Tracking von Bitcoin-Zahlungen

Hacking Session – Praktische Demonstrationen zur IT-Sicherheit

EDV-Gerichtstag Saarbrücken, 20. 9. 2017

Jörn Erbguth, IT & Law Consultant

joern@erbguth.ch +41 787256027

Lösegeldzahlungen in Millionenhöhe

ZDNet / Sicherheit / Cyberkriminalität

Ransomware: Webhoster zahlt 1 Million Dollar Lösegeld

Die Angreifer verschlüsselten die Daten auf 153 Servern und auch das Backup. Die zuvor auf Windows ausgerichtete Schadsoftware Erebus wurde für Angriffe auf Linux-Systeme modifiziert. Mit veralteter und angreifbarer Software machte es der südkoreanische Hoster den Erpressern leicht.

von Bernd Kling am 20. Juni 2017 , 18:47 Uhr

Ransomware verlangt meistens Lösegeldzahlungen in Bitcoin. Die Zahlungen gehen dabei teilweise in die Millionen.

Lösegeldzahlungen in Millionenhöhe

News

South Korean Bitcoin Exchange Hacked and $5 Million Stolen

April 30, 2017 SID 2343 Views 0 Comments bitcoin

Private Computer oder Bitcoin-Börsen werden gehacked und private Keys gestohlen, mit denen dann die Bitcoins transferiert werden können.

Quelle: https://latesthackingnews.com/2017/04/30/south-korean-bitcoin-exchange-hacked-5-million-stolen/

Die Bitcoins sind weg – was nun?

Klassische Maßnahmen gehen nicht:

- Überweisung zurückrufen ?
- Konto pfänden ?

Die Bitcoins sind transferiert. Die Zieladresse ist sichtbar – mehr aber auch erst einmal nicht.

Eine Bitcoin-Transaktion kann nicht rückgängig gemacht werden. Einmal auf der Blockchain, gibt es keine Einwirkungsmöglichkeit – vorher ggf. schon.

Es gibt auch keine Bank, die man nach dem Kontoinhaber des Zielkontos fragen kann und das Konto lässt sich auch nicht pfänden – zumindest nicht ohne zu wissen, wer den privaten Schlüssel hat.

Aber wie funktioniert eigentlich Bitcoin ? (1)

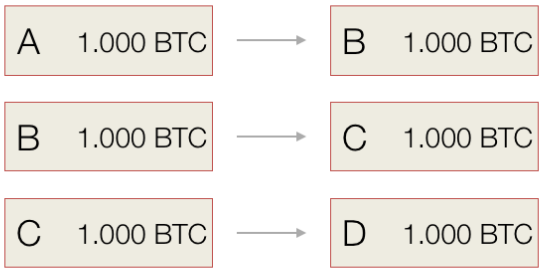
- Bitcoin ist dezentral
- Bitcoin ist pseudonym
- Bitcoin kennt keine Namen
  nur Konten und Transaktionen

Es gibt keine Zentrale Bitcoin-Stelle an die man sich wenden kann.

Auf der Bitcoin-Blockchain sind keine Namen eingetragen – es gibt nur die Bitcoin-Adressen – quasi die Kontonummern.

Aber wie funktioniert eigentlich Bitcoin ? (2)

- Bitcoin hält keine Kontostände
- Bitcoin nur Liste von Transaktionen zwischen Konten

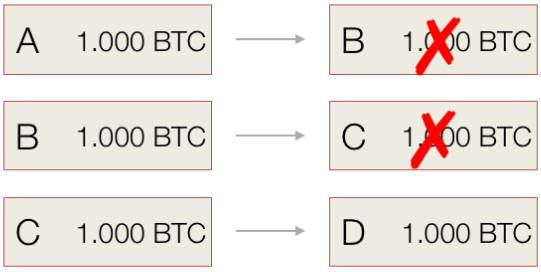


Bitcoin hat keine Kontostände – nur Transaktionen aus denen sich natürlich Kontostände berechnen lassen. Das macht auch Sinn. Schließlich hat jemand nur deshalb Bitcoins, weil sie ihm jemand übertragen hat. Bei den Mineuren ist es etwas anders.

Es wird empfohlen, dass ein Konto immer nur einmal verwendet wird. Konten können aber auch mehrfach verwendet werden. Die einzelnen Transaktionen, die auf einem Konto landen, werden jedoch trotzdem nicht auf der Blockchain saldiert, sondern werden separat weiter verwendet.

