German
Data
Security

G Data
Malware-Report

Halbjahresbericht Januar-Juni 2009

Ralf Benzmüller & Werner Klier
G Data Security Labs

Geschützt. **Geschützter. G Data.**

Auf einen Blick

Zahlen und Daten

- Im ersten Halbjahr 2009 identifizierte G Data 663.952 neue Schädlinge. Das sind mehr als doppelt so viele, wie im gleichen Zeitraum ein Jahr zuvor. Gegenüber dem zweiten Halbjahr 2008 konnte lediglich eine leichte Steigerung um 15% erzielt werden. Die Zahl der aktiven Malwarefamilien dagegen sank um 7%.
- Die häufigsten Schädlingskategorien sind Trojanische Pferde, Downloader und Backdoors. Während die Trojanischen Pferde und Downloader ihre Position ausbauen konnten, ging der Anteil an Backdoors zurück. Rootkits etablieren sich weiter. Ihre Anzahl steigt gegenüber dem Vorjahreszeitraum um mehr als das 8-fache.
- Malware mit eigenen Verbreitungsroutinen macht lediglich 4,0% der Computerschädlinge aus.
- Zu den aktivsten Malwaretypen zählen Trojanische Pferde, Backdoors und Online-Game-Accountstehler. Ebenfalls deutlich zugelegt hat die Wurmfamilie „Autorun“. Ihre Zahl hat sich gegenüber dem ersten Halbjahr 2008 fast verfünffacht und ihr Anteil stieg auf 1,6%.
- 99,3% aller Malware des zweiten Halbjahrs läuft unter Windows. Die Konzentration auf den Betriebssystem-Marktführer setzt sich fort.
- Schadcode für mobile Plattformen hat es dieses Mal in die Top 5 der Plattformen geschafft. Mit 106 Schädlingen bleibt deren Anteil aber weiterhin auf niedrigstem Niveau.
- Auch Nutzer von MacOS X werden von Malware attackiert. Die Anzahl der neuen Schädlinge für MacOSX beträgt 15. Ein erstes Botnetz aus Apple-Rechnern wurde im April entdeckt

Ereignisse und Trends

- Soziale Netzwerke werden immer häufiger zur Verbreitung von Spam und Malware genutzt.
- Conficker entwickelt sich zum Dauerbrenner. Er infizierte mehrere Millionen PCs und machte zum 1. April mit einer neuen Update-Routine von sich reden. Danach wurde es still.

Prognosen

- Immer mehr Schadcode verlagert sich ins Internet. Die Infektionsmethoden werden immer ausgereifter.
- Die Malware-Flut wird in den kommenden Monaten weiter ansteigen, aber mit geringeren Steigerungsraten und getragen von noch weniger Malwarefamilien.
- Nutzer von MacOSX und Smartphones geraten verstärkt ins Visier von Malwareautoren.

Inhalt

Malware: Zahlen und Daten

Die Malware-Flut steigt weiter - aber nicht mehr so stark

In den vergangenen Jahren ist die Anzahl neuer Schädlinge kontinuierlich angestiegen. Mit immer höheren Wachstumsraten wurden immer neue Rekorde erreicht. Auch im ersten Halbjahr 2009 ist die Anzahl der Computerschädlinge wieder gestiegen. Gegenüber dem gleichen Vorjahreszeitraum hat sich die Zahl auf 663.952 Schädlinge mehr als verdoppelt. Aber wie im letzten G Data Malware-Report bereits angekündigt hat sich die Wachstumsrate reduziert. Im Vergleich zum zweiten Halbjahr 2008 ist die Anzahl der Schädlinge um lediglich 15% angestiegen.

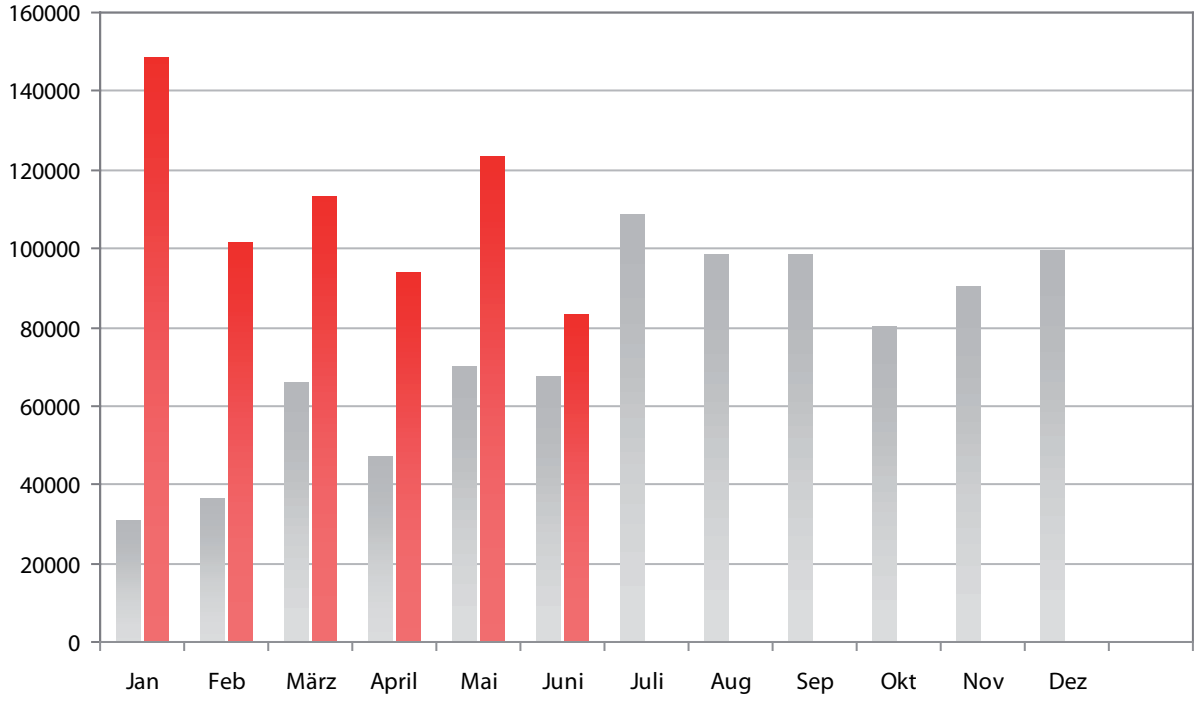


Diagramm 1: Anzahl neuer Malware pro Monat für 2008 (grau) und 2009 (rot).

