HLB BUSINESSMEETING

NIS2 & Cyberangriffe:
Prävention und Reaktion bei Blockchain-basierten Erpressungen

Albert Quehenberger
Rechtsstand 6.11.2024

HLB SCHUMACHER
HLB STÜCKMANN.
DDPGRUPPE
HLB Förderer, Keil & Partner
HLB Klein Mönstermann
TREUHAND
LW.P

AIQ FORENSICS

BLOCKCHAIN INTELLIGENCE

AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

TRUST THROUGH TRANSPARENCY

AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

NIS2 & CYBERANGRIFFE

AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

„In der Welt der Kryptowährungen ist Transparenz das schärfste Schwert gegen Betrug. Unsere forensischen Analysen helfen nicht nur, Täter zu stellen, sondern schaffen auch ein Umfeld, in dem Kriminalität weniger Chancen hat, sich zu verstecken."
Albert Quehenberger – Forbes 11/24

AGENDA

- Vorstellung
- Einführung NIS2 & Bedeutung für Unternehmen
- Cyberbedrohungen 2024
- Blockchain Ermittlung
  - Ausgangslage
  - Ermittlungsverlauf
  - Status Quo
- Q&A

Albert Quehenberger, PM.

- 2001 - 2018 Austrian Armed Forces
- 2014 -2016 Project BTC AAF/Special Force
- 2018 -2021 Chief Sales Officer Software with AI
- 2021 Certified Cryptocurrency Forensics Investigator (McAfee)
- 2021 Co-Founder & Chief Operating IT Security Startup
- 2021 Certified Transaction Examiner (Ciphertrace / Mastercard)
- 2022 Certified Blockchain Transforming Business (WU Wien),
- 2022 Certified Cryptocurrency Financial Expert (Crypto Valley)
- 2023 Sworn Court Expert Training for Blockchain and Cryptocurrencies
- 2023 Lecturer at HSO for PTGR
- 2023 Certified Crypto Research and Investigations Specialist
- 2023 Co-Author „Tax Tsunami Bitcoin 4.0“
- 2024 Supervisor Web3 Education Program Ethiopia
- 2024 Board Member DLT Austria & Germany, Web3Hub Vienna
- 2024 Advisor CHARONIUM, Web3 World Society

AQ Forensics GmbH

- ü. 1.000 Fälle
- B2C/B2B/B2G
- Blockchain Ermittlungen
- Fälle von:
  - Ponzi Schemes
  - Phishing Attacks
  - Romance Scams
  - Investment Scams
  - Ransomware Payments
  - Wallet Hacks
  - Impersonating Scams
  - Fake Smart Contracts
  - Sachverständigen Tätigkeit

EINFÜHRUNG NIS2

- Die **NIS2-Richtlinie** (Network and Information Security Directive 2), ist die überarbeitete Version der ursprünglichen NIS-Richtlinie, die 2016 als erste Cybersicherheitsrichtlinie der EU eingeführt wurde. Die NIS2-Richtlinie zielt darauf ab, das Schutzniveau gegen Cyberangriffe in der gesamten EU anzuheben und die Resilienz kritischer Infrastrukturen zu stärken.
- **17. Oktober 2024**

ZIELSETZUNG NIS2

- **Erweiterung des Anwendungsbereichs:** NIS2 bezieht mehr Unternehmen und Sektoren ein, darunter Gesundheitswesen, Energie, Telekommunikation und Finanzwesen.
- **Strengere Meldepflichten:** Unternehmen müssen schwerwiegende Cybervorfälle innerhalb einer kurzen Frist an die zuständige Behörde melden, was zu schnellerer und koordinierter Reaktion führen soll.
- **Harmonisierung und Strafen:** Die NIS2 stärkt die Zusammenarbeit zwischen den EU-Mitgliedstaaten und führt harmonisierte Sanktionen ein, um sicherzustellen, dass alle Länder gleich strenge Vorgaben und Kontrollen anwenden.
- **Förderung einer einheitlichen Sicherheitskultur:** Die Richtlinie fördert eine präventive Sicherheitskultur und fordert von Unternehmen, Sicherheitsrisiken frühzeitig zu erkennen und entsprechende Schutzmaßnahmen zu implementieren.

