

German
Data
Security



G Data

Rapporto sui malware

Semestre gennaio/giugno 2009

Ralf Benz Müller e Werner Klier
G Data Security Labs



Go safe. Go safer. G Data.

Rapporto sui malware di G Data Gennaio/giugno 2009

Ralf Benz Müller e Werner Klier

G Data Security Labs



Panoramica

Cifre e dati

- Nel primo semestre del 2009 G Data ha identificato 663.952 nuovi parassiti, il doppio rispetto allo stesso semestre dell'anno precedente. Rispetto al secondo semestre del 2008, vi è un lieve incremento del 15%. Il numero delle famiglie di malware attive è invece diminuito del 7%.
- Le più frequenti categorie di parassiti sono i cavalli di Troia, i downloader e i backdoor. Mentre i cavalli di Troia e i downloader hanno consolidato la loro posizione, la percentuale di backdoor è diminuita. I rootkit si sono ulteriormente rafforzati, il loro numero si è moltiplicato di 8 volte rispetto allo stesso periodo dell'anno scorso.
- I malware con proprie routine di diffusione costituiscono solo il 4,0% dei parassiti per computer.
- Tra i tipi di malware più attivi vi sono i cavalli di Troia, i backdoor e i ladri di account dei giochi online. Ha guadagnato terreno anche la famiglia di worm "Autorun". Rispetto al primo semestre del 2008, il loro numero è aumentato di cinque volte, raggiungendo una quota del 1,6%.
- Il 99,3% di tutti i malware del secondo semestre viene eseguito in Windows. Prosegue quindi la concentrazione sul sistema operativo leader sul mercato.
- I codici dannosi per piattaforme mobili entrano nei Top 5 delle piattaforme. Con 106 parassiti, tuttavia, la loro percentuale resta ancora la più bassa.
- Anche gli utenti di MacOS X sono attaccati dai malware. I nuovi parassiti per MacOSX sono 15. Ad aprile è stata scoperta una prima rete Bot di computer Apple.

Eventi e tendenze

- Sempre più spesso per diffondere spam e malware si utilizzano i social network.
- Conficker si è sviluppato con grande successo. Ha infettato milioni di PC e il 1° aprile, con una nuova routine di update, ha fatto parlare di sé. Dopo di che, il silenzio.

Previsioni

- Un numero crescente di codici dannosi si annida in Internet, con metodi di infezione sempre più perfezionati.
- Nei prossimi mesi, il flusso di malware aumenterà ancora, ma con percentuali di crescita inferiori e con un numero minore di famiglie.
- Gli utenti di MacOSX e Smartphone sono sempre più nel mirino degli autori di malware.

Sommario

Panoramica	2
Cifre e dati	2
Eventi e tendenze	2
Previsioni	2
Malware: cifre e dati	4
Il flusso di malware cresce ancora, ma non così tanto	4
Categorie di malware	4
Parentele tra famiglie	6
Piattaforme	8
Prospettive per il 2009	9
Previsioni	9
Eventi e tendenze del primo semestre 2009	10
Gennaio 2009.....	10
Febbraio 2009.....	11
Marzo 2009	12
Aprile 2009.....	14
Maggio 2009	14
Giugno 2009.....	15

Malware: cifre e dati

Il flusso di malware cresce ancora, ma non così tanto

Negli anni scorsi il numero di parassiti è aumentato costantemente, con percentuali di crescita sempre più elevate e nuovi record raggiunti. Anche nel primo semestre del 2009 il numero di parassiti è aumentato. Con 663.952 parassiti, la cifra è più che raddoppiata rispetto allo stesso semestre dell'anno precedente. Ma come già annunciato nell'ultimo rapporto G Data sul malware, il tasso di crescita si è ridotto. Rispetto al secondo semestre del 2008, l'incremento del numero di parassiti è solo del 15%.

