The Chainalysis 2021 Crypto Crime Report

(February 16, 2021)

Kurze Zusammenfassung

Geissbühler Weber & Partner AG I Bleicherweg 72 I CH - 8002 Zürich I T. +41 44 221 91 00 I info@gwp.ch I www.gwp.ch

Inhaltsverzeichnis

I. Einleitung

Das US-amerikanische Unternehmen Chainalysis[1] hat im Februar 2021 den Bericht «*The 2021 Crypto Crime Report - Everything you need to know about ransomware, darknet markets, and more*»[2], veröffentlicht. Die kriminellen Aktivitäten machten 2019 laut dem Bericht 2,1% des gesamten Kryptotransaktionsvolumens aus. Das entspricht einem Wert von 21,4 Milliarden US-Dollar. Diese Zahl ist im Jahr 2020 auf nur noch 0,34% des gesamten Transaktionsvolumens gesunken (Wert: 10 Milliarden US-Dollar). Das Analyseunternehmen ist der Meinung, dass der prozentuale Rückgang der kriminellen Aktivitäten auf die breite Dimension der Kryptoindustrie zurückzuführen ist.[3] Die Kryptowährung blieb trotzdem sehr attraktiv für Kriminelle, vor allem aufgrund der Leichtigkeit, mit der sie es den Nutzern erlaubt, Geldmittel sofort an jeden Ort der Welt zu senden - trotz ihres transparenten und nachvollziehbaren Designs.

II. Riskante Dienstleister

Das Ziel der Cyberkriminellen ist es, die Quelle ihrer Gelder zu verschleiern und ihre Kryptowährung in Bargeld umzuwandeln, damit sie ausgegeben oder bei einer Bank aufbewahrt werden kann. Diese einfach an eine Börse zu schicken und sich auszahlen zu lassen, stellt ein «Risiko» für die Cyberkriminellen dar. Stattdessen verlassen sie sich auch auf eine Gruppe von Dienstleistern, um ihr Kryptovermögen zu liquidieren.[4] Banken könnten die Fähigkeit von Cyberkriminellen, Kryptowährung in Bargeld umzuwandeln, erheblich beeinträchtigen, indem sie solche «Geldwäschereidienstleister» identifizieren und eine Zusammenarbeit mit ihnen vermeiden. Der Bericht zeigt auf, dass ein erhebliches Volumen von illegalen Adressen zu Diensten bewegt wurde, die als «riskant» kategorisiert werden, inkl. hochriskanter Börsen (z.B. Börsen mit schwachen oder nicht vorhandenen Compliance-Programmen), Glücksspielplattformen, Mixer und Diensten, die ihren Sitz in hochriskanten Gerichtsbarkeiten (USA, Russland, China, Südafrika, UK etc.) haben. Viele dieser Einzahlungsadressen gehören zu Drittanbietern, die u.a. Geldwäschereidienste für Cyberkriminelle bereitstellen.[5]

Ziel der Banken sollte es sein, die Zusammenarbeit mit riskanten Diensten (Risk Exchange, High Risk Jurisdiction etc). zu beobachten und im besten Fall zu vermeiden. Gemäss dem Bericht haben sich viele Börsen auf die öffentlich erklärten KYC- und AML-Richtlinien anderer Kryptowährungsdienste verlassen. In

[1] „Das Hauptgeschäft von Chainalysis beruht auf der technologischen Fähigkeit, Blockchain-Muster zu identifizieren. Auf der Chainalysis Blockchain Intelligence Platform laufen zu diesem Zweck entwickelte Compliance- und Untersuchungsprogramme, die Bitcoin-Börsen und klassische Banken-Institutionen nutzen, um Geldwäsche und illegale Transaktionen zu identifizieren“, vgl. https://www.unternehmenswelt.de/chainalysis.html, 15.02.2021.

[2] *The 2021 Crypto Crime- Everything you need to know about ransomware, darknet markets, and more* ; https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf; folgend: Bericht; 17.02.2021.

[3] Bericht S. 6 ff.

[4] Bericht S. 9 ff.

[5] Bericht S. 11.

Zukunft sollten alle Finanzintermediäre solche Richtlinien konkret prüfen und derartige Dienstleistungen mit mehr Sorgfalt behandeln. Dies gilt ebenso für Banken.[6]

III. Betrug/Scams

Die Einnahmen aus Betrugsfällen sind zurückgegangen, obwohl die Zahl der Opfer gestiegen ist. Grund dafür ist, dass es im Jahr 2020 keine gross angelegten Ponzi-Schemata (bspw. PlusToken) gab. Stattdessen entfielen 2020 fast alle Betrugseinnahmen auf Investitionsbetrüge (Mirror Trading International, J-enco, Forsage etc.). Die Betrüger haben die von den Opfern erhaltene Kryptowährung hauptsächlich an Börsen weitergeleitet, um sie in Bargeld umzuwandeln. Ebenso gab es einen Anstieg an Betrugsgeldern, die an Mixer und Hochrisikobörsen geschickt wurden.[7] Der Bericht verdeutlicht, wie wichtig es für Börsen und andere Kryptowährungsdienste - und somit auch für die Banken - ist, die Kunden über Betrugstechniken (z.B. Phishing-Techniken) aufzuklären; besonders, wenn sie wissen, dass E-Mails oder andere persönliche Informationen der Kunden kompromittiert werden könnten, was die Kunden anfälliger für Phishing-Angriffe macht.

