



G Data

## Rapporto sui malware

# Rapporto semestrale gennaio-giugno 2010

Ralf Benzmüller e Sabrina Berkenkopf  
G Data SecurityLabs

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

# Sommario

<b>Panoramica .....</b>	<b>3</b>
<b>Malware: Cifre e dati .....</b>	<b>4</b>
Cornucopia di malware.....	4
Categorie di malware .....	5
Famiglie di malware .....	6
Piattaforme: .Net cresce .....	8
<b>Conclusione e tendenze 2010.....</b>	<b>9</b>
Previsioni.....	9
<b>Eventi e tendenze del primo semestre 2010 .....</b>	<b>10</b>
Gennaio 2010 .....	10
Febbraio 2010 .....	11
Marzo 2010.....	13
Aprile 2010 .....	15
Maggio 2010.....	17
Giugno 2010 .....	18

## Panoramica

- Con ben 1.017.208 nuovi malware, anche nel primo semestre del 2010 è stato raggiunto un nuovo record.
- In confronto al semestre precedente il numero è salito del 10 %, rispetto all'anno precedente addirittura quasi del 50 %.
- Secondo le nostre previsioni, nel corso del 2010 saranno riconosciuti oltre 2 milioni di nuovi malware.
- Con una crescita del 51 %, lo spyware costituisce la categoria di malware che ha subito il maggior incremento. Questo vale soprattutto per keylogger e trojan banking.
- Il numero di nuovi adware è calato del 40 %.
- Le due famiglie di malware più produttive, Gerome e Hapigon, hanno generato più varianti rispetto a qualsiasi altro malware all'interno del 2007.
- I malware per Windows continuano a dominare la scena, con una percentuale del 99,4 %. La percentuale di malware .NET è salita di 3,4 volte e corrisponde adesso allo 0,9 %. Anche gli autori di malware sfruttano i vantaggi di .NET.
- Sono stati registrati anche degli aumenti riguardo al codice dannoso per derivati di Unix e Java.

## Tendenze

- Il furto dei dati è e rimane una funzione essenziale del malware.
- L'adware viene ormai sostituito da antivirus contraffatti (FakeAV) e da software ricattatore.
- Sempre più servizi e funzioni online vengono usati a scopi fraudolenti.

## Eventi

- Con le loro numerose innovazioni ma anche alcuni inconvenienti nella gestione dei dati, i social network figurano ai primi posti degli elenchi eventi: Twitter e il leader del settore, Facebook.
- La polizia blocca la botnet Marisposa e arresta i tre gestori.
- Anche la botnet Waledac, una tra le dieci più grandi degli Stati Uniti, è stata duramente colpita dagli investigatori: 277 domini .com sono stati rimossi dalla rete.
- La Deutsche Emissionshandelsstelle è stata vittima di un attacco di phishing gli autori di questo attacco hanno negoziato con diritti pari a circa tre milioni di euro
- I file PDF sono diventati sempre più spesso bersaglio degli autori di malware, in questo modo sono aumentati anche i rapporti riguardanti i punti deboli dei programmi utilizzati per la lettura dei PDF.

# Malware: Cifre e dati

## Cornucopia di malware

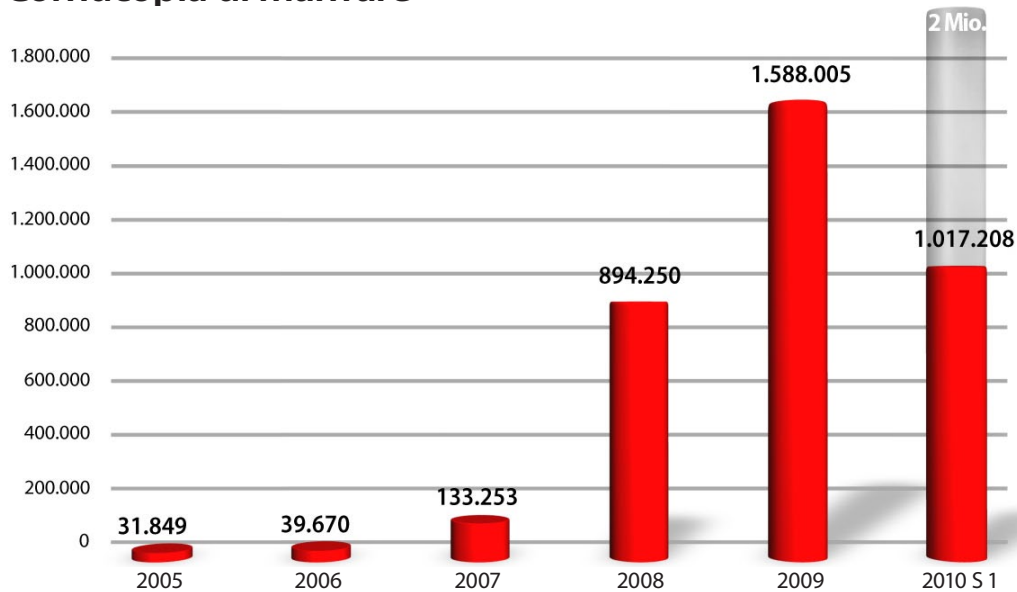


Grafico 1: numero di nuovi malware per anno dal 2005 e nel primo semestre 2010

Con 1.017.208 nuovi malware,<sup>1</sup> anche il primo semestre del 2010 ha superato di circa il 10 % il record rispetto al semestre precedente. In confronto al periodo dell'anno precedente, il numero è salito di oltre il 50 %. Già nel primo semestre del 2010 sono comparsi numerosi nuovi malware rispetto all'intero 2008. Entro la fine dell'anno, si prevede che il numero di nuovi malware superi la soglia dei due milioni.

