G DATA

Malware-Report

Halbjahresbericht Juli-Dezember 2008

Ralf Benzmüller

Geschützt. **Geschützter. G DATA.**

G DATA Malware-Report Juli-Dezember 2008

Ralf Benzmüller

Auf einen Blick

Zahlen und Daten

- 894.250 neue Schädlinge in 2008 sind ca. 6,7 Mal mehr als 2007.
- 576.002 neue Schädlinge im 2. Halbjahr 2008 sorgen für eine Steigerung um das 1,8fache gegenüber dem ersten Halbjahr.
- Die häufigsten Schädlingskategorien sind Trojanische Pferde, Backdoors und Downloader. Als weitere Kategorien folgen Spyware, Adware und Würmer.
- Zu den aktivsten Virenfamilien zählen Backdoors, Online-Game-Accountstehler und Komponenten zur Installation von Adware und Scareware. Der aktivste Wurm „Autorun" nutzt die Autostart-Funktionen für CDs und USB-Sticks zur Verbreitung.
- 99,2% aller Malware des zweiten Halbjahrs läuft unter Windows. Die Malwareautoren konzentrieren sich noch mehr auf den Marktführer. Schadcode für mobile Plattformen, Unix und Apple ist auch 2008 eher die Ausnahme.
- JavaScript-Malware nimmt um etwas mehr als ein Viertel ab, während die Anzahl der Flash-basierten Schädlinge um 38% steigt. Der Trend geht also weg von JavaScript und hin zu Flash-Malware.

Ereignisse und Trends

- Exploits - d.h. Schadcode der Sicherheitslücken ausnutzt, um Rechner zu befallen - werden immer schneller erstellt. Microsoft musste im Oktober und im Dezember zusätzliche Patches zur Verfügung stellen.
- Die wichtigsten Betrugsmaschen mit denen Internetnutzer zur Installation von Malware verleitet wurden sind 1. Aufforderungen zum Nachladen von Codecs bzw. Software, 2. Virenschutz-Imitate und Scareware und 3. E-Mails über Bestellungen, Pakete und Lieferungen.
- Die Kriege der Welt werden verstärkt im und per Internet ausgetragen. Webseiten des Gegners werden mit Überlastangriffen attackiert und Nachrichtenquellen werden gecrackt und manipuliert, um Propaganda zu betreiben.
- Zahlreiche Datenpannen machen persönliche Daten auch von Prominenten zugänglich und offenbaren streng geheime militärische Informationen. Datenschutz wird nicht ernst genommen.
- Das Online-Carding-Forum „Dark Market", das als wichtiger Umschlagplatz für Kreditkarteninformationen gilt, fliegt auf. Weltweit werden 56 Personen verhaftet.
- Intercage und McColo werden vom Netz genommen. Die Spam-Flut ebbt für eine Weile ab und der Botnetz-Markt organisiert sich neu.
- Soziale Netzwerke werden immer häufiger zur Verbreitung von Spam und Malware genutzt.
- Große Ereignisse wie die Olympiade und die Präsidentschaftswahl in den USA wird auch von Spammern und Malwareschreibern genutzt

Prognosen

- Das Internet wird gefährlicher. Web 2.0 Anwendungen, Soziale Netzwerke, Foren und Blogs bieten viel Angriffsfläche, die in den kommenden Monaten verstärkt genutzt wird.
- Flash als Verbreitungsweg für Malware wird in den kommenden Monaten zunehmen. Bislang wird das Betrachten von Flash-Filmen noch nicht als Gefahr angesehen.
- Die Malware-Flut wird weiter ansteigen, aber mit geringeren Steigerungsraten

Inhalt

Ereignisse und Trends des zweiten Halbjahrs 2008

In der zweiten Jahreshälfte von 2008 waren Online-Kriminelle an breiter Front aktiv. In den G DATA Security Labs sind die folgenden Themen so häufig aufgetreten, dass ihnen jeweils ein eigener Abschnitt gewidmet wird. Die wichtigsten Themen sind Exploits, gängige Betrugsmaschen, Krieg im Internet, Datenpannen und Datenschutz und die Bekämpfung der Cyber-Kriminalität.

Sicherheitslücken schnell ausgenutzt

Immer wieder weisen Sicherheitsexperten darauf hin, wie wichtig es ist, das Betriebssystem und die Software auf dem neuesten Stand zu halten. Viele Software-Anbieter veröffentlichen in mehr oder weniger regelmäßigen Abständen die neuesten Patches. An jedem zweiten Dienstag eines Monats rollt Microsoft Patches für neue Sicherheitslücken des Betriebssystems oder von Microsoft Software aus (daher der Name „Patch-Day"). Mit der Zeit sammeln sich so viele kleine Installationen an. Im Service Pack 3 von Windows XP werden die Patches seit Service Pack 2 zusammengefasst. Seit dem 9. Juli wird Service Pack 3 von Windows XP automatisch per Update ausgeliefert.

Microsoft Patch-Day: Fester Termin im Cybercrime-Kalender

Auch im zweiten Halbjahr 2008 reagieren Hacker und Online-Kriminelle auf den „Patch-Day". Oft werden die Sicherheitslücken unmittelbar nachdem Microsoft die Patches ausgeliefert hat auch ausgenutzt. Dazu analysieren Hacker die geänderten Dateien des Betriebssystems und entwickeln anhand der gewonnenen Informationen Exploit-Code. In vielen Fällen dauert das nur wenige Stunden. Diese Exploit-Codes werden dann von Online-Kriminellen in Malware - oder schlimmer - in Tools zur Erstellung und Verbreitung von Malware integriert.

Immer häufiger wurden auch Sicherheitslücken, für die es noch keine Patches gibt, kurz nach Microsofts „Patch-Tuesday" veröffentlicht. Die Online-Kriminellen warten den Patch-Day ab und wenn die Lücke nicht geschlossen wurde, können sie einen Monat lang Rechner infizieren, sofern Microsoft keine Sonderschicht einlegt. Und genau das ist im zweiten Halbjahr zweimal geschehen:

- Nachdem am 23. Oktober Berichte über gezielte Angriffe auf Windows-Rechner bekannt wurden, die auf der kritischen Lücke im RPC-Dienst von Windows basieren, bringt Microsoft außerhalb des üblichen Turnus ein Sicherheits-Update heraus (MS-08-067). Zwei Tage später nutzt Gimmiv.A diese Lücke, um in Rechner einzudringen und dort Daten zu stehlen. Trotz der raschen Reaktion von Microsoft wurden Anfang 2009 die Rechner der Kärntner Landesregierung und der Kärntner Krankenanstaltengesellschaft KABEG vom einem Wurm namens Conficker (alias Downadup) infiziert.
- Am 17.12. wurde in einem Sonder-Update (MS08-078) eine Sicherheitslücke im Internet Explorer 5 bis 8 geschlossen. Auf mehreren Webseiten nicht nur aus dem Rotlicht-Milieu war Exploit-Code gefunden worden, der die Lücke nutzte, um Schadcode auf anfällige Rechner zu schleusen.

Insbesondere das erste Beispiel zeigt, wie wichtig aktuelle Software und Betriebssysteme mittlerweile geworden sind.

Fallen im Internet

Mit hinterlistigen Tricks versuchen die Online-Kriminellen ihre Opfer beim Surfen zur Installation von Malware zu bringen. Die erfolgreichsten Maschen, um Nutzer reinzulegen sind

1. Aufforderung zur Installation angeblich fehlender Codecs oder Software
2. Scareware und Virenschutz-Imitate
3. Lieferungen, Bestellungen und Pakete

Im ersten Fall wird man per E-Mail oder Instant Message, aber auch von anderen Webseiten oder aus Foren und Newsgroups, auf eine Webseite gelockt, die angeblich ein interessantes Video oder andere Multimedia-Dateien enthalten. Beim Abspielen wird festgestellt, dass der notwendige Codec oder Software nicht vorhanden ist. Der Anwender wird aufgefordert die angeblich fehlenden Komponenten zu installieren. Wer dieser Aufforderung folgt, infiziert seinen Rechner.

Im Falle von Scareware (von engl. to scare - sich fürchten), wird dem Besucher vorgegaukelt, dass ein Systemscan durchgeführt wird. Der endet damit, dass auf dem Rechner (vermeintlich) Malware diagnostiziert wird. Daraufhin wird dem Nutzer ein meist funktionsloses Virenschutz-Imitat zum Download angeboten (oder besser gesagt aufgenötigt). Diese Produkte erkennen in den meisten Fällen keine Malware. Sie sorgen allenfalls dafür, dass die erfundenen Warnmeldungen ausbleiben. Im Laufe des zweiten Halbjahres sind erste Exemplare solcher Fake-AntiViren-Software aufgetaucht, die den kostenlosen Virenscanner von ClamAV integrieren. Offenbar wollen sich die Online-Kriminellen damit der Strafverfolgung entziehen.

