WHITEPAPER

LEGITIMER EINSATZ VON CRYPTO-MINING

Herausgeber:
eco – Verband der Internetwirtschaft e.V.

Autoren:
Ralf Benzmüller (G DATA), Michael Hausding (SWITCH), Patrick Koetter (sys4 AG), Peter Meyer (eyeo)

EINLEITUNG

Crypto-Mining könnte sich als neues, alternatives Geschäftsmodell zur Finanzierung von Onlinediensten im Internet etablieren. Leider ist Crypto-Mining durch den häufigen, kriminellen Missbrauch in Verruf geraten. Dieses Whitepaper gibt Empfehlungen für den legitimen Einsatz von Crypto-Mining auf Webseiten und in (mobilen) Apps. Die Empfehlungen stehen einerseits im Einklang mit den Interessen der Internetnutzer und berücksichtigen andererseits die kommerziellen Interessen von Anbietern.

Crypto-Mining findet auf den Rechnern oder Smartphones von Nutzern statt. Es bietet Webseitenbetreibern, alternativ oder kumulativ zur Onlinewerbung die Möglichkeit, Geld zu verdienen. App-Entwickler erhalten damit eine zusätzliche Möglichkeit, Entwicklung und Bereitstellung ihrer Dienstleistungen zu finanzieren.

Die Nutzung ist statthaft, solange sie mit Einwilligung der Nutzer stattfindet. Wenn Geräte jedoch ohne die Einwilligung der jeweiligen Eigentümer zum Schürfen von Kryptowährungen genutzt werden, wird daraus Missbrauch einer fremden Ressource. Die missbräuchliche und unerwünschte Nutzung überwiegt die legale Nutzung gegenwärtig so stark, dass viele Crypto-Mining-Dienste pauschal geblockt werden. Betreiber von App-Stores haben deshalb bereits ihre Richtlinien angepasst und Mining-Apps aus den Stores verbannt.

CRYPTO-MINING VS. CRYPTO-JACKING

Kryptowährungen wie Bitcoin, Ethereum, Monero oder Dash basieren darauf, dass Teilnehmer ihre Geräte komplizierte Rechenaufgaben (Berechnung einer Blockchain) lösen lassen. Im Austausch dafür erhalten Teilnehmer eine Belohnung, meist in Form von Coins (Münzen) der jeweiligen Währung. Diesen Vorgang nennt man „Mining" oder zu Deutsch „Schürfen". Es lässt sich mit jedem Computer oder Smartphone/Tablet durchführen. Crypto-Mining kostet Geld, denn die Berechnungen lasten die Prozessoren der Geräte aus und diese verbrauchen dafür mehr Strom. Für etablierte Kryptowährungen wie Bitcoin oder Ethereum ist das Schürfen mit gewöhnlichen PCs aufgrund der dafür notwendigen hohen Rechenleistung und der vergleichsweise geringen Vergütung unrentabel.

Um dennoch Geld mit dem Crypto-Mining zu verdienen, führen professionelle Miner die notwendigen Berechnungen in großen Rechenzentren mit spezieller Hardware in Regionen mit günstigem Strom durch. Nur so können sie die Kosten decken und Gewinn erwirtschaften. Andere Kryptowährungen, wie zum Beispiel Monero, gestatten mit handelsüblichen Rechnern, Notebooks und sogar Smartphones effektives Schürfen. Aber auch hier schmälern die Stromkosten den errechneten Gewinn maßgeblich. Die Stromkosten fallen weg, wenn die Berechnungen von fremden Geräten, z.B. den Rechnern von Webseitenbesuchern beziehungsweise Nutzern von Software und Apps ausgeführt werden. Dann tragen die Eigentümer der Geräte die Stromkosen. Geschieht dies mit Wissen und Zustimmung der Nutzer, ist das legitim. Dieser Ansatz hat das Potenzial, Internetangebote, aber auch Apps, auf Smartphones zu finanzieren.

Auch Cyberkriminelle haben erkannt, dass im Einsatz fremder Geräte für das Crypto-Mining ein erhebliches Ertragspotenzial liegt. Mit Schadprogrammen und im Verborgenen laufenden Skripten sorgen sie dafür, dass Rechner unbemerkt vom Nutzer zum Schürfen von Kryptogeld eingesetzt werden. Ihre Schadprogramme und Skripte verteilen sie über Websites oder App-Stores. Sie missbrauchen infizierte Smartphones und in großem

Umfang gekaperte Rechner, Rechnernetzwerke, WiFi-Hotspots und sogar Rechenzentren zum Mining. Die dadurch erzielten Erlöse fließen in die Taschen der Cyberkriminellen. Diese Art des Crypto-Mining wird Crypto-Jacking (von engl. Hijacking, entführen) genannt. Crypto-Jacking steht für den unrechtmäßigen, missbräuchlichen Einsatz von Mining-Skripten, während Crypto-Mining die legitime Nutzung von Mining-Skripten bezeichnet. Mining kann auf viele Arten durchgeführt werden. In diesem Dokument bezieht sich Crypto-Mining auf die Anwendungsfälle „Webseite“ sowie als ergänzende Funktionalität einer (mobilen) App.

