So zockt Sie der Virus ab

Neuer Conficker noch aggressiver

Conficker-Schnelltest unter *www.pcwelt.de/196378*: **Nur wenn alle Bilder der oberen Reihe zu sehen sind, ist der PC nicht infiziert**

Jetzt rollt die Conficker-Angriffswelle doch: Gespannt erwarteten PC-Experten den 1. April, aber es passierte nichts. Doch knapp eine Woche später tauchte eine neue, noch gefährlichere Version des Schädlings auf – Conficker.E, auch Downadup oder Kido genannt.

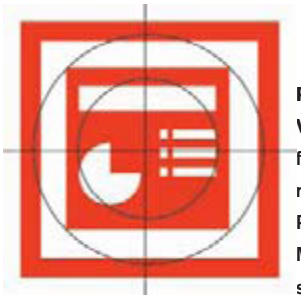
Die Kriminellen verteilen Conficker.E über eine verschlüsselte P2P-Update-Funktion. Nun lädt der Wurm eine Reihe von weiteren Schädlingen auf den Rechner, darunter den Spambot Waledac. Hinter diesem Schadcode steckt vermutlich die Sturm-Bande, denn Waledac gilt als Nachfolger des berüchtigten Sturm-Wurms. Diverse Trojanische Pferden nutzen Waledac zum Massenversand von Spammails. Die Sturm-Bande bietet den Schädling anderen Malware-Gruppen zur Nutzung an – gegen Entgelt. Ein Botnet von nur 100.000 Waledac-verseuchten PCs könnte nach Angaben von Kaspersky Lab (*www.kaspersky.de*) mehr als acht Milliarden Spammails am Tag versenden. Conficker-Verbreitung wird jedoch auf mehrere Millionen Rechner geschätzt.

Außerdem installiert Conficker.E die betrügerische Sicherheits-Software „Spyware Protect 2009“, mit der die Conficker-Programmierer wohl ebenfalls Geld verdienen. Das läuft vermutlich im Rahmen eines weiteren „Partnerprogramms“ mit anderen Kriminellen. Abgerechnet wird in solchen Fällen stets pro verseuchtem Rechner: So können auch bei nur einigen Cent pro PC erhebliche Summen zusammenkommen. Einen Conficker-Schnelltest finden Sie unter *www.pcwelt.de/196378*. **-fz**

Gezielte Angriffe

Powerpoint-Lücke

Eine neu entdeckte Schwachstelle in Microsoft Powerpoint nutzen Kriminelle für gezielte Angriffe mit präparierten Powerpoint-Dateien. Die PPS-Files erzeugen beim Öffnen in anfälligen Programmversionen einen Speicherüberlauf, der das Ablegen und Ausführen einer Programmdatei auf der Festplatte ermöglicht. Auf diesem Weg werden Trojanische Pferde eingeschleust. Microsoft hat in seiner Sicherheitsmitteilung 969136 die Lücke bestätigt: Betroffen sind Powerpoint 2000, 2002 und 2003 für Windows sowie Version 2004 für Mac-OS X. Ein Sicherheits-Update hatte Microsoft bei Redaktionsschluss noch nicht veröffentlicht. **-fz**



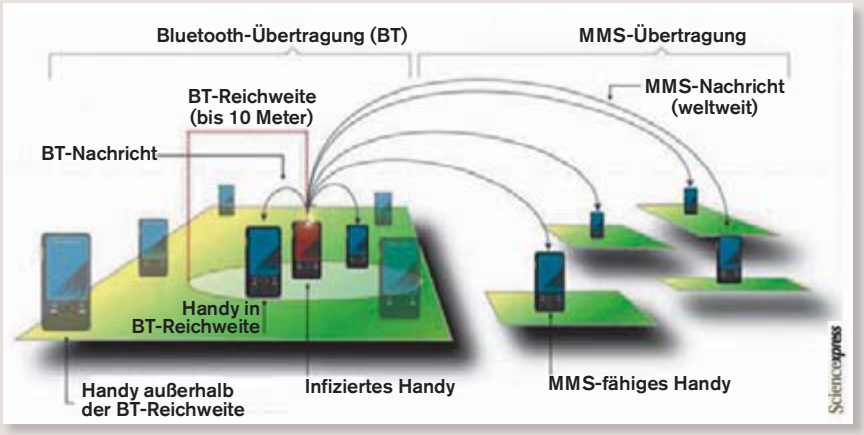
Powerpoint im Visier: Angreifer versuchen, mit präparierten PPS-Dateien, Malware einzuschleusen

Frage des Monats

Wie verteilt sich „Mobile Malware“?