Aber wie funktioniert eigentlich Bitcoin ? (3)

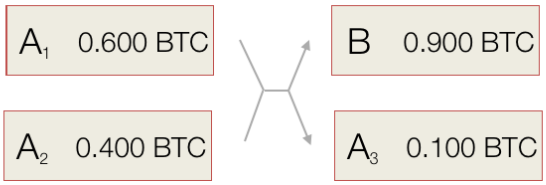
- Erhaltene Bitcoins werden immer komplett transferiert
- Die ursprüngliche Transaktion ist dann ausgegeben (spent)



Die über eine Transaktion erhaltenen Bitcoins werden vollständig weiter transferiert. Die ursprüngliche Transaktion ist damit ausgegeben. Das wird zwar nicht an der Transaktion vermerkt. Durch die Aufnahme der Folgetransaktion auf die Blockchain ist die Wirkung jedoch die gleiche.

Aber wie funktioniert eigentlich Bitcoin ? (4)

- Soll nicht der gesamte Betrag transferiert werden, wird auf ein anderes eigenes Konto zurücktransferiert
- Reicht ein Konto nicht aus, werden mehrere Konten kombiniert



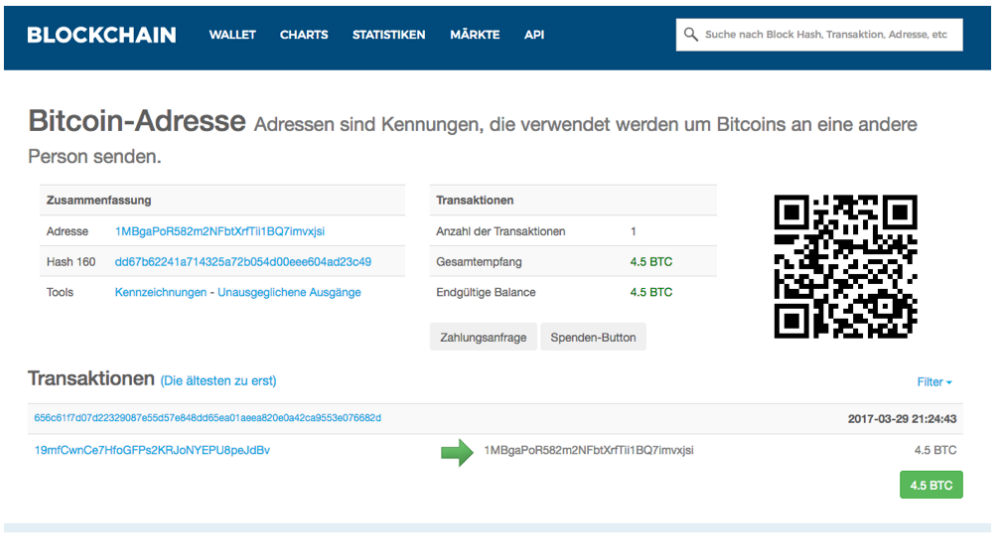
Um immer den passenden Betrag transferieren zu können, wird mit einer Art Wechselgeld gearbeitet:

Man transferiert den vollen Betrag aber teilt ihn auf zwei Konten auf – das Zielkonto und ein eigenes Konto.

Umgekehrt wird aber der Betrag einer eingegangenen Transaktion auch nicht immer reichen, um die gewollte ausgehende Transaktion zu tätigen. Deshalb lassen sich auch mehrere Konten auf Quellseite kombinieren.

Damit stellt sich eine Transaktion als eine Transaktion von mehreren Konten auf mehrere Konten dar. Genau damit lassen sich die Konten eines Nutzers verbinden. Mit dieser Transaktion wissen wir, dass Konto A1 und A2 dem Nutzer gehören und können vermuten, dass Konto B oder A3 ebenfalls zum Nutzer gehören. Da die Bitcoin-Blockchain öffentlich ist, können die einzelnen Transaktionen zu einem Netz zusammengefügt werden.

Sie haben Lösegeld gezahlt?

