Fingerspitzen-gefühl

Bitcoin-Stealer, Fake-Anbieter und merkwürdige Geschäftsgebaren

Neben dem Kursverfall bedrohen Gauner, Malware und Trojaner das Vermögen der Bitcoin-Anleger. Dabei werden gezielt menschliche Schwächen ausgenutzt, insbesondere Gutgläubigkeit und Unaufmerksamkeit. Wir erklären Ihnen, wo Sie besonders aufpassen müssen.

Von Mirko Dölle

Seit Bitcoin populär wurde und sich auch Otto Normalverbraucher an Spekulationen mit der Kryptowährung beteiligt, haben Angreifer ein neues lukratives Ziel: Statt die Daten des Rechners zu verschlüsseln und Bitcoins zu erpressen, reißen sie sich direkt das Geld der arglosen Anwender unter den Nagel – oder tun kurzerhand beides.

Bitcoin-Stealer ist der Sammelbegriff für diese Art Trojaner, bekannte Vertreter sind CryptoShuffler, Neutrino oder CryptXXX. Um nicht von den gängigen Antivirenprogrammen gefunden zu werden, verkaufen Betrüger leicht zu bedienende Baukästen, die ständig neue Varianten erzeugen – bezahlt wird selbstverständlich mit Bitcoins. Ältere, direkt einsetzbare Varianten werden etwa bei Fraudsters.se ab 50 Euro angeboten.

Die einfachen Bitcoin-Stealer nutzen aus, dass es sich bei Bitcoin-Adressen um lange Buchstaben- und Zahlenkombinationen handelt, die sich ständig ändern und die sich niemand merkt. Deshalb kopiert man die Bitcoin-Adresse einer Börse oder eines Online-Shops in die Zwischenablage und fügt sie später im Bitcoin-Client als Empfängeradresse ein. Der im Hintergrund lauernde Bitcoin-Stealer überwacht die Zwischenablage, erkennt anhand des Formats, dass es sich um eine Bitcoin-Adresse handelt, und tauscht sie gegen eine Adresse seines Schöpfers aus.

Simple Bitcoin-Stealer fügen immer die gleiche Adressen ein oder erzeugen dynamisch eine beliebige neue, sodass sich die vom Anwender kopierte und die vom Stealer eingefügte Adresse meist stark unterscheiden. Hochwertigere Stealer verwenden hingegen gezielt Adressen, die dem Anfang der vom Anwender kopierten Adresse möglichst ähneln. So bleiben auch aufmerksamere Anwender arglos und führen die Transaktion aus – womit ihre Bitcoins unwiederbringlich auf einem Wallet des Gauners landen. Sie sollten sich deshalb die Mühe machen, zumindest Anfang und Ende der im Bitcoin-Client eingetragenen Adresse zu überprüfen.

Komplexere Bitcoin-Stealer überwachen nicht nur die Zwischenablage, sondern durchsuchen den Rechner zusätzlich nach Bitcoin-Wallets und kopieren sie. Das trifft vor allem Nutzer von Bitcoin Core; die Referenz-Implementierung für Bitcoin-Clients schützt Wallets standardmäßig weder mit einem Passwort noch verschlüsselt sie sie. Fällt ein solches Wallet den Gaunern in die Hände, können sie frei darüber verfügen. Deshalb sollten Sie Ihre Wallets bei Bitcoin Core am besten unmittelbar nach dem Erzeugen über das Menü „Einstellungen“ mittels „Brieftasche verschlüsseln“ zumindest mit einem Passwort versehen.

Der Bitcoin-Client Electrum verlangt zwar seit Langem die Vergabe eines Passworts für neue Wallets, neuerdings verschlüsselt er sie sogar vollständig. Anwender müssen jedoch mit den Updates am Ball bleiben und das Programm regelmäßig aktualisieren – denn ältere Versionen sind sogar über den Internet-Browser angreifbar.

