

E-Threat-Report im Mai: Spitzenquartett unverändert – Trojaner FakeAV legt deutlich zu – drei Neueinsteiger

Autorun-Trojaner belegen drei Plätze in den BitDefender Schädlings-Top 10

Holzwickede, 14. Juni 2010 – Die Strategie der Autorun-Trojaner bleibt weltweit eine der erfolgreichsten Infektionsmethoden. Dies zeigt der aktuelle BitDefender E-Threat-Report (www.bitdefender.de), in dem sich gleich drei Mitglieder dieser Schädlingsgattung befinden. AutorunINF führt die Top 10 weiter mit deutlichem Vorsprung an, gefolgt von Conficker. Nur knapp dahinter positioniert sich FakeAV, der seine Infektionsrate des Vormonats nahezu verdoppeln konnte. Drei Top 10-Neueinsteiger komplettieren das Ranking im Mai.

Die Autorun-Funktion in Windows wurde in den vergangenen Jahren schon häufig als Grundlage für Malware-Attacken missbraucht. Aus diesem Grund hat Microsoft das Feature ab der Version Windows Vista SP2 abgeschafft. User früherer Betriebssysteme bleiben jedoch weiterhin gefährdet, was die konstant hohe Infektionsrate von Trojan.AutorunINF.Gen (13,24 %, Rang 1) unterstreicht. Weitere Vertreter der „Autorun-Familie“ sind auf Position 6 und 8 zu finden: Trojan.Autorun.AET steigt neu in die Top 10 ein und ist für 2,02 Prozent an weltweiten Infektionen verantwortlich. Worm.Autorun.VHG liegt mit 1,97 Prozent nur knapp hinter seinem „Bruder“. Der Internet-/Netzwerk-Wurm kann über einen speziellen „Remote Procedure Call“ (RPC) via Fernzugriff ausgeführt werden.

Als Conficker-Wurm bekannt, legt Downadup leicht gegenüber dem Vormonat zu und hält Platz 2 mit 5,84 Prozent. Überraschend konnte April-Neueinsteiger Trojan.FakeAV.KUE seine Infektionsrate von 2,72 auf 5,11 Prozent erhöhen. Dies verdeutlicht, wie viele Nutzer auf die gefakten Warnmeldungen hereinfließen, mit denen der Trojaner gefälschte Antivirenprogramme bewirbt. Verbreitet wird FakeAV über bösartige oder bereits verseuchte legale Websites. Der einzige Datei-Infektor im Feld der gefährlichsten E-Threats bleibt Win32.Sality.OG auf Platz 4 (2,68 %). Mit Hilfe einer speziellen Rootkit-Komponente deaktiviert dieser Schädling Sicherheitssoftware auf dem kompromittierten PC.

Höchster Neueinsteiger in den BitDefender-Top 10 ist Gen:Variant.Swizzor.2 auf Position 5 (2,12 %). Dieser Trojaner installiert ein Download-Tool auf dem jeweiligen Rechner, um weitere hochgefährliche Malware nachzuladen.

Sowohl Palevo (offizielle Bezeichnung Gen:Heur.Krypt.24) auf Rang 7 als auch Neueinsteiger Gen:Variant.Rimecud.2 auf Platz 9 verbreiten sich über Wechseldatenträger, Instant Messenger oder Peer-to-peer-Plattformen. Cyberkriminelle nutzen diese beiden Schädlinge vor allem zum Stehlen von Passwörtern. Eine integrierte Backdoor-Komponente erlaubt den Angreifern den Remote-Zugriff auf fremde PCs.

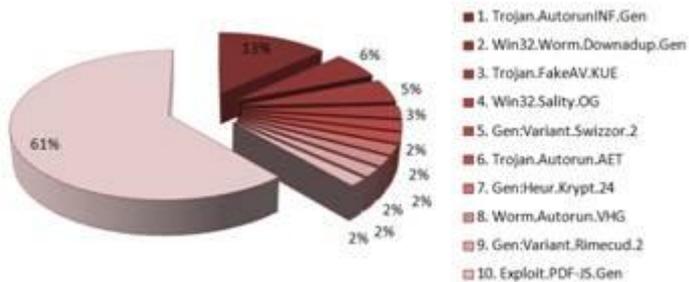
Schlusslicht PDF-JS.Gen hat in diesem Monat mit Autorun.AET die Plätze getauscht. 1,76 Prozent an weltweiten Infektionen bedeuten Rang 10. Der Exploit manipuliert den Javascript-Engine des Adobe PDF-Reader und injiziert so seinen schädlichen Code auf dem jeweiligen Rechner.

Weitere Informationen unter: www.bitdefender.de.

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

Position	Name	Anteil in Prozent	(Vormonat) in Prozent
1	Trojan.AutorunINF.Gen	13,24	(13,21)
2	Win32.Worm.Downadup.Gen	5,84	(5,77)
3	Trojan.FakeAV.KUE	5,11	(2,72)
3	Win32.Sality.OG	2,68	(2,72)
5	Gen:Variant.Swizzor.2	2,12	(Neueinsteiger)
6	Trojan.Autorun.AET	2,02	(2,05)
7	Gen:Heur.Krypt.24	2,01	(2,38)

8	Worm.Autorun.VHG	1,97	(Neueinsteiger)
9	Gen:Variant.Rimecud.2	1,91	(Neueinsteiger)
10	Exploit.PDF-JS.Gen	1,76	(2,57)
	Andere	61,33	(61,40)



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:

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