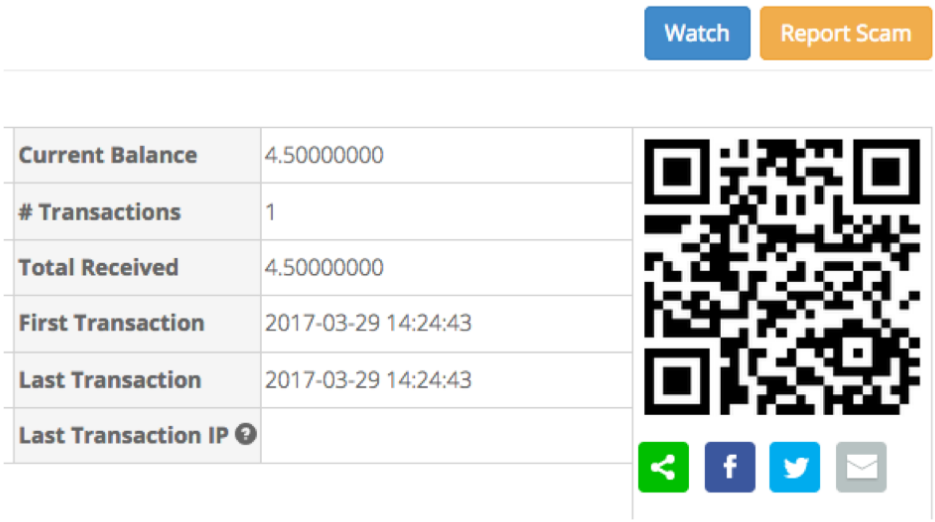


Sie haben Lösegeld gezahlt?

Sehen Sie sich die Zieladresse an! Liegt das Geld noch dort und sehen Sie auch keine andere Transaktion, können Sie nichts machen außer warten.

Naja – fast nichts.

Richten Sie einen Watch-Dienst ein



Nehmen Sie die Zieladresse als ”Watch-only” in Ihr Wallet auf oder verwenden Sie einen Alarmierungsdienst, der Sie benachrichtigt, wenn eine Transaktion vorgenommen wird.

Es gibt theoretisch noch eine weitere Spur, die jetzt schon verfolgt werden kann. Der Täter wird wissen wollen, ob das Lösegeld transferiert worden ist. Nutzt der Täter dazu nicht seinen eigenen Bitcoin-Knoten sondern einen Dienst wie Bitcoin.info etc. so können diese Dienste das Lösegeldkonto mit der IP-Adresse verknüpfen. Erfolgt diese Abfrage unverschlüsselt, so kann diese Zuordnung von allen Diensten gemacht werden, die die Kommunikation im Internet überwachen. Mit dieser Methode können Ransomware-Erpresser sogar bereits ermittelt werden, bevor das Lösegeld gezahlt wird.

Als Privatperson hat man jedoch keinen Zugriff auf diese Informationen.

Weitere Transaktion erfolgt

Nun passiert es, es erfolgt eine weitere Transaktion. Sie sehen die Transaktion. Manche Tools wie etwa bitcoinwhoiswho geben Ihnen auch eine IP-Adresse dazu. Zuverlässig war das in den Fällen, in denen ich das getestet habe jedoch nicht.
Vermuten Sie, dass die Zahlungen über eine Exchange oder einen Service abgewickelt werden, können Sie auch dort nachfragen, ob die Bitcoin-Adresse dort verwaltet wird.

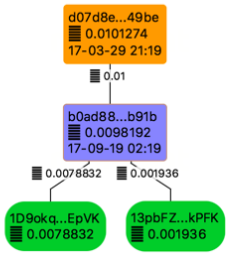
Transaktionsnetz verfolgen

TX Hash
b0ad88e875e349d5891d13ea598d2
Time of Transaction
17-09-19 02:19
Block Height
485965
Fees
0.00018080
Value In
0.01000000
Value Out
0.00981920
Inputs

