



## G DATA - Report 2006 sui malware



Ralf Benzmüller e Thorsten Urbanski

## Sommario

1.1	Diminuzione dei virus classici	3
1.2	Diffusione tramite botnet	3
1.3	Pochi malware per dispositivi mobili	3
1.4	Conclusione	3
2.	Introduzione	4
2.1	Botnet, backdoor e spyware	4
3.	Metodi di diffusione	5
3.1	Mutamento di un'infezione tipica	5
3.2	Sfruttamento delle falle nella sicurezza	5
3.3	Attacchi mirati	5
3.4	Utilizzo di finestre temporali	6
3.5	Infezioni nei collegamenti a Internet	6
4.	Botnet: la spina dorsale dell'economia dei crimini cibernetici	7
4.1	Spam	8
4.2	Adware	9
5.	I dati come l'oro	9
5.1	Ransomware	9
5.2	Phishing	9
5.3	Spyware	10
6.	Previsione per il 2007	11
7.	Tabelle allegate	12
7.1	Quantità di nuovi malware per categoria (2005 e 2006)	12
7.2	Quantità di famiglie di malware (2005 e 2006)	12
7.3	Principali famiglie di malware (2005 e 2006)	12
7.4	Principali famiglie di worm (2005 e 2006)	13

## 1. Riepilogo: trojan e adware / spyware guadagnano terreno

---

Anche nel 2006 G DATA Security ha registrato un evidente aumento nella presenza di malware. Rispetto agli anni precedenti, il 2006 non è stato l'anno dell'esplosione di nuovi virus, sebbene la diffusione di nuovi malware si sia mantenuta a un livello alto nel corso di tutto l'anno. Il tasso di crescita totale dei malware è stato pari al 25 % rispetto al 2005. Se si esprime questo dato in cifre assolute, il 2006 ha visto la diffusione di 39.670 nuovi programmi maligni, ovvero quasi 109 al giorno. Diminuisce tuttavia il numero di famiglie di virus alla base degli attacchi, che passa da 4.343 a 2.223, ovvero la metà.

### 1.1 Diminuzione dei virus classici

---

Anche i virus classici e i macrovirus sono diminuiti nel corso del 2006. I laboratori di G DATA Security registrano in questo caso una diminuzione pari al 24 %. La quantità di worm è rimasta allo stesso livello dell'anno passato.

Ad aumentare in modo evidente sono stati invece i trojan downloader (+ 60 %), gli adware / spyware (+ 43 %) e le backdoor (+ 33 %). Tale sviluppo si spiega nel crescente interesse da parte dei criminali cibernetici nei confronti di ambiti più redditizi, quali furto e commercio tramite dati bancari, dati di carte di credito o affitto di botnet.

### 1.2 Diffusione tramite botnet

---

La diffusione di spam e malware è avvenuta, nel corso del 2006, principalmente attraverso botnet, responsabili dell'invio di ben 80 % di tutto lo spam a livello mondiale. In questo caso, G DATA ha osservato un cambiamento nella tattica di attacco. Al posto dell'invio di e-mail di massa in tutto il mondo, si verificano degli attacchi mirati a intervalli irregolari. Ad esempio, agli utenti di aste online o di forum sul poker.

Anche nel 2006 la maggior parte delle infezioni si è propagata tramite gli allegati e-mail e le applicazioni software peer to peer. La diffusione di malware è stata altresì facilitata dai tempi di reazione spesso lenti di alcuni produttori di software per la sicurezza. Grazie a tempi di reazione inferiori ai trenta minuti, G

DATA Security è in grado di fornire i necessari aggiornamenti delle firme virali e di sbaragliare i principali concorrenti.

La tecnologia OutbreakShield di G DATA consente di ridurre la finestra temporale tra l'identificazione del malware e l'aggiornamento delle firme virali. In questo modo, lo spam infetto viene bloccato già in partenza.

### 1.3 Pochi malware per dispositivi mobili

---

A differenza di quanto riportato da alcuni media, i malware per i dispositivi mobili (ad esempio, PDA e cellulari) non hanno giocato nel 2006 un ruolo degno di nota. I numerosi sistemi operativi su cui si basano i dispositivi mobili, nonché la difficile memorizzazione dei malware, ne hanno infatti reso difficile la diffusione. Ciò significa che il potenziale di minaccia rappresentato dai malware per dispositivi mobili (sono stati creati solo 73 nuovi programmi maligni nel 2006) non è elevato, anche se la situazione potrebbe mutare nel 2007.

### 1.4 Conclusione

---

G DATA prevede che il livello di malware resterà elevato anche nel 2007 e che aumenteranno gli attacchi tramite adware, spyware e phishing, nonché l'impiego di potenti botnet.

Le suite di prodotti di sicurezza che offrono firewall, moduli antispam e protezione da virus acquisiranno sempre maggiore importanza.

Se l'impiego di Microsoft Windows Vista sarà in grado di aumentare la sicurezza degli utenti è ancora un dubbio. Fino ad oggi Microsoft, nonostante i suoi sforzi, non è stata in grado di fornire soluzioni convincenti in ambito di sicurezza.

