BitDefender Malware- und Spamstudie

MALWARE- UND SPAMTRENDS JANUAR - JUNI 2009

bitdefender

Inhalt

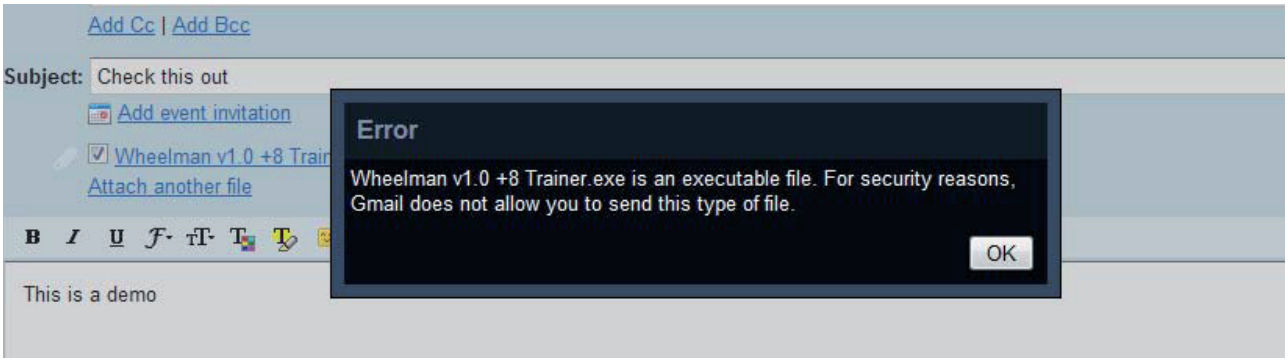
Überblick

Das Internet hat sich zweifellos zu einem der wichtigsten Kommunikationsmittel entwickelt; dabei macht es keinen Unterschied, ob es für geschäftliche, akademische oder Freizeitaktivitäten genutzt wird. Die Nutzung des Internets ist allerdings nicht auf die Übermittlung von großen Datenmengen beschränkt, sondern beinhaltet auch den Transfer von echtem Geld. Onlinebanking-Dienste, Aktien, Onlineshopping und gezielte Werbung stehen dem Benutzer mit wenigen Mausklicks zur Verfügung.

Malware wird schon lange nicht mehr nur für Streiche oder harmlose Scherze zwischen computererfahrenen Anwendern benutzt. Das Programmieren von Malware hat sich zu einem ausgewachsenen Geschäft entwickelt, das nach Unternehmensmodellen konzipiert und von Cyberkriminellen betrieben wird. Der einzige Zweck liegt darin, zwischen den Endbenutzer und dessen Finanzvermögen oder geistiges Eigentum zu gelangen, das über Webdienste verwaltet, ausgetauscht oder gespeichert wird.

Entgegen der weit verbreiteten Meinung ist es heute nicht mehr so, dass elektronische Bedrohungen ausschließlich auf MS-Windows-Betriebssysteme beschränkt sind. Obwohl es durchaus sein kann, dass sich Angreifer mehrheitlich auf Windows-Rechner konzentrieren, weil diese den größten Marktanteil haben, experimentieren Cyberkriminelle auch mit Apple Mac OS X und mobilen Plattformen wie z. B. dem iPhone.

Der Großteil der Cyberangriffe erfolgt eher über das Web als per E-Mail. Angesichts der Tatsache, dass Internetdiensteanbieter und Unternehmen die geeigneten Maßnahmen ergriffen haben, um ein- und ausgehende E-Mails zu scannen sowie die zulässigen Formate für Dateianhänge auf nicht ausführbare Dateien zu beschränken, befassen sich die Programmierer von Malware heute weitestgehend damit, vertrauenswürdige Websites mit hohen Besucherzahlen zu infizieren, um dann abzuwarten, bis unvorsichtige Benutzer den Köder schlucken.



Malware im Rampenlicht

- MS08067-Wurm – der Wurm Downadup/Conficker/Kido infizierte im ersten Halbjahr 2009 weltweit ca. 11 Millionen Computer. Der Wurm ist noch immer aktiv und infiziert täglich hunderte Systeme.

- Bei 88,3 Prozent der weltweit verschickten E-Mails handelt es sich um Spam. Bildbasierte Spamnachrichten haben einen Anteil von 3,9 Prozent, die durchschnittliche Größe einer Nachricht beträgt 4,8 KB.

- Verglichen mit Windows sind Mac-OS-X-Plattformen noch immer sicher, aber die Anzahl der Phishing-Versuche, einige Arten von Scareware und das Auftreten von voll funktionsfähigen Trojanern ebnen den Weg für Mac-OS-X-Malware.

- Bei dem Großteil des weltweiten Spams handelt es sich um Werbung für verschreibungspflichtige Medikamente. Kanadische Apotheken sind hierbei der Spitzenreiter unter den Spamversendern.

- Eine der am häufigsten missbrauchten Marken in Sachen Spam ist das Onlineunternehmen WebMD, dessen Newsletter gefälscht wurden, sodass sie Werbung für kanadische Apotheken enthielten. Auf Platz zwei der Liste der missbrauchten Marken liegen gefälschte MSN-Newsletter.

- Phishing-Angriffe haben dramatisch zugenommen; von den Hackern werden dabei in den USA ansässige Geldinstitute ins Visier genommen.

- Aktive Geldautomatenmalware: Trojan.Skimer.A greift Geldautomaten des amerikanischen Herstellers Diebold an. Die Schadsoftware ist in der Lage, Karteninformationen und PIN-Nummern zu erfassen, ohne dass der Bankkunde dies bemerkt.

- Gefälschte Reinigungsprogramme für den Downadup-Wurm: Nach der durch den Downadup-Wurm ausgelösten Pandemie (bis heute wurden ca. 11 Millionen Rechner infiziert) haben Malwareprogrammierer gefälschte Reinigungsprogramme in Umlauf gebracht, die ihrerseits Schadsoftware auf dem System installieren, insbesondere sogenannte Rogue-Software.

- Illegal veröffentlichte Kopien von Microsofts bevorstehendem Betriebssystem Windows 7 sowie eine technische Vorschau der Microsoft Office Suite 2010 sind auf Torrent-Websites aufgetaucht. Viele der verbreiteten Images wurden jedoch so modifiziert, dass sie zusätzlich zu den originalen Microsoft-Dateien auch verschiedene Malwarevarianten installieren. Angesichts des öffentlichen Interesses sind viele Nutzer Opfer ihrer eigenen Neugier geworden.

- Das erste Window-7-Proof-of-Concept-Rootkit (VBootkit) wurde unter der GPL-Lizenz veröffentlicht.

Bedrohungen durch Malware im Überblick

Während des ersten Halbjahres 2009 haben die Programmierer von Schadsoftware weiterhin alles daran gesetzt, Computer zu infizieren, um daraus entweder direkten finanziellen Nutzen zu ziehen oder die Kontrolle über die Rechner zu erlangen. Malware der Kategorie Trojaner nimmt weiter stark zu und hat einen Anteil an der weltweit erkannten, aktiven Schadsoftware von mehr als 83 Prozent.

Downadup und MS08-067

Obwohl Trojaner mit Abstand die aktivsten IT-Sicherheitsbedrohungen darstellten, wurde der größte Schaden auf Seiten der Benutzer dieses Jahr durch den berüchtigten Internetwurm Downadup verursacht. Das Aufkommen dieser brandneuen IT-Bedrohung stellt nicht nur das Comeback der Würmer hinsichtlich moderner Betriebssysteme dar, sondern zeigt auch eine neue Philosophie. Während Schadsoftware größtenteils für kriminelle Machenschaften geschrieben wird wie z. B. den Diebstahl von Waren oder Vermögenswerten (Onlinebanking, Onlinespiele und Aktienhandel) oder auch um Computerressourcen zu übernehmen (Botnets), hatte der Downadup-Wurm eigentlich keine tatsächliche Funktion. Kurz gesagt, er hat nichts gemacht.

