerose nuove versioni viene impiegato spesso con i backdoor. La maggior parte dei backdoor sono dotati di una funzione di aggiornamento che viene ampiamente sfruttata come meccanismo di mimetizzazione. I backdoor vengono aggiornati con una tale frequenza, che i programmi antivirus esaminano sempre una variante ancora sconosciuta. Quindi, anche in questo caso, i database antivirus non sono in grado di rilevare una nuova versione. Il tempo di reazione che intercorre tra l'infezione causata da un virus e la disponibilità dei database idonei svolge un ruolo fondamentale.

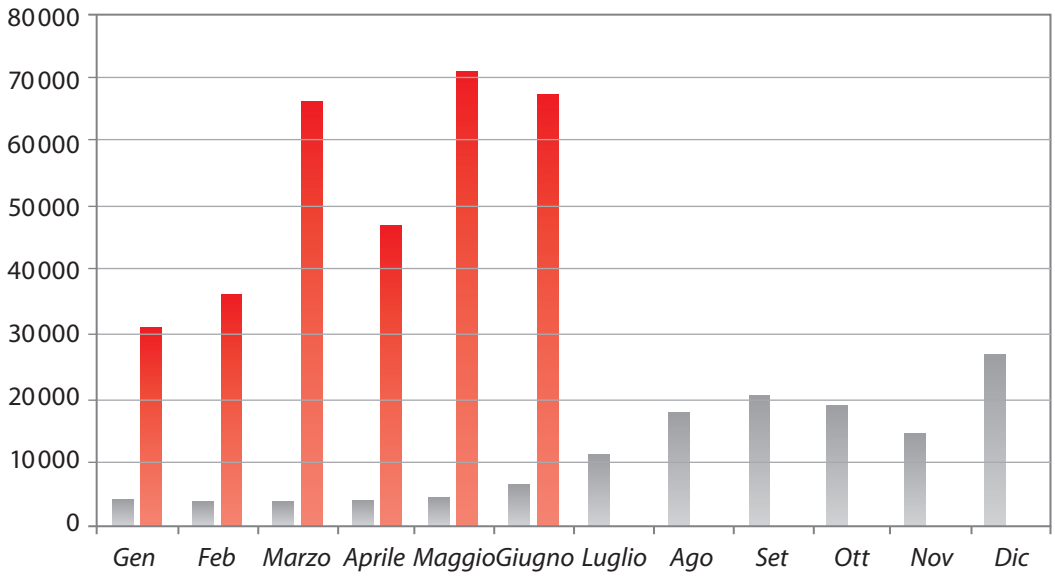


Grafico 1: Confronto - Numero totale di nuovo malware dal 2007 ai primi 6 mesi del 2008

4.2 Virus per smartphone: operazione di marketing o pericolo reale?

Il pericolo, evocato più volte, per i possessori di uno smartphone non è stato individuato da G DATA Security Labs neppure nel primo semestre di quest'anno. Nel caso dei 41 nuovi virus per smartphone si trattava quasi esclusivamente di studi di fattibilità, che servono per sondare le possibilità tecniche, o di software semilegali di monitoraggio, per genitori preoccupati e partner gelosi.

La situazione da anni stagnante di questo tipo di malware ha una spiegazione logica: la diffusione fallisce per vari motivi: esiguo raggio d'azione dei dispositivi Bluetooth, numero insufficiente di smartphone raggiungibili e abilitati per MMS e infine il fatto che sia l'instaurazione di una connessione che l'installazione devono essere confermate dall'utente.

Tuttavia, il fattore determinante e spesso non considerato è il lato economico: la criminalità online è un business su larga scala e quindi soggetta alle leggi di mercato. L'obiettivo principale è trarre i profitti maggiori nel modo più rapido e semplice possibile. Lo sviluppo di malware per smartphone comporta per gli autori costi elevati, non solo in termini finanziari. Un ritorno dell'investimento non è finora realistico per l'industria del malware poiché in altri ambiti si possono ottenere risultati maggiori con meno sforzo.

Mancano dunque da un lato i business model di profitto e dall'altro permane il rischio di essere individuati poiché finora i metodi possibili per guadagnare denaro si sono rivelati rischiosi. Il pericolo così spesso paventato sembra quindi essere soprattutto un'operazione di marketing, e al momento attuale non ha alcun fondamento.