Handys, Smartphones und PDAs stehen unter Schädlingsbeschuss. Wie sich der Schadcode auf den Mobilgeräten verbreitet, haben Wissenschaftler in Boston untersucht (*www.barabasilab.com*). Im Wesentlichen unterscheiden sie zwei Ausbreitungswege – Bluetooth-Funk und MMS.

Bluetooth hat eine Reichweite von wenigen Metern, kann jedoch innerhalb dieser Zone jedes anfällige Gerät erreichen. Ein erhöhtes Risiko besteht also in großen Menschenansammlungen. Bei MMS gibt es kein solches Reichweitenproblem – die Malware kann im Prinzip jedes MMS-fähige Gerät weltweit angreifen. Die Verbreitung wird jedoch dadurch eingeschränkt, dass MMS nur an bekannte Telefonnummern geschickt werden können. Als begrenzenden Faktor sehen die Forscher außerdem die Vielfalt der Betriebssysteme bei Mobilgeräten. **-fz**



Mobile Malware: Die Schädlinge breiten sich über MMS und Bluetooth auf Handys & Co. aus

Banking-Malware

Trojaner zerstören Windows

Der größte Teil der verbreiteten Schädlinge ist darauf aus, Zugangsdaten für Online-Dienste auszuspionieren, vor allem für Banken- und Spiele-Websites. Einige dieser Trojanischen Pferde gehen für dieses Ziel so weit, dass sie die Windows-Installation nachhaltig beschädigen. Die Folge: Das System bootet nicht mehr. So löschen beispielsweise Schädlingsfamilien wie Nethell (auch Ambler genannt), Infostealer oder Zeus (Zbot) auf Befehl ihrer Bot-Master wichtige Dateien, etwa Systemtreiber und Registry-Einträge. Durch den Schaden am System gewinnen die Täter Zeit und können die Konten der Opfer plündern, bevor diese den Betrug bemerken. **-fz**

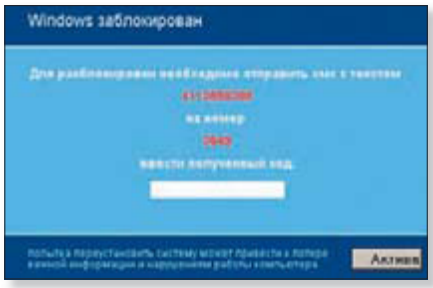
Erpresser-Malware blockiert den Desktop

Russische Malware fordert Lösegeld

Eine neue Variante erpresserischer Malware ist in Russland aufgetaucht. Der Schädling blockiert den Desktop des befallenen Rechners und verlangt den Versand einer SMS an die angegebene kostenpflichtige Nummer, damit der Anwender einen Freischalt-Code erhält. Erst nach Eingabe des Codes arbeitet der PC wieder korrekt.

Wie das Symantec Security Response Blog berichtet, handelt es sich um den Schädling „Trojan Ransomlock“. Er blockiert den gesamten Rechner und lässt sich weder per <Strg>-<Alt>-<Entf> noch mit Hilfe eines Neustarts ausschalten.

Symantec führt in dem Blog vor, wie sich ein gültiger Freischaltcode errechnen lässt, und bietet darüber hinaus ein Tool zum Entfernen des Schädlings an. Falls kein zweiter PC zum Herunterladen des Symantec-Programms zur Verfügung steht, gibt es noch eine weitere Möglichkeit: Man startet den Rechner mit Hilfe einer Boot-CD, die ein vollständiges Betriebssystem enthält, zum Beispiel Ubuntu oder Knoppix. Mehr Informationen finden Sie unter *www.pcwelt.de/196795*. **-fz/-tw**



Bei Anruf Code: Der Anwender soll eine SMS an eine bestimmte Nummer senden

Schützen Sie Ihren PC vor Angriffen!