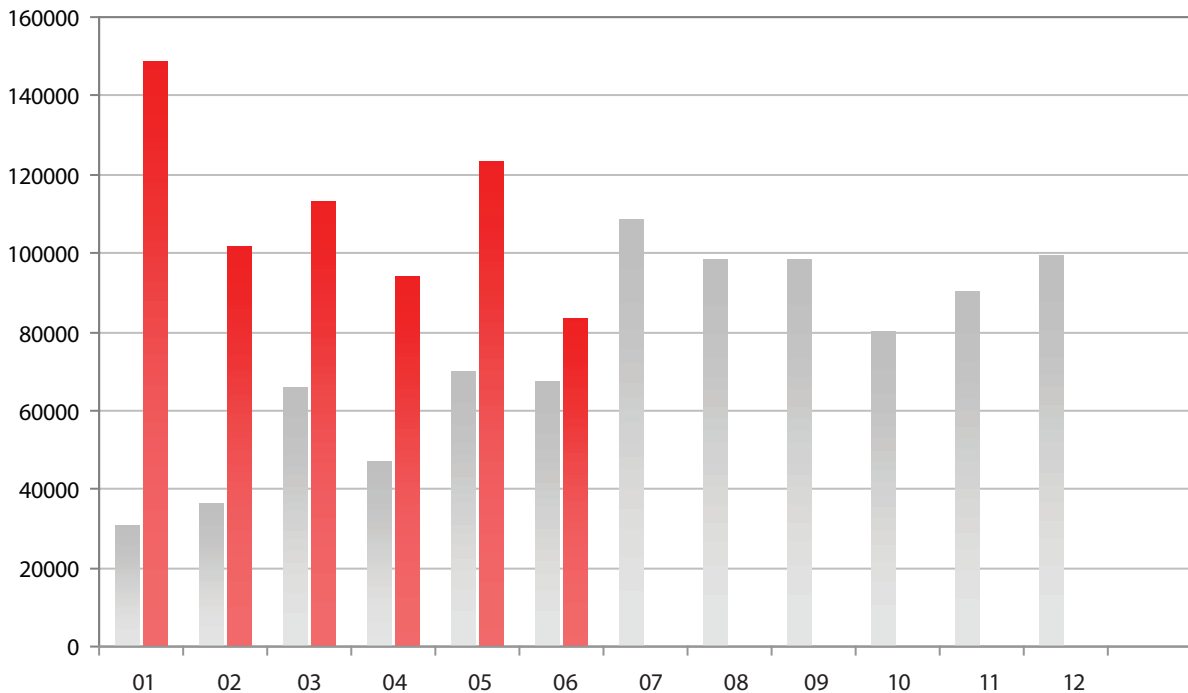


Grafico 1: Numero di nuovi malware al mese nel 2008 (grigio) e 2009 (rosso).

Categorie di malware

Uno sguardo ai cambiamenti subentrati nelle singole categorie di malware può spiegare questa diminuzione. Mentre backdoor, adware e spyware restano sotto la media, la quantità di rootkit e cavalli di Troia supera la crescita media. Anche il numero di downloader e dropper è al di sopra della media.

I backdoor vengono usati per integrare i PC zombie nelle reti Bot e controllarli a distanza. Una flessione in questo ambito indica che l'ampliamento delle reti Bot ha perso d'importanza. Il forte aumento dei rootkit indica che sempre più parassiti (anche backdoor) restano nascosti alla protezione antivirus e agli occhi dei curiosi. Evidentemente le capacità disponibili sono sufficienti a soddisfare la richiesta di attività delle reti Bot, come l'invio di spam e gli attacchi di overload. Anche il mercato degli adware sembra ristagnare. Probabilmente sono state efficaci le campagne di sensibilizzazione. Ma anche i budget pubblicitari limitati dalla crisi economica persistente hanno contribuito a ridurre l'attività economica dei cybercriminali.

Il numero di spyware è leggermente diminuito. Da un'analisi più approfondita, emerge che il numero dei keylogger è raddoppiato, mentre i cavalli di Troia di tipo banking e i ladri di dati per password o giochi online sono calati di ca. il 30%. Non è più così semplice aggirare le misure

di sicurezza adottate da istituti bancari e utenti di giochi online. Nel settore del furto di dati la tendenza è verso parassiti sempre più universali e sempre più potenti.

Categoria	# 2009 S1	Percentuale	# 2008 S2	Percentuale	Diff 2008 S1 2008 S2	# 2008 S1	Percentuale	Diff 2008 S1 2009 S1
Cavalli di Troia	221.610	33,6%	155.167	26,9%	143%	52.087	16,4%	425%
Backdoor	104.224	15,7%	125.086	21,7%	83%	75.027	23,6%	139%
Downloader/Dropper	147.942	22,1%	115.358	20,0%	128%	64.482	20,3%	229%
Spyware	97.011	14,6%	96.081	16,7%	101%	58.872	18,5%	165%
Adware	34.813	5,3%	40.680	7,1%	86%	32.068	10,1%	109%
Worm	26.542	4,0%	17.504	3,0%	152%	10.227	3,2%	260%
Tool	11.413	1,6%	7.727	1,3%	148%	12.203	3,8%	94%
Rootkit	12.229	1,9%	6.959	1,2%	176%	1.425	0,4%	858%
Exploit	2.279	0,3%	1.841	0,3%	124%	1.613	0,5%	141%
Dialer	1.153	0,2%	1013	0,2%	114%	4.760	1,5%	24%
Virus	143	0,0%	167	0,0%	86%	327	0,1%	44%
Altro	4.593	0,7%	8.419	1,5%	55%	5.170	1,6%	89%
Totale	663.952	100,0%	576.002	100,0%	115%	318248	100,0%	209%

Tabella 1: Numero e percentuale di nuove categorie di malware nel primo semestre 2008 e 2009 e cambiamenti

La Tabella 1 mostra anche che il numero dei dialer si è ridotto di circa un quarto rispetto all'anno precedente. Evidentemente il modello di business dei dialer si sta esaurendo. Anche il numero dei virus classici, ossia quelli che infettano i file, si è notevolmente ridotto rispetto allo stesso periodo dell'anno scorso. Questo mezzo di diffusione rappresenta un'eccezione. I worm, e tra questi anche il vasto gruppo di virus Autorun, sono saliti al 4,0%. Il loro numero è aumentato 2,6 volte rispetto al 1° semestre 2008 e di 1,5 volte rispetto al 2° semestre 2008.

