G DATA

Malware-Report

Halbjahresbericht Januar-Juni 2008

Ralf Benzmüller & Thorsten Urbanski

G DATA Malware-Report Januar-Juni 2008

Ralf Benzmüller & Thorsten Urbanski

1. Zusammenfassung: Explosionsartige Zunahme von Malware

Die Konsolidierungsphase der Malware-Industrie trägt 2008 ihre verheerenden Früchte. Galt 2007 mit einer Zuwachsrate von 300 Prozent im Vergleich zu 2006 als das Malware-Jahr schlechthin, bricht 2008 bereits jetzt alle Rekorde. Allein in den ersten drei Monaten des laufenden Jahres wurden mehr neue Schädlingen in Umlauf gebracht als im Vorjahr (133.253).

Mit einer Abnahme der Malware-Flut, ist in den kommende Monaten nicht zu rechnen. Nach Einschätzung der G DATA Security Labs könnte die Marke von mehr als einer halben Million neuer Schädlinge schon im 3. Quartal 2008 geknackt werden – dies käme einer Zuwachsrate von deutlich über 400 Prozent gleich.

Datendiebstahl und die Einbindung gekaperter PCs in Botnetze sind nach Analysen der Schadcode-Familien primäre Ziele der Kriminellen. Daher verzeichnen Downloader (37.546) und Backdoors (44.156) die meisten Neuzugänge im ersten Halbjahr 2008.

Schadcode	Neuzugänge	Anteil in Prozent
Backdoors	75.027	23,6 %
Downloader/ Dropper	64.482	20,3 %
Spyware	58.872	18,5 %
Trojan. Pferde	52.087	16,4 %
Adware	32.068	10,1 %

Tabelle 1: Malware Top Five Januar bis Juni 2008

1.1 Minenfelder im Netz

Die Bedrohung durch präparierte Webseiten hat deutlich zugenommen. Die von G DATA 2007 prognostizierte Verlagerung von Schadcode ins Internet ist längst Realität.

Die Täter nutzen bei diesem Konzept Sicherheitslücken im Browser oder Browser-Plugins, wie z. B. Flash, Real Player oder Adobe Reader. Entgegen landläufigen Vermutungen lauern diese Gefahren nicht so häufig in den „Rotlichtbezirken" des Internets, sondern sind überwiegend auf populären Webseiten zu finden.

1.2 Smartphones: Marketing-Luftblase geplatzt

Der Hype um Smartphone-Viren spiegelt sich in den aktuellen Zahlen nicht wider: Lediglich 41 neue Schädlinge brachten die Malware-Autoren bis Ende Juni 2008 in Umlauf. Bei den meisten dieser Schadprogramme handelt es sich nach G DATA Analysen um halblegale Überwachungssoftware oder Machbarkeitsstudien (Proof-of-Concept).

Noch deutlicher wird diese Tatsache, wenn man die Gesamtzahlen der neuen Smartphone-Schädlinge seit Januar 2006 betrachtet - 145 neue Schädlinge für alle Smartphone-Betriebssysteme. Von einer echten Gefahr für Besitzer dieser Geräte zu sprechen, erscheint zum jetzigen Zeitpunkt überzogen.

1.3 Fazit und Ausblick

Nach Einschätzung von G DATA ist von einer Sommerpause der Malware-Industrie in den kommenden Wochen und Monaten nicht auszugehen. Der Ausstoß neuer Malware wird weiter zunehmen und könnte bisher ungeahnte Dimensionen erreichen.

Die anstehenden sportlichen Großveranstaltungen – wie beispielsweise der Olympiade in Peking – könnte die Situation weiter verschärfen. Online-Kriminelle nutzen globale Events als Aufhänger, um ihrerseits verstärkt auf Datenjagd zu gehen und Kasse zu machen. Mit einem erhöhten Ausstoß an Schad-E-Mails ist daher kurzfristig zu rechnen.

Smartphone-Viren werden hingegen auch in diesem Jahr kaum eine Rolle spielen, da die Verbreitung derartiger Schädlinge immer mit einer Nutzerinteraktion verbunden und bei der Verbreitung via Bluetooth räumlich begrenzt ist und last but not least erfolgversprechende eCrime-Geschäftsmodelle fehlen. Online-Kriminalität ist schließlich ein Profi-Geschäft, das nach marktwirtschaftlichen Gesichtspunkten betrieben wird.

2. Einleitung

Die Entwicklung und Verbreitung von Malware ist ein absolutes Profigeschäft und verursacht jährlich Schäden in Milliardenhöhe. Die Täter agieren längst nicht mehr in einzelnen Cyber-Crime-Klustern, sondern arbeitsteilig in weltumspannenden Netzwerken. Malware-Autoren, Spammer und Datenhehler arbeiten Hand in Hand und sind so in der Lage, das gesamte Dienstleistungsspektrum im Bereich Online-Kriminalität abzudecken.

In diesem eCrime-Kreislauf ist es für Kriminelle aus ökonomischer Sicht unerlässlich, in immer kürzeren Intervallen neue Malware-Kreationen zu entwickeln und zu verbreiten, um so möglichst viele Rechner in kürzester Zeit zu infizieren, auszuplündern und in die Botnetzinfrastruktur zu integrieren.

Was Ende 2007 von G DATA prognostiziert wurde, ist 2008 eingetreten: Die Zahl neuer Schädlinge hat explosionsartig zugenommen! Allein in den ersten sechs Monaten des laufenden Jahres wurden mehr als 318.000 neue Schädlinge in Umlauf gebracht - 2,4 mal mehr als im gesamten Jahr 2007.