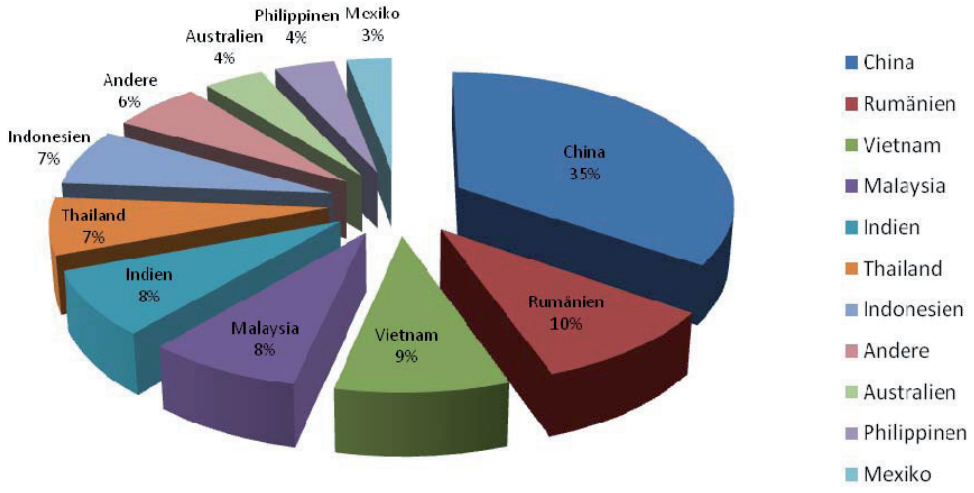


Abbildung 1: Downadup-Infektionen nach Ländern

Im Gegensatz zu ähnlichen Bedrohungen, die vor einigen Jahren für Chaos gesorgt haben (Code Red, Melissa und Nimda), wurde der brandneue Downadup sorgfältig entwickelt, um die Erkennung auf und Entfernung von infizierten Rechnern zu verhindern. Serverseitige Polymorphismen und Modifikationen der Zugriffssteuerungsliste (ACL) sind nur einige der neuartigen Funktionen, die die professionelle Gruppierung von Cyberkriminellen bei der Entwicklung des Wurms implementiert hat.

Um sich über die Netzwerke zu verbreiten, nutzt das Programm die MS08-067-Sicherheitslücke des Windows-Serverdienstes, gleichzeitig kann jedoch auch eine Verbreitung über infizierte USB-Laufwerke, die eine Autostartfunktion verwenden, erfolgen. Sobald das System erfolgreich infiziert wurde, versucht der Wurm, lokale Passwörter zu knacken, um Zugang zu im Netzwerk freigegebenen Dateien zu erhalten. Am allerwichtigsten ist, dass Downadup, wenn ein Administratorzugang kompromittiert wurde, den Windows-Task-Scheduler-Dienst[1] verwendet, um sich auf andere Systeme im Netzwerk auszubreiten. Obwohl Microsoft ein außerplanmäßiges Update für die Sicherheitslücke veröffentlicht hat, infiziert der Wurm sogar heute noch Systeme.

Um zu verhindern, dass der Benutzer an Reinigungsprogramme gelangt, die von Antimalware-Anbietern zur Verfügung gestellt werden, unterbindet der Wurm den Zugang zu deren Websites und blockiert außerdem Dateien, die bestimmte Namen beinhalten. BitDefender hat als erstes Unternehmen ein funktionierendes Entfernungsprogramm angeboten, das unter www.bdtools.net erhältlich ist[2].

Weltweite Malware-Top 10

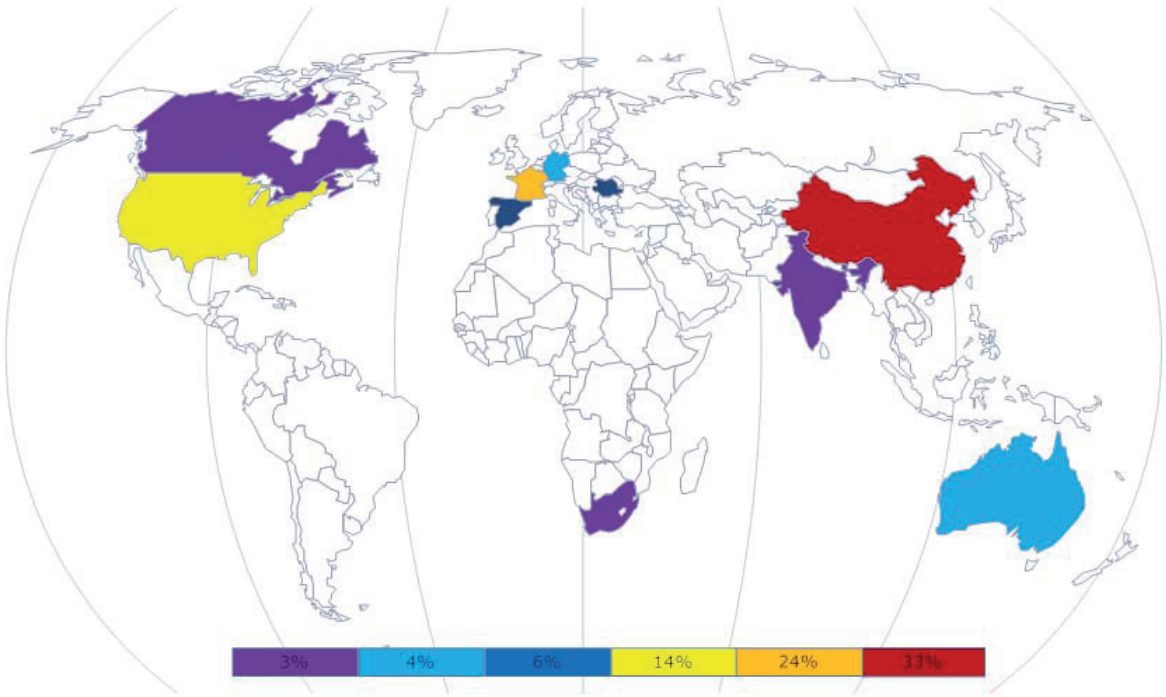


Abbildung 2: Malware-Aufschlüsselung nach Ländern

[1] Administrativ geplante Aufgaben werden automatisch, ohne Eingabeaufforderung, ausgeführt, sodass sich der Wurm kopieren und auf sauberen Systemen ausführen kann.

[2] Die Website www.bdtools.net wurde zu diesem Zeitpunkt nicht von Downadup blockiert. Im April 2008 begann eine aktualisierte Downadup-Version die Website zu blockieren, und BitDefender bot daraufhin unter der Website www.disinfecttools.net kostenlose Tools zur Entfernung an.

China, Frankreich und die USA, gefolgt von Rumänien, Spanien und Australien, waren während der letzten sechs Monate die aktivsten Länder, was die Verbreitung von Schadsoftware betrifft.

Januar – Juni 2009				
01.	TROJAN.AUTORUNINF.GEN			31 %
02.	Win32.Worm.Downadup.Gen			13 %
03.	TROJAN.WIMAD.GEN.1			13 %
04.	Trojan.Skimtrim.HTML.A			11 %
05.	TROJAN.AGENT.AKXM			10 %
06.	Trojan.Autorun.AET			7 %
07.	WORM.AUTORUN.VHG			5 %
08.	Packer.Malware.NSAnti.1			4 %
09.	TROJAN.SPY.AGENT.NXS	3 %	0,00	0,00
10.	Trojan.JS.PZB	3 %	0,00	0,00

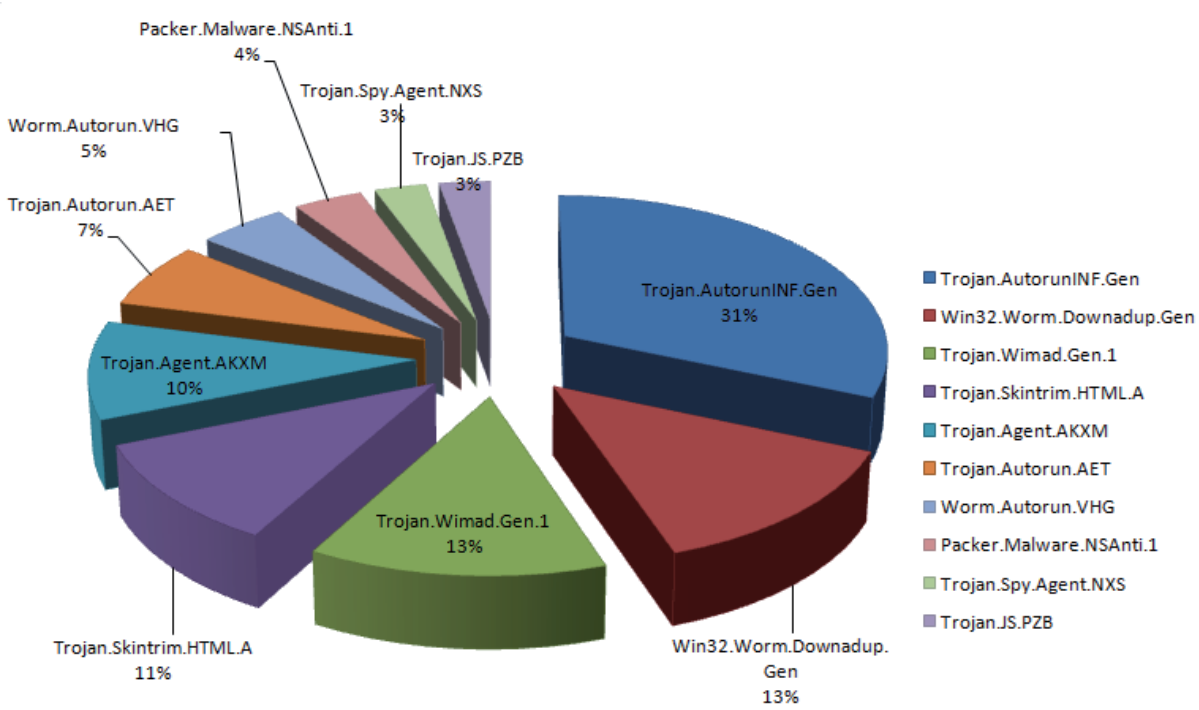


Abbildung 3: Top 10 der Malwarebedrohungen im ersten Halbjahr 2009

1. Trojan.Autorun.Inf

Der auf Platz 1 der Malwareliste des ersten Halbjahres liegende Trojan.Autorun.Inf ist für 31 Prozent der weltweiten Infektionen verantwortlich. Die äußerst hohe Zahl an Infektionen ist jedoch nicht das Ergebnis einer globalen Pandemie, sondern eher der Tatsache geschuldet, dass sich zahlreiche Malwarefamilien[3] über Wechselmedien verbreiten.