Malware-Kategorien

Ein Blick auf die Veränderungen bei den einzelnen Kategorien von Malware kann Erklärungen für diesen Rückgang liefern. Während Backdoors, Adware und Spyware unter dem Durchschnitt bleiben, übertrifft die Menge der Rootkits und der Trojanischen Pferde die durchschnittliche Zunahme deutlich. Auch die Zahl der Downloader und Dropper liegt über dem Durchschnitt.

Backdoors werden dazu benötigt Zombie-Rechner in ein Botnetz zu integrieren und fernsteuerbar zu machen. Ein Rückgang in diesem Bereich ist ein Hinweis dafür, dass der Ausbau der Botnetze an Wichtigkeit verloren hat. Der starke Anstieg der Rootkits deutet darauf hin, dass immer mehr Schädlinge (auch Backdoors) vor dem Virenschutz und neugierigen Augen versteckt werden. Offenbar reichen die verfügbaren Kapazitäten aus, um die Nachfrage nach Botnetz-Aktivitäten wie Spamversand und Überlastangriffe durchzuführen. Auch der Adware-Markt scheint auf hohem Niveau zu stagnieren. Möglicherweise greifen hier Awareness-Kampagnen. Aber auch die in der mittlerweile anhaltenden Wirtschaftkrise eingeschränkten Werbebudgets tragen ihren Teil dazu bei, dass auch in der eCrime-Ökonomie kleinere Brötchen gebacken werden müssen.

Die Anzahl der Spyware hat ein wenig abgenommen. Bei genauerem Hinsehen stellt sich heraus, dass sich die Zahl der Keylogger verdoppelt hat, während Banking-Trojaner und Datendiebe für Passwörter oder Online-Spiele um jeweils ca. 30% zurückgegangen sind. Die gestiegenen Sicherheitsvorkehrungen bei Banken und Online-Spiele-Betreibern lassen sich mit einfachen Mitteln nicht mehr umgehen. Im Bereich des Datendiebstahls geht der Trend zu immer universelleren und leistungsfähigeren Schädlingen.

Kategorie	# 2009 H1	Anteil	# 2008 H2	Anteil	Diff 2008H1 2008H2	# 2008 H1	Anteil	Diff 2008H1 2009H1
Trojan. Pferde	221.610	33,6%	155.167	26,9%	143%	52.087	16,4%	425%
Backdoors	104.224	15,7%	125.086	21,7%	83%	75.027	23,6%	139%
Downloader/ Dropper	147.942	22,1%	115.358	20,0%	128%	64.482	20,3%	229%
Spyware	97.011	14,6%	96.081	16,7%	101%	58.872	18,5%	165%
Adware	34.813	5,3%	40.680	7,1%	86%	32.068	10,1%	109%
Würmer	26.542	4,0%	17.504	3,0%	152%	10.227	3,2%	260%
Tools	11.413	1,6%	7.727	1,3%	148%	12.203	3,8%	94%
Rootkits	12.229	1,9%	6.959	1,2%	176%	1.425	0,4%	858%
Exploits	2.279	0,3%	1.841	0,3%	124%	1.613	0,5%	141%
Dialer	1.153	0,2%	1013	0,2%	114%	4.760	1,5%	24%
Viren	143	0,0%	167	0,0%	86%	327	0,1%	44%
Sonstige	4.593	0,7%	8.419	1,5%	55%	5.170	1,6%	89%
Gesamt	663.952	100,0%	576.002	100,0%	115%	318248	100,0%	209%

Tabelle 1: Anzahl sowie Anteil neuer Malwarekategorien im ersten Halbjahr 2008 und 2009 mitsamt Veränderung

Die Tabelle 1 zeigt auch, dass die Anzahl der Dialer auf knapp ein Viertel des Vorjahresvolumens gesunken ist. Das Geschäftsmodell Dialer läuft offenbar aus. Auch die Zahl der klassischen Viren (d.h. Dateiinfektoren) hat gegenüber dem gleichen Vorjahreszeitraum deutlich abgenommen. Dieser Verbreitungsweg bildet eher die Ausnahme. Die Würmer - darunter auch die große Gruppe der Autorun-Infektoren - konnten ihren Anteil auf 4.0% steigern. Ihre Anzahl ist gegenüber dem 1. Halbjahr 2008 um das 2,6-fache und gegenüber dem 2. Halbjahr 2008 um das 1,5-fache gestiegen.

Familienbande

Anhand der Funktionen und der Eigenschaften des verwendeten Codes werden Computerschädlinge in Familien untergliedert. Seit Jahren ist die Anzahl der Virenfamilien rückläufig. Im ersten Halbjahr 2008 waren es noch 2395 und im zweiten 2094. Im ersten Halbjahr 2009 wurden 1948 verschiedene Vertreter von Virenfamilien gezählt. Das heißt: Die erneut gestiegene Zahl an Schädlingen basiert auf einer gesunkenen Ziffer an Familien. Hier zeigt sich eine Konzentration des Marktes.