Address	Value
1D9okqA...Rd4EpVK	0.01

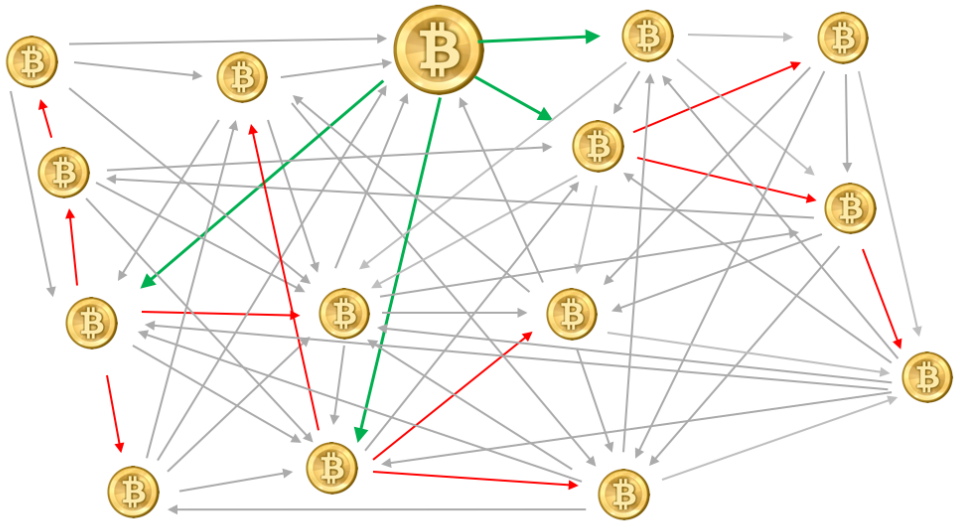
Outputs

Address	Value
13pbFZkq...ceSkPFK	0.001936
1D9okqA...Rd4EpVK	0.0078832



Sie können das Netz der Transaktionen ansehen und verfolgen. Hier sehen Sie, dass eine Transaktion getätigt wurde und der Restbetrag auf das gleiche Konto zurück transferiert wurde. Manche Wallets machen das und verwenden nicht immer neue Konten. Damit wird klar, dass hier 0.001936 BTX auf ein anderes Konto transferiert wurde.
Googlen sie die verbundenen Adressen – vielleicht war der Täter so leichtsinnig, eine der Adressen irgendwo gepostet zu haben. Haben Sie einen bestimmten Verdacht, dass die Zahlungen über eine Exchange oder einen Service abgewickelt werden, können Sie dort nachfragen. Aber ohne zusätzliche Verknüpfung werden Sie die Täter nicht identifizieren können.

Zuordnung von IP-Adressen



Eine Transaktion geht von einem Knoten aus. Dieser gibt die Information an eine Reihe von anderen Knoten weiter. Diese geben die Nachricht wiederum weiter – auch an Knoten, die die Information bereits anderweitig erhalten haben. Damit die Kommunikation nicht endlos weiter geht, gibt ein Knoten die Information nur weiter, wenn er sie das erste Mal erhält.

Ein Knoten, der eine Transaktion ein weiteres Mal erhält, weiß, dass die Transaktion ursprünglich nicht von dem sendenden Knoten sondern von einem anderen Knoten stammt. Ein Knoten, der eine Transaktion das erste Mal erhält, kann vermuten, dass die Transaktion direkt vom Absender an ihn transferiert wurde. Diese Vermutung ist manchmal richtig – dann ist der Pfeil im Bild grün gemalt und manchmal falsch – dann ist er rot. Zur Identifizierung des Ursprungs einer Nachricht reicht daher die Überwachung eines der zuerst adressierten Knoten (grüne Pfeile). Die Sekundärkommunikationen (rote Pfeile) lassen sich dann von den Primärkommunikationen (grüne Pfeile) unterscheiden, da die Primärkommunikationen vorher stattfinden. Da die Bitcoin-Kommunikation unverschlüsselt ist, müssen die Knoten nicht selbst betrieben werden sondern reicht es den Internetverkehr zu überwachen. Zudem ist die Topologie im Bitcoin-Netzwerk nicht homogen, so dass die Überwachung auf wenige Knoten beschränkt werden kann.

Wurde die Transaktion über eine Exchange oder einen Wallet Service abgewickelt, dann sind dort nicht nur die Daten der Auftraggeber hinterlegt. Der Wallet Service hat zudem die Kontrolle über die Accounts. Ein Zugriff auf die Bitcoins ist hier denkbar.

Wie kann man sich vor dieser Nachverfolgung schützen? In dem man seine IP-Adresse verbirgt. In der Vergangenheit wurde hierfür immer TOR empfohlen...

IP Adresse verbergen – aber nicht mit TOR

NETZPOLITIK.ORG

Überwachung

Geheime Dokumente: Der BND hat das Anonymisierungs-Netzwerk Tor angegriffen und warnt vor dessen Nutzung

Der BND hat ein System zur Überwachung des Tor-Netzwerks entwickelt und Bundesbehörden gewarnt, dass dessen Anonymisierung „unwirksam" ist. Das geht aus einer Reihe geheimer Dokumente hervor, die wir veröffentlichen. Der Geheimdienst gab einen Prototyp dieser Technik an die NSA, in Erwartung einer Gegenleistung.

am 14.09.2017 Andre Meister / 49 Kommentare / Teilen

Es gibt Zweifel, ob Tor noch sicher ist. Zu Tor gibt es nachher einen eigenen Vortrag – daher möchte ich an dieser Stelle nicht weiter darauf eingehen.

Was ist mit Mixern ?