Bereits bei Windows 95 wurde die Autorun-Funktion eingeführt, die technisch weniger versierten Benutzern die Installation von Anwendungen erleichtern sollte, indem automatisch die „richtige" auf einem Wechselmedium enthaltene Datei geöffnet wird. Seitdem wird die Autorun-Funktion erfolgreich von Malwareprogrammierern eingesetzt.

Die Autorun-Funktion, einer der wichtigsten Überträger von Malware, führt automatisch eine Binärdatei aus, sobald ein Wechseldatenträger an den PC angeschlossen oder eingelegt wird. Vor Windows Vista befolgten Windows-Betriebssysteme alle in einer „autorun.inf"-Datei enthaltenen Anweisungen.

Obwohl diese Funktion äußerst nützlich ist, hat sich Microsoft dazu entschlossen, diese für das bevorstehende Betriebssystem Windows 7 standardmäßig zu deaktivieren.

2. Win32.Worm.Downadup

Der bereits oben angeführte Wurm Downadup benötigt keine Einführung: Während der letzten sechs Monate ist es ihm gelungen, eine beispiellose weltweite Zahl an Computern zu infizieren und in praktisch allen Computermagazinen Schlagzeilen zu machen.

Downadup verwendet drei verschiedene Ansätze, um Computer zu kompromittieren:

- Wenn auf dem Zielsystem die MS08-067-Sicherheitslücke nicht per Update geschlossen wurde, kann sich der Wurm selbst von einem anderen Computer im Netzwerk aus, der bereits infiziert wurde, übertragen.
- Sobald er ein System infiziert hat, das Teil eines Netzwerks ist, lokalisiert der Wurm saubere Systeme und startet einen Brute-Force-Angriff auf das Remote-Administratorkonto, um Zugang zu den im Netzwerk freigegebenen Dateien des Benutzers zu erhalten.
- Wenn der Wurm auf einen Wechseldatenträger (CD-R, DVD-R, USB-Stick oder ein zugeordnetes Netzlaufwerk) kopiert wurde, nutzt er die **Autoplay**-Funktion aus (falls aktiviert), um sich selbst auf noch nicht infizierte Computer auszubreiten.

Angesichts der Tatsache, dass er weniger bekannte Windows-APIs verwendet und äußerst entfernungsresistent ist, wurde der Wurm offensichtlich von einem Team professioneller Cyberkrimineller entwickelt. So schützt sich der Wurm beispielsweise dadurch vor der Entfernung, dass er sämtliche NTFS-Dateiberechtigungen aller Systembenutzer entfernt bis auf die Funktionen Ausführen und Pfadangaben[4].

3. Trojan.Wimad

Der auf Platz 3 der Malwareliste des ersten Halbjahres 2009 liegende Trojan.Wimad nutzt eine weniger bekannte Funktion aus, die von Microsoft implementiert wurde, um koordinierte Daten digitaler Medien zu speichern. Der Trojaner befällt ASF-Dateien, ein erweiterbares Dateiformat, welches das Versenden von Daten über eine Vielzahl von Netzwerken unterstützt und besonders einfach lokal abgespielt werden kann. Das ASF-Format ist eigentlich ein Container, in dem Daten entweder im WMA- (Windows Media Audio) oder WMV-Format (Windows Media Video) gespeichert werden.

---

[3] Zu den bedeutendsten Malwarefamilien, die die Autorun-Funktion nutzen, gehören Win32.Worm.Downadup, Trojan.PWS.OnlineGames und Trojan.TDss.

[4] Weitere Informationen über den Wurm Downadup sowie BitDefenders kostenlose Tools zur Entfernung finden Sie unter http://www.bitdefender.com/VIRUS-1000462-en--Win32.Worm.Downadup.Gen.html.

Besonders wichtig ist die Tatsache, dass die ASF-Formatspezifikationen eine Kommandofunktion namens **URLANDEXIT** unterstützen. Diese erlaubt es der Datei, automatisch das erforderliche Videocodec herunterzuladen, falls dieses auf dem System nicht vorhanden ist. Dieser Mechanismus kann von Malwareprogrammierern auf einfache Art und Weise missbraucht werden, um über die Datei Trojaner herunterzuladen oder den Benutzer auf eine präparierte Website zu lotsen.

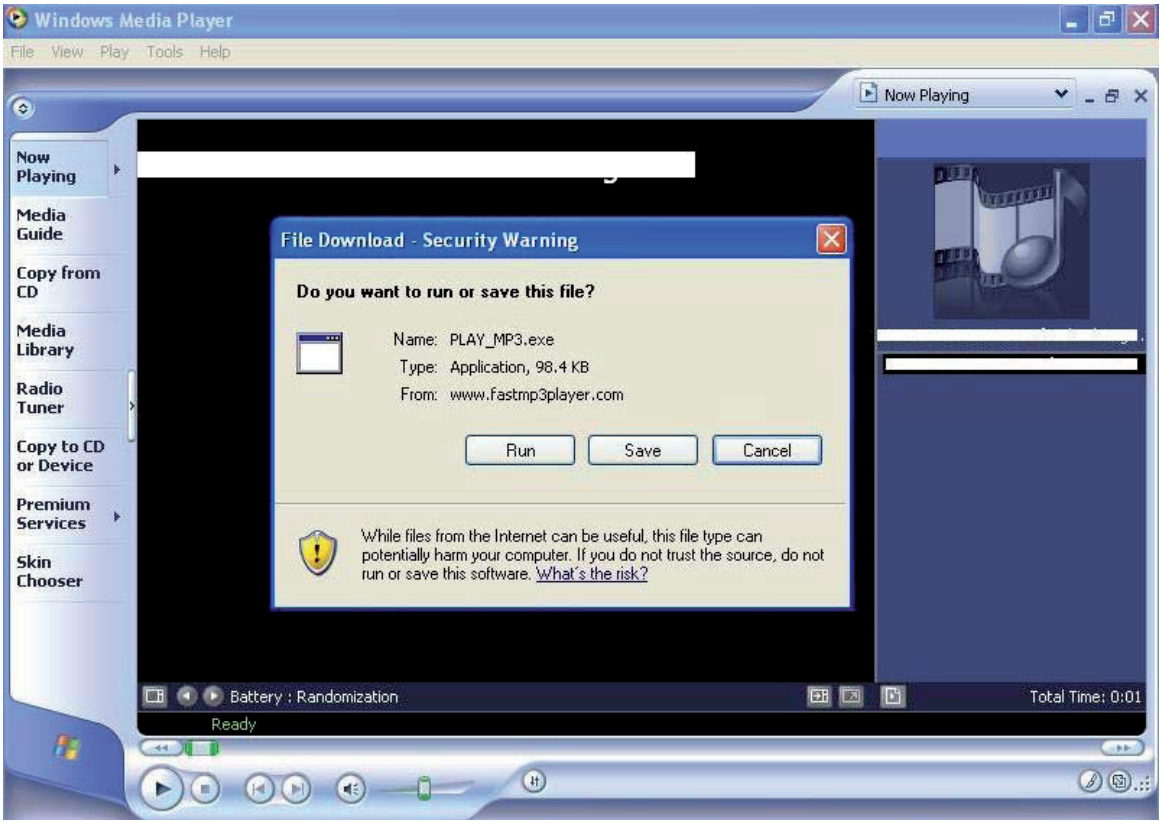


Abbildung 4: Eine infizierte Videodatei versucht, Schadsoftware herunterzuladen

4. Trojan.SkimTrim.HTML.A

Trojan.SkimTrim.HTML.A ist Teil der NaviPromo-Adware-Familie. Die besonders für ihre aggressiven Popups sowie ihre Widerstandsfähigkeit gegen Erkennung und Entfernung bekannte Adware benutzt fortschrittliche Rootkit-Techniken, um sich auf der Festplatte und im Arbeitsspeicher zu verstecken, wodurch es ihr gelingt, sich gegenüber Betriebssystemen und Antivirenscannern zu tarnen.