Un pericolo crescente è rappresentato dallo sfruttamento delle vulnerabilità delle applicazioni desktop e dei siti Web. I programmi antivirus e i firewall continueranno a essere strumenti indispensabili per la protezione.

## 2. Introduzione

In linea di massima il 2006 può essere considerato un anno tranquillo. Solo in alcuni casi isolati, i malware sono riusciti a conquistarsi la prima pagina e non si sono verificati attacchi di grosse proporzioni, come accadde invece due anni fa. Il numero di virus e worm che si propagano autonomamente diminuisce, ma questa quiete nasconde una tempesta. I gruppi organizzati internazionali si muovono di nascosto. I malware sono diventati una vera e propria attività economica, alla quale si dedicano commercianti professionisti e sviluppatori qualificati, allo scopo di aumentare i propri profitti. E poiché l'attenzione pubblica non farebbe altro che ostacolare questa attività, le organizzazioni cercano di rimanere nell'ombra. Allo stesso modo, i danni prodotti dai malware agiscono principalmente in background e non sono riconoscibili dall'utente.

In generale, il numero di nuovi malware continua a crescere e ammonta a circa 39.670 unità, ovvero il 25 % in più rispetto all'anno passato (31.849). Al posto degli invii di e-mail di massa, si verificano attacchi mirati a gruppi definiti. L'aumento più rilevante, pari al 43 %, si registra nell'ambito degli adware / spyware. Anche il numero di backdoor (+ 33 %) e di trojan downloader (+ 60 %) è chiaramente aumentato. Questi dati evidenziano altresì un cambiamento nella modalità lavorativa degli autori di malware.

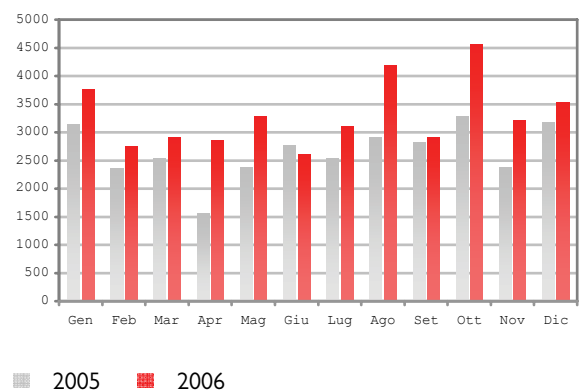
I worm e i virus, che agiscono incontrollati e innescano procedure di diffusione autonome, sono stati rimpiazzati dai trojan downloader che vengono diffusi tramite spam e attraverso botnet a gruppi target prestabiliti. A questo si aggiungono i programmi nocivi che si nascondono nei siti Web.

### 2.1 Botnet, backdoor e spyware

Le botnet rappresentano la spina dorsale di numerose attività nocive. Circa il 60 % delle infezioni sono provocate da backdoor. Il più delle volte, i computer controllati in remoto vengono raggruppati in grosse reti, anche se ultimamente si sta assistendo alla creazione di reti di medie dimensioni. Questi eserciti di zombie, ovvero di computer controllati, vengono utilizzati per diffondere spam, malware, spyware e adware. Ma non è tutto. Gli zombie vengono utilizzati anche per attaccare i siti Web e ricattarne i gestori.

I dati hanno un valore che molti utenti di Internet sottovalutano e che viene riscoperto solo quando tali dati vengono decodificati dai trojan. Per poter riottenere l'accesso ai propri dati è necessario pagare un riscatto, spesso sottoforma di software. Gli indirizzi e-mail, le informazioni relative a carte di credito e conti bancari, i dati di accesso e i profili delle preferenze di Internet rappresentano un commercio ben lucrativo per chi raccoglie dati. Ma spyware e phishing non sono gli unici sistemi utilizzati per procacciare dati e informazioni. Ultimamente, anche i call center e le aziende che elaborano i dati dei clienti sono stati presi di mira da persone che sono in grado di rubare e diffondere le informazioni.

Diagramma 1: confronto tra il numero totale di malware nel 2005 e nel 2006.



### 3. Metodi di diffusione

---

Per quanto riguarda gli utenti dei PC, non è cambiato molto in termini di punti di ingresso dei malware. I principali restano sempre gli allegati e-mail, i programmi instant messaging e i download da applicazioni software peer to peer, quali Kazaa o eMule. Analogamente all'anno passato, il tempo necessario per la creazione di una firma virale viene impiegato per l'identificazione di varianti costantemente nuove. Molto diffusi sono i malware drive-by sui siti Web. Ormai il pericolo non si cela più solo nei collegamenti contenuti nelle e-mail o nei programmi instant messaging.