Betroffen sind konkret die Electrum-Versionen bis 3.0.5. Dort ist aufgrund eines Bugs standardmäßig die Fernsteuerungsschnittstelle aktiviert, sodass Electrum auf einem zufällig ausgewählten UDP-Port auf Befehle wartet. Indem ein JavaScript-Programm die wahrscheinlichsten Ports scannt, kann es die Fernsteuerungsschnittstelle finden und ohne jegliche Authentifizierung kontaktieren – um anschließend etwa sämtliches Gut-

haben des gerade geöffneten Wallets an seinen Erschaffer zu transferieren. Solche JavaScript-Stealer werden gerne über Werbebanner auf fremden Websites eingeblendet, die mit dem Thema Bitcoin oder Kryptowährungen zu tun haben.

Trau, schau, wem!

Gefahr droht außerdem bei etlichen Online-Diensten. So gibt es unzählige Bitcoin-Adress-Generatoren, etwa bitaddress.org, die über ein JavaScript-Programm eine Bitcoin-Adresse nebst zugehörigem Public und Private Key im Browser erzeugen. Andere erzeugen Seeds für Wallets, etwa iotagenerator.info für die Kryptowährung IOTA. Vorgeblich sind die JavaScript-Programme sicher und reichen die erzeugten die Schlüssel respektive Seeds nicht an den Betreiber weiter – doch wer kann das schon selbst überprüfen?

Schlimmer noch, beide Websites arbeiten mit HTTP, sodass Angreifer den Code der JavaScript-Generatoren auf dem Weg durchs Internet spielend leicht manipulieren könnten, etwa über einen transparenten Proxy. Ende Januar 2018 verschwanden IOTAs im Wert von rund 4 Millionen Euro von privaten Wallets, weil die Angreifer offenbar die Seed kannten – spätestens seitdem stehen solche Online-Dienste unter Generalverdacht und sollten keinesfalls benutzt werden.

Zu den ebenfalls hochriskanten Diensten zählen Bitcoin-Mixer. Sie ermöglichen es rechtschaffenen Bürgern (aber auch Kriminellen), anonym mit Bitcoins zu handeln – was eigentlich unmöglich ist, da ja sämtliche Transaktionen in der Blockchain für jedermann nachvollziehbar dauerhaft gespeichert werden. Bitcoin-Mixer unterbrechen die Kette, indem sie für Einzahlungen ein anderes Wallet verwenden als für Auszahlungen und die Auszahlung auf Wunsch erst mehrere Stunden oder Tage später vornehmen. So stehen Ein- und Auszahlung in keinem logischen Zusammenhang miteinander.

Als Nutzer eines solchen Dienstes muss man darauf vertrauen, das eingezahlte Geld – abzüglich Bearbeitungsgebühr – auch wieder ausgezahlt zu bekommen. Als Vertrauensbeweis bieten viele Betreiber einen sogenannten Letter of Guarantee an, eine mit dem PGP-Schlüssel des Betreibers signierte Auflistung von Ein- und Auszahlungsadresse sowie den Beträgen. So sollen sich Nutzer im Zweifel beschweren und belegen können, dass ihr Geld nicht wieder ausgezahlt wurde.

Gelegenheit macht Diebe

Manche Bitcoin-Mixer versehen gelegentlich solche Letters of Guarantee mit einer gefälschten Signatur und zahlen auch das Geld nicht wieder aus, während alle anderen Kunden korrekt signierte Letters und auch ihr Geld erhalten. Betroffen sind davon meist Beträge im Bereich von mehreren hundert bis einigen tausend Euro. Dieses Vorgehen nennt man Selective Scam, selektiver Betrug: Beschwert sich

der Kunde, weist der Betreiber auf die falsche Signatur hin – somit steht der Kunde als Betrüger da, zumal es bei anderen Kunden keine Unstimmigkeiten gab. Auf diese Weise können Bitcoin-Mixer über Monate hinweg Gelder stehlen, bevor sie als Betrüger entlarvt werden.