Die Verbreitung von Malware erfolgt primär über Webseiten, die massenhaft mit Tools zur Auslieferung von Drive-by-Downloads versehen sind. E-Mailanhänge haben ihre führende Position als Träger von Schaddateien schon im letzten Jahr eingebüßt und dienen eher dazu, Opfer auf präparierte Internetseiten zu locken. Die Mehrzahl der Neuinfektionen erfolgt mittlerweile durch Webseiten. Das Internet gleicht somit einem Kriegsgebiet mit groß angelegten Minenfeldern!

3. Wichtige Ereignisse und Entwicklungen im ersten Halbjahr 2008

In den ersten sechs Monaten von 2008 sind die Aktivitäten der Online-Kriminellen ungebremst hoch. So feierte der sogenannte Sturmwurm – von vielen bereits Ende 2007 totgesagt - eine Geburtstags-Party der besonderen Art.

Die Sturmwurm-Gang hat die Botnetze so aufgeteilt, dass Rechner hinter einem Router nur Spam versenden. Rechner ohne Router werden dazu genutzt, um Spam- und Phishingseiten zu hosten. Die Auflösung eines Domainnamens verweist ständig auf andere Botnetzrechner (Fast Flux). Auf diese Weise ist es deutlich schwieriger die schädlichen Webseiten vom Netz zu nehmen.

Immer mehr Schadcode wird über kompromitierte Webseiten ausgeliefert. Spezielle Toolkits erleichtern es Online-Kriminellen, Malware auf Webservern zu hinterlegen. Und dann ist eine alte Technologie wieder auferweckt worden: Bootsektorviren enthalten jetzt keine Dateiinfektoren mehr, sondern verstecken Rootkits.

3.1 Der „Sturmwurm“[1] feiert Geburtstag

Die Betreiber des Storm-Botnetzes haben im ersten Halbjahr die Leistungsfähigkeit ihrer Zombie-Armeen eindrucksvoll unter Beweis gestellt. Zugleich nutzen die Täter als Trittbrettfahrer internationale Feier- und Gedenktage. Zwar begannen die Täter den Valentinstag (14. Februar) bereits Mitte Januar, dies tat dem Erfolg leider keinen Abbruch. Außerdem im Programm der Sturm-Bande waren wieder „lustige“ Postkarten und Webseiten zum 1. April. Hier wurden weltweit eine Vielzahl von Rechnern infiziert und in Zombies verwandelt.

Nach einer relativ ruhigen Phase im letzten Quartal 2007 ist Storm jetzt wieder aktiv und wird es voraussichtlich auch bleiben!

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

Hintergrundinformation zum Storm-Botnetz:

Im Januar 2007 zog der Sturm Kyrill über weite Teile Europas und richtete enorme Schäden an. Kaum war der Wind abgeflaut, kursierten E-Mails, die im Anhang readmore.exe weitere Informationen über die Folgen des Sturms versprachen. So bekam der Sturmwurm seinen Namen (ungeachtet der Tatsache, dass es sich nicht um einen Wurm, sondern ein Trojanisches Pferd handelt und von der gleichen Gruppe schon Ende Dezember 2006 E-Mails mit Festtags- und Neujahrsglückwünschen verbreitet wurden).

Ziel der E-Mails ist es nach wie vor, die infizierten Rechner in ein Botnetz zu integrieren, das zum Versenden von Spam und für verteilte Überlastangriffe (DDoS) genutzt wird. In den folgenden Monaten gab es weitere Wellen mit Falschmeldungen („Saddam Hussein alive!" oder „Fidel Castro dead") und Virenwarnungen. Auch diese Mails enthielten den Schadcode als Dateianhang.

Im Juni 2007 fand dann ein Wechsel der Taktik statt: ECards und Glückwunschkarten lockten Nutzer auf Webseiten, wo zum Betrachten der Karte eine (schädliche) Datei installiert werden muss. Zusätzlich wird im Hintergrund versucht, Sicherheitslücken der Browser bzw. von Browserkomponenten zu nutzen. Die Infektion erfolgt dann während des Betrachtens der Grußkarte. Weitere Maschen waren der Download von Codecs zum Betrachten von Videos oder Software zur sicheren Datenübertragung oder zum Schutz der Privatsphäre. Auch das Anwerben von Betatestern wurde als Masche genutzt.

Im September vergangenen Jahres wurden wieder aktuelle Ereignisse zum Anlass genommen, um Opfer auf schädliche Webseiten zu locken. Zunächst begann es mit dem „Labor Day", gefolgt vom Start der neuen Football-Saison der NFL. Hier wurden die gefährlichen Downloads als „Free NFL Game tracker" angepriesen. Weitere Maschen bezogen sich auf Online-Spiele, „Krackin"-Software, Haloween und wieder Weihnachts- und Neujahrsglückwünsche.

Im Herbst war es eine Weile ruhig um das Sturm-Botnetz. Offenbar haben die Täter ihre Aktivitäten von St. Petersburg nach China und in die Türkei verlegt, um nun umso vehementer zu agieren.

3.2 Rootkits im Bootsektor

Beim Einschalten des Rechners beginnt das Rennen zwischen Malware und Security-Software. Je früher es gelingt, die Kontrolle über das System zu übernehmen, desto besser kann eine Security-Software schützen oder umgekehrt Malware den Schutzfunktionen entgehen.

