G DATA Malware-Report 2006

Ralf Benzmüller & Thorsten Urbanski

Inhaltsverzeichnis

1. Zusammenfassung: Trojanische Pferde und Ad-/ Spyware auf dem Vormarsch --- 3
1.1 Anstieg von Ad-/ Spyware --- 3
1.2 Verbreitung durch Botnetze --- 3
1.3 Mobile-Malware ohne Bedeutung --- 3
1.4 Fazit --- 3

2. Einleitung --- 4
2.1 Botnetze, Backdoors, Spyware --- 4

3. Verbreitungswege --- 5
3.1 Ablauf einer typischen Infektion --- 5
3.2 Sicherheitslücken nutzen --- 5
3.3 Gezielte Angriffe --- 5
3.4 Nutzung von Zeitfenstern --- 6
3.5 Infektion im Vorbeisurfen --- 6

4. Botnetze - das Rückgrat der CyberCrime Ökonomie --- 7
4.1 Spam --- 8
4.2 Adware --- 8

5. Daten vergolden --- 9
5.1 Ransomware --- 9
5.2 Phishing --- 9
5.3 Spyware --- 10

6. Ausblick auf 2007 --- 10

7. Tabellarischer Anhang --- 11
7.1 Anzahl neuer Malware nach Kategorien 2005 und 2006 --- 11
7.2 Anzahl der Malwarefamilien in 2005 & 2006 --- 11
7.3 Top 10 Malwarefamilien 2005 und 2006 --- 11
7.4 Top 5 Wurmfamilien 2005 und 2006 --- 11

1. Zusammenfassung: Trojanische Pferde und Ad-/ Spyware auf dem Vormarsch

G DATA Security verzeichnet auch 2006 einen deutlichen Anstieg von Malware. Rückblickend betrachtet ist 2006 nicht das Jahr der großen Outbreaks. Die Verbreitung neuer Malware blieb allerdings im gesamten Jahr auf einem gleich bleibend hohen Niveau. Im Vergleich zu 2005 verzeichnet G DATA einen deutlichen Anstieg neuer Malware – die Zuwachsrate betrug insgesamt 25 Prozent. In absoluten Zahlen ausgedrückt bedeutet das für 2006 somit 39.670 neue Schadprogramme –knapp 109 pro Tag. Die gestiegene Anzahl an Malware wird aber von deutlich weniger Virenfamilien hervorgerufen. So halbierte sich die Anzahl von aktiven Virenfamilien nahezu von 4343 auf 2223.

1.1 Abnahme klassische Viren

Klassische Viren und Makroviren sind auch 2006 stark rückläufig. So verzeichneten die G DATA Security Labs hier eine Abnahme um 24%. Der Anteil an Würmern blieb auf dem hohen Niveau des Vorjahres.

Deutlich zugelegt haben 2006 hingegen Trojan-Downloadern (+60%), Ad-/ Spyware (+43%) und Backdoors (+33%). Diese Entwicklung erklärt sich aus der zunehmenden Fokussierung der Cyberkriminellen auf Ertrag bringende Bereiche - wie Diebstahl und Handel mit Kontodaten, Kreditkarteninformationen oder der Vermietung von Botnetzen.

1.2 Verbreitung durch Botnetze

Die Verbreitung von Spam und Malware erfolgt 2006 primär über Botnetze, die für den Versand von gut 80% aller Spam weltweit verantwortlich sind. G DATA beobachtet hier eine Veränderung der Angriffstaktik. Statt weltweiter Massenmails finden in unregelmäßigen Intervallen zielgruppenspezifische Angriffe statt – beispielsweise auf Anbieter von Online-Auktionen oder Nutzer von Pokerforen. Auch 2006 erfolgten die meisten Infektionen durch E-Mailanhänge und Peer-to-Peer Tauschbörsen. Begünstigt wurde die Verbreitung von Malware zusätzlich durch die oftmals zu langen Reaktionszeiten einzelner Security-Hersteller. Mit einer Reaktionszeit von weniger als einer halben Stunde liefert G DATA Security entsprechende Signatur-Updates und liegt somit deutlich vor den meisten Mitbewerbern.
Mit der OutbreakShield-Technologie schließt G DATA zugleich das kurze Zeitfenster zwischen Malware-Identifikation und Signatur-Update. Infizierte Spam werden dank OutbreakShield so von vorneherein geblockt.

1.3 Mobile-Malware ohne Bedeutung

Malware für mobile Geräte - wie PDAs oder Handys - spielten entgegen vereinzelten Medienberichten 2006 keine nennenswerte Rolle. Gründe hierfür sind in der Vielzahl der Betriebssysteme und der instabilen Einspeisung von Schadprogrammen zu sehen, die eine massenhafte Verbreitung erschweren. Das Bedrohungspotential von Mobile-Malware – lediglich 73 neue Schadprogramme in 2006 – ist somit als verschwindend gering einzustufen. Dies könnte sich 2007 ändern.

