G DATA

Malware-Report 2007

Ralf Benzmüller & Thorsten Urbanski

Geschützt. **Geschützter. G DATA.**

G DATA Malware-Report 2007

Ralf Benzmüller & Thorsten Urbanski

1. Zusammenfassung: Malware-Zahl dreimal so hoch wie 2006

G DATA Security verzeichnet 2007 einen enormen Anstieg von Schadcode: Der Zuwachs betrug im Vergleich zum Vorjahr mehr als 300 Prozent.

Zwar war auch 2007 nicht das Jahr der großen Outbreaks, jedoch hielten die Malware-Autoren die Security-Hersteller enorm auf Trab. Die Anzahl neuer Malware stieg bis Ende 2007 auf den Rekordwert von 133.253 neuen Schädlingen – im Vergleich hierzu: 39.670 neue Schadprogramme in 2006.

Die größten Zuwachsraten lagen im Bereich von Adware (570%), Viren (507%), Backdoors (499%) und Spyware (336%).

Eine Gruppe sticht hierbei besonders hervor: Spionier- und Datendiebstahl-Trojaner. Ihre Zahl ist 2007 massiv angestiegen, da die eCrime-Society massiv auf Datenjagd ging.
Der Diebstahl von persönlichen Daten und Identitätsdiebstahl war 2007 somit eines der zentralen Themen. Zwar stagnierte klassisches Phishing per E-Mail, jedoch haben sog. Banking-Trojaner dies mehr als wettgemacht.

Diese spezialisierten Trojanischen Pferde traten 2007 in immer neuen Varianten auf und stehlen nicht nur Zugangsdaten für Onlinebankkonten und Kreditkarteninformationen. Manche Spywareprogramme stehlen dabei alle gespeicherten Zugangsdaten oder senden komplette Inhalte von Webformularen an die kriminellen Angreifer. Auf diese Weise verloren Opfer ihre gesamte Online-Identität.

1.1 Online-Gamer im Visier der eCrime-Society

Was sich 2006 bereits abzeichnete, wurde im vergangenen Jahr Realität. Online-Gamer rücken stärker ins Visier von Kriminellen.

Mit „OnLineGames“ und „Magania“ schafften es 2007 zwei Passwortstehler sogar in die Top 10 der Malware-Charts. Der Angriff auf Online-Spieler hat im vergangenen Jahr somit deutlich zugenommen. Die Anzahl der Passwortspione, die auf Onlinespieler zielen, übersteigt mittlerweile die Anzahl der Banking-Trojaner.

1.2 Revival der Viren und Malware-Recycling

Die starke Verbreitung von USB-Sticks und Wechselfestplatten sorgte 2007 für ein Revival klassischer Dateiinfektoren. Klassische Viren, die sich an Dateien anhängen, waren in den vergangenen Jahren stark rückläufig. 2007 hat sich dies erstmals geändert und deren Zahl hat sich bereits verfünffacht.

Der Recycling-Gedanke ist 2007 auch bei Malware-Autoren angekommen. Die immens hohe Zahl neuer Schädlinge ist nicht zuletzt das Resultat sog. Wegwerf-Trojaner, die nur ein einziges Mal zum Einsatz kommen. Trojan-Dropper und Trojan-Downloader gelangen nach Gebrauch in modifizierter Form direkt wieder in Umlauf. Der Programmablauf und die Programmlogik bleiben davon unberührt. Aus cyber-ökonomischer Sicht ist dieses Konzept äußerst erfolgreich und es ist 2008 mit einer Flutwelle von Wegwerf-Malware zu rechnen.

1.3 Weiterhin keine Gefahr für Smartphones

Die vielfach herauf beschworene Gefahr für Mobiltelefone blieb 2007 aus. Mit gerade einmal 22 neuen Schädlingen - die meisten davon halblegitime Spytools, die sich hauptsächlich an eifersüchtige Ehemänner oder besorgte Eltern richten - sinkt die Anzahl der Schädlinge für Symbian auf 1/3 des Wertes vom Vorjahr. Hier von einem immensen Gefahrenpotential zu sprechen, ist nach Einschätzung von G DATA reine marktpolitisch bestimmte Panikmache.

1.4 Fazit und Ausblick

G DATA rechnet 2007 mit einem gleich bleibend hohen Malware-Niveau. Es ist absehbar, dass die etablierten Geschäftsmodelle 2008 weiter verfeinert werden. Mit einem weiteren Anstieg von Spam ist dagegen 2008 kaum zu rechnen. Vielmehr wird 2008 mit einem massiven Anstieg von personalisierten Spam zu rechnen sein. Die durch Datendiebstähle gewonnenen Informationen werden hierbei dafür genutzt, um Spam- und Phishing-Mails gezielt an passende Personengruppen zu versenden.