Mese	Numero
Gennaio 2008	6
Febbraio 2008	2
Marzo 2008	9
Aprile 2008	1
Maggio 2008	15
Giugno 2008	8

Tabella 2: Numero di nuovi malware per smartphone

4.3 Il primato spetta alle reti Bot e agli spyware

La suddivisione del malware in base ai diversi tipi è rappresentata nella Tabella 3. In tutte le categorie, ad eccezione dei virus classici, il numero di nuove varianti comparse nel primo semestre del 2008 supera già la quantità dell'intero 2007. I backdoor, con circa 1/4 del nuovo malware, ottengono la prima posizione, nonostante la loro percentuale rispetto al 2007 sia notevolmente diminuita. Essi costituiscono la base delle reti Bot, che rappresentano tuttora gli strumenti più efficaci per i criminali online. Circa 1/5 dei nuovi virus è rappresentato da downloader e dropper.

Queste famiglie di malware vengono utilizzate dagli autori per installare sui computer backdoor e altri virus. Con una percentuale di oltre il 20%, questi virus hanno occupato nei primi sei mesi la seconda posizione tra i nuovi codici nocivi. La percentuale di spyware si è notevolmente ridotta, mantenendo tuttavia la terza posizione.

	# 2008 T1	Percentuale	# 2007	Percentuale 2007	Differenza
Backdoors	75.027	23,6 %	41.477	31,0 %	362 %
Downloader/ Dropper	64.482	20,3 %	28.060	21,0 %	460 %
Spyware	58.872	18,5 %	29.887	22,4 %	394 %
Trojan. Pferde	52.087	16,4 %	13.787	10,3 %	756 %
Adware	32.068	10,1 %	7.654	5,7 %	838 %
Tool	12.203	3,8 %	1.731	1,3 %	1.410 %
Worm	10.227	3,2 %	4.647	3,5 %	440 %
Dialer	4.760	1,5 %		n.a.	
Exploit	1.613	0,5 %		n.a.	
Rootkits	1.425	0,4 %	559	0,4 %	510 %
Virus	327	0,1%	2.127	1,6 %	31 %
Altro	5.170	1,6 %	3.688	2,8 %	280 %
Totale	318.261	100,0 %	133.617	100	476 %

Tabella 3: Numero e percentuali dei nuovi tipi di malware nel primo semestre del 2008 e del 2007 e cambiamento rispetto al 2007

4.4 La crescita esplosiva dell'adware

Già nel 2007 il numero di nuovi adware si è quintuplicato. Ora si registra nuovamente un notevole incremento. All'inizio del 2008 sono stati scoperti nuovi adware per un numero otto volte superiore alla media del 2007. Ad eccezione dei tool, si tratta dell'incremento più duraturo in assoluto. Tra i metodi più amati dall'economia del crimine online vi sono pagine iniziali e file con contenuti probabilmente indesiderati, come banner pubblicitari o risultati di ricerche manipolate.

Il rappresentante più frequente di questo genere è Virtumonde. Il virus si integra come Browser Helper Object in Internet Explorer e in seguito visualizza finestre pop-up pubblicitarie. I clic provocati artificialmente con questo metodo alimentano le casse degli autori di adware.

Adware: WinFixer si presenta come programma antivirus. Dopo l'installazione, dirotta la pagina iniziale del browser e visualizza costantemente finestre pop-up pubblicitarie.

Un altro tipo di pagamento si basa sull'installazione del software. Per ciascuna installazione viene versato un importo di pochi centesimi. Anche in questo caso il fattore importante è la quantità. L'aumento notevole di nuovi malware dimostra che questa attività è remunerativa.

4.5 Ulteriore incremento dello spam

A gennaio la percentuale di spam è calata al 60%, consolidandosi tuttavia in seguito a circa il 70%. Da marzo la percentuale di messaggi di spam è tornata a superare l'80%, con un picco pari al 94% ad aprile e una cifra dell'87% a fine giugno 2008. Gli argomenti più frequenti sono classificati nella tabella seguente:

Argomento	Percentuale
Incremento della potenza sessuale	30 %
Medicinali	22 %
Repliche	21 %
Titolo accademico	5 %
Software	3 %

Tabella 3: 5 principali argomenti dei messaggi di spam nel primo semestre del 2008

Come in precedenza, parte dei messaggi di spam viene inviata attraverso la rete Bot. Nel primo semestre del 2008 la media è stata pari all'85%. Ogni giorno da 5 a 10 milioni di computer zombie partecipano alla spedizione di spam. Ogni giorno vengono trasformati in nuovi zombie da 200.000 a 500.000 computer, con una media di 360.000. La maggior parte di questi computer è ubicata in Germania, Italia e Brasile (vedere la Tabella 4). Quindi quotidianamente vengono inviati circa 130 miliardi di messaggi di spam, phishing o malware.

