

Online-Spieler weiterhin im Fadenkreuz der Cyberkriminellen

Kaspersky Lab Top 20 der Schadprogramme, Dezember 2009

Moskau/Ingolstadt, 14. Januar 2009 – Kaspersky Lab präsentiert für den Dezember 2009 seine zwei Top-20-Listen der häufigsten Schädlinge. Die mit Hilfe des Kaspersky Security Network (KSN) gewonnenen Daten basieren auf Rückmeldungen der Heimanwender-Programme Kaspersky Anti-Virus und Kaspersky Internet Security. Aufgelistet werden zum einen die am weitesten verbreiteten Schad- und Werbeprogramme. Zum anderen zeigt die Aufstellung, mit welchen Schadprogrammen die Anwendercomputer am häufigsten infiziert waren.

Die erste Hitliste zeigt die am weitesten verbreiteten Schad- und Werbeprogramme (Malware und Adware), die auf den Computern der Anwender entdeckt und entfernt wurden:

Position	Positionsänderung	Name
1	0	Net-Worm.Win32.Kido.ir
2	0	Net-Worm.Win32.Kido.iq
3	0	Net-Worm.Win32.Kido.ih
4	0	Virus.Win32.Sality.aa
5	0	Worm.Win32.FlyStudio.cu
6	Neu	not-a-virus:AdWare.Win32.GamezTar.a
7	-1	not-a-virus:AdWare.Win32.Boran.z
8	-1	Trojan-Downloader.Win32.VB.eq1
9	-1	Trojan-Downloader.WMA.GetCodec.s
10	Neu	Trojan.Win32.Swizzor.c
11	Neu	Trojan-GameThief.Win32.Magania.cpct
12	-3	Virus.Win32.Virut.ce
13	-3	Virus.Win32.Induc.a
14	0	Trojan-Dropper.Win32.Flystud.yo

15	3	Packed.Win32.Krap.ag
16	-3	Packed.Win32.Black.a
17	0	Worm.Win32.Mabezat.b
18	-2	Packed.Win32.Klone.bj
19	-7	Packed.Win32.Black.d
20	-5	Worm.Win32.AutoRun.oui

In dieser Top-20-Liste gab es – wie so oft – kaum Veränderungen. Interessant ist aber das im November bereits aufgetauchte Programm Packed.Win32.Krap.ag, das im Dezember vom 18. auf den 15. Platz stieg. Hierbei handelt es sich um einen speziellen Packer von Schadprogrammen, die sich als gefälschte Antivirus-Programme entpuppen. Die von Kaspersky Lab entdeckten Krap-Schadprogramme dieser Art sind im Dezember ebenfalls weiter gestiegen. Dies zeigt, dass gefälschte Antivirus-Programme bei Cyberkriminellen nach wie vor sehr beliebt sind. Der Grund: Die Betrüger können diese Schadprogramme effektiv verbreiten und so große Gewinne erzielen.

Ein bemerkenswerter Neuling im Dezember ist das Werbeprogramm GamezTar.a, das sofort auf den sechsten Platz eingestiegen ist. Dieses Programm ist als Toolbar für populäre Browser getarnt, verspricht den schnellen Zugang zu Online-Spielen und bringt unerwünschte Werbebanner auf den Bildschirm. Zudem installiert es Anwendungen, die unabhängig vom Toolbar eigenständig arbeiten und Internetanwender zum Beispiel bei der Suche oder der Darstellung von Web-Inhalten beeinträchtigen. Diese Komponenten sind in der Regel mit dem EULA (End User License Agreement) GamezTar (<http://www.gameztar.com/terms.do>) verbunden. Da Internetnutzer allerdings eher auf den stärker auffallenden Button “click here, get free games” als auf den Schriftzug “terms of service” am unteren Rand des Bildschirms klicken, empfiehlt Kaspersky Lab, solche rechtlichen Hinweise immer zu lesen, sofern sie vorhanden sind.

Die zweite Hitliste zeigt, mit welchen Schadprogrammen Anwender ihre PCs beim Surfen im Internet am häufigsten infiziert haben. Sie spiegelt also die Schädlingssituation im Internet wider:

Position	Positionsänderung	Name
1	0	Trojan-Downloader.JS.Gumblar.x
2	3	Trojan.JS.Redirector.l
3	Neu	not-a-virus:AdWare.Win32.GamezTar.a
4	-2	Trojan-Downloader.HTML.IFrame.sz
5	Neu	Trojan-Clicker.JS.Iframe.db
6	-2	not-a-virus:AdWare.Win32.Boran.z
7	Neu	Trojan.JS.Iframe.ez
8	Neu	Trojan.JS.Zapchast.bn
9	Neu	Packed.JS.Agent.bn
10	Neu	Packed.Win32.Krap.ai
11	8	Packed.Win32.Krap.ag
12	Neu	Exploit.JS.Pdfka.asd
13	Neu	Trojan.JS.Agent.axe
14	Neu	Trojan-Downloader.JS.Shadraem.a
15	Wieder dabei	Trojan.JS.Popupper.f
16	Neu	not-a-virus:AdWare.Win32.GamezTar.b
17	Neu	Trojan-Downloader.JS.Twetti.a
18	Neu	Trojan-Downloader.Win32.Lipler.iml
19	Neu	Trojan-Downloader.JS.Kazmet.d
20	Neu	Trojan.JS.Agent.axc

Im Gegensatz zur ersten Top-20-Liste gab es beim zweiten Ranking im Vergleich zum Vormonat zahlreiche Änderungen. Nur ein Viertel aller Schadprogramme konnte seinen Platz behaupten.

