



# G DATA Malware-Report 2006

## Kurzfassung



Ralf Benzmüller & Thorsten Urbanski

## Inhaltsverzeichnis

<b>1. Zusammenfassung: Trojanische Pferde und Ad-/ Spyware auf dem Vormarsch .....</b>	<b>3</b>
1.1 Anstieg von Ad-/Spyware .....	3
1.2 Verbreitung durch Botnetze .....	3
1.3 Mobile-Malware ohne Bedeutung .....	3
1.4 Fazit.....	3
<b>2. Analyse und Trends.....</b>	<b>4</b>
2.1 Anstieg von Malware ungebrochen.....	4
2.2 Verlagerung der Angriffstaktik.....	4
2.3 Botnetze – Rückgrat der Malware-Industrie.....	4
2.4 Zielgerichtete Angriffe statt Massenmailer .....	4
2.5 Faktor Zeit.....	5
2.6 Schädliche Webseiten.....	5
2.7 Weniger Viren - mehr Trojanische Pferde .....	6
2.8 Malware für mobile Gerät ohne Bedeutung .....	6
2.9 Daten zu Geld machen - Spyware und Phishing.....	7
2.10 Tendenzen und Ausblick.....	7

## **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 Anstieg von Ad-/ Spyware**

---

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 Poker-Foren.

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 vereinzelt 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. Analyse und Trends

### 2.1 Anstieg von Malware ungebrochen

Die Bedrohungslage durch Malware hat sich 2006 wie zu erwarten nicht entspannt. Prozentual stieg die Gesamtzahl von Malware im Jahr 2006 im Vergleich zu 2005 um 25%. In absoluten Zahlen verzeichneten die G DATA Security Labs 2006 eine Steigerung um 39670 neue Schadprogramme. Pro Tag werden somit knapp 109 neue Schädlinge in Umlauf gebracht.

### 2.2 Verlagerung der Angriffstaktik

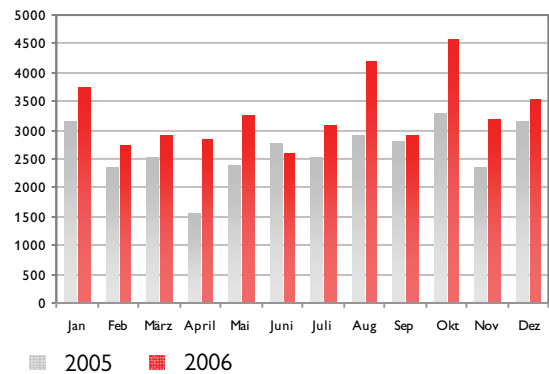
Große Outbreaks waren 2006 nicht zu beobachten - dafür bewegt sich jedoch die Verbreitung im Jahresverlauf auf einem gleich bleibend hohen Niveau. Die gestiegene Anzahl an Malware wird mit einer deutlich niedrigeren Zahl von Malwarefamilien erreicht.

Bei klassischen Viren kam es zu einer Verringerung der neu auftretenden Schadprogramme um 24%. Die größten Zugewinne hatten Trojan-Downloader (+60%), Ad-/Spyware-Programme (+43%) und Backdoors (+33%). Diese Zunahme belegt, dass Cyberkriminelle mit Botnetzen und Ad-/Spyware am meisten Geld verdienen.

Immer häufiger und immer schneller werden Sicherheitslücken in Standardanwendungen genutzt, um Rechner mit Schadprogrammen zu infizieren und anschließend zu übernehmen. 2006 wurden bei der CVE mehr als 6600 Sicherheitslücken gemeldet. Im Vergleich zum bisherigen Rekordjahr 2005 ist dies ein Anstieg um ca. 37%. Der Anteil der von Malware genutzten Sicherheitslücken stieg in gleichem Maße.

Im Fokus der Malware-Entwickler und Cyberkriminellen stehen primär Privat-anwender und kleine bis mittelständische Unternehmen. Cyberkriminelle sind in der Regel nicht Einzeltäter, sondern agieren in hoch differenzierten Netzwerken, hinter denen sich das international organisierte Verbrechen verbirgt.

Diagramm 1: Vergleich - Gesamtzahl neuer Malware 2005 zu 2006



### 2.3 Botnetze – Rückgrat der Malware-Industrie

Botnetze sind das wichtigste Werkzeug von Online-Kriminellen.