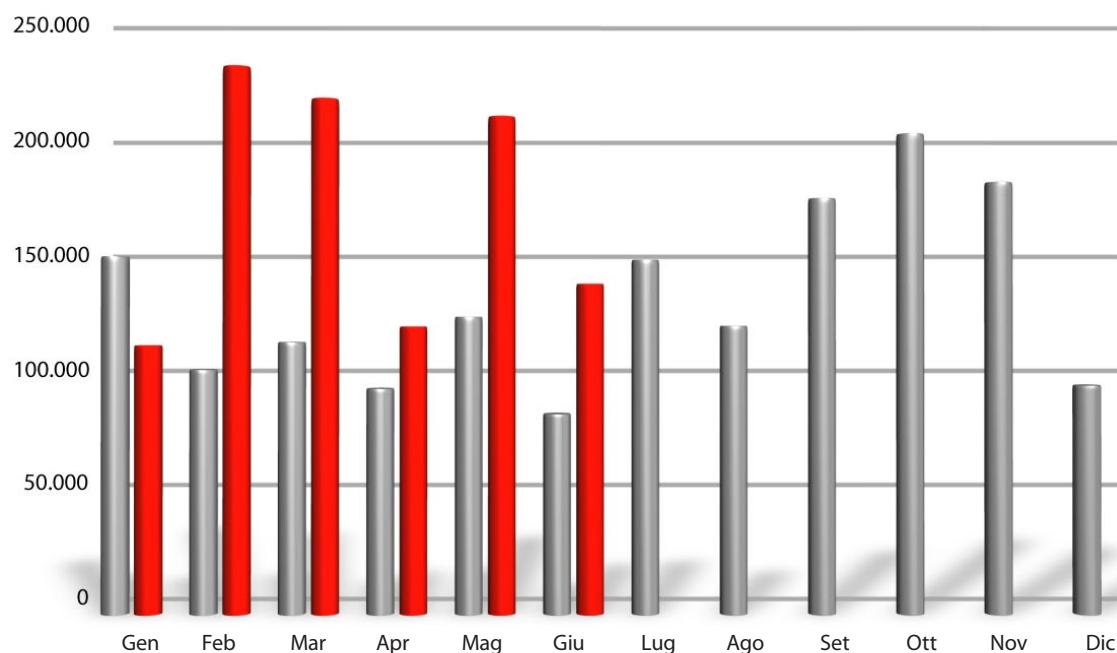


Grafico 2: Numero di nuovi malware per mese per il 2009 e il 2010

<sup>1</sup> Le cifre del presente rapporto derivano dal riconoscimento del malware sulla base dei database antivirus, a seconda delle somiglianze tra i codici dei file dannosi. Numerosi codici dannosi sono simili tra loro e vengono riuniti in famiglie, al cui interno si possono registrare come variazioni del codice le divergenze minori. Fondamentalmente, file diversi tra loro costituiscono famiglie proprie. Il conteggio si basa sui nuovi database dei virus che sono stati creati nel primo semestre del 2010.

## Categorie di malware

Rispetto al secondo semestre del 2009, la percentuale di **spyware** è salita del 3,4 %: nessun'altra categoria è riuscita a raggiungere una simile crescita percentuale. In tal modo, si è arrestata la forte flessione registrata nell'ultimo rapporto sui malware di G Data, anche se non si è tornati alle cifre dello stesso periodo dell'anno precedente. In numeri assoluti, questo equivale a una crescita del 51 %. Tassi di crescita particolarmente elevati nella categoria **spyware** vengono registrati da keylogger<sup>2</sup> e trojan banking<sup>3</sup>.

I **rootkit** continuano a venir impiegati in maniera massiccia. Nell'ultimo semestre il loro numero è aumentato del 2,6 per cento. Invece i worm, vere e proprie "shooting star" dell'ultimo rapporto sui malware di G Data, hanno mantenuto inalterata la loro posizione.

La percentuale dei **trojan** si riafferma al livello elevato del semestre precedente. In questo gruppo, il numero di ransomware (software ricatto e alcuni FakeAV) si è quasi centuplicato rispetto al periodo dell'anno precedente.

La percentuale di nuovi backdoor si è ridotta del 2,9 %, proseguendo così la tendenza al ribasso del primo semestre del 2009. Anche il numero di **tool** si riduce di circa un terzo, la loro percentuale si riduce all'1,0 %. L'aspetto più notevole è la diminuzione del numero di **adware**. Rispetto all'anno precedente (da S1 2009 a S1 2010), il loro numero si riduce del 40 % e la percentuale passa dal 5,3 % al 2,1 %.

Categoria	# 2010 S1	Percentuale	# 2009 S2	Percentuale	Diff. S1 2010 S2 2009	# 2009 S1	Percentuale	Diff. S1 2010 S1 2009
Trojan	433.367	42,6 %	393.421	42,6 %	+10 %	221.610	33,6 %	+96 %
Downloader/Dropper	206.298	20,3 %	187.958	20,3 %	+10 %	147.942	22,1 %	+39 %
Spyware	130.175	12,8 %	86.410	9,4 %	+51 %	97.011	14,6 %	+34 %
Backdoor	122.469	12,0 %	137.484	14,9 %	-11 %	104.224	15,7 %	+18 %
Worm	53.609	5,3 %	51.965	5,6 %	+3 %	26.542	4,0 %	+102 %
Rootkit	31.160	3,1 %	11.720	1,3 %	+166 %	12.229	1,9 %	+155 %
Adware	21.035	2,1 %	30.572	3,3 %	-31 %	34.813	5,3 %	-40 %
Strumenti	9.849	1,0 %	14.516	1,6 %	-32 %	11.413	1,6 %	-14 %
Exploit	2.495	0,2 %	3.412	0,4 %	-27 %	2.279	0,3 %	+9 %
Altro	6.751	0,7 %	5.543	0,5 %	+22 %	4.593	0,7 %	+47 %
<b>Totale</b>	<b>1.017.208</b>	<b>100,0 %</b>	<b>924.053</b>	<b>100,0 %</b>	<b>+10 %</b>	<b>663.952</b>	<b>100,0 %</b>	<b>+53 %</b>

Tabella 1: numero e percentuale di nuove categorie malware 2009 e 2010 e relative modifiche

<sup>2</sup> 2,5 volte superiore rispetto al secondo semestre del 2009

<sup>3</sup> 2,2 volte superiore rispetto al primo semestre del 2009

## Famiglie di malware

In base alle proprie funzioni e caratteristiche, i malware possono essere suddivisi in famiglie. Per alcune di queste vengono create sempre nuove varianti. Mentre nel passato, il numero di nuovi malware è cresciuto in modo costante, il numero delle famiglie invece è in calo. Nel primo semestre del 2010 le famiglie di malware attive erano 2.262: una cifra del 3 % superiore in confronto al valore dell'ultimo semestre e di circa un settimo superiore rispetto a quello del primo semestre del 2009.

