# G Data
# MalwareReport

# Halbjahresbericht
# Juli – Dezember 2010

Ralf Benzmüller & Sabrina Berkenkopf
G Data SecurityLabs



Geschützt. Geschützter. **G Data.**

# Inhalt

# Auf einen Blick

- Die Anzahl neuer Computerschädlinge stieg, erwartungsgemäß, auch im Jahr 2010 an, auf 2.093.444. Das macht ein Plus von 32 % gegenüber 2009 und beschreibt einen neuen Rekord.
- Der Anstieg der Zahlen hat sich jedoch im H2 2010 verlangsamt – die Wachstumsraten lagen im einstelligen Prozentbereich.
- Adware ist die Malware-Kategorie, die im zweiten Halbjahr am meisten zugelegt hat (+66 %) und sie erreicht damit einen neuen Höchststand seit dem H1 2009. Insgesamt landet sie auf Platz 6 der aktivsten Kategorien 2010. Malware-Familien aus dem Bereich Online-Games sind in diesem Halbjahr nicht in den Top 10 der aktivsten Familien enthalten. Dafür drängen neue Formen von Betrugssoftware auf die Plätze.

## Trends

- Malware-Autoren legen ein höheres Augenmerk auf Sicherheitslücken in Java
- Die Vorfälle um Stuxnet verdeutlichen, dass Sicherheitsprobleme nicht nur auf Desktop- und Server-PCs beschränkt sind, sondern auch Industrieanlagen in Gefahr sind.

## Ereignisse

- Erfreulicherweise gab es 2010 einige Verhaftungen von im Untergrund bedeutenden Cyber-Kriminellen und auch Abschaltungen von Botnetzen. Bei den Ermittlungen wurde deutlich, dass nur eine länderübergreifende Zusammenarbeit zwischen den Behörden zum Ziel führt, da das organisierte Verbrechen des Internetzeitalters hochgradig international agiert.

## Ausblick für 2011

Wenn man in die nahe Zukunft von 2011 sieht, dann werden wir vermutlich sehen, dass die Java-Plattform ein sehr beliebtes Ziel von Cyberkriminellen wird, wenn nicht sogar das Hauptziel in 2011. Ähnlich, wie es sich mit Adobe in 2010 zugetragen hat.Außerdem werden wir wieder ausgefeilte Botnet-Aktivitäten beobachten und möglicherweise sogar Zusammenschlüsse aus Botnetzen, um möglichen Eingriffen durch Ordnungskräfte zu entgehen.

Gezielte Attacken, ausgelöst durch „Hacktivismus“, Cyber-Spionage oder Cyber-Sabotage oder sogar einer Kombination aus diesen, könnten das größte Problem werden, dem wir 2011 entgegenblicken, denn sie werden anfangs unterhalb des Radars stattfinden. Deshalb ist das wirkliche Problem fast ein anderes: Werden wir die Attacken überhaupt mitbekommen?

Auf jeden Fall werden wir eine weitere Ausnutzung von Sozialen Netzwerken beobachten können. Location Services und URL-Abkürzungs-Services werden den Sozialen Netzwerken in Zukunft noch größere Malware-Probleme bereiten. Das Fehlen von einem Bewusstsein für Privatsphäre bei den Heimnutzern und dem Reichtum an Information über Individuen (auch in der Cloud) macht es für Cyber-Kriminelle möglich, gezielte Attacken zu starten, mit gezielt vorbereiteter Malware – gegen jeden Privatmann, jedes Unternehmen oder jede Organisation der Welt.

# Malware: Zahlen und Daten

## Das Ende des Wachstums?

Auch im zweiten Halbjahr 2010 ist die Anzahl[1] neuer Schädlinge gestiegen auf 1.076.236. Das sind durchschnittlich 5.849 pro Tag. Insgesamt sind 2010 mehr als 2 Millionen (vgl. Diagramm 1) neue Varianten von Schadprogrammen aufgetaucht – 32 % mehr als 2009 und fast 52-mal mehr als 2006.

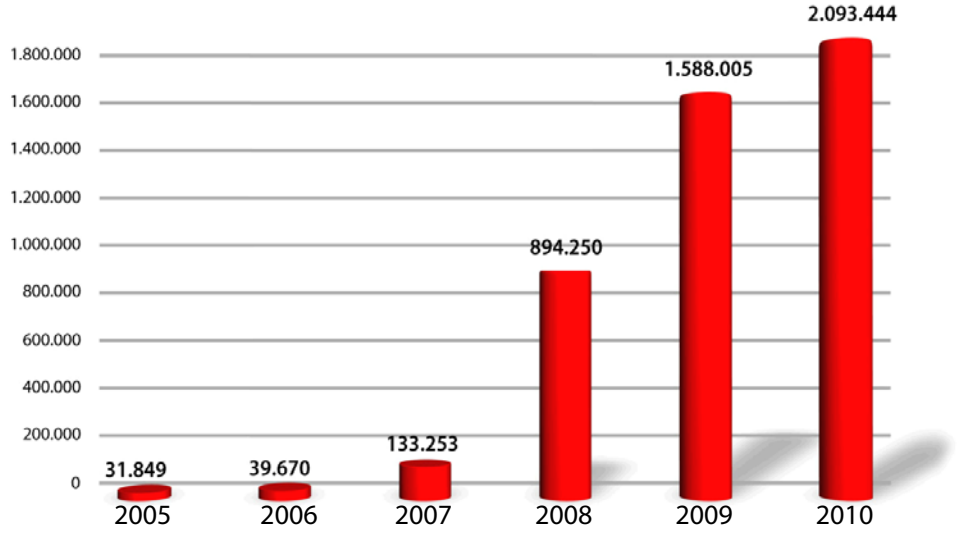



***Diagramm 1:*** *Anzahl neuer Malware pro Jahr seit 2005*

Wenn man allerdings die Verteilung der einzelnen Monate ansieht, bemerkt man, dass sich der Anstieg seit dem 2. Quartal 2009 deutlich verlangsamt hat, nämlich auf 16 % gegenüber dem Vorjahreszeitraum und nur noch 6 % Anstieg gegenüber dem 1. Halbjahr 2010. Die Wachstumsraten lagen zum ersten Mal seit langer Zeit im einstelligen Prozentbereich und es ist vorerst nicht absehbar, dass sich dies ändert.

