Rückblick und Analyse der Bedrohungen im ersten Halbjahr 2009

Hanau, 22.Juli 2009: Der russische Antimalwarehersteller Doctor Web hat seinen Sicherheitsreport für das erste Halbjahr 2009 veröffentlicht. Dabei haben sich in den vergangenen sechs Monaten interessante Trends ergeben: Insbesondere Schadsoftware in Geldautomaten, Erpresser-Trojaner und neue Bedrohungen für Mac OS X nahmen stark zu. Im Frühjahr tauchte das erste große Botnetz auf. Dazu lässt sich auch ein Gegentrend beobachten – immer weniger neue PC's werden in das Botnetz Shadow (Conficker, Downdup) eingegliedert.

Bot-Netze

In den ersten Monaten des Jahres 2009 galt die Aufmerksamkeit der Sicherheitsexperten dem Netz-Wurm Win32.HLLW.Shadow. Die mit diesem Wurm infizierten Workstations wurden zu einem Bot-Netz vereint, das Millionen von PCs weltweit umspannt. Zur Verbreitung von Win32.HLLW.Shadow wurden verschiedene Methoden eingesetzt. Unter anderem nutzte man Window-Vulnerabilities, um Administratorpasswörter auszuspähen. Auch Wechseldatenträger waren für Malware ein beliebter Verbreitungskanal.

In der Hochphase der Epidemie von Win32.HLLW.Shadow, kreierten die Autoren mehrere Varianten des Wurms. Nach der Detektion wurden die Kennungen sofort in die Dr.Web-Virendatenbankent eingetragen. Momentan sind die Aktivitäten des Wurms rückläufig, folglich taucht er nicht mehr unter den Top-10-Bedrohungen auf.

Zu den bekannten Botnetzen der ersten Jahreshälfte muss auch das Botnetz Virut gezählt werden, das mit einem polymorphen Virus operierte. Besondere Beachtung verdient auch das Bot-Netz Tdss – in diesem Fall wurden Rootkit-Technologien verwendet. Auch das BackDoor.Tdss verbreitete sich ebenfalls aktiv und verfügt über unterschiedliche neue Modifikationen. Momentan ist die Malware als Kit von Modulen, die zu einer Komponente des oben genannten Backdoors gehören, anzutreffen. Daher lässt sich schließen, dass BackDoor.Tdss-Module kommerziell genutzt werden.

Eines der bedeutendsten Botnetze in letzter Zeit, stellt die Familie von Bootkits BackDoor.MaosBoot dar. Dieses Bootkit ist hinsichtlich seiner Desinfektion eine harte

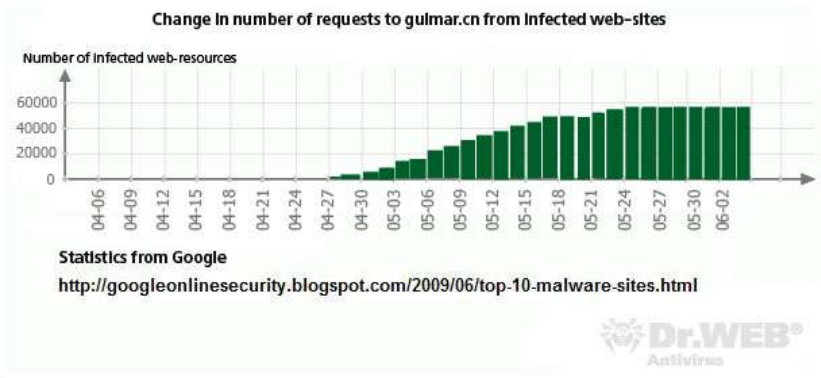
Nuss. Schon in der zweiten Jahreshälfte entdeckten Virenforscher von Doctor Web zwei neue Versionen des Schädlings.

Im April haben sich die Botnetzbetreiber den Micro-Blogging-Dienst Twitter zunutze gemacht. Auch im Mai wurde dieses Bootkit von bösartigen Malware-Websites verbreitet. Von besonderem Interesse ist die Geolokation, die hier von Cyberkriminellen eingesetzt wurde. Wenn zum Beispiel der Anwender nicht in den USA, sondern in Deutschland Zugriff auf eine bestimmte Webseite nahm, blieb der Angriff von BackDoor.MaosBoot aus.