#### 3.1 Mutamento di un'infezione tipica

---

Nel corso degli ultimi anni, un'infezione tipica ha subito un forte mutamento. Numerosi moduli compatti e specialistici, in grado di caricarsi a richiesta, sono nati sulla base di worm classici e indipendenti, quali NetSky e MyDoom, che da sempre circolano su Internet e che quest'anno sono approdati in numerose caselle di posta elettronica. Una volta assunto il controllo del computer, il modulo avvia un trojan downloader oppure un trojan dropper, che provvede alla corretta ricezione dei file nocivi sul computer e ad avviarli. Una volta eseguito l'avvio, le impostazioni di sicurezza si arrestano e il PC resta in balia del malware. Il passo successivo consiste nel caricare e installare una backdoor sul computer, il quale inizia a lavorare in background senza essere notato. Solo in alcuni casi si rende necessario utilizzare un rootkit a questo scopo. Non a caso, l'aumento del numero di rootkit in questo ambito è relativamente basso. Il computer ha ora un nuovo proprietario, il quale può agire liberamente. Le backdoor consentono, tra le altre cose, di coordinare più computer tra di loro a livello globale attraverso comandi IRC o HTTP che sono stati nel frattempo codificati. In questo modo, il computer entra a far parte di un esercito di zombie che, in alcuni casi, può assumere vaste proporzioni. In seguito all'installazione della backdoor, il sistema infetto può essere ispezionato in ogni sua parte e l'aggressore può scegliere cosa fare con il computer. Se dispone di una buona connessione a Internet, può utilizzare il computer per inviare spam, offrire file illegali da scaricare oppure ospitare phishing di siti Web. I computer che, invece, non dispongono di una

buona connessione vengono ispezionati da spyware alla ricerca di dati riutilizzabili oppure vengono dotati di adware.

#### 3.2 Sfruttamento delle falle nella sicurezza

---

La maggior parte dei malware si presentano sottoforma di file eseguibili oppure si basano su script in Visual Basic o JavaScript. Il 2006 ha assistito non solo a un aumento nel numero di vulnerabilità registrate nel database CVE da 4.813 a oltre 6.600, ma anche a un utilizzo sempre più frequente e immediato di queste vulnerabilità da parte di malware. Così i computer possono essere attaccati e controllati attraverso immagini (WMF, JPF, GIF, PNG e BMP), file audio (RM, MP3 e PLS), filmati (WMV e QT) e documenti (DOC, XLS e PDF). Questa nuova tendenza è particolarmente adatta per sferrare attacchi mirati a singole persone all'interno di grandi aziende.

Non si tratta solo di applicazioni desktop, ma di un numero sempre maggiore di applicazioni Web che, sull'onda del Web 2.0, vengono eseguite senza alcuna installazione. Accade alle volte che la sicurezza non sia presa in considerazione nelle nuove funzioni. Si presuppone che una percentuale tra il 40 % e il 50 % di tutte le applicazioni Web per Cross Site Scripting (XSS) sia vulnerabile. I siti Web nei quali i dati bancari cadono nelle mani dell'aggressore tramite SQL Injection costituiscono una percentuale ancora più elevata. I malware sfruttano queste falle nella sicurezza delle applicazioni Web, quali forum, webshop, blog e wiki. Con la crescita del Web 2.0 aumenta anche la probabilità che programmi maligni riescano ad aprirsi un varco attraverso questa strada. Questo vale soprattutto per piattaforme aperte, quali Second Life, dove gli utenti stessi possono eseguire il codice.

#### 3.3 Attacchi mirati

---

Gli unici malware per l'invio di e-mail di massa che vale la pena menzionare in relazione all'anno 2006 sono Nyxem e Warezov. Sfruttando l'espedito dei contenuti pornografici nell'allegato delle e-mail, Nymex.e ha provocato la prima grande ondata di infezioni del 2006. Questo malware di mass-

mailing è da tempo il primo che elimina i file degli utenti attaccati. Ed è stato proprio sulla base di questa funzione distruttiva che è stato possibile identificarlo rapidamente e annientarlo.

La prima variante di Warezov è comparsa a metà agosto e da allora ogni giorno vengono create nuove varianti. Con oltre 240 varianti, Warezov appartiene alle famiglie di virus più attive. Dopo aver colpito il computer, questo malware si mette alla ricerca degli indirizzi e-mail che sfrutta per autoinviarsi. Attraverso la backdoor integrata viene caricato un ulteriore software responsabile dell'invio di spam.

Oltre a questi tipi di attacchi, che sono di per sé rari e che non passano certo inosservati, questo malware compie una serie innumerevole di piccole aggressioni, che sono limitate a livello temporale o regionale oppure mirate a determinati gruppi di utenti. Accade così che, ad esempio, gli utenti di forum sul poker o di aste online ricevano delle e-mail all'apparenza innocue e persuasive, ma che in realtà contengono allegati infetti. Anche gli utenti di giochi online, quali "World of Warcraft", "Lineage" e "Legends of Mir" dovrebbero stare in guardia. Le famiglie di virus che puntano ai dati di accesso di questi giochi online sono tra le più attive dell'anno.

