Bankraub 4.0

Wie Cracker Millionen in Kryptowährungen stehlen

Statt Brechstange und Schneidbrenner benutzen moderne Bankräuber Computer und Internet: Damit brechen sie bei Bitcoin-Händlern und -Börsen ein und räumen über Nacht Coins im Wert Hunderter Millionen Euro von den Wallets der Kunden ab. Sicherer sind Ihre Bitcoins unter der heimischen Matratze.

Von Mirko Dölle

Bankraub ist ein aufstrebendes Gewerbe: Seit dem Jahreswechsel erbeuteten Cracker Kryptowährungen im Wert von rund 650 Millionen Euro. Statt mit Brechstange und Schneidbrenner umständlich Banktresore aufzustemmen, brechen die Bankräuber von heute mit Computer und Internetzugang bei einer Bitcoin-Börse oder einem Händler von Kryptowährungen ein und plündern dort die Konten (Wallets) der Kunden.

So wurde die italienischen Kryptogeldbörse Bitgrail Mitte Februar um Nano-Coins im Wert von knapp 150 Millionen Euro erleichtert. Bei Coincheck verschwanden Ende Januar über Nacht sogar 500 Millionen NEM (Handelskürzel: XEM) der gleichnamigen Kryptowährung im Wert von rund 500 Millionen Euro. Das war der bislang größte Krypto-Coin-Raubzug der Geschichte – die Täter erbeuteten fast zehn Mal so viel wie Anfang Dezember 2017 beim Einbruch beim Mining-Marktplatz Nicehash, wo 63 Millionen Euro geklaut wurden, oder beim Einbruch bei der Bitcoin-Börse Bitfinex Anfang August 2016, wo Bitcoins für 58 Millionen Euro verschwanden, oder einen Monat zuvor beim Etherum-DAO-Hack, wo 3,6 Millionen Ether mit einem Wert von gut 50 Millionen Euro abgezweigt wurden. Selbst mehr als 2014 beim legendären Hack der Bitcoin-Börse Mt. Gox, wo die Täter nur rund 350 Millionen Euro abzogen. Die etwa 4 Millionen Euro, die Unbekannte ebenfalls Ende Januar 2018 von IOTA-Wallets stahlen, sind dagegen fast schon Peanuts.

Online-Wallets heiß begehrt

Aber nur die großen Diebstähle bei Coincheck, Bitfinex, Mt. Gox und mutmaßlich Bitgrail sind mit einem klassischen Bankraub vergleichbar: In diesen Fällen bewahrten Kunden ihre Kryptogelder auf Online-Konten der jeweiligen Börse auf, sogenannten Online-Wallets, vergleichbar mit einem klassischen Online-Girokonto oder Aktiendepot.

Online-Wallets sind ein bequemer Weg, um mit Kryptowährungen zu handeln. Dazu legt der Kunde im Web-Frontend einer Bitcoin-Börse ein Konto in der gewünschten Währung an und erhält eine oder mehrere Adressen zugewiesen, an die er Gelder transferieren kann. Die gesamte Kontoverwaltung und auch Überweisungen werden im Browser getätigt, was es dem Kunden erspart, ein für die jeweilige Währung geeignetes Wallet-Programm zu installieren und die Blockchain der Währung herunterzuladen. Außerdem wickeln viele Börsen Käufe oder Verkäufe von Bitcoins über eigene Online-Wallets binnen Sekunden ab, auch wenn die Bestätigung in der Blockchain Stunden oder Tage dauert.

Was der Kunde meist nicht erfährt: Den zugehörigen privaten Schlüssel, mit dem alle Verfügungen über das Guthaben signiert werden müssen, behält allein die Bitcoin-Börse. Genau auf diese Schlüssel haben es die Räuber abgesehen, denn so können sie das Guthaben ohne Wissen der Kunden – und der Börsen – auf eigene Wallets überweisen. Da es bei den meisten Börsen auch keine Einlagensicherung gibt, hat der Kunde allein das Nachsehen. Sein Geld ist weg. Die Nutzung von Online-Wallets setzt also ein tiefes Vertrauen in die Sicherheitsmechanismen und die Liquidität der jeweiligen Online-Börse voraus.