Virtualisierung für Malware interessant

Seit mehreren Monaten enthalten alle neu ausgelieferten Prozessoren Funktionen, mit denen sich Virtuelle Maschinen sehr einfach und effektiv nutzen lassen. Diese Virtualisierungsfunktionen können u. a. zur Erstellung neuartiger Rootkits genutzt werden (Stichwort Bluepill). Andererseits bietet die Virtualisierung viele Möglichkeiten, um effektive Schutzkonzepte zu realisieren. In diesem Bereich erwartet G DATA ein starkes Forschungs-Engagement der Malware-Industrie.

Kritische Masse bei Vista und Mac OS X bald erreicht

Vista und MacOSX stehen kurz davor, die kritische Marke von 10% Marktanteil zu überschreiten. Hierdurch werden beide Betriebssysteme für Cyberkriminelle deutlich interessanter und Angriffe auf diese Systeme werden zunehmen. Die friedliche Oase für Apple-Nutzer könnte somit 2008 einige Erschütterungen hinnehmen müssen. Bei Vista könnten sich Gadgets als neues Einfallstor etablieren.

2. Einleitung

Im Ausblick des letzten Jahresberichts sind wir davon ausgegangen, *„dass die etablierten Geschäftsmodelle im Bereich Adware, Spyware , Phishing und die ausgiebige Nutzung von Botnetzen auch im kommenden Jahr fortgesetzt werden“*. Diese nicht allzu kühne Vorhersage hat sich ebenso zum Schaden vieler Computernutzer bestätigt, wie die *„Zunahme von Schadcode in Webseiten“* und die geringe Gefahr für Nutzer von Mobiltelefonen.

Die Malwareautoren haben uns 2007 enorm auf Trab gehalten. Insgesamt ist die Anzahl neuer Malware auf den Rekordwert von 133.253 neuen Schädlingen gestiegen. Das ist ein Anstieg um mehr als das Dreifache (338,6%). Die größten Zuwachsraten lagen im Bereich von Adware (570%), Viren (507%), Backdoors (499%) und Spyware (336%).

Wenn man 2007 aber einer Gruppe von Schädlingen widmen möchte, so sind dies klar die Datenklau- und Spioniertrojaner. Sie treten massiv auf und stehlen mittlerweile weit mehr als nur Zugangsdaten zu Onlinebanken. Einige der wichtigsten Ereignisse des Jahres drehen sich daher um das Thema Datendiebstahl.

3. Wichtige Ereignisse 2007

Datendiebstahl und Botnetze bestimmten 2007 auch die Schlagzeilen. Folgende Ereignisse und Entwicklungen finden wir besonders erwähnenswert.

3.1 Der „Sturmwurm“[1]

Im Januar wurden massenhaft E-Mails versendet, die sich auf den soeben abklingenden, schweren Sturm Kyrill bezogen, der weite Teile Europa verwüstete. Das Trojanische Pferd im Anhang der Mail machte den Rechner zum Zombie eines Botnetzes. Aus der gleichen Quelle wurden zuvor Videoclips von Saddam Husseins Hinrichtung oder Bilder zum bevorstehenden Atomkrieg angekündigt. In darauf folgenden Wellen wurde an weitere aktuelle Nachrichten angeknüpft. Später wurden u. a. Kunden von IKEA, Quelle und eBay mit falschen Rechnungen bedacht. Im Laufe des Jahres kamen dann Grußkarten, Spiele und Software zur Verbreitung zum Einsatz, die auf Webseiten hinterlegt waren. So konnten mehrere Millionen Rechner in das Sturm-Botnetz integriert werden - das größte Botnetz bis dahin. Es wird hauptsächlich zum Versand von Aktien-Spam und für verteilte Lastangriffe (DDoS) verwendet.

3.2 Datendiebstahl

Im Januar wurden Kunden der schwedischen Bank Nordea in persönlich gehaltenen Phishing-Mails ein Anti-Spam-Tool zum kostenlosen Download angeboten. Das Tool diente aber lediglich dazu, die Zugangsdaten der Bankkunden auszuspähen. Vorausgegangen war ein Diebstahl von Kundeninformationen. Diese Informationen wurden wiederum genutzt, um die Kunden gezielt anzugreifen. Der Erfolg gab den Tätern Recht. Mit den gestohlenen Zugangsdaten konnten ca. 900.000 EUR erbeutet werden.