	# 2009 H1	Virenfamilie	# 2008 H2	Virenfamilie	# 2008 H1	Virenfamilie
1	45.407	Monder	45.407	Hupigon	32.383	Hupigon
2	35.361	Hupigon	35.361	OnlineGames	19.415	OnLineGames
3	20.708	Genome	20.708	Monder	13.922	Virtumonde
4	18.718	Buzus	18.718	MonderB	11.933	Magania
5	15.937	OnlineGames	15.937	Cinmus	7.370	FenomenGame
6	13.133	Fraudload	13.133	Buzus	7.151	Buzus
7	13.104	Bifrose	13.104	Magania	6.779	Zlob
8	12.805	Poison	12.805	PcClient	6.247	Cinmus
9	11.530	Magania	11.530	Zlob	6.194	Banload
10	10.412	Inject	10.412	Virtumonde	5.433	Bifrose

Tabelle 2: Top 10 der aktivsten Virenfamilien im ersten Halbjahr 2009 und 2008

Während manche Familien es lediglich auf eine Hand voll Varianten bringen, sind andere besonders produktiv. Einige davon sind schon seit Jahren in den Top 10 vertreten. Dazu gehören die Backdoors der Hupigon- und der Bifrose-Familie, die ihren Spitzenplatz verloren haben, die Datenstehler für Online-Spiele aus den Familien OnlineGames und Magania sowie die Trojanischen Pferde der Familie Buzus. Neuer Spitzenreiter sind die Adware/Scareware-Trojaner von Monder, die in die Fußstapfen von Virtumonde treten. Zusammen mit dem Neueinsteiger Fraudload zeigen sie, wie populär Scareware mit imitierten Virenschutzlösungen bei Cyber-Kriminellen geworden ist. Neu in den Top 10 sind außerdem die Familien Genome, Poison und Inject.

Platz 1: Monder
Die unzähligen Monder-Varianten sind Trojanische Pferde, die auf dem infizierten System Sicherheitseinstellungen manipulieren und es auf diese Weise anfällig für weitere Attacken machen können. Zusätzlich kann eine Infektion mit Adware folgen, die unerwünschte Werbeeinblendungen auf dem infizierten System anzeigt, insbesondere für gefälschte Sicherheitssoftware. Dem Opfer wird suggeriert, dass das System auf Infektionen untersucht wird. Um diese angeblichen Infektionen zu beseitigen, wird das Opfer gedrängt, die „Vollversion" zu erwerben und per Kreditkarte (!!) zu bezahlen. Einige Varianten laden weitere Schadsoftware herunter und übermitteln an den Angreifer Informationen über das Surfverhalten des Opfers, ohne den Anwender hierüber zu informieren.

Platz 2: Hupigon
Die Backdoor Hupigon ermöglicht dem Angreifer unter anderem die Fernsteuerung des Rechners, das Mitschneiden von Tastatureingaben, Zugriff auf das Dateisystem und das Einschalten der Webcam.

Platz 3: Genome
Die Trojaner der Genome-Familie vereinen Funktionalitäten wie Downloader, Keylogger oder Dateiverschlüsselung.

Platz 4: Buzus
Trojanische Pferde der Buzus-Familie durchsuchen infizierte Systeme ihrer Opfer nach persönlichen Daten (Kreditkarten, Online-Banking, E-Mail- und FTP-Zugänge), die an den Angreifer übertragen werden. Darüber hinaus wird versucht, Sicherheitseinstellungen des Computers herabzusetzen und das System des Opfers dadurch zusätzlich verwundbar zu machen.

Platz 5: 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 Angriffe zielen überwiegend auf Games, die in Asien populär sind.

Platz 6: Fraudload
Die Fraudload-Familie umfasst unzählige Varianten sogenannter Scareware-Programme, die sich dem Anwender als Sicherheits-Software oder System-Tool präsentieren. Dem Opfer wird suggeriert, dass das System auf Infektionen untersucht wird. Um diese angeblichen Infektionen zu beseitigen, wird das Opfer gedrängt, die „Vollversion" zu erwerben und dazu seine Kreditkarteninformationen auf einer speziellen Webseite preiszugeben. Die Infektion erfolgt in der Regel über ungepatchte Sicherheitslücken im Betriebssystem oder über verwundbare Anwendungssoftware des Opfers. Es existieren aber auch Angriffsmethoden, bei denen das Opfer auf Seiten gelockt wird, auf denen vermeintlich Videos mit erotischem oder tagesaktuellem Inhalt zu sehen sind. Um die angeblichen Videos betrachten zu können, soll das Opfer einen speziellen Video-Codec installieren, in dem die Schadsoftware versteckt ist.

Platz 7: Bifrose
Die Backdoor Bifrose ermöglicht Angreifern den Zugriff auf infizierte Rechner und verbindet sich mit einem IRC-Server. Von dort nimmt der Schädling Kommandos des Angreifers entgegen.

Platz 8: Poison
Die Poison-Backdoor ermöglicht Angreifern den unauthorisierten Fernzugriff auf das System des Opfers, welches anschließend z.B. für verteilte Überlastattacken (DDoS) missbraucht werden kann.

Platz 9: Magania
Trojanische Pferde der aus China stammenden Magania-Familie haben sich auf den Diebstahl von Gaming-Accountdaten der taiwanesischen Softwareschmiede Gamania spezialisiert. In der Regel werden Magania-Exemplare per Mail verteilt, in der sich ein mehrfach gepacktes, verschachteltes RAR-Archiv befindet. Beim Ausführen der Schadsoftware wird zur Ablenkung zunächst ein Bild angezeigt, während im Hintergrund weitere Dateien im System hinterlegt werden. Zudem klinkt sich Magania per DLL in den Internet Explorer ein und kann somit den Web-Verkehr mitlesen.