Heimaufbewahrung

Die Lösung ist einfach: Schon Großmutter hat den Sparstrumpf unter der Matratze aufbewahrt, weil sie den Banken nicht vertraute. Indem Sie Ihr Wallet zu Hause

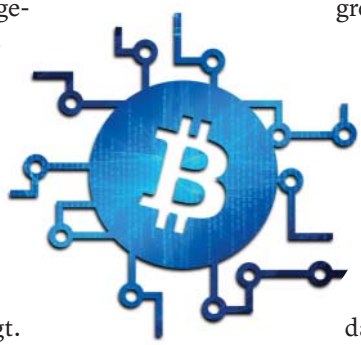
auf Ihrem eigenen PC erstellen und so die privaten Schlüssel lokal speichern, können Sie praktisch das Gleiche tun. Dazu benötigen Sie lediglich ein Programm wie Bitcoin Core, Electrum, Armory oder einen anderen der zahllosen Bitcoin-Clients für PC, Smartphone oder Tablet.

Bei den Wallet-Programmen unterscheidet man sogenannte Full-Clients und Light-Clients. Bitcoin Core gehört zu den Full-Clients, die für den Betrieb die vollständige Blockchain benötigen und diese tagesaktuell herunterladen. Das ist vor allem auf Rechnern mit SSDs ein Problem, denn die Bitcoin-Blockchain war Anfang Februar bereits 175 GByte groß – Tendenz stark steigend. Da wird der Platz auf der SSD schnell knapp, und der initiale Download beim ersten Start dauert je nach Internetanbindung etliche Tage. Dafür kann Bitcoin Core sämtliche Buchungen von Anbeginn der Blockchain selbstständig nachvollziehen.

Light-Clients wie Electrum und viele Bitcoin-Apps arbeiten ohne eigene Kopie der Blockchain. Sie fragen stattdessen einen Server, der eine Kopie der Blockchain besitzt, nach den Buchungen für die Adressen des Wallets. Die Electrum-Clients benötigen für den Betrieb also ein Netz von Electrum-Servern, die ihnen Auskunft geben. Außerdem müssen Sie darauf vertrauen, dass Ihnen die Server keine Buchungen unterschlagen. Gefälschte Buchungen kann ein Server jedoch nicht verbreiten – die Signatur der Transaktion würde nicht stimmen, und das kann ein Client leicht feststellen.

Hardware-Wallets wie die Digital Bitbox signieren Bitcoin-Transaktionen dank eingebautem Mikroprozessor selbst. Die privaten Schlüssel rücken sie nur als Backup an die mitgelieferte MicroSD-Karte heraus.

Die Wallets samt privaten Schlüsseln speichern die Bitcoin-Clients lokal, sodass sie sicher vor einem groß angelegten Raub bei den Börsen sind. Dafür droht Gefahr von Trojanern, sogenannten Bitcoin-Stealern. Sie durchsuchen den Rechner nach Bitcoin-Wallets der gängigen Clients und kopieren sie. Das ist besonders bei Bitcoin Core ein Problem, weil der Client standardmäßig ungeschützte Wallets erzeugt. Fällt ein solches einem Angreifer in die Hände, kann er sich nach Belieben bedienen.



Deshalb sollten Sie bei Bitcoin Core unbedingt Ihr Wallet über das Menü „Einstellungen“ unter „Brieftasche verschlüsseln“ mit einem starken Passwort versehen. Vollständig verschlüsselt, wie der Menüeintrag suggeriert, wird Ihr Wallet dadurch allerdings nicht: Die Transaktionen und Bitcoin-Adressen können Sie weiterhin auch ohne Passwort sehen. Nur der Zugriff auf die privaten Schlüssel ist mit dem Passwort gesichert, was wirksam unautorisierte Überweisungen verhindert. Das gilt aber auch für den Fall, dass Sie das Passwort vergessen – Sie kämen nicht mehr an Ihre Bitcoins heran.

