

## NEWSFLASH

### **Kaspersky-Analysten entdecken „großen Bruder“ des Staatstrojaners**

**Moskau/Ingolstadt, 19. Oktober 2011 – Die Kaspersky-Analysten Tillmann Werner und Stefan Ortloff berichten neue Details zum sogenannten Staatstrojaner.**

Nachdem am 11. Oktober 2011 die Analysten von F-Secure über eine eventuelle Installationskomponente des vom Chaos Computer Club entdeckten Backdoor-Trojaners schrieben [1], konnten Werner und Ortloff mit Hilfe des von F-Secure überlassenen Materials diesen so genannten Dropper genauer analysieren. Sie sprechen vom „großen Bruder“ des bekannten Backdoor-Trojaners, denn die entschlüsselte Datei enthält sogar fünf Komponenten, die jeweils verschiedene Aufgaben erfüllen. Dabei kann der Trojaner nicht nur unter 32-Bit-Versionen von Windows aktiv werden, sondern auch auf 64-Bit-Versionen.

Und nicht nur Skype steht im Visier der Malware, wie Tillmann Werner bestätigt: „Die von uns analysierte Version zeigt, dass es die Software neben Skype auch auf Web-Browser, verschiedene Instant Messenger und VoIP-Software wie ICQ, MSN Messenger, VoipBuster und Yahoo! Messenger abgesehen hat.“

Alle Komponenten des Backdoor Trojaners wurden als Rootkit vom Typ R2D2 identifiziert. Die Malware wird von den Kaspersky-Programmen erkannt und blockiert. Ein ausführlicher Blog-Artikel zur Analyse von Tillmann Werner und Stefan Ortloff ist unter [http://www.securelist.com/en/blog/208193167/Federal\\_Trojan\\_s\\_got\\_a\\_Big\\_Brother](http://www.securelist.com/en/blog/208193167/Federal_Trojan_s_got_a_Big_Brother) zu finden.

[1]

<http://www.f-secure.com/weblog/archives/00002250.html>

Für Journalisten und Redakteure hat Kaspersky Lab einen Newsroom eingerichtet. Unter <http://newsroom.kaspersky.eu> finden Sie alle aktuellen Unternehmens- und Hintergrundinformationen inklusive Audio-, Video- und Bilddateien.

**Redaktionskontakt:**

essential media GmbH

Florian Schafroth

[florian.schafroth@essentialmedia.de](mailto:florian.schafroth@essentialmedia.de)

Tel.: +49-89-7472-62-43

Fax: +49-89-7472-62-17

Landwehrstraße 61

80336 München

Kaspersky Labs GmbH

Christian Wirsig

[christian.wirsig@kaspersky.de](mailto:christian.wirsig@kaspersky.de)

Tel.: +49-841-98-189-325

Fax: +49-841-98-189-100

Despag-Straße 3

85055 Ingolstadt

© 2011 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.