RELEVANZ VON NIS2 FÜR UNTERNEHMEN

- **Erhöhte Compliance-Anforderungen**: Unternehmen müssen sicherstellen, dass sie den Anforderungen der Richtlinie entsprechen, was oft bedeutende Investitionen in IT-Infrastruktur und Sicherheitsprotokolle erfordert.

- **Verstärkte Rechenschaftspflicht**: Die Führungsebene wird stärker in die Verantwortung genommen und kann bei Nichtbeachtung oder unzureichender Sicherheitsvorkehrungen zur Verantwortung gezogen werden.

- **Risiko von Strafen und Reputationsschäden**: Verletzungen der NIS2-Vorgaben können zu hohen Geldstrafen führen und das Vertrauen in das Unternehmen beeinträchtigen.

- **Notwendigkeit für proaktive Sicherheitsmaßnahmen**: Unternehmen müssen ihre Systeme stärker auf potenzielle Bedrohungen hin überwachen und Maßnahmen ergreifen, um Cyberangriffe frühzeitig zu erkennen und abzuwehren.

NIS2 zwingt Unternehmen zu einem sicherheitsorientierten Paradigmenwechsel

CYBERBEDROHUNGEN 2024

Im Jahr 2024 dominieren verschiedene Bedrohungen die Cybersicherheitslandschaft:

- **Ransomware-Angriffe**: Diese Angriffe haben weiterhin enorm zugenommen, da Cyberkriminelle zunehmend spezialisierte Tools einsetzen und oft Kryptowährungen als Lösegeld verlangen.

- **Phishing und Social Engineering**: Auch durch Künstliche Intelligenz werden täuschend echte Phishing- und Social-Engineering-Attacken durchgeführt, die es den Angreifern ermöglichen, Zugang zu kritischen Systemen zu erlangen.

- **Kritische Infrastrukturen im Visier**: Gesundheitswesen, Energieversorgung und andere kritische Sektoren werden zunehmend angegriffen, was NIS2 noch wichtiger macht.

- **Angriffe auf Kryptowährungsbörsen**: Cyberkriminelle haben Krypto-Börsen und Wallets gezielt ins Visier genommen, da Kryptowährungen schwer nachzuverfolgen und liquide sind.

CYBERBEDROHUNGEN 2024

- **Zunahme der Cyberangriffe**: 2024 meldeten 80 % der deutschen Unternehmen eine Zunahme von Cyberattacken. Besonders häufig kommen Ransomware-Angriffe (31 % der Schäden) und Phishing vor, zunehmend auch über "Cybercrime-as-a-Service"-Angebote, bei denen Hacker ihre Dienste verkaufen. Die geschätzten Schäden durch Cyberkriminalität belaufen sich auf 178,6 Milliarden Euro, ein Anstieg von ca. 30 Milliarden Euro im Vergleich zum Vorjahr (Quellen: BKA, Bitkom).

- **Supply-Chain-Angriffe**: Angriffe auf Lieferketten stellen ein wachsendes Risiko dar, da Schwachstellen in Zulieferern genutzt werden, was oft zu Produktionsausfällen und Reputationsverlusten führt. Nur 37 % der Unternehmen haben Notfallpläne für solche Vorfälle, und lediglich 19 % führen Sicherheitsbewertungen bei Zulieferern durch (Quelle: Bitkom).

- **Ziele und Methoden**: Cyberkriminelle zielen auf sensible Unternehmensdaten wie Kundeninformationen und geistiges Eigentum. Phishing und Ransomware bleiben beliebte Angriffswege, ergänzt durch DDoS-Attacken und den Einsatz von KI zur Tarnung der Angriffe (Quellen: BKA, Bitkom).