Weitere große Fälle von Datendiebstahl:

- Durch gezielte Angriffe auf das WLAN von TJX wurden mehr als 45 Millionen Kreditkarteninformationen gestohlen
- Im Februar stahlen Kriminelle die Passwörter und E-Mail-Adressen von Nutzern des Studierenden-Portals StudiVZ - die Folge: Zurücksetzung aller Passwörter.
- Durch Trojanische Pferde konnten 1,6 Millionen Datensätze von meist amerikanischen Nutzern der Jobbörse Monster.com erbeutet werden.

Milionenfach fielen Online-Kriminellen weltweit durch diese und ähnliche Datendiebstähle Datensätze mit persönlichen Informationen in die Hände.

1 Der Sturmwurm ist technisch gesehen ein Trojanisches Pferd. Aber der resultierende Begriff „Sturmtrojaner“ ist wenig reizvoll und auch nicht völlig korrekt.

3.3 Kalter Krieg im Internet

Die Verlegung eines russischen Kriegerdenkmals in der estnischen Hauptstadt Tallin führte zu heftigen Protesten in der russischen Bevölkerung. Als die Demonstrationen niedergeschlagen wurden, erfolgten mit Botnetzen über mehrere Wochen verteilte Lastangriffe auf zahlreiche Webseiten von Ministerien, Regierungsbehörden, Banken, Zeitungen und Unternehmen. Wer hinter den Angriffen steckte ist unklar. Verdächtigungen, dass die Angriffe vom Kreml ausgingen, konnten nicht bestätigt werden. Die Art und Weise wie die Angriffe durchgeführt wurden, lässt Vermutungen über systematische Angriffsversuche zu, die wertvolle Daten für spätere Angriffe liefern sollten. Im Internet wird aufgerüstet!

Im August reiste Bundeskanzlerin Merkel zu einem Staatsbesuch nach China. Zur gleichen Zeit brachen Hacker in das Bundeskanzleramt ein – in letzer Minute konnte der Diebstahl und die Übertragung von 160 GB sensibler Daten verhindert werden. Ähnliche Angriffe gab es auch in weiteren europäischen Ländern.

4. Malwaretrends 2007

Einige Entwicklungen des vergangenen Jahres zeichneten sich bereits 2006 ab. Webbasierte Angriffe nahmen deutlich zu. Botnetze sind und bleiben Dreh- und Angelpunkt der eCrime-Society. Adware behauptet sich ebenfalls als lukrative Einnahmequelle. Viele neue Schädlingsvarianten nutzen die Zeit bis zur Erstellung und Auslieferung von neuen Virensignaturen durch zahlreiche Updates. Aber auch neue Entwicklungen zeichnen sich ab. Klassische Dateiinfektoren (also Viren im engeren Sinne) erleben ein Revival und im Bereich Phishing übernehmen spezialisierte Trojanische Pferde die Rolle von gefälschten E-Mails und Webseiten. Aber auch Spammer haben sich einiges einfallen lassen, um die Spamfilter auszutricksen. Die folgenden Abschnitte erläutern die Einzelheiten.

4.1 Verlagerung von Malware ins Internet

Schon 2006 zeichnete sich dieser Trend ab. Anstelle von Dateianhängen enthalten E-Mails und Instant Messages nur noch Links auf Dateien im Internet. Nicht nur die Sturmwurm-Varianten haben diese neue Strategie aufgegriffen. Ein Blick auf die häufigsten Schädlinge des Jahres zeigt, dass die Hälfte der Schädlinge aus der Top 10 schon seit über einem Jahr bekannt ist. Das gilt insbesondere für den Spitzenreiter, der im März 2004 zum ersten Mal auftauchte.

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

Tabelle 1: Häufigste Malwarefunde 2007 nach Virenfamilie

Als die URLs auf schädliche Dateien zum Blocken der E-Mails verwendet wurden, wechselte die Strategie erneut und die ausführbaren Dateien wurden nicht mehr direkt verlinkt, sondern die Webseiten enthielten die Links auf die Schadprogramme. Alternativ oder zusätzlich wird auf den Webseiten versucht, Sicherheitslücken des Browser auszunutzen, um die Rechner der Besucher mit Schadcode zu infizieren. Die Anzahl der Schädlinge, die per HTML- oder im Web üblichen Skriptsprachen agiert ist fast um das dreifache angestiegen. Die Besucher der Seite merken von den Angriffen nichts. Sie werden im Vorübergehen infiziert. Man spricht dann von einer Drive-By Infektion. Fazit: Spamfilter werden für die Erkennung von Malware immer wichtiger!

