Neueste Informationen zum Thema Viren am 1.9.2009

Harmlose Websites werden zu Gehilfen von Cyberkriminellen

Umleitungs-Trick: Wenn Google zur Virenfalle wird

Experten warnen regelmäßig davor, dass auch harmlose Websites mittlerweile den eigenen Computer infizieren können. Die Sicherheitsfirma Kaspersky hat jetzt eine neue Masche der Virenschreiber geschildert, bei der die Google-Suche unfreiwillig bei der Verbreitung der Schädlinge hilft.

http://www.netzwelt.de/news/79272-umleitungs-trick-google-virenfalle.html

Alle Browser-Versionen betroffen, noch kein Patch in Sicht

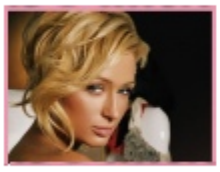
Globale Gefahr: Sicherheitslücken im Internet Explorer

Eine Sicherheitslücke bedroht aktuell Millionen von Nutzern des Internet Explorers. Noch hat Microsoft keine Aktualisierung für den Browser veröffentlicht und empfiehlt den Anwendern zweifelhafte Schutzmaßnahmen. Sicherheitsexperten raten zum Browserwechsel auf Zeit.

http://www.netzwelt.de/news/79161-globale-gefahr-sicherheitsluecken-internet-explorer.html

Insgesamt mehr als 15.000 Seiten von Sicherheitslücke betroffen

Homepage von Paris Hilton: Bei Besuch Virus



Auf der Homepage von Paris Hilton finden Besucher neben Informationen zum Star einen Schädling. Das berichtet die Sicherheitsfirma ScanSafe und warnt davor, Pop-Ups oder andere verdächtige Meldungen anzuklicken. Hiltons Web-Auftritt ist offenbar nur ein Fall von 15.000 infiltrierten Internetseiten.

Kein Einzelfall

Bei der Manipulation von Paris Hiltons Homepage scheint es sich nur um die Spitze des Eisbergs zu handeln: IT-Experten berichten von insgesamt 15.000 Websites weltweit, auf denen der gleiche Schadcode gefunden wurde - darunter auch der oft besuchte Web-Auftritt des *Major League Baseball* (MBL). Selbst wenn also die Sicherheitslücke auf ParisHilton.com geschlossen ist, könnte eine ähnliche gefälschte Warnung auch auf anderen Websites auftauchen.

http://www.netzwelt.de/news/79292-homepage-paris-hilton-besuch-virus.html

Diese Seite verrät, ob ihr System befallen ist oder nicht

Conficker: Einfacher Online-Test erkennt infizierte Computer

Der Windows-Wurm Conficker hat nach verschiedenen Schätzungen weltweit zwischen drei und zehn Millionen Computer befallen. Ein einfacher Test verrät, ob Ihr PC betroffen ist oder nicht. Für den Ernstfall existieren Lösungen.

http://www.netzwelt.de/news/79705-conficker-einfacher-online-test-erkennt-infizierte-computer.html

Britisches Fernsehmagazin erlangt Kontrolle über ferngesteuerte Computer

Für Fernsehreportage: BBC übernimmt Botnetz

Reporter der BBC-Sendung "Click" übernahmen nach eigenen Angaben die Kontrolle über ein Botnetz. Für eine Reportage über Internetkriminalität demonstrieren sie, wie Verbrecher die Zombie-Computer einsetzen.

http://www.netzwelt.de/news/79604-fernsehreportage-bbc-uebernimmt-botnetz.html

Was tun bei einem Infekt?

Wenn Sie glauben, dass Conficker Ihren PC befallen hat, können Sie Ihrem Antivirenprogramm nur bedingt vertrauen. Zwar geben die Hersteller der Sicherheitsprogramme an, dass sie inzwischen zu über 90 Prozent Conficker erkennen und entsprechende Maßnahmen wie eine Quarantäne oder eine Warnung an den Benutzer einleiten. Dies gilt aber nur, wenn die Software auf dem neuesten Stand ist. Antivirenprogramme, die schon länger nicht aktualisiert worden sind, kann Conficker ausschalten und so unbemerkt auf dem System verbleiben.