	# 2010 S1	Famiglia di virus	# 2009 S2	Famiglia di virus	# 2009 S1	Famiglia di virus
1	116.469	Genome	67.249	Genome	34.829	Monder
2	32.830	Hupigon	38.854	PcClient	26.879	Hupigon
3	30.055	Buzus	37.026	Hupigon	18.576	Genome
4	25.071	Refroso	35.115	Scar	16.719	Buzus
5	24.961	Scar	24.164	Buzus	16.675	OnlineGames
6	21.675	Lipler	20.581	Lipler	13.889	Fraudload
7	19.385	OnlineGames	19.848	Magania	13.104	Bifrose
8	17.542	Palevo	18.645	Refroso	11.106	Inject
9	16.543	Startpage	16.225	Basun	10.312	Magania
10	16.517	Magania	16.271	Sasfis	10.322	Poison

Tabella 2: le 10 famiglie di virus più attive. Numero delle nuove varianti nel 2009 e nel 2010

La tabella 2 illustra le famiglie più produttive dell'ultimo anno e mezzo.

Il leader è ancora **Genome**, la sua percentuale è salita del 73 % (dal S2 2009 al S1 2010). In media, **Genome** diffonde ogni giorno in media 640 nuove varianti. Dal primo semestre del 2010, il numero delle varianti di questa famiglia è di poco inferiore al numero di tutti i malware registrati nel 2007 (cfr. Tabella 1). Il secondo classificato dell'ultimo semestre, **PcClient**, non è riuscito a entrare nella top 10. Alle altre posizioni si ammassano vecchie conoscenze (cfr. Breve descrizione). **OnlineGames** è riuscito a entrare di nuovo nella top 10. Le famiglie di worm **Palevo** e del browser hijacker **Startpage** sono entrate per la prima volta nella Top 10.

### Genome

I Trojan della famiglia "Genome" riuniscono al loro interno le funzionalità di downloader, keylogger e cifratura dei file.

### 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.

### Buzus

I Trojan 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.

## **Refroso**

Questo Trojan è apparso per la prima volta a fine giugno 2009. Possiede funzionalità backdoor ed è in grado di attaccare gli altri computer collegati in rete.

## **Scar**

Questo Trojan carica un file di testo che viene inizializzato con l'ulteriore download di programmi dannosi come downloader, spyware, bot ecc.

## **Lipler**

"Lipler" è una famiglia di downloader che successivamente scarica altri malware da una pagina Web. Modifica inoltre la pagina iniziale del browser.

## **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. La maggioranza degli attacchi ha come obiettivo principale i giochi molto popolari in Asia.

## **Palevo**

Il worm "Palevo" si diffonde tramite supporti dati rimovibili (autorun.inf), copiandosi con nomi accattivanti nelle condivisioni dei programmi di scambio peer-to-peer come Bearshare, Kazaa, Shareaza ecc. Tramite messaggi istantanei (principalmente su MSN), invia anche link che conducono a siti Web dannosi. Inserisce funzioni backdoor in Explorer e cerca determinati server tramite comandi.

## **Startpage**

Questa famiglia di malware modifica la pagina iniziale e spesso anche molte altre impostazioni del browser. Rappresenta la variante più importante dei browser hijacker.

## **Magania**

I Trojan 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.

## Piattaforme: .Net cresce

Come in passato, il grosso dei malware viene scritto per Windows. La percentuale di file eseguibili tra i malware per Windows (Win32) si è ridotta passando al 98,5 %, anche se la percentuale è salita del 9 %. Così prosegue la tendenza segnalata nell'ultimo rapporto sui malware. Ma anche stavolta, la riduzione del numero di malware per Windows viene bilanciata dal numero di malware per la piattaforma .NET, che è aumentato del 3,4 percento. Anche gli autori di codice dannoso sfruttano i vantaggi di .NET, soprattutto perché è in dotazione nei sistemi operativi più recenti. Nel complesso, la percentuale di malware per Windows si attesta a circa il 99,4 %.

Del rimanente 0,6 %, i codici dannosi dei siti Web (ad es. JavaScript, PHP, HTML, ASP ecc.) ne costituiscono circa un terzo (quindi lo 0,4 %). Qui si registra una leggera flessione nel numero di nuove varianti. Tuttavia, le varianti disponibili sono assai diffuse.

	Piattaforma	# 2010 S1	Percentuale	# 2009 S2	Percentuale	Diff. S1 2010 S2 2009	# 2009 S1	Percentuale	Diff. S1 2010 S1 2009
1	Win32	1.001.902	98,5 %	915.197	99,0 %	+9 %	659.009	99,3 %	+52 %
2	MSIL <sup>4</sup>	9.383	0,9 %	2.732	0,3 %	+243 %	365	0,1 %	+2471 %
3	WebScript	3.942	0,4 %	4.371	0,5 %	-10 %	3.301	0,5 %	+19 %
4	Scripts <sup>5</sup>	922	0,1 %	1.124	0,1 %	-18 %	924	0,1 %	-0 %
5	NSIS <sup>6</sup>	260	0,0 %	229	0,0 %	+14 %	48	0,0 %	+442 %
6	*ix <sup>7</sup>	226	0,0 %	37	0,0 %	+511 %	66	0,0 %	+242 %
7	Java	225	0,0 %	31	0,0 %	+626 %	3	0,0 %	+7400 %
8	Mobile	212	0,0 %	120	0,0 %	+77 %	106	0,0 %	+100 %

Tabella 3: prime cinque piattaforme 2009 e 2010.

In questa massa, i malware per altre piattaforme svaniscono. Riteniamo comunque degno di nota informare che il numero di malware per i sistemi operativi basati su Unix si è più che sestuplicato e che il malware per Java è salito di quasi il sette percento (sempre rispetto al secondo semestre del 2009).

4 MSIL è il formato intermedio in cui vengono rappresentate le applicazioni .NET nella propria forma indipendente da piattaforma e linguaggio di programmazione.