- **Wirtschaftsspionage**: Neben digitalen Bedrohungen gibt es vermehrt analoge Angriffe, wie Abhöraktionen und den Diebstahl physischer Dokumente. Rund 74 % der Unternehmen berichteten von solchen Angriffen auf geschäftliche Informationen, was zeigt, dass physische Sicherheitslücken ebenfalls zunehmend ein Problem darstellen (Quelle: Bitkom).

AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

WIE HILFT DIE BLOCKCHAIN BEI DER VERHINDERUNG & AUFKLÄRUNG VON STRAFTATEN?

WAS IST EINE BLOCKCHAIN?

- Eine Blockchain ist ein digital verteiltes, dezentrales, öffentlich zugängliches Hauptbuch, das über ein Peer-to-Peer-Netzwerk existiert.
- Ausgelöst durch die globale Finanzkrise im Jahr 2007
- Inspiriert von den Cypherpunks
- Erstmals beschrieben von Satoshi Nakamoto im Jahr 2008
- Wurde der erste Genesis-Block im Jahr 2009 gemined

BLOCKCHAIN FORENSIK

- **Blockchain-Forensik** bezieht sich auf den Prozess der Analyse und Untersuchung von Blockchain-Daten, um den Fluss von Transaktionen nachzuvollziehen, betrügerische oder verdächtige Aktivitäten zu identifizieren und Beweise für rechtliche Verfahren zu sammeln. Dabei werden spezialisierte Werkzeuge und Techniken eingesetzt, um die unveränderlichen Aufzeichnungen, die auf einer Blockchain gespeichert sind, zu untersuchen. So können Ermittler die Herkunft und Ziele digitaler Vermögenswerte verfolgen, Transaktionsmuster verstehen und, wenn möglich, die Identitäten der beteiligten Parteien aufdecken.

HERAUSFORDERUNGEN

- Ca. 10.000 handelbare Kryptowährungen
- Transaktionen am selben Tag möglich
- Niedrige Transaktionsgebühren
- Täter sind schwer nachverfolgbar
- Spezielle Anonymisierungsdienste
- Dynamik und technische Komplexität

WARUM KRYPTOWÄHRUNGEN

- Global verteiltes Netzwerk
- Taggleiche Transaktionen
- Keine zentralen Entitäten
- Bürokratische Hürden
- Verfahrensökonomie
- Zu wenige Spezialisten
- Verfolgung ist extrem zeitaufwändig und teuer
- „Money-Laundering-as-a-Service“

AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

BLOCKCHAIN ERMITTLUNG

AUSGANGSLAGE

- Zwei Freunde, beide deutsche Staatsbürger, gründeten ein erfolgreiches Blockchain-Unternehmen in den USA.
- Es herrschte gegenseitiges Vertrauen zwischen ihnen.
- Unser Mandant hatte sehr früh in BTC investiert und hatte noch etwa 50 BTC in einer Wallet, auf die auch sein Partner Zugriff hatte.
- Irgendwann in der Geschäftsbeziehung muss etwas passiert sein, das möglicherweise den Partner unseres Mandanten dazu veranlasst hat, die fast 50 BTC abzuheben und sie (im Juli 2023) aus der Wallet unseres Mandanten zu transferieren.
- Unser Mandant bemerkte erst, dass die 50 BTC fehlten, als sein Partner im November 2023 auch nicht mehr zur Arbeit erschien.
- Preis 11/23 ca. 35.000 USD

AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

AUSGANGSLAGE

AUSGANGSLAGE

- Als unser Mandant den Diebstahl bemerkte, informierte er sofort das FBI (November 2023).

AUSGANGSLAGE

IC3 Complaint Referral Form 9/11/23, 8:20 PM

FEDERAL BUREAU OF INVESTIGATION | HOME | FILE A COMPLAINT | CONSUMER ALERTS | INDUSTRY ALERTS | BEC | RANSOMWARE | ELDER FRAUD | COMMON SCAMS

Victim Information

Name:	[redacted]
Are you reporting on behalf of a business?	Yes
Business Name:	[redacted]
Is the incident currently impacting business operations?	Yes
Age:	[redacted]
Address:	[redacted]
Address (continued):	
Suite/Apt./Mail Stop:	
City:	Miami
County:	[redacted]
Country:	United States of America
State:	Florida
Zip Code/Route:	[redacted]
Phone Number:	[redacted]
Email Address:	[redacted]
Business IT POC, if applicable:	
Other Business POC, if applicable:	

Description of Incident

Provide a description of the incident and how you were victimized. Provide information not captured elsewhere in this complaint form.