Alte Taktik neu aufgewärmt

Mit Backdoor.Win32.Sinowal ist Anfang Januar ein Schädling „in-the-wild" aufgetaucht, der den MBR überschreibt, um dann Tarnfunktionen im Windows XP Kernel zu verankern. Diese neue Tarntechnologie wird genutzt, um die Diebstahlfunktionen für Online-Banking zu verstecken. Im ersten Halbjahr 2008 sind 97 Varianten dieses Schädlings aufgetreten.

Das Einschleusen von Schadcode in den Bootsektor ist aber ein eigenständiges Modul und unabhängig von der Schadfunktion. Sie könnte schon bald auch in andere Malware integriert werden.

Die Malware hat dabei meist leichtes Spiel, unter XP ist es Standardanwendern möglich den MBR zu überschreiben. Unter Vista ist das etwas schwieriger.

Es gibt aber auch Schutzmechanismen: Oft bietet das BIOS die Möglichkeit den MBR mit einem Schreibschutz zu versehen. Möglicherweise ist jetzt ein guter Zeitpunkt das zu tun. Die Bootsektorviren der frühen Virentage wurden erkannt, indem man von einer sauberen Diskette bootete.

Die Boot-CD von G DATAs Virenschutzlösungen kann die aktuellen MBR-Rootkits zuverlässig erkennen.

Nach Einschätzung der G DATA Security Labs ist es nur eine Frage der Zeit bis weitere Schädlinge diese Technologie zur Tarnung nutzen.

Funktionsweise

Die erste Stelle im Bootprozess, wo die Kontrolle an veränderbare Software übergeben wird, ist der Master Boot Record (MBR) einer Festplatte bzw. der Bootsektor von anderen Bootmedien (z.B. Floppy Discs). Der MBR ist der erste Sektor einer Festplatte. Dort ist u.a. der Bootloader und die Partitionstabelle der Festplatte untergebracht. Der Bootloader enthält ausführbaren Code und ermittelt die Bootpartition und lädt die wichtigen Teile des Betriebssystems (z.B. Kernel).

Weil der Bootsektor die erste Stelle ist, in der fremder Code in ein System eingeschleust werden kann, waren schon die ersten Viren wie Brain, Stoned und Michelangelo sog. Bootsektorviren. Es ist also keineswegs neu, dass Schadcode den Bootsektor überschreibt, um frühzeitig die Kontrolle zu übernehmen.

Leider ist es unter Windows XP immer noch möglich, den MBR zu überschreiben. Davon machten aber die wenigsten Schädlinge der letzten Jahre Gebrauch. 2005 hat Derek Soeder von eEye Digital Security mit BootRoot die Möglichkeit vorgestellt, dass ein Rootkit im MBR aktiviert werden kann. Die Tarnfunktionen werden dann aktiv, bevor überhaupt das Betriebssystem geladen ist. 2007 veröffentlichten Nitin und Vipin Kumar von NVLabs das VBootkit, mit dem Tarnfunktionen für Vista implementiert wurden. Sowohl BootRoot als auch VBootkit waren technische Machbarkeitsstudien (sog. Proof-of-Concepts) ohne eigentliche Schadfunktion. Sie sind nie im Zusammenhang mit Malware aufgetreten. Das hat sich mit Sinowal nun geändert.

3.3 Minenfeld Internet: anklicken – infizieren - ausrauben

Die Bedrohung durch infizierte und präparierte Webseiten hat im ersten Halbjahr 2008 deutlich an Fahrt zugenommen, so dass das Internet mittlerweile eher einem Kriegsgebiet gleicht.

Aktuell erfolgen mehr als 70 Prozent aller Schadcode-Infektionen durch den Besuch von Internet-Angeboten. Mit einer weiteren Zunahme ist gerade im Zuge von Sport-Events – wie der Olympiade in Peking - zu rechnen. Schlecht gewartete und gecrackte Fan-Protale, könnten Tätern hier ideale Plattformen bieten.

Vorgehensweise der Online-Banden:

Nur die wenigsten E-Mails, mit denen sich aktuelle Schädlinge verbreiten, enthalten noch Dateianhänge. Die meisten verweisen entweder direkt auf eine Schaddatei oder bieten die schädliche Datei auf einer Webseite zum Download an. Oft werden dabei Täuschungsmanöver vorgeschoben wie aktuelle Nachrichten, elektronische Grußkarten, angebliche Abbuchungen oder Codecs für interessante Filme etc.

Schadcode, der in Webseiten eingeschleust wurde, versucht Schwachstellen im Browser oder in Browserkomponenten (wie Adobe Reader oder Flash) auszunutzen, um den Rechner unbemerkt beim Aufruf der Seite zu kapern. Entgegen der Annahme vieler Anwender, lauern diese **Drive-by-Downloads** nur selten in den Rotlichtbezirken des Internets.

Die überwiegende Zahl der Infektionen geht von normalen, gut besuchten Webseiten aus. Dabei werden Werbeeinblendungen missbraucht oder Webserver selbst gecrackt. Das kann z.B. durch schwache oder gestohlene FTP-Passwörter geschehen oder indem Sicherheitslücken in gängigen Webanwendungen wie Content Management Systeme oder Bulletin Boards ausgenutzt werden.