1.4 Fazit

G DATA rechnet 2007 mit einem gleich bleibend hohen Malware-Niveau. Es ist absehbar, dass die etablierten Geschäftsmodelle im Bereich Adware, Spyware und Phishing und der Einsatz von leistungsfähigen Botnetzen weiter fokussiert werden.
Security-Suiten, die Virenschutz, Firewall und AntiSpam-Module vereinen, werden als ganzheitliche Sicherheits-Lösungen noch stärker an Bedeutung gewinnen.

Ob der Einsatz von Microsoft Vista die Sicherheit der Anwender steigern kann, ist fraglich. Bisher konnte Microsoft mit seinen Bemühungen um Sicherheit nicht überzeugen. Eine zunehmende Gefahr stellt die Ausnutzung von Sicherheitslücken sowohl in Desktop-Anwendungen als auch auf Webseiten dar. Firewall und Virenschutz bleiben obligatorisch.

2. Einleitung

Von außen betrachtet könnte 2006 als ein ruhiges Jahr angesehen werden. Nur in vereinzelten Fällen hat es Malware in die Schlagzeilen geschafft. Wirklich große globale Ausbrüche, wie noch vor 2 Jahren, haben 2006 nicht stattgefunden. Die Anzahl der sich selbst verbreitenden Viren und Würmer geht weiter zurück. Aber in der Ruhe liegt die Kraft. Heimlich, still und leise wirken im Untergrund gut organisierte, international agierende Banden. Malware ist ein Geschäft geworden, in dem professionelle Händler und erfahrene Entwickler an der Maximierung ihres Profits arbeiten. Öffentliche Aufmerksamkeit stört nur die Geschäfte und darum bleiben die großen Infektionswellen aus. Auch die Schadfunktionen von Malware agieren meist im Hintergrund und sind für die Nutzer nicht zu erkennen.

Insgesamt ist die Anzahl neuer Malware erneut gestiegen. Die Anzahl neuer Computer-schädlinge liegt mit 39.670 ca. 25% über der des Vorjahres (31849). An Stelle der Massenmailer sind viele gezielte Angriffe auf fest umrissene Zielgruppen getreten. Mit 43 % verzeichnet der Bereich Ad-/Spyware den stärksten Zuwachs. Auch die Anzahl der Backdoors (+33%) und Trojan-Downloader (+60%) ist deutlich gestiegen. Diese Zahlen belegen wie sich die Arbeitsweise der Malware-Autoren geändert hat.

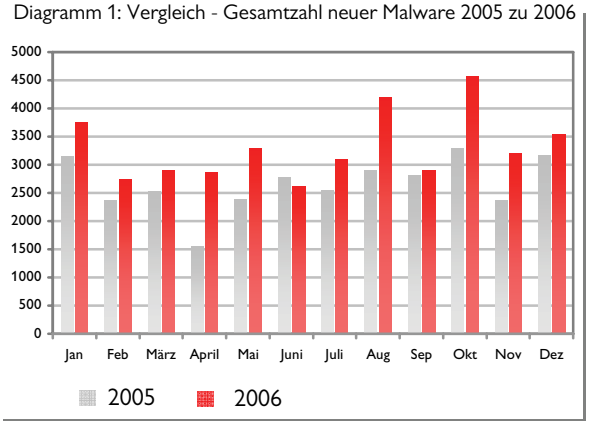
Anstelle von unkontrollierbaren Würmern und Viren, die eigene Verbreitungsroutinen mitbringen, werden gezielt einsetzbare Trojan-Downloader verwendet, die per Botnetz an festgelegte Zielgruppen gespamt werden. Zusätzlich werden immer mehr Schädlinge auf Webseiten versteckt.

2.1 Botnetze, Backdoors, Spyware

Botnetze bilden das Rückgrat vieler schädlicher Aktivitäten. Fast 60% aller infizierten Rechner sind mit einer Backdoor infiziert. Meist werden die fernsteuerbaren Rechner zu großen Netzwerken zusammengefasst. Eine Tendenz zu mittelgroßen Netzwerke ist jedoch zu beobachten. Die Zombie-Armeen dienen dazu Spam und Malware zu verbreiten. Man kann über sie Spyware und Adware verbreiten. Zusätzlich werden diese auch zu verteilten Angriffen auf Webseiten eingesetzt, um so deren Betreiber zu erpressen.

Daten haben einen bei vielen Internetnutzern unterschätzten Wert, der erst erkannt wird, wenn diese von Crypto-Trojanern verschlüsselt wurden. Der Zugang zu den eigenen Daten ist dann erst wieder nach Zahlung eines Lösegelds möglich - hierbei oft als Software-Tool getarnt. Mit E-Mailadressen, Kreditkarten- und Kontoinformationen, Zugangsdaten und Surfprofilen von Nutzern wird aber ein für die Datensammler lukrativer Handel betrieben. Aber nicht nur Spyware und Phishing wird damit betrieben. Mittlerweile werden auch CallCenter und Firmen, die viele Kundendaten bearbeiten, von Personen unterwandert, die es darauf abgesehen haben, diese Iinformationen zu stehlen und zu vertreiben.

