G DATA

Malware-Rapporto 2007

Ralf Benzmüller & Thorsten Urbanski

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

G DATA Malware-Rapporto 2007

Ralf Benzmüller & Thorsten Urbanski

1. Introduzione

Nella previsione del rapporto dell'anno scorso abbiamo scritto *„il collaudato business model nell'ambito di Adware, Spyware , Phishing e il largo uso di reti "Bot" continuerà anche nell'anno a venire"*. Questa previsione, per la verità neanche troppo ardita, è stata purtroppo, a danno di molti utenti di computer, confermata. È stato anche confermato l'*„incremento di codice nocivo su siti web "* e il pericolo limitato per gli utenti della telefonia cellulare.

Gli autori di malware nel corso del 2007 ci hanno tenuto in grande agitazione. Complessivamente il numero di nuovo malware è salito al valore record di 133.253 nuovi parassiti. Questo è un aumento di oltre il triplo (338,6%). La percentuale maggiore di crescita è stata registrata nell'ambito degli Adware (570%), Virus (507%), Backdoors (499%) e Spyware (336%).

Tuttavia, se vogliamo dedicare il 2007 ad un gruppo di parassiti, possiamo dedicarlo ai trojan di spionaggio e furto di dati. Si comportano in modo così deciso e rubano nel frattempo molto di più che un semplice accesso a banche dati online. Anche alcuni degli avvenimenti più importanti dell'anno si sono svolti intorno al tema del furto di dati.

2. Avvenimenti importanti 2007

Il furto di dati e reti “Bot” ha occupato i titoli dei giornali nel 2007. Riteniamo degni di nota i seguenti avvenimenti e sviluppi.

2.1 Lo „Storm worm“[1]

In gennaio furono inviate grandi quantità di email che si riferivano all’uragano Cirillo che proprio in quel periodo stava perdendo intensità dopo avere distrutto ampie regioni in Europa. Il cavallo di Troia contenuto nell’allegato infettava il PC rendendolo uno zombie di una rete “Bot”. In precedenza, dalla stessa sorgente venivano promessi videoclip dell’esecuzione di Saddam Hussein o immagini dell’imminente guerra nucleare. A ondate successive i messaggi venivano collegati ad altre notizie. Successivamente, tra le altre cose, i clienti di IKEA, Quelle ed eBay ricevettero fatture false. Nel corso dell’anno sono state utilizzate anche cartoline di auguri, giochi e software depositati su pagine web. In questo modo è stato possibile integrare milioni di calcolatori nella rete “Bot” Storm - la più grande rete “Bot” mai creata. Questa rete viene principalmente utilizzata per l’invio di spam azionario e attacchi Distributed Denial of Service (DDoS).

2.2 Furti di dati

In gennaio, tramite mail di phishing personalizzate, ai clienti della banca svedese Bank Nordea fu offerto il download gratuito di uno strumento Anti-Spam. Purtroppo, lo strumento serviva a ottenere i dati di accesso dei clienti della banca. In precedenza erano state rubate le informazioni relative ai clienti. Queste informazioni erano poi state utilizzate per attaccare i clienti in modo mirato. Il successo dette ragione agli autori. I dati di accesso rubati fruttarono un bottino di ca. 900.000 EUR.

Sono stati resi noti altri casi di furto di dati:

- Tramite attacchi mirati sulla WLAN della TJX furono rubate le informazioni relative a oltre 45 milioni di carte di credito
- In febbraio le password e gli indirizzi e-mail degli utenti del portale per studenti StudiVZ furono rubati e successivamente tutte le password furono modificate.
- Tramite cavalli di Troia fu rubata una serie 1,6 milioni di dati di utenti, in gran parte americani, della borsa lavoro Monster.com.
- Grazie a questo e ad altri furti simili, milioni di dati con informazioni personali sono caduti nelle mani di criminali.

1 Lo Storm worm è, da un punto di vista tecnico, un cavallo di Troia. Il termine risultante „Storm trojan“, è tuttavia meno esaltante e non è completamente corretto.