### **3.4 Utilizzo di finestre temporali**

---

Nel corso degli ultimi anni si è intensificato l'utilizzo di un ben preciso metodo per introdurre i malware nei PC. Questo metodo si basa sul funzionamento stesso dei software antivirus. Per poter individuare un malware, è innanzitutto necessario che il malware stesso sia noto e che sul computer sia disponibile un modello di riconoscimento adeguato, la cosiddetta firma. Senza tale strumento, i malware non possono essere scoperti. Dalla prima comparsa di un malware fino alla creazione di una firma passano, nel migliore dei casi, trenta minuti (ad esempio, con G DATA AntiVirusKit). In media è necessario attendere sette ore e, nel peggiore dei casi, diversi giorni. In tutto questo tempo, il malware può agire liberamente. L'impiego di questa tattica è notevolmente aumentato nel 2006. A fronte di un aumento nel numero di malware, si è invece quasi dimezzata la quantità di famiglie. In generale, il numero di famiglie di malware attive è passato da 4.343 dell'anno scorso a 2.232 di

quest'anno. Tuttavia, è aumentato il numero di varianti rispetto al 2005. In questo ambito, nel 2006 si è assistito a una sorta di "pulizia del mercato". La tendenza a sfruttare le finestre temporali dei programmi antivirus è chiaramente riconducibile alla riduzione.

Questa tendenza si verifica soprattutto nell'ambito degli adware / spyware, dove la concentrazione di famiglie è passata da 1.020 a 210. Una tendenza analoga si registra anche nell'ambito di worm che si diffondono tramite e-mail. A partire da metà agosto sono state generate oltre 240 varianti di Warezov, di cui 27 in un solo giorno. I worm delle famiglie Feebs, Viking, Scano, Bagle e Mytob agiscono analogamente. Un diverso orientamento ha invece caratterizzato le varianti di worm per smartphone, quali Kelvir e Bropia, che non sono aumentate nel 2006.

Lo scorso anno, gli autori di malware hanno sfruttato il tempo che intercorre prima che venga creata la firma virale in modo ancora più intenso, al fine di diffondere le loro creazioni liberamente. Grazie alla tecnologia OutbreakShield, G DATA è stata in grado di mettere un freno a questa tendenza. I malware diffusi come spam vengono bloccati quotidianamente e, in certi casi, già con alcune ore di anticipo rispetto alla comparsa delle prime firme.

### **3.5 Infezioni nei collegamenti a Internet**

---

Poiché gli onnipresenti antivirus individuano ormai immediatamente l'allegato infetto e bloccano l'e-mail, accade sempre più spesso che i malware si introducano nel computer attraverso e-mail prive di allegati. Al loro posto vengono utilizzati i collegamenti a siti Web che consentono di colpire i computer in (almeno) tre modi diversi:

1. Adducendo un pretesto convincente (ad esempio, un aggiornamento Windows), l'utente viene spinto a scaricare direttamente il software nocivo. Anche alcune varianti del trojan "Telekom" (fenomeno prevalentemente riscontrato in Germania, dove il trojan si diffonde tramite e-mail di presunte fatture telefoniche) sono celate nei siti Web. In alcuni siti Web, i programmi maligni vengono celati nei plugin che è necessario scaricare per visualizzare in modo corretto la pagina o il contenuto (perlopiù multimediale). Un esempio

potrebbero essere i filmati di un sito pornografico che possono essere visualizzati solo con uno speciale codec. Invece di scaricare il codec in questione, l'utente esegue il download di un trojan e al posto del filmato vedrà un messaggio di errore sullo schermo.

2. Un metodo di maggiore efficacia è rappresentato dallo sfruttamento delle falle nella sicurezza del browser e dei suoi componenti. I contenuti attivi, quali Java, JavaScript e ActiveX Controls, consentono di accedere ai dati che vengono elaborati nel browser e in alcuni casi addirittura ai file di sistema. Oltre alle falle nella sicurezza del browser e dei suoi componenti, anche le librerie grafiche, i file Flash, RealMedia e QuickTime vengono sfruttati per controllare il computer dell'ignaro visitatore del sito Web.

3. Cross Site Scripting (XSS) sfrutta le vulnerabilità delle applicazioni Web sviluppate male (ad esempio, forum, webshop, blog e wiki), ovvero circa quattro applicazioni Web su dieci. Lo sfruttamento di queste vulnerabilità da parte di malware si è ulteriormente rafforzato con lo sviluppo del Web

2.0. Il problema principale è rappresentato dal fatto che i programmi antivirus classici si attivano solo quando il file viene salvato sul disco rigido. Tuttavia il browser esegue le istruzioni contenute nel file ancor prima di attivarsi. Ciò significa che quando il programma antivirus classico rileva il pericolo è già troppo tardi. Nel riquadro riportato in questa pagina viene illustrato come verificare se il programma

antivirus installato sul proprio computer sia in grado di proteggere dai pericoli celati nei siti Web.