Platz 10: Inject
Die Inject-Familie umfasst eine Vielzahl von Trojanischen Pferden, die sich in laufende Prozesse einklinken und hierdurch die Kontrolle über den jeweiligen Prozess übernehmen können. Dies ermöglicht es dem Angreifer, die befallenen Prozesse nach Belieben in bösartiger Absicht zu manipulieren.

Die aktivste **Wurmfamilie** ist „Autorun“ mit 9.689 Varianten und einem Anteil von 1,6%. Vertreter dieser Familie nutzen den Mechanismus, der beim Einlegen von CDs/DVDs oder beim Anschließen von USB-Datenträgern automatisch Dateien ausführt. Dazu kopiert er sich auf den Datenträger und erzeugt eine passende Datei namens autorun.inf. Angesichts der weiten Verbreitung dieses Schädlings ist es angebracht den Autorun-Mechanismus von Windows zu deaktivieren. Damit das auch wirklich funktioniert, hat Microsoft ein eigenes Patch erstellt.

Die häufigsten **Exploits** betrafen die WMF-Sicherheitslücke und Schwachstellen in PDFs. Die Anzahl der schädlichen PDF-Dateien hat in den letzten Monaten deutlich zugenommen. Dabei werden nicht nur die Sicherheitslücken ausgenutzt. Auch die Möglichkeit in PDFs JavaScript-Code auszuführen erfreut sich wachsender Beliebtheit unter Malware-Autoren.

Plattformen

Auch im ersten Halbjahr 2009 konzentrieren sich Malware-Autoren auf Windows-Rechner als Angriffsziel. Mit 99,3% ist der Anteil an Windows-Malware erneut gestiegen. Schadsoftware für andere Betriebssysteme ist äußerst selten. Für Unix-basierte Systeme erschienen 66 Schädlinge (im Vergleich zu 16 im zweiten Halbjahr 2009) und für Apples OSX wurden 15 neue Schädlinge gefunden. Im zweiten Halbjahr 2008 waren es 6. Auch wenn hier eine steigende Tendenz zu Malware für andere Betriebssysteme auszumachen ist, so ist deren Anzahl im Vergleich zu der Flut an Windows-Malware verschwindend gering.

	Plattform	#2009 H1	% 2009 H1	#2008 H2	% 2008 H2	#2008 H1	Anteil
1	Win32	659.009	99,3%	571.568	99,2%	312.656	98,2%
2	WebScripts	3.301	0,5%	2.961	0,5%	3.849	1,4%
3	Scripts	924	0,1%	1.062	0,2%	1.155	0,3%
4	MSIL	365	0,1%	318	0,1%	252	0,1%
5	Mobile	106	0,0%	70	0,0%	41	0,0%

Tabelle 3: Top 5 Plattformen 2008 und im ersten Halbjahr 2009. Unter WebScripts ist Malware zusammengefasst, die auf JavaScript, HTML, Flash/Shockwave, PHP oder ASP basiert und üblicherweise Schwachstellen per Browser nutzt. „Scripts“ sind Batch- beziehungsweise 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. Unter Mobile ist Malware für J2ME, Symbian und Windows CE zusammengefasst.

Die Anzahl an neuer Malware für Smartphones und Mobilrechner ist um ca. die Hälfte angestiegen und Schädlinge für mobile Endgeräte haben es wieder in die Top 5 geschafft. Insgesamt sind 106 neue Schädlinge aufgetaucht. Ca. 90 dieser Schädlinge haben keine eigene Verbreitungsroutine und werden zum Versand von SMS an vorwiegend russische und chinesische Telefonkunden verwendet. Nur die Familie Yxe verbreitet sich selbständig per SMS mit Link auf eine Webseite. Die Datei, die dort zum Download angeboten wird, ist von Symbian signiert. Dadurch wird die nach wie vor notwendige Benutzeraktion auf einen Klick reduziert.

Ausblick 2009

Mit Malware wird auch in den kommenden Monaten sehr viel Geld verdient. Die eCrime-Ökonomie ist fest etabliert und die bewährten Geschäftsmodelle um Spam, Spyware und Adware werden weiterhin für gefüllte Kassen bei den Schreibern, Verbreitern und Nutzern von Malware sorgen. Daran werden auch gelegentliche Erfolge der Ermittlungsbehörden nichts ändern. Nutzer von Windows werden auch weiterhin im Visier der Cyber-Kriminellen sein.

Die Malware-Flut wird weiter wachsen. Allerdings ist absehbar, dass die steigende Anzahl von immer weniger Familien abgedeckt wird. Die Steigerungsraten werden nicht mehr so deutlich ausfallen wie in den vergangenen Jahren.

Angesichts der Professionalität der Schattenwirtschaft ist es nicht verwunderlich, dass Sicherheitslücken im Betriebssystem und in populären Anwendungen bereits wenige Tage nach deren Veröffentlichung auch von Malware genutzt werden. Binnen kürzester Zeit stehen sie auch für Laien über einfach zu bedienende Tools zur Erstellung von Malware zur Verfügung. Das schwächste Glied in der Kette ist momentan der Browser und seine Komponenten. Hier werden die meisten Sicherheitslücken gefunden und genutzt. Wer seinen Rechner nicht auf dem neuesten Stand hält, bietet Malware-Angriffen eine breitere Angriffsfläche.

Aber auch auf anderen Plattformen wird weiterhin experimentiert. Die Anzahl der Schädlinge für Apple-, Unix- und Mobilrechner wird steigen. Allerdings ist eine massenhafte Nutzung nicht zu erwarten.