Mit gefälschten Bestellungen, Mitteilungen von Inkassobüros oder Benachrichtigungen über Probleme bei der Paketzustellung werden E-Mail-Nutzer zum Öffnen eines Dateianhangs oder zum Besuch einer schädlichen Webseite aufgefordert. Dort lauert Schadsoftware, die den Rechner infiziert.

Hier einige Beispiele:

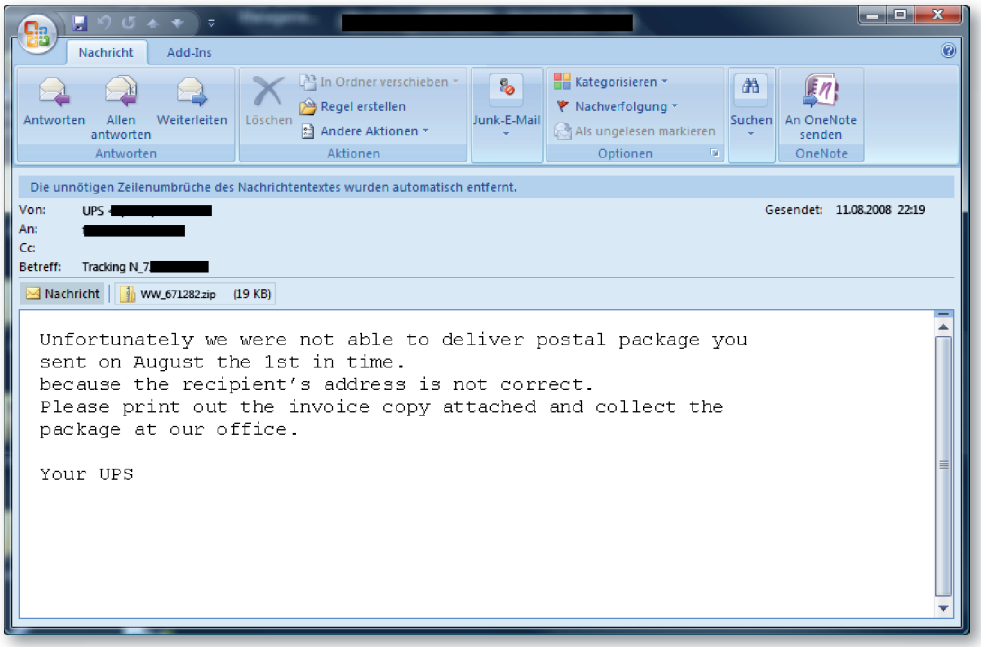

Abb. 1: Gefälschte UPS-Benachrichtigung vom 11. August. Die Datei im Anhang installiert Spyware.

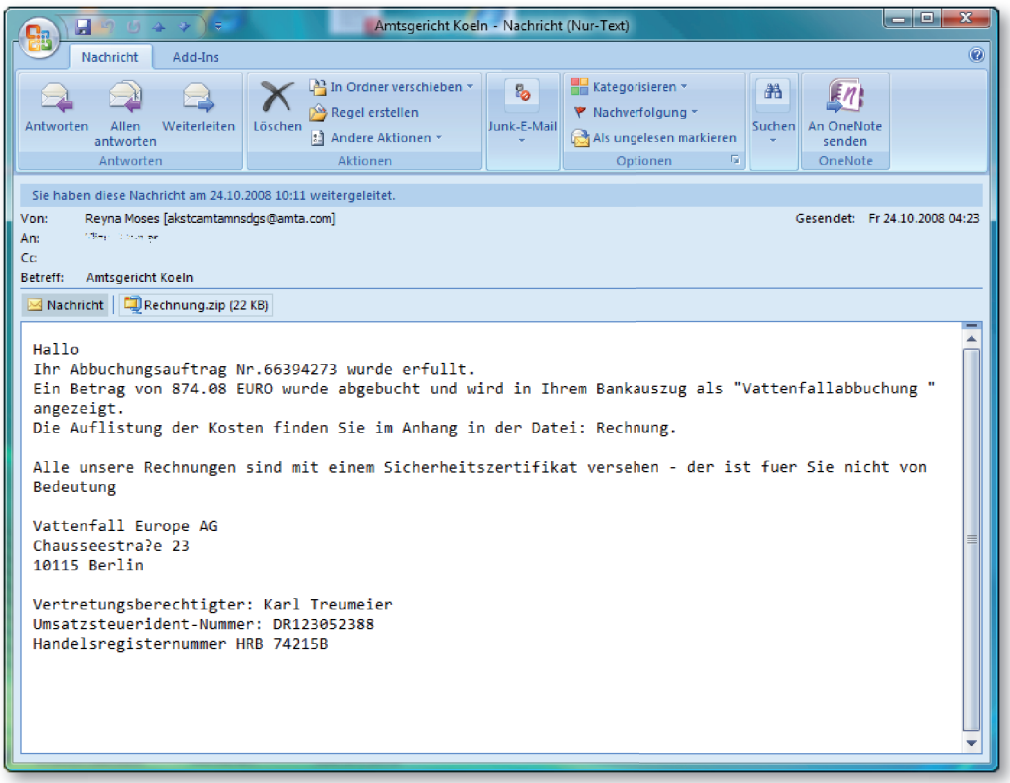

Abb. 2: Angeblicher Abbuchungsauftrag vom Amtsgericht Köln. Der Dateianhang „Rechnung.zip“ enthält einen Link namens „Rechnung.txt“ und den Schadcode als „Zertifikat.ssl“. Der Link führt diesen Schadcode als Kommandozeilenbefehl aus. (vgl. http://www.gdata.de/de/virenforschung/news/news-details/article/928-warnung-vor-gefaelschten-rechn.html)

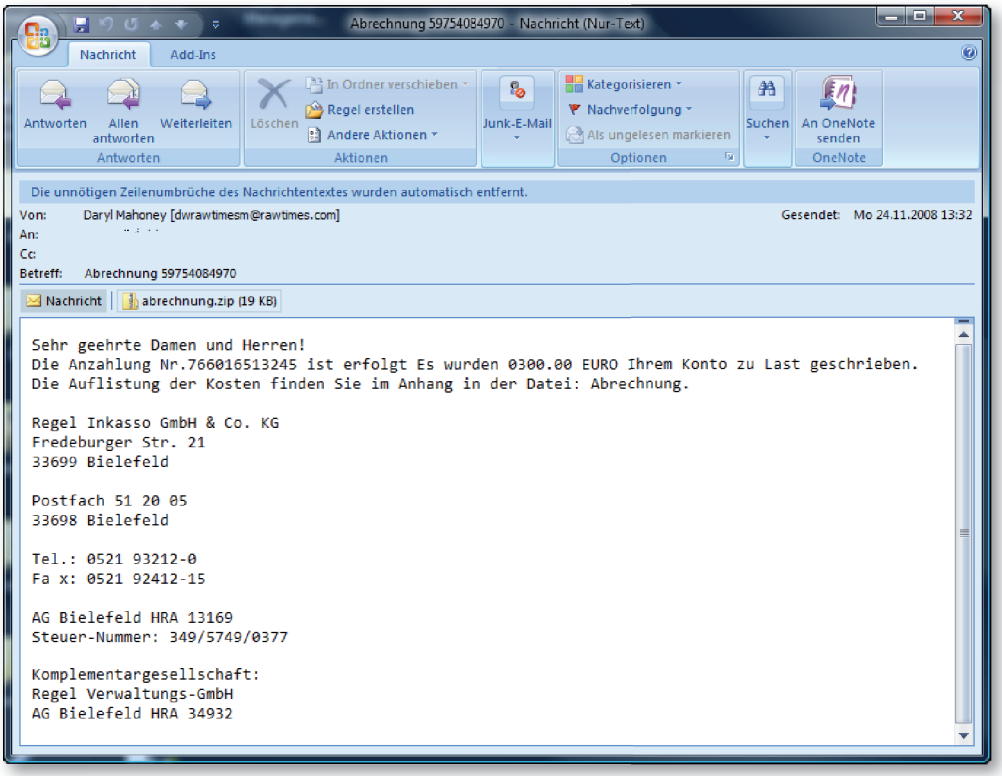

Abb. 3: Im Namen von Regel Inkasso werden „Abrechnungen“ verschickt, die den Rechner in ein Botnetz integrieren.

Cyber-War - das Internet als Waffe

Neben der weit verbreiteten kommerziellen Nutzung von Malware, werden Schadprogramme auch für politische Ziele eingesetzt. Mit Malware werden politische Gegner ausspioniert und es wird mit ihrer Hilfe Propaganda betrieben. Angriffe auf die gegnerische IT-Infrastruktur gehören in Konflikten schon seit einiger Zeit zum Arsenal der Streitkräfte. Der letzte größere Vorfall ereignete sich im Mai 2007, als russische Nationalisten in Estland Botnetze dazu nutzten, um die politische Auseinandersetzung über ein russisches Kriegerdenkmal zu ihren Gunsten zu entscheiden. Auch im zweiten Halbjahr 2008 wurden kriegerische Auseinandersetzungen ins Internet getragen.