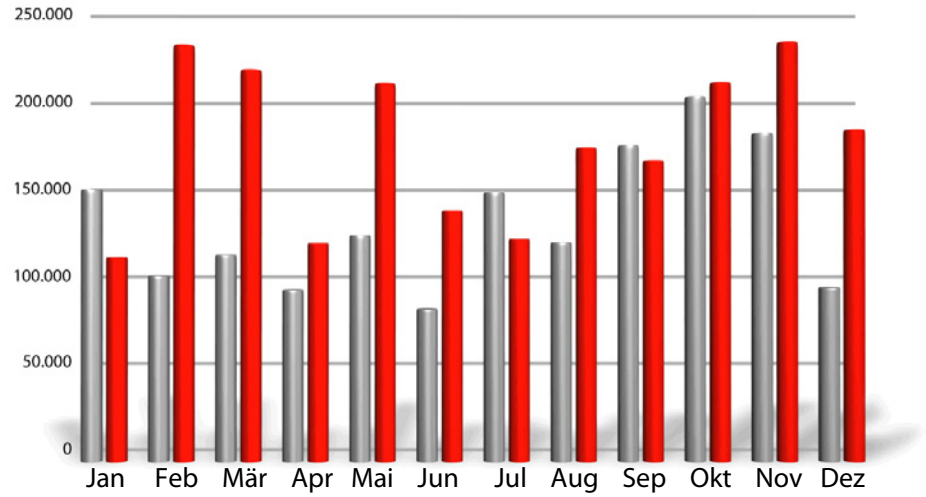



***Diagramm 2:*** *Anzahl neuer Malware pro Monat für 2009 (grau) und 2010 (rot)*

[1]Die Zahlen in diesem Report basieren auf der Erkennung von Malware anhand von Virensignaturen. Sie basieren auf Ähnlichkeiten im Code von Schaddateien. Viele Schadcodes ähneln sich und werden dann in Familien zusammengefasst, in denen kleinere Abweichungen als Variationen erfasst werden. Grundlegend unterschiedliche Dateien begründen eigene Familien. Die Zählung basiert auf neuen Signaturvarianten, die im zweiten Halbjahr 2010 erstellt wurden.

# Malware Kategorien

Malware kann anhand ihrer wichtigsten Schadaktivitäten in Kategorien untergliedert werden. In Tabelle 1 sind die Anzahl und der Anteil der einzelnen Kategorien für die letzten Halbjahre und die Unterschiede zwischen den einzelnen Halbjahren aufgelistet. Die meisten neuen Schädlingsvarianten gab es im Bereich der **Adware**. Das Geschäft mit ergaunerten Klicks und Werbeeinblendungen floriert. Auch die Anzahl der **Downloader** hat erneut überdurchschnittlich zugenommen. Die Anzahl neuer **Backdoors** ist gegenüber dem ersten Halbjahr 2010 wieder deutlich gestiegen (+22 %) und damit auch den Rückgang gegenüber dem Halbjahr 2 aus 2009 kompensiert. Die Zahl neuer **Rootkits** hat im Vergleich zum ersten Halbjahr deutlich abgenommen. Der starke Anstieg aus dem ersten Halbjahr wird damit etwas relativiert. Gegenüber dem Vorjahr entspricht die Steigerung um 5 % in etwa der durchschnittlichen Zunahme. Die Anzahl der **Exploits** nimmt aber jetzt schon zum dritten Mal in Folge ab.

| Kategorie | # 2010 H2 | Anteil | # 2010 H1 | Anteil | Diff. 2010 H2 2010 H1 | # 2009 H2 | Anteil | Diff 2010H2 2009H2 |
|---|---|---|---|---|---|---|---|---|
| Trojanische Pferde | 447.644 | 41,6 % | 433.367 | 42,6 % | +3 % | 393.421 | 42,6 % | +14 % |
| Downloader/ Dropper | 240.124 | 22,3 % | 206.298 | 20,3 % | +16 % | 187.958 | 20,3 % | +28 % |
| Backdoors | 149.723 | 13,9 % | 122.469 | 12,0 % | +22 % | 137.484 | 14,9 % | +9 % |
| Spyware | 113.117 | 10,5 % | 130.175 | 12,8 % | -13 % | 86.410 | 9,4 % | +31 % |
| Würmer | 48.324 | 4,5 % | 53.609 | 5,3 % | -10 % | 51.965 | 5,6 % | -7 % |
| Adware | 34.882 | 3,2 % | 21.035 | 2,1 % | +66 % | 30.572 | 3,3 % | +14 % |
| Tools | 13.499 | 1,3 % | 9.849 | 1,0 % | +37 % | 14.516 | 1,6 % | -7 % |
| Rootkits | 12.305 | 1,1 % | 31.160 | 3,1 % | -61 % | 11.720 | 1,3 % | + 5% |
| Exploits | 1.691 | 0,2 % | 2.495 | 0,2 % | -32 % | 3.412 | 0,4 % | -50 % |
| Sonstige | 14.927 | 1,4 % | 6.751 | 0,7 % | +121 % | 6.595 | 0,6 % | +126 % |
| **Gesamt** | **1.076.236** | **100,0 %** | **1.017.208** | **100,0 %** | **+6 %** | **924.053** | **100,0 %** | **+16 %** |

***Tabelle 1:*** *Anzahl und Anteil neuer Malwarekategorien sowie deren Veränderung in den letzten drei Halbjahren*

# Malware Familien

Anhand der Eigenschaften und Aktivitäten werden Schädlinge in Familien gruppiert. Für einige Familien entstehen ständig neue Varianten. Tabelle 2 enthält die produktivsten Familien der letzten Halbjahre. Nachdem in den letzen Jahren eine Konzentration auf immer weniger Schadfamilien stattgefunden hat, setzt sich der gegenteilige Trend aus dem ersten Halbjahr fort. Die Zahl der aktiven Familien im zweiten Halbjahr 2010 lag mit 2.608 ca. 15 % über den 2.262 aus dem ersten Halbjahr. Betrachtet man die Zahl der aktiven Familien im gesamten Jahr, fällt der Trend jedoch geringer aus:  2009 zählten wir 3.267 verschiedene Familien und 2010 sogar 3.313.

Die obersten Plätze der Rangliste werden von alten Bekannten belegt, wenn auch in unterschiedlicher Reihenfolge. Neu in den Top 10 sind Arten von Betrugssoftware und die Rootkits aus der TDSS-Familie, die sich zum Standard in der Malware-Szene entwickelt haben.

Die Familien aus dem Bereich der Online-Games (OnlineGames, Magania etc.) sind in diesem Halbjahr zum ersten Mal nicht in den Top 10 der produktivsten Malwarefamilien enthalten.

| | # 2010 H2 | Virenfamilie | # 2010 H1 | Virenfamilie | # 2009 H2 | Virenfamilie |
|---|---|---|---|---|---|---|
| 1 | 70.570 | Genome | 116.469 | Genome | 67.249 | Genome |
| 2 | 34.412 | Buzus | 32.830 | Hupigon | 38.854 | PcClient |
| 3 | 31.834 | Hupigon | 30.055 | Buzus | 37.026 | Hupigon |
| 4 | 27.052 | FraudPack | 25.071 | Refroso | 35.115 | Scar |
| 5 | 26.013 | TDSS | 24.961 | Scar | 24.164 | Buzus |
| 6 | 24.276 | FakeInstaller | 21.675 | Lipler | 20.581 | Lipler |
| 7 | 22.411 | Refroso | 19.385 | OnlineGames | 19.848 | Magania |
| 8 | 17.535 | FraudLoad | 17.542 | Palevo | 18.645 | Refroso |
| 9 | 17.272 | BHO | 16.543 | Startpage | 16.271 | Sasfis |
| 10 | 16.645 | FakeAV | 16.517 | Magania | 16.225 | Basun |

***Tabelle 2:*** *Top 10 der aktivsten Virenfamilien. Anzahl neuer Varianten 2009 und 2010*

**Genome**
Die Trojanischen Pferde der „Genome"-Familie vereinen Funktionalitäten wie Downloader, Keylogger, Dateiverschlüsselung.