JS.Gumblar

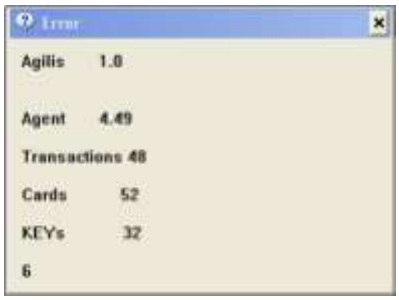
Früher bestanden Bot-Netze hauptsächlich aus infizierten Workstations. Nun ändert sich die Lage. Der Grund dafür: JS.Gumblar. Mit dieser Malware konnte ein Botnetz aus über 60.000 infizierten Webseiten aufgebaut werden. Jetzt, Mitte Mai rollte die Welle der Javascript-Malware an. Zu diesem Zeitpunkt begann auch der Streifzug von JS.Gumblar. Bösartige Szenarien von JS.Gumblar befielen viele Internetinhalte, denen bisher die Infizierung erspart blieb.

Somit gelang es den Cyberkriminellenein ein Bot-Netz aus Web-Inhalten zu kreieren, das Hunderttausende Besucher locken kann. Auf diese Art und Weise lässt sich Schadsoftware an Internetanwender weltweit verteilen.



Malware in Geldautomaten

Im März 2009 sorgte die Nachricht über Trojan.Skimer, der in Geldausgabeautomaten einiger russischer Banken entdeckt wurde, für Besorgnis.



Trojan.Skimer speichert Daten von Bankkarten sowie Daten über den Kontostand – wenn der Benutzer diese anfordert. Die Übeltäter können danach mit fingierten Karten die Konten ihrer Opfer komplett ausräumen. In der Zwischenzeit ist die Sicherheitslücke der GAA-Software, die Trojan.Skimer ausnutzte, geschlossen und der Geldautomatenhersteller verschickte an die betroffenen Banken entsprechende Handlungsanleitungen.

Erpresser-Programme

Auch der SMS-Betrug gewinnt immer mehr an Beliebtheit. Der Anwender wird dabei von Cyberkriminellen gezwungen, kostenpflichtige SMS zu versenden. Zu diesem Zweck kreieren Virenschreiber spezielle Erpresserprogramme, die wie Trojan.Winlock den Zugriff auf Windows blockieren, oder beispielsweise Pornbanner für Web-Browser (Trojan.Blackmailer) erstellen.

Der Anwender kann über ICQ-Chat, in sozialen Netzwerken sowie Spam-Mails kontaktiert werden. Die generelle Straflosigkeit der Kurznummerbesitzer und die vielfältigen Möglichkeiten, das ergaunerte Geld leicht hin und her zu verschieben, bieten den Übeltätern einen uneingeschränkten Spielraum.

Mac OS X

Seit Januar steigt das Interesse Cyberkrimineller an der Mac OS X-Plattform von Apple. Der Trojaner Mac.Iservice, der infizierte PCs ins Bot-Netz iBotnet eingliedert, trug somit wesentlich zum ersten Problemfall von MAC OS X bei.

Ende des Frühlings schlug die zweite Welle von Mac-Malware ein. Diesmal war es der Familienstrang von Mac.DnsChange, der sich via Links zum bösartigen Videospot verbreitete. Ein prominenter Verteilerkanal war auch der Micro-Blogging-Dienst Twitter.

Interessant ist dabei folgendes: Durch die Aktivierung des Schadcodes wurde nach User-Agent-Daten das Betriebssystem des Anwenders identifiziert, danach wurde die Schadsoftware entweder für Windows, oder Mac OS X geladen.

Mit der wachsenden Beliebtheit von Mac OS X, steigt auch das Interesse der Cyberkriminellen an dieser Plattform. Bisher sind die neuen Bedrohungen unter Windows und Mac OS X nicht vergleichbar. Zukünftig ist aber nicht ausgeschlossen, dass sich das Verhältnis ändert.

Exploits

Anfang Juli wurde eine ernsthafte Anfälligkeit in einer der Komponenten von Microsoft DirectX entdeckt. Diese Komponente kommt im MS Internet Explorer 6 und 7 zum Einsatz.

Bedroht waren alle Nutzer von Windows 2000/2003/XP (einschließlich aller letzten Updates und x64-Versionen dieser Betriebssysteme). Dabei wurde das Video in der ActiveX-Komponente msVidCtl.dll inkorrekt bearbeitet. Diese Vulnerability kann zur Verbreitung von Malware durch speziell angefertigte Websites genutzt werden.

Alle entdeckten Exploits, die diese Anfälligkeit ausnutzen, fallen unter Exploit.DirectShow.