Parentele tra famiglie

In base alle funzioni e alle proprietà dei codici utilizzati, i parassiti per computer vengono classificati in famiglie. Da anni il numero delle famiglie di virus è in diminuzione. Nel primo semestre del 2008 erano 2395, nel secondo 2094. Nel primo semestre 2009 sono stati contati 1948 diversi rappresentanti di famiglie di virus. Ciò significa che il nuovo incremento del numero di parassiti si basa sulla diminuzione delle famiglie. Emerge dunque una concentrazione del mercato.

	# 2009 S1	Famiglia di virus	# 2008 S2	Famiglia di virus	# 2008 S1	Famiglia di virus
1	45.407	Monder	45.407	Hupigon	32.383	Hupigon
2	35.361	Hupigon	35.361	OnlineGames	19.415	OnLineGames
3	20.708	Genome	20.708	Monder	13.922	Virtumonde
4	18.718	Buzus	18.718	MonderB	11.933	Magania
5	15.937	OnlineGames	15.937	Cinmus	7.370	FenomenGame
6	13.133	Fraudload	13.133	Buzus	7.151	Buzus
7	13.104	Bifrose	13.104	Magania	6.779	Zlob
8	12.805	Poison	12.805	PcClient	6.247	Cinmus
9	11.530	Magania	11.530	Zlob	6.194	Banload
10	10.412	Inject	10.412	Virtumonde	5.433	Bifrose

Tabella 2: Le 10 famiglie di virus più attive nel primo semestre 2008 e 2009

Mentre alcune famiglie comprendono solo poche varianti, altre risultano particolarmente produttive. Alcune sono nei Top 10 già da anni. Tra queste i backdoor delle famiglie Hupigon e Bifrose, che hanno perso la prima posizione, i ladri di dati per giochi online delle famiglie OnlineGames e Magania e infine i cavalli di Troia della famiglia Buzus. I nuovi leader sono i cavalli di Troia adware/scareware di Monder, che seguono le orme di Virtumonde. Insieme al nuovo arrivato Fraudload, mostrano quanto siano diventati popolari presso i cybercriminali gli scareware, che imitano soluzioni di protezione antivirus. Sono inoltre nuove nei Top 10 le famiglie Genome, Poison ed Inject.

1° posto: Monder

Le innumerevoli varianti di Monder sono cavalli di Troia che manipolano le impostazioni di protezione nel sistema infetto e in questo modo possono rendere il sistema vulnerabile per altri attacchi. La conseguenza può essere un'infezione di adware, che visualizza sul sistema infetto annunci pubblicitari indesiderati, in particolare di falsi programmi di protezione. Alla vittima viene suggerito di cercare le infezioni nel sistema. Per eliminare queste presunte infezioni, l'utente viene sollecitato ad acquistare la "versione completa" e a pagare con carta di credito(!!). Alcune varianti caricano altri software dannosi che comunicano all'aggressore informazioni sul comportamento di navigazione della vittima, all'insaputa dell'utente.

2° posto: Hupigon

I backdoor Hupigon permettono all'aggressore anche il controllo remoto del computer, la registrazione delle immissioni da tastiera, l'accesso al file system e l'attivazione della webcam.

3° posto: Genome

I cavalli di Troia della famiglia Genome riuniscono in sé le funzionalità di downloader, keylogger o cifratura dei file.

4° posto: Buzus

I cavalli di Troia della famiglia Buzus cercano in un sistema infetto i dati personali della vittima (carte di credito, dati per online banking, accessi ad e-mail e FTP), che verranno poi trasmessi all'aggressore. Cercano inoltre di disabilitare le impostazioni di protezione del computer e di rendere quindi il sistema dell'utente ancora più vulnerabile.

5° posto: OnlineGames

I membri della famiglia OnlineGames rubano principalmente i dati di accesso per giochi online, cercando determinati file e voci di registro e/o installando keylogger. In quest'ultimo caso, non vengono rubati soltanto i dati dei giochi. Gli attacchi hanno come obiettivo principale i giochi molto popolari in Asia.

6° posto: Fraudload

La famiglia Fraudload comprende numerose varianti dei cosiddetti programmi scareware, che si presenta-

no all'utente come software di protezione o tool per il sistema. Alla vittima viene suggerito di cercare le infezioni nel sistema. Per eliminare queste presunte infezioni, l'utente viene sollecitato ad acquistare la "versione completa" e a fornire i dati della propria carta di credito in una speciale pagina Web. Di solito l'infezione avviene attraverso falle di sicurezza del sistema operativo o software applicativi vulnerabili dell'utente. Tuttavia, alcuni metodi di aggressione attirano la vittima su pagine che presumibilmente mostrano video con contenuti erotici o di attualità. Per poter visionare tali video, la vittima deve installare uno speciale codec video in cui si nasconde il software nocivo.

