

Meldung | Nachrichten | News & Facts | Pressemitteilung

© powered by premiumpresse.de

<http://www.premiumpresse.de/bitdefender-top-10-im-november-autoruninf-an-der-spitze-der-bedrohungscharts-PR638846.html>

BitDefender Top 10 im November: AutorunINF an der Spitze der Bedrohungscharts

(openBroadcast) - E-Threat-Report: Clicker nicht mehr der gefährlichste Trojaner

Holzwickede, 04. Dezember 2009 – Die Herrschaft von Clicker unter den gefährlichsten Malware-Bedrohungen ist (vorerst) zu Ende. Fünf Monate in Folge belegte der Trojaner Rang eins der BitDefender E-Threat-Top 10. Im November tauscht er die Plätze mit AutorunINF, der zu seiner Verbreitung die Autorun-Funktion im Windows-Betriebssystem missbraucht. Mit dieser Strategie ist er innerhalb der Top 10 nicht allein. Gleich drei Trojaner nutzen diese Windows-Schwachstelle. Conficker hält dagegen Position drei und legt an Infektionsrate leicht zu. Trojan.Inject.RA und Trojan.Downloader.Bredolab.AZ sind die Neueinsteiger des Monats auf den Plätzen neun und zehn.

Trojan.AutorunINF.Gen (8,45 Prozent Infektionsrate) nutzt zur Verbreitung ein autorun.ini-Skript, über das alle Wechseldatenträger standardmäßig verfügen. Über diese Funktion wird eine bestimmte Datei nach dem Anschluss des Datenträgers an den PC automatisch ausgeführt. Malware-Autoren nutzen diese Windows-Funktion und manipulieren solche Dateien, um schädliche Anwendungen zu starten, ohne dass der User etwas merkt.

Trojan.Clicker.CM (7,87 Prozent) verliert 1,6 Prozentpunkte im Vergleich zum Vormonat. Dieser Trojaner versteckt sich überwiegend auf Websites, die illegale Anwendungen wie Cracks, Keygens und Seriennummern zum Download anbieten. Conficker (offizielle Bezeichnung: Win32.Worm.Downadup.Gen) ist im November für 5,62 Prozent der weltweiten Infektionen verantwortlich, womit er Platz drei belegt. Der Wurm beschränkt den Zugang zu Webseiten von IT-Security-Anbietern und verweigert Usern die Ausführung von Windows-Updates. Neuere Varianten des Schädlings installieren zusätzlich fehlerhafte „Security-Software“.

Auch Trojan.Wimad hält mit dem vierten Platz und exakt 5 Prozent Infektionsrate die Position. Der Trojaner infiziert vor allem Advanced System Format(ASF)-Dateien mit einem Codec, um weitere Schädlinge nachzuladen. Diesem Trojaner folgt mit nur wenig Abstand auf Rang fünf Exploit.PDF-JS.Gen (3,23 Prozent). Dieser Exploit nutzt verschiedene Sicherheitslücken in Javascript-Engines des Adobe PDF Reader. Auf dem PC führt er bösartige Codes aus, die wiederum den Download schädlicher Binaries auslösen.

Win32.Sality.OG belegt mit 2,57 Prozent den sechsten Rang. Der polymorphe Datei-Infector schleust seinen verschlüsselten Code über exe- und scr-Dateien ein. Um seine Präsenz auf dem infizierten Computer zu verbergen, verwendet er ein Rootkit und versucht Antivirus-Anwendungen auf dem PC stillzulegen. Auf Platz sieben und acht folgen mit Trojan.Autorun.AET (2,05) und Worm.Autorun.VHG (1,59) zwei Schädlinge, die es – wie der Name bereits verrät – ebenfalls auf die Autorun-Funktion in Windows abgesehen haben. Ersterer verbreitet sich über in Windows freigegebene Ordner sowie durch Wechseldatenträger. Worm.Autorun.VHG ist ein Internet- und Netzwerk-Wurm, der die Windows-Schwachstelle MS08-067 ausnutzt.

Neueinsteiger Trojan.Inject.RA (1,45 Prozent) auf Position neun ist ein Passwort-stehlender Trojaner, der es meist auf Spieler des Fantasy-Games Lineage II abgesehen hat. Diese spezielle Trojaner-Variante verfügt über eine Keylogger-Komponente, die Tastatureingaben abfängt und sie via HTTP oder SMTP-Protokolle an die Angreifer zurückschickt. Trojan.Downloader.Bredolab.AZ (10. Platz, 1,20 Prozent) ist der zweite neue Threat in den BitDefender Top 10. Als Microsoft-Word-Dokument getarnt, installiert der Trojaner eine DLL-Datei und registriert sie als „Browser Helper Object“. Anschließend überwacht auch er die Tastatureingaben des Benutzers über eine Keylogger-Komponente und sendet die Daten an eine Website in Russland.

Top Ten des BitDefender-E-Threat-Report im November 2009:

Position	Name	Anteil in Prozent
----------	------	-------------------

- | | | |
|---|-------------------------|------|
| 1 | Trojan.AutorunINF.Gen | 8,45 |
| 2 | Trojan.Clicker.CM | 7,87 |
| 3 | Win32.Worm.Downadup.Gen | 5,62 |
| 4 | Trojan.Wimad.Gen.1 | 5,00 |
| 5 | Exploit.PDF-JS.Gen | 3,23 |
| 6 | Win32.Sality.OG | 2,57 |
| 7 | Trojan.Autorun.AET | 2,05 |
| 8 | Worm.Autorun.VHG | 1,59 |
| 9 | Trojan.Inject.RA | 1,45 |

10 Trojan.Downloader.Bredolab.AZ 1,20

Andere 60,97

Über BitDefender®

BitDefender ist Softwareentwickler einer der branchenweit schnellsten und effizientesten Produktlinien international zertifizierter Sicherheitssoftware. Seit der Gründung des Unternehmens im Jahr 2001 hat BitDefender permanent neue Standards im Bereich des proaktiven Schutzes vor Gefahren aus dem Internet gesetzt. Tagtäglich beschützt BitDefender viele Millionen Privat- und Geschäftskunden rund um den Globus und gibt ihnen das gute Gefühl, dass ihr digitales Leben sicher ist. BitDefender vertreibt seine Sicherheitslösungen in mehr als 100 Ländern über ein globales VAD- und Reseller-Netzwerk. Ausführlichere Informationen über BitDefender und BitDefender-Produkte sind online im Pressecenter verfügbar. Zusätzlich bietet BitDefender in englischer Sprache unter www.malwarecity.com Hintergrundinformationen und aktuelle Neuigkeiten im täglichen Kampf gegen Bedrohungen aus dem Internet.

Pressekontakt

Pressekontakt:

BitDefender GmbH

Robert-Bosch-Str. 2

D-59439 Holzwickede

Ansprechpartner:

Hans-Peter Lange

PR-Manager

Tel.: +49 (0)2301 – 9184-330

Fax: +49 (0)2301 – 9184-499