IV. Ransomware-Ökosystem

Nicht zu unterschätzen ist weiter das Cyberrisiko «Ransomware». Insbesondere erwähnt der Bericht die Ransomware Ryuk, NetWalker, Maze, Snatch, welche die Banken genauer zu analysieren haben. Dabei kommt der Bericht zum Schluss, dass weit weniger kriminelle Gruppierungen aktiv sind, als es die Anzahl der Versionen von Ransomware vermuten lassen würde. Gemäss dem Bericht ist es den Ransomware-Opfern und Consultants verboten, Zahlungen an Angreifer zu tätigen. Ransomware-Ersteller und Angreifer, die auf der OFAC-Sanktionsliste aufgeführt sind, sollten beachtet werden.[8] Die Banken sollten alle Sanktionslisten in ihr Cyber Risk Management integrieren. Folgende Punkte sind bei der Bekämpfung der Ransomware-Risiken zu beachten: Alerts verfolgen, Antiviren-Softwareprogramme installieren, Mitarbeitende schulen, Remotezugänge stärken, Offline-Backups und Benutzerrechte einschränken.[9]

V. Darknet Markets

Die Umsätze im Darknet (37 aktive Darknet-Marktplätze vorhanden) sind 2020 ebenfalls gestiegen, dabei spielt der aktuell grösste illegale Marktplatz, Hydra, eine grosse Rolle. Hydra bedient russischsprachige Länder und macht 75% der globalen Darknet-Umsätze aus. Hydra könnte in der nahen Zukunft auch für die EU und die USA zu einem Problem werden, wenn der Online-Marktplatz seine Expansionspläne

[6] Bericht S. 111-112.
[7] Bericht S. 74.
[8] Bericht S. 26 ff.
[9] https://www.inside-it.ch/de/post/schweizer-ransomware-opfer-was-sie-falsch-machen-20200219; 15.02.2021.

umsetzt. Während Hydra in erster Linie zu einer Plattform für Online-Drogenhandel geworden ist, dienen die restlichen illegalen Marktplätze zur Abwicklung für Deals mit gehackten persönlichen Daten und Kreditkartennummern.[10] Nichtsdestotrotz gibt es einen Rückgang der Dark Markets. Ein neues dezentralisiertes Modell, das von Plattformen wie Televend verkörpert wird, ist eine neue Plattform, auf der Darknet-Markt-Anbieter u.a. Drogen über automatisierte Chatbots verkaufen können, deren Kommunikation mit den Käufern hochgradig verschlüsselt ist. Käufer greifen einfach auf die Telegram-Gruppe von Televend zu, wo sie ein Verzeichnis der Drogenverkäufer finden - aufgeschlüsselt nach Region und angebotener Ware. Von dort aus geben sie die Bestellung beim Chatbot auf, erhalten eine automatisch generierte Bitcoin-Adresse, an die sie eine Kryptowährung transferieren, und erhalten danach ihre Post. Televend erhält Provisionen für jeden Verkauf, berührt aber nie das Vermögen. Es gibt also keine zentrale Instanz, die die Strafverfolgungsbehörden durch Blockchain-Analyse aufspüren könnten - die Transaktionen mischen sich viel leichter. Gemäss Chainalysis scheinen Kunden hauptsächlich über Kryptowährungsbörsen zu bezahlen.[11] Dies verdeutlicht wieder, dass die Zusammenarbeit mit Börsen und Kryptowährungsbörsen genauer unter die Lupe zu nehmen ist.[12]

VI. Hacking

Im Jahr 2020 wurden Kryptowährungen im Wert von über 520 Millionen US-Dollar von Diensten und Einzelpersonen durch Hacking (bspw. Phishing) gestohlen. Die meisten Gelder flossen 2020 in die Börsen. Aber auch DeFi-Plattformen haben sich zu Geldwäschereimechanismen entwickelt. Ihre dezentralisierte Natur ist wahrscheinlich das, was sie für den Geldwäschereimechanismus attraktiv macht - da diese Plattformen die Gelder nie direkt in Verwahrung nehmen, die bei ihnen eingezahlt werden. Häufig werden auch keine KYC-Informationen gesammelt und nicht über Transaktionsaktivitäten berichtet.

[10] https://www.businessinsider.de/wirtschaft/finanzen/kriminalitaetsbericht-ueber-bitcoin-co-beim-is-der-alt-right-bewegung-und-im-darknet-stehen-kryptowaehrungen-hoch-im-kurs/; 15.02.2021.

[11] Bericht S. 43 ff. und S. 61 ff.

[12] Bericht S.84.