Paese	Percentuale
Brasile	10,2%
Germania	9,3%
Italia	8,9%
Turchia	8,3 %
Cina	6,6 %

Tabella 4: 5 principali paesi con il maggior numero di PC zombie

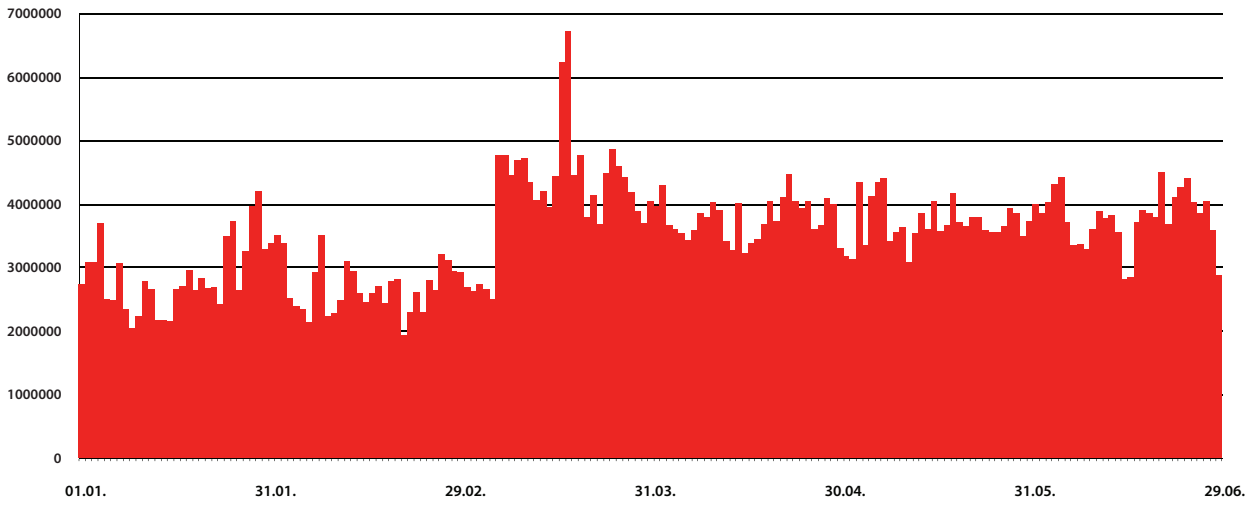
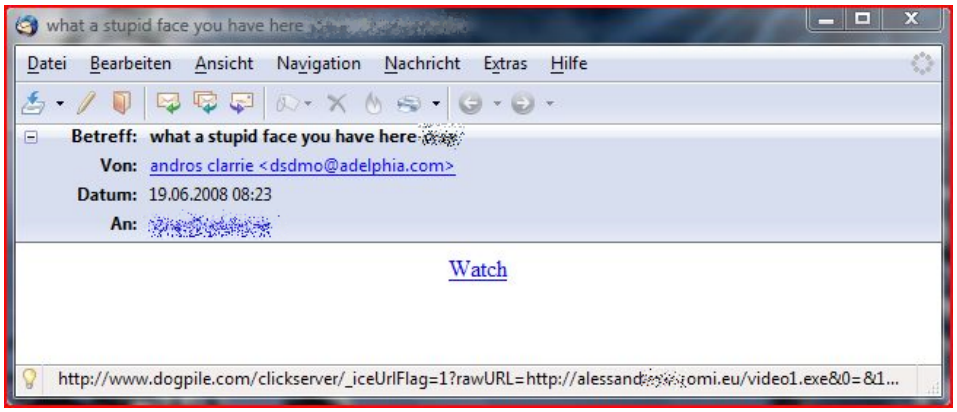


Grafico 2: e-mail di spam nel primo semestre del 2008

Per raggirare i filtri antispam, gli spammer fanno ricorso a pagine conosciute e ritenute affidabili. Sfruttano, ad esempio, le funzioni di reindirizzamento di Google, Yahoo e di altre pagine. In questo modo gli utenti e i filtri antispam credono di avere richiamato una pagina affidabile.