Nel 2006 il numero di siti Web pericolosi è aumentato in modo costante. E-mail e programmi instant messaging non rappresentato più il principale metodo di propagazione di questi malware che, nel frattempo, hanno trovato altri mezzi di diffusione, quali le pagine dei risultati di una ricerca oppure i banner pubblicitari. Anche i siti che ospitano reti sociali e nei quali ciascun utente può pubblicare i propri contenuti vengono utilizzati per diffondere i malware. Ad esempio, un articolo tedesco pubblicato su Wikipedia in merito al virus Blaster collegava i visitatori a uno strumento di rimozione dei malware che, in realtà, era un trojan. Un altro esempio è fornito da myspace.com. Con

l'utilizzo di un crawler è stato possibile raggiungere in breve tempo oltre un milione di utenti. A dicembre, su questo sito sono stati pubblicati dei filmati che, sfruttando una vulnerabilità di QuickTime, possono controllare i computer.

Chi naviga in Internet dovrebbe adottare delle

misure di sicurezza adatte a impedire ai malware di intrufolarsi nel proprio computer. Ad esempio, patch sempre aggiornate e un programma antivirus con le ultime firme virali, in grado di verificare i contenuti dei siti Web prima che vengano aperti dal browser.

Come verificare se un programma antivirus è in grado di fornire una copertura online:

Ecco un semplice metodo per verificare se il programma antivirus in uso è in grado di riconoscere il codice maligno nei siti Web.

1. Aprire il browser.
2. Immettere il seguente URL:  
<http://www.eicar.org/download/eicar.com.txt>
3. Se il browser è in grado di aprire la pagina correttamente e non viene visualizzato alcun messaggio di avviso, il PC in uso non dispone di protezioni sufficienti.

## 4. Botnet: la spina dorsale dell'economia dei criminali cibernetici

Le botnet sono una delle armi principali utilizzate dai criminali cibernetici e forniscono diverse possibilità di guadagno. Innanzitutto per i creatori e gestori delle botnet, i quali traggono guadagno dall'affitto delle reti. In base alle necessità del committente, le botnet possono essere strutturate per portare a termine determinate funzioni, dalle quali i committenti trarranno a loro volta un guadagno. Tali funzioni sono:

### Invio di spam e phishing

Per ulteriori informazioni, consultare la sezione 4.1.

### Negazione del servizio distribuita

Si tratta del cosiddetto DDoS, ovvero Distributed Denial of Service. In questo caso i computer in Internet (perlopiù server Web o server di posta) vengono sommersi da numerose richieste false e/o errate, rendendo

impossibile il funzionamento del computer. Le botnet di medie dimensioni sono in grado di causare un traffico dati talmente elevato da coinvolgere anche i backbone dei provider. Le vittime di questi attacchi non sono unicamente i gestori di popolari webshop o ricevitorie. I gestori dei siti sono costretti al pagamento di un riscatto, che spesso risulta essere la soluzione più semplice. Il più delle volte però il ricatto si trasforma in un "rapporto commerciale" a lungo termine.

#### **Furto di dati**

Le password, i dati di accesso e i codici delle licenze software memorizzati sul computer vengono rubati attraverso trojan ruba-password e keylogger, per poi essere rivenduti in vere e proprie borse online. Sniffer, proxy e redirector vengono impiegati per intercettare i dati nel traffico di una rete.

Quando le botnet non sono sfruttate al massimo, i computer infetti vengono impiegati per la manutenzione della rete. Dopodiché il software bot viene aggiornato e si ricomincia con nuove ondate di spam contenenti malware.

Si stima che il numero di botnet nel mondo si aggiri intorno alle 10.000 unità. In molti casi, i server command-and-control (C&C) basati su IRC sono stati in grado di infiltrarsi nelle botnet e di registrarne la comunicazione. In questo modo, nel 2006 è stato possibile distruggere alcune botnet. La rete più grande era situata in Olanda, dove circa un milione e mezzo di computer erano collegati alla botnet. Negli ultimi tempi si sta assistendo a una suddivisione delle botnet in numerose piccole reti e la comunicazione nei canali C&C viene sempre più spesso codificata. Si stanno sperimentando anche nuove vie per controllare le botnet. Ad esempio, il protocollo HTTP si sta diffondendo come meccanismo di controllo. Sono in corso anche dei tentativi con le strutture peer to peer, le quali tuttavia non sono ancora adatte e vengono implementate solo in casi di emergenza.

### **4.1 Spam**

Quasi tutti gli utenti di Internet conoscono il problema dello spam per esperienza personale. La percentuale di spam registrata a partire dal secondo trimestre del 2006 è stata superiore rispetto ai primi mesi dell'anno e ha continuato ad aumentare in modo costante fino a raggiungere i valori più alti nel periodo

prenatalizio. In generale, la percentuale di spam è quasi raddoppiata dall'inizio dell'anno. L'aumento più evidente è stato registrato negli ultimi tre mesi. Si calcola che nel corso del 2006 ogni utente di Internet abbia ricevuto una media di sei e-mail contenenti spam al giorno.