Da mittlerweile viele Einfallstore für Malware durch Sicherheitstechnologien geschützt sind, weichen die Angreifer auf schwächer geschützte Bereiche aus. Hier bieten Webseiten mit ihren zahlreichen Anwendungen momentan die größten Erfolgschancen. Daher ist zu erwarten, dass dieser Bereich auch in den kommenden Monaten mit immer neuen und gewiefteren Angriffsszenarien genutzt wird. Dabei könnten bislang unterschätzte Medien wie Flash oder PDF verstärkt genutzt werden. Auch die Trickkiste der Betrüger, mit denen Internetnutzer zum Besuch einer Webseite oder zum Ausführen von Dateien verleitet werden, wird sicher Zuwachs bekommen. Insbesondere in Sozialen Netzwerken rechnen wir mit neuen Täuschungsmanövern. Twitter bietet hier derzeit die meisten Möglichkeiten.

Prognosen

Kategorie	Trend
Trojan. Pferde	↗
Backdoors	→
Downloader/ Dropper	→
Spyware	→
Adware	→
Viren/Würmer	↘
Tools	↗

Kategorie	Trend
Rootkits	↗
Exploits	↗
Win32	↗
WebScripts	↑
Scripts	→
MSIL	→
Mobile	↑

Ereignisse und Trends des ersten Halbjahrs 2009

Die wichtigen Ereignisse rund um Malware stellen wir in der zeitlichen Reihenfolge dar. Am meisten stechen die Ereignisse um Conficker hervor, der in den ersten Monaten des Jahres für viel Aufsehen sorgte. Auffallend sind aber auch die vielen Vorfälle in beliebten Sozialen Netzwerken wie Twitter, LinkedIn, MySpace und Facebook. Mittlerweile nehmen Malware-Designer solche Trends sehr schnell wahr und nutzen die sich bietenden Gelegenheiten. Abgesehen von den einzelnen Vorfällen zeigen aber auch andere Trends, dass Soziale Netzwerke an Attraktivität gewinnen. War Phishing noch vor Jahresfrist fast ausschließlich auf Banken und eBay beschränkt, so sind im letzten halben Jahr Google und die Sozialen Netzwerke Facebook, Sulake und MySpace zu ständigen Vertretern in der Phishtank Top 10 geworden. Soziale Netzwerke dienen Cyber-Kriminellen schon seit geraumer Zeit als Informationsquelle zur Vorbereitung von gezielten Angriffen und personalisierter Spam. Soziale Netzwerke werden immer beliebter - auch bei Malware-Autoren.

Das belegt insbesondere die Entwicklung des Wurms **Koobface**. War er anfangs - wie der Name ja andeutet - auf Facebook und kurz darauf auf MySpace als Verbreitungsplattform konzentriert, so wurde die Liste in den letzten Monaten um Soziale Netzwerke wie hi5.com, friendster.com, myyearbook.com, bebo.com, tagged.com, netlog.com, fubar.com und livejournal.com erweitert. Die Links, die dort hinterlegt werden, zeigen auf Webseiten, wo die bewährten Betrugsmuster „Schummel-AntiVirus“ oder „Codec/Flash-Download“ probiert werden. Aber Koobface expandiert auch in der Anzahl, wie die folgende Tabelle zeigt. Im Juni hat sich die Anzahl der Varianten fast verzehnfacht.

Monat	Jan 09	Feb 09	Mrz 09	Apr 09	Mai 09	Jun 09
# Varianten Koobface	18	14	23	50	56	541

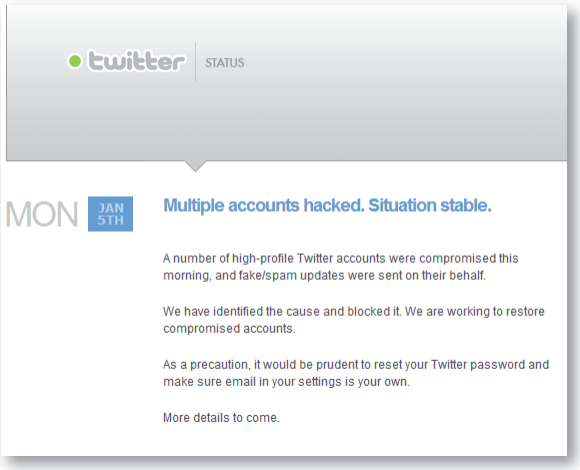
Tabelle 4: Anzahl der Koobface-Varianten im ersten Halbjahr 2009

In den kommenden Monaten rechnen wir mit mehr Malware in Sozialen Netzwerken. Mit den wachsenden Nutzerzahlen steigt auch die Attraktivität für Malware-Verbreiter.

Januar 2009

05.01. Nutzer des Micro-Blogs Twitter werden durch gezielte Kurznachrichten auf eine gefälschte Login-Seite des Dienstes gelockt, um Zugangsdaten für künftige Spam-Kampagnen zu stehlen.

06.01. **Twitter** warnt: “Multiple accounts hacked. Situation stable”. Betroffen sind unter anderem die Accounts von Britney Spears und Barack Obama. Im Namen der Opfer werden teils anzügliche Nachrichten verschickt



07.01. Auf der Social-Networking-Seite **LinkedIn** werden gefälschte Promi-Profile angelegt. Sie enthalten Links, die auf gefälschte Virenscanner oder eine mit einem Trojanischen Pferd verseuchte Version des Windows Media Players zeigen. Prominente Opfer: Victoria Beckham, Beyoncé Knowles, Salma Hayek u.v.m.

08.01. Bei der Landesregierung des österreichischen Bundeslandes Kärnten fallen 3000 Rechner durch Befall mit dem **Conficker**-Wurm aus. Grund: Das von Microsoft bereits im Oktober 2008 veröffentlichte Sicherheitsupdate, das eine von Conficker ausgenutzte Sicherheitslücke schließen soll, ist bisher nicht eingespielt worden.