2.3 Guerra fredda su Internet

Il trasloco di un monumento di guerra russo nella capitale estone Tallin provocò violenti manifestazioni da parte della popolazione russa. Mentre le manifestazioni venivano represse, le reti "Bot" portarono per molte settimane attacchi di Distributed Denial of Service su numerosi siti web di ministeri, funzionari governativi, banche, giornali e imprese. Non è chiaro chi si nascondesse dietro questi attacchi. Non è stato possibile confermare i sospetti che questi attacchi provenissero direttamente dal Cremlino. Il modo e tipo in cui furono condotti questi attacchi, lasciano però sospettare tentativi sistematici intrapresi per raccogliere dati di valore da utilizzare per attacchi successivi. Su Internet è in corso un potenziamento delle installazioni.

In agosto, il cancelliere tedesco Merkel si è recato per una visita di stato in Cina. Nello stesso periodo alcuni hacker sono penetrati nella Cancelleria Federale e solo all'ultimo momento è stato possibile impedire che 160 GB di dati sensibili venissero trasmessi a server cinesi. Attacchi simili si sono verificati in altri paesi europei. Anche i servizi segreti utilizzano Internet.

3. I trend del Malware nel 2007

Alcuni degli sviluppi dell'anno passato già si erano annunciati nel 2006. Gli attacchi via web si sono chiaramente intensificati. Le reti "Bot" sono e rimangono la chiave di volta della eCrime-Society. In ogni caso, anche l'Adware è una fonte di utili molto lucrosa. Molte delle nuove varianti di parassiti utilizzano il tempo che trascorre fino a quando non vengono creati e consegnati nuovi database antivirus tramite numerosi aggiornamenti. Si delineano, tuttavia, anche nuovi sviluppi. I codici classici di infezione di file (vale a dire i virus nel senso più stretto della parola) stanno godendo di un revival e nell'ambito Phishing i cavalli di Troia specializzati assumono il ruolo delle e-mail e dei siti web falsificati. Anche gli spammer si sono inventati nuovi processi per aggirare i filtri antispam. Nei paragrafi che seguono sono riportati i dettagli.

3.1 Conservazione del malware su Internet

Già nel 2006 era stato rilevato questo trend. Al posto degli allegati, le e-mail contengono sempre più spesso solo i collegamenti a file conservati su Internet. Questa nuova strategia non è stata adottata solo dalle varianti dello storm worm. Se si osserva l'elenco dei parassiti più comuni dell'anno, si nota che la metà contenuta nei Top 10 è già conosciuta da oltre un anno. Questo è valido in particolar modo per il primo classificato che era comparso per la prima volta nel marzo del 2004.

1	NetSky	31,0
2	Bagle	10,5
3	Mytob	7,8
4	Warezov	6,7
5	Feebs	3,5
6	Mydoom	3,5
7	Bankfraud	3,4
8	Zhelatin	3,1
9	Scano	2,8
10	Small	2,6

Tabella 1: Malware rilevati più di frequente nel 2007 classificati per famiglia di virus

Con l'utilizzo del blocco delle e-mail contenenti le URL dei file dannosi, la strategia venne ulteriormente modificata e invece di collegare direttamente i file eseguibili, i collegamenti ai programmi dannosi venivano riportati sui siti web. In alternativa, o in aggiunta, sui siti web si cercava di sfruttare le falle di sicurezza del browser per infettare il calcolatore del visitatore con il codice dannoso. Il numero di parassiti che agiscono tramite HTML o sfruttando le lingue degli script comunemente utilizzati su Internet si è quasi triplicato. I visitatori di questi siti non hanno assolutamente alcuna avvisaglia di questi attacchi. Vengono immediatamente infettati. Questo tipo di infezione viene denominato infezione Drive-By. Le conseguenze: i filtri antispam per il rilevamento del malware diventano sempre più importanti.

Per i cyber criminali, il deposito del malware su Internet offre molti vantaggi.
1. Il malware può essere costantemente aggiornato, 2. Successivamente a una prima analisi è possibile caricare parassiti adatti al sistema operativo e browser, 3. L'accesso al sito web può essere impedito a utenti specifici. 4. I ricercatori di virus che ad esempio si rendono sospetti visitando spesso siti web che contengono malware, devono prendere in considerazione il fatto di ottenere solo file innocui oppure di venire attaccati.