Ähnliche Artikel
- Conficker: **Bundeswehr kämpft gegen Computerwurm**
- Conficker: **Diese Programme entfernen den Computer-Virus**
- 250.000 Dollar Kopfgeld: **Microsoft jagt "Conficker"-Autor**

Konkret bedeutet das: Aktualisieren Sie Ihren Virenschutz. Sollte dies nicht möglich sein oder Sie immer noch glauben, dass Ihr PC befallen ist, gibt es zwei weitere Möglichkeiten: Die radikalste und sicherste Maßnahme wäre eine komplette Neuinstallation von Windows. Alternativ können Sie sich eines der Programme herunterladen, die die Hersteller von Sicherheitssoftware zur Entfernung von Conficker bereitstellen. Bei Verwendung der Programme ist aber zu beachten, dass ein einmal infiziertes System auch nach einer Reinigung weiterhin als kompromittiert gilt.

Trojaner-Tausendsassa

Der Grund für die Effizienz des Schädlings liegt in seinem komplexen Verhalten. Einmal auf dem System, vervielfältigt sich Conficker in Verzeichnissen von Movie Maker, Internet Explorer sowie in temporären und System-Ordnern von Windows. Zusätzlich erstellt er für sich selbst einen Autostart-Eintrag - so gehen die Virenschreiber sicher, dass der Schädling bei jedem Start des Betriebssystems auf der Matte steht.

Ähnliche Artikel

- 250.000 Dollar Kopfgeld: **Microsoft jagt "Conficker"-Autor**
- Conficker: **Bundeswehr kämpft gegen Computerwurm**
- Conficker: **Diese Programme entfernen den Computer-Virus**

Doch wo andere Viren schon Schluss machen, legt Conficker erst richtig los - und das macht ihn so unberechenbar. Der Wurm hängt sich an die wichtigen System-Prozesse *svchost.exe, explorer.exe* und *services.exe* und deaktiviert auf der anderen Seite ein halbes Dutzend Dienste, die normalerweise auf dem Computer für die Sicherheit und Fehlermeldungen zuständig sind.

16.01.2009 powered by

Trickreicher Schädling infiziert 2,5 Millionen Systeme

Conficker: Wenn ein Windows-Wurm Katz und Maus spielt

Sicherheit

Auf zu neuen Ufern

In der System-Bibliothek von Windows, der Registry, verwischt Conficker seine Spuren: Die Firewall wird umgangen, Windows Defender und Sicherheitswarnungen werden deaktiviert und Wiederherstellungspunkte gelöscht. Gibt der Nutzer eines befallenen Rechners Domain-Namen in seinen Browser ein, die mit Sicherheit oder einem Virenscanner zu tun haben, blockiert der Wurm den Zugriff.

Zu diesem Zeitpunkt hat Conficker das Betriebssystem unterwandert, Registry und Dienste manipuliert und den Kontakt zur Außenwelt abgeschnitten. Doch all das ist nur eine Vorsichtsmaßnahme. Denn wirklich gefährlich wird der Wurm erst jetzt: Er öffnet in dem geschwächten System einen zufällig gewählten Port, richtet einen HTTP-Server ein und ist so in der Lage, weitere Schädlinge ohne Wissen des Nutzers nachzuladen. Und diese können den PC dann fernsteuern, persönliche Daten sammeln und mehr - ein fremdbestimmtes Botnetz entsteht.

Um diesen Effekt zu verstärken, sucht Conficker selbstständig im Netzwerk nach anderen Computern, die er infiltrieren kann. Ist der Rechner mit einem schwachen Administratoren-Kennwort gesichert, knackt der Schädling das Kennwort dank mitgelieferter Standard-Phrasen in Sekundenschnelle. Dort macht er es sich dann nach Schema F gemütlich.