Für Cyberkriminelle bietet die Verlagerung der Malware ins Internet etliche Vorteile: 1. die Malware kann ständig aktualisiert werden, 2. nach einer ersten Analyse des Rechners können für das Betriebssystem und den Browser passende Schädlinge nachgeladen werden, 3. der Zugang zur Webseite kann bestimmten Nutzern verweigert werden. 4. Fallen Virenforscher durch den häufigen Besuch einer Malwarewebsite auf, müssen sie damit rechnen, nur harmlose Dateien zu erhalten oder sogar attackiert zu werden.

4.2 Malware-Recycling.

Die Anzahl neuer Computerschädlinge sprengt 2007 alle Rekorde. Mit 133.253 neuen Schädlingen hat sich deren Zahl gegenüber dem Vorjahr mehr als verdreifacht.

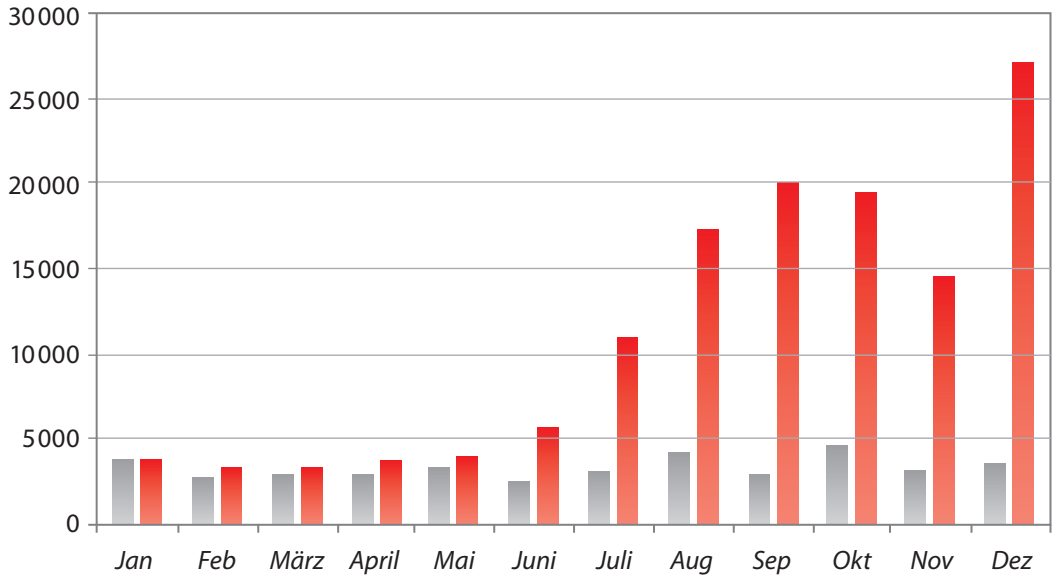

Diagramm 1: Vergleich - Gesamtzahl neuer Malware 2006 zu 2007

Ein Grund, warum die Anzahl der Computerschädlinge derart gestiegen ist, liegt in der Art, wie Trojan-Dropper und Trojan-Downloader verwendet und wiederverwertet werden. Diese beiden Malwaretypen sind zur einmaligen Verwendung gedacht - quasi als Wegwerf-Trojaner. Wenn eine Virensignatur für den Schädling erstellt wurde, gilt die Malware als verbrannt („burned“). Mit sog. Runtime-Packern kann der gleiche Schadcode aber wiederverwertet werden. Dazu wurden zunächst Standardpacker mit ungewöhnlichen Parametern verwendet. Mittlerweile gibt es aber Hunderte von speziell entwickelten Packern, die über polymorphe Mechanismen verfügen und so jede Kopie des Ausgangscodes in ein anderes Gewand packen. Die Malwareautoren machen das so lange, bis der neue Code von den gängigen Virenscannern nicht mehr erkannt wird. So schließt sich der Recycling-Kreis! Dieses Verfahren ist offenbar so erfolgreich, dass sich die Anzahl der Downloader und Dropper zwar fast verdoppelt hat, mit 263,7% aber deutlich unter dem Gesamtwachstum von 338,6% liegt.