3.2 Riciclaggio del malware.

Nel 2007 il numero di nuovi parassiti ha infranto tutti i record. Con 133.253 nuovi parassiti il numero di parassiti di nuova generazione è triplicato rispetto all'anno precedente.

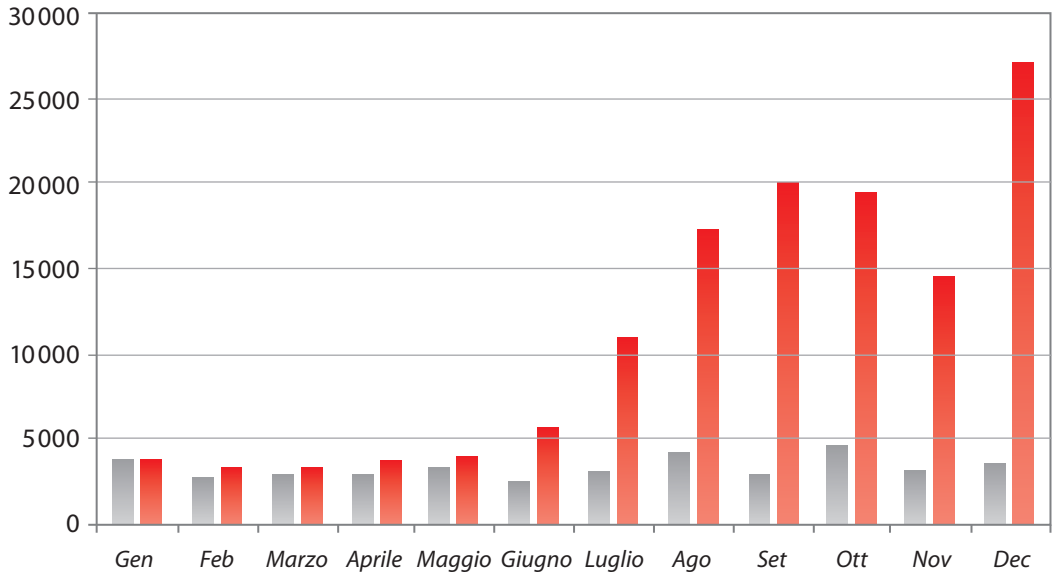

Grafico 1: Confronto del numero complessivo di nuovo malware tra 2006 e 2007

Uno dei motivi per i quali il numero di nuovi parassiti è cresciuto così tanto è da cercare nel modo in cui i Trojan-Dropper e Trojan-Downloader vengono utilizzati e nuovamente sfruttati. Questi due tipi di malware sono pensati per il singolo utilizzo, quasi un trojan usa e getta. Il momento in cui viene creato un codice antivirus per il parassita in questione, il malware è bruciato („burned"). Con l'utilizzo di runtime packer il codice dannoso può essere riutilizzato. Per fare questo si utilizzano dei packer standard con parametri inusuali. Nel frattempo, ci sono centinaia di packer specificamente sviluppati che adottano meccanismi polimorfi e 'confezionano' un vestito diverso per lo stesso codice di output. Gli autori di malware procedono fino a quando il nuovo codice non venga più individuato dagli scanner antivirus. In questo modo viene chiuso il ciclo di riciclaggio. Questo procedimento è così efficace che il numero di downloader e dropper è quasi raddoppiato. arrivando all' 263,7% ma si trova chiaramente sotto alla crescita complessiva del 338,6%.

3.3 Le reti „Bot“ rimangono il punto centrale della eCrime-Society.

Le reti “Bot” non servono solo per inviare e per eseguire attacchi di tipo Denial of Service. I calcolatori zombie vengono anche utilizzati per accogliere pagine di phishing e malware e per andare in perlustrazione di indirizzi di server email. Non deve quindi sorprendere se nel 2007 il numero di calcolatori “Bot” sia aumentato. Poiché la rete “BOT” è stata segmentata in unità più piccole, anche il numero delle reti “Bot” è aumentato considerevolmente. Nella maggioranza dei casi vengono noleggiate a costi molto vantaggiosi.