- Während Russlands Feldzug gegen Georgien haben anti-georgische Spammer versucht, mit angeblichen BBC Meldungen ein Botnetz aufzubauen. Im August 2008 hat Georgien Russland beschuldigt die Webseite des Außenministeriums unzugänglich gemacht haben, so dass die Nachrichten des georgischen Außenministeriums auf einer Blogspot-Seite und der Seite des polnischen Präsidenten publiziert werden mussten. Auch gegen andere georgische Nachrichtenseiten (apsny.ge, news.ge) wurden verteilte Überlastangriffe (DDoS) ausgeführt. Die Webseite der georgischen Nationalbank wurde mit Bildern von Diktatoren und dem georgischen Präsidenten verunstaltet.
  Auch auf der Gegenseite wurden Überlastangriffe auf Webseiten der südossetischen Regierung und der russischen Nachrichtenagentur RIA Novosti ausgeführt.
- Im Konflikt zwischen Pakistan und Indien kommt es immer wieder zu virtuellen Auseinandersetzungen. So wurde im Oktober die Webseite der indischen Eisenbahngesellschaft Eastern Railway offenbar von pakistanischen Angreifern verunstaltet.
- Schon kurz nachdem Israel begonnen hat die Siedlungen im Gaza-Streifen zu bombardieren, wurden mehr als 300 israelische Webseiten mit anti-israelischen und anti-amerikanischen Botschaften versehen. Im Gegenzug starteten die Israelis eine Propaganda-Kampagne in der Blogosphäre. Sie eröffneten einen eigenen Youtube-Kanal und veranstalteten eine Pressekonferenz per Twitter. Auch bei Facebook werden Grabenkämpfe geführt. In Gruppen wie „Hamas, I don't like them" oder „Fxxk Israel" melden sich die Anhänger der jeweiligen Lager zu Wort. Einige dieser Gruppen wurden von der „Jewish Internet Defense Force" unzugänglich gemacht. Auf der Webseite „help-israel-win" konnte man freiwillig ein Programm herunterladen, das den Rechner in ein Botnetz integriert. Es führt Attacken auf feindliche Webdienste aus. Die israelische Übermacht auf diesem Gebiet wird noch dadurch gefestigt, dass Schiiten und Sunniten sich gegenseitig mit Cyber-Attacken behindern. Der sunnitischen Hamas kommt dieser Zwist momentan nicht gelegen.

Daten - Pleiten, Diebe und Pannen

Auch im 2. Halbjahr von 2008 wurden zahlreiche Fälle von Datendiebstahl, Datenpannen und Datenschutzverletzungen bekannt. Hier eine Auswahl:

Der gläserne Bürger

Bei der Verbraucherzentrale Schleswig-Holstein beschweren sich Bürger über unautorisierte Abbuchungen. Es stellt sich heraus, dass alle Kunden kurz zuvor Lose der Süddeutschen Klassenlotterie (SKL) per Kontoabbuchung bezahlt haben. Den Call-Center-Angestellten liegen offenbar die Kontodaten der Opfer vor. Die Verbraucherzentrale erhält Anfang August anonym eine CD mit den Daten von 17.000 Bundesbürgern. Die Daten mit Name, Geburtsdatum, Adresse, Telefon- und Kontonummer wurden von einer Firma aus NRW verkauft. Einige betrügerische Call-Center-Mitarbeiter nutzen solche Daten offenbar dazu, um nach einem kurzen – möglicherweise auch belanglosen – Gespräch, Geld vom Konto des Angerufenen abzuheben. Die Wirtschaftswoche führte weitere Recherchen durch, die letztlich zur Call-Center-Affäre führten. Sie gab im November bekannt, dass die Kontodaten von ca. 21 Millionen Bürgern im Umlauf sind. Das betrifft also 3 von 4 Kontoinhabern. Als Urheber kommen meist kleine Call-Center in Betracht.

vgl: http://www.verbraucherzentrale-sh.de/UNIQ123246437731306/link481821A.html

http://www.wiwo.de/unternehmer-maerkte/kontonummern-von-21-millionen-buergern-illegal-im-umlauf-380382/

Best Western

25. August
8 Millionen Datensätze von Kunden der Hotelkette Best Western, die im letzten Jahr dort übernachtet hatten, wurden von einem indischen Cracker gestohlen und über ein Untergrundforum an die russische Mafia verkauft.

Datenpannen in Großbritannien

In der zweiten Jahreshälfte wurde die Serie von Datenverlusten in Großbritannien fortgesetzt. Die Ereignisse zeigen einerseits wie vielfältig die Möglichkeiten zum Verlust von Daten sind und andererseits wie unbedarft und leichtfertig mit persönlichen Daten umgegangen wird.

- Juli: In einem Zug werden Geheimdokumente über das Terror-Netzwerk Al-Kaida gefunden.
- 25. August: Ein USB-Stick mit den Daten von 84.000 britischen Gefängnisinsassen – darunter 33.000 Datensätze von mehrfach Verurteilten - wird vermisst. Eine Firma, die ein System zur Datenverwaltung schreiben sollte, hat den Datenträger verschlampt. Insgesamt verschwanden 2008 in Großbritannien 26 USB-Sticks mit teilweise als geheim eingestuften Informationen.
- 27. August: Bei eBay wird für 45 € ein Computer versteigert, der die Namen, Mobilfunktelefonnummern, Kontodaten und Unterschriften von mehr als einer Million Kunden der Royal Bank of Scotland (RBS) enthielt.
- 8. September: Eine Festplatte mit Angaben zu Name, Geburtsdatum, Versicherungsnummer und Wohnort von ungefähr 5000 Gefängnismitarbeitern des britischen National Offender Management Service (NOMS) ist verschwunden. Jeder 9. Angestellte der Firma ist betroffen. Einige fordern eine Versetzung zu einem anderen Arbeitsplatz und/oder einen Umzug, um ihre Familien vor möglichen Übergriffen zu schützen.

- 18. September: Die Insolvenzbehörde gibt den Verlust eines Laptops mit persönlichen Daten von 122 früheren Firmenchefs bekannt. Außerdem befanden sich auf dem Laptop Informationen über Gläubiger, Investoren und Mitarbeiter.
- 30.September: Eine Digitalkamera, die bei eBay für 25 € versteigert wurde, enthielt hochbrisante Daten des britischen Geheimdienstes MI6 über Al-Kaida Terrorverdächtige mit Bildern und Fingerabdrücken und über Waffenlieferungen.
- 10. Oktober: Aus einem Büro des IT-Dienstleisters EDS verschwindet eine tragbare Festplatte mit den Namen, Adressen, Geburtsdatum und weitere Informationen von 100.000 Armeeangehörigen und 600.000 Bewerbern.
- 10. November: In der Weihnachtswoche hat der Zahlungsdienstleister RBS WorldPay nach ersten Betrugsfällen zugegeben, dass durch einen Hackerangriff ca. 1,5 Mio. Datensätze gestohlen wurden. Bei den Daten handelte es sich um persönliche Daten von Nutzern von PrePaid- und Geschenkkarten und um die PINs aller PIN-basierten Karten. Von ca. 1.1 Millionen Kunden wurde die - in den USA so wichtige - Sozialversicherungsnummer gestohlen.

Datenpannen in Deutschland

Aber auch in Deutschland wurde der Datenschutz mit Füßen getreten:

- Bei LIDL, Penny, Plus, Norma, Rewe, Edeka, Tegut, Hagebau und in vielen anderen Betrieben werden Mitarbeiter überwacht und bespitzelt.
- Die Telekom nimmt das Recht selbst in die Hand und nutzt die vorliegenden Verbindungsdaten, um Löcher in der eigenen Unternehmenskommunikation aufzuspüren.
- Die Lufthansa wertet illegal die Flugdaten von Passagieren (darunter auch Journalisten) aus
- Über die Gewerkschaft der Polizei waren die Handynummern von 13.500 Berliner Polizisten frei im Internet zugänglich.
- Zwei ehemalige Mitarbeiter von T-Mobile stehlen 17 Millionen Kundendaten (Adressen, Mobilfunknummer, Geburtsdatum und evtl. E-Mail-Adressen) darunter auch Prominente aus Politik, Wirtschaft und Medien und verkaufen sie an dubiose Datenhändler

Prominente Hacks

Auch in diesem Halbjahr waren wieder einige Persönlichkeiten des öffentlichen Lebens Opfer von mehr oder weniger gezielten Angriffen:

- Am 18. September wird bekannt, dass Sarah Palin privater Mail-Account bei Yahoo gehackt wurde. Der Angreifer beantwortete dazu die Sicherheitsfragen, wenn man sein Passwort vergessen hat. *(vgl. http://blog.wired.com/27bstroke6/2008/09/palin-e-mail-ha.html)*
- Im September wird von einem Konto des französischen Präsidenten Sarkozy ein kleiner Betrag abgebucht. Es ist ziemlich unwahrscheinlich, dass Sarkozy seine Daten auf einer Phishing-Seite eingegeben hat. Es handelt sich auch nicht um einen gezielten Angriff. Viel wahrscheinlicher ist, dass einer seiner Rechner mit einem Banking-Trojaner verseucht war. Solche Daten werden in Hunderter oder Tausender Paketen verkauft. Beim Kauf werden üblicherweise einige wenige Accounts zum Testen verwendet. Die Datenkäufer haben Sarkozys Daten zur Prüfung der Validität des gesamten Datenpakets genutzt. Offenbar waren sich die Datendealer nicht darüber bewusst, mit wem sie es zu tun hatten.