**Buzus**
Trojanische Pferde der „Buzus"-Familie durchsuchen infizierte Systeme ihrer Opfer nach persönlichen Daten (Kreditkarten, Online-Banking, E-Mail- und FTP-Zugänge), die an den Angreifer übertragen werden. Darüber hinaus wird versucht, Sicherheitseinstellungen des Computers herabzusetzen und das System des Opfers dadurch zusätzlich verwundbar zu machen.

**Hupigon**
Die Backdoor „Hupigon" ermöglicht dem Angreifer unter anderem die Fernsteuerung des Rechners, das Mitschneiden von Tastatureingaben, Zugriff auf das Dateisystem und das Einschalten der Webcam.

**FraudPack**
Die Trojanischen Pferde der Familie FraudPack tarnen sich als eine Vielzahl von legitim erscheinenden Sicherheits-Tools. Allerdings sind diese Tools alles andere als sicher, sondern es handelt sich um Scareware: Die Tools haben keinerlei Sicherheitsfunktion und schaden dem PC mehr, als sie helfen. Schädlinge der Familie FraudPack platzieren unbemerkt zusätzlichen Schadcode auf der Festplatte des Opfers - daher zählt man die Schädlinge auch zu den Droppern.

**TDSS**
Das Rootkit TDSS hat sich mit seinen vielfältigen und technisch sehr ausgereiften Möglichkeiten zur Tarnung von Schaddateien zu einem Standard in der Malware-Szene entwickelt. Es wird verwendet, um die Dateien und Registry-Einträge von Backdoors, Spyware und Adware zu verstecken.

**FakeInstaller**
Bei einem FakeInstaller handelt es sich um ein Betrugsprogramm, das vortäuscht beliebte, legale Software zu installieren. Nach den üblichen Angaben zu Installationpfaden erscheinen entsprechende Fortschrittsbalken, die damit enden, dass eine SMS mit einem bestimmten Inhalt an eine teure Premium-Nummer verschickt werden soll. Die meisten FakeInstaller sind in Russland aktiv.

**Refroso**
Dieses Trojanische Pferd tauchte Ende Juni 2009 erstmals auf. Es hat Backdoor-Funktionen und kann andere Rechner im Netzwerk attackieren.

**FraudLoad**
Die Fraudload-Familie umfasst unzählige Varianten sogenannter Scareware-Programme, die sich dem Anwender als Sicherheits-Software oder System-Tool präsentieren. Dem Opfer wird suggeriert, dass das System auf Infektionen untersucht wird. Um diese angeblichen Infektionen zu beseitigen, wird das Opfer gedrängt, die „Vollversion" zu erwerben und dazu seine Kreditkarteninformationen auf einer speziellen Webseite preiszugeben. Die Infektion erfolgt in der Regel über ungepatchte Sicherheitslücken im Betriebssystem oder über verwundbare Anwendungssoftware des Opfers. Es existieren aber auch Angriffsmethoden, bei denen das Opfer auf Seiten gelockt wird, auf denen vermeintlich Videos mit erotischem oder tagesaktuellem Inhalt zu sehen sind. Um die angeblichen Videos betrachten zu können, soll das Opfer einen speziellen Video-Codec installieren, in dem die Schadsoftware versteckt ist.

**BHO**
Bei den Varianten der BHO-Familie handelt es sich um Plug-ins für den Internet Explorer, die den Benutzer ausspähen. So wird meistens versucht, heimlich Verbindungen zu verschiedenen Servern aufzubauen. Das Plug-in selbst ist eine DLL Datei, aber auch die Dropper, die das Plug-in installieren und aktivieren, werden der Familie zugerechnet.

**FakeAV**
Dieses Trojanische Pferd gibt sich als Anti-Virus Programm oder als ein anderes sicherheitsrelevantes Programm aus. Es simuliert die Entdeckung von mehreren Sicherheitsrisiken oder schädlichen Infektionen auf dem System des Benutzers. Dadurch soll der Nutzer ausgetrickst werden und für eine Software zur Entfernung der gefälschten Alarme Geld bezahlen.

## Plattformen: Windows und Web

In den vergangenen Jahren hat der Anteil der Malware für Windows-Rechner kontinuierlich zugenommen. Das gilt auch für das 2. Halbjahr 2010. Der Anteil der Schädlinge, die nur auf 32-bit Versionen von Windows funktionieren, nimmt allerdings ab. Das wird durch die verstärkte Zunahme an Schädlingen für die moderneren .NET Anwendungen aber mehr als kompensiert. Diese beiden Gruppen machen zusammen 99,5 % aller neu aufgetauchten Computerschädlinge im 2. Halbjahr 2010 aus.

| | Plattform | #2010 H2 | Anteil | #2010 H1 | Anteil | Diff. 2010H2 2010H1 | #2009 H2 | Anteil | Diff. 2010H2 2009H2 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Win32 | 1.056.304 | 98,1 % | 1.001.902 | 98,5 % | +5 % | 915.197 | 99,0 % | +15 % |
| 2 | .NET | 15.475 | 1,4 % | 9.383 | 0,9 % | +65 % | 2.732 | 0,3 % | +466 % |
| 3 | WebScripts | 2.237 | 0,2 % | 3.942 | 0,4 % | -43 % | 4.371 | 0,5 % | -49 % |
| 4 | Scripts[2] | 1.111 | 0,1 % | 922 | 0,1 % | +20 % | 1.124 | 0,1 % | -1 % |
| 5 | Java | 517 | < 0,1 % | 225 | < 0,1 % | +130 % | 31 | < 0,1 % | +1.568 % |
| 6 | *ix[3] | 382 | < 0,1 % | 226 | < 0,1 % | +69 % | 37 | < 0,1 % | +932 % |
| 7 | NSIS[4] | 130 | < 0,1 % | 260 | < 0,1 % | -50 % | 229 | < 0,1 % | -43 % |
| 8 | Mobile | 55 | < 0,1 % | 212 | < 0,1 % | -74 % | 120 | < 0,1 % | -54 % |

***Tabelle 3:*** *Top 8 Plattformen in den letzten drei Halbjahren*

[2] "Scripts" sind Batch- oder Shell-Skripte oder Programme, die in den Skriptsprachen VBS, Perl, Python oder Ruby geschrieben wurden
[3] *ix bezeichnet alle Unix-Derivate, wie z.B. Linux, FreeBSD, Solaris etc.
[4] NSIS ist die Installationsplattform, die u.a. dazu genutzt wird den Mediaplayer Winamp zu installieren

Die restlichen 0,5 % werden von Web-basiertem Schadcode angeführt. Dessen Anzahl hat allerdings deutlich abgenommen. Das liegt u.a. daran, dass auf Webseiten in den letzten Monaten verstärkt Sicherheitslücken in Java verwendet werden, um Schadcode auszuführen. Das erklärt auch warum der Anteil an Java-Malware am deutlichsten gestiegen ist[5]. Auch die Anzahl von Schadcode für Unix-basierte Rechner hat stark zugenommen, während die Zahl der Familien aus dem Bereich der Malware für Smartphones am deutlichsten abgenommen hat.