12.01. **Conficker** schlägt in Kärnten abermals zu, diesmal in Spitälern der Kärntner Krankenanstaltengesellschaft KABEG. Wieder sind rund 3000 Rechner betroffen.

14.01. Schätzungen gehen von bereits 2.5 Mio. **Conficker**-Infektionen aus. Erstmals wird bekannt, dass Conficker mittels eines speziellen Algorithmus permanent Domainnamen generiert, zu denen nach dem Zufallsprinzip Kontakt aufgenommen wird. Ziel: Die Angreifer haben viele der Zufallsdomains vorab registriert und können diese dazu nutzen, weiteren Schadcode nachzuladen oder infizierte Rechner mit weiteren Instruktionen zu versorgen.

21.01. Die **Conficker**-Epidemie greift unvermindert um sich: Weite Teile der britischen Streitkräfte sind betroffen.

23.01. Eine trojanisierte Kopie von Apples Layout- und Präsentationssoftware **iWork 09** kursiert im BitTorrent-Netzwerk. Etwa 20.000 Anwender sollen die seit Anfang des Monats verbreitete Kopie bereits heruntergeladen haben.

25.01. Die Job-Börse **Monster.com** teilt mit, Opfer eines Datendiebstahls geworden zu sein. Durch „unerlaubte Zugriffe" auf die Datenbank des Unternehmens seien Zugangsdaten, Namen, Telefonnummern, E-Mail-Adressen und einige demografische Daten erbeutet worden.

Februar 2009

01.02. Aufgrund einer Sicherheitslücke lässt sich in der Beta-Version von **Windows 7** mittels eines einfachen Skripts die Benutzerkontensteuerung (UAC) außer Gefecht setzen, wodurch Angreifer dem Betriebssystem unbemerkt weitere Schadsoftware unterschieben könnten.

02.02. Angreifer manipulieren den Webauftritt des **Hamburger Abendblatts**, um Besucher der Seiten mit Schadsoftware zu infizieren.

04.02. Über eine gefälschte Login-Seite des zu RTL gehörenden Sozialen Netzwerks **werkennt-wen.de** werden Zugangsdaten von dessen Benutzern ausgespäht.

08.02. Mittels einer gezielten verteilten **Denial-of-Service**-Attacke werden diverse Security-Webseiten wie Metasploit, Milw0rm oder Packetstorm zeitweise lahmgelegt.

10.02. Nur zwei Tage nach der ersten Attacke steht die Internetpräsenz des Projekts **Metasploit** erneut im Fadenkreuz einer DDoS-Attacke. Die Angreifer variieren die Technik des Angriffs mehrfach.

11.02. Über eine tags zuvor bekannt gewordene Sicherheitslücke im Content-Management-System **Typo 3** werden diverse deutschsprachige Webseiten, die das entsprechende Sicherheits-Update noch nicht eingespielt haben, manipuliert. Betroffen sind z.B. die Webseiten des **FC Schalke 04**, auf denen über die Entlassung von Kevin Kuranyi berichtet wird, oder die Internetpräsenz von Wolfgang Schäuble, auf der ein Link zum Thema Vorratsdatenspeicherung platziert wird.

12.02. **Microsoft** setzt ein **Kopfgeld** von 250.000 Dollar für die Verhaftung und Bestrafung der Urheber des **Conficker**-Wurms aus. Gleichzeitig kündigt der Software-Hersteller an, zur Eingrenzung der fortschreitenden Infektion eng mit der ICANN und den Betreibern zentraler DNS-Server zusammenzuarbeiten.

14.02. Mehrere hundert Rechner der Bundeswehr werden von **Conficker** befallen.

17.02. Aufgrund einer Router-Fehlkonfiguration bei einem tschechischen Internet-Provider wird die Stabilität der Datenübertragung in einigen Teilen des globalen Internets stark beeinträchtigt.

23.02. Malware-Forscher analysieren die Varianten B sowie B++ des Conficker-Wurms und stellen fest, dass diese durch ihren modularen Aufbau noch weitaus flexibler agieren können als die ursprüngliche Variante A.

25.02. Mithilfe präparierter Flash-Banner verteilen Angreifer über die Webseite des Online-Magazins eWeek und weitere Online-Präsenzen des Ziff-Davis-Netzwerkes manipulierte PDF-Dokumente, die eine gefälschte Antivirus-Software auf den Rechnern der Opfer installieren.

März 2009

01.03. Malware-Forscher entziffern den Algorithmus, den **Conficker** nutzt, um Domainnamen eines Control-Servers zu generieren. Er erzeugt auch Namen, die bereits verwendet werden. Im Laufe des Monats März sollen die legitimen Domains jogli.com (Musik-Suchmaschine), wnsux.com (Fluglinie Southwest-Airlines), qhflh.com (chinesisches Frauennetzwerk) und praat.org (Audio-Analyse) durch Verbindungsversuche von Conficker-Rechnern gestört werden.

04.03. Ein Team aus Spezialisten des LKA Baden-Württemberg legt die illegale Handelsplattform **codesoft.cc** still, auf der Trojanische Pferde und illegale Informationen über das Stehlen von Daten und Fälschen von Kreditkarten zum Kauf angeboten werden.

09.03. **Conficker** nutzt einen neuen Algorithmus, der statt wie bisher 250 nun 50.000 Domains pro Tag berechnet. Darüber hinaus werden auf befallenen Rechnern Prozesse beendet, die bestimmte Zeichenketten beinhalten, die mit speziellen gegen den Wurm gerichteten Analysetools in Zusammenhang stehen. Der Schädling setzt sich somit aktiv gegen Maßnahmen zur Eindämmung der Epidemie zur Wehr.