4.3 Botnetze sind weiterhin das zentrale Mittel der eCrime-Society.

Botnetze dienen nicht nur dem Versenden von Spam oder Ausführen von Denial-of-Service-Angriffen. Zombie-Rechner werden auch dazu genutzt, Phishing- und Malwareseiten zu hosten - und um die Adressen von E-Mailservern auszukundschaften. Es ist daher nicht verwunderlich, dass die Zahl der Botnetzrechner 2007 zugenommen hat. Da die Botnetze in kleinere Einheiten segmentiert wurden, ist auch die Zahl der Botnetze deutlich gewachsen. Sie werden meist zu immer günstigeren Konditionen vermietet.

Erfolgte die Steuerung im letzten Jahr fast ausschließlich per IRC, so entstanden 2007 mehr Botnetze, die andere Protokolle zur Steuerung nutzen. Das Sturm-Botnetz ist als P2P-Netz angelegt. Das ebenso mächtige Zunker-Botnetz kommuniziert per HTTP. Die Tarnmechanismen werden zudem immer ausgefeilter und mit häufigen Updates und Rootkits werden die Backdoors effizient getarnt. Die Programme und Daten für einen Auftrag werden erst unmittelbar zuvor übertragen und anschließend wieder gelöscht.

	# 2007	%	# 2006	%	% 2006 - 07
Backdoors	41.477	31,1	8.321	21,1	498,5
Spyware	29.887	22,4	8.889	22,7	336,2
Downloader/ Dropper	28.060	21,1	10.640	27,2	263,7
Trojan. Pferde	13.787	10,3	5.230	13,4	263,6
Adware	7.654	5,7	1.343	3,4	569,9
Würmer	4.647	3,5	1.751	4,5	265,4
Viren	2.127	1,6	419	1,1	507,6
Tools	1.366	1,0	526	1,3	259,7
Rootkits	559	0,4	229	0,6	244,3
Sonstige	3.688	2,8	1.776	4,5	207,7
Gesamt	133.253	100,0	39.124	100,0	338,6

Tabelle 2: Anzahl und Anteil neuer Malware 2007 nach Typ und Veränderung gegenüber 2006

Dass Botnetze das Zentrum der Aktivitäten von Cyberkriminellen waren (und weiterhin sind), zeigt auch der Blick auf die Entwicklung bei den Malwaretypen. Infizierte PCs lassen sich über Hintertürprogramme aktualisieren und ferngesteuert koordinieren. Diese Backdoors konnten nicht nur ihre Gesamtzahl gegenüber 2006 annähernd verfünffachen. Mit ca. 3 von 10 neuen Varianten konnten diese ihren Anteil steigern und bei den Malwaretypen sogar Downloader und Spyware hinter sich lassen.

Die weiteren Spitzenreiter bei den Malwaretypen belegen die übliche Vorgehensweise bei einer Infektion. Zunächst wird der Rechner mit einem Downloader oder Dropper infiziert, der abgesehen von dem Laden und Starten einer Datei die Sicherheitseinstellungen des Systems herunterfährt. So geschwächt sorgt eine Backdoor dafür, dass der Rechner ferngesteuert und mit weiterer Malware versehen werden kann. Dabei handelt es sich oft um Spyware oder andere Trojanische Pferde, die Rechner in Spamschleudern oder Web- und Dateiserver verwandeln.

4.4 Adware - stark im Kommen

Abgesehen von Botnetzen gibt es eine weitere Möglichkeit infizierte Rechner lukrativ auszunutzen: Adware. Die Programme stehlen zwar keine Daten, zeichnen aber mitunter das Surfverhalten des Nutzers auf und blenden beim Aufruf entsprechender Seiten Werbung ein oder manipulieren Suchabfragen. Die Bezahlung der Adware erfolgt entweder nach Anzahl der erzeugten Clicks (dann wird z.B. die Startseite befallener Rechner manipuliert) oder pro installierter Version. Entsprechende Affiliate-Programme finden sich in einschlägigen Onlineforen.

Obwohl im vergangenen Jahr auch große Firmen der Branche juristische Niederlagen verkraften mussten, hat sich die Anzahl der Werbe-Malware und potenziell unerwünschten Programme mehr als verfünffacht (vgl. Tabelle 2).

4.5 Revival der Dateiinfektoren

Klassische Viren, die sich an Dateien anhängen nahmen seit Jahren bis zur Bedeutungslosigkeit ab. Die verbreitete Nutzung von Wechseldatenträgern wie USB-Sticks und Wechselfestplatten machen diesen Verbreitungsmechanismus aber wieder effektiv. Die Anzahl der Viren im engeren Sinne stieg fast um das Fünffache.