7° posto: Bifrose

Il backdoor Bifrose permette agli aggressori di accedere al PC infetto e di collegarsi a un server IRC. Da qui il parassita riceve i comandi dall'aggressore.

8° posto: Poison

Il backdoor Poison permette all'aggressore il controllo remoto non autorizzato sul sistema della vittima, che potrà quindi essere utilizzato ad es. per attacchi DDoS (Distributed Denial of Service).

9° posto: Magania

I cavalli di Troia della famiglia Magania, originaria della Cina, si sono specializzati nel furto di dati degli account per giochi online del produttore di software di Taiwan Gamania. Di solito vengono diffusi per e-mail esemplari di Magania contenenti un archivio RAR compresso e nidificato più volte. Quando si esegue il software dannoso, per deviare l'attenzione dell'utente viene inizialmente visualizzata un'immagine, mentre in background vengono memorizzati altri file nel sistema. Magania si introduce per DLL in Internet Explorer e legge il traffico Web.

10° posto: Inject

La famiglia Inject comprende svariati cavalli di Troia che si introducono nei processi in esecuzione ed assumono il controllo su tali processi, permettendo all'aggressore di manipolarli a piacere per scopi dannosi.

La più attiva **famiglia di worm** è "Autorun", con 9.689 varianti e una percentuale del 1,6%. I rappresentanti di questa famiglia sfruttano il meccanismo che esegue automaticamente i file quando si inserisce un CD/DVD o si collega un supporto dati USB. Il virus copia sé stesso sul supporto dati e crea un file adatto chiamato autorun.inf. Data l'ampia diffusione di questo parassita, è consigliabile disattivare il meccanismo Autorun di Windows. Per garantirne il funzionamento, Microsoft ha creato una propria patch.

Gli **exploit** più diffusi colpiscono le falle di sicurezza nei file WMF e i punti deboli dei PDF. Il numero di PDF nocivi è aumentato notevolmente negli ultimi mesi. Non solo vengono sfruttate le falle nella sicurezza, ma anche la possibilità di eseguire codici JavaScript nei PDF è particolarmente apprezzata dagli autori di malware.

Piattaforme

Anche nel primo semestre del 2009 gli autori di malware si sono concentrati negli attacchi a computer Windows. Con il 99,3%, la percentuale di malware per Windows è di nuovo aumentata. I software dannosi per altri sistemi operativi sono alquanto rari. Per i sistemi basati su Unix sono comparsi 66 parassiti (16 nel secondo semestre 2009) e per Apple OSX 15 nuovi parassiti (nel secondo semestre 2008 erano 6). Anche se si nota una tendenza di crescita del malware per altri sistemi operativi, il loro numero è estremamente basso in confronto alla marea di malware per Windows.

	Piattaforma	# 2009 S1	% 2009 S1	#2008 S2	% 2008 S2	# 2008 S1	Percentuale
1	Win32	659.009	99,3%	571.568	99,2%	312.656	98,2%
2	WebScript	3.301	0,5%	2.961	0,5%	3.849	1,4%
3	Script	924	0,1%	1.062	0,2%	1.155	0,3%
4	MSIL	365	0,1%	318	0,1%	252	0,1%
5	Mobile	106	0,0%	70	0,0%	41	0,0%

Tabella 3: Prime 5 piattaforme nel 2008 e nel primo semestre 2009. WebScript raggruppa i malware basati su JavaScript, HTML, Flash/Shockwave, PHP o ASP che solitamente sfruttano i punti deboli tramite il browser. "Script" 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. In Mobile sono raggruppati i malware per J2ME, Symbian e Windows CE.

Il numero di nuovi malware per Smartphone e computer portatili è aumentato di circa la metà e i parassiti per dispositivi mobili sono entrati nei Top 5. In totale sono apparsi 106 nuovi parassiti. Circa 90 di questi parassiti non hanno una propria routine di diffusione e vengono utilizzati per l'invio di SMS prevalentemente a clienti di telefoni russi e cinesi. Solo la famiglia Yxe si diffonde in modo autonomo via SMS con un link a una pagina Web. Il file, che viene offerto qui per il download, è firmato Symbian. In questo modo l'azione richiesta da parte dell'utente viene ridotta a un clic.

Prospettive per il 2009

Il malware permetterà di guadagnare molto denaro anche nei prossimi mesi. L'economia eCrime è ben consolidata e i modelli di business collaudati per spam, spyware e adware continueranno a riempire le casse di autori, distributori e utilizzatori di malware. Anche i successi occasionali degli enti preposti al controllo non cambieranno la situazione. Anche gli utenti di Windows resteranno nel mirino dei cybercriminali.

Il flusso di malware continuerà a crescere. Si prevede, tuttavia, che il numero crescente verrà ricoperto sempre più spesso da un numero inferiore di famiglie. Le percentuali di crescita non saranno più così evidenti come negli anni precedenti.