Diagramm 1: Vergleich - Gesamtzahl neuer Malware 2005 zu 2006



3. Verbreitungswege

Für PC-Nutzer hat sich an den wichtigsten Einfallstoren für Malware wenig geändert. Dateianhänge von E-Mails und Instant Messages und Downloads aus Peer-to-Peer Tauschbörsen wie Kazaa oder eMule bleiben die häufigsten Einfallstore. Wie auch schon im letzten Jahr wird die Zeit zur Erstellung einer Virensignatur durch ständig neue Varianten genutzt. Stark im Kommen sind sog. Drive-by Infektionen auf Webseiten. Nicht nur durch Links in E-Mails und Instant Messages werden Opfer auf präparierte Webseiten gelotst.

3.1 Ablauf einer typischen Infektion

Eine typische Infektion hat sich im Laufe der letzten Jahre stark gewandelt. Aus den herkömmlichen, selbständigen Würmern, wie NetSky und MyDoom, die nach wie vor im Internet ihre Runden drehen und auch in diesem Jahr in vielen Postfächern eintrafen, sind viele kompakte und spezialisierte Module geworden, die nach Bedarf nachgeladen werden. Nach der Übernahme des Rechners wird meist ein Trojan-Downloader oder ein Trojan-Dropper gestartet. Beide Typen sorgen dafür, dass die schädlichen Dateien auf den Rechner gelangen und gestartet werden. Nach dem Start erfolgt das Herunterfahren der Sicherheitseinstellungen. Der PC ist somit den weiteren Aktivitäten der Malware schutzlos ausgeliefert. Im nächsten Schritt wird dann eine Backdoor auf den Rechner geladen und so installiert, dass dieser unbemerkt im Hintergrund läuft. Dazu ist nur in besonderen Fällen ein Rootkit notwendig - daher auch der, verglichen mit der Medienresonanz relativ geringe Anstieg in diesem Bereich. Mit dieser Hintertür bekommt der infizierte Rechner einen neuen Besitzer, der nun nach Belieben mit dem Rechner agiert. Die Backdoor erlaubt es u. a. den Rechner durch mittlerweile verschlüsselte IRC-oder HTTP-Kommandos mit vielen anderen Rechnern weltweit zu koordinieren. So wird der Rechner Teil einer mitunter riesigen Zombie-Armee. Nach der Installation der Backdoor wird das infizierte System genauer inspiziert und der Angreifer entscheidet, was er mit dem Rechner anfangen will. Wenn er über eine gute Anbindung ins Internet verfügt, kann er zum Versand von Spam verwendet werden, illegale Dateien zum Download anbieten oder Phishing-Webseiten hosten. Weniger gut angebundene Rechner werden mit Spyware nach verwertbaren Daten untersucht und/oder mit Adware ausgestattet.

3.2 Sicherheitslücken nutzen

Die meisten Schädlinge sind ausführbare Dateien oder basieren auf Skriptsprachen - wie Visual Basic oder JavaScript. 2006 hat nicht nur die Anzahl der CVE registrierten Sicherheitslücken von 4813 auf über 6600 zugenommen. Diese größere Zahl an Sicherheitslücken wird auch immer häufiger und immer schneller von Malware genutzt. So können Rechner auch mit präparierten Bildern (WMF, JPF, GIF, PNG, BMP), Audiodateien (RM, MP3, PLS), Filmen (WMV, QT) Dokumenten (DOC, XLS, PDF) uvm. angegriffen und übernommen werden. Dieser neue Trend eignet sich insbesondere für gezielte Angriffe auf einzelne Personen in großen Unternehmen.

Nicht nur Desktop-Anwendungen stehen im Visier. Unter dem Schlagwort Web 2.0 entstehen immer mehr Webapplikationen, die ohne Installation im Browser laufen. Bei den vielen neuen Funktionen bleibt gelegentlich die Sicherheit unberücksichtigt. Wir gehen davon aus, dass zwischen 40% und 50% aller Webanwendungen für Cross Site Scripting (XSS) anfällig sind. Bei einem noch höheren Anteil an Webseiten lassen sich die dazugehörigen Datenbanken per SQL Injection hacken. Malware nutzt diese Sicherheitslücken in Webanwendungen wie Foren, WebShops, Blogs und Wikis. Mit dem wachsenden Web 2.0 steigt auch die Wahrscheinlichkeit, dass Schadcode über diesen Weg eingeschleust wird. Das gilt insbesondere für so offene Plattformen wie Second Life , wo Anwender selbst Programmcode ausführen können.

3.3 Gezielte Angriffe

Die beiden einzigen Massenmailer, die 2006 erwähnenswert sind, heißen Nyxem und Warezov. Nyxem.e lockt in E-Mails mit erotischen Bildern und interessanten Informationen und sorgte so für die erste große Infektionswelle 2006. Er ist seit langer Zeit der erste Massenmailer, der Dateien eines Nutzers löscht. Aufgrund dieser zerstörerischen Schadfunktion wurde er schnell identifiziert und

konnte kaum Schaden anrichten.