## Trends 2011

| Kategorie | Trend |
|---|---|
| Trojanische Pferde | → |
| Backdoors | → |
| Downloader / Dropper | → |
| Spyware | → |
| Adware | → |
| Viren/Würmer | → |
| Tools | → |
| Rootkits | ↗ |
| Exploits | → |
| Win32 | ↘ |
| WebScripts | ↗ |
| Java | ↗ |
| MSIL | ↗ |
| Mobile | ↗ |
| *ix | → |

[5] Siehe auch: Kapitel „Angriffe: Java löst PDFs ab“

# Top-Themen des zweiten Halbjahres 2010

## WikiLeaks ruft „Hacktivisten“ auf den Plan

Die erneuten Veröffentlichungen von teils geheimen Dokumenten der US-Regierung lösen einen enormen Aufruhr aus und eröffnen eine heftig geführte Debatte über den Umgang mit Daten und Informationen. Am 25. Juli veröffentlichte die nicht-kommerzielle Webseite WikiLeaks das so genannte „Afghan War Diary“. Doch die Enthüllungen des 28. November 2010 übertrafen die Brisanz der Dokumente aus dem Juli. Insgesamt wurden 251.287 diplomatische US-Berichte (engl.: cables) aus der Zeit von 1966 bis 2010 ins Netz gestellt, die nun als „Cablegate“ bekannt geworden sind. Kurz vor der Veröffentlichung wurden WikiLeaks-Server nach eigenen Angaben von DDoS-Angriffen getroffen. Als mutmaßlicher Informant gilt Bradley Manning, Private First Class der US-Streitkräfte, dem eine 52-jährige Haftstrafe droht, sollte er in allen Anklagepunkten für schuldig gesprochen werden. Laut Medienberichten untersagte das Pentagon seinen Mitarbeitern nicht nur das Ansehen der WikiLeaks-Dokumente, sondern sperrte auch den Zugang aus dem US Air Force Netzwerk auf rund 25 Medienseiten, die die Dokumente diskutierten und darüber berichteten.

Durch den entstandenen öffentlichen Druck haben einige Internetunternehmen (z.B. Amazon.com) die WikiLeaks Dokumente von ihren Webservern gelöscht oder die Spendenkonten und den Zahlungsverkehr zu WikiLeaks gesperrt (z.B. PayPal und MasterCard). Damit zogen die Firmen sich den Zorn vieler WikiLeaks-Anhänger zu. Die Sympathisanten starteten die „Operation PayBack“ und führten DDoS-Attacken gegen die Schweizer PostFinance, Mastercard, Visa, PayPal, EveryDNS und Amazon durch. Die betroffenen Seiten waren daraufhin für einige Zeit nicht erreichbar. Nach unseren Erkenntnissen scheidet ein Angriff aus Kreisen des organisierten Verbrechens jedoch aus. Die Angriffe gingen stattdessen auf Sympathisanten von WikiLeaks zurück, die frei verfügbare Tools für Lasttests von Servern dazu nutzten, um die Seiten mit Anfragen zu überlasten. Diese Form des Protests wurde bislang von Privatpersonen wenig genutzt. Die zumeist jungen Männer, die sich den DDoS-Attacken gegen Webseiten aus Idealismus anschlossen, waren sich meist wohl nicht darüber bewusst, dass sie mit strafrechtlichen Konsequenzen rechnen müssen. In den Niederlanden wurden zwei Männer, 16 und 19 Jahre alt, in diesem Zusammenhang verhaftet.

Nicht nur WikiLeaks als Plattform geriet in die Kritik. Der Sprecher und Chefredakteur von WikiLeaks, der Australier Julian Assange, wurde am 7. Dezember zwischenzeitlich in London (England) festgenommen. Dort ist er nun gegen Kaution frei, jedoch bis zur Auslieferungsanhörung unter Hausarrest gestellt. In Schweden soll er sich wegen mutmaßlichem sexuellen Missbrauchs verantworten. Assange bestreitet diese Vorwürfe und beschreibt sie als politisch motiviert und abgekartetes Spiel. In den USA prüft man wohl rechtliche Schritte gegen Assange, allerdings ist noch nicht bekannt, wie der Grund für die Anklage lauten könnte – In den Medien werden „Verschwörung“ und „Spionage, nach einem Gesetz von 1917,“ diskutiert. Es ist allerdings zweifelhaft, ob diese Gesetze gegen die immer wieder beschworene Redefreiheit bestehen können.

## Industrieanlagen in Gefahr: Der Fall Stuxnet

Über den Computer-Wurm Stuxnet wurde zum ersten Mal im Juli 2010 berichtet. Die Einzelheiten wurden schrittweise und erst nach teils sehr aufwändigen Analysen ermittelt. Die sogenannte „LNK Sicherheitslücke“ (CVE-2010-2568) war dabei nur die Spitze des Eisbergs. Nur weil diese Lücke zu

einer unkontrollierten Verbreitung von Schadcode aus dem Stuxnet-Umfeld führte, kamen die Details über die Schadsoftware nach und nach ans Tageslicht. Insgesamt wurden vier bis dahin unbekannte Sicherheitslücken genutzt, um die Schädlinge zu verbreiten und den Schadcode auf den Zielsystemen mit den notwendigen Rechten auszuführen. Davon waren nicht nur Windows-Systeme betroffen.
Um die Schaddateien zu verstecken, werden Rootkits eingesetzt und gestohlene Zertifikate verwendet. Ziel der Angriffe ist eine bestimmte Steuersoftware für Industriesteueranlagen der Firma Siemens. Diese Software erstellt mit einer eigenen Programmiersprache (Step 7) Programme, mit denen Industrieanlagen gesteuert werden können. Die eigentliche Schadfunktion wird beim Kompilieren des Steuercodes für die Maschinenanlage in das entstehende Steuerprogramm eingeschleust. Lange Zeit war jedoch unklar, was der eigentliche Hintergrund der Attacke war. Schließlich stellte sich heraus, dass die Zentrifuge einer atomaren Wiederaufbereitungsanlage im Iran für kurze Zeit angehalten wurde. Durch einen kurzen Stopp vermischen sich die zu trennenden Isotope und die Qualität des aufbereiteten Materials wird vermindert.
Die Entwicklung des gesamten Codes für den Stuxnet-Schädling erforderte das Zusammenspiel von vielen Spezialisten, die mit hohem finanziellen Aufwand arbeiten konnten, und erforderte insgesamt mehrere Mannjahre. Wer hinter der Entwicklung steckt, ist unklar und sorgt für viele Spekulationen.

Der Fall Stuxnet zeigte, dass es Personenkreise gibt, die mit hohem Aufwand Schadcode entwickeln, um gezielt Industrieanlagen – auch aus dem Bereich der sogenannten Kritischen Infrastrukturen - zu manipulieren. Die Vorfälle um Stuxnet verdeutlichen, dass Sicherheitsprobleme nicht nur auf Desktop- und Server-PCs beschränkt sind. Im Prinzip können alle Steuergeräte mit IP-Adresse missbraucht werden.

Sicherheit wurde in vielen Industrieanlagen lange Zeit vernachlässigt. Die Enthüllungen um Stuxnet machen aber klar, dass man sich hier Gedanken und Sorgen machen muss, nicht nur im Bereich der als kritisch erfassten Infrastrukturen.