5 "Scripts" sono script Batch o Shell o programmi scritti nelle lingue di script VBS, Perl, Python o Ruby.

6 NSIS è una piattaforma di installazione che serve anche per installare MediaPlayer Winamp.

7 \*ix indica tutti i derivati di Unix, come ad es. Linux, FreeBSD, Solaris ecc.

## Conclusioni e tendenze 2010

La marea dei malware non si placa. All'interno della nostra economia, backdoor, spyware ecc. occupano un posto fisso. Gli autori di malware dedicano particolare attenzione allo spyware nei settori keylogging, online banking e giochi online. Il furto dei dati è e rimane una delle funzioni essenziali del malware, la cui commercializzazione è ormai un classico dei forum underground.

Il numero di nuove varianti adware si abbassa notevolmente. Probabilmente ciò è dovuto al fatto che con metodi pubblicitari aggressivi, imitazioni di programmi antivirus (Fake AV) o altri software di protezione e crittografia (Ransomware), è possibile guadagnare più soldi.

Windows rimane l'obiettivo numero 1 degli attacchi. Ma gli autori di malware sono sempre alla costante ricerca di possibili alternative.

### Previsioni

Categoria	Trend
Trojan	→
Backdoor	→
Downloader/Dropper	→
Spyware	→
Adware	↘
Virus/Worm	→
Strumenti	→
Rootkit	↗
Exploit	↘
Win32	↘
WebScript	↗
MSIL	↗
Mobile	↗
*ix	↗

## Eventi del primo semestre 2010

### Gennaio 2010

- 04.01. **Curiosità:** la presenza Web del **presidente di turno spagnolo del consiglio europeo** cambia letteralmente volto: utilizzando un attacco di cross-site scripting, un **hacker** ha sostituito il ritratto del premier spagnolo Zapatero con una foto del personaggio comico Mr. Bean.
- 06.01. **Curiosità:** un 26enne inglese lascia un messaggio di rabbia su **Twitter** e viene arrestato una settimana **dopo**. "You've got a week and a bit to get your s\*\*\* together, otherwise I'm blowing the airport sky high", era la sua minaccia al Robin Hood Airport, perché temeva che il cattivo tempo avrebbe potuto cancellare il suo volo previsto per il 15 gennaio. Per questo tweet, è stato interrogato per quasi sette ore, ha perso il lavoro e gli è stato interdetto a vita l'accesso all'aeroporto di Doncaster. La comunità di Internet ha benevolmente soprannominato Paul Chambers un "**twidiot**". Lo stesso Chambers non riesce a comprendere il motivo di tanto baccano.
- 12.01. L'"**Iranian Cyber Army**" cattura il più grande motore di ricerca cinese **Baidu** utilizzando dei record DNS modificati e lasciando il proprio banner. Nel dicembre 2009, sempre tramite record DNS modificati, erano riusciti a bloccare per alcune ore il servizio di micro blogging Twitter.
- 14.01. I gestori della pagina Internet **opendownload.de** perdono in seconda istanza davanti al tribunale di Mannheim, senza possibilità di ricorso. All'inizio del 2008, un utente aveva ricevuto una **fattura** da opendownload.de, senza che l'obbligo di pagamento "fosse facilmente riconoscibile ed esplicito e che l'utente medio sia chiaramente informato dei costi derivanti", così **si è espresso il tribunale di Mannheim** nella sua sentenza. Rivolgendosi a un avvocato, il cliente si è rifiutato di effettuare il pagamento, richiedendo il risarcimento delle sue spese legali. Già alla fine del 2008, la Verbraucherzentrale Rheinland-Pfalz (centrale dei consumatori della Renania-Palatinato) aveva segnalato i metodi discutibili adottati dal sito.
- 14.01. Un ex amministratore del **sito Web underground DarkMarket** è stato condannato a dieci anni di carcere. Il 33enne di Londra, Renukanth Subramaniam, a sua insaputa aveva gestito il sito Web accanto a un agente sotto copertura dell'**FBI**. La polizia federale statunitense aveva creato la pagina, utilizzandola per eseguire indagini nell'ambiente dei cyber criminali.
- 19.01. Sul blog della pagina Web **netzpolitik.org** viene pubblicata la notizia che un **attacco cyber** ha consentito il furto di dati dell'azienda Ruf-Jugendreisen. Gli autori del crimine sono riusciti a ottenere principalmente i dati dei giovani membri della community dell'organizzatore di viaggi. Secondo netzpolitik.org, l'azienda Ruf aveva ricevuto tre anni prima delle segnalazioni riguardo a dell **falle di sicurezza**, ma apparentemente le aveva ignorate, come riportato il 21.1.
- 21.01. **Microsoft** pubblica una **patch di sicurezza** all'infuori del solito ciclo. La patch di emergenza si è rilevata necessaria a causa della pubblicazione su Internet a inizio settimana del codice **Exploit** che a dicembre 2009 aveva permesso l'attacco a Google e ad altre aziende. La patch risolve nel complesso otto falle di sicurezza.

25.01. I **cyber attacchi ai danni di Google** e di altre aziende, che hanno destato un grandissimo scalpore a inizio gennaio, sono stati sicuramente possibili soprattutto grazie all'utilizzo dei **social network**. Gli esperti hanno ricostruito che gli aggressori sono riusciti a trovare persone che ricoprivano ruoli importanti, le hanno spiate tramite il Web 2.0 e quindi hanno compromesso gli account degli amici della vittima. Camuffati da amici, hanno inviato messaggi con link a pagine Web infette, accedendo così alle reti aziendali. Il gruppo sta pensando di abbandonare l'economia della **Cina** e di chiudere google.cn.



Illustrazione: G Data 2009

29.01. La **Deutsche Emissionshandelsstelle** (DEHSt) si esprime sugli **attacchi di phishing** del giorno precedente: i truffatori hanno inviato e-mail fraudolente camuffandole come provenienti da DEHSt, portando così i destinatari a registrarsi a una pagina Web, per potersi, ironicamente, proteggere da attacchi hacker. Grazie ai dati di accesso rubati, gli autori hanno trasferito i diritti di emissione, soprattutto in Danimarca e Gran Bretagna, guadagnando probabilmente fino a tre miliardi di euro. È chiaro: gli attacchi di phishing mirati possono risultare assai lucrativi.

