



G Data MalwareReport

Halbjahresbericht Januar – Juni 2011

Ralf Benz Müller & Sabrina Berkenkopf
G Data SecurityLabs

Inhalt

Auf einen Blick	2
Malware: Zahlen und Daten.....	3
Das Wachstum geht weiter	3
Malware Kategorien	3
Malware Familien.....	4
Plattformen	7
Trends 2011	8
Mobile Malware	9
Ereignisse des ersten Halbjahrs 2011	11
Januar 2011	11
Februar 2011	12
März 2011	13
April 2011	14
Mai 2011	15
Juni 2011	17

Auf einen Blick

- Im ersten Halbjahr 2011 wurden 1.245.403 neue Computerschädlinge identifiziert. Das sind 15,7% mehr als im Halbjahr zuvor. Die durchschnittliche Anzahl neuer Schadprogramme pro Tag steigt auf 6.881.
- Bei den Malware-Kategorien ist ein überdurchschnittlicher Anstieg bei Trojanischen Pferden und Adware zu verzeichnen. Dagegen ist die Anzahl von Downloadern und Backdoors leicht rückläufig. Offenbar ist die Nutzung der infizierten Rechner wichtiger als die Rekrutierung neuer Bots.
- Im ersten Halbjahr 2011 waren insgesamt 2.670 Malware-Familien aktiv.
- Der Anteil an Windows Malware steigt auf 99,6%. Klassische Windows Programmdateien verlieren zwar einen Anteil von 0,3%. Der Verlust wird aber durch das Wachstum von .NET-Programmen kompensiert.
- Schadprogramme, die auf Webseiten aktiv sind, und Malware für mobile Geräte zeigen einen Aufwärtstrend.

Trends

- Haktivismus gewinnt als Form der politischen Meinungsäußerung immer mehr Zuläufer.
- Malware für mobile Endgeräte ist stark im Kommen. Die Anzahl neuer Schädlinge steigt rapide.

Ereignisse

- In enger Kooperation zwischen Microsofts Digital Crimes Unit und internationalen Polizeibehörden konnte in diesem Jahr das bedeutende Botnetz Rustock lahm gelegt werden. Im März gelang die Abschaltung des Rechnerverbunds, der für Milliarden von Spam Mails pro Tag verantwortlich gemacht werden kann.
- Seit April gibt es eine Reihe von medienwirksam durchgeführten Cyber-Attacks auf japanischen Konzern Sony. Vor allem das Sony Playstation Network und seine Spieler waren betroffen. Die dafür vermeintlich verantwortlich gemachte Hackergruppe, Anonymous, tritt in den folgenden Wochen häufiger in Erscheinung. Ebenso, wie die Hacker von LulzSec.

Ausblick für das zweite Halbjahr 2011

Wir erwarten, dass die Anzahl der Malware auch im zweiten Halbjahr leicht zunimmt und im laufenden Jahr mehr als 2,5 Millionen Schadprogramme gefunden werden.

In der zweiten Jahreshälfte werden mobile Plattformen, insbesondere Android, von Cyberkriminellen verstärkt für Angriffe genutzt.

Malware: Zahlen und Daten

Das Wachstum geht weiter

Die Befürchtung, die Malware-Flut könnte kaum noch ansteigen, hat sich in den ersten sechs Monaten des laufenden Jahres nicht erfüllt. Im ersten Halbjahr 2011 ist die Anzahl¹ neuer Schädlinge um 15,7% auf 1.245.403 gestiegen. Das entspricht durchschnittlich 6.881 neuen Schadprogrammen pro Tag. Wir erwarten, dass bis zum Ende des Jahres die Grenze von 2,5 Millionen neuen Samples überschritten wird. Bei noch stärkerem Wachstum würden 2011 mehr neue Schädlinge zu Buche stehen, als in den Jahren 2006 bis 2009 zusammen.

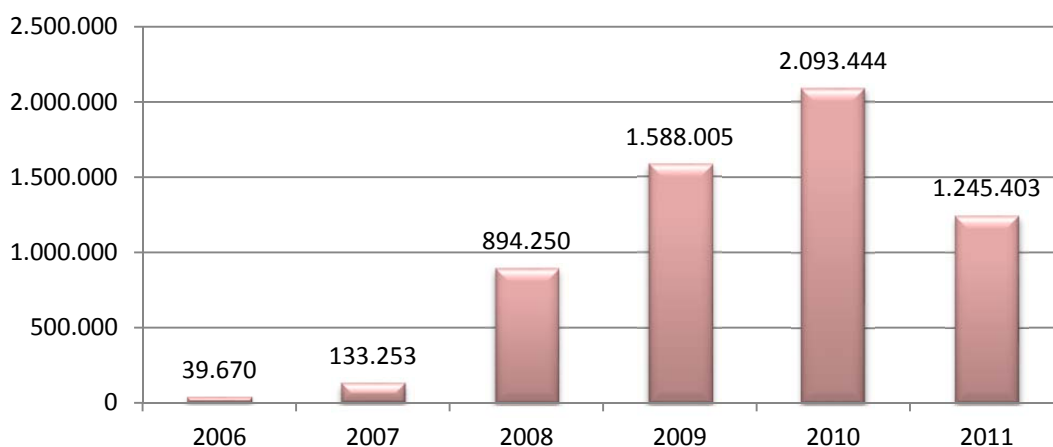


Diagramm 1: Anzahl neuer Malware pro Jahr seit 2006

Malware Kategorien

Anhand ihrer wichtigsten Schadaktivitäten wird Malware in Kategorien untergliedert. Diagramm 2 zeigt die Anzahl der einzelnen Kategorien für die letzten Halbjahre. Den stärksten Anstieg verzeichnet im ersten Halbjahr 2011 die Gruppe der **Trojanischen Pferde**. In ihr sind Schadprogramme zusammengefasst, die spezifische Schadfunktionen ausüben. Sie enthalten überwiegend Programme, die über Backdoors auf infizierte Rechner nachgeladen werden, um kriminelle Aktionen durchzuführen. Spamversand, Überlastangriffe, Proxy-Dienste und ähnliche Angebote aus dem Katalog der Dienstleistungen der Cyber-Crime-Economy gehören in diese Gruppe. Auch die vielen Varianten der Online-Banking-Trojaner Zeus und SpyEye fallen in diese Gruppe. Das Wachstum belegt, dass die Geschäfte im Untergrund gut laufen.