Datenschutz

Nach wie vor sind sich viele Bürger nicht darüber bewusst, wie viele Daten über sie erhoben werden und wie wertvoll diese Daten werden können. Erst langsam zeigen Missbrauchsfälle, die z.B. zu Belästigungen, Beeinträchtigungen der Sicherheit oder zu finanziellen Verlusten führen, wie Daten missbraucht werden können. Neben den Online-Kriminellen, die mit solchen Daten ihre Opfer um Geld betrügen, profitieren dubiose Geschäftemacher vom sorglosen Umgang mit Kundendaten und Meldeinformationen. Durch die Call-Center-Affäre ist klar geworden, dass das Ausmaß weit über Einzelfälle hinausgeht. Die Daten der meisten Bürger sind längst bei Datenvermarktern zugänglich. Der Wert von Daten und deren Schutz wird immer noch unterschätzt.

Im Kampf gegen die eCrime-Ökonomie

Im Oktober 2008 ist es den Strafverfolgungsbehörden nach einer zwei-jährigen Undercover-Mission gelungen das Online-Carding-Forum „Dark Market" zu schließen und weltweit insgesamt 56 Personen zu verhaften. Dark Market war einer der berüchtigten Umschlagplätze für Kreditkarten- und Bankzugangsdaten.

Als weitaus effektiver hat sich aber ein anderer Ansatz erwiesen. Auch die Webseiten, Daten und Kontrollserver der Malware-Industrie müssen auf irgendwelchen Rechnern gehostet werden. Das Russian Business Network (RBN) hat es im Bereich „Bullet-Proof-Hosting" im letzten Jahr zu trauriger Berühmtheit gebracht. Die gestiegene Aufmerksamkeit - auch bei den Verfolgern - war allerdings den Geschäften abträglich. Das RBN teilte sich in mehrere Splittergruppen in China und Osteuropa. So konnten andere Hosting Services in die Bresche springen, die nicht in Osteuropa oder China, sondern in den USA agierten.

Ende August 2008 wurde berichtet, dass die kalifornische Firma Intercage - die kurz zuvor noch Atrivo hieß - ihre Hosting und Domain-Registrierungs Dienstleistungen hauptsächlich in den Dienst von illegalen Anbietern stellen *(vgl. http://hostexploit.com/downloads/Atrivo%20white%20paper%20090308ad.pdf)*. Bei Spamhaus ist Atrivo/Intercage in 3 Jahren mit mehr als 350 Fällen von Malwareverbreitung und Command & Control Server für Botnetze aufgefallen. Zwei Provider von Intercage kündigten aufgrund des öffentlichen Drucks die Verträge mit Intercage und so waren die Server aus dem Internet nicht mehr erreichbar. Ein mit Intercage befreundeter Provider, der eingesprungen war, beugte sich nach wenigen Tagen dem öffentlichen Druck. Damit waren die Malware- und Spam-beladenen Server von Intercage seit dem 21. September nicht mehr erreichbar. Kurze Zeit später wechselte Intercage zu einem estnischen Provider. Resultate waren:

- für kurze Zeit reduzierte sich das Spam-Aufkommen.
- Die Turbulenzen um Intercage führten dazu, dass die Aktivitäten des Sturm-Botnetzes zum Erliegen kamen.

Im Zusammenhang mit den Nachforschungen zu Intercage gerät Anfang September der Privacy Protection Service des indischen Domain-Registrars Directi in die Kritik. Diese wurde aber schnell ausgeräumt. *(vgl. http://www.knujon.com/news.html#09042008)*. Beim estnischen Registrar ESTDomains entwickelte sich das allerdings anders. Immer wieder wurden dort Domains registriert, die in illegale Geschäfte, Spam und Phishing verwickelt waren. Am 28. Oktober kündigt ICANN die Zusammenarbeit mit ESTDomains auf und schreibt die Verwaltung der 281.000 Domainnamen, die von ESTDomains betreut werden aus *(vgl. http://www.icann.org/en/announcements/announcement-2-28oct08-en.htm)*

Die stärksten Auswirkungen auf die Internet-Community hatte allerdings die Isolierung des kalifornischen Hosting-Providers McColo. Brian Krebs von der Washington Post publizierte die Zusammenhänge von McColo mit Pharma Domains und Payment Sites, Scareware, Kinderpornografie-Webseiten, Anonymisierungs-Diensten und last not least Botnetz-Controller für die notorischsten Spam-Botnetze. Als McColo am 11. November vom Netz genommen wurde, sank das Spam-Volumen von einem auf den anderen Tag auf ein Drittel (vgl. Abb. 4). Auch der Proxy-Dienst von Fraudcrew kommt zum Erliegen.

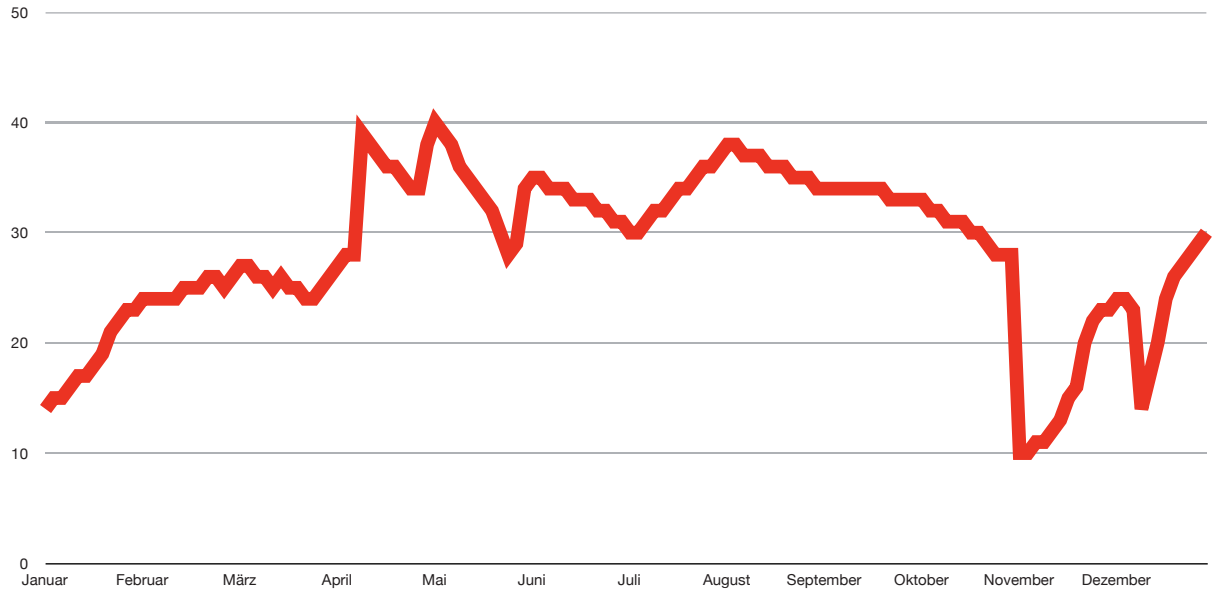

Abb. 4: Anzahl der Spam-Mails pro Sekunde von Januar bis Dezember 2008.

Der Shutdown von McColo war so überraschend für die Botnetzbetreiber, dass mit einem Schlag mehrere Hunderttausend Zombie-PCs herrenlos waren. Alle 72 Stunden berechnen die Zombies 4 Notfall-Domains und suchen dort nach einem neuen Master. Aber die Spezialisten der Firma FireEye haben den Algorithmus geknackt und die resultierenden Domains für sich registriert. Da FireEye die Registrierungsgebühren von ca. 4000 $ pro Woche nicht länger tragen konnte, wurde Ende November die Registrierung aufgegeben. So konnten die Bot-Herder wieder auf ihr Botnetz zugreifen. Auf die aus technischer Sicht durchführbare Desinfektion der infizierten Rechner hat FireEye aus rechtlichen Gründen verzichtet. Da auf den McColo Servern die Kommando-Server von etlichen Botnetzen gehostet wurden, hat sich in der Folge die Botnetz-Szene stark verändert (vgl. Abb. 5). Der Effekt auf das Srizbi-Botnetz war durchschlagend. Srizbi war bis dahin das größte Botnetz (ca. 450.000 Zombies), über das die meisten Spam-Mails verschickt wurden. Im November sank der Anteil des Srizbi-Botnetzes gegen Null. Offenbar waren die „Kunden“ nicht willens zu warten, bis Srizbi wieder einsatzbereit ist. Kurz-

fristig übernahmen Pushdo (alias Cutwail) und Bobax. Seit Anfang Dezember ist Mega-D das stärkste Botnetz, aber zum Jahreswechsel holen Rustock und das neue Botnetz Xarvester auf. Mit Waledec und Cimbot stehen weitere Botnetze in den Startlöchern. Diese neuen Botnetze sind so angelegt, dass sie aus den Erfahrungen der Vergangenheit lernen. Die Kommunikation ist verschlüsselt und die Fall-Back-Mechanismen sind so ausgeklügelt, dass ähnliche Engpässe wie bei McColo vermieden werden. Es wäre zwar zu wünschen, dass 2009 weitere Erfolge dieser Art verzeichnet werden können. Aber man sollte die Botnetzbetreiber nicht unterschätzen und zu hohe Erwartungen stellen.