4.6 Spam

Unerwünschte zugesendete Massenmails füllten auch 2007 tagtäglich Millionen von E-Mail-postfächern. Im November erreichten Spam-Mails einen Anteil von 95% am gesamten Maildatenverkehr. Mit immer neuen Tricks versuchten die Spammer ihre Massenfracht an den Spamfiltern vorbeizumogeln. Zunächst überschwemmten Image-Spams die Postfächer. Hier war die eigentliche Werbebotschaft in einem Bild versteckt. Die Texte, die in der Mail enthalten waren, dienten lediglich dazu, die Bayes-Filter auszutricksen. Mit zahlreichen Tricks, wie etwa dem Zerschneiden von Bildern oder zufällige Farb- und Schriftvariationen, wurden auch weitergehende Analysemethoden wie Texterkennung und Datenbankbasierte Ansätze unterlaufen.
Als Mitte des Jahres die Spamfilter auf die Bilddateien umgestellt waren, schwenkten die Spammer wieder um und versendeten die Spam-Mails als Excel-, PDF-, MP3- und Videodateien. Zum Ende des Jahres hat der Anteil dieser ungewöhnlichen Dateiformate wieder abgenommen.

Aber Spam bleibt ein wichtiges Thema. Nicht nur wegen der hohen Erträge, die damit erzielt werden. Auch weil Spammer und Malwareautoren immer enger zusammenarbeiten. Etwa 90% aller Spam-Mails werden per Botnetz versendet. Aber auch die neue Strategie E-Mails mit Links auf Malwareseiten zu versenden machen Spamfilter zu einer wichtigen Komponente des Malwareschutzes.

4.7 Phishing, Pharming, Banking-Trojaner und Identitätsdiebstahl

Klassisches Phishing stagniert. Betrugsversuche mit angeblichen E-Mails von Banken und Online-Shops, die auf eine mittlerweile gut gefälschte Website verweisen, spielen dank allgegenwärtiger Phishing-Toolbars und verbesserter Spamfilter eine immer geringere Rolle. Diesen Rückgang haben spezialisierte Trojanische Pferde aber mehr als wett gemacht - sog. Banking-Trojaner. Neuere Varianten stehlen aber nicht nur Zugangsdaten für Onlinebankkonten und Kreditkarteninformationen. Manche Spywareprogramme stehlen alle gespeicherten Zugangsdaten aus dem Protected Storage Area. Andere wie z.B. Bzub senden alle Inhalte von Webformularen an Angreifer. Auf diese Weise können Opfer von Trojanischen Pferden ihre gesamte Online-Identität verlieren. Immer häufiger werden so Unschuldige in die Machenschaften der Cyberkriminellen verstrickt.

Hier ein kurzer Überblick über die wichtigsten technischen Ausprägungen von Spyware

- Mit **Pharming** kann man unbemerkt auf falsche Webseiten geleitet werden. obwohl der korrekte Domainname im Browser eingegeben wurde. Basis dieser Angriffe ist die Ermittlung der IP-Adresse des Domainnamens. Dazu kann einerseits das DNS-System selbst angegriffen werden, aber auch die Client-Rechner bieten einige Angriffspunkte. Die Vertreter der Virenfamilie Qhosts ändern zum Beispiel die Einträge der HOSTS-Datei für bestimmte Webseiten oder sie tragen einen DNS-Server ein, der unter der Kontrolle der Angreifer steht.
- **Keylogger** zeichnen Tastaturaktionen auf und senden diese an unbefugte Dritte. Oft werden Keylogger auch nur aktiv, wenn bestimmte Bedingungen erfüllt sind – z. B. wenn die gerade geöffnete Webseite in einer oft sehr langen Liste von Domainnamen enthalten ist oder wenn Fenster mit bestimmten Titeln geöffnet werden.
  Als Gegenmaßnahme gegen Keylogger wurden Bildschirmtastaturen entwickelt. Die Reaktion darauf sind **Screenlogger**. Sie schießen entweder in regelmäßigen Abständen Bilder des gesamten Bildschirminhalts (z.B. **Rbot**) oder erzeugen bei jedem Mausklick eine Grafik des Umfelds der Maus. Manchmal werden die Bildsequenzen gleich in einen AVI-Film umgewandelt. Bestimmte Spionagetools (z.B. **Rbot**) nutzen WebCams und Mikrofone von infizierten Rechnern.
- Einige Schädlinge (z.B. **Torpig**) verändern das Aussehen und die Inhalte des Browsers. Sie sind in der Lage die Adresszeile mit der korrekten Adresse darzustellen, obwohl die Inhalte von einer anderen, gefälschten Domain kommen. Auch das Schloss, das eine verschlüsselte Verbindung symbolisiert, kann ungerechtfertigt eingeblendet werden. Andere Schädlinge (z.B. **Bancos**-Varianten oder **Nurech**) fügen entweder weitere Formularfelder in eine Seite oder zusätzliche Webseiten in den Dialog ein. Dabei bleiben bestehende SSL-Zertifikate aktiv. Ohne spezielle Tools ist es nicht möglich, zu erkennen, ob diese Daten gefälscht sind oder nicht.
- **Session Hijacker** übernehmen die Browsersitzung so, dass der Angreifer die Beträge und Kontoangaben zu seinen Gunsten ändert (z.B. Bancos). Dem Opfer werden weiterhin seine Angaben angezeigt und sogar der Kontostand wird entsprechend gefälscht. Auch hier wird der Betrug erst beim Blick auf die Kontoauszüge ersichtlich.
- Redirector lenken den Datenfluss so um, dass ein **Man-in-the-middle** Angriff möglich wird. Das kann ein lokaler Proxy sein oder ein Proxy-Server, der unter der Kontrolle des Angreifers steht. Darüber lässt sich die gesamte Netzkommunikation des Opfers belauschen. E-Mails, Chats, besuchte Webseiten, Formulardaten und Dateidownloads können so überwacht werden.
- **Sniffer** belauschen den Datenverkehr im Netzwerk des Opfers. Die Anzahl neuer Sniffer hat deutlich abgenommen.