Considerando la professionalità di quest'economia nascosta, non stupisce che le falle nella sicurezza dei sistemi operativi e di popolari applicazioni vengano sfruttate dal malware già pochi giorni dopo la loro pubblicazione. In breve tempo si rendono disponibili anche per i dilettanti tool di uso semplice per la creazione di malware. L'anello debole della catena è attualmente il browser e i suoi componenti. Qui viene trovata e sfruttata la maggior parte delle falle di sicurezza. Chi non mantiene il proprio computer sempre aggiornato, offre ai malware un'area vulnerabile più ampia per gli attacchi.

Ma i criminali stanno sperimentando anche su altre piattaforme. Aumenterà il numero di parassiti per computer Apple, Unix e portatili. Tuttavia, non si prevede un'invasione di massa.

Poiché nel frattempo molti punti di accesso per il malware sono protetti dalle tecnologie di sicurezza, gli aggressori ripiegano su ambiti meno protetti. Le maggiori possibilità di successo sono attualmente offerte dalle pagine Web, ricche di applicazioni. Perciò si prevede che quest'area verrà sfruttata anche nei prossimi mesi, con nuovi scenari di attacco sempre più scaltri, utilizzando intensamente alcuni media finora sottovalutati, come Flash o PDF. Aumenteranno anche i trucchi usati dai truffatori per attirare gli utenti Internet su determinate pagine Web o per indurli ad eseguire file. In particolare nei social network si attendono nuove manovre di inganno. Twitter offre in questo contesto le maggiori possibilità.

Previsioni

Categoria	Trend
Cavalli di Troia	↗
Backdoor	→
Downloader/Dropper	→
Spyware	→
Adware	→
Virus/Worm	↘
Tool	↗

Categoria	Trend
Rootkit	↗
Exploit	↗
Win32	↗
WebScript	↑
Script	→
MSIL	→
Mobile	↑

Eventi e tendenze del primo semestre 2009

Illustriamo i più importanti eventi inerenti il malware in sequenza temporale. Risaltano in particolare gli eventi relativi a Conficker, che è balzato alla ribalta nei primi mesi dell'anno. Significativi sono inoltre i molti casi verificatisi nei social network come Twitter, LinkedIn, MySpace e Facebook. Gli ideatori di malware si accorgono di questi trend molto rapidamente e ne sfruttano le opportunità. A parte i singoli casi, ulteriori tendenze indicano che i social network stanno guadagnando interesse. Se l'anno scorso il phishing era quasi esclusivamente limitato a istituti bancari e ad eBay, nell'ultimo semestre Google e i social network Facebook, Sulake e MySpace occupano stabilmente una posizione nei Top 10 come principali serbatoi di phishing. Già da tempo i cybercriminali usano i social network come fonte di informazioni per preparare attacchi mirati e spam personalizzato. I social network piacciono sempre di più, anche agli autori di malware.

Ciò è dimostrato in particolare dallo sviluppo del worm **Koobface**. Come indica il nome stesso, all'inizio era concentrato in Facebook come piattaforma di diffusione e poco dopo in MySpace, ma negli ultimi mesi l'elenco dei social network si è ampliato, includendo hi5.com, friendster.com, myyearbook.com, bebo.com, tagged.com, netlog.com, fubar.com e livejournal.com. I link che vengono creati qui indirizzano a pagine Web in cui viene offerto il collaudato schema del falso antivirus o del download di Codec/Flash. Koobface, tuttavia, è cresciuto anche nel numero, come mostra la tabella seguente. A giugno il numero delle varianti era quasi decuplicato.

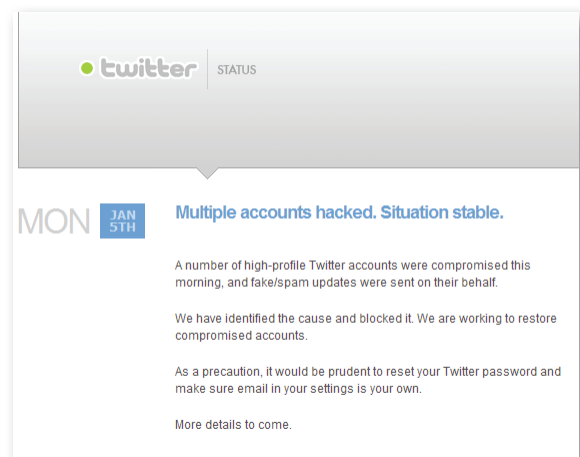
Mese	Gen 09	Feb 09	Mar 09	Apr 09	Mag 09	Giu 09
# Varianti di Koobface	18	14	23	50	56	541

Tabella 4: Numero di varianti di Koobface nel primo semestre 2009

Nei prossimi mesi si prevede un incremento di malware nei social network. Con l'aumento del numero di utenti, cresce anche l'interesse dei diffusori di malware.

Gennaio 2009

- 05.01. Gli utenti del microblog Twitter vengono attirati da brevi messaggi mirati su false pagine di login del servizio per rubare i dati di accesso per future campagne di spam.
- 06.01. **Twitter** avvisa: "Multiple accounts hacked. Situation stable". Sono colpiti tra gli altri anche gli account di Britney Spears e Barack Obama. A nome della vittima, vengono inviati messaggi indecenti.
- 07.01. Nella pagina del social network **LinkedIn** vengono creati falsi profili di vip. Contengono link che indirizzano a falsi programmi antivirus o a una versione di Windows Media Player infettata con un cavallo di Troia. Vittime illustri: Victoria Beckham,



Beyoncé Knowles, Salma Hayek ecc.