AUSGANGSLAGE

- Unser Mandant beauftragte ein Unternehmen mit der forensischen Analyse und Nachverfolgung der BTC-Transaktionen
- Es gelang, fast alle fehlenden BTC zurückzuverfolgen.
- Fünf VASPs (Virtual Asset Service Providers) wurden identifiziert, an die die BTC gesendet wurden
- FBI reagierte nicht
- Hinzuziehung Miami PD

AUSGANGSLAGE

AUSGANGSLAGE

Date	Transaction Hash	Initial Receiving Address Name	Initial Receiving Address	Bitcoin Sent	USD	Page
July 30, 2023	[redacted]7aaed6[redacted] [redacted]04a5dec[redacted] [redacted]7771f56[redacted]	Address 1	1[redacted]56f Q[redacted]PC L[redacted]uW to	45.00909	$1,317,534	19
TOTAL CONFIRMED TRANSFERS				**45.00909 BTC**		

AUSGANGSLAGE

- Der Bericht mit den Ergebnissen wurde an das FBI und die Polizei von Miami weitergeleitet
- Es geschah nur wenig
- Im Februar 2024 wandte sich unser Mandant an uns

AUSGANGSLAGE

- Wir haben uns intensiv mit dem Fall beschäftigt und mit der Polizei von Miami zusammengearbeitet, um die betroffenen VASPs darüber zu informieren, dass die gestohlenen BTC auf ihre Plattformen übertragen worden waren
- Durch die Behörden wurden offizielle Anfragen an die relevanten Plattformen gesendet. Neben den Identitätsdaten der Empfänger wurden alle relevanten Informationen zu den nachverfolgten Konten angefordert. Dies sollte zusätzliche Informationen über den Verbleib der gestohlenen Bitcoin liefern
- In der Zwischenzeit begann der Preis von BTC zu steigen, was zusätzlichen emotionalen Stress für unseren Mandanten verursachte

ERMITTLUNGEN

- Da unser Mandant uns mitteilte, dass seit der Einreichung des Berichts wenig Fortschritt erzielt wurde, haben wir uns intensiver mit dem Fall beschäftigt und mit der Polizei von Miami zusammengearbeitet, um die betroffenen VASPs darüber zu informieren, dass die gestohlenen BTC auf ihre Plattformen überwiesen worden waren
- Durch die Behörden wurden offizielle Anfragen an die relevanten Plattformen gesendet. Neben den Identitätsdaten der Empfänger wurden alle relevanten Informationen zu den nachverfolgten Konten angefordert. Dies sollte zusätzliche Informationen über den Verbleib, der gestohlenen Bitcoin, liefern

ERMITTLUNGEN

- Nach mehreren Wochen erhielten wir die angeforderten Daten von den ausgeforschten Plattformen

ERMITTLUNGEN

Withdraw Address
[redacted]3f52a857F22b32f6e
[redacted]1845e7b88fD65d8d
[redacted]Z2LF2L6RN5HMINZ53WP6FACKIANQOWR3T
[redacted]a7A1eDE8eBcC31f3
[redacted]8D0B0Eb06D3138f
[redacted]8D0B0Eb06D3138f

ERMITTLUNGEN

Spot Wallet	Balance	Available Balance	Total Deposit & Buy Crypto	Total Withdrawal & Sell Crypto
BTC	0,00000014	0,00000014	3,84771614	0
USDT	0,02255233	0,02255233	0	0
ETH	0,33019947	0,33019947	0	15,58150616
XLM	0	0	0	190 927,36
USDC	0,00000033	0,00000033	0	49 612,99
BRZ	0	0	0	0
ARB	0,000118	0,000118	0	0

