Wer hat von meinem Tablet geschürft?

Das Schürfen von Kryptowährungen erlebt einen Boom an Beliebtheit – legal wie illegal. Man unterscheidet daher zwischen Cryptomining und Cryptojacking. Ganz schön kryptisch alles.

Sophos bringt etwas Licht ins Dunkel und erklärt den Unterschied zwischen legalem und schadhaftem Schürfen von Kryptowährungen und zeigt auf, wie man merkt, dass illegale Goldgräber auf den eigenen Geräten schürfen und wie ein Schutz dagegen aussehen kann.

Cryptojacking ist das neue Lieblingsarbeitsgebiet in der Cyberkriminellen-Szene – dank des starken Ansturms an Kryptowährungen in 2017 wie Bitcoin, Monera und Ethereum. Die Kriminellen zielen dabei aggressiv auf Laptops, Desktop-PCs, Server und mobile Geräte, um einschließlich des Netzwerks alles zu infizieren. Das Ziel: die gehijackten Computer-Kapazitäten dafür zu nutzen, um intensiv Kryptowährungen zu schürfen. Ein cleveres Prinzip, denn der geschädigte Besitzer der infizierten Geräte hat die Arbeit, zahlt für den Strom und die Hardware und die Kriminellen stecken sich die Vergütung in die Taschen.

Was ist der Unterschied zwischen Mining und Jacking?
Cryptomining und Cryptojacking sind zwei Begriffe, die in der Diskussion oft verwechselt werden. Cryptomining bezeichnet zunächst den komplexen Prozess, um den alles geht: das Schürfen von Kryptowährungen. Das kann sowohl legal (also mit Erlaubnis) oder illegal, schadhaft (ohne Wissen des Nutzers, dessen Rechenleistung zum Schürfern genutzt wird) sein, dann nennt man es Cryptojacking.

Legales und illegales Cryptomining sind ansonsten fast kongruent. Allerdings verdient bei Letzterem eben nur der Kriminelle Geld und zwar auf Kosten anderer. Für sein Ziel, das schnelle Geld zu machen, platziert der Gangster dabei Cryptomining-Code auf einem Gerät des Opfers. Er kapert es auf diese Weise heimlich, um es als Teil eines kriminellen Rechner-Pools arbeiten zu lassen. Dabei wird nicht gekleckert, sondern geklotzt. Schließlich soll viel Geld in Gangsters Taschen landen. Die Betrüger streben einen möglichst hohen Infektionsgrad und zahlreiche Geräte an. Und sie sind pfiffig. Schadhafte JavaScript-Miner zum Beispiel kidnappen ihre Opfer via Browser.

Breitgefächert: Angriff per JavaScript-Miner
Clever, denn nahezu alle Laptops, Handys, Tablets oder Server sind damit gefährdet. Doch JavaScript-Miner sind Durchreisende, so dass der Browser nur während der kurzen Periode des Schürfens etwas leisten muss. Sobald man den Browser mit der infizierten Webseite schließt, stoppt das Schürfen.

Surft man als Nutzer über eine infizierte Seite wird man nicht um Erlaubnis gefragt, den JavaScript-Miner zu starten. Er läuft einfach los. Wie man das erkennt? Die CPU auf dem Gerät wird zum Maximum ausgelastet und Handy, Tablet, PC etc. werden extrem langsam. Je mehr der Prozessor arbeiten muss, desto mehr Strom verbraucht er, desto mehr muss die Lüftung arbeiten und desto heißer wird das Gerät. Für mobile Endgeräte heißt das oft „Überhitzung“ oder starker Akkuverbrauch. Einige JavaScript-Miner sind schlau und erkennen, dass sie auf einem Handy oder Tablet laufen. Sie setzen deshalb erst dann zum vollen Schürfern an, wenn die Geräte an den Strom angeschlossen sind. So können die Miner länger und gänzlich unbemerkt ihr Unwesen treiben. Ein weiterer Vorteil für die Gangster: Die Nutzer schließen oftmals die Browser auf ihrem Handy oder Tablet nicht.

