

## Gestohlene Stuxnet-Zertifikate verunsichern die IT-Welt

*Kaspersky Lab beantwortet die wichtigsten Fragen*

**Moskau/Ingolstadt, 22. Juli 2010** – Die Zero-Day-Lücke Stuxnet verunsichert aktuell die Microsoft-Anwender. Laut BSI wurde die Schwachstelle, die sich vor allem über mobile Datenträger wie USB-Sticks verbreitet, für gezielte Angriffe im Unternehmensumfeld missbraucht [1]. Kaspersky Lab identifiziert aktuell über 16.000 Komponenten von Stuxnet-Schadprogrammen. Die Süddeutsche Zeitung vermutet hinter Stuxnet Industriespionage oder einen Sabotageakt in großem Stil [2]. Costin Raiu, Viren-Analyst bei Kaspersky Lab, informiert Unternehmensanwender über die aktuelle Gefahrenlage von Stuxnet.

### **Q&A über Stuxnet, von Costin Raiu, Viren-Analyst bei Kaspersky Lab**

**1. Microsoft und Verisign haben die gestohlenen Realtek-Zertifikate zurück genommen. Bedeutet das, dass Anwender ab sofort vor Stuxnet sicher sind?**  
Durch die Funktionsweise solcher Zertifikate, bedeutet das nicht, dass die Schadprogramme nicht mehr funktionieren. Man kann immer noch mit Stuxnet infiziert werden und der Treiber wird sicher immer noch ohne jede Vorwarnung selbstständig laden. Die einzige Auswirkung durch die Rückrufaktion von Microsoft und Verisign ist, dass Cyberkriminelle nicht mehr in der Lage sind, weitere Malware mit Stuxnet nachzuladen.

### **2. Wie wurden die Zertifikate gestohlen?**

Bisher hat Kaspersky Lab Stuxnet-Treiber mit Zertifikaten der Unternehmen JMicon Technology und Realtek identifiziert. Es ist möglich, dass die Zertifikate mit Hilfe eines speziellen Trojaners wie Zeus gestohlen wurden. Damit wäre die Stuxnet-Affäre aber weitaus größer.

### **3. Sind Anwender von Realtek- oder JMicon-Motherboards und/oder -Netzwerken besonders gefährdet?**

Bisher hat Kaspersky Lab keine verdächtigen Programme auf Realtek- oder JMicon-Hardware-Treibern gefunden.

### **4. Microsoft und Verisign haben Zertifikate von Realtek und JMicon zurück genommen. Bedeutet das, dass die eingesetzten Realtek- beziehungsweise JMicon-Treiber nicht mehr funktionieren?**

Nein. Aufgrund der Art, wie Zertifikate und Signaturen arbeiten, hat der Widerruf keine Auswirkungen auf eingesetzte Treiber. Beide Unternehmen haben neue Zertifikate veröffentlicht, mit denen sie neue Treiber signieren können.

### **5. Wird man in Zukunft mehr Malware mit Zertifikaten sehen?**

Wahrscheinlich ja. Derzeit gibt es bereits Zehntausende von Schadprogrammen, die digital signiert wurden.

Blogbeiträge der Kaspersky-Experten zu Stuxnet finden Sie unter:

[http://www.securelist.com/en/blog/2236/Stuxnet\\_signed\\_certificates\\_frequently\\_asked\\_questions](http://www.securelist.com/en/blog/2236/Stuxnet_signed_certificates_frequently_asked_questions)

[http://www.securelist.com/en/blog/2234/Stuxnet\\_and\\_stolen\\_certificates](http://www.securelist.com/en/blog/2234/Stuxnet_and_stolen_certificates)

[http://www.securelist.com/en/blog?print\\_mode=1&weblogid=269](http://www.securelist.com/en/blog?print_mode=1&weblogid=269)

[http://www.securelist.com/en/blog?print\\_mode=1&weblogid=271](http://www.securelist.com/en/blog?print_mode=1&weblogid=271)

[http://www.securelist.com/en/blog?print\\_mode=1&weblogid=272](http://www.securelist.com/en/blog?print_mode=1&weblogid=272)

[1]

[https://www.bsi.bund.de/cln\\_165/ContentBSI/Presse/Pressemitteilungen/Sicherheitsl%C3%BCcke\\_Windows\\_210710.html](https://www.bsi.bund.de/cln_165/ContentBSI/Presse/Pressemitteilungen/Sicherheitsl%C3%BCcke_Windows_210710.html)

[2]: <http://www.sueddeutsche.de/digital/trojaner-per-usb-siemens-und-der-digitale-industrie-spion-1.977866>

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](http://www.kaspersky.de) zu finden. Kurzinformationen von Kaspersky Lab erhalten Sie zudem über [http://twitter.com/Kaspersky\\_DACH](http://twitter.com/Kaspersky_DACH). Aktuelles zu Viren, Spyware und Spam sowie Informationen zu anderen IT-Sicherheitsproblemen und Trends sind unter [www.viruslist.de](http://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.