Die erste Variante von Warezov erschien Mitte August. Seitdem werden täglich neue Varianten erstellt. Mit mehr als 240 Varianten gehört Warezov zu den aktivsten Familien. Warezov sucht auf den infizierten Rechnern nach E-Mailadressen, an die er sich versendet. Durch die integrierte Backdoor wird weitere Software nachgeladen, die für den Versand von Spam verantwortlich ist.

Neben diesen seltenen und auffälligen Attacken gab es aber zahllose kleine Angriffe, die entweder zeitlich oder regional begrenzt waren oder sich an bestimmte Nutzergruppen wandten. So erhielten z.B. Nutzer von Poker-Foren oder Anbieter von Online-Auktionen schädliche Post, die immer öfter stimmig und überzeugend ist. Auch Spieler von Online-Games, wie World of Warcraft, Lineage und Legends of Mir, sollten sich vorsehen. Die Virenfamillen, die es auf die Login-Daten zu diesen Spielen abgesehen haben, gehören zu den aktivsten des Jahres.

3.4 Nutzung von Zeitfenstern

Im Laufe des letzten Jahres wurde eine Möglichkeit, Malware auf den PC zu schleusen, besonders intensiv genutzt. Sie basiert auf der allgemeinen Funktionsweise von Antiviren-Software. Um einen Schädling zu erkennen, muss er bekannt sein und auf dem Rechner eine passende Erkennungsschablone - eine sog. Signatur - vorhanden sein. Ohne eine passende Signatur werden Computerschädlinge nicht entdeckt. Vom ersten Auftreten eines Schädlings bis zur Erstellung einer Signatur vergehen im günstigsten Fall eine halbe Stunde (z.B. G DATA AntiVirenKit), im Durchschnitt sind es 7 Stunden und im schlechtesten Fall mehrere Tage. In dieser Zeit kann der Schädling ungehindert agieren. Diese Taktik wurde 2006 verstärkt eingesetzt. Die erhöhte Anzahl an Malware wird von einer nahezu halbierten Zahl an Malware-Familien bestritten. Insgesamt hat sich die Zahl aktiver Malwarefamilien von 4343 im letzten Jahr auf 2232 im laufenden Jahr verringert. Die nahezu halbierte Anzahl an Familien führte dennoch zu mehr Varianten als 2005. In diesem Bereich kam es 2006 zu einer „Marktbereinigung“. Der Trend zur Nutzung der Zeitlücke im Virenschutz ist an der Reduzierung deutlich erkennbar. Insbesondere im Bereich von Ad-/Spyware ist eine Konzentration von 1020 auf 210 Familien auszumachen. Eine vergleichbare Tendenz ist auch bei den Email-Würmern erkennbar. Warezov hat es seit Mitte August auf mehr als 240 Varianten gebracht - 27 davon an einem einzigen Tag. In ähnlicher Weise agieren auch die Würmer aus den Familien Feebs, Viking, Scano. Bagle und Mytob. Der Variantenreichtum der Smartphone-Würmer Kelvir und Bropia verebbte hingegen 2006.

Im vergangenen Jahr haben Malware-Autoren die Zeit bis Virensignaturen verfügbar sind, noch aktiver ausgenutzt, um ihre Kreationen unbehindert zu verbreiten. G DATA hat diesem Treiben mit OutbreakShield einen effektiven Riegel vorgeschoben. Täglich wird gespamte Malware blockiert - oft schon Stunden bevor die ersten Signaturen erscheinen.

3.5 Infektion im Vorbeisurfen

Immer häufiger fehlt in Malware-E-Mails der Dateianhang. Die allgegenwärtigen E-Mail-Scanner würden den schädlichen Anhang schnell finden und die E-Mail nicht zustellen. Stattdessen verweist ein Link auf eine Webseite, die auf (mindestens) drei Arten die schädliche Fracht überbringt:

1. Unter einem schlüssigen Vorwand wird schädliche Software direkt zum Download angeboten. Als Vorwand diente z.B. ein Windows Update. Auch Varianten des Telekom-Trojaners, der jeden Monat zeitgleich mit der offiziellen Telekom-Rechnung umgeht, werden auf Webseiten hinterlegt. Auf manchen Webseiten werden die Schadprogramme als Plugins getarnt, die für die perfekte Wiedergabe der Seite oder eines (meist multimedialen) Inhalts Voraussetzung sind. So konnten etwa die Filme auf einer Erotikseite nur mit einem speziellen "Codec" angesehen werden. Der Download stellte sich dann als Trojanisches Pferd heraus und die Wiedergabe wurde mit einer vorgetäuschten Fehlermeldung abgebrochen.

2. Bedeutend effizienter ist aber die Ausnutzung von Sicherheitslücken des Browsers oder seiner Komponenten. Aktive Inhalte wie Java, JavaScript und ActiveX Controls ermöglichen Zugriffe auf die im Browser verarbeiteten Daten und teilweise sogar auf das Dateisystem. Sicherheitslücken im Browser und in Browserkomponenten. Grafikbibliotheken,

Flash, RealMedia und Quicktime, werden genutzt, um den Rechner eines Besuchers der präparierten Webseite zu übernehmen.