Il controllo della rete negli anni passati avveniva principalmente tramite IRC, nel 2007 sono nate altre reti “Bot” che utilizzano protocolli diversi per il controllo. La rete “Bot” Storm è organizzata come rete P2P. Anche la potente rete “Bot” Zunker comunica tramite HTTP. Di conseguenza, anche i meccanismi di camuffamento diventano sempre più sofisticati. Con l’aggiornamento frequente del rootkit, i backdoor vengono mimetizzati. I programmi e dati necessari a un compito vengono trasmessi appena prima ed eliminati subito dopo.

	# 2007	%	# 2006	%	% 2006 - 07
Backdoors	41.477	31,1	8.321	22,3	498,5
Spyware	29.887	22,4	8.889	22,3	336,2
Downloader/ Dropper	28.060	21,1	10.640	26,7	263,7
Cavalli di Troia	13.787	10,3	5.230	13,1	263,6
Adware	7.654	5,7	1.343	3,4	569,9
Worms	4.647	3,5	1.751	4,7	265,4
Virus	2.127	1,6	419	1,1	507,6
Tools	1.366	1,0	229	0,6	259,7
Rootkits	559	0,4	229	0,6	244,3
Altro	3.688	2,8	1.776	4,5	207,7
Totale	133.253	100,0	39.349	100,0	338,6

Tabella 2: Numero e quota di nuovi malware 2007 suddivisi per tipo e variazione in confronto al 2006

Il fatto che le reti “Bot” fossero il centro delle attività dei cyber criminali (e continuano a esserlo), si vede anche guardando lo sviluppo del tipo di malware. I PC infetti possono essere aggiornati e coordinati in remoto tramite applicativi backdoor. Questi backdoor, non solo hanno quasi quintuplicato il loro numero complessivo rispetto al 2006. Con circa 3 varianti nuove su 10 sono riusciti non solo ad aumentare la loro quota rispetto ai tipi di malware ma a superare anche Downloader e Spyware. Gli altri leader della classifica dei tipi di malware occupano i processi standard di infezione. Per prima cosa il calcolatore viene infettato con un downloader o dropper, che a prescindere dal caricamento e avvio di un file disattiva le impostazioni di sicurezza del sistema. Indebolito in questo modo, il backdoor si assicura che il calcolatore possa essere controllato a distanza e che vi possano essere caricati altri malware. Spesso si tratta di spyware o cavalli di Troia, che utilizzano il calcolatore come distributore di spam oppure lo tramutano in server web o di file.

3.4 Adware in forte crescita

A parte le reti "Bot" ci sono altri modi per utilizzare in modo molto lucroso un calcolatore infetto: Adware. Questi programmi non rubano dati, ma danno indicazioni sulle abitudini di navigazione internet e, a richiesta, visualizzano pagine di pubblicità oppure manipolano le ricerche. Il pagamento del Adware avviene tramite il conteggio del numero di clic prodotti (in questo caso, ad esempio, viene manipolata la pagina iniziale del calcolatore infetto) oppure per versione installata. Programmi affiliati corrispondenti si trovano in relativi forum online.

Nonostante nell'anno passato anche grandi aziende del settore hanno dovuto incassare sconfitte legali, il numero di malware pubblicitario e programmi indesiderati è aumentato di oltre cinque volte (vedi la tabella 2).

3.5 Revival degli agenti infettanti dei file

I virus classici che si attaccano ai file, negli anni hanno perso di importanza. Tuttavia, l'uso esteso di supporti per lo scambio di dati come ad esempio le chiavette USB e hard disk esterni ha fatto sì che questo meccanismo di diffusione riacquistasse importanza. Il numero di virus nel senso più stretto è aumentato di circa cinque volte.

3.6 Spam

Gli invii di posta elettronica massiva indesiderata hanno riempito quotidianamente anche nel 2007 milioni di caselle di posta. In novembre, la posta spam ha raggiunto il 95% del traffico complessivo di e-mail. Con trucchi sempre nuovi, gli spammer cercano di far superare indenni i loro invii ai filtri antispam. All'inizio le caselle di posta sono state inondate di spam sotto forma di immagini. In questo caso il messaggio pubblicitario era nascosto in un'immagine. I testi contenuti nella e-mail stessa servivano a ingannare il filtro Bayes. Con molti trucchi, come ad esempio il taglio delle immagini o variazioni casuali di immagine e testo, venivano elusi i metodi di analisi più diffusi, come il riconoscimento dei testi e le serie basate su banche dati. Quando a metà anno i filtri antispam sono stati convertiti per riconoscere i file immagine, gli spammer modificarono nuovamente metodo inviando la posta spam come file Excel, PDF, MP3 e Video. Alla conclusione dell'anno la percentuale insolita di questi formati è di nuovo diminuita.