Einfallstor Forensoftware

Im ersten Drittel von 2008 sind verstärkt Massenangriffe auf Schwachstellen in Webanwendungen aufgetaucht. So sorgten z.B. Fehler in der Forensoftware phpBB seit Februar für tausende von verseuchten Webseiten. Im April wurden Hundertausende Webseiten per SQL Injection angegriffen und lieferten einen schädlichen IFRAME an Besucher der Webseite aus. Auch die Anzahl der Flash-basierten Schädlinge hat deutlich zugenommen.

Für die so übernommenen Server sind noch bessere Tools veröffentlicht worden, mit denen auf einer gekaperten Website Schadcode hinterlegt werden kann, der einem Besucher unbemerkt beim Besuch der Webseite untergeschoben wird.

Anfang des Jahres erschien FirePack, das mittlerweile sogar in einer chinesischen Version vorliegt. Im Februar tauchte ein neues Multi-Exploit Toolkit auf. Aber auch MPack, IcePack, TrafficPro, Nuclear Malware Kit, Web-Attacker, SmartPack uvm. werden im Internet zu Preisen zwischen 40$ und 3000$ gehandelt.

Es wird deutlich, dass auf jeder Webseite Schadcode lauern kann. Der Virenschutz sollte daher unbedingt so eingestellt sein, dass er den HTTP-Datenstrom prüft bevor der Browser ihn verarbeitet.

Um das zu überprüfen, versuchen Sie die Textversion der EICAR-Testdatei herunterzuladen. Dabei handelt es sich um ein DOS-Programm, das den Text „EICAR-STANDARD-ANTIVIRUS-TEST-FILE!“ ausgibt. Dieses an sich harmlose Programm wird allerdings von jeder Antiviren-Software als Schädling erkannt.

Wenn sie die Textversion dieser Datei von http://www.eicar.org/download/eicar.com.txt herunterladen erhalten Sie entweder eine Warnmeldung, die den Zugang zur Seite verhindert oder im Browser erscheint eine Zeile mit kryptischem Text (inkl. der o.g. Textausgabe). Im letzteren Fall ist ihr Rechner gegenüber Angriffen aus dem Internet völlig ungeschützt. Genau wie dieser Text kann Skriptcode in den Browser geladen werden. Der wird zunächst ausgeführt und erst wenn der Browser die Dateien in „Temporary Internet Files“ abspeichert merkt der Virenschutz, dass ein Schädling aktiv war - die Warnung kommt dann aber zu spät.

4. Zahlen und Trends zu Malware im ersten Halbjahr 2008

Die Anzahl neuer Malware ist erneut deutlich angestiegen – mitverantwortlich hierfür sind nicht zuletzt auch Laufzeitpacker. Nach wie vor wird das Geschehen von Botnetzen, Spyware und Adware bestimmt. Der Spamanteil hat sich auf hohem Niveau eingepegelt und die Spammer haben ein paar neue Tricks parat. Die folgenden Abschnitte erläutern die Einzelheiten.

4.1 Malware-Sintflut 2008

2008 könnte bereits jetzt in die Malware-Geschichte eingehen. In bisher einmaliger Weise haben es die Täter geschafft, in drei Monaten das Rekordjahr 2007 in den Schatten zu stellen. Bereits Ende März 2008 registrierten die Experten der G DATA Security Labs mehr neuen Schadcode als im gesamten Vorjahr.

Bis zum Ende des Jahres rechnet G DATA mindestens mit einer Vervierfachung der Anzahl neuer Schädlinge. Der Grund dafür liegt in der Tatsache, dass Signaturscanner nur bekannte Malware finden. Das nutzen Malwareschreiber aus. Schadcode wird - wie im letzten Malware Report unter „Malware-Recycling“ beschrieben - mit Hilfe von Packern und anderen Verschleierungstools so umgeformt, dass die Virensignaturen nicht mehr greifen. Die Funktionalität des eigentlichen Schadcodes bleibt davon unberührt. Der so geänderte, nicht mehr erkannte Code wird umgehend ausgeliefert.

Ein weiterer Mechanismus, der ebenfalls zu zahlreichen neuen Versionen führt, wird häufig bei Backdoors eingesetzt. Die meisten Backdoors verfügen über eine Update-Funktion. Und von der wird ausgiebig als Tarnmechanismus Gebrauch gemacht. Die Backdoors werden so häufig aktualisiert, dass der Virenscanner immer eine Variante prüft, die er noch nicht kennt. Denn auch hier wird vorher sichergestellt, dass eine neue Version nicht vom Signaturscanner erkannt wird.

Die Reaktionszeit zwischen Viren-Outbreak und Bereitstellung entsprechender Signaturen spielt hierbei eine entscheidende Rolle.