NaviPromo ist üblicherweise an andere, im Internet erhältliche Software gebunden. Sie installiert sich ohne Einwilligung des Benutzers und injiziert dann ihren Programmcode in die Datei explorer.exe. Während der Benutzer im Internet surft, überwacht NaviPromo das Surfverhalten, sammelt und versendet persönliche Daten, die für die Erstellung kommerzieller Profile genutzt werden. Ist die Profilerstellung abgeschlossen, wird dem Computernutzer Popup-Werbung angezeigt, die zu den Inhalten der Websites passt, die der Benutzer gerade betrachtet.

5. Trojan.Agent.AKXM

Während „autorun.inf“-Dateien an sich nicht schädlich sind, werden sie jedoch von Malwareprogrammierern dazu verwendet, um automatisch verschiedene Arten von Schadsoftware zu starten, sobald ein infiziertes Medium gemountet wird. Trojant.Agent.AKXM ist ein Beispiel für ein Schadprogramm, das die Autorun-Funktion verwendet. Der Inhalt der Datei ist verschleiert und mit Text zugemüllt, um die Erkennung zu verhindern. Immer dann, wenn auf das infizierte Laufwerk zugegriffen wird, lässt die inf-Datei rundll32.exe eine dll-Datei laden, die sich unter *RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665* befindet. Die Analyse hat gezeigt, dass es sich dabei in Wirklichkeit um eine Kopie des Wurms Downadup handelt.

6. Trojan.Autorun.AET

Bei Trojan.Autorun.AET handelt es sich um Malware, die sich über unter Windows freigegebene Ordner sowie über Wechselmedien (Netzlaufwerke oder verbundene Laufwerke) verbreitet. Der Trojaner nutzt die in Windows-Betriebssystemen enthaltene Autorun-Funktion aus, um sich selbst automatisch auszuführen, sobald ein infiziertes Laufwerk angeschlossen wird. Weitere Informationen darüber, wie die Autorun-Funktion die Sicherheit Ihres Computers beeinträchtigen kann, finden Sie unter dem Punkt 1. „Trojan.Autorun.Inf“.

7. Worm.Autorun.WHG

Worm.Autorun.WHG ist eine weitere Version des Trojan.Agent.AKXM, einer „autorun.inf“-Datei, die der Wurm Downadup verwendet, um sich über infizierte Wechselmedien zu verbreiten.

8. Packer.Malware.NSAnti.1

Zu dieser Kategorie gehören verschiedene Arten von Malware, die mithilfe des NSAnti-Schutzsystems gepackt bzw. geschützt werden. NSAnti ist eine Technologie, die Cyberkriminelle entwickelt haben, um ihre Malwareinhalte vor Antivirenscannern zu schützen.

Eine der wichtigsten Funktionen der NSAnti-Packer ist die Tatsache, dass die beinhalteten Dateien spontan ausgeführt werden können, ohne dass sie in das Dateisystem geschrieben werden müssen, wo sie von einem Antivirenscanner aufgespürt werden könnten. NSAnti nutzt besonders Polymorphismen (die Fähigkeit, seinen Programmcode zu modifizieren, um die signaturbasierte Erkennung zu verhindern) und ist äußerst resistent gegen die Emulation (der Code kann virtuelle Maschinen abstürzen lassen). Der NSAnti-Code wird zudem stetig verändert, um der Erkennung durch Antivirenprodukte zu entgehen.

9. Trojan.Spy.Agent.NXS

Platz 9 der Malwareliste für das erste Halbjahr 2009 geht an Trojan.Spy.Agent.NXS, eine Schadsoftware, die Shell-Befehle ausführen kann. Obwohl diese Malware keine permanente UDP- oder TCP-Verbindung beinhaltet, kann der Bot als Hintertür für Remote-Eindringlinge fungieren.

10. Trojan.JS.PZB

Der letzte Platz geht an Trojan.JS.PZB, der iFrame-Techniken verwendet, um schädliche Inhalte in legitime Websites zu injizieren. Kurz gesagt kann eine legitime Website dahin gehend kompromittiert werden, dass sie ein unsichtbares „Fenster“ zu einer schädlichen Dritt-URL beinhaltet. Jedes Mal, wenn der Benutzer die infizierte Website besucht, kann dies einen beiläufigen Malwaredownload auslösen.

Web-2.0-Malware

Die zunehmende Beliebtheit von Web-2.0-Diensten wie z. B. sozialen Netzwerken, Blogs und Wiki-Plattformen hat es den Angreifern erleichtert, ihre heimtückischen Ziele zu erreichen. Aufgrund der Tatsache, dass die Mehrheit der Web-2.0-Dienste, im Gegensatz zu klassischen Online-Communitys oder Blogs, die Angabe genauer persönlicher Daten erfordert, besteht die Gefahr, dass der Benutzer, wenn diese Daten in die falschen Hände gelangen, ungeschützt dasteht.

Spam und Phishing

Benutzerkonten bei sozialen Netzwerken sind Schlüsselelemente für die Ausführung nachfolgender Angriffe auf andere Netzwerkbenutzer. Nachdem seriöse Anbieter strengere Sicherheitsmaßnahmen eingeführt haben, um die persönlichen Daten ihrer Benutzer zu schützen, haben die Angreifer gefälschte Anmeldeseiten eingerichtet, mit deren Hilfe sie versuchen, an echte Anmeldeinformationen zu gelangen.

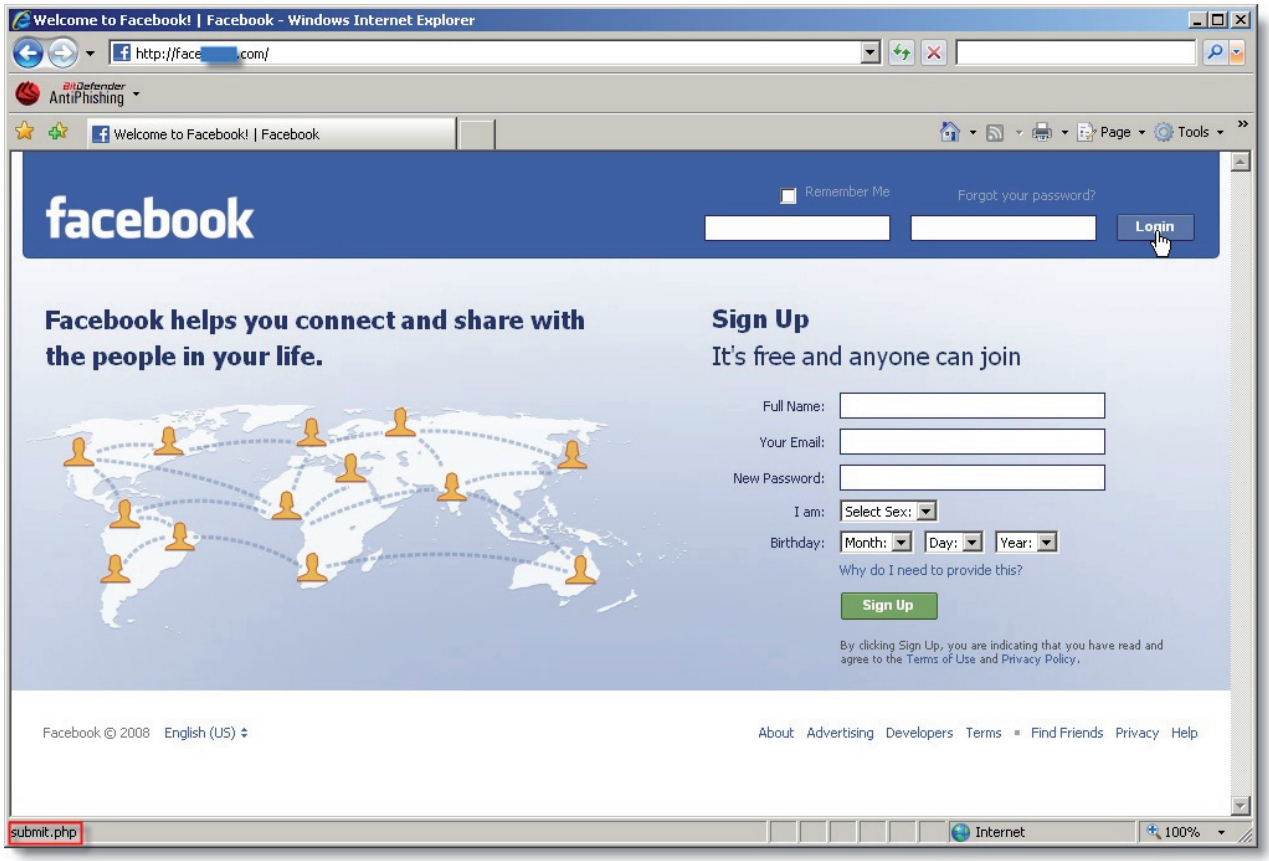


Abbildung 5: Facebook-Phishing-Seite

Soziale Netzwerke verzeichnen außerdem höchste Besucherzahlen und sind der perfekte Ort, um eigene Werbung zu platzieren. Spammer erstellen Benutzerkonten, mit dem einzigen Zweck, Links zu Werbewebsites oder zu Schadsoftware zu veröffentlichen.