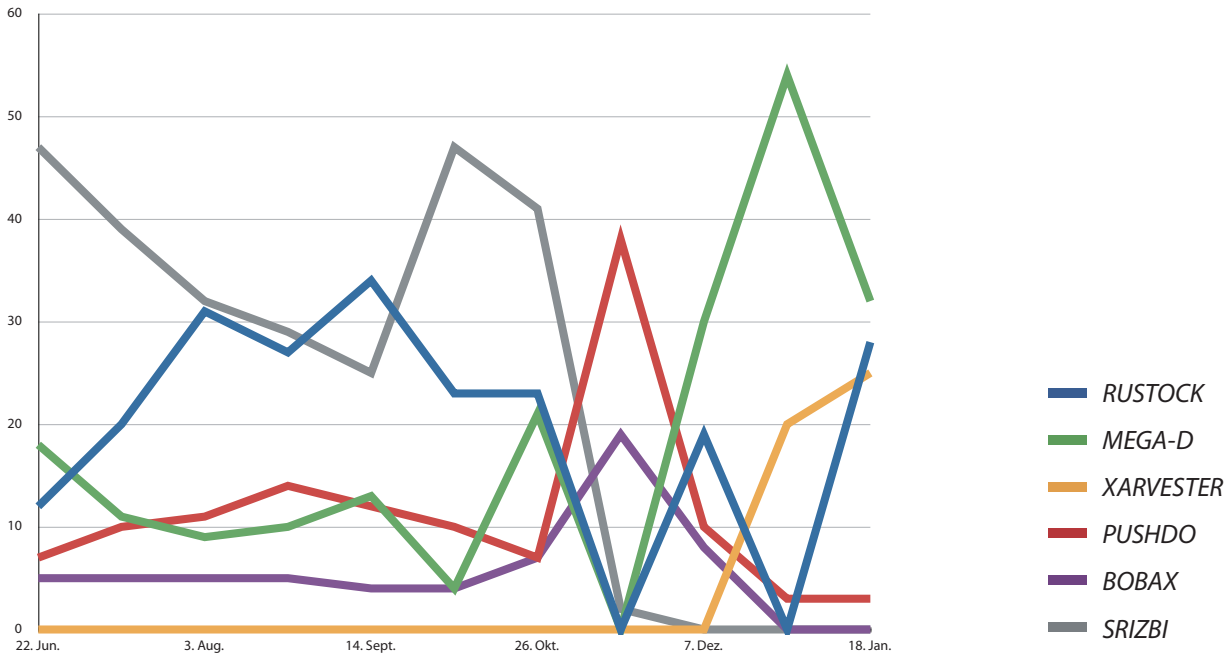

Abb. 5: Anteil der Botnetze am Spamversand

Kalender

Neben den thematisch gruppierten Ereignissen aus dem vorangegangenen Kapitel gab es auch einige interessante Neuerungen und Ereignisse, die hier kalendarisch aufgelistet werden sollen.

Juli 2008

GetCodec-Wurm nutzt Audio- und Videodateien zur Verbreitung

Am 9. Juli taucht ein neuer Wurm namens „GetCodec“ auf, der sich über Multimedia-Dateien des Formats WMA/WMV verbreitet. In diesem Dateiformat ist weit mehr enthalten als die reinen Audio- bzw. Videodaten. Sie enthalten auch Informationen über benötigte Codecs. GetCodec verändert diese Informationen so, dass der MediaPlayer den Codec nicht findet und stattdessen versucht einen Codec aus dem Internet nachzuladen. Bis dahin waren solche Anfragen zur Installation von Codecs nur aus dem Browser bekannt. GetCodec erweitert die Gefahrenzone auf den Media Player selbst. Wenn der Nutzer den Bestätigungsdialog mit OK schließt, wird anstelle des Codecs ein Trojanisches Pferd installiert, das weitere Schadsoftware nachlädt - darunter auch einen Wurm, der weitere WMA/WMV-Dateien infiziert. Spätere Varianten können auch MP2 und MP3 Dateien infizieren. Die Dateien werden in das WMA/WMV-Format umgewandelt, die Dateiendung ändert sich dadurch aber nicht.

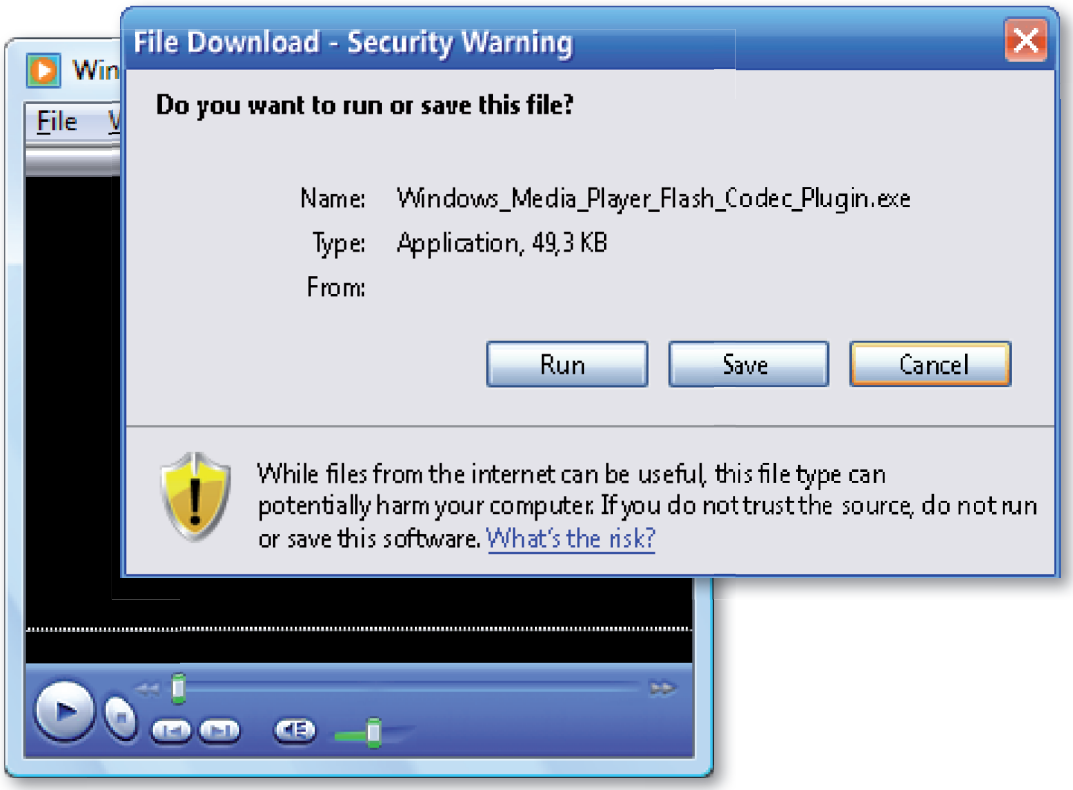

Abb. 6: GetCodec fordert zur Installation eines Codec aus dem Media Player auf

3. Weltkrieg

Am 10. Juli wird in E-Mails des Sturm-Botnetzes der 3. Weltkrieg angekündigt. Die Videos, die angeblich von Soldaten gedreht wurden, verlangen nach einem trojanisierten Codec. Ansonsten versiegen die Aktivitäten des Sturm-Botnetzes in den folgenden Monaten vollständig.

Abb. 7: Video-Ankündigung des 3. Weltkriegs

Monster-Phisher

Nutzer der Jobbörse Monster werden am 14. Juli Ziel von Phishing-Mails. In E-Mails mit Betreffs wie „Monster customer service: new security measures. „ wird den Empfängern vorgetäuscht, dass durch eine technische Änderung eine Neuanmeldung erforderlich ist. Wer dem in der E-Mail enthaltenen Link folgt, wird auf eine gefälschte Seite geleitet, die der echten sehr ähnlich sieht. Wer dort seine Login-Daten eingibt, gibt Lebensläufe und enthaltene persönlichen Daten den Phishern preis.