Spam und E-Mail-Viren

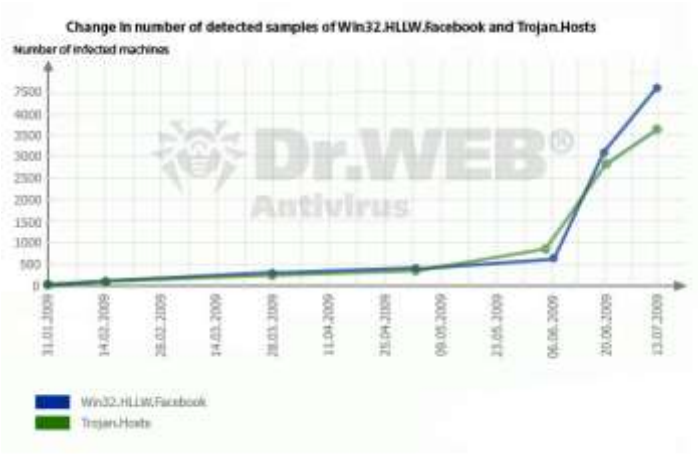
Spammer nutzen Ad-hoc-News in ihren Mails weiter aus. Bereits einige Stunden nach dem Tod von Michael Jackson wurde diese Nachricht in Spam-Mails und sozialen Netzwerken zynisch ausgeschlachtet. Auch die Themen rund um die politischen Entwicklungen im Iran fassten die Spamschreiber ins Auge.

Im Juni konnten die Virenforscher von Doctor Web einen Anstieg von Phishing-Mails verzeichnen. Insgesamt nahm der Versand von allgemeinen Spam-Mails sowie vermeintlichen Mails von Banken und Bezahlsystemen zu. Diese Mails haben auf Kunden amerikanischer (Bank of America, JPMorgan Chase Bank, Community State Bank) und australischer (St. George Bank) Banken sowie von PayPal, des Auktionshauses eBay und den Versandhändler Amazon abgezielt.

E-Mail-Viren kamen Anfang Juni ins Gerede. Ohne Übertreibung lässt sich sagen, dass der Monat Juni, im Rating bösartiger Mails mit Links zu Malware und infizierten Websites, die gesamte Tabelle anführte. So verbreitete sich in der Nacht vom 1. auf den 2 Juni Trojan.PWS.Panda.122, der sich als E-Card ausgab. Der Bösewicht scannt den Internetverkehr des Anwender-PCs und klaut Passwörter für Online-Banking-Services und Bezahlungsdienste.

Soziale Netzwerke

Im Frühling erhöhte sich auch die Virenaktivität in internationalen sozialen Netzwerken. Auf dem Vormarsch ist insbesondere die Familie Win32.HLLW.Facebook (bekannt auch als Koobface). Bereits in den Sommermonaten hat sich die Infizierung verdoppelt. Anfang Juli wurde die Dr.Web-Virendefinitionsdatei um neue Varianten von Win32.HLLW.Facebook, die in Facebook, MySpace und Twitter aktiv sind, erweitert.



Der Micro-Blogging-Dienst Twitter muss hier gesondert behandelt werden. Viele Cyber-Kriminelle haben sich diesen Malware-Verbreitungskanal ernsthaft vorgenommen. Die

Gesamtzahl von Spam-Mails mit Links zu Malware-Websites ist folglich angestiegen. Die Links sind dabei kaschiert und der Anwender kann auf den ersten Blick nicht erkennen, was sich schlussendlich hinter einem angeblich sicheren Link versteckt.

Ende Mai tauchte die Familie von JS.Twitter auf. Derzeitig sind es XSS-Würmer, die sich in sozialen Netzwerken verbreiten. Bei russischen sozialen Netzwerken lässt sich die Familie der Erpresser-Trojaner Trojan.Hosts hervorheben.

Zusammenfassung

Zur Sommerzeit hat sich die Zahl der Infizierungen durch Win32.HLLW.Shadow wesentlich verringert. Das Auftauchen dieser Malware im vergangenen Jahr spricht aber dafür, dass große Bedrohungen 2009 noch im Kommen sind. Im Frühjahr rückte JS.Gumblar in den Vordergrund, der eine riesige Zahl von Websites infizierte.

Die Cyber-Kriminellen bekunden auch ihr Interesse an der Mac OS-Plattform. Die Infizierungsmethoden gewinnen weitere neue Facetten: zunächst wird das Betriebssystem identifiziert und danach erfolgt ein gezielter Angriff.

Soziale Netzwerke geraten immer mehr ins Visier der Betrüger. Anfang Juni ist die Zahl von Win32.HLLW.Facebook explodiert. Das gestiegene Interesse der digitalen Räuber gilt auch Twitter.

