WEBWELT & TECHNIK LUKRATIVE ANGRIFFE

So nutzen Hacker den Kryptowährungsboom für sich aus

Von Benedikt Fuest | Stand: 06:00 Uhr | Lesedauer: 4 Minuten

Die massiven Kurssteigerungen bei Bitcoin und Co. ziehen auch immer mehr Kriminelle an. Für ihre Machenschaften nutzen die Hacker auch Computer von nicht Bitcoin-Besitzern. Und verdienen daran gutes Geld.

Als der Start-up-Gründer Noah Dinkin vor zwei Wochen in einem Starbucks-Cafe seinen Rechner ins lokale Drahtlosnetzwerk einwählte, wunderte er sich, wie langsam Webseiten luden – und suchte nach der Ursache. Prompt bemerkte er, dass unbekannte Angreifer das Starbucks-WLAN für eigene sinistre Zwecke gekapert hatten.

Die Täter ließen in den Internetbrowsern auf den Rechnern der Starbucks-Besucher ein kleines Skript laufen. Seine Aufgabe: Münzen der Kryptowährung Monero „minen“ – der Fachbegriff für das Schürfen von Digitalwährungen. Was die Hacker lockt, ist dabei nicht die Software der gehackten Geräte, sondern ihre Rechenleistung. Hintergrund ist, dass das Schürfen von Kryptowährungen sehr energieaufwändig ist. Die Hacker steuern die Rechenleistung der gekaperten PCs und Mobiltelefone den Netzwerken bei, in denen die Digitalwährungen erschaffen und Transaktionen vorgenommen werden – und werden im Gegenzug ihrerseits mit dem digitalen Geld bezahlt.

Auch wenn jeder Besucher nur wenige Minuten Rechenzeit unfreiwillig zur Verfügung stellt, lohnt sich in Summe der Aufwand für die Täter. Im konkreten Fall generierten die Hacker Monero-Coins auf Kosten anderer. Dinkin beschwerte sich prompt bei Starbucks via Twitter, die Admins der Kaffee-Kette versprachen Besserung. Doch Starbucks ist nicht das einzige Opfer.

LESEN SIE AUCH

WELT+ KRYPTOWÄHRUNGEN

Die Konkurrenten des Bitcoin sind deutlich effizienter

Während im Falle des Bitcoin mittlerweile ganze Warenhäuser voller Spezial-Computer notwendig sind, um neue Münzen zu erschaffen, reichen bei Kryptowährungen wie Monero noch normale PCs aus. Tatsächlich verzeichnen Monero und Co im Schatten des aktuellen Bitcoin-Booms enorme Kursgewinne. Und das wiederum löst eine Flut neuer Hackerangriffe aus: „Mining auf Kosten anderer ist keineswegs neu – aber mittlerweile lohnt es sich auch bei zuvor obskuren Kryptowährungen“, erklärt Candid Wüest, Sicherheitsforscher bei Symantec.

In einer neuen Studie haben die Symantec-Experten die Folgen des Kryptogeld-Booms auf die Sicherheit im Netz ausgewertet und kommen zu dem Schluss: Von September bis November hat sich die Anzahl der Angriffe verzehnfacht – und der Trend hält an.

Angriffe sind einfach zu einfach

Dabei spielt auch eine Rolle, wie einfach ein Angriff ist, erklärt Wüest: „Die Hacker müssen lediglich ungeschützte Webserver finden und dann drei Zeilen Programmcode in eine Webseite einfügen.“ Bei jedem Besucher der Webseite läuft dann im Hintergrund ein Programm, das die Rechenleistung des jeweiligen Rechners für Mining-Zwecke kapert. Die Koordination der verteilten Rechenaufgaben übernehmen Plattformen wie Coinhive, die die entsprechenden Programmskripte eigentlich für legale Zwecke zur Verfügung stellen.

Die Opfer merken von der Attacke meist nichts, da die Täter den jeweiligen Computer nicht komplett blockieren. „Manche Angriffe öffnen einfach ein kleines Pop-up-Fenster und minimieren es im Hintergrund – so bleibt das Mining länger unentdeckt“, erklärt Wüest. „Die Administratoren der jeweiligen Webseiten merken meist ebenfalls nicht, dass ihre Webseiten verändert wurden – ihnen schadet die Attacke schließlich nicht direkt.“

Wüest und seine Kollegen stoßen aktuell immer öfter auf kreative Versuche, mit Kryptomining auf fremden Rechnern reich zu werden: „Da gab es etwa einen Systemadministrator in einem größeren Unternehmen, der einfach bei tausenden

Computern über Nacht ein Miningskript laufen ließ – das fiel zunächst nicht auf, da die Geräte öfters mal für Fernwartung nachts angeschaltet wurden."

Auch auf Mobiltelefonen versuchen die Täter abzuräumen: 2017 fanden die Symantec-Forscher bereits 35 harmlos erscheinende Apps in Android-Appstores, die im Hintergrund den Akku der Mobilgeräte mit rechenintensiven Kryptomining-Aufgaben leerten.

Experten rechnen mit steigenden Angriffszahlen

Doch nicht nur per Mining profitieren Hacker vom Kryptocoin-Boom: „Auch die Zahl klassischer Attacken hat zugenommen", weiß Wüest. „Etwa indem Täter gezielt in Foren und sozialen Netzwerken Bitcoin-Investoren heraussuchen und dann per Spearfishing-Attacke gezielt deren digitale Geldbörsen leerräumen." Bei Spearfishing-Attacken greifen Hacker gezielt einzelne Opfer an und versuchen maßgeschneiderte Attacken.

Als aufgrund des Ansturms neuer Nutzer die Webseiten diverser populärer Bitcoin-Handelsplätze zusammenbrachen, meldeten sich die Täter teils per Telefon bei empörten Stammkunden der Handelsplätze, gaben sich als Supportmitarbeiter aus und überredeten ihre Opfer zur Herausgabe von Passwörtern. Anschließend räumten sie die digitalen Geldbörsen leer.

LESEN SIE AUCH

WELT+ DIGITALWÄHRUNG

Dieses neue Risiko bedroht den Bitcoin-Hype

Ein wenig raffinierter gingen die Täter vor, die unter leicht abgewandelten Namen gefälschte Versionen populärer Wallet-Apps für Mobiltelefone veröffentlichten. Die Apps täuschten den Nutzern vor, sichere Aufbewahrungsorte für Bitcoin und Co zu sein. Unsichtbar, also im Hintergrund reichten sie die Passwörter und Kontodaten der Nutzer an die Hacker weiter, die prompt die Konten leerräumten.

Solange der Kryptowährungsboom anhält, rechnen die Symantec-Forscher mit einer steigenden Zahl von Attacken: „Für Angreifer lohnt sich der Krypto-Diebstahl aktuell sehr – erfolgreiche Angriffe sind zudem teils erschreckend einfach."