Un principio simile viene applicato anche a immagini e pagine Web che vengono ospitate nei portali preferiti, come Flickr o Blogspot. Così vengono ingannate le tecnologie di riconoscimento, basate sulla reputazione.

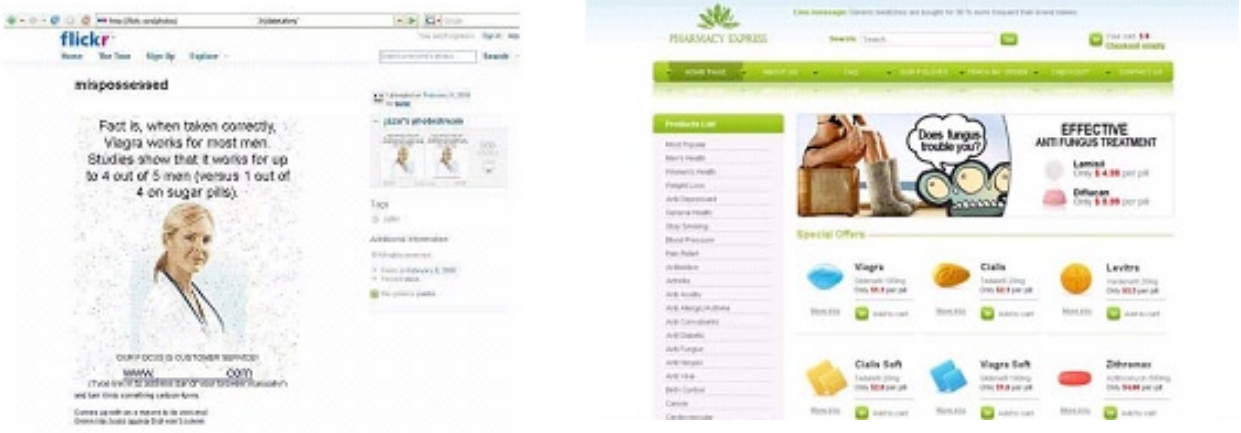


Grafico 3: Immagini e spam ospitati nei portali Flickr e Blogspot

4.6 Giocatori online nel mirino

Osservando le famiglie di virus più attive, riportate nella Tabella 5, saltano all'occhio non soltanto i backdoor Hupigon e Bifrose. Il vecchio e nuovo leader della categoria, il backdoor Hupigon, appartiene a una famiglia di malware molto utilizzata dai runtime packer. Le nuove versioni possono essere raccolte velocemente e in modo efficiente con un clic di un toolkit. Alcune varianti utilizzano contemporaneamente 11 packer diversi.

I cavalli di Troia come OnlineGames e Magania (giochi di GameMania), che rubano i dati di accesso dai giochi online, si sono creati una loro posizione nelle famiglie di malware più attive in assoluto. Ciò significa che, come in passato, i giocatori online sono tuttora nel mirino dei ladri di dati. I dati di accesso per i giochi online, così come i personaggi e gli oggetti dei giochi, vengono considerati come denaro reale in numerosi forum. Ciò attira anche i truffatori della vita reale.

	#2006	Famiglia di virus	#2007	Famiglia di virus
1	32.383	Hupigon	16.983	Hupigon
2	19.415	OnLineGames	8.692	OnLineGames
3	13.922	Virtumonde	3.002	Rbot
4	11.933	Magania	2.973	Banker
5	7.370	FenomenGame	2.848	Banload
6	7.151	Buzus	2.627	Zlob
7	6.779	Zlob	2.533	Virtumonde
8	6.247	Cinmus	1.922	Magania
9	6.194	Banload	1.882	LdPinch
10	5.433	Bifrose	1.751	BZub

Tabella 3: Le 10 famiglie di virus più attive nel 1° semestre del 2008 e del 2007

Le altre posizioni nella Tabella 5 sono occupate dai seguenti virus:

- **Virtumonde:** adware che si integra in IE e visualizza finestre pop-up pubblicitarie.
- **FenomenGame:** rilevamento di errore a causa della creazione automatica di firme
- **Buzus:** spyware-cavallo di Troia e keylogger con backdoor
- **Zlob:** uno dei più amati cavalli di Troia-downloader, in grado di modificare anche le impostazioni in IE e di visualizzare le pagine pornografiche ed installare rogueware
- **Cinmus** è un programma adware che si integra in Internet Explorer e visualizza finestre pop-up pubblicitarie.
- **Banload:** downloader per cavalli di Troia di tipo banking, indirizzati principalmente agli istituti bancari brasiliani e portoghesi

4.7 Codici dannosi su diverse piattaforme - Concentrazione in Windows

Nel primo semestre del 2008 la percentuale di codici dannosi per Windows è aumentata dal 95,2% al 98,2%. Ciò dimostra che gli autori di malware si concentrano principalmente sui computer con sistema operativo Windows. Evidentemente qui si fanno gli affari più lucrosi.