- 08.01. 3000 computer del Governo Regionale della Carinzia (Austria) si arrestano in seguito a un attacco del worm **Conficker**. Motivo: un update di protezione pubblicato da Microsoft già nell'ottobre 2008, che doveva impedire a Conficker di sfruttare una falla nella sicurezza, non era ancora stato installato.
- 12.01. In Carinzia **Conficker** colpisce ancora, questa volta negli ospedali della società di gestione ospedaliera KABEG. Di nuovo, vengono colpiti 3000 computer.
- 14.01. Le stime calcolano già 2,5 milioni di infezioni da **Conficker**. Per la prima volta si capisce che Conficker usa un algoritmo speciale per generare nomi di dominio permanenti, tramite i quali si acquisiscono i contatti secondo il principio della casualità. Obiettivo: gli aggressori hanno precedentemente registrato i numerosi domini e posso utilizzarli per caricare altri codici nocivi o fornire ulteriori istruzioni ai PC infetti.
- 21.01. L'epidemia di **Conficker** fa altre vittime: vengono colpiti ampi settori delle Forze Armate Britanniche.
- 23.01. Una copia del software Apple **iWork 09** per layout e presentazioni, infettata da un cavallo di Troia, gira nella rete BitTorrent. Si presume che dall'inizio del mese circa 20.000 utenti abbiano già scaricato questa copia.
- 25.01. La borsa lavoro **Monster.com** comunica di essere stata vittima di un furto di dati. Tramite "accessi non autorizzati" sono stati rubati dal database dell'azienda dati di accesso, nomi, numeri di telefono, indirizzi e-mail e alcuni dati demografici.

Febbraio 2009

- 01.02. A causa di una falla nella sicurezza, la funzione di gestione degli account (UAC) nella versione beta di **Windows 7** viene messa fuori uso da un semplice script, permettendo agli aggressori di introdurre inosservati altri software dannosi.
- 02.02. Alcuni criminali manipolano la pagina Web iniziale dell'**Hamburger Abendblatt** per infettare i visitatori con codici nocivi.
- 04.02. Usando una falsa pagina di login del social network di RTL **wer-kennt-wen.de**, vengono spiati i dati di accesso degli utenti.
- 08.02. Mediante ripetuti attacchi **Denial-of-Service** mirati, vengono temporaneamente bloccate varie pagine Web di sicurezza come Metasploit, Milw0rm e Packetstorm.
- 10.02. Solo due giorni dopo il primo attacco, il sito Internet del progetto **Metasploit** subisce nuovamente il fuoco incrociato di un attacco DDoS. Gli aggressori variano più volte la tecnica di attacco.
- 11.02. Attraverso una falla nella sicurezza del sistema di gestione contenuti **Typo 3**, scoperta solo il giorno prima, vengono manipolate numerose pagine Web in lingua tedesca, in cui non era ancora stato installato l'update di protezione. Vengono colpite, ad es., le pagine Web della famosa squadra di calcio **FC Schalke 04**, in cui si annunciano le dimissioni di Kevin Kuranyi, e il sito Web del Ministro dell'Interno Wolfgang Schäuble, in cui viene inserito un link relativo alla conservazione dei dati.



- 12.02. **Microsoft** offre una **taglia** di 250.000 dollari per l'arresto e la punizione dell'autore del worm **Conficker**. Al tempo stesso annuncia che sta collaborando con ICANN e con i gestori dei server centrali DNS per limitare la crescente infezione.
- 14.02. Centinaia di computer delle Forze Armate Tedesche vengono infettati da **Conficker**.
- 17.02. In seguito a un'errata configurazione del router di un Internet provider in Cechia, viene seriamente compromessa la stabilità della trasmissione dati in alcuni punti della rete Internet globale.
- 23.02. I ricercatori di malware analizzano le varianti B e B++ del worm Conficker e stabiliscono che, grazie alla loro struttura modulare, sono in grado di agire con maggiore flessibilità rispetto alla variante A originale.
- 25.02. Utilizzando alcuni banner Flash appositamente preparati, gli aggressori distribuiscono, tramite le pagine Web della rivista online eWeek e di ulteriori pagine online della rete Ziff-Davis, documenti PDF manipolati che installano un falso programma antivirus sui computer delle vittime.

Marzo 2009

- 01.03. I ricercatori di malware decodificano l'algoritmo utilizzato da **Conficker** per generare nomi di dominio di un server di controllo. Crea inoltre nomi che sono già utilizzati. Durante il mese di marzo i legittimi domini jogli.com (motore di ricerca di musica), wnsux.com (compagnia aerea Southwest Airlines), qhflh.com (rete cinese per donne) e praat.org (analisi audio) vengono disturbati da tentativi di connessione da parte di computer Conficker.