## Angriffe: Java löst PDFs ab

Sowohl die gestiegene Produktivität im Bereich von Java-basiertem Schadcode als auch die Auswertung der monatlichen G Data Malware Statistiken zeigte zum Ende des Jahres eine deutliche Veränderung der Bedrohungslage. Onlinekriminelle setzen für die Verbreitung von Schadcode stärker als in den vergangenen Monaten auf Sicherheitslücken in Java. Im Oktober änderte sich erstmals seit Februar die Top-Platzierung der Malware Rangliste: Java.Trojan.Exploit.Bytverify.N verdrängte JS:Pdfka-OE [Expl] schon im Oktober von Platz 1 und wurde erst im Dezember wieder abgelöst, von Java.Trojan.Downloader.OpenConnection.AI, einer weiteren Java-basierten bedrohung.
Auch JavaScript-basierte Downloader vom Typ JS:Downloader, sind aktuell äußerst aktiv und werden von den Malware-Autoren ständig weiter entwickelt. Aktuell sind jeden Monat Versionen dieses Schadcodes in den Top 10 zu finden.

Sicherheitslücken in Java bieten den Tätern technisch viel Potenzial und die Herstellung und Verbreitung von Schadcode ist im Vergleich zu anderen Infektionsformen deutlich einfacher – Die Angriffsbausteine können einfach in sogenannte Exploit-Kits eingebaut werden. Die Verbreitung

von Java auf heimischen und betrieblichen PCs ist enorm: Im zweiten Halbjahr war auf durchschnittlich 79 % aller Rechner ein Java Plug-In installiert[6].

Außerdem haben die Warnmeldungen der vergangenen Monate zum Thema PDF-Lücken auf Anwenderseite zudem zu einer gestiegenen Sensibilisierung geführt und die Hersteller der PDF-Reader haben Dank der Vielzahl der Sicherheits-Updates die Entwicklung lauffähiger Schadprogramme deutlich erschwert. Insbesondere die Neuerungen in Version 10 des Adobe Reader erschweren es deutlich Schadcode auszuführen.

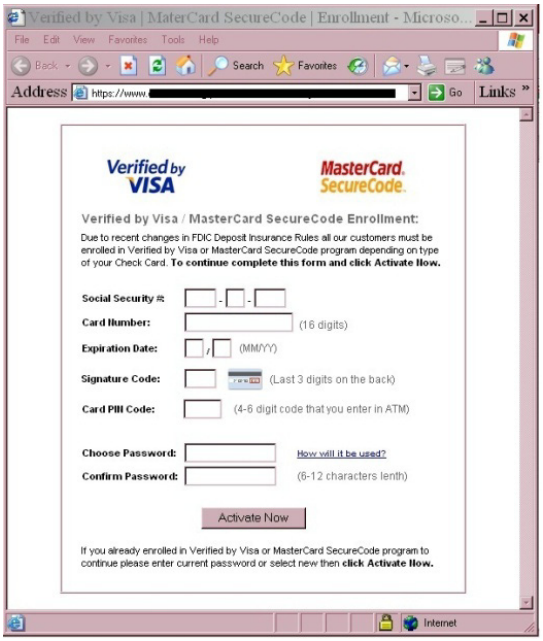
[6] Quelle: http://www.statowl.com/java.php

# Ereignisse des zweiten Halbjahrs 2010

## Juli 2010

13.07. **Microsoft** stellt den **Support** für sein Produkt **Windows XP 32-bit Service Pack 2** ein. Kunden sollten ein Upgrade auf Windows Vista, bzw. Windows 7 machen oder mindestens das Service Pack 3 für Windows XP installieren (Support bis April 2014). Kunden, die weiterhin Windows XP benutzen, geraten so stärker ins Visier von Cyberkriminellen.

15.07. Der **ZeuS Banking Trojaner** zielt nun auch auf die Kreditkarten-Sicherheitstechniken „Verified by Visa“ und „SecureCode Protection“ ab. Die Benutzer von Onlinebanking werden auf einem gefälschten, in den Browser injizierten Fenster aufgefordert, ihre Sozialversicherungsnummer und Kreditkarteninformation / Bankkarteninformationen einzugeben – obwohl dies eigentlich beim reinen Banking-Vorgang nicht notwendig ist. Es seien 15 führende US Finanzinstitute Ziel dieser Angriffe.

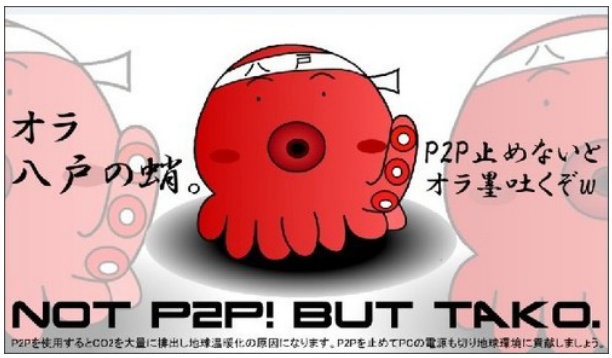



***Screenshot 1:*** *Das von ZeuS gefälschte Eingabefenster für Banking-Informationen (Quelle: trusteer.com)*

28.07. Das FBI gibt bekannt, dass nun auch der mutmaßlichen Urheber des **Mariposa-Botnetzes** identifiziert und verhaftet wurde. Die slowenische Polizei schnappte den 23-jährigen slowenischen Staatsbürger, der unter dem Namen „Iserdo“ bekannt ist. Behörden aus Spanien, den USA und Slowenien hatten in den zwei Jahre andauernden Untersuchungen das „Schmetterlings-Botnetz“ ausgehoben.

## August 2010

05.08. Die **Tokyo Metropolitan Police** verhaftete einen 27-jährigen Mann, Masato Nakatsuji, der einen **Computervirus** verbreitet hat, der sämtliche Daten auf einem PC löscht und sie durch Oktopus- und Tintenfisch-Cartoonbilder im Manga-Stil ersetzt. Vor dem Löschen werden alle Dateien noch zu einem Webserver verschickt. Die Polizei hat bis jetzt Daten von **20.000 Nutzern** identifiziert. Nakatsuji, der 2008 schon einmal wegen Urheberrechtsverletzungen verurteilt wurde, glaubt nicht, dass er Probleme bekommt, denn dieses Mal habe er die Bilder der Meeresbewohner für den **„Ikatako-Virus“** alle selbst entworfen und nicht gestohlen.




***Screenshot 2:*** *Ein Ikatako-Manga (Quelle: http://birthofblues.livedoor.biz)*

16.08. Die Firma Scapegaming muss über **88 Millionen US$ als Strafe** an den Spielekonzern **Blizzard** bezahlen. Scapegaming hatte unerlaubt private WOW-Spieleserver eingerichtet und sich diese von den Nutzern auch bezahlen lassen (etwa 3 Millionen US$ in drei Jahren). Das Gericht urteilte auf Urheberrechtsverletzung wegen unrechtmäßigem Gewinn.

19.08. Das Weltunternehmen **Intel kündigt an**, den kalifornischen Security Software Hersteller **McAfee Inc zu übernehmen.** für einen Gesamtbetrag von etwa 7,68 Milliarden US-Dollar. McAfee wird eine 100%ige Tochter von Intel sein.