3. Cross-Site Scripting (XSS) nutzt Sicherheitslücken in schlampig programmierten Webanwendungen wie Foren, WebShops, Blogs und Wikis. XSS-Sicherheitslücken stecken in etwa vier von zehn Webanwendungen. Diese werden mit dem wachsenden Web 2.0 auch verstärkt von Malware genutzt.

Das größte Problem ist dabei, dass der klassische Virenschutz erst greift, wenn eine Datei auf die Festplatte gespeichert wurde. Bevor der Browser tätig wird, führt er die in den Dateien enthalten Anweisungen aber erst einmal aus -d. h. wenn der klassische Virenschutz Alarm schlägt, ist es bereits zu spät. Im Kästchen auf dieser Seite steht, wie Nutzer prüfen können, ob der installierte Virenschutz auch vor Gefahren in Webseiten schützt.

Die Anzahl schädlicher Webseiten stieg 2006 kontinuierlich an. Bislang wurden die meisten schädlichen Webseiten per E-Mail oder Instant Message bekannt gemacht. Mittlerweile findet man sie aber auch auf den Ergebnisseiten von Suchmaschinen oder hinter den dort dargestellten Werbebannern. Auch beliebte Social-Networking-Seiten, in denen jeder Besucher eigene Inhalte veröffentlichen kann, werden verstärkt zur Verbreitung von Malware genutzt. So verlinkte etwa ein deutscher Artikel bei Wikipedia über Blaster auf ein angebliches Removal-Tool, das sich als Trojanisches Pferd herausstellte. In ähnlicher weise agierte auch myspace.com . Mit einem Crawler hat es ein Nutzer innerhalb kürzester Zeit zu mehr als einer Million "Freunde" gebracht. Im Dezember wurden dort Filme veröffentlicht, die eine Sicherheitslücke in Quicktime ausnutzten, um Rechner zu übernehmen.

Überprüfung des Online-Virenschutzes:

So ist es für Nutzer auf einfache Weise mögliche zu prüfen, ob der Virenschutz in der Lage ist auch Schadcode in Webseiten zu erkennen.

1. Öffnen Sie den Browser
2. Eingabe folgender URL:
   http://www.eicar.org/download/eicar.com.txt
3. Falls der Browser die Seite problemlos öffnet und keine Warnmeldung erscheint, ist der getestete PC nicht ausreichend geschützt.

Wer im Internet surft sollte entsprechende „Sicherheitsmaßnahmen“ treffen, die das Einschleusen von Malware verhindern. Dazu gehören u. a. ein Rechner mit den aktuellen Patches und ein Virenschutz mit aktuellen Signaturen, der die Inhalte von Webseiten prüft, bevor diese in den Browser gelangen.

4. Botnetze - das Rückgrat der CyberCrime Ökonomie

Eine der wichtigsten Waffen von Online-Kriminellen sind ihre Botnetze. Es gibt viele Möglichkeiten, wie man mit einem Botnetz Geld verdienen kann. Zunächst sind das die Bot-Herder, die solche Botnetze aufbauen und pflegen. Sie verdienen ihr Geld damit, dass sie die von ihnen betreuten Botnetze vermieten. Die Botnetze werden je nach Anforderungen der Mieter für bestimmte Einsatzzwecke ausgerichtet Die Mieter des Botnetzes können ihrerseits mit folgenden Aktivitäten Kapital schlagen:

Versand von Spam & Phishing-Mails

Mehr dazu in Abschnitt 4.1

Verteilte Überlastangriffe

Mit einem Distributed Denial of Service ´(DDoS)-Angriff werden Rechner im Internet (meist Webserver oder Mailserver) mit so vielen unsinnigen und/oder inkorrekten Anfragen überhäuft, dass ein regulärer Betrieb nicht mehr möglich ist. Mittelgroße Botnetze können einen so hohen Datenverkehr verursachen, dass selbst die Backbones der Provider in Mitleidenschaft gezogen werden. Nicht nur Betreiber von beliebten Webshops oder Online-Wettbüros sind Opfer solcher Angriffe. Die Betreiber der Seiten werden zur Zahlung von Lösegeld erpresst. Oft scheint dann die Zahlung des geforderten Schutzgelds der einfachste Ausweg. Meist wird daraus aber eine langfristige „Geschäftsbeziehung“.

Datendiebstahl

Mit Passwort-Trojanern und Keyloggern werden auf dem Rechner gespeicherte Passwörter, Zugangsdaten und Lizenzschlüssel von Software gestohlen und in entsprechenden Internetbörsen verkauft. Sniffer, Proxies und Redirector werden verwendet, um Daten aus dem Netzwerkverkehr mitzuschreiben.

In der Zeit, in der die Botnetze nicht ausgelastet sind, werden die infizierten Rechner zu deren Pflege eingesetzt. Dann wird die Bot-Software aktualisiert und es werden neue Spamwellen mit Malware gestartet.