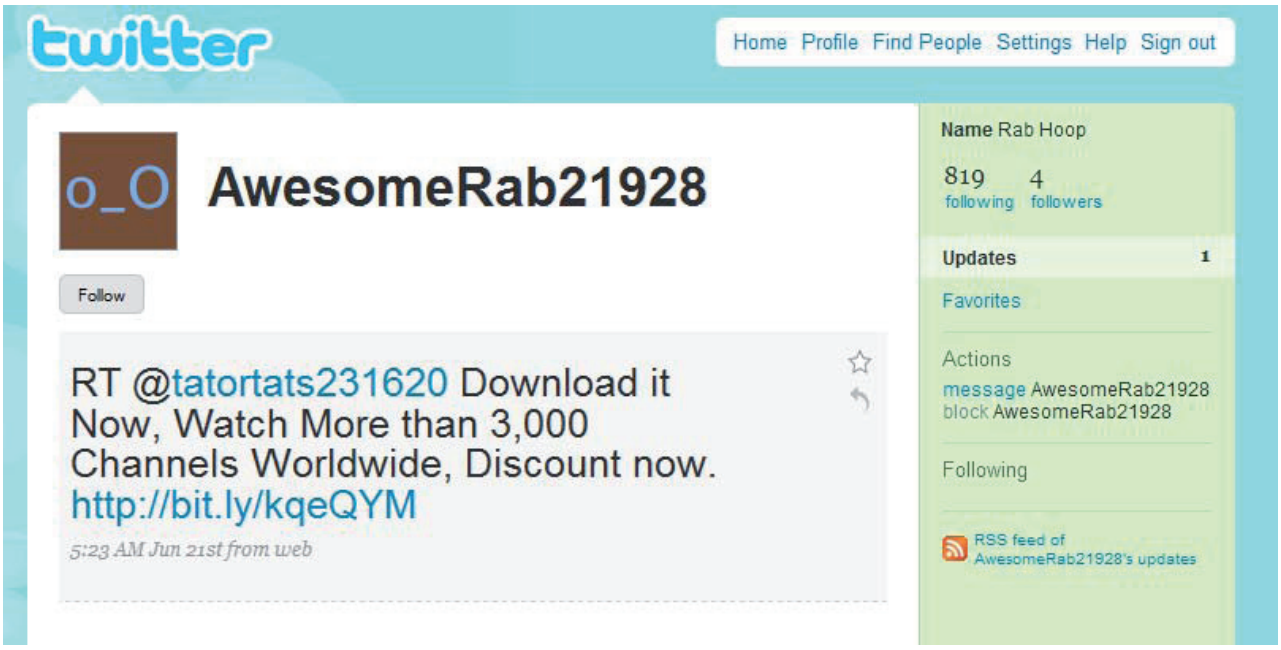


Abbildung 6: Twitter-Profil, das Satellitenschüsseln bewirbt

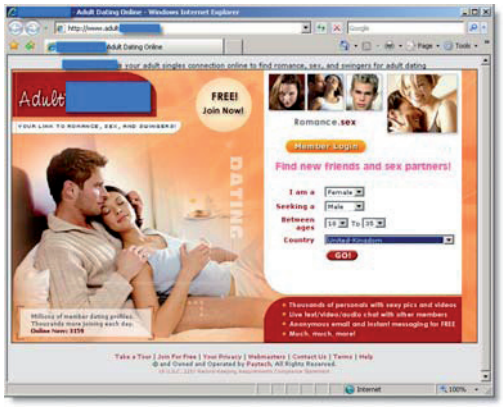
Spam und Phishing sind die geläufigsten Bedrohungen im Bereich der Web-2.0-Dienste, stellen jedoch nicht die einzigen Gefahren dar, denen Nutzer sozialer Netzwerke ausgesetzt sind. Web-2.0-Communitys haben sich auch zu einem wichtigen Überträger für Malware, insbesondere Trojaner und Rogue-Software, entwickelt.

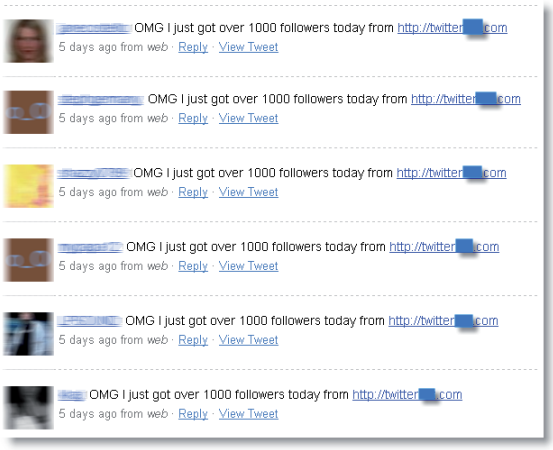
Es muss außerdem erwähnt werden, dass sich die meisten Versuche speziell darauf konzentrieren, Anmeldeinformationen sowie andere Daten zu stehlen, die den Zugang zu Twitter und ähnlichen Plattformen ermöglichen wie z. B. E-Mail-, Blog- oder Onlineshoppingkonten. Gelingt der Zugang, bietet sich ein breites Spektrum an kriminellen Möglichkeiten, von weiteren Spam- und Phishing-Versuchen (unter Verwendung der Liste an Followern/Freunden/Kontakten) über Identitätsdiebstahl bis hin zum Diebstahl gewerblicher Daten und Erpressung.

Die meisten dieser Phishing-Versuche basieren auf sozialer Manipulation und spekulieren auf die Naivität der Benutzer. Der Twitter-Betrug mit Pornonamen ist ein gutes Beispiel. Der Benutzer wird dabei aufgefordert, den Namen seines ersten Haustieres und den Namen der ersten Straße, in der er gelebt hat, anzugeben. Die Antworten auf diese Fragen werden häufig für Sicherheitsfragen der zuvor genannten Anwendungen verwendet. Ein Cyberkrimineller, der über diese Antworten und den Benutzernamen einer Person verfügt, kann ganz einfach ein „vergessenes“ Passwort abfragen, mit dem er oder sie später auf das Benutzerkonto

zugreifen kann, um darüber Spamnachrichten zu versenden, Zugang zu Transaktionen zu erhalten oder das Konto auf sonstige profitbringende Art und Weise zu nutzen (hierzu gehört sogar die Forderung eines Lösegelds für das gekidnappte Benutzerkonto).

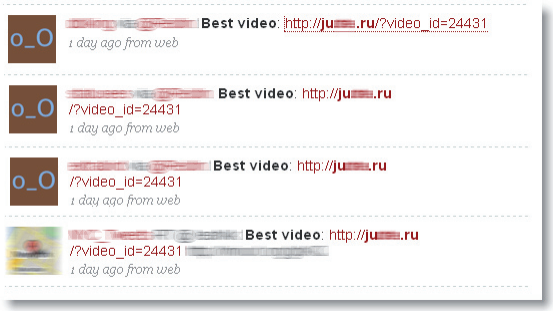
Eine andere Möglichkeit sind Websites, die auf Tippfehler des Benutzers spekulieren wie z. B. tvvitter.com (momentan nicht verfügbar), über die Anmeldeinformationen gesammelt und automatisch ungewünschte Follower hinzugefügt wurden. Die in diesen (möglicherweise gefälschten oder gekidnappten) Profilen enthaltenen Links führten den Benutzer auf eine Partnervermittlungsseite, die wahrscheinlich im Rahmen eines Pay-per-Click- oder Ranking-Betrugs benutzt wurde.