23.08. **Microsoft** warnt vor einer Sicherheitslücke im Zusammenhang mit Programmbibliotheken. Programme könnten präparierte DLL Dateien laden, wenn sie im selben Verzeichnis liegen, wie die startende Datei, und so Schadcode ausführen – man nennt diese Attacke **DLL-Spoofing**. Die aktuell einzige Methode, die Gefahr zumindest abzuschwächen, liegt in der Deaktivierung des WebDAV Dienstes und des File Sharing Protokolls SMB. Secunias Liste mit 160 gefährdeten Programmen zeigt lediglich 22, die die Sicherheitslücke behoben haben (Stand: 6.12.2010)

28.08. Die deutsche Discounter-Kette „**Schlecker**“ war von einem **Datenleck** betroffen. Rund 150.000 Kundendatensätze und 7,1 Millionen E-Mail-Adressen von Newsletter-Abonnenten konnten ausgelesen werden.

## September 2010

06.09. Die Schadenssumme, die durch **Internetkriminalität in Deutschland** entsteht, schätzen das Bundeskriminalamt und der Branchenverband Bitkom für 2010 auf **17 Millionen Euro**. Umfragen ergeben, dass rund 43 % der Deutschen von einer Infektion ihres PCs mit Schadsoftware betroffen waren/sind. 5 % der Internet-Nutzer erlitten bis jetzt **finanziellen Schaden** durch Schadprogramme / Datenklau.

08.09. Die belgische Bundespolizei bestätigt, dass eine europaweite Aktion von **Europol** gegen **Internetpiraterie** stattgefunden hat. Es wurden Durchsuchungen, 50 Beschlagnahmungen und auch Festnahmen in 14 europäischen Ländern vorgenommen. Die sogenannten Release Groups seien für **80 % aller neuen, illegal online gestellten Filme** auf Niederländisch verantwortlich. Die Verbreitung von urheberrechtlich geschützter Musik, Software und PC-Spielen wird ihnen ebenfalls angelastet.

14.09. Betreiber des deutschsprachigen **Social Networks** Lokalisten.de schlossen kurzfristig eine Sicherheitslücke, die es Angreifern möglich machte, **Cross Site Scripting** auf der Plattform mit Hilfe von persönlichen Nachrichten auszuführen. Die Textfilter konnten verschachtelten JavaScript Code nicht filtern.

14.09. Durch eine **Sicherheitslücke** in einem Video-PlugIn von OpenX Ad-Servern konnten Kriminelle in ausgelieferten **Werbebannern** auf Webseiten Schadcode ausliefern. Die infizierten Anzeigen waren unter anderem auf The Pirate Bay, esarcasm und AfterDawn.

15.09. Das **Deutsche Bundesamtes für Sicherheit in der Informationstechnik** (BSI) und der Verband der deutschen Internetwirtschaft eco starten heute mit weiteren Partnern ihr **Anti-Botnet-Beratungszentrum**. Im Kampf gegen Botnetze gibt es Software zum Download, Informationen und Beratungsangebote.

20.09. ZoneAlarms Marketingfirma Check Point wird kritisiert, da sie eine für die **Sicherheitsbranche** eher unglücklich Form der Verkaufsförderung eingesetzt haben: Kunden der kostenlosen ZoneAlarm Firewall wurden durch ein Pop-Up animiert, das kostenpflichtige Sicherheits-Komplett-Paket zu kaufen. Die Aufmachung der **Werbung** erinnert jedoch sehr an **Scareware**.


***Screenshot 3:*** *Werbungs Pop-Up in der kostenlosen ZoneAlarm Firewall (Quelle: http://www.theregister.co.uk)*

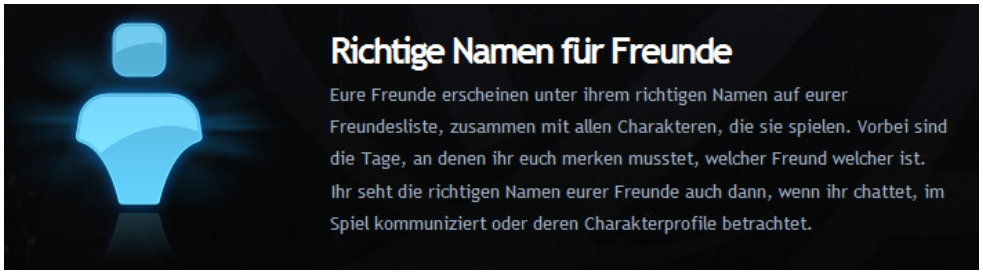
22.09. Der 49-jährige Amerikaner Bruce Raisley wurde von einem Gericht verurteilt. Er hatte seinen eigenen Computerschädling programmiert, um rund **100.000 Zombie-PCs** für ein Botnetz zu rekrutieren. Dieses Botnetz nutze er, um DDoS-Attacken auf Webserver zu fahren, die Kopien von 2 Magazin-Artikeln über ihn veröffentlichten. Der Schaden, den die Webseiten durch Raisleys **persönlichen Rachefeldzug** erlitten, beträgt rund 100.000 US$.

23.09. Eine deutsche Firma zur Verarbeitung von **EC-Karten-Zahlungen** (Easycash GmbH) benutzt die bei der Kaufabwicklung entstehenden Daten laut NDR nicht konform zum **Bundesdatenschutzgesetz**, sondern leitet aus den Daten eigene Empfehlungen ab, die Aussagen über die Zahlungsfähigkeit und Kreditwürdigkeit eines Karteninhabers zulassen sollen.

24.09. Das Kinderhilfswerk der Vereinten Nationen, **UNICEF**, verlinkte ungewollt eine Liste mit 147 Firmendaten der Aktion „Spenden statt Schenken“ auf dem Jahr 2009 ins Internet. Über die Suchmaschine Google waren die Daten zugänglich geworden. Ursache für die Datenpanne war ein Serverumzug, bei dem Schutzeinstellungen fehlerhaft vorgenommen wurden.

27.09. Der Internet-Bezahldienst **PayPal** gerät unter Druck, nachdem bekannt wird, dass Transaktionen mit fremden Kreditkartendaten bis zu **1.500 Euro** ohne große Probleme möglich seien. Die **Verifizierung der Kundendaten** nehme Zeit in Anspruch und innerhalb dieser Zeit „gibt es keine Beschränkung für die Bezahlung, den Empfang und die Entnahme von Geldern“, so eine Sprecherin.

30.09. **Blizzard** kündigte im Juli an, dass in Zukunft alle Beiträge in den eigenen Foren mit den realen Namen von Spielern angezeigt werden (der **Real ID**). Die Games sollen sich mit diesem und anderen Features dieser Art mehr **an Soziale Netzwerke angleichen**. Die Spiele-Community reagiert mit Ablehnung. Ein Nutzer veröffentlichte z.B. in seinem Blog viele persönliche Informationen von Activision / Blizzard Mitarbeitern, die er mit Hilfe der Real ID im Internet fand (u.a. Familienstatus, Adressen, Namen von Angehörigen, etc.). **Blizzard änderte nun seine angekündigten Pläne** dahingehend, dass die Forenbeiträge weitgehend anonym bleiben und die Real ID Features im Spiel optional sind.