Der starke Anstieg im Bereich **Adware** aus dem zweiten Halbjahr 2010 hat sich etwas verlangsamt. Der Anstieg um 14,6% zeigt aber, dass Adware für die Täter weiterhin ein lukratives und wenig beachtetes Geschäft ist.

¹Die 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 ersten Halbjahr 2011 erstellt wurden.

Leicht rückläufig ist die Anzahl der **Downloader/Dropper**, die für die Infektion von Rechnern zuständig sind. Die Anzahl von **Backdoors** sinkt ebenfalls leicht. Diese Schadprogramme machen Rechner fernsteuerbar und integrieren sie in Botnetze. Offenbar steht der Neuaufbau und die Pflege von Botnetzen nicht mehr im Vordergrund. Die Anzahl der **Exploits** nimmt zum ersten Mal seit einer langen Talfahrt wieder leicht zu.

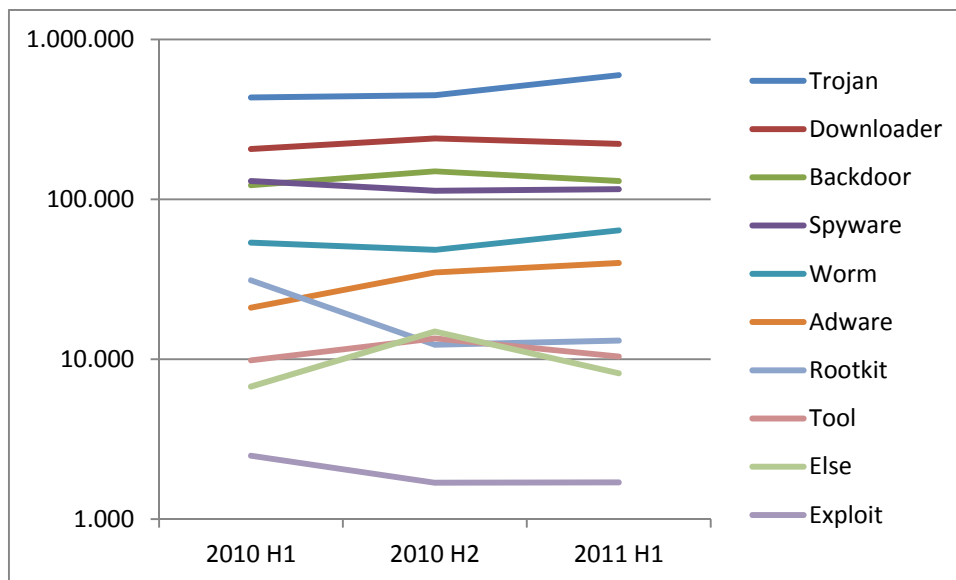


Diagramm 2: Anzahl neuer Schädlinge pro Malwarekategorie in den letzten drei Halbjahren

Malware Familien

Anhand ihrer Eigenschaften und Aktivitäten werden Schadprogramme in Familien unterteilt. Einige Familien sind sehr produktiv und es entstehen ständig neue Varianten. Diagramm 3 zeigt die produktivsten Familien der letzten Halbjahre. Die Gesamtanzahl der Malware-Familien ist im ersten Halbjahr 2011 um 2,4% auf 2.670 leicht angestiegen.

Der Spitzenplatz geht erneut an Genome, einem Trojanischen Pferd mit vielen Schadfunktionen. Auf Platz zwei folgt mit FakeAV ein Vertreter der unter Cyber-Kriminellen sehr populären Kategorie von Software-Imitaten für Virenschutz oder Systemtools. Mit VBKrypt hat es ein neues Tarnprogramm für Schaddateien in die Top 10 geschafft. Die Rootkits der TDSS-Familie - auch bekannt als TDL-Rootkit konnten mit der vierten, noch leistungsfähigeren Version ihre marktführende Stellung in der Cybercrime-Ökonomie ausbauen. Die starke Zunahme von Würmern aus der Palevo-Familie ist für den deutlichen Anstieg von Würmern verantwortlich. Den vorletzten Platz hat ein Neueinsteiger erreicht. Menti ist wie die erstplatzierten Genome ein Trojanisches Pferd. So zeigt sich, dass Trojaner auch weiterhin die beliebtesten Schadprogramme sind, die die Täter zum Einsatz bringen.