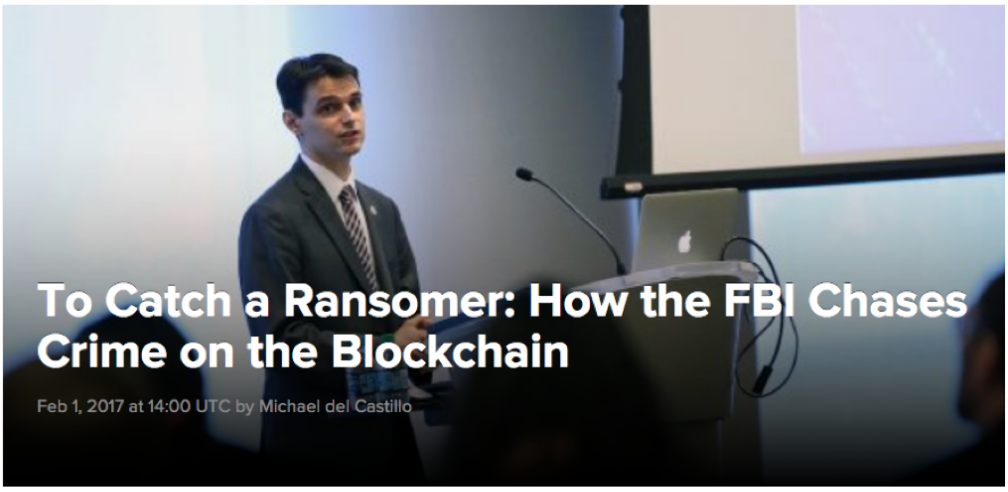
Kriminelle verwenden Mixer-Services um die Herkunft der Bitcoins zu verschleiern. In einen Mixer kommen viele Bitcoins hinein und es werden viele wieder ausgezahlt, so dass eine Zuordnung schwierig ist.

Doch viele Mixer funktionieren gar nicht richtig.

Selbst wenn sie richtig funktionieren würden, erzeugen sie Patterns, die mit spezieller Analysesoftware zumindest zum Teil wieder aufgelöst werden kann.

Selbst wenn der Mixer perfekt wäre – die Identifizierung der IP-Adresse erfolgt bereits bevor die Bitcoins in den Mixer kommen. Davor schützt auch der Mixer nicht.

Das FBI fängt Ransomware-Erpresser



Das FBI identifiziert auf dieser Basis Ransomware-Erpresser.

https://www.coindesk.com/catch-bitcoin-ransomer-inside-fbis-cyber-investigation-process/

Das FBI nutzt private Dienstleister

MOTHERBOARD

LONG ARM OF THE LAW

US Law Enforcement Have Spent Hundreds of Thousands on Bitcoin Tracking Tools

JOSEPH COX
May 25 2017, 5:30pm

The blockchain can be pretty overwhelming, with criminals moving their funds through a string of addresses before finally cashing them out. Presumably to deal with that issue, several US law enforcement agencies, including the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), and Immigration and Customs Enforcement (ICE) have all paid for software from bitcoin tracking company Chainalysis according to public records, with one purchase order being signed just this month.

Die Auswertung macht das FBI dabei nicht selbst, sondern greift auf private Dienstleister zurück.

Dienstleister beauftragen

- Private Dienstleister in den USA forschen nach
  - Ohne Garantie den Täter zu identifizieren
  - Ohne Garantie die Zahlung zurück zu erhalten
  - Kosten ca. 5000 € für die initiale Recherche

Diese Dienstleister bieten auch Privatleuten ihre Dienste an. Aber das ist zum einen weder billig noch hgibt es eine Erfolgsgarantie

Doch nicht nur das FBI nutzt diese Software

Die US-Steuerbehörden verwendet Bitcoin-Tracking Software. Auch die dänische Polizei arbeitet ebenfalls mit solchen Werkzeugen. Die deutschen Staatsanwaltschaften tracken Bitcoin-Transaktionen ebenfalls – die von mir angefragte Staatsanwaltschaft wollte jedoch keine Auskunft über die konkret dazu eingesetzten Werkzeuge geben.

Die Nutzung dieser Dienstleister ist nicht ganz unkritisch, denn damit die Ermittlung funktioniert, müssen IP-Adressen der Transaktionen auf Vorrat gespeichert werden. Eine gesetzliche Grundlage dazu gibt es wohl aktuell noch nicht – auch wenn der Vorschlag zur 5. Geldwäsche-RL in diese Richtung geht.

https://www.randombrick.de/daenische-polizei-verwendet-bitcoin-tracking-software-um-drogenhaendler-festzunehmen/
https://www.coindesk.com/irs-using-bitcoin-tracking-software-since-2015/

Vielen Dank für Ihre Aufmerksamkeit!

Fragen, Diskussion