***Screenshot 4:*** *Beschreibung einer der RealID-Funktionen (Quelle: us.battle.net)*

## Oktober 2010

01.10. Das **FBI** schließt seine **Operation Trident BreACH** erfolgreich ab, die gegen Cyberkriminelle und vor allem gegen das **ZeuS Botnet** vor über 18 Monaten ins Leben gerufen wurde. In den letzten Tagen wurden in den USA, den Niederlanden, der Ukraine und dem Vereinigten Königreich 16 Durchsuchungsbefehle vollstreckt und 39 gezielte Festnahmen durchgeführt. Die Summe des gestohlenen Geldes beläuft sich auf 220 Millionen US-Dollar.

09.10. Laut Medienberichten dürfen **Zollfahnder** in Deutschland mit einer richterlichen Anordnung auch **VoIP-Telefonate mithören** und handeln damit konform zum Urteil des Bundesverfassungsgerichts zur sogenannten Online-Durchsuchung. Ermittler spielen heimlich ein Programm zum Mitlauschen auf den Rechner des Verdächtigen und greifen die Sprachdaten ab, **bevor sie verschlüsselt werden**.

17.10. Die amerikanische Webseite des AV-Herstellers **Kaspersky** verbreitete heute für fast 4 Stunden **Scareware** an die Internetuser. Hacker nutzen eine Schwachstelle in einer Applikation eines Drittanbieters aus, um Kunden, die die Kaspersky-Produkte herunterladen wollten, auf eine infizierte Webseite mit FakeAV umzuleiten.

22.10. Das im Mai aktivierte **Cyber Command der US-Regierung** nimmt nun seinen Dienst auf. Der genaue Auftrag der Spezialeinheit mit Basis in Ft. Maede, Maryland, ist jedoch weiterhin unklar. Präsident Obama sagte im Mai: „Es ist nun klar, dass **Cyber-Bedrohung** eine der größten Herausforderungen für die wirtschaftliche und nationale Sicherheit unserer Nation ist." Er versicherte allerdings, dass die neue Spezialeinheit keine Überwachung von Privatnetzwerken oder E-Mail Accounts durchführen wird - das sei nicht Sinn und Zweck.


***Abbildung 1:*** *Das offizielle Logo des US Cyber Commands*

27.10. **Mozilla** berichtet über eine kritische Sicherheitslücke in ihren Browsern Firefox 3.5 und 3.6, die erstmals von Hackern ausgenutzt wurde, die ein Trojanisches Pferd auf der **Webseite des Friedensnobelpreises** hinterlegten, dass per **Drive-by-Download** auf den Rechner des Opfers gespielt wurde. Die Schwachstelle wurde binnen 48 Stunden durch ein Browserupdate auf 3.6.12 geschlossen und galt Angaben zu Folge nur für Benutzer von Windows 2000 und Windows XP.

29.10. Der **Ermittlungskommission „Katusha"** ist es gelungen, eine **internationale Bande auszuheben**, die Online-Banking Transaktionen im großen Stil manipuliert hat. Die Hintermänner konnten in Kooperation mit estnischen und britischen Behörden ermittelt werden und sollen über 260 Überweisungen manipuliert und **mindestens 1,65 Millionen Euro erbeutet** haben. Die PCs der Opfer wurden mit manipulierten PDF Dateien und durch Drive-by-Downloads mit Schadsoftware infiziert.

# November 2010

04.11. Der mutmaßliche Betreiber des **Botnetzes Mega D** wurde verhaftet. Oleg Nikolaenko, ein 23-jähriger Russe, wurde in Las Vegas vom FBI gefasst. Bislang ist unklar, ob er allein hinter dem Botnetz steckt, dass für **19 % des weltweit versendeten Spams** verantwortlich sein soll - 2008 gingen laut SPAMfighter sogar 32 % auf das Konto von Mega D. Der Moskauer Nikolaenko wird wegen Verletzung des Can-Spam-Act angeklagt werden.

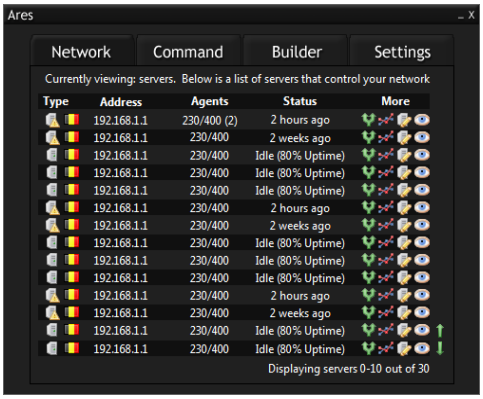
05.11. Der sogenannte **„Origami Trojaner“** verbreitet sich vornehmlich in Russland und der Ukraine. Der „sehr leistungsfähige Trojaner“, der vor allem **persönliche Daten** stiehlt, hat es auf **Bankdaten** abgesehen. Es ist nicht üblich, dass Malware, die mutmaßlich aus Russland, bzw. der Ukraine kommt, auch dort Rechner angreift - das widerspricht einem ungeschriebenen Gesetz.

8.11. In Florida (USA) ist die Polizei einem **Einbrecher** auf die Schliche gekommen, weil dieser vergessen hatte, sich aus seinem **MySpace Profil** auszuloggen - Er hatte den Computer im Schlafzimmer des Hauses benutzt, in das er eingebrochen war. Der 18-jährige wurde in der Nähe des Hauses aufgegriffen.

09.11. Keine 24 Stunden nach der Veröffentlichung der **Software zum neuen deutschen elektronischen Personalausweis** ist eine Sicherheitslücke aufgedeckt. Anders als bei Tests des Chaos Computer Clubs (CCC) musste nun der Rechner des Nutzers nicht mit Schadcode verseucht werden. Angreifer können nach Angaben von Blogger Jan Schejbal mit eigenen SSL-Zertifikaten die Updatefunktion der Applikation austricksen und dem Nutzer eigene, schädliche Software unterschieben.

12.11. Der 22-jährige **David Kernell**, der 2008 unter anderem in den privaten E-Mail Account der **amerikanischen Vizepräsidentschaftskandidatin Sarah Palin** einbegrochen war, wurde heute in zu einem Jahr und einem Tag Gefängnisstrafe verurteilt. Ein Anwalt des US Justizministeriums sagte, Kernells Tat sei „eine politische Tat gewesen, mit politischen Motiven, um eine politische Kampagne entgleisen zu lassen“. Kernell hatte im Internet persönliche Informationen über Palin gesammlt und damit die **Sicherheitsfrage** ihres E-Mail Accounts beantwortet. Er veröffentlichte dann Bilder und E-Mails von Sarah Palin und sorgte damit für weltweites Aufsehen.

18.11. Google startet seinen neuen Dienst **Google StreetView**. Das umstrittene Projekt, das schon zu Beginn des Jahres für viel Aufregung gesorgt hatte, schaltet heute **Bilder aus 20 deutschen Städten** frei, die der User virtuell durchfahren kann. Laut Medienberichten reichten vor dem Start schon **250.000 Menschen Widerspruch** gegen die Veröffentlichung von Bildern ihres Hauses ein. Google versprach, Nummernschilder und Gesichter generell unkenntlich zu machen.