	#2008 H1	Piattaforma	#2007	Piattaforma
1	312.668	Win32	126.854	Win32
2	2.650	JS	2.463	JS
3	845	HTML	1.106	HTML
4	572	VBS	1.007	VBS
5	545	BAT	707	BAT
6	252	MSIL	197	PHP
7	231	SWF	166	MSWord
8	92	MSWord	139	Perl
9	91	PHP	137	Linux
10	33	MSExcel	70	ASP

Tabella 4: 10 piattaforme principali nel primo semestre del 2008 e nell'intero 2007

Gli attacchi basati sul Web in Javascript, HTML, VBSkript, Flash (SWF), PHP e Perl hanno ridotto la loro percentuale dal 2,5% al 1,4%. Tuttavia, calcolando l'intero 2008, questo significa quasi il doppio degli attacchi basati sul Web. Ciò dimostra che, indipendentemente dal malware per Windows che viene creato nelle pagine Web, attualmente vengono effettuati sempre più attacchi mirati a specifiche piattaforme Web. Poiché i meccanismi di protezione contro questi attacchi sono ancora agli albori, non vengono neppure aggiornati di frequente.

Per Linux sono stati scoperti soltanto 21 nuovi virus e non più di 41 per i dispositivi mobili (di cui 20 per Symbian, 19 per J2ME e 2 per Win CE. 2007). Mancano nei primi sei mesi del 2008 i tanto annunciati pericoli per i telefoni cellulari.

5. Previsione per il 2° semestre del 2008

Per le prossime settimane e i mesi a venire, G DATA prevede i seguenti sviluppi:

- **Malware nelle pagine Web:**
  La diffusione di malware tramite le pagine Web non si è affatto esaurita. Gli internauti, da parte loro, dovrebbero provvedere a chiudere determinate falle. Non soltanto il browser dovrebbe essere chiuso ermeticamente, bensì anche tutti i relativi plug-in. Anche da parte dei provider di servizi Internet c'è ancora da fare. Le applicazioni Web contengono numerose falle nella protezione, come Cross-Site Scripting, Cross Site Request Forgery e iniezioni SQL, che vengono sfruttate per infiltrare contenuti estranei nelle pagine Web. Ci vorrà ancora del tempo prima che gli sviluppatori di applicazioni Web adottino seriamente ed implementino le misure di protezione necessarie. Fino ad allora, i visitatori delle pagine Web resteranno esposti a un elevato pericolo di infezione. Solo un programma antivirus che verifica anche i codici dannosi nei dati HTTP è in grado di offrire una protezione affidabile. Ciò vale in particolare per gli utenti che fanno un uso frequente delle offerte Web 2.0 come MySpace, Flickr, Facebook ecc.

- **Business model lucrosi:**
  Spam, furto di dati e adware sono affari multimiliardari a cui i cybercriminali non hanno intenzione di rinunciare, nonostante le conseguenze penali. Il nucleo di queste attività sono attualmente le potenti reti Bot. Perciò, anche nei prossimi mesi, verremo inondati da downloader e backdoor che trasformeranno i PC in zombie di spam.

- **Fiorisce il commercio dei dati.**
  Gli spyware non si limitano a spiare i dati di accesso per i servizi di online banking. Chi viene infettato con un keylogger può perdere completamente la propria identità online.

- **L'adware è uno dei settori in maggior crescita.**
  Mediante i clic carpiti o l'installazione di software pubblicitari si possono guadagnare molti soldi.

- **Nuovi meccanismi di mimetizzazione:**
  Si presume che nei prossimi mesi verrà potenziato l'utilizzo di rootkit e funzioni dannose che si ancorano nel settore di boot o nel record di avvio principale.

- **Occasioni:**
  I prossimi eventi importanti, come le Olimpiadi, verranno sicuramente sfruttati per compiere macchinazioni fraudolente.

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