## Febbraio 2010

02.02. **Password di Twitter** azzerate: i responsabili del sito di microblogging hanno registrato attacchi ai propri utenti, probabilmente eseguiti tramite le pagine dei torrent, dovuti al fatto che gli utenti hanno utilizzato i **medesimi dati di accesso** su più piattaforme, rendendosi in tal modo vulnerabili. Le password di ogni account devono essere diverse. A volte sono sufficienti semplici variazioni di una password di base.

03.02. Le pagine Web di famosi **portali di news online** tedeschi vengono colpiti dal cosiddetto **malvertising**. Golem.de, Handelsblatt.com e Zeit.de hanno inviato tramite banner pubblicitari infetti, codici dannosi agli utenti del proprio sito, tramite banner pubblicitari infetti. Il pericolo di infezione non è più circoscritto al lato più oscuro di Internet. Una protezione antivirus affidabile deve controllare la presenza di codici dannosi all'interno dei contenuti della pagine Web.

03.02. Nel tribunale distrettuale del New Jersey, Edwin Andrew Pena si è dichiarato colpevole di aver guadagnato tra il 2004 e il 2006 circa 1.000.000 di dollari con la **vendita illegale di minuti di Voice over IP**. Pena inviava i pacchetti dati ai server dei fornitori di servizi di telecomunicazione che "protegevano" il proprio server utilizzando solo le **password standard** predefinite.

09.02. Cinque giorni dopo il messaggio sulla presenza di due **componenti aggiuntivi** infetti, **Mozilla** ha dovuto ammettere che uno dei due programmi era stato selezionato erroneamente. Una scansione successiva aveva riconosciuto lo strumento infetto come un **False Positive**.

- 09.02. Uno strumento di rimozione per un Trojan porta una novità sul computer: „**Kill Zeus**” è il nome del programma di "Spy Eye Toolkit". Questo programma pur rimuovendo il "Trojan Zeus" dal computer, contiene parti dannose e procede alla lettura di dati utente e password. **Zeus-Toolkit** gira nei forum underground dalla fine del 2009 e viene venduto per circa 500 dollari.
- 09.02. Uno **scareware olandese** fa la sua comparsa nella rete. Anche se l'interfaccia utente è piena di errori ortografici, nei paesi di lingua non inglese, una versione non inglese viene considerata come un'inequivocabile ampliamento del prodotto. Questo scareware supporta nel complesso **19 lingue**.
- 10.02. Il **governo australiano** viene bloccato da **attacchi DDoS** del gruppo di attivisti "Anonymous". Gli attacchi vengono descritti come un attivismo con motivazioni politiche e vengono giudicati severamente sia dal governo che dagli oppositori della censura. Il motivo di tanta agitazione: l'Australia ha intenzione di applicare la **censura** ad alcuni contenuti online pornografici, gli oppositori temono che venga adottato un filtro inadeguato.

17.02. **Curiosità:** Un gruppo di giovani **olandesi** pubblica la pagina **PleaseRobMe.com**, per richiamare l'attenzione sul pericolo dei messaggi di assenza dalla propria abitazione, che gli utenti lasciano sbadatamente nei social network. Gli utenti dovrebbero riflettere sul fatto che i tweet e i post indicano la propria **residenza** a tutti, non solo agli amici. Così i ladri sanno con certezza quando non ci sarà nessuno a casa e potranno sfruttare l'occasione. Secondo le voci, le assicurazioni dovrebbero considerare un incremento dei premi assicurativi, quando esistono le prove che i clienti utilizzano i servizi di **geolocalizzazione**.



Schermata 1: Fonte: pleaserobme.com

17.02. **Microsoft** dichiara che il **rootkit Alureon** è responsabile dei crash **bluescreen** di numerosi pc Windows XP e alcuni Windows 7. I bluescreen of death (BSOD) si sono moltiplicati in seguito all'aggiornamento di sistema MS10-015 della settimana precedente. Sono interessati i computer che erano stati infettati da Alureon prima dell'aggiornamento.

23.02. **Microsoft** rende noto di aver eseguito un duro e finora singolare colpo ai danni di una delle più grandi botnet degli Stati Uniti, "**Waledac**". Ciò ha consentito di ricevere dal giudice l'autorizzazione a rimuovere dalla rete 277 domini Internet .com dove si supponeva l'esistenza di una connessione alla botnet "Waledac". In tal modo, i **computer bot** infettati avrebbero perso il contatto con i server Command&Control che li gestivano. Si stima che la botnet "Waledac" abbia inviato oltre **1,5 miliardi di messaggi spam** al giorno.



