F5 entdeckt neue Version des Banking-Trojaners VBKlip

F5 Networks (NASDAQ: FFIV) hat eine weitere Gefahr für Online-Banking-Kunden identifiziert:

München, 8. Mai 2015 - F5 Networks (NASDAQ: FFIV) hat eine weitere Gefahr für Online-Banking-Kunden identifiziert: Eine neue "Man-in-the-Browser?•-Version der 2013 erstmals entdeckten VBKlip-Malware manipuliert IBAN-Daten, indem sie die über die Windows-Funktionalität "Copy & Paste?• in den Zwischenspeicher geladenen Informationen abfängt und stattdessen die Malware-eigene IBAN einsetzt. Den Banking-Trojaner hat F5 über sein Security Operations Center (SOC) entdeckt.

Das Infektionsschema beginnt mit einem Downloader, der zwei Dateien herunterlädt: wmc.exe und windows.sys (DLL). Nachdem die infizierte Windows.sys-DLL-Datei in den Arbeitsspeicher geladen ist, wird versucht, eine Kommunikation mit verschiedenen Domänen aufzubauen. Das Besondere an der neuen Version des Trojaners ist, dass die Komponenten einzeln heruntergeladen werden und jede eine eigene Funktion im Hinblick auf die gesamte Ablaufsteuerung des Betrugs hat. Der Vorgang ist in verschiedene Module aufgeteilt, wobei der Download der jeweils nächsten Komponente über Command-and-Control-Server-Kommunikation erfolgt, sodass es immens schwierig ist, alle involvierten Komponenten zu ermitteln und die Attacke als Ganzes zu analysieren. Eine Erweiterung zur vorherigen Version ist die Möglichkeit zur Synchronisierung. Konnte zuvor lediglich ein laufender Browserprozess beeinflusst werden, ist es nun möglich, mithilfe eines Mutex-Formats die IBAN in allen laufenden Prozessen auszutauschen. Die Malware richtet sich auf die drei wichtigsten Browser: Internet Explorer, Firefox und Chrome.

"Zwar ist dieser Ansatz für betrügerische Transaktionen relativ simpel im Vergleich zu bekannten Pendants wie ?Zeus?, dennoch ist er sehr erfolgreich. Man kann sicher davon ausgehen, dass die Weiterentwicklung des Trojaners noch längst nicht am Ende angelangt ist?•, erklärt Markus Härtner, Senior Director Sales DACH bei F5 Networks.

Weiterführende technische Details zur Funktionsweise des VBKlip-Trojaners gibt es unter: https://devcentral.f5.com/articles/vbklip-banking-trojan-goes-man-in-the-browser .

ca. 2.100 Zeichen mit Leerzeichen

Pressekontakt

Dr. Haffa & Partner GmbH

Frau Anja Klauck
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