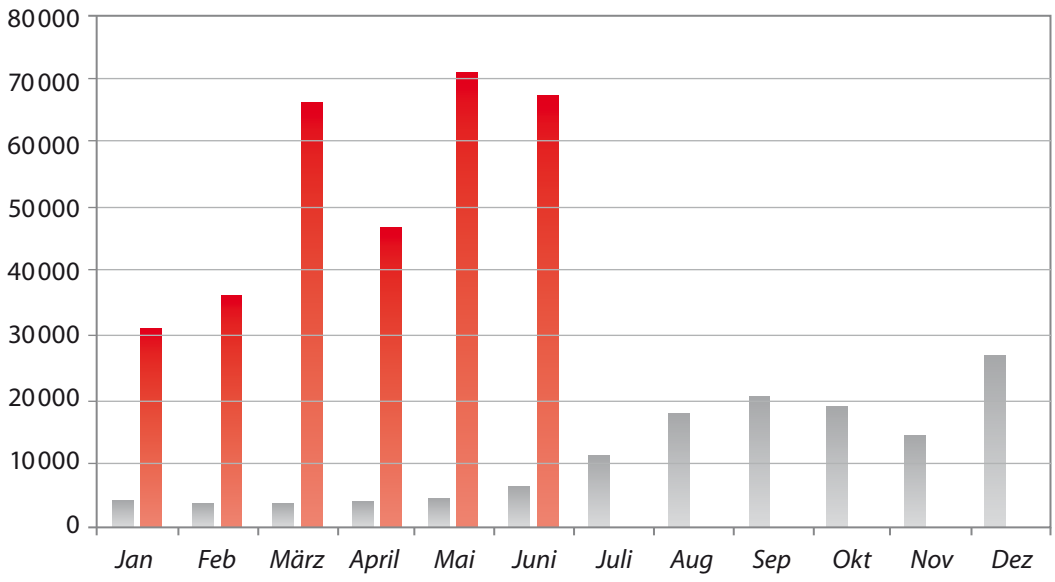


Diagramm 1: Vergleich - Gesamtzahl neuer Malware 2007 zu den ersten 6 Monaten in 2008

4.2 Smartphone-Viren: Marketing oder reale Gefahr?

Die vielfach heraufbeschworene Gefahr für Smartphone-Besitzer war von den G DATA Security Labs auch in der ersten Hälfte des laufenden Jahres nicht auszumachen. Bei den insgesamt 41 neuen Schädlingen für Smartphones handelte es sich fast ausschließlich um Proof-of-Concept Studien, mit denen die technischen Möglichkeiten ausgelotet wurden oder um halblegale Überwachungssoftware für besorgte Eltern und eifersüchtige Ehepartner.

Die seit Jahren anhaltende Stagnation bei dieser Malware-Gattung ist nicht verwunderlich: Die Verbreitung scheitert einerseits an der geringen Reichweite von Bluetooth, an der unzureichenden Zahl an erreichbaren MMS-fähigen Smartphones und nicht zuletzt daran, dass sowohl der Verbindungsaufbau als auch die Installation vom Benutzer bestätigt werden müssen.

Der entscheidende und häufig außer Acht gelassene Grund ist jedoch auf ökonomischer Seite zu suchen: Online-Kriminalität ist Big Business und damit den Gesetzen des Marktes unterworfen. Das wichtigste Ziel ist es, mit möglichst wenig Aufwand möglichst hohen Profit zu machen. Die Entwicklung von Smartphone-Malware ist für die Täter mit hohen Kosten (nicht nur finanzielle) verbunden. Ein „Return on Investment“ ist bisher für die Malware-Industrie nicht realistisch. In anderen Bereichen ist bislang mit weniger Aufwand mehr zu erreichen.

Es fehlen also einerseits profitable Geschäftsmodelle und andererseits bergen bislang alle Wege, um letztlich ans Geld zu kommen die Gefahr, erwischt zu werden. Die häufig publizierte Gefahr erscheint daher eher marketingpolitisch begründet und entbehrt zum jetzigen Zeitpunkt jeglicher Grundlage.

Monat	Anzahl
Januar 2008	6
Februar 2008	2
März 2008	9
April 2008	1
Mai 2008	15
Juni 2008	8

Tabelle 2: Anzahl neuer Smartphone-Malware

4.3 Botnetze und Spyware an der Spitze

Die Verteilung der Malware nach verschiedenen Typen wird in Tabelle 3 dargestellt. In allen Kategorien - außer bei den klassischen Viren - übertrifft die Anzahl neuer Varianten in der ersten Hälfte von 2008 bereits die Anzahl des gesamten Jahres 2007. Backdoors behalten mit knapp einem Viertel der neuen Malware die Spitzenposition, obwohl Ihr Anteil gegenüber 2007 deutlich gesunken ist. Sie bilden die Grundlage von Botnetzen, die weiterhin die effektivsten Instrumente für Onlinekriminelle darstellen. Gut ein Fünftel der neuen Schädlinge sind Downloader und Dropper.

Diese Malware-Familien werden von den Tätern genutzt, um Backdoors und weitere Schädlinge auf Rechner zu installieren. Mit einem Anteil von mehr als 20 Prozent belegten diese in den ersten sechs Monaten Platz zwei bei neuen Schädlingen. Der Anteil von Spyware ist deutlich zurückgegangen, konnte aber den dritten Platz verteidigen.

	# 2008 T1	Anteil	# 2007	Anteil 2007	Differenz
Backdoors	75.027	23,6 %	41.477	31,0 %	362 %
Downloader/ Dropper	64.482	20,3 %	28.060	21,0 %	460 %
Spyware	58.872	18,5 %	29.887	22,4 %	394 %
Trojan. Pferde	52.087	16,4 %	13.787	10,3 %	756 %
Adware	32.068	10,1 %	7.654	5,7 %	838 %
Tools	12.203	3,8 %	1.731	1,3 %	1.410 %
Würmer	10.227	3,2 %	4.647	3,5 %	440 %
Dialer	4.760	1,5 %		n.a.	
Exploit	1.613	0,5 %		n.a.	
Rootkits	1.425	0,4 %	559	0,4 %	510 %
Viren	327	0,1%	2.127	1,6 %	31 %
Sonstige	5.170	1,6 %	3.688	2,8 %	280 %
Gesamt	318.261	100,0 %	133.617	100	476 %