Illustrazione: G Data 2009

## Marzo 2010

- 01.03. I file PDF corrotti rientrano tra gli incidenti della cosiddetta "**Operation Aurora**" contro Google e la notizia assunse rilevanza soprattutto quando centinaia di altre aziende si resero conto che gli attacchi potevano essere eseguiti anche tramite **file PDF infetti**. Su alcuni dei computer esaminati dagli esperti furono trovati documenti PDF dannosi, che sicuramente erano collegati all'attacco. I file presentavano sicure somiglianze di periodo, origine e tipologia rispetto alle tracce finora individuate. In questo contesto, anche il produttore di chip **Intel** rende noto nel suo rapporto finanziario che anch'egli è stato oggetto di un "**sofisticato incidente di sicurezza**", tuttavia non fornisce informazioni sulla portata o sugli effetti.
- 03.03. Le autorità spagnole rendono noto di aver arrestato **tre presunti gestori** della botnet "**Mariposa**" (spagnolo, in italiano = farfalla). Gli spagnoli, di un'età compresa tra i 25 e i 31 anni, si presume che abbiano utilizzato la botnet per rubare dati di carte di credito e di conti online. Secondo le stime, la botnet si estendeva a **oltre 13 milioni di computer** in 190 paesi.
- 06.03. Sono stati **violati** numerosi **account di Twitter** e sono stati usati gli indirizzi e-mail di spam relativi a una cosiddetta dieta. "Check out this diet I tried, it works!" e "I lost 20 lbs in 2 weeks" erano le frasi di richiamo. Ancora non confermata ma concepibile la compromissione degli account tramite **attacchi brute force** (attacchi a dizionario) alle interfacce di Twitter (API).
- 07.03. Un sondaggio di GlobeScan per BBC World Service rivela che quasi **l'80 % della popolazione** considera l'accesso a **Internet un diritto fondamentale**. Ciò che è già regolato dalla legge in paesi come Finlandia ed Estonia, viene auspicato dalla maggioranza dei circa 28.000 intervistati provenienti da 26 paesi, di cui 14.306 degli intervistati sono già utenti di Internet.
- 09.03. **Twitter** avvia una nuova misura di protezione relativa ai link inviati. Tutti i link che vengono inviati a Twitter vengono controllati alla ricerca di possibili effetti dannosi (phishing e altri attacchi) **prima di essere inviati**. In tal modo, dovrebbe essere possibile rilevare una diffusione di link dannosi tramite il servizio di Twitter, così da poterla intercettare e bloccare.
- 10.03. Gli utenti del browser **Internet Explorer 6 e 7** sono presi di mira dagli hacker. Microsoft pubblica un allarme di sicurezza relativo a uno **0 day exploit**. In alcune circostanze, gli aggressori hanno potuto eseguire comandi dannosi sui PC attaccati. Lo stesso Internet Explorer 7 è ancora assai diffuso, gli esperti prevedono, una volta pubblicato il codice di exploit, uno sfruttamento di massa della falla di sicurezza.
- 11.03. Il numero dei server di controllo (Command&Control Server) della **botnet di Zeus** si è di nuovo ristabilito. Negli ultimi due giorni, l'iniziativa svizzera Zeus Tracker ha registrato un'incredibile diminuzione dei numeri dei server C&C (da 249 a 104), riconducendola alla disattivazione temporanea dell'upstream provider Troyak-as. Rispetto a oggi, il **numero dei server** è di nuovo salito a 191.
- 12.03. Il rapporto annuale ufficiale dell'**Internet Crime Complaint Centers** (abbreviato in IC3) registra una crescita dei **messaggi di reclamo**. Nel 2009 sono stati registrati 336.655 episodi, indicando un aumento del 22,3 % rispetto al 2008. La maggioranza delle denunce è stata

effettuata per truffa online legata a danni finanziari, qui la perdita monetaria ammonta a **559,7 milioni di dollari**. IC3 nasce dall'unione di FBI e del National White Collar Crime Center ed è l'ufficio reclami centrale per la criminalità su Internet negli Stati Uniti.

- 16.03. Due **studenti liceali** della città olandese di Heeswijk-Dinther sono stati espulsi dalla scuola perché erano riusciti ad accedere a **19 account di posta elettronica** degli insegnanti, utilizzando i **keylogger**. Hanno rubato documenti d'esame e condiviso le informazioni con i loro amici.
- 19.03. A causa di una **falla di sicurezza critica** nel browser **Firefox 3.6**, il Bürger-CERT, un progetto dell'ufficio federale tedesco per la sicurezza informatica (BSI), ha emanato un avviso di utilizzo, invitando gli utenti a non utilizzare la versione 3.6. Mozilla ha reagito rapidamente rilasciando il 23.03, una patch di sicurezza che chiude la falla **CVE-2010-1028**.
- 22.03. L'operatore di telefonia cellulare Vodafone ammette di aver distribuito quasi 3.000 dispositivi con **schede di memoria infette**. Tre settimane prima, Vodafone aveva comunicato che si trattava solo di un caso singolo isolato: un analista malware aveva infatti scoperto il codice dannoso in seguito all'acquisto di uno **smartphone**. L'incidente sarebbe limitato alla **Spagna**. I clienti presumibilmente colpiti sono stati contattati ed è possibile scaricare gli strumenti per la rimozione del software dannoso. Vale la pena controllare la presenza di virus nei nuovi gadget acquistati.
- 24.03. L'organizzazione **Messaging Anti-Abuse Working Group** (MAAWG) pubblica i risultati di uno studio sui comportamenti di utilizzo relativi all'argomento **sicurezza della posta elettronica**. Lo studio, condotto in America e nell'Europa occidentale, mostra che: il 43 % dei 3.716 intervistati ha aperto messaggi di posta che personalmente classificava come **spam**, l'11 % ha persino selezionato un collegamento in una di queste e-mail. L'8 % degli intervistati stima che non sarà mai vittima di un'infezione bot.
- 26.03. Negli Stati Uniti, **Albert Gonzalez** è stato condannato a 20 anni di carcere. Il 28enne è stato il mandante del sicuramente "più grande e costoso esempio di computer hacking nella storia degli Stati Uniti", così la sentenza del giudice. Gonzales, insieme a due **cospiratori russi**, dovrebbe aver rubato oltre **130 milioni di record di dati di carte di credito e di debito**.
- 29.03. **Didier Stevens**, esperto di sicurezza, utilizza una **funzione del PDF**, che all'apertura di un documento avvia un numero a piacere di programmi. In questo caso non aiuta nemmeno la disattivazione della funzione Java Script. Foxit Reader esegue il codice senza bisogno dell'utente e fino alla pubblicazione di un aggiornamento, Adobe Reader visualizza un messaggio di avviso. Il testo della finestra di avviso interessata può essere tuttavia modificato e si presta al **social engineering**.
- 30.03. Si sta diffondendo un'applicazione antivirus su **Facebook**, ma è un tentativo di truffa, in quanto nel social più famoso non è presente nessuna applicazione di protezione. Dopo l'installazione la **falsa applicazione**,



Schermata 2: "Fake Facebook Antivirus"  
Fonte: SecurityWatch Blog

inserisce 20 amici nell'immagine in modo da attirare anche loro nella trappola.

- 31.03. **Facebook** è di nuovo su tutti i giornali: per errore, il gigante dei social network ha visualizzato **pubblicamente** per circa 30 minuti **tutti gli indirizzi e-mail** dei quasi 400 milioni di utenti. Gli utenti non hanno avuto alcuna possibilità di eliminare l'indirizzo o di nascondere.
- 31.03. Come è stato reso noto oggi, il sito Web dell'**Istituto federale dell'ambiente tedesco** ha diffuso un **trojan Zeus** tra il 19 e il 22.3. Non è ancora ufficialmente noto in che modo sia stata infettata la pagina.