August 08

Soziale Netzwerke im Visier

Social Networks erfreuen sich immer größerer Beliebtheit - auch bei Cyber-Gangstern. Gestohlene Accounts werden dazu verwendet Spam-Nachrichten zu hosten und zu verbreiten. Am 2. August verschickt ein Schädling namens „Koobface“ Nachrichten an Freunde in MySpace und Facebook, in denen ein interessantes Youtube-Video angepriesen wird. Auf dem russischen Youtube-Imitat wird zum Update des Flash-Players aufgefordert, der sich als Downloader herausstellt.

Auch bei Twitter kommt es Anfang August zu ersten Fällen der Malware-Verbreitung. Auf speziell erstellten Profilen wird mit verlockenden Bildern und Texten auf Webseiten mit Videos verwiesen. Dort wird man zur Installation des Flash Players aufgefordert, der sich als Downloader entpuppt und Banking-Trojaner nachlädt. Der Besuch der präparierten Profile kann per Spam oder Instant Message beworben werden. Twitter bietet hier allerdings eine weitere Möglichkeit. Durch eine Sicherheitslücke kann man durch einen unbedachten Klick auf einen Link zum „Follower“ eines bestimmten Profils werden *(vgl. http://blogs.zdnet.com/security/?p=1611).*

Trojaner im Weltall

Auf der Weltraumstation ISS wird ein Online-Gaming-Trojaner gefunden. Er ist offenbar per USB-Stick oder über ein verseuchtes Laptop dorthin gelangt. Die Rechner der ISS sind nicht mit dem Internet verbunden. *(vgl. http://blog.wired.com/27bstroke6/2008/08/virus-infects-s.html)*

Olympia - auch für Malware

Sportliche Großereignisse wie z.B. das Superbowl-Endspiel in den USA wurden auch im letzten Jahr schon von Malware-Autoren ausgenutzt. Auch im Umfeld der Olympischen Spiele in China kam es zu verstärkten Aktivitäten bei Spam und Malware. Hier einige Beispiele:

- Ein Imitat einer PowerPoint-SlideShow, zeigt Bilder der Eröffnungszeremonie und installiert eine Backdoor.
- Word und PDF-Dokumente versprechen Informationen zu den Olympischen Spielen
- Screensaver mit Namen wie „2008BejingOlympics.scr“ oder „100Olymp.scr“ verseuchen den PC mit Downloadern und Backdoors.
- Mehrere hundert Webseiten, die Informationen zu den Olympischen Spielen enthalten sollen, werden zur Verbreitung von Malware genutzt. Am häufigsten waren asiatische Nutzer betroffen.

September 08

Google Chrome Beta

Die meisten Angriffe auf Rechner erfolgen über den Browser. Die Wahl des Browser ist daher für viele Anwender eine Vertrauensfrage. Anfang September 2008 bietet Google mit „Chrome“ eine erste Beta-Version eines Browsers an. Durch den internen Aufbau soll er gegen Angriffe wie Cross Site Request Forgery schützen. Die meisten Bedenken richten sich aber gegen die Datensammelwut von Google.

Oktober 2008

ClickJacking

Am 15. Oktober wird eine neue Methode zum Ändern von Einstellungen im Browser vorgestellt, bei der die Klicks in speziell erstellten Online-Spielen dazu genutzt werden können, um z.B. die Einstellungen von Flash so zu ändern, dass die Webcam angeschaltet wird. *(vgl. http://video.google.com/videoplay?docid=-1023253423246814538&hl=en)*

November 2008

Ähnlich wie die Olympischen Spiele wurde auch die Präsidentschaftswahl genutzt, um Malware zu verbreiten. Obama und McCain sind immer wieder in Betreffzeilen von Spam-Mails vertreten, die auf Seiten von Pharmazieprodukten oder auf Malwareseiten verweisen. Auch einige Dateinamen enthielten den Namen Obama:

- „Beat_Obama_NNN.exe“ (NNN steht für eine zufällige Zahlenfolge) installierte Backdoors der PcClient-Familie.
- Ein anderer Dateiname suggeriert sexuelle Aktivitäten von Obama mit einer 17 jährigen.

Wie testet man Antiviren-Software?

10. November
AMTSO veröffentlicht Richtlinien zum Testen von Anti-Malware. Die Anti-Malware Testing Standards Organization ist ein Zusammenschluss von Malware-Testinstituten, Journalisten, Akademikern und Herstellern von Virenschutzlösungen. Nach langen Diskussionen werden am 10. November Richtlinien für die Durchführung von aussagekräftigen und neutralen Vergleichstests veröffentlicht. Die Richtlinien sollen offene, transparente und neutrale Tests ermöglichen, die mit angemessenen Testmethoden durchgeführt werden und zu brauchbaren und sinnvollen Ergebnissen führen. *(vgl. vgl. http://www.amtso.org)*

Dezember 08

Malware-Fox

5.Dezember
ChromeInject ist ein Trojanisches Pferd, das sich unter dem Namen des GreaseMonkey-Add-Ons in Firefox integriert und anschließend die eingegebenen Daten auf mehr als 100 Bankenseiten mitliest und an einen Server in Russland schickt.

Scareware wird verboten

11. Dezember
Die amerikanische Federal Trade Commission (FTC) gewinnt vor Gericht gegen zwei Herstellern von Scareware. Ihnen wird der Verkauf ihrer angeblichen Schutzprogramme untersagt. Diese werden häufig auf Webseiten „beworben“, indem ein gefälschter Scan den Rechner als verseucht klassifiziert. Produkte wie WinFixer, WinAntivirus, DriveCleaner, ErrorSafe und XP Antivirus schützen aber nicht vor Malware. Außerdem wurde das Vermögen der beiden beklagten Firmen Innovative Marketing, Inc. und ByteHosting Internet Services, LLC eingefroren.

Curse of Silence

Auf dem 25. Chaos Computer Congress in Berlin präsentierte Tobias Engel eine Sicherheitslücke für Symbian S60 Smartphones von Nokia und Sony Ericsson. Mit einer besonders formatierten SMS bricht beim empfangenden Smartphone ohne weitere Hinweise oder Warnmeldungen der SMS-Dienst zusammen. Danach können keine SMS/MMS mehr empfangen werden.

Malware: Zahlen und Daten

Die Malware-Flut steigt weiter

Im zweiten Halbjahr 2008 ist die Zahl der neuen Schädlinge weiter gestiegen. Im ersten Halbjahr waren es 318.248 neue Schädlinge, im zweiten 576.002. Damit wurden die Rekordzahlen des vergangenen Halbjahres um fast das Doppelte übertroffen. Über das ganze Jahr 2008 gesehen wurden 894.250 neue Schädlinge gezählt - 6,7 Mal mehr als 2007. Die Anzahl der Virenfamilien für das gesamte Jahr 2008 liegt - gemessen an der deutlich gestiegenen Anzahl - mit 3069 gegenüber 2313 aus 2007 nur wenig über der Zahl von 2007. Im zweiten Halbjahr hat die Anzahl der Virenfamilien gegenüber dem ersten Halbjahr von 2395 auf 2094 sogar abgenommen. Die gestiegene Zahl an Malware geht wohl nicht auf eine stark gestiegene Zahl an neuen Malware-Autoren.