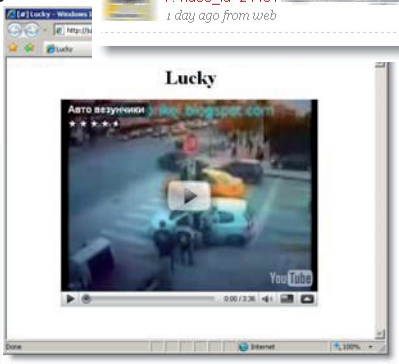




Eine weitere Phishing-Methode beinhaltete eine vermeintliche Drittwebsite, die Nachrichten darüber verschickte, wie man schnell die Anzahl seiner Twitter-Follower erhöhen kann. Um den Vorgang abzuschließen, forderte die Website den Twitter-Benutzernamen sowie das Passwort. Wenn diese preisgegeben wurden, wurde die Follower-Liste des unvorsichtigen Benutzers automatisch mit derselben Nachricht zugespammt.

Zu guter Letzt ist da noch eine der jüngsten Attacken, die auf über verschiedene Konten versendete Spamnachrichten und einer schädlichen PDF-Datei basiert, die über ein iFrame-Exploit heruntergeladen wurde, wenn der Benutzer auf einen Link klickte, der angeblich zum „Besten Video“ führte. Neben dem Clip lieferte die in Russland gehostete Seite auch die Rogue-Software „System Security 2009“.





Am 30. April wurde Microsofts Technet-Dienst mit schädlichen Links überflutet, die in Benutzerprofile eingetragen wurden. Die als Videoplayer getarnten Signaturen versprachen pornografisches Material verschiedener Berühmtheiten (Rihanna und Angelina Jolie sind nur zwei Beispiele der zahlreich verwendeten Namen von Hollywood-Persönlichkeiten) und verlangten vom Benutzer, dass dieser die Datei Mediacodec_v3.7.exe herunterlädt und installiert. Dabei handelte es sich um eine 1,93 MB große Binärdatei, die in Wirklichkeit eine als **Privacy Center** bekannte Rogue-Software installierte.

Bedrohungen durch Spam im Überblick

Im ersten Halbjahr 2009 war ein starker Anstieg im Bereich des Newsletter-Spams zu erkennen. Bei diesen Nachrichten handelt es sich um HTML-Vorlagen, denen die Spamversender üblicherweise ein Spambild beifügen (Werbung für Cialis, Viagra und Levitra), das auf einen chinesischen Domain-Namen verlinkt ist.

Spamverbreitung nach Ländern

Nachfolgend sehen Sie die im Bereich Spam aktivsten Länder.

Spamverbreitung nach Ursprungsland Januar – Juni 2009	
	SPAMINDEX
BRASILIEN	13,6
USA	10,1
INDIEN	5
RUSSLAND	4,2
CHINA	3,3
ARGENTINIEN	2,8
SPANIEN	2,7
KOLUMBIEN	2,6

Am Ende stehen Kanada, Ägypten, Marokko und Korea mit weniger als 0,5 Prozent des weltweiten Spams.

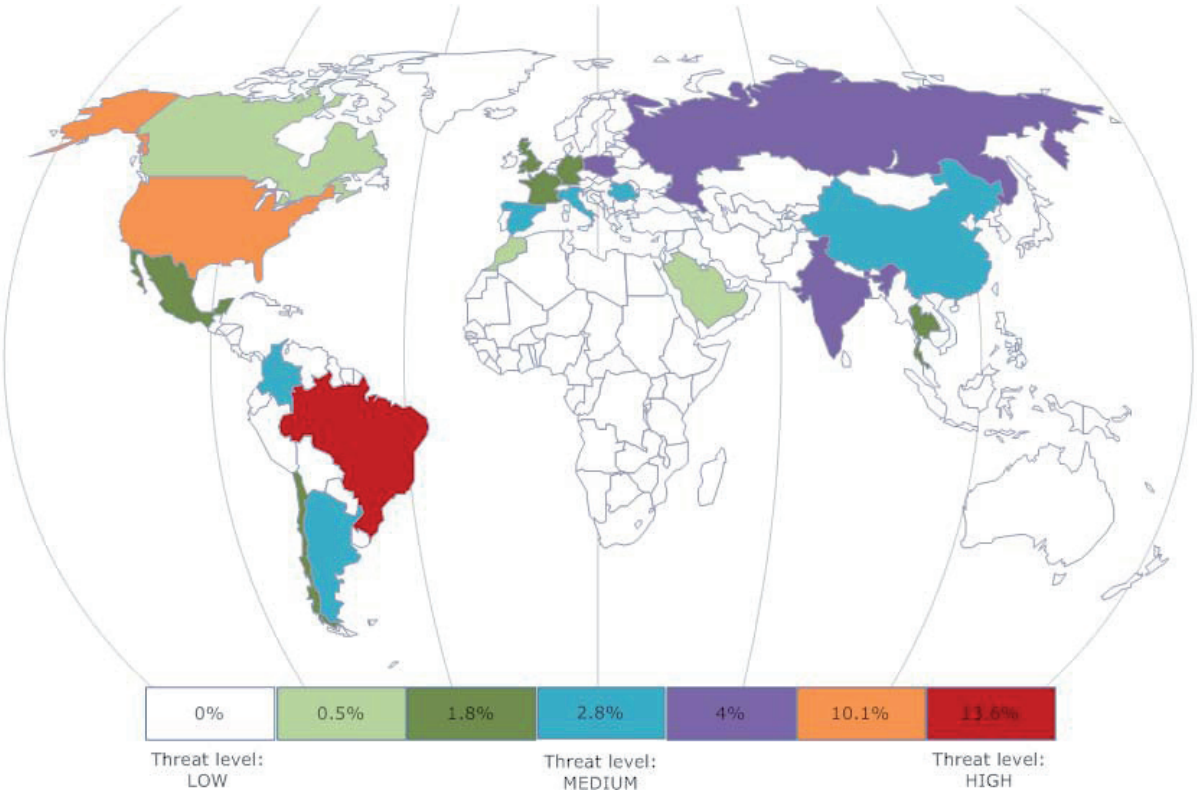
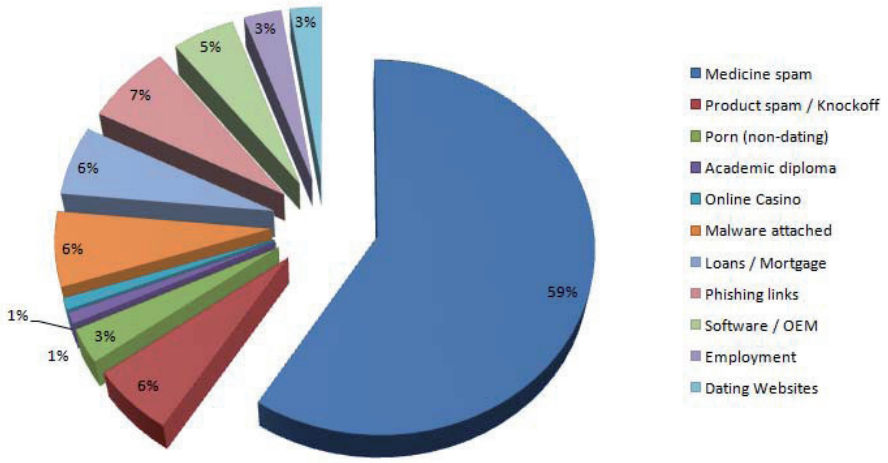


Abbildung 7: Spamverbreitung nach Ländern

Spamaufschlüsselung nach Art

Im Vergleich zum Vorjahreszeitraum hat auch die Anzahl an Spamnachrichten, die Raubkopien von Softwareprodukten oder OEM-Software bewerben, dramatisch zugenommen. Gemäß den vom BitDefender Antispam Lab zur Verfügung gestellten Statistiken hat Software-Spam einen weltweiten Anteil von 3 %. Bis Juni dieses Jahres haben es unerwünschte E-Mails, die im Zusammenhang mit Softwareprodukten stehen, unter die Top 5 der Spambedrohungen geschafft und einen Anteil von 5 % an den weltweit verschickten Spamnachrichten erreicht.