La percentuale di spam calcolata sul totale delle e-mail si aggira intorno al 50 %, con punte che superano il 90 %. La quantità di spam che un utente può ricevere dipende, tra le altre cose, dal luogo di residenza e dal settore di lavoro. In Giappone, ad esempio, la percentuale di spam è meno della metà rispetto a Israele e Stati Uniti. Le persone che operano in aziende di grandi dimensioni ricevono solo un terzo circa dello spam rispetto ai dipendenti di piccole imprese. Gli enti culturali e le aziende produttive ricevono il 50 % di spam in più rispetto a chi opera nell'ambito dei servizi finanziari ed enti statali.

Più dell'80 % di tutte le e-mail contenenti spam vengono inviate tramite botnet. In tutto il mondo, i computer infetti da backdoor si trasformano in "porte di servizio". Una buona quota di spam viene attualmente prodotta da WarezoV, un malware molto attivo. Grazie alla continua generazione di nuove varianti di questo malware, gli eserciti di zombie che inviano spam crescono giorno dopo giorno, fino a superare il milione di computer attivi.

Tutto ciò è preoccupante. Lo spam è da sempre un affare redditizio. L'invio di milioni di e-mail costa poche centinaia di dollari. Già con una minima percentuale di risposta l'invio è vantaggioso. Sebbene lo spam che ha per oggetto contenuti di tipo pornografico suscita molto scalpore, sono di altra natura le offerte che riescono a ritagliarsi percentuali più elevate, ovvero: prodotti di lusso, offerte finanziarie, benessere e salute.

Le prime e-mail di spam contenenti immagini sono comparse nel 2005. Da allora la loro presenza si è più che triplicata. A novembre la percentuale di spam di questo tipo si aggirava intorno al 45 %. Poiché le dimensioni delle immagini sono maggiori rispetto al testo in esse contenuto, il volume di dati aumenta soprattutto dove vengono elaborate le e-mail. Il flusso di immagini viene sottoposto alla classica procedura di riconoscimento dello spam basata sul testo e con trucchi ingegnosi vengono aggirati anche i procedimenti di analisi delle immagini, di riconoscimento del testo e le

impostazioni orientate al database.

Grazie alla tecnologia OutbreakShield, G DATA Internet Security ha ottenuto nei test di confronto i più alti risultati di riconoscimento con le percentuali più basse di errore. Attualmente, la soluzione offerta da G DATA è l'unica in grado di fornire una protezione dallo spam di questo tipo.

## 4.2 Adware

---

La pubblicità ha da tempo preso piede in Internet. I gestori dei siti Web più popolari si finanziano proprio attraverso la pubblicità. I gestori dei motori di ricerca o dei grandi negozi online non sono gli unici a offrire un interessante esempio di come la pubblicità online possa essere redditizia. Il concetto si basa principalmente sul fatto che la pagina pubblicizzata possa essere aperta con un semplice clic sul relativo banner. Ad ogni clic vengono pagate frazioni di centesimi e quando i clic diventano molti, l'affare diventa redditizio. Questo metodo può tuttavia anche essere sfruttato in modo improprio, la cosiddetta truffa del clic.

I browser hijacker non fanno altro che

modificare la pagina iniziale o la pagina di ricerca di un computer infetto. In questo modo, ogni volta che il browser viene aperto oppure viene effettuata una ricerca, si genera un clic su una pagina web precedentemente stabilita. Poiché questa procedura avviene principalmente nei computer che fanno parte di una botnet, ne consegue che le tasche di chi ha attivato la truffa si riempiranno con estrema rapidità. In modo analogo si comportano anche alcuni strumenti che registrano le preferenze di navigazione in Internet delle vittime ignare e visualizzano dei popup pubblicitari nei punti appropriati. L'autore di questo malware guadagna dei soldi ogni volta che il popup viene visualizzato e ogni volta in cui l'utente fa clic su una pagina pubblicizzata.

L'installazione di programmi che registrano le preferenze di navigazione dell'utente è più aggressiva, ma al contempo più redditizia. Ipotizzando che un'azienda sia disposta a pagare 0,40 \$ per ciascuna installazione, è evidente che i costi per l'utilizzo della botnet saranno presto ammortizzati e le percentuali di guadagno si centuplicheranno rispetto ai costi.

## 5. I dati come l'oro

---

L'attività economica più redditizia è rappresentata al momento dai dati rubati. Molti utenti di Internet non sono consapevoli del valore che possono avere i dati personali. In Internet è nato un intenso commercio di indirizzi e-mail, informazioni relative alle carte di credito, dati dei conti bancari, codici di software e dati di accesso ad aste e giochi online. Il prezzo per le informazioni valide sulle carte di credito è di 50 € oppure 60 € se il PIN è incluso. I dati raggruppati vengono pagati dai 2 \$ ai 5 \$.