Die zugenommenen Erpresser-Programme sprechen dafür, dass Cyber-Kriminelle schnell zu Geld kommen wollen.

Der besondere Trend 2009 ist die Malware für Geldautomaten.

Malware im ersten Halbjahr 2009 im E-Mail-Verkehr

01.01.2009 00:00 - 01.07.2009 00:00		
1	Win32.HLLM.Netsky.35328	27763294 (34.82%)
2	Win32.HLLM.MyDoom.33808	7635271 (9.58%)
3	Win32.HLLM.Beagle	7400948 (9.28%)
4	Trojan.DownLoad.36339	5816485 (7.29%)
5	Win32.HLLM.MyDoom.44	3053357 (3.83%)
6	Win32.HLLM.MyDoom.based	2738829 (3.43%)
7	Win32.HLLM.Netsky.based	2557757 (3.21%)
8	Win32.HLLM.Netsky.28672	2484754 (3.12%)
9	Win32.HLLM.Netsky	2252999 (2.83%)
10	Win32.HLLM.Perf	2012539 (2.52%)
11	Trojan.Botnetlog.9	1988614 (2.49%)
12	Trojan.MulDrop.19648	1705059 (2.14%)
13	Win32.HLLM.Beagle.32768	1500116 (1.88%)
14	Trojan.MulDrop.13408	1470765 (1.84%)
15	Win32.HLLM.MyDoom.49	1101971 (1.38%)
16	Trojan.PWS.Panda.114	1024091 (1.28%)
17	Win32.HLLM.Beagle.27136	999536 (1.25%)
18	Exploit.IFrame.43	917203 (1.15%)
19	Win32.HLLM.Beagle.pswzip	629979 (0.79%)
20	Exploit.IframeBO	573008 (0.72%)

Insgesamt geprüft: 353,878,451,872
Infiziert: 79,738,624 (0.0225%)

Malware im ersten Halbjahr 2009 auf PCs der Anwender

01.01.2009 00:00 - 01.07.2009 00:00		
1	Win32.HLLW.Gavir.ini	7954841 (7.76%)
2	Win32.HLLW.Shadow.based	4996557 (4.88%)
3	Trojan.DownLoad.36339	4610048 (4.50%)
4	DDoS.Kardraw	3730909 (3.64%)
5	Win32.HLLM.Beagle	3497040 (3.41%)
6	JS.Nimda	3026751 (2.95%)
7	Trojan.Botnetlog.9	2836732 (2.77%)

8	Win32.Virut.5	2811911 (2.74%)
9	Trojan.Starter.516	2510767 (2.45%)
10	W97M.Thus	2336936 (2.28%)
11	Win32.Virut.14	2162374 (2.11%)
12	Win32.HLLM.Netsky.35328	2141902 (2.09%)
13	Trojan.PWS.Panda.114	1988995 (1.94%)
14	Win32.Alman	1895646 (1.85%)
15	Trojan.DownLoader.42350	1876554 (1.83%)
16	Win32.HLLW.Autoruner.5555	1802659 (1.76%)
17	Trojan.MulDrop.16727	1635885 (1.60%)
18	Trojan.Blackmailer.1094	1594609 (1.56%)
19	VBS.Generic.548	1540792 (1.50%)
20	Win32.Sector.17	1200103 (1.17%)

Insgesamt geprüft: 730,787,813,411
Infiziert: 102,456,427 (0.0140%)

Über Doctor Web:

Das russische Unternehmen Doctor Web Ltd. ist einer der führenden Hersteller von Antivirus- und Anti-Spam-Lösungen mit Hauptsitz in Moskau. Doctor Web verfügt über eine 17-jährige Erfahrung in der Antimalwareentwicklung und beschäftigt 190 Mitarbeiter, davon 100 im Research & Development. Doctor Web ist nicht nur Pionier, sondern auch einer der wenigen Anbieter, die ihre Lösungen vollständig innerbetrieblich entwickeln. Das Unternehmen legt großen Wert auf die effektive Beseitigung von Kundenproblemen und bietet schnelle Antworten auf akute Virengefahren. Die umfangreiche Produktpalette von Doctor Web umfasst effiziente Lösungen zur Absicherung von einzelnen Arbeitsplätzen bis hin zu komplexen Netzwerken. Im deutschsprachigen Raum werden die Produkte von der Doctor Web Deutschland GmbH in Hanau vertrieben. Zu den nationalen und internationalen Kunden zählen neben privaten Anwendern namhafte börsennotierte Unternehmen wie Gazprom oder Arcelor Mittal sowie Bildungseinrichtungen und öffentliche Auftraggeber.