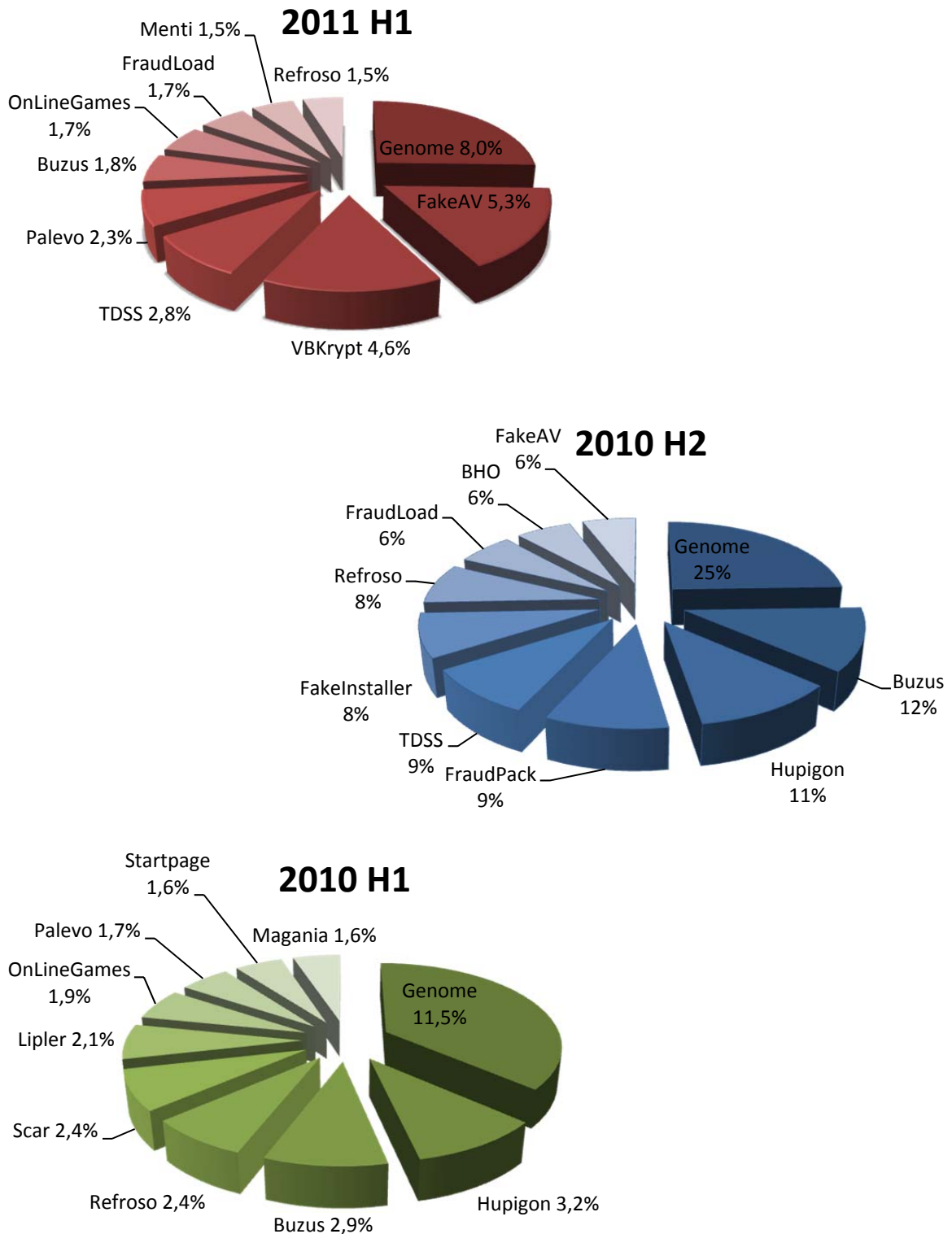


Diagramm 3a-c: Top 10 der aktivsten Schädlingfamilien. Anteil neuer Varianten 2010 und 2011

Genome

Die Trojanischen Pferde der Genome-Familie vereinen Funktionalitäten wie Downloader, Keylogger und Dateiverschlüsselung.

FakeAV

Dieses Trojanische Pferd gibt sich als Antivirus-Software 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.

VBKrypt

VBKrypt ist ein Tool, das zur Tarnung von Schaddateien eingesetzt wird. Die Tarnroutinen sind in Visual Basic geschrieben. Der Inhalt der getarnten Dateien ist weit gefächert und reicht von Downloadern über Backdoors bis hin zu Spyware und Würmern.

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.

Palevo

Der Wurm Palevo verbreitet sich über Wechseldatenträger (autorun.inf) und kopiert sich unter verlockenden Namen in Freigaben von Peer-to-Peer-Tauschbörsenprogrammen wie Bearshare, Kazaa, Shareaza etc. Er verschickt auch per Instant Messages (vorwiegend MSN) Links auf schädliche Webseiten. Außerdem injiziert er Backdoor-Funktionen in den Explorer und sucht auf bestimmten Servern nach Befehlen.

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 so zusätzlich verwundbar zu machen.

OnLineGames

Die Mitglieder der OnlineGames-Familie stehlen vorrangig die Zugangsdaten von Online-Spielen. Dazu werden bestimmte Dateien und Registry-Einträge durchsucht und/oder ein Keylogger installiert. Im letzteren Fall werden dann nicht nur die Daten von Spielen gestohlen. Die meisten Angriffe zielen auf Spiele, die in Asien populär sind.

FraudLoad

Die Fraudload-Familie umfasst unzählige Varianten sogenannter Scareware-Programme, die sich dem Anwender als Sicherheits-Software oder System-Tool präsentieren. Dem Opfer wird ein System-Scan auf mögliche Infektionen vorgetäuscht. 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 der Nutzer 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.

Menti

Das Trojanische Pferd Menti nistet sich im betroffenen System ein und verbindet sich regelmäßig mit einem Server. Damit wird der Rechner Bestandteil eines Botnetzes.

Refroso

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

Plattformen

Auch im ersten Halbjahr 2011 wurde der überwiegende Anteil an Malware für Windows-Systeme geschrieben. Lediglich eins von zweihundertfünfzig Schadprogrammen ist keine Windows Programmdatei². Der Anteil der klassischen Windows Programmdateien (Win32) ist weiterhin rückläufig. Der Verlust von 0,3% wird aber von den .NET Programmen (MSIL) kompensiert und der gesamte Anteil von Windows-Schadprogrammen steigt.

	Plattform	#2011 H1	Anteil	#2010 H2	Anteil	Diff. 2011H1 2010H2	#2010 H1	Anteil	Diff. 2011H1 2010H1
1	Win32	1.218.138	97,8 %	1.056.304	98,1 %	+15,3 %	1.001.902	98,5 %	+21,6 %
2	MSIL	21.736	1,7 %	15.475	1,4 %	+40,5 %	9.383	0,9 %	+131,7 %
3	WebScripts	3.123	0,3 %	2.237	0,2 %	+39,6 %	3.942	0,4 %	-20,8 %
4	Scripts ³	832	0,1 %	1.111	0,1 %	-25,1 %	922	0,1 %	-9,8 %
5	Mobile	803	0,1 %	55	<0,1 %	+138,2 %	212	<0,1 %	+273,1 %
6	Java	313	<0,1 %	517	<0,1 %	-39,5 %	225	<0,1 %	+39,1 %
7	*ix ⁴	233	<0,1 %	382	<0,1 %	-39,0 %	226	<0,1 %	+3,1 %
8	NSIS ⁵	131	<0,1 %	130	<0,1 %	+0,8 %	260	<0,1 %	-49,6 %

Table 1: Top 8 Plattformen in den letzten drei Halbjahren

Die restlichen knapp 0,5 % werden von Web-basiertem Schadcode angeführt, deren Anzahl deutlich angestiegen ist. Dagegen hat die Anzahl von skriptbasierter Malware abgenommen.

