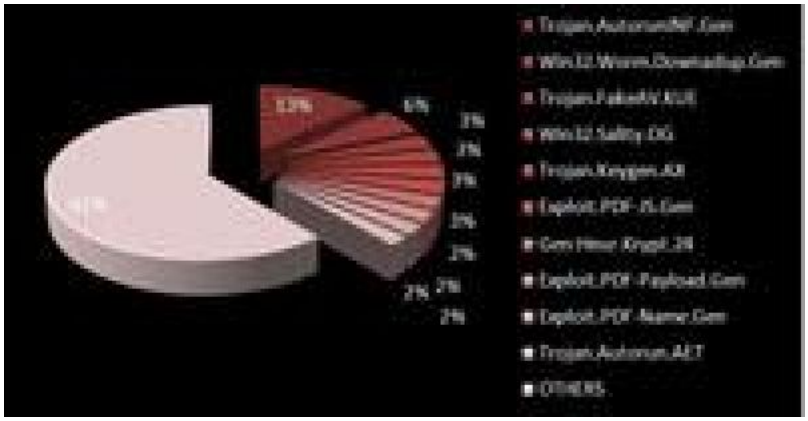
Drei PDF-Exploits in den BitDefender-Top 10 im April

06.05.2010, 13:21 | IT, New Media & Software

Pressemitteilung von: *BitDefender GmbH*



Top Ten des BitDefender E-Threat-Report im April 2010

AutorunINF.Gen mit großem Vorsprung gefährlichster E-Threat des Monats – Neuer Fake-Trojaner steigt auf Platz 3 ein

Holzwickede, 06. Mai 2010 – Das Feld der weltweit bedrohlichsten E-Threats rückt näher zusammen. Im aktuellen BitDefender-Ranking (bitdefender.de) liegen der drittplatzierte Neueinsteiger Trojan.FakeAV.KUE und der letztplatzierte Trojaner Autorun.AET bei der Infektionsrate nur 0,67 Prozentpunkte auseinander. Vorne weg marschiert mit großem Vorsprung AutorunINF, gefolgt vom altbekannten Conficker. Zudem hat sich ein weiterer PDF-Infektor unter die Top 10 gemischt. Somit nutzen bereits drei Exploits Sicherheitslücken im Adobe-Reader aus.

Zum dritten Mal in Folge ist AutorunINF der weit verbreitetste Schädling des Monats. Dabei hält der Trojaner, der über Wechseldatenträger fremde Rechner kompromittiert, mit 13,21 Prozent Infektionsrate das Niveau des März-Rankings. Conficker (5,77 %) verliert leicht bleibt aber auf Rang 2 – ein Zeichen, dass immer noch zu wenige User regelmäßig ihren PC updaten, um Sicherheitslücken in Windows zu schließen.

Mit Trojan.FakeAV.KUE (2,72 %) steigt ein neuer Threat gleich auf Position 3 ein. Diese Bedrohung belästigt den PC-Nutzer mit gefakten Warnmeldungen und bewirbt ein gefälschtes Antivirusprogramm, dass der User kaufen soll. Verbreitet wird der Schädling über bösartige oder bereits verseuchte legale Websites. FakeAV teilt sich Rang 3 mit „Top 10-Stammgast“ Win32.Sality.OG. Dieser Datei-Infektor verfügt zusätzlich über eine Rootkit-Komponente, die Sicherheitssoftware auf dem infizierten Rechner deaktiviert. Der zweite Newcomer des Monats ist Trojan.Keygen.AX auf Position 5 (2,66 %). Wie der Name schon preisgibt, verbreitet sich dieser Trojaner über illegale Websites, auf denen Cracks, Patches und Keygens zum Download angeboten werden.

Von den folgenden vier Plätzen werden drei allein von Exploits eingenommen, die Sicherheitslücken im Adobe pdf-Reader ausnutzen. PDF-JS.Gen positioniert sich dabei auf Rang 6 (2,57 %). Dieser Schädling manipuliert den Javascript-Engine des Adobe-Tools und führt so seinen schädlichen Code auf dem jeweiligen Rechner aus. In derselben Art und Weise verseuchen PDF-Payload (2,34 %) und PDF-Name (2,12 %) auf den Plätzen 8 und 9 fremde Rechner weltweit.

Gen:Heur.Krypt.24 (auch bekannt unter der Bezeichnung Worm.P2P.Palveo.AT) unterbricht die Exploit-Parade und belegt Platz 7 in den BitDefender-Top 10. Im April ist er für 2,38 % aller weltweiten Virusinfektionen verantwortlich.

Der Schädling verbreitet sich über Wechseldatenträger, Instant Messenger oder Peer-to-peer-Plattformen. Er injiziert seinen Schadcode in die explorer.exe-Datei, um sich so zu tarnen und für den PC-User unentdeckt zu bleiben. Die Top 10 beschließt der bekannte Trojaner Autorun.AET, der somit im Ranking weiter abrutscht, auch wenn er im Vergleich zum Vormonat leicht an Prozentpunkten zulegt (2,05 %). Er gehört zur gleichen Familie wie der Spitzenreiter der aktuellen Top 10.

Weitere Informationen unter: www.bitdefender.de.

Top Ten des BitDefender-E-Threat-Report im April 2010:

Position Name Anteil
in Prozent (Vormonat)
in Prozent
1 Trojan.AutorunINF.Gen 13,21 (13,40)
2 Win32.Worm.Downadup.Gen 5,77 (6,19)
3 Trojan.FakeAV.KUE 2,72 (Neueinsteiger)
3 Win32.Sality.OG 2,72 (2,58)
5 Trojan.Keygen.AX 2,66 (Neueinsteiger)
6 Exploit.PDF-JS.Gen 2,57 (5,30)
7 Gen:Heur.Krypt.24 2,38 (Neueinsteiger)
8 Exploit.PDF-Payload.Gen 2,34 (1,67)
9 Exploit.PDF-Name.Gen 2,12 (Neueinsteiger)
10 Trojan.Autorun.AET 2,05 (1,95)
Andere 61,40 (61,61)

Portrait

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.