

Stuxnet-Trojaner öffnet Zero-Day-Lücke in Windows

Moskau/Ingolstadt, 16. Juli 2010 – Kaspersky Lab warnt vor einem neuartigem Schadprogramm, das derzeit Virenexperten noch Rätsel aufgibt: der Stuxnet-Trojaner. Alex Gostev, Virenanalyst bei Kaspersky Lab, nimmt in drei Blogbeiträgen die neue Windows-Zero-Day-Lücke genauer unter die Lupe.

Der Trojaner Stuxnet, von Kaspersky Lab als Trojan-Dropper.Win32.Stuxnet identifiziert, infiziert USB-Sticks mittels Lnk-Dateien [1] und verbreitet sich anschließend durch die mobilen Datenträger über die Autorun-Funktion von Windows. Das Neue dabei: die Nutzung von Lnk-Dateien. Ausführliche Informationen dazu finden Sie im ersten Blogbeitrag von Alex Gostev:

http://www.securelist.com/en/blog/269/Myrtus_and_Guava_Episode_1

Interessant ist auch die digitale Signatur von Stuxnet: Der Trojaner enthält eine legale Signatur von Realtek Semiconductor. Die Gefahr dadurch: Der Großteil aller PC-Nutzer weltweit nutzt Hardware und Treiber von Realtek. Stuxnet erstellt Treiberdateien, die Rootkit-Funktionalitäten unterstützen und Malware in Computersystemen und auf infizierten USB-Sticks verstecken. Informationen hierzu finden Sie im zweiten Blogbeitrag:

http://www.securelist.com/en/blog/271/Myrtus_and_Guava_Episode_2

Das Kaspersky Security Network [2] entdeckte bereits Komponenten der Schadprogramme Rootkit.Win.32.Stuxnet und Trojan-Dropper.Win32.Stuxnet auf mehr als 16.000 Computern weltweit – vor allem im Iran, in Indien und Indonesien. Der Hauptverbreitungsweg über mobile Speichermedien ist zwar nicht der schnellste, aber ein effektiver Weg, um längerfristig Schadprogramme zu verbreiten. Alex Gostev geht davon aus, dass Stuxnet aus Indien stammt. Nähere Infos zur geografischen Verteilung von Stuxnet finden Sie im dritten Blogbeitrag:

http://www.securelist.com/en/blog/272/Myrtus_and_Guava_Episode_3

[1] siehe <http://de.wikipedia.org/wiki/Dateiverkn%C3%BCpfung>

[2] Die mit Hilfe des Kaspersky Security Network (KSN) gewonnenen Daten basieren auf Rückmeldungen der Heimanwender-Programme Kaspersky Anti-Virus und Kaspersky Internet Security.

Die Kaspersky Virus-Analysten bloggen regelmäßig über aktuelle Malware-Gefahren: in Deutsch auf <http://www.viruslist.com/de/weblog> und in Englisch auf <http://www.securelist.com/en/blog>.

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 www.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: +49-89-7472-62-843
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
Despag-Straße 3
85055 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.