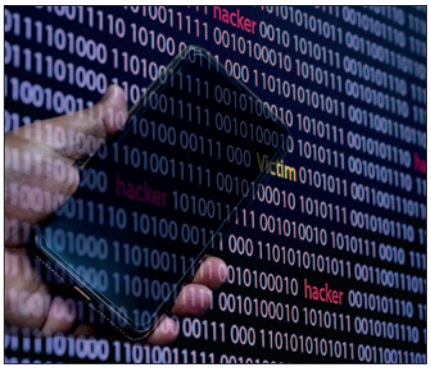
Schadsoftware und Bitcoins

Wer im Internet Infoapps über das Coronavirus runterlädt, kann sich eine Schadsoftware einhandeln, die Daten verschlüsselt. Betroffen sind vor allem Mobiltelefone.

Internetbetrüger nützen das Verlangen nach Information in Zusammenhang mit dem Coronavirus aus. Unzählige Coronavirus-Karten oder Infoapps sind im Appstore verfügbar. Viele enthalten nützliche Informationen und sind leicht bedienbar, bei einigen kann man sich unbemerkt eine Spysoftware (Spionagesoftware) oder Ransomware (Verschlüsselungssoftware) auf seinen Rechner laden. Die meisten Fälle zielen auf das Handy ab. Einmal installiert, verschlüsselt eine in der App versteckte Ransomware Daten, und ein weiterer Zugriff auf das Handy ist nicht mehr möglich. Durch Zahlung von z. B. 100 US-Dollar in Bitcoin kann man sein Handy wieder freischalten lassen. Behörden warnen vor einer Überweisung, da dies den Verbrechnern weitere finanzielle Möglichkeiten gibt. Solche „CovidLock"-Kits sind im Darknet erhältlich und könnten eine kommende flächendeckende Cyber-Angriffswelle sein.

„Smurfing". Was passiert mit den Bitcoins, die an Betrüger überwiesen werden? Bei der Nachverfolgung größerer Bitcointransaktionen bei Ransomware-Erpressungen ist es durchaus üblich, den Weg der Bitcoins im Netzwerk zu verfolgen. In vielen Fällen wird der große Betrag in viele kleine Beträge zerteilt und auf unterschiedlichen Wegen in einem Muster weitergeleitet. Dies nennt sich im Fachjargon „smurfing" (Verschleierung großer Beträge durch Aufteilung und Weiterleitung in Kleinstbeträgen). Nachdem die erpressten Bitcoinbeträge Kleinstbeträge darstellen, wäre es mittels Spezialsoftware möglich, den Weg nachzuverfolgen und mögliche Mustererkennungen durchzuführen. Dazu ist es notwendig, die vielen Bitcoin-Einzahlungswallets namhaft zu machen und zu melden. Dies kann in Österreich nur über eine Betrugsanzeige geschehen.

Das Sammeln dieser Transaktionsdaten und die Übermittlung oder der Informationsaustausch mit Spezialfirmen (z. B. Chainalysis, Coinfirm oder andere) kann helfen, Hintergrundinformationen zu erhalten. Das funktioniert



Schadsoftware in Infoapps: Betroffen sind vor allem Smartphones.

auch bei älteren Delikten. Etwa beim Diebstahl von über 7.000 Bitcoins von der weltweit größten Kryptobörse Binance sind noch immer Transaktionsinformationen zu erhalten. (Siehe Beitrag „Blockchain-Spur zum Dieb", Öffentliche Sicherheit, Ausgabe 7-8/2019, S. 39-40). Weiters wäre es möglich, Auszahlungswünsche (z. B. Verkauf von Bitcoin in Euro) auf Börsenplattformen zu unterbinden bzw. Verdachtsmeldungen von den Börsen oder Brokern zu erhalten.

Nachverfolgung. Nachdem alle Bitcointransaktionen auf ewig und fälschungssicher in der Blockchain aufbewahrt werden, kann auch eine Transaktionszuordnung noch Jahre später erfolgen. Wie in einem Puzzlespiel kann jeder Informationsteil zusammengesetzt werden. Vorausgesetzt, man hat Zugang zu den Infos, kann diese lesen und maschinell aufbereiten. Wenn Täter ihre Bitcoins nicht bewegen, ist es fast ausgeschlossen, ihnen auf die Spur zu kommen. Je mehr Transaktionen jedoch stattfinden, desto mehr Anknüpfungspunkte für Nachforschungen gibt es.