Einen deutlichen Anstieg konnten auch die Schädlinge für Mobile Malware verzeichnen. Die Art der Schadfunktionen deuten auf eine wirtschaftliche Nutzung hin – ca. zwei von drei Smartphone-Schädlingen versenden SMS an teure Rufnummern. Auch Spionageprogramme und Backdoors haben deutlich zugenommen. Hier etabliert sich gerade ein neues Nutzungsfeld für Cyberkriminelle, das in den zukünftigen Monaten von den G Data SecurityLabs beobachtet wird.

² Wenn man die Programmdateien für Windows 32-bit und 64-bit Systeme und .NET Programme (MSIL) zusammenfasst.

³ "Scripts" sind Batch- oder Shell-Skripte oder Programme, die in den Skriptsprachen VBS, Perl, Python oder Ruby geschrieben wurden

⁴ *ix bezeichnet alle Unix-Derivate, wie z.B. Linux, FreeBSD, Solaris etc.

⁵ NSIS ist die Installationsplattform, die u.a. dazu genutzt wird den Mediaplayer Winamp zu installieren

Trends 2011

Die von uns erwartete Entwicklung der einzelnen Kategorien von Malware und der Plattformen sind in der folgenden Tabelle dargestellt.

Kategorie	Trend
Trojanische Pferde	➔
Backdoors	➔
Downloader / Dropper	➔
Spyware	➔
Adware	↗
Viren/Würmer	➔
Rootkits	➔
Exploits	➔
Win32	➔
WebScripts	↗
Java	➔
MSIL	↗
Mobile	↗
*ix	➔

Tabelle 2: Erwartete Entwicklung von Malware-Kategorien und Plattformen

Mobile Malware

Mobile Geräte mit einem Android-Betriebssystem werden immer populärer. So bezeichnen die IDC-Marktforscher Android als zukünftigen „King of the Hill“. Mit der wachsenden Beliebtheit ist allerdings auch das Interesse von Malware-Autoren an der Plattform und den mobilen Medien gestiegen. G Data sieht daher ein hohes Gefahrenpotential für mobile Endgeräte mit steigender Tendenz. Die weitere Entwicklung von mobilen Schädlingen dürfte schneller verlaufen als bei Malware für PCs, da bereits etablierte Verwertungsstrukturen im Untergrund existieren.

Schon in der Vergangenheit sorgte die Entdeckung der mit Schadcode infizierten Apps im Google Android Market für Schlagzeilen in den Medien.

Feature phones und Smartphones erfreuen sich derweil bei den Nutzern weltweit einer immer größer werdenden Beliebtheit.

Featurephones und Smartphone erfreuen sich jedoch weltweit immer größerer Beliebtheit. Sie werden immer häufiger als Medium für Bezahl Dienste genutzt und damit werden sie immer attraktiver für Kriminelle. Die können in einigen Ländern teure Premium-SMS-Nummern anonym registrieren und damit Opfern von SMS-Abos hohe Telefonrechnungen beschere. Diese neuen Möglichkeiten wurden von Cyberkriminellen auch intensiv genutzt: Mehr als zwei Drittel aller mobilen Schädlinge versenden SMS an teure Premium-Dienste. Auch die Zahl der Backdoors, mit denen Smartphones in Botnetze integriert werden, steigt dramatisch. Mit Zeus in the Mobile (ZITMO) ist ein spezialisierter Online-Banking-Trojaner aufgetaucht, der das mTAN Verfahren angreift. Der Versand der TAN per SMS sollte ursprünglich durch die Kanaltrennung für zusätzliche Sicherheit sorgen. Da ZITMO die SMS mit der TAN abfängt, ist die Sicherheit des Verfahrens nicht mehr gegeben. Es wird klar: Das Stadium des Proof-of-Concept hat Mobile Malware hinter sich gelassen.

Gerade die Android-Plattform gewinnt bei den Kunden immer weiter an Zuspruch, da die Geräte mit Android Betriebssystemen günstiger sind als beispielsweise die der Konkurrenz mit iOS. Außerdem gibt es bei Android eine größere Gerätevielfalt mit zahlreichen Brandings von Telekommunikationsunternehmen. Diese Vielfalt hat jedoch den entscheidenden Nachteil, dass die eigene Qualitätskontrolle enorm erschwert wird und das Verteilen von Updates nicht für alle Kunden zeitnah zu realisieren ist. Ein Beispiel hierfür sind die Geräte der Konkurrenz aus dem US-amerikanischen Cupertino. Außerdem kann bei älteren Telefonmodellen oft kein Upgrade durchgeführt werden. So war zum Beispiel Anfang Juli der Anteil der Nutzer, die den Android Market noch mit einer älteren Android OS-Version besuchten, sehr hoch (siehe Abbildung 1). Durch den langen Auslieferungsweg für neue Betriebssystemversionen von Google zu den Geräteherstellern über die Service-Provider bis zum Kunden haben Bösewichte die Chance, in der Zwischenzeit Schwachstellen in älteren Betriebssystemen auszunutzen. Bei den Verzögerungen handelt es sich dabei nicht um Tage, sondern um Monate. Dieser Schwachpunkt wird in Zukunft weiter in den Fokus der Cyberkriminellen geraten.