- **Trojan-PSW-Programme** durchsuchen den gesamten PC nach verwertbaren Informationen. Das können E-Mail-Adressen sein oder Dateien mit bestimmten Inhalten oder eines bestimmten Dateityps. Diese Daten werden gepackt und an den Angreifer gesendet. Sehr beliebt sind auf dem System gespeicherte Login-Informationen, Registrierungsschlüssel und Passwörter (oder deren Hashes). Im Protected Storage Area werden die Passwörter von Webseiten und E-Mail-Accounts gespeichert, sofern ein Nutzer das allzu nützliche Angebot des Browsers oder E-Mailclients annimmt, die Passwörter zu speichern. Es ist also eine gute Idee, auf das automatische Speichern der Passwörter und Anmeldeinformationen zu verzichten. Ein prominenter Vertreter dieser Kategorie ist LdPinch.

Man sieht, die Methoden werden immer raffinierter und effektiver. Das sorgte auch 2007 dafür, dass die Zahl der Opfer und Schäden anstieg.

4.8 Online-Gamer im Visier

Beim Blick auf die Tabelle mit den aktivsten Virenfamilien fallen nicht nur die Backdoors auf. Der alte und neue Spitzenreiter - die Backdoor Hupigon - ist eine der Malwarefamilien, die am eifrigsten von Packern Gebrauch macht. Neue Versionen lassen sich mit einem Toolkit schnell und effizient zusammenklicken. Manche Varianten benutzen gleich 11 verschiedene Packer. Rbot geht mit aggressiven Methoden auf Schutzprogramme von Rechnern los.

	#2006	Virenfamilie	#2007	Virenfamilie
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

Tabelle 3: Top 10 Virenfamilien 2007

Interessant ist vor allem, dass mit „OnLineGames“ und „Magania“ zwei Passwortstehler in den Top 10 gelandet sind, die es auf Passwörter von Onlinespielen abgesehen haben. 2006 war schon bemerkenswert, dass mit Lineage ein solches Programm die vorderen Plätze erreicht hat. Die beiden Vertreter dieses Jahres konnten das Ergebnis des Vorjahres aber deutlich übertreffen. Das zeigt, dass Onlinespieler immer stärker angegriffen wurden. Die Anzahl der Passwortspione, die auf Onlinespieler zielen übersteigt mittlerweile die Anzahl der Banking-Trojaner.

4.9 Schadcode auf verschiedenen Plattformen - Keine Gefahr für Mobiltelefone

Wenn man die Plattformen betrachtet, für die Computerschädlinge entwickelt wurden, dann dominiert Windows eindeutig das Geschehen. Auf den Plätzen dahinter haben die webbasierten Angriffe in Javascript, HTML, VBSkript, PHP und Perl um mehr als das Dreifache zugelegt. Für Linux wurden lediglich 137 Schädlinge entdeckt.