Tabelle 3: Anzahl und Anteil neuer Malwaretypen im ersten Halbjahr 2008 und2007 und Veränderung gegenüber 2007

4.4 Adware - explosionsartiger Anstieg

Schon 2007 hat sich die Anzahl neuer Adware verfünffacht. Nun ist er erneut deutlich gestiegen. Über acht mal mehr neue Adware wurde Anfang 2008 gegenüber dem Jahresdurchschnitt 2007 entdeckt. Das ist abgesehen von den Tools die nachhaltigste Steigerung. Entführte Startseiten und Dateien mit möglicherweise unerwünschtem Inhalt wie z.B. Werbeeinblendungen oder manipulierten Suchergebnissen erfreuen sich in der eCrime-Ökonomie weiterhin einer großen Beliebtheit.

Der häufigste Vertreter dieser Gattung ist Virtumonde. Der Schädling integriert sich als Browser Helper Object in den Internet Explorer und zeigt dann Werbung in Pop-Up-Fenstern an. Die auf diese Weise massenhaft erzeugten künstlichen Klicks füllen die Kassen der Adware-Autoren.

Adware: WinFixer gibt sich als AntiVirus Programm. Nach der Installation entführt er die Startseite des Browsers und zeigt ständig Werbe-PopUps.

Eine andere Art der Bezahlung basiert auf der Installation von Software. Für jede Installation werden Beträge von wenigen Cent bezahlt. Auch hier macht es die Masse. Der deutliche Anstieg von neuer Malware zeigt, dass sich dieses Geschäft lohnt.

4.5 Spam nimmt wieder zu

Im Januar ist der Anteil an Spam auf ca. 60 Prozent zurückgegangen, hat sich aber bald darauf auf ca. 70% eingependelt. Seit März liegt der Anteil an Spam-Mails wieder über 80%, mit einem Spitzenwert von 94% im April und betrug Ende Juni 2008 87%.

Die häufigsten Themen sind in folgender Tabelle kategorisiert:

Thema	Proz. Anteil
Sexuelle Leistungssteigerung	30 %
Medikamente	22 %
Replicas	21 %
Akademische Titel	5 %
Software	3 %

Tabelle 3: Top Five der Themen von Spam-Mails in der ersten Hälfte 2008

Nach wie vor wird ein Großteil aller Spam-Mails per Botnetz verschickt. In der ersten Hälfte 2008 waren es im Durchschnitt 85%. Täglich sind zwischen 5 und 10 Millionen Zombies am Spamversand beteiligt. Jeden Tag werden zwischen 200.000 und 500.000 (im Schnitt 360.000) Rechner in neue Zombies verwandelt. Die meisten davon in Deutschland, Italien und Brasilien (vgl. Tabelle 4). So werden täglich ca. 130 Milliarden Spam- Phishing- oder Malware-Mails versendet.

Land	Proz. Anteil
Brasilien	10,2%
Deutschland	9,3%
Italien	8,9%
Türkei	8,3 %
China	6,6 %

Tabelle 4: Top Five der Länder mit den meisten Zombie-PCs

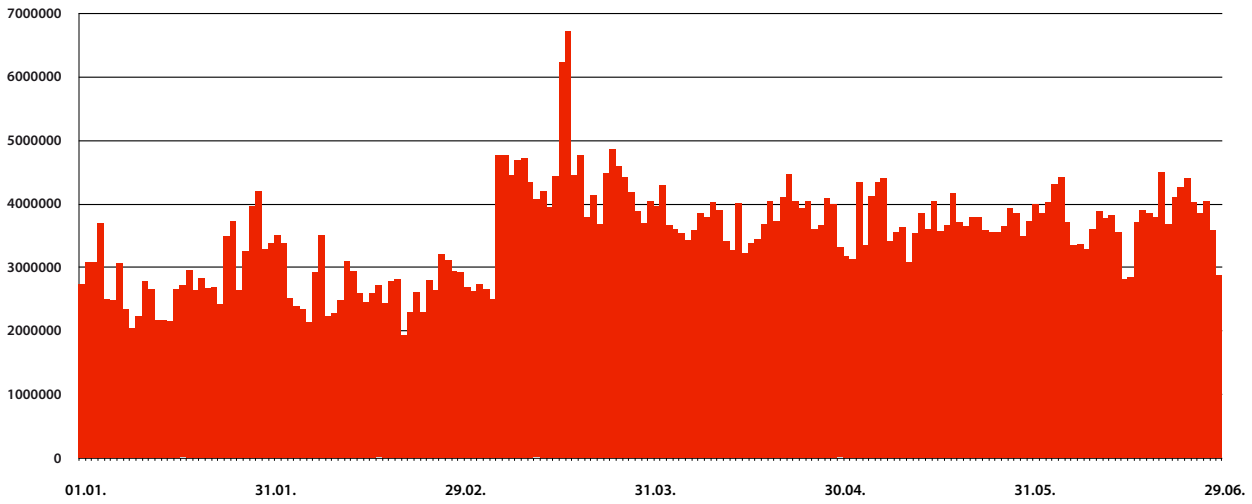
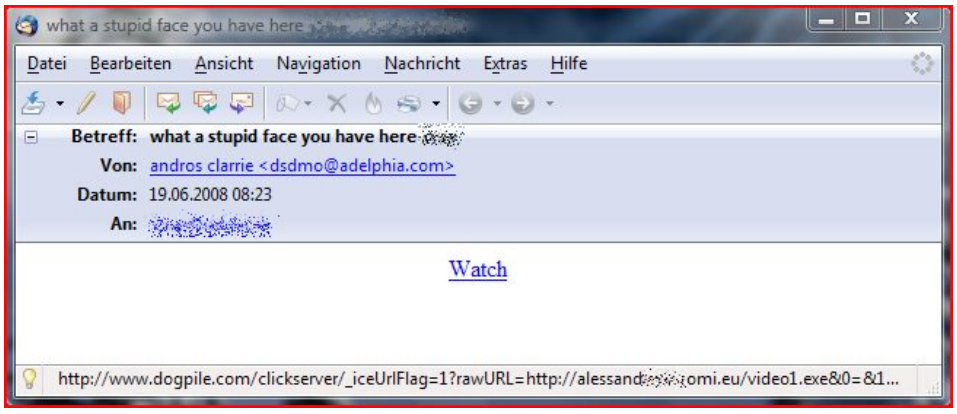