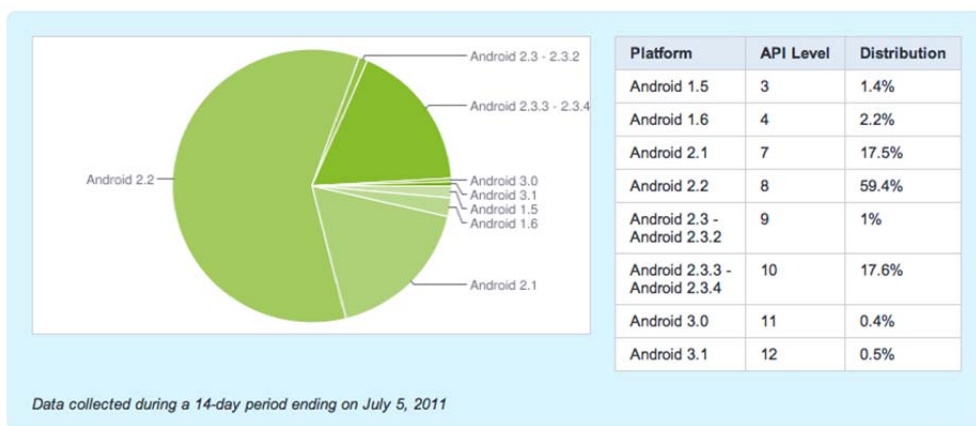


Abbildung 1: Verbreitung der Android Plattformen von Besuchern des Android Marktes (Quelle: <http://developer.android.com/resources/dashboard/platform-versions.html>)

Abgesehen von hardwareseitigen Risiken ist der ‚Faktor Mensch nicht zu unterschätzen: Schnell sind die bei der Installation angezeigten erforderlichen Berechtigungen unbeachtet bestätigt. Damit ist der Weg für die Applikationen, Informationen zu sammeln, Premium-Nummern anzurufen und vieles mehr. Ein Beispiel sind die manipulierten Applikationen von Zsone aus dem Google Android Market. Die Apps senden, vom Nutzer unbemerkt, Abo-Anmeldungen zu chinesischen Premium-SMS-Nummern und fangen sogar die Antwort-SMS des Abo-

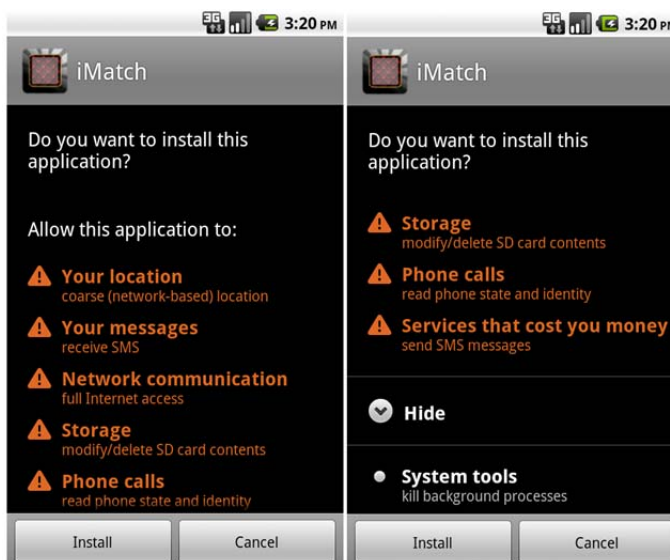


Abbildung2: Eine infizierte App von Zsone verschafft sich zahlreiche Berechtigungen auf dem Handy, die dem Nutzer in diesem Fall schaden können. (Quelle: G Data Software)

Dienstes ab. Der Nutzer bekommt von den kostspieligen Textnachrichten nichts mit – bis er auf seine Telefonrechnung bekommt. Bei diesem Schädling besteht aktuell allerdings nur Gefahr für Android-Nutzer in chinesischen Telekommunikationsnetzen.

Fazit

Mobile Geräte werden immer weiter in den Fokus der digitalen Kriminellen rücken und daher wird sich die Entwicklung immer neuer Schädlinge beschleunigen, je mehr Profit für die Angreifer zu holen ist. Durch die steigenden Absatzzahlen der Android-Geräte wird dieser Markt für den Untergrund immer interessanter.

Da außerdem die Nutzungsmöglichkeiten für Smartphones noch lange nicht ausgeschöpft sind, werden immer neue Technologien auch immer neue Angriffspunkte mit sich bringen – ein Beispiel für die nahe Zukunft wäre die Bezahlung mit dem Smartphone per NFC (in Android implementiert seit Version 2.3).

Ereignisse des ersten Halbjahrs 2011

Januar 2011

- 09.01. Das australische Medienunternehmen Fairfax beschuldigt **Vodafone**, seine Kundendaten nur unzureichend in Datenbanken zu sichern, so dass sie für viele sichtbar sind, u.a. für alle Vodafone Händler. So seien persönliche Informationen sowie **SMS- und Anrufprotokolle** auch an Dritte gelangt, die in einer Art „pay per view“ Verfahren Einblick in die Daten bekommen haben sollen. Die Enthüllung wird als eine Nachwehe der Wikileaks „Cablegate“-Affäre bezeichnet.
- 11.01. Die **Twitter- und YouTube-Konten** der nordkoreanischen Regierung werden gehackt und von Unbekannten missbraucht. Zum Geburtstag von Kim Jong-un, dem designierten Nachfolger von Kim Jong-il, verbreiteten die Hacker auf den Accounts **regimekritische Nachrichten**. Außerdem veröffentlichen die Eindringlinge ein animiertes Video, das ihn in einem Sportwagen zeigt, mit dem er notleidende Personen überfährt. Mitglieder des südkoreanischen Internetforums DC Inside bekennen sich zu dem Hack.
- 16.01. Das **Bundeskriminalamt (BKA)** nimmt eine bulgarische **Skimming-Bande** fest, die in Dresden Geldautomaten manipuliert hatten. Die drei Männer werden auf frischer Tat in einer Bankfiliale festgenommen, als sie an ihrem Equipment arbeiteten. Über die Summe der Beute wird nichts bekannt.
- 23.01. Die Facebook-Accounts des französischen Präsidenten **Nicolas Sarkozy** und des Facebook-Chefs **Mark Zuckerberg** werden kompromittiert. Die Eindringlinge veröffentlichen auf beiden Seiten im Namen der Prominenten täuschend echte Kommentare. Wie die Täter an die Schreibberechtigungen kommen, bleibt unklar.
- 24.01. Der Iran kündigt eine sogenannte **Cyber-Polizei** an, die u.a. die Kommunikation zwischen politischen Dissidenten, vor allem über soziale Netzwerke, verhindern soll. Bezogen auf die Proteste gegen die Wiederwahl von Präsident Ahmadinejads 2009 erklärt Polizeichef Esmaeil Ahmadi Moghaddam: „Durch soziale Netzwerke in unserem Land haben sich **anti-revolutionäre Gruppen und Dissidenten** gefunden, das Ausland kontaktiert und Unruhen angezettelt“.
- 31.01. **Kurios:** Der **gestohlene Laptop** einer 25-jährigen Amerikanerin meldet sich selbständig per E-Mail und erleichtert der Polizei von Newport, Virginia so die Ermittlungsarbeit. **Das Gerät macht Bilder** mit der eingebauten Webcam und sendet sie an die Besitzerin. Nun müssen nur die beiden Personen auf dem von der Polizei veröffentlichten Bild identifiziert werden, um zu klären, wie sie in den Besitz des Laptops kamen.