Die Anzahl der Botnetze wird weltweit auf ca. 10.000 geschätzt. In etlichen Fällen gelingt es die IRC-basierten Command & Control (C&C) Server der Botnetze zu infiltrieren und deren Kommunikation mitzuschneiden. So gelang es 2006 einige Botnetze erfolgreich zu zerschlagen. Das größte befand sich in den Niederlanden – hier waren ca. 1,5 Millionen Rechner vernetzt. In letzter Zeit werden Botnetze in viele kleinere Netze aufgeteilt und die Kommunikation in den C&C Channels wird immer häufiger verschlüsselt. Es werden auch andere Wege zur Steuerung der Botnetze beschritten. So scheint sich HTTP als Steuermechanismus zu verbreiten. Auch Versuche mit Peer-to-Peer Strukturen werden unternommen. Letztere sind aber bislang noch nicht alltagstauglich und allenfalls als Notlösungen implementiert.

4.1 Spam

Fast jeder Internetnutzer kennt das Problem von Spam aus eigener Erfahrung. Während der Anteil an Spam zu Anfang des Jahres auf einem niedrigen Niveau lag, steigt seit dem 2. Quartal 2006 die Anzahl der Spam-Mails wieder kontinuierlich an und erreicht in der Vorweihnachtszeit Spitzenwerte. Insgesamt stieg die Anzahl der Spam-Mails seit Anfang des Jahres um knapp die Hälfte. Der deutlichste Anstieg erfolgte in den letzten drei Monaten. Über das Jahr 2006 erhält jeder Internetnutzer durchschnittlich 6 Spam-Mails pro Tag.

Der Anteil von Spam am gesamten Mailaufkommen liegt zwischen 50% und spitzen Zeiten bei über 90%. Wer wie viel Spam bekommt, hängt u. a. davon ab, wo man wohnt und in welcher Branche der jeweilige Nutzer arbeitet. In Japan ist der Anteil an Spam mehr als die Hälfte geringer als in Israel und den USA. Beschäftigte in sehr großen Firmen erhalten nur etwa 1/3 an Spam-Mails im Vergleich zu einem Angestellten eines kleineren Unternehmens. Bildungseinrichtungen und produzierende Firmen erhalten 50% mehr Spam als etwa Finanzdienstleister und Behörden.

Mehr als 80% aller Spam-Mails werden per Botnetz verschickt. Weltweit werden mit Backdoors infizierte Rechner in „Spamschleudern“ verwandelt. Einen wichtigen Anteil daran trägt die momentan sehr aktive Malware Warezov. Mit ihren ständig neuen Varianten vergrößerten sie die Spam versendenden Zombie-Armeen täglich auf über 1 Million aktive Rechner.

Beängstigend - Spam ist nach wie vor ein lukratives Geschäft. Der Versand von Millionen von E-Mails kostet wenige hundert US-Dollar. Selbst mit geringsten Rücklaufquoten rechnet sich der Versand. Spam mit erotisch/pornografischen Inhalten erregen zwar das meiste Aufsehen, ihr Anteil liegt aber meist unter dem von anderen Angeboten, wie: Luxusprodukte, Finanzangebote, Wellness und Gesundheit.

Ende 2005 tauchten die ersten Spam-Mails mit Bildern auf. Seitdem ist Ihr Anteil am gesamten Spamaufkommen um mehr als das dreifache gestiegen. Im November lag der Anteil an Spam-Mails mit Bildern bei 45%. Da Bilder viel größer sind, als der darin enthaltene Text, steigt das Datenvolumen überall wo E-Mails verarbeitet werden. Die Flut der Bilder umgeht die klassischen textbasierten Spamerkennungsverfahren und mit ausgeklügelten Kniffen werden auch Bildanalyseverfahren, Texterkennung und datenbankorientierte Ansätze unterlaufen.

Dank der OutbreakShield Technologie erreicht G DATA Internet Security in Vergleichstests dennoch höchste Erkennungsraten mit der geringsten Fehlerquote. Zum jetzigen Zeitpunkt ist diese ausschließlich von G DATA eingesetzte Technologie der einzige wirksame Schutz vor Bilder-Spam.

4.2 Adware

Die Werbung hat schon lange im Internet Fuß gefasst. Die Betreiber beliebter Webseiten finanzieren so den Unterhalt ihrer Angebote. Nicht nur Suchmaschinenbetreiber und große Online-Shops bieten interessante Konzepte für Werbeeinnahmen, die meist darauf beruhen, dass die beworbene Seite per Klick auf das Werbebanner geöffnet wird. Pro Klick werden Bruchteile von Cents bezahlt. Bei vielen Klicks ist dies ein lukratives Geschäft. Das bietet aber auch Möglichkeiten zum Missbrauch - dem sog. Klick-Betrug.
Browser-Hijacker ändern die Startseite oder die Suchseite eines infizierten Rechners. So

wird bei jedem Öffnen des Browsers und bei jeder Suche ein Klick auf eine vorher bestimmte Webseite generiert. Da dies meist auf vielen Rechnern von Botnetzen geschieht, füllen sich die Taschen der Klickbetrüger. Ähnlich funktionieren auch Tools, die das Surfverhalten des Opfers aufzeichnen und an geeigneter Stelle PopUp-Werbung einblenden. Jede Einblendung und jeder Klick auf eine solche Seite bringt den Malware-Autoren Geld.