## Aprile 2010

- 01.04. In **Belgio** viene aperto un nuovo **centro esperti sull'argomento cybercrime**. Per questo progetto, l'università di Lovanio collaborerà insieme ad altre istituzioni accademiche, al governo belga, alla Commissione europea e ad altre aziende private. Lo scopo del centro è lo sviluppo di misure di formazione adeguate e la trasmissione della conoscenza.
- 15.04. Dopo che sono stati resi noti i dettagli riguardanti una nuova **falla di sicurezza** all'interno **Java Development Toolkit**, oggi è stato avvistato il Java 0-Day Exploit "in the wild". Tavis Ormandy e Rubèn Santamarta hanno pubblicato informazioni dettagliate riguardo a questa falla di sicurezza. Tuttavia, dopo che erano aumentate le previsioni di **un'ondata di infezione**, la Sun ha recentemente deciso di eseguire un **aggiornamento straordinario**. Da oggi è disponibile per il download la versione 6u20, che chiude la falla.
- 15.04. Tramite il download di un **falso programma hentai** per computer si è diffuso un **malware giapponese**. Questo malware preleva informazioni dai computer infetti e le rende accessibili su una homepage. Secondo i rapporti sulla homepage vengono pubblicati i nomi delle vittime, dei preferiti di IE, della cronologia del browser ecc. L'utente riceve una mail in cui gli viene intimato di versare **1.500 yen**, se vuole che i dati vengano eliminati dalla pagina Web.
- 15.04. La **società ferroviaria olandese**, Nederlandse Spoorwegen, lotta contro gli **skimmer**. Da agosto 2009, la società ha sostituito tutti gli slot per carte delle biglietterie automatiche, dopo che nel 2009 erano state scoperte nel complesso 467 dispositivi di skimming. Finora, nel 2010 non è stato registrato nessun singolo apparecchio estraneo.
- 16.04. Un ex collaboratore della **polizia di Gwent (UK)** ha inviato una scottante **tabella di Excel** con i dati e le informazioni personali del **casellario penale della polizia** di 10.006 persone. A causa della disattenzione dell'addetto e dalla funzione attivata di "compilazione automatica" nel programma di posta, **l'elenco, privo di misure di protezione e di sicurezza**, è finito nelle mani di un giornalista di "The Register". Grazie alla collaborazione della polizia, l'elenco è stato eliminato dal sistema del giornalista evitandone così la pubblicazione.
- 19.04. Viene arrestato l'**hacker olandese "Woopie"**, ovvero il 22enne Kevin de J.. Viene accusato di aver violato i siti Web CrimeClub e ExtremeClub e di aver rubato e pubblicato gli **script** dal database dell'amministratore. Sembra che avesse bloccato queste pagine tramite **attacchi**



Illustrazione: G Data 2009

- DDoS.** La sua pagina Web personale, woopie.nl, è stata confiscata dall'unità speciale della polizia, il Team High Tech Crime. È sicuramente la prima volta che viene sequestrato un sito Web olandese.
- 21.04. Da oggi su **Facebook** è possibile effettuare delle modifiche alle **impostazioni sulla privacy**. La funzione si chiama "**Instant Personalization**" e consente ai gestori di siti Web l'accesso al profilo pubblico degli utenti, in modo da poter personalizzare la pagina Web visualizzata. La funzione "Instant Personalization" è stata creata come cosiddetta **opt-out**, in altre parole viene applicata a ogni utente a meno che questi non la rifiuti. Questa funzione rappresenta un altro passaggio verso un **utente sempre più trasparente** e può essere sfruttata sia per finalità di marketing/pubblicità mirata che utilizzata **dai ladri di identità** per le ricerche.
- 22.04. **Curiosità:** secondo le statistiche di zone-h.org, ad aprile 2010 sono stati violati già quasi **900 domini .be**. Il weblog Belsec ha accennato che il numero delle violazioni è stato **straordinariamente alto** questo mese. Tra i motivi, l'utilizzo di shared hosting, dunque la gestione di più siti Web su un server Web.
- 24.04. Una sorta di Twitter per i tour di shopping online è "**Blippy**". Gli **acquisti** effettuati vengono visualizzati dal network sotto forma di **messaggio breve**, con indicazione del prezzo e descrizione dell'articolo acquistato. Tuttavia, cinque membri del servizio Web 2.0 hanno trovato i **dati della loro carta di credito postati su Google**. Secondo "Blippy" si è trattato di "incidenti isolati", derivanti dalla prima fase di betatesting del servizio.
- 27.04. Da giorni il progetto **Google Street View** è al centro delle critiche in Germania. Nel suo blog ufficiale Google Policy Europe, il provider di servizi Internet Google ha fornito i dettagli sui dati raccolti dalle auto Street View. Sembra che tra i dati WLAN raccolti vi siano anche i SSID e l'indirizzo MAC. Peter Schaar, il responsabile tedesco della tutela della privacy, ha richiesto l'immediata eliminazione dei dati e l'interruzione della raccolta dati futura. Google afferma che non vi sia alcuna raccolta né archiviazione di dati payload e di pacchetti di dati inviati. Queste informazioni verranno rivedute il 14.05.2010.
- 29.04. Uno **skimmer bulgaro** viene condannato a **quattro anni di carcere**, dopo aver commesso skimming a Brügge, Anversa e Bruxelles. È stato condannato per interruzione delle operazioni di banca valide e per associazione all'interno di un'organizzazione **criminale internazionale organizzata**.