WIE FUNKTIONIERT CRYPTO-MINING?

JavaScript auf einer Webseite

JavaScript ist eine Programmiersprache, die auf dem Gerät eines Nutzers ausgeführt werden kann. Webseitenbesitzer können ein in JavaScript geschriebenes Skript in ihr Webangebot integrieren. Der Browser lädt es auf der Website und es wird auf dem Gerät des Webseitenbesuchers ausgeführt. Aufgrund dieser Funktionalität bieten Crypto-Mining-Dienstleister wie zum Beispiel Coinhive, CoinImp oder Crypto-Loot in JavaScript geschriebene Mining-Skripte an. Sie werden über Websites an die Geräte der Websitebesucher verteilt. Das ausgelieferte Skript startet im Browser die Rechenoperationen, die zum Schürfen von Kryptogeld notwendig sind und liefert die Ergebnisse an den Betreiber zurück. Der so erwirtschaftete Gewinn fließt an den registrierten Kunden des Crypto-Mining-Dienstleisters – abzüglich einer Provision für den Dienstleister. Kunde kann der rechtmäßige Betreiber einer Webseite sein, der so seine Angebote finanziert. Andererseits könnte es aber auch ein krimineller Angreifer sein, der sich Zugriff zum Webserver verschafft hat und diesen nun für sich arbeiten lässt. Der beschriebene Missbrauch ist deutlich häufiger der Fall.

Apps auf dem PC und Smartphone

Die Crypto-Mining-Funktionen können zudem direkt in die jeweilige App integriert sein und werden bei der Nutzung der App im Hintergrund ausgeführt. In vielen Fällen verbreiten sich diese Apps auch auf andere Rechner im Netzwerk.

CRYPTO-MINING AUS SICHT DER VERBRAUCHER

Crypto-Mining bzw. Crypto-Jacking erfolgt häufig ohne die Zustimmung oder das Wissen des Nutzers.

Es verursacht durch den zusätzlichen Stromverbrauch in erster Linie Kosten und mindert häufig die Arbeitsgeschwindigkeit eines Geräts. Das geht teilweise so weit, dass von Crypto-Jacking betroffene Geräte nur noch eingeschränkt oder überhaupt nicht mehr genutzt werden können.

Auf mobilen Geräten reduziert Crypto-Mining signifikant die Dauer des Batteriebetriebs. Es führt in manchen Fällen zur Überhitzung oder zu irreparablen Schäden am Gerät. Crypto-Mining verletzt zudem eventuell Softwarerechte und öffnet mögliche Hintertüren für die Übermittlung von Schadcode.

Problematisch ist Crypto-Mining auch auf Fremdgeräten, zum Beispiel in Unternehmensnetzen, wenn hier nicht die eigenen Ressourcen des Mitarbeiters genutzt werden, sondern die Dritter – ohne deren Zustimmung. Der Besuch einer Webseite oder die Nutzung einer App mit Crypto-Mining verstößt möglicherweise gegen die Unternehmensrichtlinien.

Aufgrund dieser teils massiven Konsequenzen ist es notwendig, dass Nutzer über den richtigen und rechtmäßigen Einsatz von Crypto-Mining informiert und ihnen mögliche Konsequenzen aufgezeigt werden.

CRYPTO-MINING AUS SICHT EINES WEBSEITENBETREIBERS ODER APP-HERSTELLERS

Crypto-Mining auf einer Webseite oder als Teil einer App einzusetzen, ist für den Betreiber mit einem Risiko verbunden.

Der Einsatz kann schnell dazu führen, dass die Webseite von Browsern, Schutzsoftware und Werbeblockern gesperrt wird. Apps mit Mining-Funktionen werden aus den gängigen App-Stores entfernt. Im schlimmsten Fall werden sämtliche Angebote eines Herstellers aus dem App-Store verbannt, selbiges kann auch einem Webseitenbetreiber widerfahren. In beiden Fällen drohen Betreibern Umsatzeinbußen, da ihr Angebot nicht mehr erreichbar oder verfügbar ist.

Deshalb ist es für Betreiber erforderlich, dass sie sich an eine saubere Implementierung halten, um einen Eintrag auf einer Blacklist oder ein Entfernen ihres Angebots zu vermeiden. Für den legitimen Einsatz von Crypto-Mining sollten also Spielregeln gelten.