Die vielfach herbei geredete Gefahr für Mobiltelefone konnten wir 2007 allerdings nicht ausmachen. Mit gerade einmal 22 neuen Schädlingen - die meisten davon halblegitime Spytools, die sich hauptsächlich an eifersüchtige Ehemänner oder besorgte Eltern richten - sinkt die Anzahl der Schädlinge für Symbian auf 1/3 des Wertes vom Vorjahr und ist mit Platz 14 nicht mehr in der Top 10 vertreten.

	#2007	Plattform	#2006	Plattform
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

Tabelle 4: Top 10 Plattformen 2006 und 2007

5. Ausblick 2008

Für 2008 erwarten wir, dass die bewährten Methoden beibehalten und verfeinert werden. In diese Kategorie fallen folgende Punkte:

- **Noch mehr internetbasierte Malware.** Die neuen Möglichkeiten des Web 2.0 werden auch verstärkt von Onlinekriminellen genutzt. Besonderes Augenmerk liegt hier auf Sicherheitslücken in Webanwendungen über die man Schadcode in die resultierenden Webseiten einschleusen kann. Auch Angriffe auf die Datenbanken hinter den Webanwendungen werden zunehmen. Kommende (Versionen von) Tools werden diese Prozesse stark vereinfachen.
- **Personalisierte Massenmails.** Die durch Datendiebstähle gewonnenen Informationen werden im kommenden Jahr dazu genutzt, um Spam- und Phishing-Mails gezielt an passende Personengruppen zu versenden. Diese E-Mails werden persönliche Anreden enthalten und die Absenderadresse wird so gefälscht, dass sie von einem Bekannten geschickt wurde.
- **Noch mehr Spam?** Insgesamt wird die Anzahl der Spammails kaum zunehmen. Spam wird aber deutlich zielgerichteter und damit effektiver. Blog- und Forenspam wird im kommenden Jahr ein massives Problem.
- **Phishing per E-Mail und Website wird weltweit im Bankenbereich deutlich abnehmen.** Neue Ziele sind OnlineShops, Social Networking Plattformen (MySpace, Facebook, LinkedIn etc.), Jobbörsen und OnlineGames. Prognose: Die Anzahl der missbrauchten Marken („Brands“) wird im kommenden Jahr deutlich ansteigen.
- **Ein hartes Jahr für Malwareforscher.**
  Die Masse an Malware wird nicht abnehmen. Die Komplexität der Malware wird aber steigen. Verschlüsselung, spezielle Runtime-Packer, Tools für Codeverschleierung, gezielt ausgelieferte Malware sind nur einige der anstehenden Herausforderungen.

Wir erwarten aber auch einige Neuheiten:

- **Mehr Erpressung.** Ransomware war 2007 sehr selten. Wir erwarten im kommenden Jahr Verbesserungen in der Botnetzinfrastruktur und bei den Bullet-Proof-Hostern (der bekannteste ist das Russian Business Network RBN). Wenn somit die Anonymität des Angreifers sichergestellt werden kann, wird die Anzahl der Erpressungen wegen verschlüsselter Office- und Bilddateien zunehmen. Abhilfe: Datensicherung
- **Virtualisierung.** Seit mehreren Monaten enthalten alle neu ausgelieferten Prozessoren Funktionen, mit denen sich Virtuelle Maschinen sehr einfach und effektiv nutzen lassen. Diese Virtualisierungsfunktionen können u.a. zur Erstellung neuartiger Rootkits genutzt werden (Stichwort Bluepill). Andererseits bietet die Virtualisierung viele Möglichkeiten um effektive Schutzkonzepte zu realisieren. In diesem Bereich werden sowohl die Angreifer als auch die Verteidiger verstärkt forschen
- **Wachsende und neue Technologien.** Vista und MacOSX stehen kurz davor, die kritische Marke von 10% Marktanteil zu überschreiten. Dadurch werden sie für Cyberkriminelle immer interessanter und die Anzahl der Angriffe auf diese Systeme wird steigen. Bei Vista könnten sich Gadgets als neues Einfallstor etablieren. Auch die friedliche Oase der Apple-Nutzer wird 2008 einige Erschütterungen hinnehmen müssen.
- Welche **neuen Technologien** in den Fokus von Hackern und Crackern geraten, lässt sich nur schwer prognostizieren. Mit größeren Attacken rechnen wir vorerst nicht. Wir erwarten aber Testangriffe auf VoIP und internetfähige Spielekonsolen.

Geschützt. **Geschützter. G DATA.**