12.03. Die britische **BBC** übernimmt im Zuge von Recherchen die Kontrolle über ein **Botnetz** mit rund 22.000 Rechnern. Da auf die Übernahme Vorwürfe gegen die BBC folgen, lässt diese verlauten, dass die Recherche im öffentlichen Interesse stehe und sich somit mit den Richtlinien der britischen Medienaufsichtsbehörde OFCOM decke. Die Frage, ob für die Übernahme des Botnetzes Geld geflossen sei, bleibt seitens der BBC unbeantwortet.

17.03. Unter Verwendung der authentisch wirkenden Domain dhl-packstation.info locken Internet-Kriminelle im Zuge einer Phishing-Kampagne **Packstation**-Benutzer auf eine gefälschte Login-Seite, um deren Zugangsdaten auszuspähen.

23.03. **DSL-Router** vom Typ Netcomm NB5 sind aufgrund einer veralteten Firmware per Web-Interface und SSH-Zugang aus dem Internet ohne Passwort manipulierbar und bilden ein Botnetz namens **Psybot**, dessen Größe auf 80.000 bis 100.000 infizierte Router geschätzt wird.

30.03. Nach Angaben von Experten wird **Conficker** am 1. April beginnen, die unzähligen, von seinem Algorithmus generierten Domains nach Updates zu durchsuchen. Was im Zuge der Kontaktaufnahme genau passieren wird, kann zu diesem Zeitpunkt niemand sagen.

31.03. Das breite Medieninteresse an **Conficker** ruft Trittbrettfahrer auf den Plan, die mittels gezielter Manipulationen Webseiten mit angeblichen Desinfektions-Tools in den Trefferlisten der Suchmaschine Google positionieren. In Wirklichkeit handelt es sich bei den angeblich hilfreichen Tools um **Scareware**, also gefälschte Antiviren-Software, die dem Opfer eine Infektion des Rechners suggeriert und ihm Kreditkarteninformationen entlocken will.

April 2009

01.04. Die erwarteten Update-Versuche von **Conficker** laufen zunächst ins Leere. Offensichtlich nehmen infizierte Systeme zwar wie im Vorfeld erwartet Kontakt zu bestimmten Domains auf. Vermutlich liegt zu diesem Zeitpunkt dort aber noch kein Update bereit.

09.04. Entgegen den ursprünglichen Erwartungen lädt **Conficker** Updates nicht über die von einem Algorithmus generierten Domainnamen nach. Stattdessen greift er auf einen alternativen P2P-Mechanismus zurück und kommuniziert darüber direkt mit anderen infizierten Systemen. Die neue Variante blockiert gezielt den Zugang zu Webseiten von Antivirenherstellern, um den Zugriff auf spezielle Removal-Tools zu erschweren.

12.04. **Conficker** lädt von einem ukrainischen Server die Scareware „SpywareProtect2009“ nach, die auf den Systemen der Opfer gefälschte Virenwarnungen ausgibt. Für die Entfernung der gemeldeten (und de facto nicht vorhandenen) Schädlinge soll der geplagte Anwender 49.95 Dollar bezahlen.

18.04. Sicherheits-Experten entdecken Anzeichen für ein erstes **Botnetz aus Apple-Rechnern**. Offensichtlich besteht ein Zusammenhang zu den Anfang des Jahres in der Tauschbörse BitTorent aufgetauchten trojanisierten Versionen von Apples iWork 09. Außerdem soll eine ebenfalls trojanisierte Version von Adobe Photoshop CS4 kursieren.

22.04. Das **größte jemals entdeckte Botnetz** der Welt wird aufgespürt. Es enthält fast zwei Millionen infizierte Zombie-PCs. Betreiber ist vermutlich eine aus nur sechs Personen bestehende Bande, die in der Ukraine den zugehörigen Command & Control-Server betreibt.

23.04. Im russischen Teil des World Wide Web taucht ein **Trojanisches Pferd** auf, das Anwender aus ihrem Windows-PC aussperrt und zur Freischaltung ein **Lösegeld** fordert. Betroffene Anwender sollen eine SMS an eine besonders teure Premium-Nummer schicken und daraufhin einen Freischalt-Code erhalten.