Von allen mit Schadprogrammen verseuchten Rechnern sind etwa 60 % mit Backdoors infiziert.

Für die Verbreitung von Spam und Malware zeichnen sich auch 2006 in erster Linie Botnetze verantwortlich. Der Versand von Spam-Mails erfolgt zu etwa 80% mit Botnetzen. Bei der Verbreitung von Malware werden Email-Würmer immer häufiger von kompakten Trojan-Downloadern verdrängt, die sich besser für den massenhaften Versand per Botnetz eignen.

Die sog. Zombies werden von den Betreibern regelmäßig mit den neuesten Adware- und Spyware-Kreationen versehen.

Die in Botnetze zusammengefassten „Zombiearmeen“ sind für Onlinekriminelle die wirkungsvollsten Werkzeuge für ihre verteilten Angriffe auf Online-Angebote.

### 2.4 Zielgerichtete Angriffe statt Massenmailer

Öffentliches Interesse an den Aktivitäten von Cyberkriminellen ist in der Regel für deren Zielerreichung nicht zuträglich.

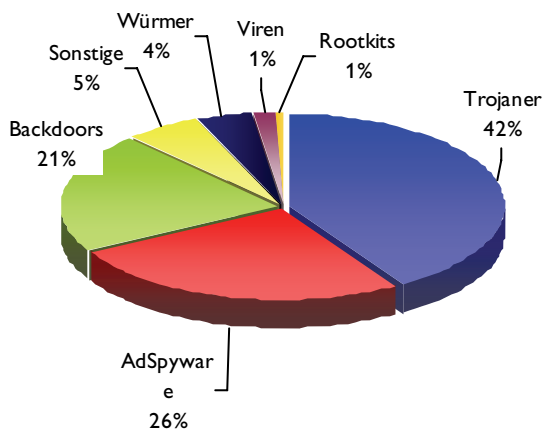
Nyxem.e machte hier Anfang des Jahres eine Ausnahme. Seit langem war Nyxem.e der erste Massenmailer mit einer gravierenden

Schadfunktion. An jedem Dritten eines Monats löscht er Dateien von allen zugänglichen Festplatten. Gerade aufgrund dieser massiven Schadfunktion war Nyxem.e innerhalb kurzer Zeit eliminiert.

Anstelle weltweiter Massenmails traten 2006 vermehrt gezielte Angriffe auf spezifische Zielgruppen auf. Diese erfolgten in kurzen und unregelmäßigen Intervallen. So erhielten z.B. Nutzer von Poker-Foren oder Anbieter von Online-Auktionen schädliche Post.

G DATA Security Labs verzeichnen eine deutlich größere Zielgerichtetheit der Schadprogramme und deren Verbreitungswege, als dies noch 2005 zu beobachten war.

Diagramm 2: prozentuale Aufteilung



## 2.5 Faktor Zeit

Schon im vergangenen Jahr nutzte immer mehr Malware für die Verbreitung den Zeitraum zwischen Identifikation und Bereitstellung einer passenden Virensignatur. Diese Taktik wurde 2006 verstärkt eingesetzt. Die erhöhte Anzahl an Malware wird von einer deutlich reduzierten Zahl an Malware-Familien bestritten. Insgesamt hat sich die Zahl aktiver Malwarefamilien von 4343 im letzten Jahr auf 2232 im laufenden Jahr verringert. Insbesondere im Bereich von Ad-/Spyware ist eine Konzentration von 1020 auf 210 Familien festzustellen.

Eine ähnliche Tendenz ist ebenfalls bei Email-

Wurmern zu beobachten. Warezov hat es seit Mitte August auf mehr als 240 Varianten gebracht - 27 davon an einem einzigen Tag. Ähnlich agieren auch die Würmer aus den Familien Feebs, Viking, Scano. Bagle und Mytob.

Tab. 1: Anzahl der Malwarefamilien 2005 und 2006

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

Die Strategie ist klar: So lange noch keine Virensignatur erstellt ist, ist der Rechner ungeschützt. Bei G DATA liegt die Reaktionszeit mit weniger als einer halben Stunde weit vor Konkurrenzprodukten.

Trotz der schnellen Bereitstellung eines entsprechenden Signatur-Updates besteht weiterhin ein kritisches Zeitfenster. Effektive InternetSecurity-Lösungen müssen auch diese Sicherheitslücke schließen.