Heimliche Gefahr: Native-Code-Attacken
Eine besonders üble Spezies sind Native-Code-Attacken. Ähnlich Ransomware-Angriffen infizieren sie Geräte durch traditionelle Schadsoftware und installieren heimlich Cryptoming Code, um das Opfergerät (und später ganze Netzwerke) fürs Schürfern zu verwenden. Namentlich setzen sie auf EternalBlue and Mimikatz Exploits, aber anders als Ransomware bleiben sie im Hintergrund, verstärken aber ihre Boshaftigkeit. Sie entfernen jede andere Mining Software, um alle Ressourcen für sich zu nutzen und downloaden die effizientesten Schürfer. Die beliebtesten Varianten wurden auf Windows, MacOS und Linux-Systemen gefunden. Allerdings haben SophosLabs Experten auch eine wachsende Anzahl von Mining-Funktionalität in Native Apps auf Android Geräten ausmachen können, entweder in den Apps selbst (Mining-Code inkludiert) oder in populären Apps, die modifiziert wurden.

Falls das noch nicht ausreicht, werden Remote Access Trojaner (RAT) installiert. Das heißt, dass Kriminelle nicht nur unsichtbar das eigene Gerät steuern können, sondern die komplette Kontrolle übernehmen. Löschen, Modifizieren, Up- und Downloads und Installieren von weiterer Schadsoftware. Bei einer derartigen Großübernahme ist die Cryptomining Software das kleinste Problem.

Wie kann man sich schützen?
Es bleibt die Erkenntnis, dass es angesichts der Ähnlichkeit von legalem und illegalem Cryptomining auch für IT-Profis schwer ist, den Unterschied zu erkennen, da ein Krimineller eine legale Software durch simple Methoden zu einer Schadhaften machen kann. Gegen Cryptojacking hilft leider keine Wunderwaffe, aber – ähnlich den Schutzmaßnahmen gegen Ransomware – braucht es ein mehrschichtiges Vorgehen. Die Sophos Experten empfehlen als grundlegende Gegenmaßnahmen Folgendes:

1. Webseite blockieren, die JavaScript-Miner hosten (bei Sophos Security-Lösungen werden bekannte JavaScripts zum Cryptomining wie CoinHive durch die WebControl automatisch geblockt).

2. Cryptomining-Schadware an jedem Punkt der Attacke-Kette stoppen.
   So funktioniert es: Moderne Endpoint-Security-Lösungen arbeiten mehrschichtig. Zunächst wird über Funktionen wie Device Control, WebControl oder ApplicationControl verhindert, dass Malware überhaupt erst auf den Rechner kommt. Technologien wie Virenscan, Heuristiken und DeepLearning/MachineLearning wiederum untersuchen heruntergeladene Dateien. Schließlich greifen während der Ausführung eines Programmes Mechanismen wie Verhaltenserkennung und Exploit-Verhinderung, um auch Infektionen über dateilose Malware sowie Skripte oder Makros zu erkennen und zu verhindern.

3. Kein Zugriff für Cryptomining-Applikationen auf dem eigenen Netzwerk (auch hier werden bei Sophos bekannte Cryptomining-Anwendungen als PUAs oder Malware blockiert).

4. Update aller Geräte, also regelmäßige Patches einspielen, um das Risiko von Exploit-Attacken zu minimieren, Sicherheitssoftware einsetzen (Sophos Central mit Intercept X, Endpoint, Server und Mobile Protection blockt verdächtige Malware, Webseiten mit JacaScript-Minern und Exploits), eine starke Passwort-Politik verfolgen und auf die oben vorgestellten Hijacking-Signale achten. Ein langsames Netzwerk, plötzlich hohe Stromkosten, Geräte werden warm oder eine hohe CPU-Auslastung sind Zeichen, bei denen man aufmerksam werden sollte.

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 +49-172-4536839
sophos@tc-communications.de