# World Wide Western: Coin Miner nehmen Android ins Visier

*Illegale Cryptomining-Software auf dem Vormarsch. SophoLabs hat die neue Trend-Malware in einem Report genauer unter die Lupe genommen.*

**Wiesbaden, 14. Februar 2018 –** Ransoware ist brutal und zerstörerisch und steht aktuell im Rampenlicht. Doch im Schatten dieses aktuellen Malware-Stars hat sich still und leise eine andere Spezies einen Platz im Markt der Cyberkriminalität ergaunert: Cryptomining. Mit der virtuellen Geldschürferei werden sich Security-Sheriffs in 2018 zu beschäftigen haben.

Forscher der SophosLabs haben auf den offiziellen Plattformen zuletzt zahlreiche schadhafte Apps entdeckt, die verstecktes Java Script enthalten, das sich in die Prozessoren der Mobilgeräte unbedarfter Opfer gräbt und dort Cryptowährungen schürft.

**Wie funktioniert Cryptomining-Malware?**

Betrüger infizieren unbemerkt die Computer von arglosen Nutzern mit einer Cryptomining-Software, die zahlreiche Kalkulationen durchführt, die notwendig sind, um eine Cryptowährung (Bitcoin, Monero oder Ethereum) zu erstellen. Dieses Prozedere fläuft im Verborgenen ab, und die kriminellen Goldschürfer machen sich dabei unbefugt die Rechnerleistung fremder Computer zu nutze. Um real existierendes Geld mit Coinmining (also dem Sammeln von virtueller Währung) zu verdienen, benötigt man leistungsfähige Computer. Und zwar viele.

Nun könnten die Coin Miner sich hierfür einfach einen Platz in einer gigantischen Coinmining-Server-Farm mieten, zum Beispiel in Island, denn dort ist der Strom, den die zahlreichen Computer nutzen, günstig. Das illegal Erwirtschaftete würde so also nicht dirket wieder den Kosten für die Platzmiete zum Opfer fallen. Die Schürfer haben aber eine andere Möglichkeit für sich entdeckt: Den Diebstahl von Rechnerleistung und Klimaanlagen durch den Einsatz von Schadsoftware. Und das mit doppeltem Effekt, denn die Cryptominer nutzen nicht nur Rechnerleistung, sondern können obendrein in den eingedrungenen Netzwerken herumschnüffeln und etwa Surf- oder Kaufverhalten des betroffenen Computerbesitzers ausspionieren.

**Was macht Cryptominer so gefährlich?**

Ist der Computer mit einem Cryptominer infiziert, bleiben alle Daten, wo sie hingehören und sind uneingeschränkt erreichbar. Kein Vergleich zu Ransomware also. Aber: der PC wird ärgerlich langsam, die Laptop-Lüfter rauschen wie ein Wirbelsturm und die Akkulaufzeit sinkt dramatisch.

Auf einem mobilen Gerät erweisen sich diese Nebenwirkungen als noch deutlich unangenehmer: kurze Batterieleistung mit der Folge schneller Nicht-Verfügbarkeit. Obendrein kann eine Akkuüberhitzung durch kontinuierlich hohe Prozessorauslastung permanenten Schaden anrichten. Es gibt zahrleiche Coinmining-Software-Versionen, die dem Nutzer von vornherein empfehlen, sich nicht damit abzuplagen, die Software auf einem mobilen Gerät laufen zu lassen: die Rechenleistung des Tablets oder Handys ist schlichtweg nicht

ausreichend für anständige Ergebnisse, so dass die Kosten die Vorteile nicht ausgleichen. Die illegalen Schürfer interessiert das allerdings offenbar wenig. Schon bei der Infektion von PCs haben sie nicht um Erlaubnis gefragt und ihre Opfer die (Strom-) Kosten zahlen lassen. Wie gleichgültig den Kriminellen ihre Opfer tatsächlich sind beschreibt SophosLabs in einem kürzlich veröffentlichten technischen Report zum Coin Mining. Ein faszinierender Einblick in die Arbeitsweise von Cyberkriminellen und wie viel Mühe sie sich beispielsweise geben, damit der App Store ihren Cryptomining Code akzeptiert...

**Über Sophos**

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.

Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. 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 +49-172-4536839
sophos@tc-communications.de