### 5.1 Ransomware

---

L'idea di codificare i dati è tornata di attualità. PGPCoder codifica i dati nei documenti di Word, nelle tabelle di Excel, nelle presentazioni di PowerPoint e in qualche altro tipo di file. Per riottenere i propri dati è necessario acquistare uno strumento di decodifica. Le primissime procedure di codifica potevano essere facilmente aggirate. Nel corso dell'anno sono state tuttavia sostituite da procedure sempre più complesse e sicure. L'idea di sequestrare i dati non è nuova. Venne infatti introdotta nel

1989 dal trojan AIDS. Ma era già evidente allora che questo modello non era ben collaudato. Lavorando sulla memoria, i dati possono infatti essere decodificati. Inoltre, vendere uno strumento di decodifica significa stabilire un contatto con la vittima della truffa e, in molti casi, questo contatto è stato utilizzato per rintracciare il malfattore. Il rischio è maggiore dei possibili guadagni.

### 5.2 Phishing

---

Se si potesse assegnare il titolo di malware dell'anno 2006 a una determinata categoria, sarebbe senza dubbio quella del phishing a vincerlo. Il furto di dati e identità ha sperimentato una rapida diffusione nel corso dell'anno. Da due anni ormai il numero di e-mail e di malware di tipo phishing sta aumentando in modo evidente e nel 2006 la quantità è quasi raddoppiata. Un malware su quattro che si propaga tramite e-mail ha a che fare con il phishing. I dati vengono procacciati illecitamente tramite le e-mail di phishing e i relativi siti Web. Per quanto riguarda le banche online tedesche, questo metodo è ormai

inutile. In Germania, infatti, i meccanismi di protezione iTAN e mTAN hanno dato buoni risultati, laddove sono stati impiegati.

Tuttavia i truffatori online non hanno per questo deciso di abbandonare il campo. La maggior parte di furti di dati online avviene in Germania tramite trojan. I keylogger e gli screenlogger vengono impiegati per rubare le password quando vengono immesse. Gli spy trojan ispezionano il disco rigido in determinati punti alla ricerca di informazioni importanti. Sniffer, proxy e redirector fanno in modo che l'aggressore possa intercettare il transito dei dati come MITM (Man In The Middle). Spesso questi strumenti sono così ingegnosi che la vittima si accorge della perdita di preziosi dati solo a conti fatti.

I dati vengono quindi venduti e trasformati in moneta sonante dai compratori stessi tramite acquisti in Internet. Il denaro depredata viene riciclato attraverso ingenui agenti finanziari, che sono caduti nel tranello di una delle allettanti offerte di lavoro. Per una provvigione che si aggira tra il 5 % e il 10 % dell'importo trasferito, gli agenti dovrebbero utilizzare il proprio conto personale per trasferire importi inferiori ai 12.000 € tramite Western Union o MoneyGram su un conto in un paese dell'Europa dell'Est o dell'America del Sud. Questi agenti, i cosiddetti "Money Mules", non sono per niente furbi. Sia le banche, sia i criminali cibernetici chiedono loro dei soldi e dal punto di vista legale vengono accusati di riciclaggio di denaro.

Un altro trucco è il bonifico di importi errati su eBay. Si ipotizza di acquistare all'asta un articolo per un importo di 120 €. "Per errore" viene trasferito un importo di denaro superiore (ad esempio, 1.200 €). Viene quindi richiesto il rimborso del denaro versato in eccesso che, di norma, viene trasferito tramite Western Union su un conto estero. In generale, gli affari che ruotano intorno ai dati rubati sono molto redditizi per i criminali cibernetici.

### 5.3 Spyware

Il software in grado di risalire automaticamente ai dati rappresentano, insieme ai trojan downloader, la categoria che nel corso del 2006 ha subito la più forte spinta all'aumento. Gli spyware ricercano le informazioni di valore in diversi modi.

- I keylogger captano ogni tasto che viene digitato, mentre gli screenlogger catturano degli screenshot ad ogni clic del mouse.
- Gli spy trojan ispezionano le unità alla ricerca di informazioni utilizzabili.
- I browser helper object si inseriscono nel browser e scoprono le preferenze di navigazione delle vittime. Gli sniffer leggono tutte le informazioni della rete.

I dati così ottenuti vengono utilizzati per diversi scopi. I profili di navigazione e degli utenti vengono venduti ad aziende che si occupano di popup pubblicitari. Gli spy trojan possono creare elenchi di indirizzi e-mail che vengono venduti agli spammer. Possono inoltre rubare i codici delle licenze software e vendere i software tramite negozi o aste online. Anche le informazioni relative alle carte di credito e le credenziali di accesso ai conti online sono molto redditizie. Può accadere che gli spy trojan si imbattano in informazioni sensibili di utenti o aziende. Tali informazioni possono essere utilizzate per estorcere denaro. Anche gli utenti di giochi online, quali "World of Warcraft", "Lineage" e "Legends of Mir" devono stare attenti. Le famiglie di virus che puntano ai dati di accesso di questi giochi online sono tra le più attive dell'anno. Gli oggetti più popolari, così come i personaggi laboriosamente creati vengono rivenduti in aste online a cifre da quattro zeri.