Diagramm 2: Spam-Mails im ersten Halbjahr 2008

Um die Spamfilter zu überlisten, greifen Spammer auf bekannte und vertrauenswürdige Seiten zurück. Dabei nutzen Sie z.B. die Umleitungsfunktionen von Google, Yahoo und anderen Seiten. Nutzer und Spamfilter wird so vorgegaukelt, dass ein vertrauenswürdige Seite aufgerufen wird.



Ein ähnlicher Ansatz wird auch bei Bildern und Webseiten verfolgt. Sie werden in beliebten Portalen wie Flickr oder Blogspot gehostet. Reputationsbasierte Erkennungstechnologien werden so überlistet.

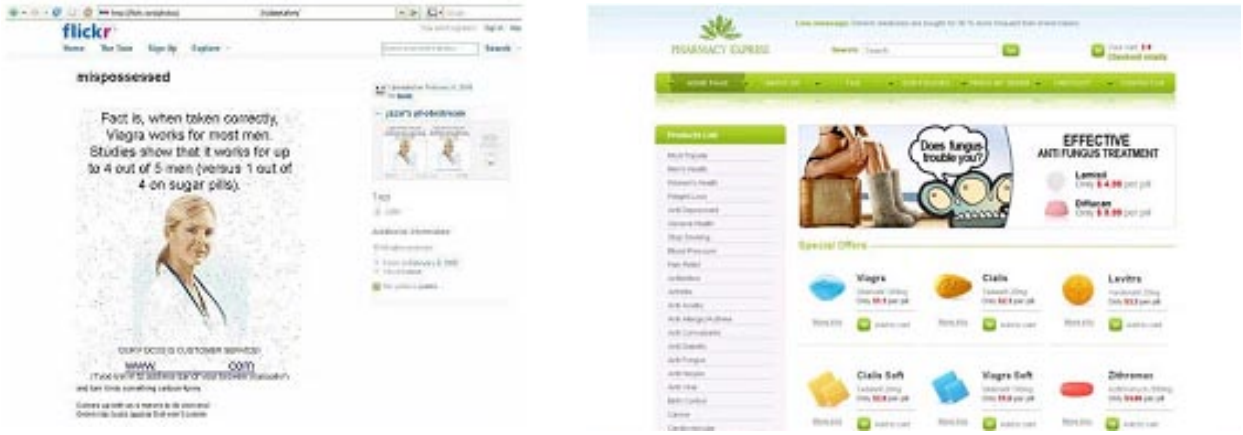


Diagramm 3: Bilder und Spam gehostet bei Flickr und Blogspot

4.6 Online-Spieler im Visier

Beim Blick auf die aktivsten Virenfamilien in Tabelle 5 fallen nicht nur die Backdoors Hupigon und Bifrose auf. Der alte und neue Spitzenreiter - die Backdoor Hupigon - ist eine der Malwarefamilien, die am eifrigsten von Laufzeitpackern Gebrauch macht. Neue Versionen lassen sich mit einem Toolkit schnell und effizient zusammenklicken. Manche Varianten benutzen gleich 11 verschiedene Packer.

Trojanische Pferde wie OnlineGames und Magania (GameMania-Spiele), die Zugangsdaten für Online-Spiele stehlen, haben ihre Position in den aktivsten Malwarefamilien ausgebaut. D.h. Online-Spieler stehen nach wie vor im Visier der Datendiebe. Zugangsdaten für Onlinespiele sowie Charaktere und Gegenstände aus Spielen werden in zahlreichen Foren für echtes Geld gehandelt. Das zieht auch Betrüger aus dem echten Leben an.