Die Tracing-Firma *Coinfirm* ist den von Binance gestohlenen Bitcoins auf der Spur. Sie veröffentlichte eine Darstellung der Diebstahls-Transaktionen. Demnach sind bereits Bitcoins bei Krypto-Börsen gelandet und wurden dort in andere Kryptowährungen gewechselt oder ausbezahlt. Eine derartige Nachverfolgung ist nur möglich, wenn man Zugang zu den kostenpflichtigen Informationen der Tracinganbieter hat.

Probleme bei der Nachverfolgung stellen Mixingservices und Kryptobörsen dar. Mixing deshalb, weil die ursprüngliche Senderwallet nicht direkt mit der Empfängerwallet in Verbindung zu bringen ist. Dies wird im Normalfall dadurch erzielt, dass nicht eine einzelne Transaktion von Wallet A nach Wallet B erfolgt, sondern viele Transaktionen gleichzeitig gebündelt werden (eine Art „Sammelauftrag").

Durch die dadurch entstandene hohe Anzahl an gleichzeitigen Transaktionen kann kein Rückschluss auf den direkten Sender/Empfänger mehr stattfinden. Diese Services sind in Europa bereits stark eingeschränkt, aber weltweit noch buchbar. Kryptobörsen stellen deshalb ein Problem bei der Nachverfolgung dar, weil eine Börse im Regelfall die anvertrauten Gelder für die Kunden beaufsichtigt. Transaktionen auf der Börsenplattform werden zwi-

PRÄVENTIONSTIPPS

Malware vermeiden

- Laufend die neuesten Updates/Patches zu den wichtigen Systemen auf PC und Handy installieren.
- Ad-Blocker oder Antivirus-Software benutzen, die automatisch unsichere Webseiten blockieren.
- Sicherere Browser wie *Firefox* oder *Google Chrome* verwenden.
- Nur Links oder Anhänge in Mails öffnen, wo der Absender bekannt ist.
- Sicherungen/Back-ups für PC und Handy erstellen.

Im Android-Appstore ist zu beachten:

- Nicht nur Kartenapps, alles mit Corona/COVID-19 kann betroffen sein.
- Vor Appdownload auf die Bewertungen achten und Kommentare lesen.
- Den Anbieter der App auf *Google* überprüfen.

Bitcointransaktionen können mit Spezialsoftware nachverfolgt werden.

schen zwei Börsenkunden (Käufer und Verkäufer) nicht direkt in die Blockchain „geschrieben", sondern durch einen Saldotransfer von Subkonten buchhalterisch erledigt. Erst beim Versand außerhalb der Börse wird der entsprechende Bitcoin-Betrag wieder in die Blockchain geschrieben.

Trotz der ansonsten transparenten Transaktionsinformationen konnte bis dato noch kein nennenswerter Erfolg bei der Auffindung der Binance-Diebe vermeldet werden. Es wird noch dauern, um weltweit oder zumindest teilstaatliche einheitliche Tracingstandards abzustimmen und den Informationsaustausch mit Tracinganbietern zu verbessern.

ICANN. Laut der *Internet Corporation for Assigned Names and Numbers (ICANN – http://icann.org)*, würden Cyber-Kriminelle aktuelle Schlagwörter bei der Erstellung von Domains nutzen, um Nutzer auf Phishing-Webseiten zu locken und sie mit Spam oder Malware zu überhäufen. In der Corona-Krise werde diese Strategie laut ICANN stark eingesetzt. Im März 2020 wurden etwa 100.000 neue Webseiten registriert, die entweder das Wort „Covid", „Corona" oder „Virus" im Titel tragen. *Matthias Reder*

Der Autor Mag. (FH) Matthias Reder ist Leiter Compliance und AML bei Coinfinity GmbH und Ansprechpartner für Großkunden sowie Banken und Behörden (www.coinfinity.co)

FOTO: ZEPHYR_P/STOCK.ADOBE.COM