Electrum fragt beim Anlegen eines neuen Wallets standardmäßig nach einem Passwort für die privaten Schlüssel, außerdem können Sie das Wallet vollständig verschlüsseln lassen, sodass auch niemand ohne das Passwort an Ihre Bitcoin-Adressen und damit Ihren Gesamtkontostand herankommt. Im Unterschied zu Bitcoin Core zeigt Electrum den Master Private Key jedes neu erzeugten Wallets in Form von dreizehn englischen Wörtern nach BIP-0039 (Bitcoin Improvement Proposal) an, den sogenannten Seed – und verlangt von Ihnen, dass Sie ihn auf Papier notieren und anschließend von Hand neu eingeben. Versuchen Sie gar nicht erst, Electrum durch Copy & Paste zu überlisten – die Zwischenablage leert das Programm vorsorglich, und ohne Eingabe der Wörter in der korrekten Reihenfolge wird das Wallet nicht erzeugt.

Sicherheit durch Offline-Wallets

Indem Sie die Wörter des Master Private Key aufschreiben, erzeugen Sie ein sogenanntes Paper Wallet als Backup Ihres Electrum-Wallets. Es ist die einfachste Form der Offline-Wallets oder Cold Storages, mit denen Sie Ihre Bitcoins außerhalb der Reichweite jeglicher Angreifer aus dem Internet aufbewahren können. Passen Sie auf Ihr Paper Wallet gut auf: Jeder, der den Seed kennt, kann frei und ohne jeglichen Passwortschutz über Ihr Guthaben verfügen.

Ein Nachteil des Paper Wallets ist, dass Sie daraus erst mit Electrum oder einem anderen Wallet-Client ein lokales Wallet erzeugen müssen, bevor Sie Ihr Guthaben transferieren können. Ein Paper Wallet taugt also nicht für den täglichen Einsatz, sondern nur als Backup oder langfristige Aufbewahrungsmöglichkeit. Die Alternative sind sogenannte Hardware Wallets, die ebenfalls zu den Offline-Wallets zählen und die privaten Schlüssel wirksam vor Angreifern schützen, aber deutlich komfortabler in der Handhabung sind.

Ein einfaches und mit knapp 100 Euro relativ günstiges ist die Digital Bitbox. Der unscheinbare schwarze USB-Stick enthält einen Mikroprozessor, der die privaten Schlüssel des Hardware-Wallets speichert und Bitcoin-Transaktionen eigenständig signiert – nachdem man das Wallet zunächst mit dem richtigen Passwort entsperrt und die Transaktion durch Anfassen des Sticks im richtigen Moment bestätigt hat. Der private Schlüssel verbleibt in der Bitbox. Um bei einem Hardware-Defekt nicht das gesamte Guthaben zu verlieren, gehört zum Lieferumfang des USB-Sticks eine MicroSD-Karte, die man seitlich in den Stick schieben und dann darauf ein Backup des Wallets speichern kann.

Der größte Nachteil der Digital Bitbox ist, dass man die Zieladresse und den Betrag der Transaktion nur auf dem Monitor des Rechners angezeigt bekommt. Man unterschreibt die Überweisungen quasi blind. Die Hardware-Wallets Ledger Nano S und der Trezor für jeweils rund 150 Euro beheben das Problem mit eingebauten Displays, auf denen sie Zieladresse und Betrag der zu signierenden Transaktion anzeigen. Im Hardware-Wallet können Sie Ihre Bitcoins wie Großmutter unter der Matratze verstecken und sicher sein, dass sie nicht in falsche Hände geraten. *(mid@ct.de)* c't