***Screenshot 5:*** *Das Ares Command & Control Interface*

18.11. Die Experten der **G Data SecurityLabs** entdecken einen **potentiellen Nachfolger des ZeuS-Trojaners**. Der Autor des Schadcodes preist sein Trojanisches Pferd in einem Forum an und verspricht ein baldiges Release. Da die Beschreibung des Schädlings **sehr viele Variationen** verspricht, wäre er praktisch für jedes Angriffsziel verwendbar.

Ein Starterpaket soll für 850 US-Dollar verfügbar werden.

23.11. Aus dem Wohnzimmer seiner Mutter steuerte der 33-jährige Schotte Matthew Anderson ein **Botnetz** und verschickte damit Millionen Spam E-Mails, stahl persönliche Daten von Opferrechnern und spionierte seine Opfer sogar mit deren Webcam aus. In seinem eigenen Zuhause habe der Vater von fünf Kindern keinen Breitband-Internetzugang gehabt. Er wurde zu **5.000 £ und 18 Monaten Gefängnis** verurteilt.

24.11. Die **französische Regierung** will ab dem 1.1.2011 eine Steuer auf den „Ankauf von Online-Werbungsdiensten" einführen. Bezahlt werden muss diese Steuer von den Online-Unternehmen, die die Aufträge annehmen - allerdings nur von denen, die ihren Sitz in Frankreich haben. Die Regierung rechnet mit Zusatzeinnahmen von 10 bis 20 Millionen Euro pro Jahr durch die so genannte **„Google-Steuer"**.

28.11. **WikiLeaks** veröffentlicht knapp eine Viertelmillion teils als geheim klassifizierter **US-Depeschen** im Internet. Im Zusammenhang damit werden in den Niederlanden im Dezember zwei junge Männer, 16 und 19 Jahre alt, festgenommen werden. Auch der WikiLeaks-Sprecher, **Julian Assange**, wird zeitweilig verhaftet und später unter Arrest gestellt. Detaillierte Informationen dazu im Kapitel „Top-Themen des zweiten Halbjahres 2010".

## Dezember 2010

01.12. **Musikpiraterie** der besonderen Art wird zwei Männern aus Nordrhein-Westfalen (Deutschland) vorgeworfen. Ein 17-jähriger und ein 23-jähriger verschafften sich Zugang zu E-Mail Konten von Personen **im Umfeld prominenter Musiker** und stahlen so noch unveröffentlichte Songs. Sie sollen mit Trojanischen Pferden **infizierte MP3-Dateien** verbreitet haben, um dadurch Zugang zu den Rechnern zu erlangen. Die Polizei schaltete sich ein, als die Männer ihre Beute bei einem Kelly-Clarkson Online-Fanclub anpriesen.

3.12. Die große Kammer des **Schweizer Parlaments** ist besorgt um die **Sicherheit wichtiger Kommunikations- und Datennetze**. Sie verlangt Gesetze zur aktiven und passiven Sicherung dieser. Auch der Verteidigungsminister sieht **Handlungsbedarf im Bezug auf die Themen Cyberwar und Cyberdefence** – es müssten Absprachen über eine Koordination getroffen werden. Die Politiker der Grünen sehen ein pauschales Gesetz als schwierig an, denn die Bürger sollten nicht eingeschränkt werden dürfen.

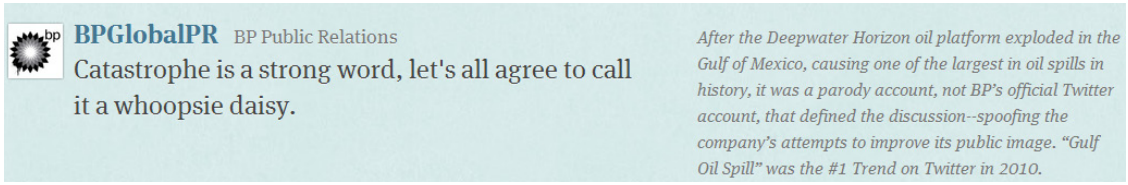
08.12. Das **Landeskriminalamt Sachsen** teilt mit, dass **Betrugsfälle beim Online-Banking** in Sachsen stark zugenommen haben. In den Monaten Januar bis einschließlich September gab es **407 registrierte Fälle**, die einen Schaden von knapp 2 Millionen Euro verursachten. 2009 enstanden rund 813.00 Euro Schaden bei 171 registrierten Fällen.

10.12. Ein 44-jähriger Mann aus Dülmen (Deutschland) wurde zu **einem Jahr und 10 Monaten Haft auf Bewährung** verurteilt, weil er sich mit Hilfe eines Trojanischen Pferdes Zugang zu **fast 100 privaten Rechnern** verschaffte und die Besitzer **mit ihrer eigenen Webcam beobachtete**. Das jüngste Opfer war ein 13-jähriges Mädchen, das nach einiger Zeit bemerkte, dass die Kontrollleuchte ihrer Webcam nicht mehr ausging und sich mitteilte.

14.12. In **Colorado (USA)** ist dem „Sheriff's Department" eine weitereichende **Datenpanne** unterlaufen. **200.000 Datensätze** von Verdächtigen, Opfern und Informanten waren online ungeschützt zugänglich. Nach dem Kopieren auf einen sicher geglaubten Server im April,

durch einen Abteilungsmitarbeiter, wurden die Daten unbeabsichtigt öffentlich und könnten so eine **Gefahr für die aufgelisteten Personen** darstellen. Aufgefallen ist das Datenleck im November, als eine Person der Liste den eigenen Namen im Internet fand.

18.12. Der Micro-Blogging Dienst **Twitter** veröffentlicht seine **Jahresstatistiken 2010**: Auf Platz 1 der Top Trends liegt die Ölkatastrophe im Golf von Mexiko, gefolgt von der FIFA Fußball-Weltmeisterschaft und dem Kinofilm Inception. Sogar der Kraken Paul schaffte es in die **Top Ten**, wenn auch nur auf Platz 10. Auf Platz 4 der ‚**Most powerful Tweets**' schaffte es ein Kommentar zur Deepwater Horizon Katastrophe, gezwitschert von einem Spaß-Account:




***Screenshot 6:*** *Jemand erstellte einen Spaß-Account, um Tweets dieser Art im Zusammenhang mit der Ölkatastrophe zu posten (Quelle: http://yearinreview.twitter.com/powerful-tweets/)*

25.12. Das US-amerikanische **Magazin TIME** ernennt den Facebook-Gründer **Mark Zuckerberg** zur **Person des Jahres 2010**. Er habe die Gesellschaft verändert und über 550 Millionen Menschen weltweit vereint – etwa 70 % der Facebook-Nutzer leben außerhalb der USA. Die britische Wirtschaftszeitung **Financial Times** dagegen würdigte **Steve Jobs** als herausragendste Persönlichkeit 2010.

28.12. Die Polizeichefin aus **Zuidwest-Drenthe** (Niederlande) wurde aufgrund eines unpassenden **Twitter-Beitrags** suspendiert. Sie hatte voreilig Mutmaßungen zur Todesursache von zwei weiblichen Personen gezwitschert und damit möglicherweise die Persönlichkeitsrechte der Opfer verletzt.