Ma lo spam rimane un tema importante. Non solo per via degli alti guadagni che possono essere raggiunti con questo tipo di posta. Anche perché il contatto di lavoro di spammer e autori di malware è sempre più stretto. Circa il 90% di tutta la posta spam è stata inviata tramite la rete "Bot". Ma anche la nuova strategia di mandare e-mail con collegamenti verso i siti con malware rendono i filtri anti spam un elemento importante della protezione da malware.

3.7 Phishing, pharming, Banking e furto di identità

Il phishing classico ristagna. Grazie a filtri antispam migliorati e toolbar antiphishing, i tentativi di frode con supposte e-mail provenienti da banche e negozi online che portano a un sito web ben falsificato hanno un ruolo sempre minore. Tuttavia gli applicativi cavalli di Troia con questa flessione hanno fatto più che pari, con i cosiddetti Banking-Trojans. Le nuove varianti non si limitano a rubare le informazioni relative ai conti online e alle carte di credito. Alcuni programmi spyware rubano tutti i dati di accesso memorizzati dalla Protected Storage Area. Altri, ad esempio Bzub inviano il contenuto di tutti i moduli web agli aggressori. In questo modo le vittime dei cavalli di Troia possono perdere completamente la loro identità online. E sempre più spesso innocenti vengono coinvolti nelle malefatte dei cyber criminali.

Ecco una breve panoramica delle caratteristiche tecniche dello spyware

- Con il**PHARMING** è possibile essere condotti senza accorgersene su siti web falsi anche se nel browser si è inserito il nome corretto del dominio. La base di questo tipo di attacco è l'individuazione dell'indirizzo IP del nome del dominio. Inoltre, da un lato può essere attaccato lo stesso sistema DNS. Ma anche gli stesso calcolatori client offrono alcuni punti di attacco. I rappresentanti della famiglia di virus Qhosts, ad esempio, modificano le registrazioni del file HOSTS di alcune pagine web oppure registrano un server DNS che viene controllato dagli aggressori.
- I **KEYLOGGER** riprendono le attività dei tasti e le inviano a terzi non autorizzati. Spesso si attivano quando vengono soddisfatte condizioni precise, ad esempio quando il sito web è incluso in un elenco spesso molto lungo di nomi di dominio oppure quando vengono aperte finestre con titoli precisi
  Per controbattere i keylogger sono state sviluppate le tastiere su schermo. Come reazione a queste sono arrivati gli **SCREENLOGGER**. Questi eseguono a intervalli regolari un'immagine del contenuto completo dello schermo (es. **RBOT**) oppure creano con ogni clic del mouse un'immagine del campo circostante il mouse. A volte le sequenze di immagini vengono convertite in filmati AVI.

Ci sono strumenti di spionaggio specifici (es.**RBOT**) che utilizzano WebCam e microfoni dei calcolatori infetti

- Alcuni parassiti (es. **TORPIG**) modificano l'aspetto e il contenuto del browser. Sono in grado di visualizzare la riga contenente l'indirizzo corretto nonostante i contenuti arrivino da un altro dominio falsificato. Anche il lucchetto, che indica la presenza di una connessione sicura può essere visualizzato senza giustificazione. Altri parassiti (es. varianti di **BANCOS** oppure **NURECH**) aggiungono ulteriori campi modello in una pagina oppure pagine web supplementari nella finestra di dialogo. In questo modo i certificati SSL rimangono attivi. Senza strumenti speciali non è possibile riconoscere se questi dati siano stati falsificati o meno.
- **SESSION HIJACKER** acquisiscono la seduta del browser in modo che l'aggressore è in grado di acquisire importi e dettagli relativi al conto a proprio favore (es. Bancos). Alla vittima però vengono mostrate le proprie informazioni. Anche la situazione del conto viene falsificata in modo corrispondente. Anche in questo caso la frode diventa evidente al momento di ricezione dell'estratto conto.
- Redirector indirizza il flusso dei dati in modo tale da rendere possibile un attacco di tipo **MAN-IN-THE-MIDDLE**. Questo può essere un proxy locale oppure un server proxy che si trova sotto il controllo dell'aggressore. In questo modo la comunicazione sulla rete della vittima può essere spiata. E-mail, chat, siti web visitati, dati dei moduli e scaricamento di file possono essere tutti sorvegliati.