G DATA Security erreicht dies mit der OutbreakShield-Technologie. Innerhalb weniger Minuten wird per Botnetz verbreitete Malware erkannt und blockiert.

## 2.6 Schädliche Webseiten

Dateianhänge von E-Mails sind neben Peer-to-Peer Tauschbörsen - wie beispielsweise Kazaa oder eMule - weiterhin für die meisten Infektionen mit Malware verantwortlich. Neben diesen klassischen Verbreitungswegen hat sich im Laufe von 2006 ein weiterer Verbreitungsweg etabliert.

Immer mehr Infektionen finden über präparierte Webseiten statt. Diese nutzen eine grundlegende Schwachstelle zwischen Virenschutz und Browser. Der Virenschutz greift normalerweise erst, wenn eine Datei auf der Festplatte gespeichert wird. Zuvor lädt der Browser die Datei aber in seinen Speicher und führt deren Code aus. Bis der Virenschutz dann Alarm schlägt ist es mitunter zu spät.

Malwareinfektionen auf Webseiten können auf (mindestens) drei Arten erfolgen:

1. Unter einem schlüssigen Vorwand wird schädliche Software direkt zum Download angeboten. Als Vorwand diente z.B. ein Windows Update oder Plugins, die für die perfekte Wiedergabe der Seite erforderlich waren. So konnten etwa die Filme auf einer pornografischen Seite nur mit einem speziellen "Codec" angesehen werden. Der Download stellte sich dann als eine Variante des Trojan-Downloaders Zlob heraus.
2. Weitaus trickreicher ist aber die Ausnutzung von Sicherheitslücken des Browsers oder seiner Komponenten. Aktive Inhalte, wie JavaScript und ActiveX Controls, ermöglichen Zugriffe auf die im Browser verarbeiteten Daten und teilweise sogar auf das System.
3. Cross-Site Scripting (XSS) nutzt Sicherheitslücken in schlampig programmierten Webanwendungen wie Foren, WebShops, Blogs und Wikis. XSS-Sicherheitslücken stecken in etwa vier von fünf Webanwendungen. Sie werden mit dem wachsenden Web 2.0 auch verstärkt von Malware genutzt werden.

Sicherheitslücken im Browser und in Browserkomponenten - wie beispielsweise Grafikbibliotheken, Flash, RealMedia und Quicktime - werden genutzt, um Rechner mit präparierten Inhalten zu übernehmen.

Diese sog. Drive-by Infektionen auf Webseiten werden nach Einschätzung von G DATA im kommenden Jahr zunehmen.

## 2.7 Weniger Viren - mehr Trojanische Pferde

Die Anzahl der klassischen Viren ist weiterhin rückläufig. Sie spielen im täglichen Geschehen kaum noch eine Rolle, da ihre Verbreitung nicht ökonomisch ist. Lukrativer sind Adware-Programme. Durch Werbeeinblendungen, künstlich erzeugte Klicks auf Webseiten und Banner kann ein Botnetz-Betreiber oder -Mieter enorme Summen verdienen. Ebenso lukrativ ist für Onlinekriminelle die Installation von Werbe-Software. Manche Anbieter zahlen hierfür bis zu 5 \$ pro Installation.

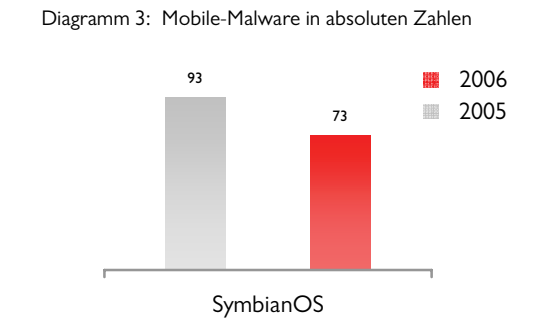
Ein anderes "Geschäftsmodell" sind Verschlüsselungs-Trojaner. Sie verschlüsseln die wichtigen Daten auf einem Rechner und verlangen dann ein Lösegeld meist in Form von Software.

Dieses Modell birgt jedoch den Nachteil, dass die Erpresser mit den Opfern in Kontakt treten müssen. Die Gefahr der Identifikation ist für die Täter hierbei deutlich größer.

