

Überraschung im BitDefender Malware-Ranking: Trojaner Clicker nicht mehr unter den ersten Zehn

Holzwickede, 04. März 2010 – Viel Bewegung im aktuellen BitDefender E-Threat-Report (www.bitdefender.de): Gleich drei Neueinsteiger mischen sich im Februar unter die weltweit gefährlichsten Malware-Bedrohungen. Exploit.PDF-Payload.Gen belegt sogar auf Anhieb Rang vier. Für eine kleine Sensation sorgt dagegen Clicker. Noch im Vormonat auf Position eins und im gesamten vergangenen Jahr stets unter den ersten drei platziert, ist der bekannte Trojaner plötzlich nicht mehr in den Top 10 zu finden.

Mit vier Trojanern, drei Exploits, zwei Würmern und einem Virus ist das BitDefender-Ranking im Februar bunt gemischt. Vom überraschenden Clicker-Absturz profitieren die nun führenden AutorunINF und Downadup (auch bekannt als Conficker). Ersterer belegt mit 9,09 % weltweiter Infektionsrate Platz eins. „Die Verbreitungstaktik von AutorunINF über tragbare Speichermedien wie USB-Sticks oder Flash Drives etc. stellt für PC-User weiterhin eine große Gefahr dar. Aus diesem Grund sollten auch externe Geräte umfassend und regelmäßig auf Malware geprüft werden“, unterstreicht Catalin Cosoi, Senior Spam-Forscher bei BitDefender.

Conficker auf Platz zwei kann im Vergleich zum Vormonat wieder leicht an Infektionsrate zulegen (6,24 %). Die beiden folgenden Positionen belegen zwei pdf-Exploits: Neben PDF-JS.Gen (5,13 %) auf Rang drei ist PDF-Payload.Gen (4,21 %) als neue Bedrohung gleich auf Platz vier eingestiegen. Beide nutzen Schwachstellen im Javascript-Engine von Adobes PDF-Reader aus, um ihren schädlichen Code auf dem betroffenen PC auszuführen.

Zu den beliebtesten Verbreitungsquellen der Cyberkriminellen gehören weiterhin Torrent-Websites, wie der fünftplatzierte Trojan.Wimad.Gen1 (3,37 %) zeigt. Ihm folgt mit Win32.Sality.OG (Rang sechs; 2,77 %) der einzige Datei-Infektor in den Februar-Top 10. Diese Malware-Familie ist auf Grund ihres sich ständig verändernden Codes nur sehr schwer zu entdecken und zu beseitigen. Zudem versucht die Rootkit-Komponente dieses Threats, auf dem System vorhandene Security-Software zu deaktivieren.

Auf die Windows-Autorun-Funktion haben es Trojan.Autorun.AET (Rang sieben; 1,92 %) und Worm.Autorun.VHG (Rang acht; 1,85 %) abgesehen – beides Stammgäste in den BitDefender-Top 10. Freigegebene Netzwerkordner sowie externe Speichermedien sind die „Spielplätze“ dieser Schädlinge. Letzterer versteckt sich so lange auf dem infizierten System, bis er über einen speziellen „Remote Procedure Call“ (RPC) via Fernzugriff aktiviert wird.

Zwei Neueinsteiger beschließen das Februar-Ranking: Der Exploit Comele.A rangiert mit 1,48 % Infektionsrate auf dem neunten Platz. Eine Sicherheitslücke im Internet Explorer ist der Grund für seine weltweite Verbreitung. „Die Präsenz dieses Exploits zeigt, dass viele User immer noch zu selten ihr System updaten, denn diese Sicherheitslücke wurde von Microsoft bereits vor einigen Wochen mit Hilfe eines Patches geschlossen“, erklärt Cosoi. Trojan.SWF.HeapSpray.B belegt knapp dahinter mit 1,40 % den zehnten Platz. Sein Schadcode hat es auf den Datenspeicher des jeweils befallenen PCs abgesehen.

Weitere Informationen unter: www.bitdefender.de.

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

Position	Name	Anteil in Prozent	(Vormonat) in Prozent
1	Trojan.AutorunINF.Gen	9,09	(8,17)
2	Win32.Worm.Downadup.Gen	6,24	(6,18)
3	Exploit.PDF-JS.Gen	5,13	(5,76)
4	Exploit.PDF-Payload.Gen	4,21	(Neueinsteiger)
5	Trojan.Wimad.Gen.1	3,37	(4,30)
6	Win32.Sality.OG	2,77	(2,73)
7	Trojan.Autorun.AET	1,92	(2,01)
8	Worm.Autorun.VHG	1,85	(1,69)
9	Exploit.Comele.A	1,48	(Neueinsteiger)
10	Trojan.SWF.HeapSpray.B	1,40	(Neueinsteiger)
	Andere	62,53	(58,01)

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 schützt 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:

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
E-Mail: presse@bitdefender.de

PR-Agentur:
Sprengel & Partner GmbH
Nisterstraße 3
D-56472 Nisterau

Ansprechpartner:
Fabian Sprengel
Tel.: +49 (0)2661 – 91260-0
E-Mail: bitdefender@sprengel-pr.com