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

(Mynewsdesk) Das von G Data entdeckte Spionageprogramm Uroburos hat in weiteren Analysen seinen Status als komplexe und hochentwickelte Schadsoftware für High-Profile-Netzwerke weiter untermauert. Die G Data SecurityLabs untersuchten, wie Rechner mit dem Rootkit infiziert werden. Die Experten fanden dabei heraus, dass die Schadcodeentwickler eine neue Kombination von Techniken anwenden, mit denen der Schädling zentrale Sicherheitsmechanismen im Kern von Windows 64-Bit-Systemen, dem sog. Kernel überwindet. Die vollständige Analyse ist im G Data SecurityBlog unter http://blog.gdata.de/ verfügbar.Windows ?PatchGuard? ausgehebeltEinmal auf dem PC eingeschleust, überwindet Uroburos die sogenannte Kernel Patch Protection ? auch PatchgGuard 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 unsignierte 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 ist im G Data SecurityBlog verfügbar unter: http://blog.gdata.de/artikel/uroburos-detaillierte-einblicke-in-die-umgehung-des-kernelschutzes/

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/c77cz6

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/it-hightech/update-im-fall-uroburos-schaedling-nutzt-neue-technik-um-windows-kernel-schutz-zu-umgehen-71059

Pressekontakt

-

Kathrin Beckert
Königsallee b 178
44799 Bochum

kathrin.beckert@gdata.de

Firmenkontakt

-

Kathrin Beckert
Königsallee b 178
44799 Bochum

shortpr.com/c77cz6
kathrin.beckert@gdata.de

IT Security wurde in Deutschland erfunden: Die G Data Software AG gilt als Erfinder des AntiVirus. Das 1985 in Bochum gegründete Unternehmen hat vor mehr als 25 Jahren das erste Programm gegen Computerviren entwickelt. Heute gehört G Data zu den weltweit führenden Anbietern von IT-Security-Lösungen.

Testergebnisse beweisen: IT-Security Made in Germany schützt Internetnutzer am besten. Seit 2005 testet die Stiftung Warentest InternetSecurity Produkte. In allen sechs Tests, die von 2005 bis 2013 durchgeführt wurden, erreichte G Data die beste Virenerkennung. In Vergleichstests von AV-TEST demonstriert G Data regelmäßig beste Ergebnisse bei der Erkennung von Computerschädlingen. Auch international wurde G Data InternetSecurity von unabhängigen Verbrauchermagazinen als bestes Internetsicherheitspaket ausgezeichnet u.a. in Australien, Belgien, Frankreich, Italien, den Niederlanden, Österreich, Spanien und den USA.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind weltweit in mehr als 90 Ländern erhältlich.Â

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter http://www.gdata.de