- **Sniffer** sorvegliano il traffico dati sulla rete della vittima. Il numero di nuovi sniffer è aumentato in modo considerevole.
- **Programmi Trojan-PSW** eseguono una ricerca sul PC per tutte le informazioni di valore. Queste possono essere indirizzi e-mail oppure file con un contenuto specifico, oppure un tipo specifico di file. Questi dati vengono compressi e inviati all'aggressore. Sono anche molto ricercate le informazioni relative ai login registrate sul sistema, chiavi di registro e password (o il loro Hash). Le password dei siti web e degli account di posta vengono salvate nella zona Protected Storage Area, se l'utente accetta l'utile offerta del browser o client e-mail di salvare le password. È una buona idea rinunciare al salvataggio automatico di password e informazioni inserite nei moduli. Un degno rappresentante di questa categoria è LdPinch.

Si può vedere che i metodi diventano sempre più raffinati ed efficaci. Anche questo ha fatto sì che nel 2007 il numero di vittime e danni sia aumentato.

3.8 I gamer online nel mirino

Guardando la tabella che riporta le famiglie di virus più attive non si notano solamente i backdoor. Il vecchio e nuovo leader della categoria, il backdoor Hupigon appartiene a una famiglia di malware molto utilizzata dai packer. Le nuove versioni possono essere raccolte velocemente e in modo efficiente con un clic di un toolkit. Alcune varianti utilizzano contemporaneamente 11 packer diversi. Rbot attacca con metodi aggressivi i programmi di protezione dei calcolatori.

	#2006	Famiglia di virus	#2007	Famiglia di virus
1	2.549	Hupigon	16.983	Hupigon
2	1.474	Zlob	8.692	OnLineGames
3	1.420	Banload	3.002	Rbot
4	1.147	Banker	2.973	Banker
5	869	LdPinch	2.848	Banload
6	848	Rbot	2.627	Zlob
7	562	Horst	2.533	Virtumonde
8	555	Lineage	1.922	Magania
9	497	SdBot	1.882	LdPinch
10	489	QQHelper	1.751	BZub

Tabella 3: Famiglie di virus Top 10 nel 2007

Molto più interessante che con „OnLineGames“ e „Magania“ due applicazioni per rubare le password si trovano tra i primi 10, dedicate ai giochi online. Il 2006 era già stato degno di nota poiché con Lineage un programma simile aveva già raggiunto i primi posti. I due rappresentanti di quest'anno hanno superato chiaramente il risultato dell'anno scorso. Questo indica che i giocatori online sono sempre più presi di mira. Il numero di applicativi spia delle password che guardano ai giocatori online nel frattempo superano il numero di banking-trojans.

3.9 Codici nocivi sulle diverse piattaforme - Nessun pericolo per i cellulari

Quando si guardano le piattaforme per le quali vengono sviluppati parassiti, allora Windows domina chiaramente la scena. Nei posti seguenti gli attacchi basati su web nei Javascript, HTML, VBSkript, PHP e Perl si sono quasi triplicati. Sono stati rilevati solo 137 parassiti per Linux.

D'altro canto non abbiamo potuto rilevare nel corso del 2007 il pericolo annunciato più volte per i cellulari. Con un numero complessivo di 26 parassiti, la maggioranza di cui strumenti di spionaggio più o meno legali pensati per mariti gelosi o genitori preoccupati - il numero di codici parassiti per Symbian scendono a 1/3 dei codici scoperti nell'anno precedente e, piazzandosi al 145esimo posto, non si trovano più tra i primi 10.