Die neuesten Sicherheits-Updates

Neue Version	Risiko Vorversion
Adobe Reader 8.1.4	
Adobe Reader 9.1	
Google Chrome 1.0.154.53	
Filezilla FTP-Client 3.2.3	–
Firefox 3.0.8	
Adobe Flash Player 10.0.22.87	
Foxit PDF-Reader 3.0 Build 1506	
Internet Explorer MS09-014 (KB963027)	
iTunes 8.1.1	–
Java Runtime 1.6.0_13 (JRE 6 Update 13)	

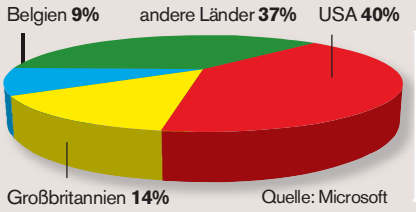
Neue Version	Risiko Vorversion
Opera 9.64	
Pidgin (Gaim) 2.5.5	–
Seamonkey 1.1.16	
Skype 4.0.0.224	–
Thunderbird 2.0.0.21	
VLC Player 0.9.9	–
Vmware Player 2.5.2, Workstation 6.5.2	
Winamp 5.551	
Windows Patch Day April	

– = keine Angabe = niedrig = mittel = hoch = kritisch Quelle: *wwww.pcwelt.de/c31*

MALWARE KOMPAKT

Microsoft bekämpft Koobface-Wurm

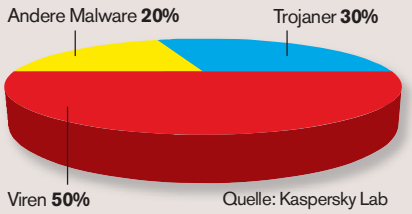
Der erstmals im Mai 2008 aufgetauchte Wurm Koobface macht sich vor allem im sozialen Netzwerk Facebook breit, neuere Versionen auch in anderen Netzen. Die Facebook-Betreiber arbeiten mit Microsoft zusammen, um den Schädling loszuwerden. Microsoft hat am Patch Day im März eine neue Version seines Antimalware-Tools bereitgestellt, die Koobface ins Visier nimmt. In den ersten zwei Wochen hat es den Wurm bereits auf knapp 200.000 PCs in 140 Ländern entfernt, vor allem in den USA (40 Prozent). **-fz**



Weg mit Koobface: Erstaunlich oft fand das Antimalware-Tool den Wurm auf PCs in Belgien

Conficker: Rang 1 in der Schädlingsliste

In der Hitliste der meistverbreiteten Schädlinge hat der Wurm Conficker, der auch Downadup oder Kido genannt wird, im März 2009 den ersten Platz übernommen. Insgesamt sind im März mehr als 45.000 unterschiedliche Malware-Dateien gemeldet worden – das sind ähnlich viele wie im Vormonat. Der Höchstplatzierte unter den Neu-Einsteigern ist „Trojan-Dropper.Win32.Flystud.ko“: Dabei handelt es sich um ein Trojanisches Pferd, das in der Scriptsprache Fly Studio geschrieben ist und aus China stammt. Die Schädlingsliste wird jeden Monat von Kaspersky Labs herausgegeben. **-fz**



Ungebremst: Viren machen auch im März 2009 die Hälfte der Schädlinge aus

UPDATE-TELEGRAMM

Firefox 3.5 ist Ende April als Beta 4 erschienen. Für die endgültige Version, die im Sommer veröffentlicht wird, sind noch einige Dutzend Fehler zu beheben (*www.mozilla.com*).

Firefox 3.6 („Namoroka") wird XP SP3, Vista oder Windows 7 voraussetzen. Die älteren Windows-Versionen 2000, XP SP1 und XP SP2 will Mozilla für den 2010 geplanten Browser voraussichtlich nicht mehr unterstützen.

Imgburn 2.4.4.0 enthält mehr als 30 Änderungen und Bugfixes gegenüber der Vorgängerversion. Es handelt sich ausnahmslos um kleine, spezielle Anpassungen der Brenn-Software (*www.imgburn.com*).

Miranda 0.7.19 arbeitet weiter an Stabilitätsproblemen nach der Anmeldung bei ICQ. Die jüngste Version der Multi-Messenger-Software war kurz nach Version 0.7.18 notwendig geworden (*www.miranda-im.org*).