Screenshot 1: Ein animiertes Video zeigt Kim Jong-un (Quelle: YouTube.com)



Screenshot 2: Foto von der Webcam des gestohlenen Notebooks (Quelle: wavy.com)

Februar 2011

- 05.02. Aaron Barr, ein Mitarbeiter der Sicherheitsfirma **HBGary Federal**, handelt seinem Unternehmen eine ausgedehnte mehrstufige Attacke der Gruppe Anonymous ein. Er hatte zuvor damit geprahlt, dass er die Mitglieder der **Haktivisten-Gruppe** identifiziert hatte, die kurz zuvor die Operation Payback durchgeführt hatten. Sogar die New York Times berichtete und diese Publicity veranlasste die Beschuldigten, sich zu wehren. In der Folge verschafften sich Anonymous über eine Reihe von Fehlern, die in einem Sicherheitsunternehmen nicht vorkommen sollten, Zugang zu den Passwörtern der HBGary-Mitarbeiter und letztlich auf das Google-Mail Postfach von Greg Hoglund, dem Mitgründer und technischen Leiter der Firma. Es enthielt neben brisanten Informationen über Rüstungsaufträge auch die Zugangsdaten zu Hoglunds Seite **rootkit.com**. Die dort vorhandenen Daten wurden von Anonymous zusammen mit Hoglunds E-Mails veröffentlicht. Aaron Barrs großer Wurf führt letztlich zu seinem Rücktritt.
- 07.02. Hamburgs Polizeibehörden nehmen zwei mutmaßliche Betreiber von **Abofallen-Webseiten** fest. Die beiden hatten seit Ende 2008 über 65.000 Webseitenbesucher geprellt und dabei nahezu 5 Mio. EUR eingenommen. Die Betrüger boten grundsätzlich freie oder zumindest als Testversion kostenlos erhältliche Software zum Download an und jubelten dabei den Besuchern unbemerkt Abo-Verträge unter.
- 09.02. Im Untergrund wird für rund 25 USD ein Toolkit namens „**Tinie App**“ verkauft, das es quasi jedem möglich macht, eigene **schädliche Anwendung für Facebook** zu entwerfen, wie etwa „Profile Creeps“ oder „Creeper Tracker“. Eine Vielzahl von Nutzern klickt noch immer auf solche Apps in Facebook und verbreitet diese damit weiter - zur Freude der Entwickler, die mit Affiliate-Programmen Geld für die Klicks einstreichen.
- 12.02. Das **amerikanische Justizministerium und Ministerium für innere Sicherheit** haben fälschlicherweise 84.000 Domains mit einem Banner versehen, der empfindliche Strafen für Personen aufzählt, die in Verbindung mit **Kinderpornografie** stehen. Durch einen Fehler in der Datenübermittlung werden alle Domains des DNS Providers FreeDNS auf das Banner umgeleitet und verunsichern so die Besitzer und Besucher der Webseiten.
- 13.02. Die **Kundendaten** von Millionen Nutzern der Dienste Pixmania, Eidos, eHarmony und diversitybusiness werden **im Untergrund gehandelt**. Einige Datensätze werden dort zu Preisen zwischen 2.000 und 3.000 USD (ca. 1.400 bis 2.100 EUR) angeboten. Potentiell verantwortlich für den Datendiebstahl ist der Argentinier Chris Russo. Im Fall von eHarmony wurden die Daten durch das Ausnutzen einer **SQL Injektion Schwachstelle** gestohlen.
- 15.02. In den **Webauftritt des BBC 6 Music Web** und der Webseite des BBC 1extra Radio wird als Folge einer **massenhaften Infektion verwundbarer Webseiten** bössartiger Code injiziert.



Screenshot 3: Der Banner, der auf 84.000 Domains fälschlicher Weise angezeigt wurde (Quelle: torrentfreak.com)

Der eingefügte Code lädt Dateien von einer Webseite nach und versucht den Webseitenbesucher ohne sein Wissen zu infizieren (**Drive-by-Infektion**). Die Angreifer benutzen ein Phoenix Exploit Kit, um die Schwachstellen auf dem Rechner auszunutzen.

- 17.02. Eine Studie ermittelt, dass das **Vereinigte Königreich** allein durch **Cyber-Kriminalität** mit einem jährlichen Schaden von 27 Mrd. GBP (ca. 30,7 Mrd. EUR) belastet wird. Dabei habe der Diebstahl von geistigem Eigentum den größten Anteil an den kriminellen Handlungen, gefolgt von Industriespionage und Erpressung.
- 28.02. **Kurios:** Ein 48-jähriger Mann aus Naperville, Illinois wird Opfer einer **betrügerischen Online-Bekanntschafft**. Er hatte der Dame innerhalb von zwei Jahren insgesamt **200.000 USD**(ca. 139.000 EUR) auf Konten in England, den USA, Malaysia und sogar Nigeria überwiesen. Als sie sich nicht mehr meldete fürchtete er, sie könnte entführt worden sein und rief die Polizei. Die klärte ihn dann darüber auf, dass er betrogen wurde. Selbst der Führerschein, den die Dame einst übersendet hatte, war nicht echt. Es war ein **Muster-Ausweis** des US-Bundesstaates Florida.

März 2011

- 05.03. Google erläutert offiziell, dass es am vergangenen Dienstag eine Vielzahl von Apps aus dem **Android Market** entfernt hat. Die Applikationen waren mit dem sogenannten **DroidDream** Schadcode infiziert, der u.a. versucht, auf den betroffenen Mobilgeräten Root-Rechte zu erlangen. Per Fernsteuerung deinstallierte Google die schädlichen Programme auf den betroffenen Geräten. Zusätzlich gibt das Unternehmen ein "Android Market Security Tool March 2011" aus, welches jedoch kurze Zeit später als **trojanisierte App** ebenfalls im Market auftaucht.



