Spurensicherung

Wie die Blockchain Kriminelle überführt

Als die Betreiber der Drogen-Handelsplattform Wall Street Market mit den Bitcoins ihrer Kunden untertauchen wollten, klickten die Handschellen. Möglich wurde das durch kleine Fehler der Täter und die Analyse der Blockchain. Das lässt hoffen, dass die Behörden auch die Einbrecher schnappen können, die die Kryptobörse Biance um 7000 Bitcoin erleichtert haben.

Von Mirko Dölle

Die Admins des Wall Street Markets hatten sich gerade die Bitcoins ihrer kriminellen Kundschaft unter den Nagel gerissen und wollten untertauchen, als die Polizei ums Eck kam. Einem der drei Täter kamen die Ermittler im Wesentlichen durch intensive Analyse der Bitcoin-Geldflüsse mittels der Blockchain auf die Schliche – und das, obwohl die Täter die Bitcoins in einem Mixer gewaschen hatten.

Die Festnahme der Admins des weltweit zweitgrößten Darknet-Markets Ende April ist nicht der erste Fall, in dem die Blockchain eine entscheidende Rolle spielte: Auch der Admin des größten deutschen Darknet-Forums „Deutschland im Deep Web“ wurde enttarnt, weil die Ermittler mittels Blockchain den Weg von Geldern nachvollziehen konnten. Im Fall des Foren-Admins Alexander U. waren es Spendengelder, die U. angeblich über die Kryptobörse Bitcoin.de umtauschte und auf seinem Girokonto gutschreiben ließ.

Beweiskette

Einer der drei Admins von Wall Street Market verriet sich nach Angaben der Ermittler durch Unachtsamkeit: Anstatt wie sonst in der Szene mit Tor zu arbeiten, verwendeten Tibo L. und Jonathan K. lediglich ein VPN, um sich auf dem Darknet-Server einzuloggen. L. beging den Fehler, nach einem Zusammenbruch der VPN-Verbindung weiterzuarbeiten – sodass die IP-Adresse seines Internetanschlusses sichtbar wurde. K. wurde durch eine Korrelationsanalyse enttarnt: Die Ermittler fanden heraus, dass K. immer dann eine Verbindung zu einem bestimmten VPN-Provider aufbaute, wenn auf den Admin-Bereich des Markets zugegriffen wurde.

Den entscheidenden Hinweis, um den dritten Admin, Klaus-Martin F., zu überführen, fanden die Ermittler des US Postal Inspection Service in der Blockchain. Bereits im Vorfeld hatte das BKA entdeckt, dass der Admin von Wall Street Market denselben PGP-Schlüssels verwendete wie ein Benutzer des im letzten Jahr beschlagnahmten Hansa Market. Dort hatte F. für Auszahlungen eine Bitcoin-Adresse angegeben. Die Bitcoins dieser und anderer Adressen des Wallets wusch F. in einem Bitcoin-Mixer – dazu später mehr –, transferierte sie auf ein neues Wallet und bezahlte damit eine Bestellung. Doch die Geldwäsche war nutzlos, die Experten des US Postal Inspection Service konnten die Zahlung trotzdem nachvollziehen. So mussten die Ermittler nur noch die Kundendaten über den Zahlungsdienstleister erfragen, um F. zu enttarnen und anschließend festzunehmen.

Virtuelle Geldbörsen

Wie kompliziert solche Ermittlungen sind, wird einem erst bewusst, wenn man sich ins Gedächtnis ruft, dass die Blockchain selbst keine Wallets kennt. Für die Blockchain existieren lediglich einzelne, unzusammenhängende Adressen, auf die zu einem beliebigen Zeitpunkt in der Vergangenheit Bitcoins transferiert wurden.

Früher war ein Bitcoin-Wallet eine Datenbank, in der man den öffentlichen und den privaten Schlüssel seiner je nach Bedarf erzeugten Bitcoin-Adressen speicherte. Oftmals verwendete man dauerhaft dieselbe Adresse für mehrere Transaktionen. Ging das Wallet mit den Schlüsseln verloren, kam man nicht mehr an seine Bitcoins heran.

Heute wird der Begriff Wallet aber meist als Synonym für ein Hierarchical Deterministic Wallet (HD-Wallet) benutzt: Hier wird ein sogenannter Seed, den man sich in 12 oder 24 Wörter umgewandelt leicht aufschreiben kann, als Basis zur Erzeugung der ersten Bitcoin-Adresse verwendet. Für die Schlüssel der nächsten und aller weiteren Bitcoin-Adressen wird nur eine Zählvariable dieser Basis um eins erhöht. So muss man nur noch den Seed aufbewahren und kann damit jederzeit die Schlüssel aller Adressen neu generieren. Ein HD-Wallet ist also üblicherweise die Sammlung der Schlüssel aller Bitcoin-Adressen, die mit dem selben Seed erzeugt wurden.

Da die Bitcoin-Adresse ein vereinfachter Hash des Schlüssels ist, können Außenstehende aber nicht feststellen, ob zwei Bitcoin-Adressen mit demselben Seed erzeugt wurden, also zum selben Wallet gehören, oder nicht. Die Anonymität bleibt grundsätzlich gewahrt. Es sind die Geldflüsse, mit denen sich der Täter selbst verraten hat.