Noch dreister sind Plagiateure, die bekannte Bitcoin-Mixer kopieren und so vom Renommee der Originale profitieren. Der wohl prominenteste Fall ist der des Bitcoin-Mixers Helix Light. Der Dienst der nur über das Tor-Netz erreichbaren Suchmaschine Grams mit der Adresse grams7enufi7jmdl.onion genoss einen ausgezeichneten Ruf, schnell und ehrlich zu sein – wurde jedoch Mitte Dezember 2017 eingestellt. Das hindert Plagiateure nicht daran, bis heute optisch nahezu perfekte Fakes unter ähnlichen Adressen anzubieten – zum Beispiel unter grams7enqfy4nieo.onion. Dabei nutzen die Betrüger aus, dass sich viele Nutzer nur den Anfang der Tor-Hostnamen merken – und nicht auf das Ende achten.

Einkassiert statt ausbezahlt

Selbst Online-Wallet-Anbieter und Bitcoin-Börsen, denen viele Anleger ihr Kryptogeld bedenkenlos anvertrauen, sollte man kritisch beobachten. Wichtig ist vor allem eine Einlagensicherung, sodass man sein Geld wiederbekommt, falls der Betreiber wie in den Fällen von Mt. Gox, Coincheck oder Bitgrail gehackt und beraubt wird.

Andererseits sollte der Betreiber dem Kunden die Gewinne aus Bitcoin-Forks aber auch ausbezahlen. Doch das passiert nur in den seltensten Fällen, meist kassieren die Betreiber diese Gelder stillschweigend. Ein Grund für diese Praxis ist, dass insbesondere Bitcoin-Börsen die ihnen anvertrauten Kundenvermögen auf sogenannten Cold Storages vor automatischen Zugriffen geschützt aufbewahren.

Bei den Hard-Forks des Bitcoin, wobei am 1. August 2017 die neue Währung Bitcoin Cash und am 28. Februar 2018 Bitcoin Private entstanden, wurden allen Bitcoin-Adressen, auf denen sich zum Zeitpunkt des Forks ein Guthaben befand, die gleiche Menge der neuen Währung gutgeschrieben. Da die Bitcoin-Börsen ihren Kunden meist nur Einzahlungsadressen und keine separaten Online-Wallets zuordnen und die eingezahlten Bitcoins aller Kunden regelmäßig gesammelt ins Cold Storage transferieren, liegen die Bitcoins des Kunden während des Forks auf einer Adresse des Betreibers und nicht mehr auf der Einzahlungsadresse. Die Bitcoins werden so zu einem reinen Buchwert, das Guthaben wird wie bei einem Online-Girokonto nur noch in der Datenbank verwaltet – allerdings in Bitcoin und nicht in Euro. Die Börsen könnten die Bitcoins ihrer Kunden sogar verkaufen und so selbst mit der Kryptowährung spekulieren, ohne dass der Kunde dies bemerkt.

Damit der Kunde etwa seine Bitcoin Private aus dem letzten Bitcoin-Fork erhält, müsste die Börse zunächst die Bitcoin Private für sich beanspruchen und dann jedem Kunden seinen Anteil ausbezahlen. Statt diesen Aufwand zu treiben und den Kunden zu informieren, behalten viele Bitcoin-Börsen kurzerhand das Geld und freuen sich über den Extra-Gewinn.

Solche unechten Online-Wallets sind also doppelt gefährlich: Man muss nicht nur aufpassen, dass sich Langfinger nicht am Bitcoin-Vermögen vergreifen, sondern auch, dass nicht der eigene Geschäftspartner hinterrücks die Hand aufhält. Deshalb bewahrt man seine Bitcoins am besten zu Hause in seinem eigenen Wallet auf. So fließt das Geld beim nächsten Fork mit Sicherheit in die eigene Tasche.

(mid@ct.de) c't