Aggressiver aber lukrativer ist die Installation von Programmen, die das Nutzerverhalten aufzeichnen. Wenn eine Firma pro Installation 0,40$ zahlt, sind die Kosten für die Nutzung des Botnetzes schnell amortisiert und Gewinnraten bis zum 100fachen der Kosten erreichbar.

5. Daten vergolden

Das größte Geschäft sind derzeit gestohlene Daten. Vielen Internetnutzern ist nicht bewusst, welchen Wert persönliche Daten haben. Im Internet ist ein reger Handel mit Emailadressen, Kreditkarteninformationen, Kontodaten, Software-Keys und Zugangsdaten zu Online-Auktionen und Online-Spielen entstanden. Für gültige Kreditkarteninformationen werden bis zu 50 € gezahlt - mit PIN 60 €. Im Bündel gibt es die Daten aber auch schon für 2 - 5 $.

5.1 Ransomware

Ein Revival hat die Idee der Verschlüsselung von Daten erlebt. PGCoder verschlüsselt die Daten in Word-Dokumenten, Excel-Tabellen, PowerPoint Präsentationen und einigen weiteren Dateitypen. Wer seine Daten wieder haben möchte, muss das Tool zur Entschlüsselung kaufen. Die anfänglich sehr einfachen Verschlüsselungsverfahren waren leicht zu umgehen. Im Laufe des Jahres wurden sie durch immer komplexere und sicherere Verfahren ersetzt. Die Idee des Daten-Kidnapping ist nicht neu, Sie wurde schon 1989 vom AIDS-Trojaner eingesetzt. Aber schon damals hat sich dieses Modell offenbar nicht bewährt. Einerseits lassen sich Daten mit genügend Rechenaufwand auch wieder entschlüsseln. Der Vertrieb der Tools setzt aber einen Kontakt zu den Opfern voraus, der häufig genutzt wird, um die Täter zu ermitteln. Das Risiko macht die möglichen Gewinne wohl nicht wett.

5.2 Phishing

Wenn man 2006 einer Malware-Kategorie widmen könnte, dann dem Phishing. Der Diebstahl von Daten und Identitäten hat im Laufe des Jahres den größten Boom erlebt. Seit zwei Jahren nimmt die Anzahl der Phishing-Mails und der Phishing-Malware deutlich zu. Auch 2006 hat sich deren Aufkommen fast verdoppelt. Jeder vierte Schädling, der per Mail umging hatte mit Phishing zu tun. Die Daten werden einerseits durch Phishing-Mails und entsprechende Webseiten ergaunert. Bei deutschen Online-Banken hat diese Methode mittlerweile aber fast ausgedient. Die Schutzmechanismen iTAN und mTAN zeigen - da wo sie eingesetzt werden - ihre Wirkung.

Online-Betrüger sind jedoch weit davon entfernt, deshalb die Flinte ins Korn zu werfen. Die überwiegende Mehrheit aller Online-Datendiebstähle in Deutschland geschehen mittlerweile per Trojanischem Pferd. Key- und Screenlogger stehlen Passwörter bei der Eingabe. Trojan-Spys durchsuchen die Festplatte an geeigneten Stellen nach kritischen Informationen. Sniffer, Proxies und Redirector sorgen dafür, dass ein Angreifer als Man-in-the-Middle alle Eingaben abfangen kann. Oft gehen die Tools so geschickt vor, dass das Opfer den Verlust seiner wertvollen Daten erst bei der nächsten Kontoabrechnung bemerkt.

Die Daten werden dann verkauft und von deren Käufern durch Einkäufe im Internet versilbert. Danach wird das erbeutete Geld über unbedarfte Finanzagenten gewaschen, die auf eins der verlockenden Jobangebote hereingefallen sind. Für eine Provision zwischen 5 und 10% des überwiesenen Betrags sollen sie ihr privates Konto nutzen, um Beträge unter 12.000 € per Western Union oder MoneyGram auf ein Konto in einem osteuropäischen oder südamerikanischen Land zu überweisen. Diese sog. Money Mules sind am Ende aber die Dummen. Sowohl die Bank als auch die Kriminellen fordern Geld von ihnen und die Staatanwaltschaft ermittelt gegen sie wegen Geldwäsche.

Eine andere Masche ist die falsche Überweisung bei eBay. Es werden Artikel für z.B. 120 € ersteigert. "Aus Versehen" wird dann aber zu viel überwiesen (z.B. 1.200 €). Der zuviel

gezahlt Betrag wird zurückgefordert und soll meist per Western Union auf ein ausländisches Konto überwiesen werden. Insgesamt ist der Handel mit den gestohlenen Daten für CyberKriminelle sehr einträglich.

5.3 Spyware

Software, die ungefragt Daten ermittelt, ist neben Trojan-Downloadern die Malware-Kategorie, die 2006 am stärksten zugenommen hat. Spyware sucht auf zahlreichen Wegen nach verwertbaren Informationen.

