28.06.2018
von Verbrauchermagazin-Redaktion

Kurzgefasst

Um Kryptowährungen wie Bitcoins herzustellen, müssen Computer komplexe Rechenaufgaben lösen. Das erfolgt nicht immer auf legalem Weg: Seitdem die Kurse vieler dieser Währungen rasant gestiegen sind, zapfen Betrüger immer häufiger private Computer an, um selbst Strom und Prozessorleistung zu sparen und mehr Einheiten produzieren zu können. Wie Sie feststellen, ob Ihr Computer für diesen Zweck gekapert wurde, und wie Sie sich vor dem sogenannten Kryptojacking schützen, erklären wir im Blog.

Schlagworte

Bitcoin
Cyberkriminalität

Kryptojacking: Wie Sie verhindern, dass Ihr Rechner für Fremde arbeitet

Über Kryptowährungen wie Bitcoin oder Monero wird derzeit in den Medien viel gesprochen und geschrieben. Doch inzwischen missbrauchen manche Hacker die Idee hinter den virtuellen Währungen – und benutzen dafür vielleicht auch Ihren Rechner. So können Sie sich vor dem „Kryptojacking“ schützen.

Das öffentliche Interesse für Kryptowährungen stieg Ende 2017 stark an, als der Kurs für den Bitcoin unerwartete Höhen erreichte. Mehr als 15.000 Euro war so eine virtuelle Münze zeitweise wert. Inzwischen (Stand: 27.6.2018) sind es nur noch etwas mehr als 5.000 Euro. Doch die hohe Nachfrage nach Kryptowährungen kann auch für Unbeteiligte zum Risiko werden: Denn um das virtuelle Geld zu erschaffen, braucht

man Strom und eine hohe Prozessorleistung. Hacker nutzen daher vermehrt Schwachstellen in privaten Computern aus, um diese unbemerkt für sich arbeiten zu lassen. Diesen neuen Trick nennt man Kryptojacking.

Was ist Kryptojacking?

Kryptowährungen wie Bitcoin, Monero oder Ripple entstehen, vereinfacht gesagt, indem ein PC hoch-komplexe mathematische Aufgaben löst. Sobald eine gelöst ist, hat man einen Bitcoin (oder eine Einheit einer anderen Kryptowährung) auf seiner Festplatte. Normale Rechner brauchen für das sogenannte Schürfen („Mining“) inzwischen mehrere Tage oder Wochen, weil die Rechenaufgaben mit steigender Menge an Kryptogeld immer schwieriger werden. Beim „Kryptojacking“ (vom englischen „to hijack“ für „entführen“) schleusen Hacker versteckte Programme auf andere Rechner ein und nutzen deren Leistung zum Minen. Das dabei entstehende Geld behalten sie natürlich.

Ist mein PC gefährdet?

Grundsätzlich können alle Rechner und auch Smartphones oder Tablets betroffen sein. Denn Hacker werden immer geschickter darin, ihre Schadsoftware auf harmlosen Webseiten unterzubringen. So befand sich der Verbraucherzentrale Bayern zufolge zum Beispiel auf der Seite abi-physik.de ein Krypto-Miner. Jedes Mal, wenn Nutzer diese Seite aufriefen, wurde ein Teil ihrer Rechenleistung für das Mining angezapft. Ohne ihr Wissen oder Einverständnis.

Wie merke ich, dass ich Opfer von Kryptojacking bin?

Wenn Ihr PC oder Mobilgerät zum Beispiel plötzlich langsamer wird oder die Lüftung lauter ist, sollten Sie Verdacht schöpfen. Sie können immer dann ein Opfer von Kryptojacking sein, wenn Ihr Rechner ohne erkennbaren Grund viel leistet und damit ungewöhnlich viel Strom verbraucht. Die Kosten dafür bleiben nämlich bei Ihnen hängen.

Wie schütze ich mich davor?

Es gibt spezielle Add-ons, die Sie bei gängigen Browsern wie Chrome oder Firefox installieren können. Auch aktuelle Anti-Viren-Programme schützen oft. Zudem haben einige Ad-Blocker die Möglichkeit von konfigurierbaren Filterlisten. Auch schadet es nicht, die installierten Programme regelmäßig zu überprüfen.


Abonnieren Sie den Blog Verbraucher-Magazin!
Zum Abonnement