	#2006	Virenfamilie	#2007	Virenfamilie
1	32.383	Hupigon	16.983	Hupigon
2	19.415	OnLineGames	8.692	OnLineGames
3	13.922	Virtumonde	3.002	Rbot
4	11.933	Magania	2.973	Banker
5	7.370	FenomenGame	2.848	Banload
6	7.151	Buzus	2.627	Zlob
7	6.779	Zlob	2.533	Virtumonde
8	6.247	Cinmus	1.922	Magania
9	6.194	Banload	1.882	LdPinch
10	5.433	Bifrose	1.751	BZub

Tabelle 3: Top 10 Aktivste Virenfamilien 1. Hj. 2008 und 2007

Die weiteren Plätze in Tabelle 5 werden von folgenden Schädlingen belegt:

- **Virtumonde:** Adware, die sich in den IE integriert und PopUp-Werbung anzeigt.
- **FenomenGame:** Fehlerkennung wegen automatischer Erstellung von Signaturen
- **Buzus:** Spy-Trojan und Keylogger mit Backdoor
- **Zlob:** beliebter Trojan-Downloader, der auch Einstellungen des IE ändert um Pornoseiten anzuzeigen und Rogueware zu installieren
- **Cinmus** ist ein Adware-Programm, das sich in den Internet Explorer integriert und Werbe-PopUps anzeigt.
- **Banload:** Downloader für Banking-Trojaner, der hauptsächlich auf brasilianische und portugiesische Banken abzielt

4.7 Schadcode auf verschieden Plattformen - Konzentration auf Windows

Im ersten Halbjahr 2008 ist der Anteil an Schadcode für Windows von 95,2% auf 98,2% weiter angestiegen. Das zeigt, dass sich die Malwareautoren auf das Kerngeschäft mit Windows-Rechnern konzentrieren. Offenbar sind dort die effektivsten Geschäfte zu machen.

	#2008 H1	Plattform	#2007	Plattform
1	312.668	Win32	126.854	Win32
2	2.650	JS	2.463	JS
3	845	HTML	1.106	HTML
4	572	VBS	1.007	VBS
5	545	BAT	707	BAT
6	252	MSIL	197	PHP
7	231	SWF	166	MSWord
8	92	MSWord	139	Perl
9	91	PHP	137	Linux
10	33	MSExcel	70	ASP

Tabelle 4: Top 10 Plattformen im ersten Halbjahr 2008 und Gesamtjahr 2007

Die webbasierten Angriffe in Javascript, HTML, VBSkript, Flash (SWF), PHP und Perl haben zwar ihren Anteil von 2,5% auf 1,4% reduziert. Hochgerechnet auf das gesamte Jahr 2008, ist aber mit mehr als einer Verdoppelung der webbasierten Angriffe zu rechnen. Dies zeigt, dass abgesehen von der Windows-Malware, die auf Webseiten hinterlegt wird, momentan immer mehr gezielte Angriffe über webspezifische Plattformen ausgeführt werden. Da die Schutzmechanismen für diese Angriffe noch in den Kinderschuhen stecken, müssen sie auch nicht so oft aktualisiert werden.

Für Linux wurden lediglich 21 neue Schädlinge entdeckt und für Mobilgeräte nicht mehr als 41 (20 davon für Symbian, 19 für J2ME und 2 für Win CE. 2007). Damit bleibt auch in den ersten sechs Monaten von 2008 die so oft herbei geredete Gefahr für Mobiltelefone aus.

5. Ausblick 2. Hälfte 2008

G DATA erwartet in kommenden Wochen und Monaten folgende Entwicklungen:

- **Malware in Webseiten:**
  Die Verbreitung von Malware per Webseiten ist noch lange nicht ausgereizt. Auf der Seite des Surfers sind noch manche Lücken zu schließen. Nicht nur der Browser muss abgeschottet werden, sondern auch alle seine Plugins. Aber auch auf der Seite der Anbieter von Internet-Dienstleistungen ist noch einiges zu tun. Webanwendungen beherbergen massenhaft Sicherheitslücken wie Cross-Site Scripting, Cross Site Request Forgery und SQL Injection, die sich zum Einschleusen von fremden Inhalten in Webseiten ausnutzen lassen. Bis alle Entwickler von Webanwendungen die notwendigen Sicherheitsmaßnahmen beherzigen und umgesetzt haben wird noch einige Zeit vergehen. Bis dahin bleiben Besucher von Webseiten einer erhöhten Infektionsgefahr ausgesetzt. Nur ein Virenschutz, der auch HTTP-Daten auf Schadcode prüft, bietet hier einen zuverlässigen Schutz. Das gilt insbesondere für Nutzer, die intensiv von Web 2.0 Angeboten wie MySpace, Flickr, Facebook etc. Gebrauch machen.

- **Lukrative Geschäftsmodelle:**
  Spam, Datendiebstahl und Adware sind Multimilliarden-Geschäfte, die Online-Kriminelle trotz aller Bemühungen der Strafverfolger nicht ohne weiteres aufgeben werden. Kern dieser Industrie sind weiterhin die leistungsfähigen Botnetze. Daher werden wir auch in den nächsten Monaten von Downloadern und Backdoors überflutet, die Rechner in Spam-Zombies verwandeln.

- **Der Handel mit Daten blüht.**
  Spyware spioniert mittlerweile weit mehr aus als nur die Zugangsdaten zum Online-Banking. Wer sich einen Keylogger einfängt kann seine komplette Online-Identität verlieren.

- **Adware ist der Bereich, der am meisten wächst.**
  Mit ergaunerten Klicks oder mit der Installation von Werbesoftware ist viel Geld zu machen.

- **Neue Tarnmechanismen:**
  Möglicherweise werden Rootkits und Schadfunktionen, die im Bootsektor bzw. MasterBoot-Record verankert sind, in den kommenden Monaten verstärkt eingesetzt

- **Trittbrettfahrer:**
  Anstehende Großereignisse wie die Olympiade werden sicher für betrügerische Machenschaften ausgenutzt.

Geschützt. **Geschützter. G DATA.**