- 04.03. Un team di specialisti del LKA (Ufficio Regionale Investigativo) del Baden-Württemberg neutralizza la piattaforma commerciale illegale **codesoft.cc** nella quale venivano venduti cavalli di Troia e informazioni illegali sul furto di dati e sulla falsificazione di carte di credito.



- 09.03. **Conficker** usa un nuovo algoritmo che, anziché 250 come in passato, ora esamina 50.000 domini al giorno. Sui computer infetti vengono eseguiti alcuni processi che contengono determinate stringhe di caratteri per rilevare gli strumenti di analisi indirizzati espressamente contro il worm. In questo modo il parassita si difende attivamente dalle misure adottate per arginare l'epidemia.
- 12.03. Nell'ambito di alcune ricerche, la britannica **BBC** prende il controllo di una **rete Bot** con circa 22.000 PC. Poiché questa acquisizione scatena commenti negativi contro la BBC, essa comunica che le ricerche erano state condotte nel pubblico interesse ed erano conformi alle norme dell'OFCOM (Autorità di Vigilanza Britannica). La domanda se per l'acquisizione della rete Bot la BBC abbia versato del denaro resta senza risposta.
- 17.03. Nell'ambito di una campagna di phishing e utilizzando il dominio autentico dhl-packstation.info, i cybercriminali attirano gli utenti di **Packstation** su una pagina di login falsificata per spiare i dati di accesso.
- 23.03. I **router DSL** del tipo Netcomm NB5, a causa di un firmware obsoleto, diventano manipolabili da Internet senza password tramite interfaccia Web e accesso SSH e formano una rete Bot chiamata **Psybot**, la cui grandezza è stimata da 80.000 a 100.000 router infetti.
- 30.03. Secondo gli esperti, il 1° aprile **Conficker** comincerà



a perlustrare gli innumerevoli domini generati dal suo algoritmo alla ricerca di update. Cosa accadrà esattamente durante il contatto, nessuno sa prevederlo.

- 31.03. Il vasto interesse suscitato nei media da **Conficker** richiama gli opportunisti, che mediante pagine Web appositamente manipolate in cui si offrono presunti tool di disinfezione, si posizionano nell'elenco dei risultati di Google. In realtà questi tool di disinfezione sono **scareware**, ossia falsi software antivirus, che suggeriscono alla vittima un'infezione del computer per carpirgli i dati della carta di credito.

Aprile 2009

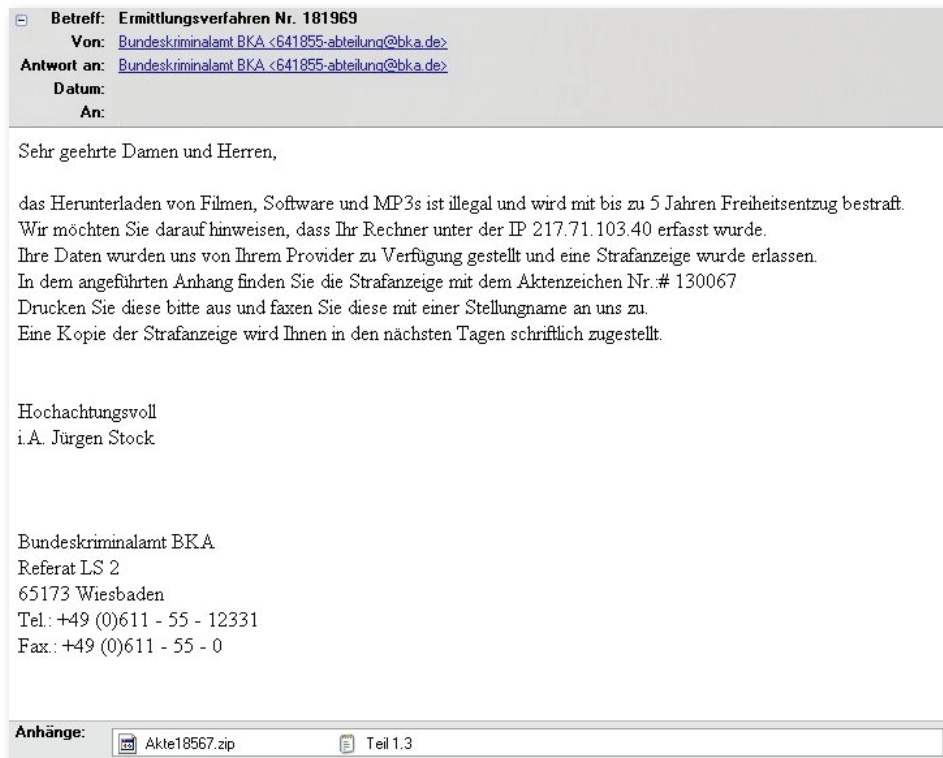
- 01.04. I previsti tentativi di **Conficker** di aggiornarsi cadono nel vuoto. Evidentemente i sistemi infetti prendono contatto con determinati domini. Tuttavia, in quel momento pare non vi siano update disponibili.
- 09.04. Contrariamente alle aspettative, **Conficker** non carica gli aggiornamenti tramite i nomi di dominio generati dall'algoritmo, bensì ricorre a un meccanismo P2P alternativo e comunica direttamente con altri sistemi infetti. La nuova variante blocca in modo mirato l'accesso alle pagine Web di produttori di antivirus per contrastare l'acquisizione di speciali tool di rimozione.
- 12.04. **Conficker** carica da un server ucraino lo scareware "SpywareProtect2009" che emette falsi avvisi di virus sui sistemi delle vittime. Per rimuovere il parassita segnalato (e di fatto mai esistito), l'utente colpito dovrebbe sborsare 49,95 dollari.
- 18.04. Gli esperti in sicurezza scoprono indizi della prima **rete Bot di computer Apple**. Esiste evidentemente una relazione con le versioni di Apple iWork 09 infettate da cavalli di Troia e comparse all'inizio dell'anno nel sito di scambio BitTorrent. Inoltre, pare che giri una versione di Adobe Photoshop CS4 infettata con cavalli di Troia.
- 22.04. Viene scovata la **più grande rete Bot del mondo mai esistita**. Comprende circa due milioni di PC zombie infetti. Si presume che sia controllata da una banda di sole sei persone, le quali gestiscono in Ucraina il server di comando e controllo.
- 23.04. Nella parte russa del World Wide Web fa la sua apparizione un **cavallo di Troia** che blocca all'utente l'accesso al proprio PC e che per sbloccarlo pretende un **riscatto**. Gli utenti colpiti devono inviare un SMS a un numero particolarmente costoso e ricevono in seguito il codice di sblocco.