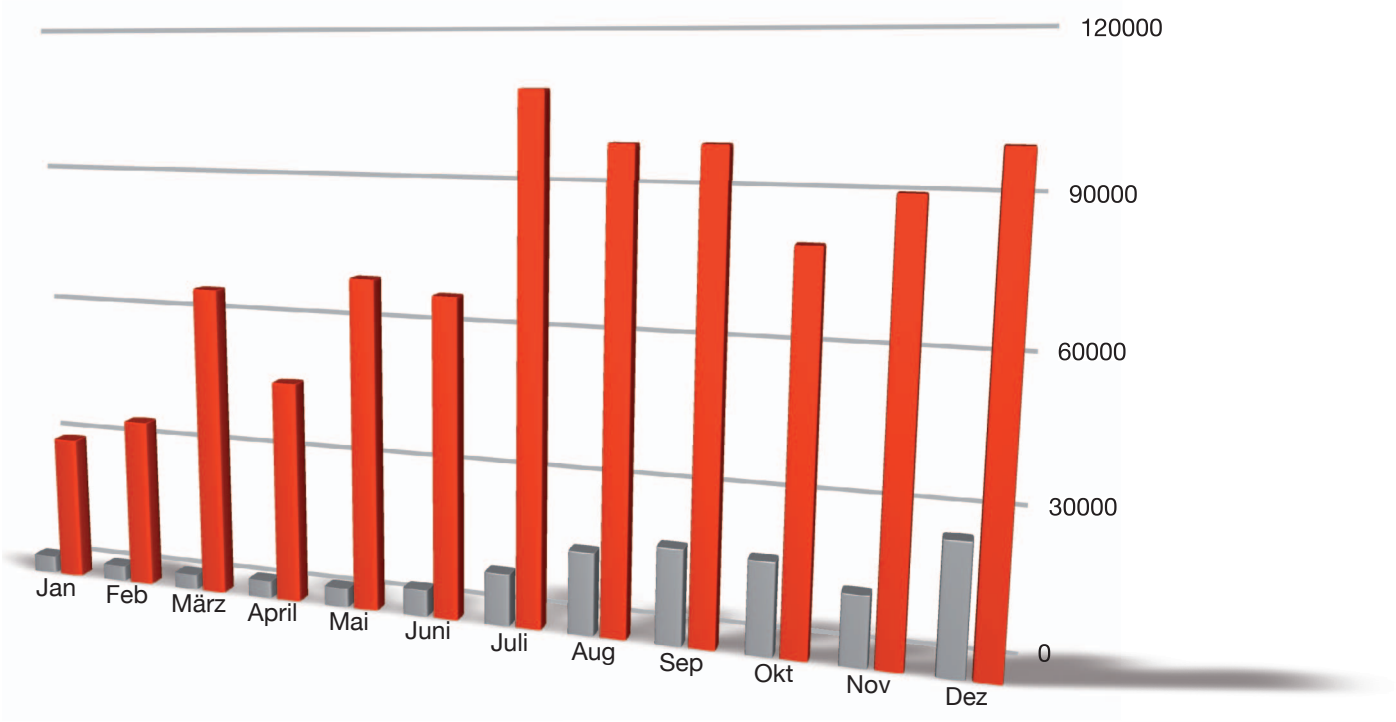

Diagramm 1: Anzahl neuer Malware pro Monat für 2007 (grau) und 2008 (rot).

Ursachen für die erneut gestiegene Zahl sind u.a.

- Modularisierung: Malware kommt nicht mehr als monolithischer großer Block. Stattdessen werden alle Funktionen in spezielle Unterprogramme aufgeschlüsselt.
- Mehrfachnutzung: Um der Entdeckung durch Signaturen zu entgehen, können Malware-Dateien z.B. durch verschiedene Verschleierungstechniken und/oder Laufzeitpacker so verändert werden, dass sie von Virenschutzprogrammen nicht mehr erkannt werden. Die Funktionalität der Malware bleibt dabei (weitestgehend) erhalten
- Wegwerf-Trojaner: Viele Downloader und zahlreiche Trojanische Pferde sind für den einmaligen Gebrauch gedacht. Nachdem sie ihren Dienst getan haben, werden sie von den infizierten Systemen eliminiert und von den Malware-Autoren in dieser Form nicht wieder verwendet

- Update als Tarnmechanismus: Einige Botnetzbetreiber führen häufig Updates der Backdoor-Komponenten durch. Das dient einerseits zur Software-Pflege, wird aber auch genutzt, um neue Versionen zu installieren, bevor die Signatur-Updates der AV-Hersteller die Malware erkennen.
- Auftragsarbeit: Die Zombie-PCs in Botnetzen sind die Erfüllungsgehilfen von Spam-Versendern, Phishern, Erpressern und Malware-Distributoren. Die Botnetzbetreiber vermieten ihre Netze für bestimmte Zeit oder für die Durchführung bestimmter Aufträge. Dazu bekommt jeder Zombie ein Software- und Datenpaket, das er abarbeiten soll. Wenn die Arbeit beendet ist, werden Software und Daten vom betroffenen Rechner gelöscht. Je vielfältiger die Nutzung eines Botnetzes, desto mehr spezielle Malware wird verbreitet.
- Server-seitige Polymorphie: Immer mehr Malware wird über Webseiten ausgeliefert. Wenn ein Opfer auf eine verseuchte Seite gelangt, wird anhand der IP-Adresse die Region des Besuchers, und weiterhin der Browser und das Betriebssystem und deren Versionen ermittelt. Anhand dieser Informationen erhält jeder Besucher maßgeschneiderte Malware. Theoretisch könnte auf dem Server anhand dieser Informationen eine Verschlüsselung der Datei erfolgen, so dass jeder Besucher einer Webseite eine unterschiedliche Version der Malware erhält. Auf diese Weise können Tausende Varianten der gleichen Malware verbreitet werden.

Um die Malware-Flut weiterhin unter Kontrolle zu halten, wird die proaktive Erkennung immer wichtiger. Heuristische Signaturen erkennen Malware anhand spezifischer Merkmale, die auch auf neue Malware zutrifft. Die Erkennung anhand des Verhaltens ist eine weitere Möglichkeit Schadcode, der auf den Rechner gelangt ist zu erkennen. G DATA hat in der Generation 2009 die proaktive Erkennung weiter verbessert und bietet trotz der Malware-Schwemme höchste Erkennungsraten in kürzester Zeit auch bei bislang unbekannter Malware.

Botnetze, Spyware und Adware bestimmen das Geschehen

Betrachtet man die Kategorien von Malware und ihre Entwicklung, so ergibt sich ein ähnliches Bild wie im ersten Halbjahr. Es gibt allerdings auch einige Neuerungen. Nach wie vor gehören Spyware und Adware zu den häufigsten Kategorien. Auch die Downloader, die zur Infektion von Rechnern eingesetzt werden und die Backdoors, die es ermöglichen Rechner fernzusteuern und in Botnetze zusammenzufassen belegen die vorderen Plätze. Die Steigerungsraten in diesen Bereichen liegen im Großen und Ganzen auf dem Durchschnittsniveau von 181%.

Kategorie	# 2008 H2	Anteil	# 2008 H1	Anteil	Diff 2008 H1 und 2008 H2
Trojan. Pferde	155.167	26,9%	52.087	16,40%	321%
Backdoors	125.086	21,7%	75.027	23,60%	166%
Downloader/ Dropper	115.358	20,0%	64.482	20,30%	172%
Spyware	96.081	16,7%	58.872	18,50%	162%
Adware	40.680	7,1%	32.068	10,10%	127%
Würmer	17.504	3,0%	10.227	3,20%	171%
Tools	7.727	1,3%	12.203	3,80%	60%
Rootkits	6.959	1,2%	1.425	0,40%	487%
Exploits	1.841	0,3%	1.613	0,50%	114%
Dialer	1013	0,2%	4.760	1,50%	21%
Viren	167	0,0%	327	0,10%	51%
Sonstige	8.419	1,5%	5.170	1,60%	163%
Gesamt	576.002	100,0%	318.248	100,00%	181%

Tabelle 1: Anzahl und Anteil neuer Malwarekategorien im ersten und zweiten Halbjahr 2008 und deren Veränderung

Allerdings ist die Kategorie der Trojanischen Pferde[1] im zweiten Halbjahr um mehr als das dreifache angestiegen und vom 4. Platz auf die Spitzenposition gelangt. Dieser Anstieg ist durch die o.g. Auftrags-Trojaner zu erklären. Sie zeugen von der aktiven Nutzung von Botnetzen zum Versand von Spam, zur Durchführung von verteilten Überlastangriffen und von der stärkeren Modularisierung von Malware.

Die Anzahl der Exploits ist zwar gestiegen. Aber hier kommt es nicht auf Masse an. Wichtig ist, dass die verfügbaren Exploits möglichst schnell und effektiv ausgenutzt werden, wie bereits oben geschildert.

Die größte Steigerung erfolgte im Bereich der Rootkits. Das zeigt, dass sie sich als Tarnmechanismus für Malware bewährt und etabliert haben. Am deutlichsten abgenommen hat die Zahl der Viren (d.h. sich selbst replizierende Bootsektor- oder Dateiinfektoren) und Dialer. Die Bedeutung der Dialer nimmt mit der geringeren Nutzung von Modems immer mehr ab.

1 Die Kategorie der Trojanischen Pferde wird hier in einem engeren Sinn verwendet. Eigentlich gelten alle Computerschädlinge, die keine eigene Verbreitungsroutine besitzen als Trojanische Pferde. Also im Prinzip alle außer Würmer und Viren (z.B. Backdoors, Downloader, Spyware, Adware, Tools, Rootkits, Exploits und Dialer). In unserer Kategorie Trojanische Pferde zählen wir nur solche Trojanische Pferde, die keiner anderen Kategorie zugeordnet werden können.

Vorsicht Autorun

Die Top 10 der Virenfamilien zeigt einen Querschnitt durch die aktivsten Spielarten der Malware. Die aktivste Virenfamilie ist nach wie vor die Backdoor Hupigon. An zweiter Stelle unverändert die Varianten von „OnlineGames“, die meist per Keylogger die Zugangsdaten zu Onlinespielen stiehlt. Magania, die andere Familie, die Zugangsdaten zu Online-Spielen stiehlt, hat trotz erhöhter Aktivität drei Plätze verloren. Neu sind die Familien Monder und MonderB. Sie dienen dazu die Scareware-Programme aus der Virtumonde-Familie zu installieren, die mit falschen und nervigen Virenwarnmeldungen versuchen Programme namens WinFixer oder AntiVirus XP zu installieren. Durch diese Modularisierung war es nicht mehr notwendig die Kernkomponenten von Virtumonde so häufig zu aktualisieren, die vom 3. auf den 10 Platz rutscht. Die Autoren der Adware Cinmus, die sich in den Internet Explorer integriert und Werbe-PopUps anzeigt, waren in der zweiten Jahreshälfte deutlich fleißiger und haben mehr als doppelt so viele Variante erstellt als in der Ersten. Die Spyware Buzus konnte den 6. Rang behaupten. Einziger Neuzugang in der Top 10 ist die Backdoor PcClient, die es anstelle der Backdoors der Bifrose-Familie in die Top 10 geschafft hat.