Il commercio di dati e informazioni rappresenta un'attività economica redditizia che aumenterà anche nel corso dell'anno prossimo.

## 6. Previsione per il 2007

---

Fare previsioni per il futuro è sempre difficile. Si può tuttavia presupporre che i modelli stabiliti di adware, spyware e phishing, nonché l'abbondante utilizzo delle botnet continueranno anche nell'anno a venire. G DATA prevede un'ulteriore concentrazione del mercato dei malware in ambiti redditizi. Nell'anno passato i malware celati nei siti Web hanno evidentemente costituito un ottimo profitto. Questo tipo di minaccia è ancora sconosciuta agli utenti e rappresenta per questo motivo un elevato potenziale di pericolo.

I criminali cibernetici sono molto creativi nello sviluppo di nuove idee per fare affari. Indipendentemente dalle strutture già stabilite, G DATA prevede per l'anno prossimo un aumento del codice nocivo nei siti Web. Anche le vulnerabilità presenti nelle applicazioni desktop (exploit) e nelle applicazioni Web del Web 2.0 (Cross Site Scripting) verranno

sfruttate.

Le truffe sistematiche sono possibili anche attraverso i dispositivi mobili. Al momento attuale il rischio per gli utenti è tuttavia limitato.

Il nuovo sistema operativo Microsoft Windows Vista potrebbe segnare un punto a favore della protezione dei computer. Questo sistema operativo è infatti stato concepito con una serie di funzioni di protezione. Se l'impiego di Microsoft Windows Vista sarà in grado di aumentare la sicurezza degli utenti è ancora un dubbio. Fino ad oggi Microsoft, nonostante i suoi sforzi, non è stata in grado di fornire soluzioni convincenti in ambito di sicurezza. Per questo motivo, in seguito all'introduzione sul mercato del nuovo sistema operativo, G DATA prevede solo un breve periodo di adattamento, ma nessun cambiamento a lungo termine. I programmi antivirus e i firewall continueranno a fare parte degli strumenti da cui nessun computer potrà prescindere.

## 7. Tabelle allegate

### 7.1 Quantità di nuovi malware per categoria (2005 e 2006)

Mese	Virus		Worm		Backdoor		Adware/Spyware		Trojan		Altro	
Gennaio	197	33	326	166	393	868	1.375	1.387	690	742	160	546
Febbraio	83	24	130	148	417	697	1.112	1.172	511	544	104	130
Marzo	44	26	139	120	431	724	1.102	1.322	658	539	159	149
Aprile	30	201	105	162	282	652	572	1.118	458	583	105	126
Maggio	36	36	125	147	441	802	860	1.457	620	603	296	212
Giugno	46	45	147	108	515	582	1.152	1.163	608	519	231	185
Luglio	48	47	123	95	467	696	1.137	1.554	557	540	201	150
Agosto	37	17	136	113	561	866	1.306	2.267	621	760	238	145
Settembre	156	21	144	124	607	551	1.112	1.547	583	537	191	117
Ottobre	23	36	132	226	802	603	1.376	3.068	680	506	250	105
Novembre	28	30	97	187	552	560	1.110	1.651	476	635	108	104
Dicembre	30	28	127	155	793	720	1.372	1.754	642	615	183	163
<b>Totale</b>	<b>758</b>	<b>544</b>	<b>1.731</b>	<b>1.751</b>	<b>6.261</b>	<b>8.321</b>	<b>13.586</b>	<b>19.460</b>	<b>7.104</b>	<b>7.141</b>	<b>2.226</b>	<b>2132</b>

■ 2005 ■ 2006

### 7.2 Quantità di famiglie di malware (2005 e 2006)

Tipo	2005	2006
Adware/Spyware	1020	210
Backdoor	755	385
Worm	406	242
	163 (e-mail)	105 (e-mail)
Trojan	888	615
<b>Totale</b>	<b>4343</b>	<b>2223</b>

### 7.3 Principali famiglie di malware (2005 e 2006)

Posizione	2005	Quantità	Categoria	2006	Quantità	Categoria
1	Spybot	1835	Backdoor	Hupigon	2249	Backdoor
2	SDbot	1610	Backdoor	Banload	1370	Downloader
3	Agobot	1382	Backdoor	Nilage	1317	Password Spy
4	Banker	874	Phishing	Zlob	1301	Downloader
5	Hupigon	611	Backdoor	Banker	1095	Phishing
6	Legendmir	501	Password Spy	Ld pinch	756	Password Spy
7	Ld pinch	498	Password Spy	Rbot	688	Backdoor
8	Lineage	479	Password Spy	Lineage	558	Password Spy
9	Lmir	470	Password Spy	QQhelper	462	
10	Rbot	450	Backdoor	Bifrose	459	

## 7.4 Principali famiglie di worm (2005 e 2006)

---

Posizione	2005	Quantità	2006	Quantità
1	Kelvir	135	Feebs	256
2	Mytob	118	Warezov	242
3	Bagle	101	Viking	80
4	Bropia	55	Scano	65
5	Silly	47	Bagle	40