Neuer Bank-Trojaner im Umlauf: F5 Networks analysiert "Slave"-Malware und veröffentlicht technische Details

Slave-Trojaner ähnelt berüchtigtem Trojaner-Baukasten Zeus

München, 07. Juli 2015 - F5 Networks (NASDAQ: FFIV) hat eine neue Gefahrenquelle für Online-Banking-Nutzer entdeckt: Der sogenannte "Slave"-Trojaner wird von Cyberkriminellen für den Diebstahl von Credentials und der Identität, für IBAN-Manipulationen und automatische Überweisungen verwendet. Erstmals tauchte der in Visual Basic geschriebene Schädling im März auf. Inzwischen ist aber eine neue, deutlich ausgereiftere Variante im Umlauf. Beide Varianten haben die Sicherheitsexperten von F5 im firmeneigenen Security Operations Center (SOC) gründlich analysiert.

Die ursprüngliche Version von Slave tauscht lediglich per "Man-in-the-Browser?• in zwei Schritten die eingegebenen IBAN-Daten aus und ändert das Empfängerkonto bei einer Überweisung. Die neue Variante hingegen nutzt ausgefeilte Tarnmechanismen und Webinjektionen und ähnelt damit dem berüchtigten Trojaner-Baukasten "Zeus".

Slave kommuniziert mit einem Command & Control Server über einen im Browser erstellten Thread. Beim Browserstart verschickt die Malware einen HTTP-Request für die Webinjektion und erhält sie in Plain-Text als JSON-Objekt. Der Schadcode wird beim Online-Banking injiziert - und ist für jede Bank unterschiedlich. Die manipulierte Konfiguration bleibt dann im Browser gespeichert.

Slave kopiert sich selbst in den Autostart-Ordner und erstellt einen automatisch startenden sys.exe Registry-Eintrag. Um unerkannt zu bleiben, legt der Trojaner nach jedem Neustart einen als "Internet Explorer" getarnten Registry-Schlüssel mit einem zufälligen Namen an, der eine Kopie des Binary-Files der Malware startet und nach jedem Neustart anders heißt. Allerdings löscht der Schädling vorherige Einträge nicht, deshalb füllt sich die Registry schnell.

Slave zielt auf die drei gängigsten Webbrowser - Internet Explorer, Firefox und Chrome. Nach einer Infektion eines Browsers starten die anderen nicht mehr korrekt.

Umfangreiche, technische Details zur Funktionsweise von Slave gibt es im ausführlichen Report unter: https://devcentral.f5.com/d/f5-soc-slave-malware-analysis-report?download=true

ca. 2.000 Zeichen mit Leerzeichen

Pressekontakt

Dr. Haffa & Partner GmbH

Herr Axel Schreiber
Burgauerstr. 117
81929 München

haffapartner.de
postbox@haffapartner.de

Firmenkontakt

F5 Networks

Frau Sibylle Greiser
Lehrer-Wirth-Straße 2
81829 München

f5.com/
s.greiser@f5.com

F5 (NASDAQ: FFIV) bietet Lösungen für eine Welt voller Applikationen. F5 unterstützt Unternehmen, Cloud-Systeme, Rechenzentren und Software Defined Networks (SDN) zu skalieren, um für jeden, jederzeit und überall Anwendungen optimal bereitzustellen. Die Lösungen von F5 erweitern die IT durch eine offene, skalierbare Struktur und unterstützen durch ein starkes Netzwerk aus Partnern und Allianzen der führenden Anbieter im Bereich Technologie- und Rechenzentren. Dieser Ansatz ermöglicht Kunden, eine Infrastruktur zu entwickeln, die zukünftigen Anforderungen gerecht wird. Führende Konzerne und internationale Unternehmen, Service Provider sowie Institutionen des öffentlichen Dienstes verlassen sich auf F5, wenn es um Cloud-, Security- und Mobility-Trends geht.

Weitere Informationen finden Sie auf http://www.f5.com/.

Folgen Sie F5 auf Twitter (https://twitter.com/F5networksde) oder besuchen Sie uns auf Facebook (http://www.facebook.com/f5networksinc), um mehr über F5, die Partner und Technologien zu erfahren.

Anlage: Bild