

Update im Fall Uroburos: Schädling nutzt neue Technik, um den Windows-Kernel-Schutz zu umgehen

Neue G Data-Teilanalyse zeigt, wie das Rootkit Rechner infiziert

Bochum (Deutschland), 7. März 2014

Das von G Data entdeckte Spionageprogramm hat in weiteren Analysen seinen Status als komplexe Schadsoftware für High-Profile-Netzwerke weiter untermauert. Die Experten der G Data SecurityLabs veröffentlichen weitere Details, wie Rechner mit dem Rootkit infiziert werden.

Windows „PatchGuard“ ausgehebelt

Einmal auf dem PC eingeschleust, überwindet Uroburos die sogenannte Kernel Patch Protection – auch PatchGuard genannt – die das Herzstück von Windows 64-Bit-Betriebssystemen absichert und Veränderungen an diesem verhindern soll. Der Schadcode manipuliert den Kernel und versetzt ihn in den „Test Modus“. Das Rootkit kann sich dort ungehindert einnisten und wird vom Betriebssystem als valider Systemtreiber akzeptiert.

Dieser „Test Modus“ ist für Treiber-Entwickler gedacht, die so auch unsigned Treiber verwenden können, um sie während der Entwicklungsphase zu überprüfen. Die Schadcode-Autoren nutzen das Verfahren, um die Treiber-Verifizierungen zu deaktivieren. Uroburos kann so direkt als Treiber in den Betriebssystemkern eingeschleust werden, um dort sensible Daten auszuspionieren.

Die [Analyse zu Uroburos ist im G Data Security Blog verfügbar](#).

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG
G DATA Campus
Königsallee 178
44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de
Tel.: +49 (0) 234 9762-239
Fax: +49 (0) 234 9762-299