	# 2008 H2	Virenfamilie	# 2008 H1	Virenfamilie
1	45.407	Hupigon	32.383	Hupigon
2	35.361	OnlineGames	19.415	OnLineGames
3	20.708	Monder	13.922	Virtumonde
4	18.718	MonderB	11.933	Magania
5	15.937	Cinmus	7.370	FenomenGame
6	13.133	Buzus	7.151	Buzus
7	13.104	Magania	6.779	Zlob
8	12.805	PcClient	6.247	Cinmus
9	11.530	Zlob	6.194	Banload
10	10.412	Virtumonde	5.433	Bifrose

Tabelle 2: Top 10 Aktivste Virenfamilien im ersten und zweiten Halbjahr 2008

Eine Familie sei noch erwähnt. Die aktivste Wurm-Familie Autorun schafft es mit 7256 neuen Varianten gegenüber 2756 im ersten Halbjahr auf Rang 14. Diese Familie nutzt u.a. die Autostart-Funktionen des Betriebssystems, um sich zu verbreiten. Dazu schreiben sie Informationen in die Datei autorun.inf. Diese wird z.B. ausgewertet, wenn eine CD/DVD, ein USB-Datenträger oder eine Speicherkarte eingelegt bzw. angeschlossen wird. Auf diese Art und Weise erhielt Autorun zwar keine große Aufmerksamkeit, sorgte aber dennoch für zahlreiche Infektionen.

Flash-Malware im Aufwind

99,2% aller Malware zielt auf das Windows-Betriebssystem. Der Anteil ist im zweiten Halbjahr um ein weiteres Prozent gestiegen und auch absolut gesehen ist der Anteil an Nicht-Windows-Malware um ca. ein Fünftel gesunken. Das mag einerseits daran liegen, dass die aufwändigen Verschleierungsverfahren auf anderen Plattformen nicht notwendig sind. Es zeigt aber auch, dass die Malware-Autoren den Weg des geringsten Widerstands gehen und sich an Nutzer des Betriebssystem-Marktführers halten. Malware für andere Betriebssysteme wie UNIX (16) oder Apple (6) kommt äußerst selten vor. J2ME, die Java-Version für mobile Endgeräte und Smartphones, sticht hier mit 59 neuen Malware-Exemplaren hervor. Insgesamt sind für mobile Plattformen (J2ME, Windows CE und SymbianOS) 70 neue Schädlinge aufgetaucht. Die große Angriffswelle auf Smartphones und Mobilgeräte ist bislang ausgeblieben.

	Plattform	#2008 H2	% 2008 H2	#2008 H1	% 2008 H1
1	Win32	571.568	99,2%	312.656	98,2%
2	WebScripts	2.961	0,5%	3.849	1,4%
3	Scripts	1.062	0,2%	1.155	0,3%
4	MSIL	318	0,1%	252	0,1%
5	Makros	93	0,0%	164	0,0%

Tabelle 3: Top 5 Plattformen im ersten und zweiten Halbjahr 2008. WebScripts bezieht sich auf Malware, die auf JavaScript, HTML, Flash/Shockwave, PHP oder ASP basiert und üblicherweise Schwachstellen per Browser nutzt. „Scripts" sind Batch- oder Shell-Skripte oder Programme, die in den Skriptsprachen VBS, Perl, Python oder Ruby geschrieben wurden. MSIL ist Malware, die im Zwischencode von .NET-Programmen vorliegt. Makros sind in Makrosprachen für Anwendungen wie Word, Excel, AutoCAD, PowerPoint usw. geschrieben.

Auch Malware-Autoren nutzen die Möglichkeiten des .NET Framework bei der Programmierung. .NET-Anwendungen laufen - ähnlich wie Java-Anwendungen - auf unterschiedlicher Hardware. Darüber hinaus bietet .NET noch die Möglichkeit Anwendungen aus mehreren Projekten, die unterschiedliche Programmiersprachen nutzen, zusammenzusetzen. Damit dies gelingt werden sie in die Microsoft Intermediate Language (MSIL) übersetzt. Die Anzahl der Malware, die in dieser Zwischensprache von .NET-Applikationen erstellt ist, hat im zweiten Halbjahr gegen den Trend zugenommen und übertrifft die Anzahl an Java-Malware bei Weitem.

Obwohl immer mehr Angriffe über Webseiten erfolgen, ist die Zahl der Malware, die auf Web-basierten Skriptsprachen wie JavaScript, ASP, PHP oder ActionScript für Shockwave und Flash basieren insgesamt zurückgegangen. Insbesondere im Bereich der JavaScript-Malware sind im zweiten Halbjahr deutlich weniger Schädlinge aufgetreten (1910 vs. 2650 im ersten Halbjahr). Doch in dieser Gruppe stach Malware im SWF-Format heraus. Sie verzeichnete den prozentual stärksten Zuwachs (321 vs. 231 im ersten Halbjahr). Das SWF-Format nutzt die Skriptsprache ActionScript des Flash-Players. Dieser neue Weg ist noch wenig bekannt und nur die wenigsten Nutzer befürchten, dass ihr Rechner beim betrachten von Flash-Videos infiziert werden kann.

Ausblick 2009

Anhand der geschilderten Ereignisse, Zahlen und Trends kann man für die Entwicklung der Malware-Szene in der nächsten Zeit ein paar Vermutungen anstellen.

Mehr schädliche Webseiten

Der Browser wird als Einfallstor für Malware immer wichtiger und Angriffe auf den Browser und seine Komponenten werden ausgenutzt, sobald sie bekannt werden. Aber auch viele im Internet vorhandene Dienste werden verstärkt ausgenutzt, um ungewollte Werbebotschaften und Malware zu verbreiten. Insbesondere die Nutzer von Sozialen Netzwerken, Foren, Blogs, Online-Spielen und Web 2.0 Anwendungen sollten umsichtig agieren. Gecrackte Webserver, manipulierte Suchergebnisse und Tippfehler bei der Eingabe der URL können auf Seiten führen, auf denen der Rechner des Besuchers unbemerkt im Hintergrund infiziert wird (Drive-by-Download).

Mehr Flash Malware

Die Anzahl der Malware, die Flashs ActionScript zur Verbreitung von Malware nutzt ist im letzten Halbjahr deutlich gestiegen und wird voraussichtlich auch noch weiter zunehmen. Bislang werden Flash-Videos nicht als Bedrohung angesehen und das sind die besten Voraussetzungen für eine massive Nutzung durch Cyber-Kriminelle.

Abkehr von Windows?

In den letzten Jahren konzentriert sich Malware auf das Windows Betriebssystem. Der überwiegende Anteil der Infektionen erfolgt auf Rechnern mit Windows XP. Möglicherweise ändert sich das, wenn mehr Nutzer auf Vista oder Mitte des Jahres auf Windows 7 umsteigen. Im kommenden Halbjahr erwarten wir aber nicht, dass Windows aus der Schusslinie gerät. Es ist allerdings wahrscheinlich, dass Nutzer von Apples OS X sich verstärkt mit Malware befassen müssen. Malware für Smartphones wird auch in den kommenden Monaten eine untergeordnete Rolle spielen.

Die Jagd nach Daten geht weiter

Die Berichterstattung über Datenpannen und Datendiebstähle hat im letzten Halbjahr dazu geführt, dass das Bewusstsein für den Wert persönlicher Daten zugenommen hat. Dennoch bleibt hier noch einiges zu tun und Kriminelle werden weiterhin versuchen an Bank- und Kreditkartendaten zu gelangen. So wird Spyware auch in Zukunft einen tragenden Anteil der Malware ausmachen. Und wir werden wieder von Datenpannen hören.

Noch mehr Malware?

Im Jahresdurchschnitt wurde im 2. Halbjahr 2008 ein neuer Schädling pro Minute entdeckt[2]. Es ist durchaus denkbar, dass dieser Wert noch gesteigert werden kann. Klar ist, dass die Cyber-Crime-Ökonomie nicht verschwinden wird und weiterhin sehr produktiv sein wird. Die Frage ist aber ob die Online-Kriminellen noch mehr Dateien produzieren müssen. Wir erwarten zwar weitere Steigerungen, allerdings mit sinkenden Wachstumsraten.

2 Genau genommen waren es 65,75 pro Stunde.

Geschützt. **Geschützter. G DATA.**