Das Anzapfen von Rechenleistung für des Generieren von Kryptowährungen ist eine neue Form der Bedrohung im Internet.

Schutz vor ungewolltem Zugriff

Kriminelle zapfen Computer an, um die Rechnerleistung zum Generieren von Kryptowährungen zu nutzen. Die Software „CoinEater“ der FH St. Pölten blockiert ungewollten Zugriff auf Rechnerleistung.

Wenn der Rechner langsam und laut wird, könnte der Grund dafür „Kryptomining“ sein, der Zugriff auf Rechnerleistung zum Generieren von Kryptowährungen ohne Wissen der Nutzer. Da Mining ein rechenintensiver Vorgang ist, kann dies auf mobilen Geräten zu einer stark verminderten Akkulaufzeit führen.

Mitarbeiter der Fachhochschule St. Pölten *(www.fhstp.ac.at)* haben die Open-Source-Software „Coin-Eater“ entwickelt, die Online-Kryptominer erkennt und deren Ausführung verhindert. Sie ist gratis als Add-on für *Firefox* und *Chrome* erhältlich unter *www.coineater.io*. „Zum Erzeugen von Kryptowährungen wird normalerweise Hochleistungshardware verwendet. Kryptojacking verteilt das Mining auf viele, weniger leistungsfähige Geräte und ist eine neue Form der Bedrohung im Internet“, erklärt Sebastian Schrittwieser, Leiter des Instituts für IT Sicherheitsforschung der FH St. Pölten, der die Software mitgestaltet hat. Angreifer generieren die Kryptowährung dadurch nicht auf ihren Rechnern mit ihrem Strom, sondern bei jemand anderem. Der Computer läuft auf Anschlag, der Akku wird schnell leer, der Profit geht an die Angreifer.

Suche nach neuen Bedrohungen. Ein an Schrittwiesers Institut entwickelter Scanner untersucht regelmäßig automatisiert das Internet nach Kryptojacking und lässt die Ergebnisse in die „Coin-Eater“-Software einfließen. Dazu haben die Forscherinnen und Forscher über eine Million der beliebtesten Webseiten durchsucht und unter diesen mehr als 3.000 Seiten gefunden, die ohne Wissen der Besucher nach Kryptowährungen schürfen. Das Programm der Forscher bietet zudem eine technische Analyse der auf diesen Webseiten verwendeten Methoden. „Der Einsatz solcher Techniken ist durchaus legitim, wenn die Webseiten-Besucher dem zustimmen, zum Beispiel, um Werbung auf den Webseiten ausblenden zu lassen“, sagt Schrittwieser. Kryptojacking hingegen ist ein Missbrauch der Geräte der Benutzer. „Auch wenn mit *Coinhive* der größte Anbieter von Online-Mining-Software seinen Betrieb einstellt, ist das Problem nicht ganz aus der Welt und das Mining könnte sich zu einem späteren Zeitpunkt wieder mehr lohnen“, erklärt Schrittwieser. Der entwickelte Scanner erkennt auch andere Anbieter von Kryptomining.

Schutz vor Pop-ups. Der Scanner erkennt auch ein weiteres neues Phänomen im Internet: den Pop-up-Scam. Dabei öffnen sich beim Besuch von Webseiten Pop-up-Fenster mit Werbung oder kurzen Nachrichten, die zu kostenpflichtigen Angeboten oder Schadsoftware verlinken und von den Webseitenbesuchern mühsam weggeklickt werden müssen. „CoinEater“ wurde im Forschungsprojekt *PriSAd (Privacy and Security in Online Advertisement) entwickelt,* gefördert von der *Österreichischen Forschungsförderungsgesellschaft FFG*. Partner im Projekt war das IT-Sicherheitsunternehmen *Nimbusec*. Die Software wird laufend aktualisiert. Pro Tag werden circa 100.000 Seiten gescannt, alle zehn Tage gibt es ein Update für die eine Million Seiten.

Foto: Dan Eady/Stock.adobe.com