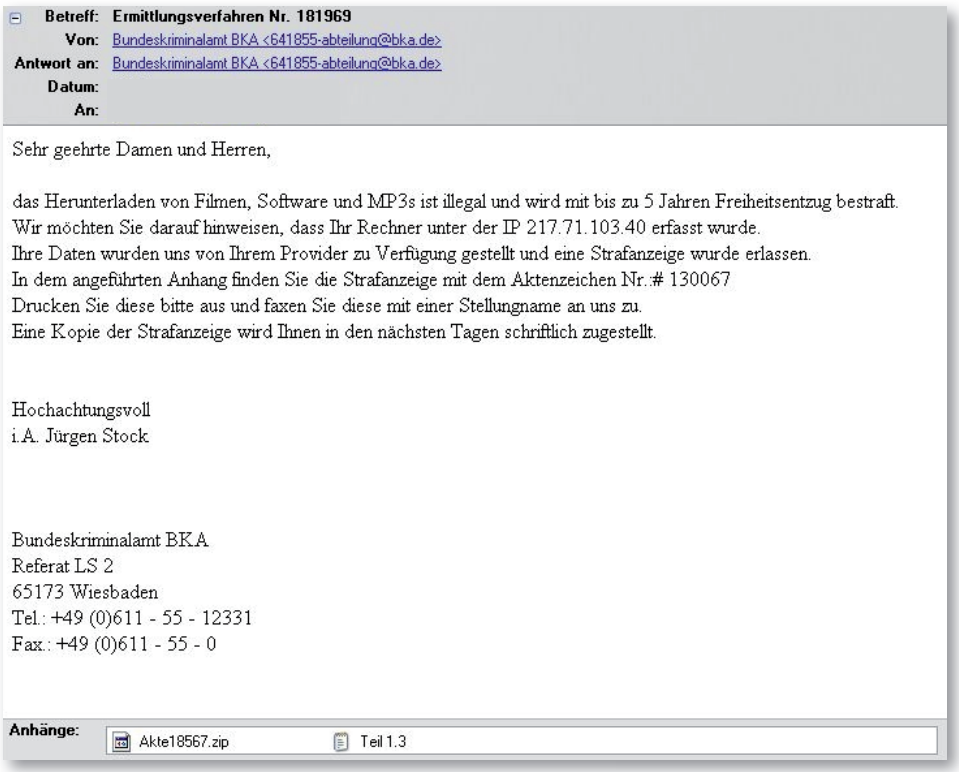
Mai 2009

07.05. Eine Studie des Telekommunikationskonzerns BT deckt auf, dass gebrauchte **Festplatten** vor ihrem Weiterverkauf oft nur unzureichend gelöscht werden und mitunter äußerst sensible Daten enthalten können. Bei einem Testkauf von 300 gebrauchten Festplatten fanden sich unter anderem vertrauliche Details über Testreihen eines US-amerikanischen Raketenabwehrsystems sowie Blaupausen des US-Rüstungskonzerns Lockheed Martin.

08.05. Laut einem Bericht der US-Flugaufsichtsbehörde FAA seien in den vergangenen Jahren mehrfach **Hacker in Systeme der Flugüberwachung eingedrungen**. Das Ausmaß reiche vom illegalen Zugriff auf fast 50.000 persönliche Datensätze von FAA-Angestellten bis hin zu der Möglichkeit, die Stromversorgung wichtiger Server abzuschalten.

09.05. Gefälschte Installationspakete eines angeblichen Release Candidate von **Windows 7** enthalten ein **Trojanisches Pferd**, das während der Setup-Ausführung aktiviert wird.

24.05. Das **Bundeskriminalamt** warnt vor gefälschten Mails, die in dessen Namen verschickt werden und die Empfänger zur Zahlung eines Bußgeldes infolge einer angeblich durch das BKA erstellten Strafanzeige wegen illegalen Herunterladens von Filmen, Software und MP3-Dateien auffordern.



Betreff: Ermittlungsverfahren Nr. 181969
Von: Bundeskriminalamt BKA <641855-abteilung@bka.de>
Antwort an: Bundeskriminalamt BKA <641855-abteilung@bka.de>
Datum:
An:

Sehr geehrte Damen und Herren,

das Herunterladen von Filmen, Software und MP3s ist illegal und wird mit bis zu 5 Jahren Freiheitsentzug bestraft.
Wir möchten Sie darauf hinweisen, dass Ihr Rechner unter der IP 217.71.103.40 erfasst wurde.
Ihre Daten wurden uns von Ihrem Provider zu Verfügung gestellt und eine Strafanzeige wurde erlassen.
In dem angeführten Anhang finden Sie die Strafanzeige mit dem Aktenzeichen Nr.:# 130067
Drucken Sie diese bitte aus und faxen Sie diese mit einer Stellungname an uns zu.
Eine Kopie der Strafanzeige wird Ihnen in den nächsten Tagen schriftlich zugestellt.

Hochachtungsvoll
i.A. Jürgen Stock

Bundeskriminalamt BKA
Referat LS 2
65173 Wiesbaden
Tel.: +49 (0)611 - 55 - 12331
Fax.: +49 (0)611 - 55 - 0

Anhänge: Akte18567.zip Teil 1.3

30.05. Durch einen Bericht der Zeitschrift InformationWeek wird bekannt, dass türkische Aktivisten mehrfach **Webserver der US-Army gekapert** haben sollen. Zugriffe auf die betroffenen Webseiten wurden auf andere Webseiten umgeleitet, auf denen sich politischen Parolen befanden.

Juni 2009

03.06. Mehrere zehntausend legitime Webseiten fallen einem **Massenhack** zum Opfer. Besucher der manipulierten Webseiten werden auf einen ukrainischen Server umgeleitet, der Exploits für den Internet Explorer, Firefox und Quicktime verteilt.

05.06. Der kalifornische Internet-Service-Provider **Pricewert LLC**, der auch unter den Aliasnamen **3FN** und **APS Telecom** agiert, wird auf Druck der amerikanischen Handels-Aufsichtsbehörde FTC vom Netz genommen. Neben dem Hosting von Command & Control Servern zur Steuerung von über 4500 Spyware-Programmen soll das Unternehmen aktiv Kriminelle rekrutiert und die Verfolgung illegaler Inhalte gezielt erschwert haben. Im Gegensatz zu dem einschneidenden Shutdown von McColo im November 2008 wirkt sich diese Aktion nur geringfügig auf den Versand von Spam und Malware aus.

09.06. Unbekannte dringen in die Systeme des britischen Webhosters **VAserv** ein und manipulieren oder löschen die Daten von mehr als 100.000 dort gehosteten Websites.

17.06. Rund 2.2 Mio. URLs des URL-Verkürzungsdienst **cli.gs** werden manipuliert und auf ein anderes Ziel umgeleitet

24.06. Das Pentagon richtet auf Anordnung des US-Verteidigungs-Ministers ein **Cyberwar-Kommando** ein, welches fähig sein müsse, kriegerische Auswirkungen auf das globale Sicherheitsumfeld zu kontern.

25.06. Die Staatsanwaltschaft Hannover ermittelt wegen massenhaften Betruges von Computerbenutzern gegen die Betreiber der Webseite **mega-downloads.net** und friert im Zuge der Ermittlungen u.a. Firmenkonten mit fast einer Mio. Euro ein. Nach Schätzungen von Verbraucherzentralen wurden pro Monat fast 20.000 Computerbenutzer durch versteckte Abo-Fallen abgezockt.