MS Translator 1.0 integriert sich als Schaltfläche „Übersetzen" in die Komponenten von Microsoft Office 2003 und 2007 (*www.pcwelt.de/tl1*).

Microsoft Office für den Mac: Die 2004- und 2008-Updates enthalten neben den üblichen Sicherheits-Patches auch Leistungsverbesserungen für beide Office-Versionen.

Outlook Connector 12.1 integriert die Daten aus Windows Live (Kontakte, Kalender, Mail) in Outlook 2003 oder 2007. Die neue Version leistet dies laut Microsoft zuverlässiger und stabiler (*www.pcwelt.de/olc*).

PDF Creator 0.9.8 ist eine systemweite kostenlose Lösung zur Erstellung von PDF-Dateien inklusive optionaler Rechteverwaltung. Die jüngste Version nutzt das im Februar aktualisierte GPL-Ghostscript 8.64 (*www.pdfforge.org*).

Total Commander 7.50 ist als Public Beta 1 verfügbar. Der universale Dateimanager (Shareware) bietet in Version 7.50 unter anderem vollständige Unicode-Unterstützung, einen verbesserten FTP-Client, erweiterte Hotkey-Vergabe und die von Vista bekannte Breadcrumb-Navigation (*www.ghisler.com*).

Umfangreiches Office-Update

Office 2007 Service Pack 2 verfügbar

Große Teile von Office 2007 ersetzt das 287 MB umfassende Service Pack 2 für das Büro-Software-Paket von Microsoft. Neben den zahlreichen Sicherheits-Updates bringt es eine ganze Reihe funktionaler Verbesserungen. So speichern die Office-Programme optional oder auf Wunsch standardmäßig Dateien im Open Document Format (ODF) von Open Office, ferner als XML oder PDF. Fast alle Komponenten wurden leistungsoptimiert, insbesondere Outlook, Excel und Powerpoint. Generelle Beschleunigung verspricht Microsoft bei Bildern, Diagrammen und anderen grafischen Objekten.

Office wird offener: Mit SP2 kann die Büro-Software auch Open-Document-Formate speichern

Das SP2 für Office 2007 ist auf Vista SP2, Windows 7 und Server R2 getestet und damit für die Neuerungen der kommenden Monate gerüstet. Beim Test der noch inoffiziellen englischen Beta (siehe Abbildung) integrierte sich das Service Pack mühelos in wenigen Minuten, ohne Benutzerabfrage und ohne Neustart. Gibt es dennoch Probleme, bietet Microsoft als separaten Download erstmals ein Uninstall-Tool, das das SP2 im Bedarfsfall wieder entsorgt. Dies erspart eine komplette Neuinstallation. **-ha**

Microsoft-Patchday im April

Win-Lücke gestopft – nach einem Jahr

Viel zu spät: Erst der Patch Day im April 2009 stopfte eine Sicherheitslücke in allen Windows-Versionen, die bereits seit März 2008 (!) als „Token Kidnapping" bekannt ist. Eine Demo-Exploit namens „Churrasco2" hatte die Ausnutzbarkeit im Oktober 2008 nachgewiesen. Seitdem kann durch die Schwachstelle Malware auf Web-Server eingeschleust werden.

Mit dem kumulativen Update 963027 für den Internet Explorer (5 bis 7) löst Microsoft jetzt und damit sehr spät ein ebenfalls uraltes Sicherheitsproblem der „Safari Carpet Bomb" auch für die Windows-Seite. Apple hatte die Lücke bereits Mitte 2008 Browser-seitig mit Version 3.1.2 behoben. Allerdings war die Ausnützbarkeit dieser Lücke gering. **-fz/-ha**

Windows 7 Release Candidate

Die Vorab-Version ist fertig

Die Partnerseite von Microsoft (*https://partnerbeta.microsoft.com*) hat den Release Candidate von Windows 7 für den 5. Mai angekündigt. Für MSDN- und Technet-Abonnenten gibt es den Download der RC-Version voraussichtlich schon einige Tage früher. Einen weiteren Zwischenschritt zum endgültigen RTM (Release to Manufacturing) wird es laut Microsoft nicht mehr geben. Damit befindet sich Windows 7 zumindest technisch endgültig auf der Zielgeraden. **-ha**