Screenshot 4: Android Robot (Quelle: android.com)

- 06.03. Bei einem Überfall auf die Zentrale des ägyptischen Staatssicherheitsdienstes finden Regime-Gegner Dokumente der britischen Firma Gamma International, die der Regierung ein **Spionageprogramm namens FinFisher** zum Kauf anbot. Die Schadsoftware eignet sich zum Ausspähen, Abhören und Übernehmen der Computer von Dissidenten und sollte inklusive Trainings 525.000 USD (ca. 364.000 EUR) kosten.
- 16.03. Gut ein Jahr nach der Zerschlagung des Waledac Botnetzes, berichtet Microsoft erneut von einer **erfolgreichen Botnetz-Deaktivierung**: Eines der weltweit größten Botnetze, namens **Rustock**. Die Microsoft Digital Crimes Unit (DCU) schätzt, dass etwa eine Million Computer mit dem Rustock-Schadcode infiziert waren und das Botnetz so für Milliarden

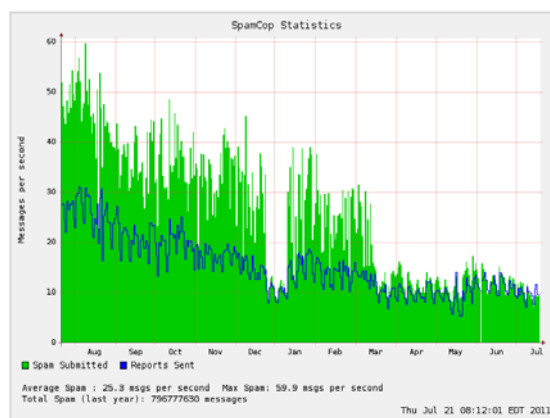


Abbildung 3: Der Graph zeigt seit Mitte März einen deutlichen Rückgang der Nachrichten pro Sekunde (Quelle: Spamcop.net)

von Spam-Mails pro Tag verantwortlich gemacht werden kann.

- 17.03. Angreifer attackieren die Server der **Sicherheitsfirma RSA** und stehlen Daten zur-Zwei-Faktor-Authentifizierung **SecurID**. Der als Advanced Persistent Threat bezeichnete Angriff erfolgte gezielt, über **manipulierte Excel-Dateien**, die per Mail an eine kleine Gruppe von RSA-Mitarbeitern gesendet wurden. Beim Öffnen der .xls-Dateien nutzt der Schadcode eine Zero-Day Sicherheitslücke aus, um Zugriff auf die privilegierten Benutzerkonten zu erlangen.
- 18.03. Der 29-jährige Ashley Mitchell wird zu zwei Jahren Haft verurteilt, weil er **400 Milliarden virtuelle Pokerchips**, im Wert von 12 Mio. USD (ca. 8,4 Mio. EUR) von der amerikanischen Firma **Zynga** geklaut hatte. Zynga betreibt unter anderem das weltweit bekannte Online-Spiel Farmville. Einen Teil seiner Beute verkaufte Mitchell auf dem **Schwarzmarkt** für 53.000 GBP (ca. 60.000 EUR).
- 20.03. Die Plattform **TripAdvisor** wird Opfer von Datendiebstahl. Kriminelle attackieren die populäre Reisewebseite und stehlen **E-Mail Adressen von Mitgliedern** aus einer Datenbank. TripAdvisor schließt die Lücke umgehend und geht nicht von einem größeren Schaden aus. „Sie könnten in Folge des Vorfalls Spam E-Mails erhalten“, heißt es in einer Mail an die Mitglieder.
- 23.03. Unbekannte Angreifer verschaffen sich Zugang zu **SLL Zertifikaten** bestehender Webseiten, indem sie mit einem kompromittierten Account in Comodos Certificate Authority (CA) eindringen. Die Zertifikate wurden bereits am 15. März gestohlen und könnten eingesetzt werden, um Webseiten täuschend echt zu fälschen. **Comodo** sagt in einem Bericht, dass „die Angriffe von mehreren IPs kamen, aber hauptsächlich aus dem Iran“.

April 2011

- 04.04. Einzelheiten über eine groß angelegte **Massen-SQL-Injektions-Attacke** werden bekannt. Der Angriff, der als **Lizamoon-Attacke** bezeichnet wird, schleuste böartigen Code in viele Millionen Webseiten. Die Säuberung der betroffenen Seiten ist eine langwierige Angelegenheit. Die Besucher der eigentlichen Webseite wurden durch den Schadcode auf **FakeAV-Webseiten** umgeleitet, womit die Betrüger Geld machen wollen.
- 08.04. **Kurios:** Eine Softwarefirma schaltet eine Stellenanzeige für **Programmiererinnen und Vertriebsmitarbeiterinnen**. Zu erfüllende Voraussetzungen: Die Bewerberinnen müssen zwischen 20 und 39 Jahre alt sein und völlig textilfrei arbeiten wollen. Der 63-jährige Betreiber verspricht seriöse Jobangebote in einem seriösen Unternehmen.
- 20.04. Der **amerikanische Heimatschutz** plant zukünftig, seine **nationalen Terrorwarnmeldungen** nicht nur auf der eigenen Homepage, in TV und Radio zu publizieren, sondern auch in sozialen Netzwerken, wie **Facebook und Twitter**. Durchsagen in Flughäfen und Anzeigen auf Regierungswebseiten sollen dann entfallen.
- 24.4. Der 20-jährige Sohn des Security-Software Herstellers **Eugene Kaspersky** wird von den russischen Sicherheitsbehörden wohlbehalten aus den Fängen von fünf Entführern befreit.

Laut eigenen Angaben habe es **keine Lösegeldzahlung** gegeben. Die Kidnapper forderten 3 Mio EUR.