Quelle: http://www.netzwelt.de/news/79324_2-conficker-windows-wurm-katz-maus-spielt.html

Aufpassen und Passwörter

Zwar sind viele Privatnutzer mit diesem vielschichtigen Verhalten des Wurms überfordert, doch den größten Schaden richtet Conficker in Unternehmens-Netzwerken an. Hier sind oft hunderte Windows-Rechner miteinander verbunden und nicht immer mit den aktuellsten Sicherheits-Aktualisierungen versorgt. Zudem lässt sich auch ein gut gesichertes Netzwerk durch einen USB-Stick mit infizierten Dateien unbeabsichtigt unterwandern.

Ähnliche Artikel
- Conficker: **Bundeswehr kämpft gegen Computerwurm**
- 250.000 Dollar Kopfgeld: **Microsoft jagt "Conficker"-Autor**
- Conficker.A: **Microsoft warnt vor Windows-Wurm**

Zwar sind alle gängigen Virenscanner und auch Windows selbst mittlerweile auf der Hut, was Conficker betrifft. Dieser Schutz funktioniert aber nur bei Nutzern, die Virendefinitionen auf dem neuesten Stand halten und die über *Windows Update* verteilten Aktualisierungen installieren. Am Firmen-Rechner ist ein starkes Passwort Pflicht, damit sich der Wurm nicht unbefugten Zutritt verschafft.

Sicherheitslücke in Windows-Systemen bereitet große Sorgen

Conficker.A: Microsoft warnt vor Windows-Wurm

Sicherheit

Ein Wurm mit der Bezeichnung Win32/Conficker.A bereitet Microsoft zurzeit Kopfzerbrechen. Dieser nutzt eine Sicherheitslücke im Windows-Server-Dienst "SVCHOST.EXE", nistet sich unter wechselnden Namen, als dll-Datei, auf den betroffenen Rechnern ein und setzt sich zusätzlich in der Registry fest. Nach erfolgreichem Entern baut er einen Webserver auf und öffnet dabei einen beliebigen Port zwischen 1.024 und 10.000.

Laut Microsoft verbreitet er sich über diese offenen Türen dann auf andere Rechner, wobei es egal ist, ob man sich mit dem Firmennetzwerk oder dem Internet vernetzt hat. Die Schwachstelle, die Conficker.A nutzt, sorgte schon 2003 für ordentlich Unruhe. Damals hat es der Wurm W32.Blaster, auch W32.Lovsan oder MSBLAST genannt, auf die Rechner geschafft und konnte in kürzester Zeit über eine halbe Million PCs lahm legen.

Wurm bring Sicherheitspatch gleich mit

Das Interessante bei dieser Wurm-Variante: Ist der Server-Dienst erst einmal ausgetrickst, spielt der Wurm den benötigten Sicherheits-Patch selbst auf das System, wobei die Sicherheitslücke damit nicht geschlossen ist. Lediglich andere Würmer werden daran gehindert, das System zu befallen.

Als wenn das noch nicht reichen würde, nimmt er nebenher noch Kontakt mit Internetseiten auf, um deren nach außen erscheinende IP-Adresse und aktuelle Zeit zu ermitteln. Über diese Abfrage ist der Wurm in der Lage, eine Liste von Domains zu erstellen, um dann über die gesammelten Seiten weitere Codes nachzuladen - ähnlich wie bei den Rechner selbst.

Updates und Firewall helfen

Ähnliche Artikel
- 250.000 Dollar Kopfgeld: **Microsoft jagt "Conficker"-Autor**
- Conficker: **Bundeswehr kämpft gegen Computerwurm**
- Conficker: **Diese Domains legt der Wurm im März lahm**

Dem Wurm kann man mit dem aktuellen Sicherheits-Update von Microsoft Einhalt gebieten. Auf dem Windows-Rechner sollten daher *Automatische Updates* immer aktiviert sein. Aber auch eine Firewall ist ein Muss auf jedem Rechner. Die seit Windows XP integrierte Firewall reicht für eine Abwehr aus. Nutzer sollten dennoch die Firewall-Einstellungen überprüfen, ob nicht doch irgendwelche Port-Ausnahmen den Zugriff auf solche Dienste erlauben. Eine beliebte Ausnahme ist etwa die Datei- und Druckerfreigabe.

Stand: 29.08.2009