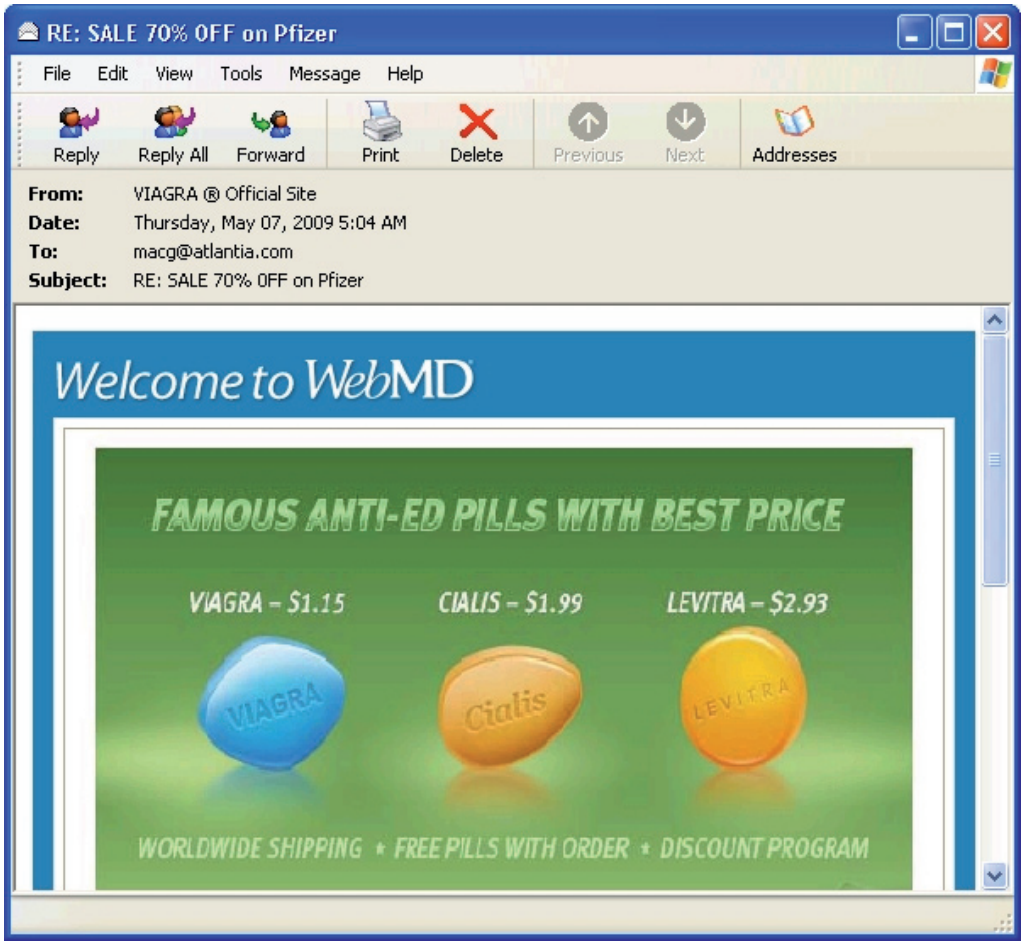


Spamtrends

Wie im vorangegangenen Halbjahr verlassen sich Spamversender von unerwünschten E-Mails noch immer auf Nachrichten in Klartext. Gemäß den Antispamforschern hat Spam in Klartext einen weltweiten Anteil von über 80 %. Bildbasierte Spamnachrichten verzeichnen im Vergleich zum ersten Halbjahr 2008 ebenfalls einen bedeutenden Anstieg von 150 %.

Medizinischer Spam – das gängigste Segment im Bereich unerwünschter E-Mails – zeichnet sich nun durch suggestive Bilder in legitimen Newslettern aus (insbesondere HTML-Mail-Updates von WebMD).

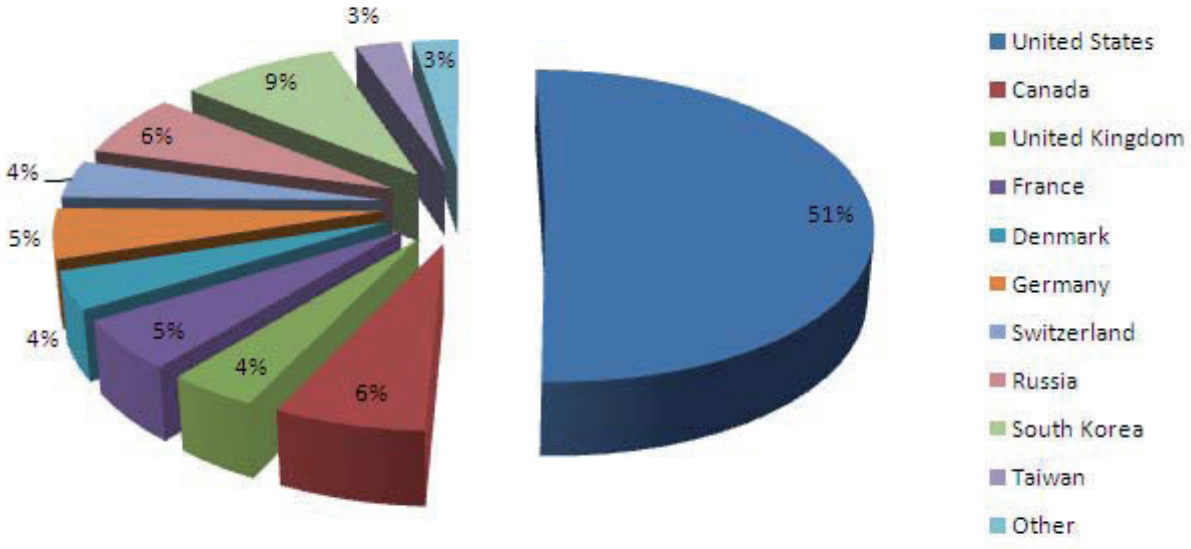
Durch diese Strategie wird der Benutzer dahin gehend ausgetrickst, dass er durch das E-Mail-Programm blockierte Bilddateien akzeptiert. Gleichzeitig wird die Farbpalette der Bilddateien geringfügig verändert, um Spamfilter zu umgehen.



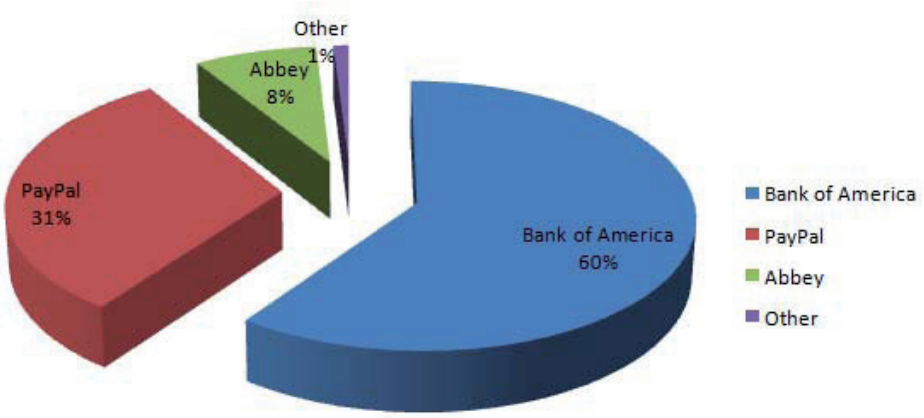
Phishing und Identitätsdiebstahl

Phishing-Versuche, eine der bedeutendsten Bedrohungen für den durchschnittlichen E-Mail-Benutzer, verzeichneten während der letzten sechs Monate einen dramatischen Anstieg. Diese Art von Angriff, die in erster Linie auf englischsprachige und weniger computererfahrene Internetnutzer abzielt, kann dramatische Auswirkungen auf den Kontostand des Benutzers haben.

Aufgrund der Tatsache, dass mehr und mehr Phishing-Versuche Banken zum Ziel haben und genauso gefährlich sind wie Malwareinfektionen, überwacht BitDefender ständig die Phishing-Trends und analysiert Nachrichten, die mithilfe des weltweiten Honeypot-Netzwerks gesammelt werden.



Während der letzten sechs Monate haben Phishing-Nachrichten im Bereich der weltweit verschickten Spamnachrichten einen Anteil in Höhe von 7 % erreicht. Erwartungsgemäß handelte es sich bei den für Phishing empfänglichsten Ländern um die USA, Kanada und Großbritannien – drei englischsprachige Länder. Russland ist jedoch eine weitere bedeutende Quelle von Phishing-Nachrichten. Der Grund dafür liegt in den nachlässigen Rechtsvorschriften im Bereich der Cyberkriminalität sowie in der aktuellen Arbeitslosenquote des Landes.

