Bitcoin-Hype ruft immer neue „Goldgräber“ auf den Plan: Sophos registriert starken Anstieg des heimlichen Schürfens von Kryptowährungen auf Rechnern ahnungsloser Webseitenbesucher

- JavaScript-Anwendung des Anbieters Coinhive schürft heimlich die Kryptowährung Monero (XMR)
- Webseitenbetreiber verdienen an Rechenleistungen auf Besucher-Computern
- Webseitenbesucher registrieren u.a. Verlangsamung der Rechnerleistung, erhöhte Wärmeentwicklung und kürzere Akkuleistungen
- Neue Varianten von IoT-Botnetzen wie Mirai beginnen, IoT-Geräte für das Mining von Bitcoins zu nutzen

Statement von Michael Veit, Security Evangelist bei Sophos

Wiesbanden, 14. Dezember 2017 Immer mehr Akteure wollen am Bitcoin-Hype mitverdienen – und ahnungslose Webseitenbesucher sind in diesem Fall die Leidtragenden: Seit September 2017 beobachten wir, dass bei dem Besuch vieler Webseiten die Prozessorlast des eigenen Rechners aus zunächst unerfindlichen Gründen auf 100% hochschnellt. Der Grund dafür ist, dass beim Besuch der Webseite eine in JavaScript geschriebene Anwendung des Anbieters Coinhive heruntergeladen und gestartet wird, die dann im Hintergrund läuft und die Kryptowährung Monero (XMR) schürft. Unter Schürfen einer Kryptowährung versteht man dabei das rechenintensive Lösen mathematischer Aufgaben mit dem Ziel, neu herausgegebene Einheiten einer Kryptowährung zu erhalten. Der Betreiber der Webseite erhält für die auf den Rechnern der Webseitenbesucher geleisteten Rechenoperationen von Coinhive Geld. Die Konsequenz für den Besucher der Webseite ist, dass sein Rechner langsamer ist, und gerade bei Notebooks sich die Wärmeentwicklung erhöht und die Akkulaufzeit reduziert.

Prinzipiell ist es ein legitimes Vorgehen, dass der Betreiber einer Webseite die Rechenleistung des Computers des Besuchers als Bezahlung für die (dann beispielsweise werbefreie) Nutzung einer Webseite verlangt – sofern der Besucher darauf hingewiesen wird. Es gibt zwar Webseiten, die entsprechende Meldungen anzeigen und teilweise auch die Nutzung des Prozessors auf einige Sekunden oder Minuten begrenzen – aber in den allermeisten Fällen ist das nicht der Fall. Oft handelt es sich bei Webseiten mit Coinhive-Skripten um halbseidene oder illegale Angebote, wie Börsen oder Download-Portale für Software und Videos. Coinhive-Skripte wurden aber auch schon auf seriösen Webseiten gefunden. Nicht in jedem Fall war und ist dabei klar, ob dies mit Absicht seitens des Webseitenbetreibers geschah oder ob die Webseite Opfer von Malvertising- oder Hacking-Angriffen wurde.

Zweckentfremdung von Rechenleistung privater Geräte wird weiter Schule machen
Das Thema Kryptowährungen mit Bitcoin als prominentestem Vertreter tritt immer stärker ins Bewusstsein der Öffentlichkeit. Die anfangs als anonymes Zahlungsmittel für Kriminelle angesehenen Kryptowährungen werden zunehmend hoffähig für Investoren in der traditionellen Finanzwelt, mittlerweile können etwa bereits Terminkontrakte auf die Bitcoin-Wertentwicklung an regulierten Börsen erworben werden.

Von dem hohen Wertzuwachs den Bitcoin in den letzten Wochen profitieren auch andere Kryptowährungen wie Monero, welche durch Coinhive geschürft wird. Sowohl der Wert des Bitcoin als auch der Wert des Monero verdreifachten sich im Zeitraum von Ende Oktober bis Anfang Dezember 2017.

Im Zuge dessen beobachten wir seit Ende November 2017 einen rapiden Anstieg von Webseiten mit Coinhive – von wenigen hundert Webseiten schnellte die Anzahl auf über 10.000, Tendenz stark steigend. Dieser Zusammenhang ist in der ergänzenden Grafik gut ersichtlich.

Es ist zu erwarten, dass – zumindest solange der Boom der Kryptowährungen andauert – die Zweckentfremdung von Rechenleistung auf Privatgeräten weiter Schule machen. Der Weg über Skripte von Coinhive auf Webseiten ist dabei nur eine Spielart. Neue Varianten von IoT-Botnetzen wie Mirai fangen an, gekaperte IoT-Geräte für das Mining von Bitcoins zu nutzen. Und je wertvoller pure Rechenleistung wird, desto mehr Wege werden Cyberkriminelle finden, um die Computer ahnungsloser Endanwender dafür zu nutzen.

Weitere Informationen zum Thema finden Sie hier:
https://nakedsecurity.sophos.com/2017/09/20/pirate-bay-hits-users-cpus-with-secret-cryptocurrency-mining/).

Eine ergänzende Grafik findet sich unter diesem Link

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. Weitere Informationen unter www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +172 4536839
sophos@tc-communications.de