Maggio 2009

- 07.05. Uno studio condotto dalla società di telecomunicazioni BT scopre che i **dischi rigidi** usati, prima di essere rivenduti, vengono cancellati in maniera insufficiente e potrebbero ancora contenere dati riservati. Acquistando nell'ambito di un test 300 dischi rigidi usati, vengono trovati anche dettagli confidenziali di alcune serie di test per un sistema di difesa antimissile USA e copie cianografiche della società di armamenti Lockheed Martin.
- 08.05. Secondo un rapporto dell'Autorità di controllo dell'aeronautica americana FAA, negli anni scorsi si sono verificate più volte **infiltrazioni di hacker nei sistemi di controllo dell'aeronautica**. L'entità di queste aggressioni varia dall'accesso illegale a circa 50.000 record di dati personali dei dipendenti FAA, fino alla possibilità di interrompere l'alimentazione elettrica ad importanti server.
- 09.05. Alcuni falsi pacchetti di installazione di una presunta versione di prova di **Windows 7**

contengono un **cavallo di Troia** che si attiva durante il setup.

- 24.05. L'**Ufficio Federale Anticrimine** segnala e-mail falsificate inviate a suo nome che richiedono al destinatario di pagare una multa in seguito a una presunta denuncia da parte della polizia per il download illegale di film, software e file MP3.



- 30.05. Un rapporto pubblicato dalla rivista InformationWeek rende noto che gli attivisti turchi hanno più volte **catturato i server Web dell'Esercito USA**. Gli accessi alle pagine Web colpite sono stati deviati su altre pagine Web contenenti slogan politici.

Giugno 2009

- 03.06. Varie decine di migliaia di pagine Web legittime sono vittima di un **attacco di massa**. I visitatori delle pagine Web manipolate vengono indirizzati a un server ucraino in cui vengono distribuiti exploit per Internet Explorer, Firefox e Quicktime.
- 05.06. L'ISP californiano **Pricewert LLC**, che opera anche con gli pseudonimi **3FN** e **APS Telecom**, viene sospeso da Internet dietro sollecitazione dell'Autorità Americana di Sorveglianza del Commercio FTC. Oltre ad ospitare server di comando e controllo per il controllo di oltre 4500 programmi spyware, pare che l'azienda abbia reclutato attivamente criminali e che abbia intenzionalmente ostacolato il rilevamento di contenuti illegali. Al contrario della decisiva chiusura di McColo a novembre 2008, questa azione ha avuto scarse conseguenze sull'invio di spam e malware.
- 09.06. Alcuni sconosciuti penetrano nei sistemi del Web host **VAserv** e manipolano o cancellano i dati di oltre 100.000 pagine Web ospitate.
- 17.06. Circa 2,2 milioni di URL del servizio di abbreviazione URL **cli.gs** vengono manipolati e deviati su un altro sito.
- 24.06. Su ordine del Ministero della Difesa USA, il Pentagono allestisce un **reparto anti-eCrime** che dovrà essere in grado di contrastare gli eventuali effetti bellici nell'ambito della sicurezza globale.



- 25.06. La Procura della Repubblica di Hannover indaga sul gestore della pagina Web **mega-downloads.net** per frode di massa perpetrata ai danni di utenti di computer e nel corso delle indagini congela i conti bancari dell'azienda di quasi un milione di Euro. Secondo le stime delle associazioni dei consumatori, ogni mese ca. 20.000 utenti sono stati frodati con casi di abbonamenti nascosti.

Go safe. Go safer. **G Data.**