## Maggio 2010

- 04.05. Due delle menti presumibilmente alle spalle della **botnet Mariposa**, "Netkairo" e "Ostiator", hanno cercato di ottenere un impiego presso un'azienda spagnola **di software per la sicurezza**. La risposta del capo dell'azienda: "Non so cosa avevate in mente, ma utilizzare Mariposa come biglietto da visita non è veramente un grande aiuto, anzi gioca a vostro sfavore". Nel momento in cui la ditta non si è dimostrata, uno dei due ha minacciato di rivelare le falle di sicurezza del loro software.
- 04.05. Il portale Internet **netzpolitik.org** segnala una nuova violazione dei dati della piattaforma tedesca del Web 2.0 per studenti: **SchülerVZ**. Anche se dopo gli ultimi incidenti verificatisi i gestori del portale VZ avevano investito nella sicurezza dei dati, ricevendo tra l'altro un **marchio di controllo TÜV per la sicurezza dei dati e la funzionalità**, uno studente è riuscito a raccogliere i dati degli oltre **due milioni di studenti**, di cui la maggior parte minorenni. Il suo crawler avrebbe funzionato anche nelle piattaforme MeinVZ e StudiVZ, ma per il programmatore era importante dirigere l'attenzione sulla tutela dei dati dei minorenni. Secondo i propri dati, SchülerVZ aveva a maggio 2010 oltre 5,8 milioni di membri.
- 05.05. Una nuova **falla di sicurezza su Facebook** suscita scalpore: l'**opzione di anteprima** del proprio profilo, disponibile nelle impostazioni della privacy, offre una visione indesiderata delle chat e delle richieste di amicizia della persona selezionata come osservatore dell'anteprima. Facebook reagisce eliminando immediatamente la funzione di chat dalla rete. *Schermata 3: Fonte: Facebook.com*
- 
- 14.05. Le informazioni fornite a fine aprile sulla mole dei **dati WLAN raccolti dai veicoli Google Street View** risultano errate. In un post sul blog, Google ha cambiato tono, indicando che "**sono stati raccolti per errore dei campioni** dei dati di utilizzo dalle reti WiFi aperte (ad es. non rese sicure da password)", scrive Alan Eustace. "Inoltre, considerati i dubbi sorti, abbiamo deciso che la soluzione migliore è quella di interrompere completamente la raccolta dei dati di rete WiFi da parte delle nostre auto Google Street View".
- 17.05. Quasi 200 **soldati delle milizie israeliane** sono stati visibilmente abbindolati dalla **milizia scita libanese** nel social network di Facebook. Camuffati dietro al nome israeliano Reut Zukerman e una foto femminile, i mandanti del profilo si sarebbero procurati con la frode le informazioni insider della milizia. La milizia sarebbe stata già avvertita da circa un anno che le conoscenze su Internet possono risultare rischiose.
- 18.05. L'azienda spagnola UPCnet ha realizzato delle proiezioni: **gli enti pubblici spagnoli** sono esposti ogni anno a circa **5.400 cyber-attacchi**. Le rilevazioni sono state effettuate tramite il programma SIGVI dell'Università tecnica della Catalogna, che nella sola università ha registrato tra i **12 e 15 attacchi al giorno**.
- 19.05. È stato violato uno dei più grandi **forum underground**: „**Carders.cc**“, una piattaforma che principalmente si interessa dell'argomento carte di credito. I presunti aggressori dovrebbero essere gli stessi che a novembre 2009 hanno violato il forum di "**1337 Crew**". Il bottino dell'attuale attacco: un **database con gli indirizzi e-mail, gli indirizzi IP e altro**.

24.05. Aza Raski, un collaboratore di **Mozilla Labs**, pubblica un **Proof-of-Concept** relativo a quello che ha battezzato come "**tabnabbing**". Se la scheda viene lasciata aperta per un certo periodo, la favicon e il contenuto della pagina cambiano aspetto tramite Javascript. La pagina così modificata può rispecchiare una **qualsiasi pagina di accesso a dei servizi online** e far credere all'utente di averla richiamata lui stesso. Quando l'utente inserisce i suoi dati di accesso, l'**attacco di phishing** è andato a buon fine.

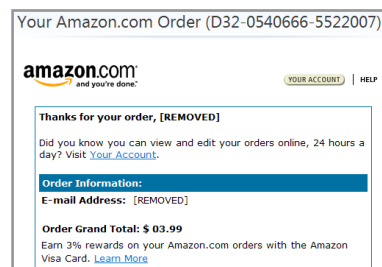
## Giugno 2010

04.06. **Adobe** segnala sul proprio sito Web la presenza di una falla di sicurezza critica (CVE-2010-1297) multiplatforma per Adobe Flash Player 9.0.277.0 e 10.x, Adobe Reader 9 e Acrobat 9 e 8. Tramite dei file flash appositamente preparati, i computer vengono compromessi.

07.06. **Le forze di polizia giapponesi** hanno arrestato due uomini accusati di furto dati ed estorsione. Questi risultano collegati alla diffusione di un **malware** attraverso i **giochi hentai**. Il malware raccoglieva informazioni personali della vittima dai loro computer e le pubblicava su un sito Web. Sembra che i due collaborassero insieme dalle fine del 2009, che abbiano infettato **almeno 5.000** computer, carpando così con la frode oltre **3,8 milioni di yen** (circa 34.000 euro).

10.06. Microsoft segnala sul proprio sito Web la presenza di una **falla di sicurezza nel proprio sito di Supporto tecnico**, che può essere sfruttata in alcune versioni di Windows XP e Windows Server 2003 per la diffusione di **codice dannoso**. Il richiamo di documenti della guida può aprire la porta agli aggressori, che tramite la falla di sicurezza possono avviare programmi sul computer della vittima o scaricarvi del malware.

25.06. Un'ondata di **conferme d'ordine falsificate di Amazon.com e Buy.com** inonda le cassette postali di posta elettronica. Il sito Web incluso nel link contiene un codice dannoso e scarica un **software Fake AV** sul computer della vittima. L'aspetto particolare di questo **scareware**: può leggere le **password** memorizzate in Explorer 6 e visualizzarle.



Schermata 4: "Fake Amazon Order"

28.06. Secondo un sondaggio rappresentativo dell'**Associazione federale tedesca Bitkom**, il 41 per cento dei cittadini federali tedeschi non modifica di propria iniziativa le proprie **password** per i conti bancari online, la posta elettronica ecc. Nella modifica dei dati di accesso, le donne risulterebbero ancora meno attive: il 45 % non li modificano mai, rispetto al 38 % degli uomini. Il motivo più frequente per questa **pigrizia di aggiornamento** sarebbe riconducibile alla paura di dimenticare la password. Una passeggiata per i **ladri di dati**.