EMPFEHLUNGEN FÜR DEN LEGITIMEN EINSATZ VON CRYPTO-MINING

1. Betreiber einer Webseite oder Hersteller einer App müssen den Nutzer explizit darauf hinweisen, dass die Webseite oder die App Crypto-Mining durchführt und dabei auf die Ressourcen des Nutzers zugreift.
2. Der Nutzer muss für den Einsatz von Crypto-Mining explizit per Opt-in seine Einverständniserklärung geben.
3. Der Nutzer muss den Crypto-Mining-Prozess jederzeit beenden können.
4. Der Hinweis, die Einverständniserklärung und das Beenden des Crypto-Minings müssen für den Nutzer klar erkennbar („Accessibility Guidelines“) und zweifelsfrei bedienbar sein.
5. Der Hinweis, die Einverständniserklärung und das Beenden des Crypto-Minings erfolgen anhand geltender Interface-Standards.
6. Das Risiko, Schadcode zu übermitteln, ist geringstmöglich zu halten. Dabei sollte der eingesetzte Code nicht von der Standardkonfiguration des eingesetzten Crypto-Mining-Tools abweichen, um eine mögliche Verschleierung von Schadsoftware auszuschließen. Bei Apps dient hier der BSI-Standard als Grundlage.
7. Der eingesetzte Code darf ausschließlich für Crypto-Mining verwendet werden. Eine andere Nutzung – zum Beispiel als Bundle/Paket mit Funktionen wie Werbung oder Tracking – muss explizit ausgeschlossen werden.
8. Der eingesetzte Code muss jederzeit maschinenlesbar sein. Die Verschleierung von URLs und JavaScript-Code sollte unterbleiben.
9. Beim Einsatz von Crypto-Mining muss sichergestellt werden, dass die Ressourcen des genutzten Geräts nicht überbeansprucht werden. Die reguläre Nutzung seitens des Nutzers darf nicht beeinträchtigt werden und das Gerät darf durch das Mining keinen physischen Schaden erleiden. Idealerweise kann ein Nutzer die maximale CPU-Last begrenzen.
10. Der Betreiber einer Webseite muss sicherstellen, dass die Nutzung von Crypto-Mining gegenüber den Webseitenbesuchern transparent erfolgt und er muss sämtliche datenschutzrelevanten Informationen bereitstellen.

SCHLUSSWORT

Crypto-Mining könnte sich zukünftig als eine alternative Möglichkeit zur Finanzierung von Websites etablieren. Neben der Onlinewerbung hätten Betreiber von Internetangeboten damit eine weitere Möglichkeit, hochwertigen Content oder andere Inhalte zu finanzieren.

Die Autoren schlagen mit diesem Dokument Rahmenbedingungen vor, die als Grundlage für einen fairen Einsatz von Crypto-Mining dienen sollen. Dabei haben sie versucht, die Interessen aller Stakeholder zu berücksichtigen – sowohl die Sicht der Betreiber von Webseitenangeboten als auch die der Besucher. Dadurch sollen die Spielregeln aufgestellt werden, die es ermöglichen, dass Crypto-Mining sich künftig als Geschäftsmodell für Webseitenbetreiber und App-Entwickler etablieren kann.

Die Autoren empfehlen internationalen Gremien beziehungsweise Organisationen, auf der Grundlage der Ideen in diesem Dokument technische Standards für das Crypto-Mining zu definieren.

ÜBER DIE AUTOREN

Ralf Benzmüller

Unter der Leitung von Ralf Benzmüller entstanden in Bochum seit 2004 die G DATA SecurityLabs. Dort war er verantwortlich für die Entwicklung von effizienten Analyseverfahren und die Integration von proaktiven Schutztechnologien gegen Malware-Bedrohungen. Ralf Benzmüller ist Autor zahlreicher Fachartikel über Online-Bedrohungen. Er ist u.a. Mitglied des BSI-Expertenkreis Cyber-Sicherheit, der eco Kompetenzgruppe Sicherheit sowie Dozent an mehreren Hochschulen.

Michael Hausding

Michael Hausding verantwortet bei SWITCH, der Registrierungstelle für .ch und .li Domain-Namen, den Competence Lead DNS & Domain Abuse. Außerdem ist er Incident Handler bei SWITCH-CERT und Trainer für Incident Response bei FIRST, dem weltweiten Forum of Incident Response and Security Teams. Er engagiert sich ferner als Vorstandsmitglied im ISOC Switzerland Chapter sowie in der Swiss Internet Security Alliance. Michael Hausding hat Informatik an der Technischen Universität Darmstadt studiert und einen MAS in Management, Technology and Economics von der ETH Zürich.

Patrick Koetter

Patrick Koetter ist CEO der sys4 AG, Experte für E-Mail-Sicherheit und Leiter der eco Kompetenzgruppen Anti-Abuse und E-Mail. Er berät Behörden und Unternehmen bei Planung, Aufbau und Betrieb sicherer E-Mail-Plattformen. In Internet-Standardisierungsgremium IETF wirkt er aktiv an der Schaffung neuer Sicherheitstechnologien für E-Mail und andere Dienste mit.

Peter Meyer

Peter Meyer ist bei der eyeo GmbH als Projektmanager IT-Sicherheit tätig. Er ist Referent und Fachautor zahlreicher Veröffentlichungen mit den Schwerpunkten IT Security Awareness (Phishing, Botnetze, Malvertising und Online-Betrug). Zudem ist er Mitglied des Expert Boards beim EU-Projekt Cyberwiser.eu und des Kölner Security Startups SoSafe. Darüber hinaus ist er in den Arbeitsgruppen Anti-Abuse und Sicherheit beim eco Verband aktiv, wo er die Projekte Botfrei, SIWECOS und das EU-Projekt ACDC geleitet hat.