- Keylogger notieren alle Tastatureingaben, Screenlogger erzeugen Screenshot bei Mausklicks.
- Spy-Trojans durchsuchen erreichbare Laufwerke nach verwertbaren Informationen.
- Browser Helper Objects klinken sich in den Browser ein und ermitteln die Surfgewohnheiten des Opfers.
- Sniffer lesen alle Informationen aus dem Netzwerk mit

Die so gewonnenen Daten werden zu unterschiedlichen Zwecken genutzt. Die Surf- und Nutzerprofile werden an Firmen verkauft, die Pop-Up-Werbung einblenden. Die Spy-Trojans können Listen mit Email-Adressen erstellen, die an Spammer verkauft werden. Sie können auch Lizenzschlüssel von Software stehlen und die Software in Online-Shops oder Auktionen verkaufen. Auch Kreditkarten-informationen und Logins von Online-Accounts lassen sich zu Geld machen. Möglicherweise stoßen die Spy-Trojans aber auch auf sensible Informationen einer Person oder eines Unternehmens. Diese werden so erpressbar. Selbst Spieler von Online-Games, wie World of Warcraft, Lineage und Legends of Mir, sollten sich vorsehen. Die Virenfamillen, die es auf die Login-Daten zu diesen Spielen abgesehen haben, gehören zu den aktivsten des Jahres. Beliebte Gegenstände und langwierig zu erstellende Charaktere werden in Online-Auktionen mit vierstelligen Dollar-Beträgen gehandelt.

Der Handel mit Daten und Informationen ist ein einträgliches Geschäft, das auch im kommenden Jahr weiter zunehmen wird.

6. Ausblick auf 2007

Ein Blick in die Zukunft ist immer schwierig. Es ist jedoch davon auszugehen, dass die etablierten Geschäftsmodelle im Bereich Adware, Spyware , Phishing und die ausgiebige Nutzung von Botnetzen auch im kommenden Jahr fortgesetzt werden. G DATA erwartet eine weitere Konzentration des Malware-Marktes auf die rentablen Geschäfte. Offenbar hat es sich im letzten Jahr bewährt Malware auch auf Webseiten zu hinterlegen. Dieser Infektionsherd ist bei Nutzern noch äußerst unbekannt und birgt daher ein besonderes Gefahrenpotential.

CyberKriminelle sind sehr kreativ in der Entwicklung neuer Geschäftsideen. Abgesehen von den etablierten Strukturen erwartet G DATA daher im kommenden Jahr eine Zunahme von Schadcode in Webseiten. Sicherheitslücken - sowohl in Desktop-Anwendungen (Exploits) als auch in Webapplikationen des Web 2.0 (Cross Site Scripting) werden weiterhin genutzt.
Auch mit mobilen Geräten sind systematische Betrügereien möglich. Zum jetzigen Zeitpunkt ist die Gefahr für Nutzer aber äußerst gering.

Ein Hoffnungsträger für sicheres Computing ist das neue Betriebssystem von Microsoft Windows Vista. Es wurde mit einer Reihe von Sicherheitsfunktionen konzipiert. Ob der Einsatz von Microsoft Vista die Sicherheit der Anwender steigern kann, ist fraglich. Bisher konnte Microsoft mit seinen Bemühungen um Sicherheit nicht überzeugen. G DATA erwartet daher nach Markteinführung von Vista lediglich eine kurze "Gewöhnungsphase" aber keine längerfristige Änderung. Virenschutz und Firewall werden auch weiterhin zur Pflichtausstattung eines Rechners gehören.

7. Tabellarischer Anhang

7.1 Anzahl neuer Malware nach Kategorien 2005 und 2006

Monat	Viren		Würmer		Backdoor		Ad-/ Spyware		Trojaner		Sonstige	
Januar	197	33	326	166	393	868	1.375	1.387	690	742	160	546
Februar	83	24	130	148	417	697	1.112	1.172	511	544	104	130
März	44	26	139	120	431	724	1.102	1.322	658	539	159	149
April	30	201	105	162	282	652	572	1.118	458	583	105	126
Mai	36	36	125	147	441	802	860	1.457	620	603	296	212
Juni	46	45	147	108	515	582	1.152	1.163	608	519	231	185
Juli	48	47	123	95	467	696	1.137	1.554	557	540	201	150
August	37	17	136	113	561	866	1.306	2.267	621	760	238	145
September	156	21	144	124	607	551	1.112	1.547	583	537	191	117
Oktober	23	36	132	226	802	603	1.376	3.068	680	506	250	105
November	28	30	97	187	552	560	1.110	1.651	476	635	108	104
Dezember	30	28	127	155	793	720	1.372	1.754	642	615	183	163
Total	758	544	1.731	1.751	6.261	8.321	13.586	19.460	7.104	7.141	2.226	2132

2005 2006

7.2 Anzahl der Malwarefamilien in 2005 & 2006

Typ	2005	2006
AdSpyware	1020	210
Backdoors	755	385
Würmer	406 163 (E-Mail)	242 105 (E-Mail)
Troj. Pferde	888	615
Insgesamt	4343	2223

7.3 Top 10 Malwarefamilien 2005 und 2006

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

7.4 Top 5 Wurmfamilien 2005 und 2006

Rang	2005	Anzahl	2006	Anzahl
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