Auf Platz eins ist nach wie vor Gumblar.x. Allerdings werden die von Gumblar infizierten Webseiten von den Webmastern allmählich gesäubert. So entdeckte Kaspersky Lab im

Dezember weniger Einzelversuche Gumblar zu installieren, nur ein Viertel im Vergleich zum November.

Das im ersten Ranking auftauchende Programm Krap.ag ist auch in der zweiten Rangliste aufgestiegen, und zwar um acht Plätze. Dabei gab es im Dezember anderthalb Mal mehr Versuche dieses Programm zu installieren als im Vormonat.

GamezTar.a taucht auch in der zweiten Rangliste auf. Das ist keine große Überraschung, wenn man dessen Fokussierung auf Online-Spiele berücksichtigt. Auf Platz 16 landete sogar eine weitere Modifikation dieses Schadprogramms – GamezTar.b.

Beim Neueinsteiger Trojan-Clicker.JS.Iframe.db (Platz 5) handelt es sich um ein Iframe-Installationsprogramm. Trojan.JS.Iframe.ez (neu auf Platz 7), Trojan.JS.Zapchast.bn (neu auf Platz 8), Packed.JS.Agent.bn (neu auf Platz 9), Trojan.JS.Agent.axe (neu auf Platz 13), Trojan-Downloader.JS.Shadraem.a (neu auf Platz 14) und Trojan-Downloader.JS.Kazmet.d (neu auf Platz 19) sind Skripte, die Schwachstellen in Adobe- und Microsoft-Anwendungen ausnutzen.

Interessant ist auch Trojan-Downloader.JS.Twetti.a auf Platz 17, mit dem eine Vielzahl offizieller Webseiten infiziert worden ist. Dabei sollte man vor allem den Funktions-Algorithmus dieses Installationsprogramms beachten: Nach der Entschlüsselung fanden sich in ihm weder ein Verweis auf eine auszuführende Hauptdatei noch Exploits oder Links auf Exploits! Bei der genaueren Analyse stellte sich dann heraus, dass das Skript die API-Schnittstelle des auch unter Cyberkriminellen populären sozialen Netzwerks Twitter verwendet.

Der Trojaner funktioniert demnach folgendermaßen: Zuerst wird eine Anfrage an die API-Schnittstelle gestellt, deren Ergebnis Daten zu so genannten „Trends“ sind – also den am meisten in Twitter veröffentlichten Themen. Anschließend wird aus den diesen Angaben ein scheinbar zufälliger Domain-Name gebildet und darauf verlinkt, natürlich wurde die Domain zuvor von den Cyberkriminellen registriert. Auf dieser Domain wird auch der Hauptteil des Schadcodes untergebracht, entweder über ein PDF-Exploit oder eine auszuführende Datei. So entstehen fast in Echtzeit schädliche Links über einen Mittelsmann, in diesem Fall über Twitter.

Das Fazit für den Dezember 2009 lautet: Die Angriffe werden immer ausgeklügelter und sind immer schwerer zu analysieren. Ihr Ziel ist es, über Betrug Gewinne zu erzielen. Virtuelle Bedrohungen stellen eine immer größere Gefahr dar, die sich für Internetanwender in Wirklichkeit als völlig real erweisen.

Kaspersky Lab ist Europas größtes Unternehmen für Antivirus-Technologie und reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crimeware, Hacker, Phishing-Attacken und Spam. Das Unternehmen gehört zu den weltweit vier erfolgreichsten Herstellern von Sicherheits-Lösungen für den Endpoint (IDC 2008). Die Produkte von Kaspersky Lab haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und kurzen Reaktionszeiten einen Namen gemacht. Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen.

Weitere Details zum Unternehmen sind unter <http://kaspersky.de> zu finden. Kurzinformationen von Kaspersky Lab erhalten Sie zudem über http://twitter.com/Kaspersky_DACH. Aktuelles zu Viren, Spyware und Spam sowie Informationen zu anderen IT-Sicherheitsproblemen und Trends sind unter www.viruslist.de abrufbar.

Redaktionskontakt:

essential media GmbH
Florian Schafroth
florian.schafroth@essentialmedia.de
Tel.: +49-89-7472-62-43
Fax: +49-89-7472-62-841
Augustenstraße 24
80333 München

Kaspersky Labs GmbH
Christian Wirsig
christian.wirsig@kaspersky.de
Tel.: +49-841-98-189-325
Fax: +49-841-98-189-100
Steinheilstraße 13
85053 Ingolstadt

© 2010 Kaspersky Lab. The information contained herein is subject to change without notice. The only warranties for Kaspersky Lab products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Kaspersky Lab shall not be liable for technical or editorial errors or omissions contained herein.