	#2007	Piattaforma	#2006	Piattaforma
1	126.854	Win32	37.397	Win32
2	2.463	JS	487	HTML
3	1.106	HTML	334	JS
4	1.007	VBS	323	VBS
5	707	BAT	287	BAT
6	197	PHP	145	Linux
7	166	MSWord	123	MSWord
8	139	Perl	101	DOS
9	137	Linux	73	SymbOS
10	90	ASP	70	Perl

Tabella 4: Piattaforme Top 10 2006 e 2007

4. Previsione 2008

Per il 2008 pensiamo che i metodi collaudati verranno mantenuti e migliorati. In questa categoria è necessario notare i seguenti punti:

- **Un aumento del malware basato su Internet.** Le nuove possibilità offerte da Web 2.0 verranno rafforzate e anche utilizzate dai criminali online. Particolare attenzione meritano le falle di sicurezza negli applicativi web tramite le quali il codice dannoso può penetrare nelle pagine web risultanti. Aumenteranno anche gli attacchi alle banche dati che si trovano dietro agli applicativi web. Le versioni in preparazione dei tool renderanno questi processi molto più semplici.
- **Mailing personalizzati.** Le informazioni ottenute con il furto di dati verranno utilizzate nell'anno che verrà, per l'invio mirato di mail di Spam e phishing a gruppi di persone. Queste E-Mail conterranno saluti personalizzati e l'indirizzo del mittente falsificato in modo tale che sembreranno inviate da un conoscente.
- **Lo spam aumenterà ulteriormente?** Nel complesso il numero di e-mail di spam aumenterà di poco. Tuttavia, lo spam diventerà chiaramente più mirato e quindi più efficiente. Nell'anno venturo, lo spam su blog e forum diventerà un problema di grandi dimensioni.
- **Phishing tramite e-mail e siti web diminuirà sensibilmente anche nell'area bancaria.** I nuovi obiettivi sono i negozi online, le piattaforme di Social Networking (MySpace, Facebook, LinkedIn etc.), le borse lavoro e OnlineGames. Previsione: il numero di marche aumenterà considerevolmente nell'anno a venire
- **Un anno duro per i ricercatori di malware.** La massa di malware non diminuirà, ma la complessità del malware aumenterà. Crittografia, runtime packer speciali, strumenti per il camuffamento di codice, malware consegnato in modo mirato sono solo alcune delle sfide che stanno affiorando

Però prevediamo anche delle novità:

- **Più estorsioni.** Il Ransomware è stato abbastanza raro nel 2007. Prevediamo per il prossimo anno miglioramenti nell'infrastruttura "Bot" e presso i siti host Bullet-Proof (il più conosciuto è il Russian Business Network RBN). In questo modo, l'anonimità dell'aggressore potrà essere garantita, e aumenterà il numero di estorsioni verso file di Office o immagini codificati. Rimedi: Backup dei dati
- **Virtualizzazione.** Da molti mesi tutti, i nuovi processori prevedono nuove funzioni che possono essere utilizzate in modo molto semplice ed efficace per macchine virtuali. Queste funzioni di virtualizzazione possono, fra l'altro, essere utilizzate per la creazione di Rootkit di tipo nuovo (parola d'ordine Pillola blu). D'altronde, la virtualizzazione offre molte possibilità per la realizzazione di concetti efficaci di protezione. Sia gli aggressori sia i difensori investiranno molta ricerca in quest'area
- **Nuove tecnologie in crescita.** Vista e MacOSX stanno per superare il punto critico del 10% della quota di mercato. Per questo diventeranno sempre più interessanti per i cyber criminali e il numero di attacchi a questi sistemi sarà sempre maggiore. Con Vista i gadget potranno essere la nuova porta di invasione. Nel corso del 2008 anche la pacifica oasi degli utenti Apple verrà sottoposta a qualche scossa.
- Quali saranno le **nuove tecnologie** che attireranno l'attenzione di hacker e cracker è difficile da prevedere. Non pensiamo che in un primo momento ci saranno attacchi di grandi dimensioni. Però riteniamo che ci saranno degli attacchi di prova su VoIP e sulle consolle di gioco in grado di connettersi a Internet.

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