- 27.4. Der erste Sony PlayStation-Kunde **verklagt die Sony Corp.** wegen unzureichenden Schutzes der persönlichen Daten. Hacker hatten zwischen dem 17. und dem 19.4. das Sony PlayStationNetwork (PSN) und den Qriocity Onlineservice angegriffen und **77 Millionen Nutzerdaten** gestohlen.

Mai 2011

- 10.05. Die finnische Polizei zerschlägt eine Bande von **Online-Banking-Betrügnern** und verhaftet 17 Verdächtige. Kunden der finnischen Nordea Bank waren das Ziel der Kriminellen und sie **erbeuteten rund 1,2 Millionen EUR** mit über 100 manipulierten Transaktionen. Bis auf 178.000 EUR konnte das Geld wieder an die rechtmäßigen Besitzer zurücküberwiesen werden.

- 11.05. Der verkündete **Tod von Osama Bin Laden** ruft Malwareautoren auf den Plan, die z.B. mit der Verbreitung von angeblichen Beweisfotos Benutzer in die Falle locken wollen. Die auffälligen **Angriffsvektoren** sind in diesem Fall E-Mails mit Links zu Schadcode und präparierte Word Dokumente, die eine Sicherheitslücke (CVE-2010-3333) ausnutzen sollten.



Screenshot 5: Gefährliche Osama Bin Laden E-Mail.

- 11.05. Die Webseite der russischen Medienagentur **Pravda** wird gehackt und attackiert unbemerkt die Besucher. Die Kriminellen verwenden **eingebettete Exploit-Skripte**, die anfällige Java-Version auf den Rechnern der Webseitenbesucher angreifen. Die Angreifer änderten optisch nichts an der Webseite, was es ungleich gefährlicher macht.
- 20.05. Der unabhängige Security-Forscher Rosario stellt einen **Exploit für Microsofts Internet Explorer** vor, der Angreifern Zugriff auf anmeldepflichtige Webseiten ermöglicht, wie z.B. Facebook. Nach der Eingabe der Login-Daten erstellt die Webseite einen Cookie als digitalen Schlüssel. Wird dieser **Cookie gestohlen**, können Dritte ebenfalls auf die eigentlich zugangsgeschützten Seiten zugreifen. Der Angriff wird „**Cookiejacking**“ genannt.
- 23.05. Der komplette **Source Code** des Banking-Trojaners **Zeus** ist öffentlich verfügbar. Zeus war unbestritten der mächtigste Banking-Trojaner der letzten Jahre.
- 25.05. Ein Doktorand der Universität von Amsterdam bestückt eine Datenbank mit **35 Millionen Datensätzen von Google Profiles**. Diese enthält Namen, E-Mail Adressen und biographische Informationen. Das Einsammeln der Informationen sollte ein Experiment sein, um zu sehen, wie schnell sich z.B. Privatdetektive und Phisher gezielt persönliche Informationen beschaffen können. Google verbietet das Indexieren der Listen nicht.
- 26.05. Das **chinesische Militär** bestätigt zum ersten Mal, dass in ihrer Armee eine **Eliteeinheit von Cyber-Kriegern** existiert. Die Spezialkräfte werden „Cyber Blue Team“ genannt. Ob es sich



bei der Einheit um reine Abwehrmaßnahmen oder auch um potentiell offensive Kräfte handelt, ist nicht bekannt.

Juni 2011

- 03.06. Nach den Angriffen auf das **Sony PSN und Qirocity** wird jetzt die Plattform von **Sony Pictures** gehackt. Verantwortlich für den Angriff zeichnet sich eine Gruppe namens **Lulz Security, kurz LulzSec**. Laut eigenen Angaben stahlen sie persönliche Informationen von mehr als 1 Million Benutzern.
- 04.06. **Microsofts DCU** arbeitet weiterhin daran, die Hintermänner hinter dem im März lahm gelegten **Rustock Botnetzes** zu entlarven. Die DCU vermutet, dass die **Drahtzieher aus Russland** operiert haben, bzw. noch operieren. Deswegen schalten sie für 30 Tage große Werbeanzeigen in populären, russischen Tageszeitungen, um mit Besitzern der abgeschalteten IP Adressen und Domains in Kontakt zu kommen.
- 07.06. Die Rüstungsfirma **Lockheed Martin** gibt bekannt, dass kürzlich ein Angriff auf ihr Netzwerk stattgefunden hat, der durch die im März gestohlenen **RSA SecurID Token** begünstigt wurde. Ein Diebstahl von Daten sei durch ein schnelles Eingreifen verhindert worden. Sie sind aktuell dabei 45.000 SecureID Token zu erneuern.
- 20.06. Die virtuelle Währung **Bitcoin** erlebt auf der Handelsplattform Mt Gox einen **Kursverfall**. Ein Unbekannter hackte einen kapitalen Bitcoin Account (7,7% aller Bitcoins), tauschte das virtuelle Geld in US-Dollar um und kurz darauf wieder zurück. Der Kurs sank von 17,50 USD pro Bitcoin auf einen Cent pro Bitcoin ab.
- 26.06. Nach nur 50 Tagen gibt die Hackergruppe **LulzSec** ihre Auflösung bekannt. Die von der Polizei gejagte Gruppe wird für viele Hacker-Attacken und Überlastangriffe auf Webseiten der letzten Wochen verantwortlich gemacht. Zahlreiche erbeutete Datensätze veröffentlichte LulzSec im Internet. Experten werten LulzSec als Ableger der Gruppe Anonymous.
- 29.06. Das soziale Netzwerk **MySpace** wird verkauft. **Medienmogul Rupert Murdoch** hatte die Plattform im Jahr 2005 für 580 Mio. USD (ca. 403 Mio. EUR) gekauft und nun unter hohem Verlust für **35 Mio. USD** (ca. 24 Mio. EUR) an eine kalifornische Werbefirma verkauft. Die Benutzerzahlen von MySpace gingen mit dem Aufstreben von Facebook zurück.
- 30.06. Das BKA stellt die **deutsche Kriminalstatistik 2010** vor: Im vergangenen Jahr wurden ca. 250.000 Fälle von Internetkriminalität registriert. Im Gegensatz zu 2009 bedeutet dies einen Anstieg dieser Delikte um rund **20 Prozent**. Die Schadenssumme beläuft sich auf 61,5 Mio. EUR.