Spurensuche

Ausgerechnet beim Versuch, Gelder von einem Darknet-Marktplatz in Sicherheit zu bringen, in einem Bitcoin-Mixer zu waschen oder es auszugeben, hinterlassen die Täter nachverfolgbare Spuren in der Blockchain. Und das funktioniert so: Wer etwa 2 Gramm Cannabis für 20 Euro im Darknet kauft, bekommt vom Marktplatz oder vom Drogenhändler eine Bitcoin-Adresse für die Überweisung genannt. Damit die Zahlung leicht dem Einkauf zugeordnet werden kann und man außerdem nicht die Zahlungen anderer Käufer sieht, bekommt man für jeden Einkauf eine eigene Bitcoin-Adresse.

Doch wenn der Händler die Bitcoins zum Waschen an einen Bitcoin-Mixer schickt oder der Darknet-Marktplatz die Gelder aus den letzten Geschäften an den Händler transferiert, werden die einzelnen Kleinbeträge zu einem größeren Betrag zusammengefasst: Die Quelle der Transaktion sind die vielen Bitcoin-Adressen aus den einzelnen Käufen, das Ziel ist eine einzelne Adresse im Wallet des Händlers oder im Bitcoin-Mixer.

Haben die Behörden im Rahmen ihrer Ermittlungen auch etwas eingekauft, so können sie durch diese zusammenfassen-

de Transaktion die Käufe anderer Kunden identifizieren und, wenn etwa jemand die Bitcoins unter seinem richtigen Namen bei einer Kryptobörse gekauft hat, deren Adressen ermitteln. Dies kann übrigens jeder selbst nachvollziehen: Die Website walletexplorer.com wertet solche Indizien automatisch aus und ordnet einzelnen Adressen, die miteinander in Beziehung stehen, virtuellen Wallets zu, sodass man Geldflüsse gut nachvollziehen kann.

Schlechter Mix

Durch den Einsatz eines Bitcoin-Mixers wähnt sich der Drogenhändler in Sicherheit. Dessen Aufgabe ist es, den durch die Blockchain für jedermann transparenten Geldfluss zu verschleiern. Dazu verwendet der Mixer im einfachsten Fall zwei verschiedene Wallets: Kunden, die Bitcoins auf dem ersten Wallet einzahlen, bekommen eine Überweisung aus dem zweiten Wallet – und andere Kunden lässt man auf das zweite Wallet einzahlen und bedient sie aus dem ersten. Einen in der Blockchain nachvollziehbaren Zusammenhang zwischen Ein- und Auszahlung gibt es auf diese Weise nicht; theoretisch könnte nur der Mixer-Betreiber den Zusammenhang herstellen. Dafür erheben die Dienste eine Service-Gebühr von üblicherweise ein bis drei Prozent.

Die Ermittler profitieren an dieser Stelle von der Gier und dem Misstrauen der Kriminellen: Niemand zahlt freiwillig eine hohe Gebühr, schon gar nicht bei großen Geldbeträgen, wie sie beim finalen Absahnen der Wall-Street-Market-Admins oder bei geschäftigen Drogenhändlern anfallen. Deshalb sind der eingezahlte und der vom Mixer ausgezahlte Betrag nahezu gleich groß.

Hinzu kommt, dass Mixer-Betreiber generell im Verdacht stehen, gelegentlich zu betrügen und eingegangene Gelder nicht wieder auszuzahlen – Anzeigen ihrer kriminellen Kundschaft müssen sie schließlich nicht fürchten. Lange auf das gewaschene Geld warten möchte man deshalb nicht.

Beides spielt den Ermittlern unmittelbar in die Hände: Die Sammel-Einzahlung der Kleinbeträge beim Mixer lässt sich leicht in der Blockchain nachvollziehen, inklusive der Gesamtsumme. Nun braucht man nur noch nach Transaktionen in den nächsten ein bis zwei Dutzend Blöcken zu suchen, bei denen ein ähnlicher, wenige Prozent niedrigerer Geldbetrag transferiert wird und der in keinem Zusammenhang mit einer Einzahlung aus dem Zeitraum steht. Von den etwa 50.000 bis 100.000 Transaktionen der infrage kommenden Blöcke sind das nur einige wenige.

Erst die Ware, dann die Polizei

Anschließend müssen die verdächtigen Transaktionen lediglich in der Blockchain weiter beobachtet werden. Im Fall des Admins F. von Wall Street Market warteten die Ermittler, bis er mit den Bitcoins online einkaufte und sie an einen Zahlungsdienstleister transferierte. Von dem Zahlungsdienstleister besorgten sie sich dann die Kundendaten der bezahlten Bestellung – und hatten so Klaus-Martin F. enttarnt. Mit dem Paket kam auch die Polizei.

Der Erfolg im Fall Wall Street Market macht Hoffnungen, dass die Ermittler auch die Einbrecher bei der Kryptobörse Biance aufgreifen können: Diese hatten durch Hacking-Angriffe Zugriff auf das Hot Wallet, also quasi die Bargeldkasse des Unternehmens. Dort stahlen sie am 7. Mai 7074 Bitcoins im Wert von damals fast 40 Millionen Euro – durch den zwischenzeitlichen Kursanstieg ist die Beute heute über 50 Millionen Euro wert. Doch die Krux ist es, die Bitcoins umzutauschen – entweder in andere Kryptowährungen, in Papiergeld oder in Waren. Und genau hier stehen die Biance-Einbrecher vor denselben Herausforderungen wie die Admins von Wall Street Market. Die Ermittler warten nur darauf, dass die Täter weitere Indizien liefern oder einen klitzekleinen Fehler machen. *(mid@ct.de)* c't