## 2.8 Malware für mobile Gerät ohne Bedeutung

Die in Publikationen geschürte Panik vor Schadprogrammen für mobile Geräte – wie beispielsweise PDAs und Handys - ist nach Erkenntnissen der G DATA Security Labs unbegründet. Die Zahl der verbreiteten Malware ist verschwindend gering und hat im Vergleich zu 2005 sogar leicht abgenommen. Gerade bei Handys ist die massenhafte Verbreitung von Schadprogrammen technisch etwas komplexer. Zum einen ergibt sich dies aus der Vielzahl der eingesetzten Betriebssysteme und zum anderen aus der instabilen Einspeisung von Schadprogrammen, beispielsweise via Bluetooth oder Infrarot.

Diagramm 3: Mobile-Malware in absoluten Zahlen



Weitere Aspekte: Der für die Verbreitung erforderliche Aufwand steht für Kriminelle in keinem wirtschaftlich ertragreichen Verhältnis. Dialer könnten jedoch eine neue Dimension erreichen.

Die fehlende Entwicklung eines lukrativen Geschäftsmodells schlägt sich sichtbar im geringen Engagement der Malware-Entwickler nieder.

## 2.9 Daten zu Geld machen - Spyware und Phishing

---

Das größte Geschäft sind derzeit aber Daten. Vielen Internetnutzern ist nicht bewusst, welchen Wert persönliche Daten haben. Im Internet ist ein reger Handel mit 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 100er oder 1.000er Bündel gibt es diese Daten aber auch schon für 2 - 5 \$.

Spieler von Online-Games, wie World of Warcraft, Lineage und Legends of Mir, geraten ebenfalls ins Visier der Datendiebe. Die Virenfamilien, die es auf die Login-Daten zu diesen Spielen abgesehen haben, gehören zu den aktivsten des Jahres 2006. Beliebte Gegenstände und langwierig zu erstellende Charaktere werden in Online-Auktionen mit vierstelligen Dollar-Beträgen gehandelt.

Die Daten werden durch Phishing-Mails und entsprechende Webseiten ergaunert. Insbesondere im Online-Banking hat diese Methode aber mittlerweile fast ausgedient.

Mehr als 80% aller Online-Datendiebstähle erfolgen per Trojanischem Pferd: Key- und Screenlogger stehlen Passwörter bei der Eingabe. Trojan-Spys durchsuchen die Festplatte an geeigneten Stellen nach kritischen Informationen. Proxies und Redirector sorgen dafür, dass ein Angreifer als Man-in-the-Middle alle Eingaben abfangen kann.

Spyware ist neben Trojan-Downloadern die Malware-Kategorie, die 2006 am stärksten zugenommen hat.

## 2.10 Tendenzen und Ausblick

---

Malware wird zunehmend ein Geschäft. Gut organisierte, international agierende Banden vereinen effizienten Handel mit effektiv programmierter Software. Mit großer Kreativität werden bestehende Schwachstellen auf allen Ebenen genutzt. Im kommenden Jahr wird sich daran nicht viel ändern. Die Methoden werden schnell an möglicherweise geänderte Anforderungen angepasst. Phishing-Filter und verbesserter Virenschutz sind also weiterhin obligatorisch.

Ein Hoffnungsträger ist das neue Betriebssystem von Microsoft Windows Vista. Es wurde mit einer Reihe von Sicherheitsfunktionen konzipiert. Ob Vista aber in der Lage ist, den gut organisierten Online-Kriminellen etwas entgegen zu setzen, bleibt abzuwarten. G DATA erwartet hier eine kurze "Gewöhnungsphase" aber keine längerfristige Besserung.

Mit der verstärkten Nutzung von Anwendungen des Web 2.0 wird im kommenden Jahr auch deren Missbrauch zunehmen. Die neuen Möglichkeiten besitzen für Onlinekriminelle eine nicht zu unterschätzende Attraktivität.

Zusätzlich zur vorliegenden Kurzfassung stehen Ihnen detaillierte Informationen zum Thema Malware in unserem ausführlichen Jahresbericht 2006 zur Verfügung. Sie finden ihn unter:

<http://www.antiviruslab.com/whitepapers/AnnualReport.Malware2006DE.pdf>

G DATA Security  
Königsallee 178 b  
D-44709 Bochum  
Tel.. 0234. 9762.239  
[presse@gdata.de](mailto:presse@gdata.de)  
[www.gdata.de](http://www.gdata.de)