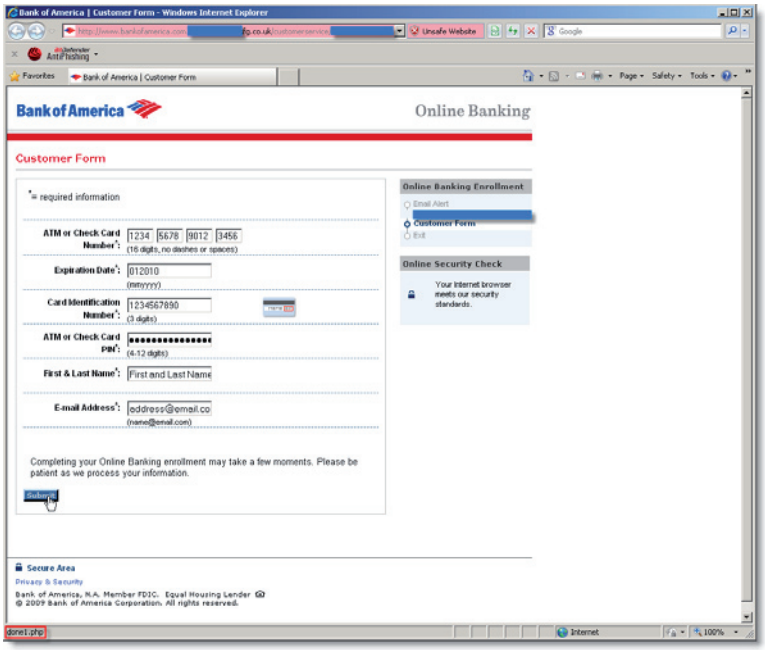


Die Phishing-Landschaft verzeichnet eine stete Entwicklung und Veränderung, die Lieblingsziele der Phisher bleiben dabei jedoch gleich. Die durchschnittlich am häufigsten missbrauchten Identitäten kommen aus dem Finanzsektor, vornehmlich Banken sowie Institutionen für elektronische Geldüberweisungen. Nebenbei bemerkt: Die meisten Phishing-Nachrichten basieren auf sozialer Manipulation. Hierbei wird der Benutzer darüber informiert, dass sein Konto entweder eingefroren wurde oder abgelaufen ist und für die Reaktivierung die Eingabe der Anmeldeinformationen erforderlich ist. Bei anderen Varianten wird dem Empfänger mitgeteilt, dass sein Konto von einer unbefugten Person leergeräumt wurde und er sich nun einloggen müsse, um die Transaktion rückgängig zu machen.

BitDefender schätzt, dass monatlich mehr als 55.000 Menschen Opfer von Phishing-Betrügereien werden. Für das erste Halbjahr 2009 ergibt sich dadurch die beeindruckende Gesamtzahl von 330.000 Opfern. Am allerwichtigsten ist, dass es sich bei **Phishing-Angriffen und Spam**, im Gegensatz zu Malware, um **universelle Sicherheitsbedrohungen** handelt, die unabhängig von Betriebssystem und Sicherheitsupdates auf allen Computern funktionieren. Besondere Vorsicht und eine hochwertige Anti-Malware-Lösung mit Anti-Spam-, Anti-Phishing und Anti-Malware-Modulen sind ein absolutes Muss für jeden, der im Internet surft.

Um seine Opfer erfolgreich zu täuschen, muss der Phisher die Originalseite so präzise wie möglich kopieren (man spricht hier von Spoofing). Während es sich beim Nachmachen der Originalwebsite lediglich um simples Kopieren und Einfügen handelt, stellt man jedoch fest, dass die Spamnachricht üblicherweise Rechtschreibfehler oder schlampige Formatierungen enthält.

Bei der Mehrheit der Phishing-Angriffe auf die Bank of America ist dies allerdings nicht der Fall. Hierbei ist nicht nur der Text in einem tadellosen Zustand; die Phishing-Seite zeigt eine ungewöhnliche Detailtreue, was vermuten lässt, dass es sich bei den für die Angriffe Verantwortlichen um eine hochgradig organisierte Gruppierung von Cyberkriminellen handelt.



Die Verbreitung unerwünschter Nachrichten erfolgt über das Pushdo-Botnet, ein Zombienetzwerk aus mit Malware infizierten Computern, das ebenfalls für den kanadischen Apothekenspam sowie andere Aktivitäten verantwortlich ist.

Sicherheitslücken, Exploits und Sicherheitsverletzungen

Obwohl Malware für die Mehrheit der weltweiten Sicherheitsvorfälle verantwortlich ist, gilt es zu bedenken, dass auch Sicherheitslücken und Exploits eine wichtige Rolle in der IT-Bedrohungslandschaft spielen. Neben Sicherheitslücken, wie z. B. die im Folgenden genannten, die Schlagzeilen machten, war das erste Halbjahr 2009 von einer kontinuierlichen Veränderung der Exploit-Ziele geprägt. Mac OS X, der Safari-Browser und verwandte Technologien werden mit steigendem Marktanteil sowohl für Sicherheitsexperten als auch Hacker immer interessanter. Open-Source-Software wie z. B. Linux und der Firefox-Browser erregen aufgrund von Programmierfehlern und Sicherheitslücken zunehmend mehr Aufmerksamkeit.

Ein dritter wichtiger Bereich sind Web-2.0-Anwendungen und -Dienste. Die relativ unausgereiften zugrundeliegenden Technologien ermöglichen fortwährend zahlreiche Sicherheitsverletzungen. PHP-basierte Web-Frameworks gehörten zu den am stärksten betroffenen Zielen, andere Dienst- und Softwarearten waren jedoch ebenfalls umfassenden Angriffen ausgesetzt.

MD5-Kollisionsangriffe

Bei dem ersten im Jahr 2009 gemeldeten Sicherheitsvorfall handelte es sich um die im Januar entdeckte praktische Möglichkeit, Kollisionen im MD5-Hash-Algorithmus zu bewirken. Das MD5-

Format findet breite Anwendung in der Passwortverschlüsselung, bei der es nicht möglich ist, das Passwort wieder zu entschlüsseln, sowie in der Signierung digitaler Zertifikate.

Die Forschungsgruppe, bestehend aus Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik und Benne de Weger, bewies, dass mithilfe eines präparierten Zertifikats einer Zertifizierungsstelle virtuell nicht erkennbare Phishing-Angriffe möglich sind. Sobald das Zertifikat erfolgreich hinzugefügt wurde, vertraut der Browser allen von der Zertifizierungsstelle ausgegebenen Zertifikaten. Auf diese Art und Weise können Angreifer digitale Zertifikate signieren, die von den kompromittierten Browsern akzeptiert werden.

Ein Kollisionsangriff lässt also praktisch eine Datei als eine andere durchgehen. Um eine Zertifizierungsstelle zu übernehmen, mussten die Forscher denselben Hash-Code für zwei unterschiedliche Datenteile generieren. Dabei benutzten sie 200 verbundene PlayStation-3-Konsolen, da deren Prozessoren für diese Art von Operation besonders optimiert sind.

Linux-Befehl „sudo“ ermöglicht Sicherheitsverletzungen

Im Februar wurde eine kritische Schwachstelle in der zunehmend beliebten Linux-Distribution „Ubuntu“ entdeckt. Der als CVE-2009-0034 bezeichnete Programmierfehler betrifft nur die Ubuntu-Versionen 8.04 und 8.10 und ermöglichte es Benutzern ohne Administratorrechte, Anwendungen als Root-Benutzer auszuführen oder Dateien anderer Benutzer zu manipulieren.

Der Befehl „sudo“ ist dazu gedacht, dass normale Systembenutzer ihre Rechte um Administratorrechte erweitern können. Damit diese Benutzer Software installieren oder systemübergreifende Änderungen vornehmen können, müssen sie in einer gesonderten Datei namens „sudoers“ eingetragen sein. Dieselbe Datei kann so konfiguriert werden, dass Benutzerkonten Programme mit den Rechten von anderen Benutzerkonten ausführen können (sodass z. B. Benutzer, die per Fernzugriff auf das System zugreifen, Druckaufträge ausführen können, als wären sie lokale Benutzer). Diese spezielle Art der Konfiguration kann für andere Benutzerkonten allerdings eine bedeutende Sicherheitsproblematik bedeuten.

Schlussfolgerungen

Die Entwicklung von Malware ist ein schnell avancierendes Geschäft, zum einen, weil die Programmierer dieser besonderen Art von Software von illegalem Profitstreben angetrieben werden, und zum anderen, weil sich die Technologie schnell weiterentwickelt.

Die meisten Softwareunternehmen arbeiten mit knappen Zeitvorgaben; je kürzer die Zeitspanne zwischen Produktplanung und Auslieferung an den Kunden, desto höher die Umsätze. Häufig werden solche Anwendungen aber nicht umfassend getestet oder hinsichtlich ihrer Anfälligkeit gegen Angriffe oder auf Programmierfehler überprüft.

Eine weitere Schwachstelle, die für die Verbreitung von Malware genutzt wird, ist der Endbenutzer, dessen mangelndes Bewusstsein für die neuesten Trends in der Malwarelandschaft sowohl auf seine Finanzen als auch hinsichtlich des Datenschutzes dramatische Auswirkungen haben kann.

Das freiwillige Preisgeben trivialer Informationen über Web-2.0-Websites oder Blog-Plattformen kann es böswilligen Dritten erleichtern, persönliche Profile zu erstellen oder zusätzliche Daten zu sammeln, die für Phishing-Versuche benutzt werden.

Um sicherzustellen, dass sich das Surfen im Internet für Sie als sicheres und angenehmes Erlebnis gestaltet, empfiehlt BitDefender, dass Sie eine umfassende Anti-Malware-Sicherheitslösung installieren, aktivieren und aktualisieren.

Rechtlicher Hinweis