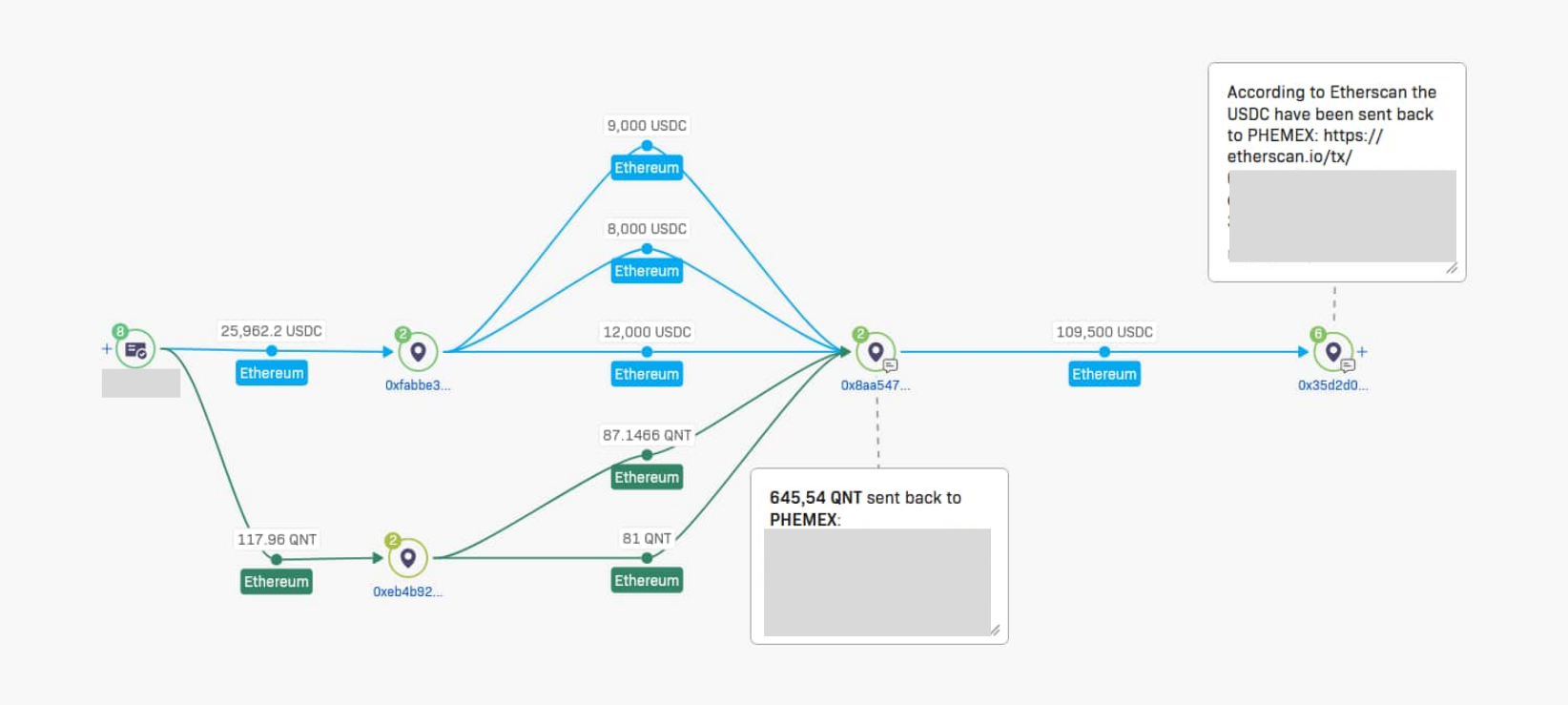
ERMITTLUNGEN

Registered Email Address	[redacted]
UID	[redacted]
Current Balance	~1200 USDT
Register Time	2023-08-18 18:30:07 UTC
Fiat Deposit	N/A
OTC Payment	N/A
Account Status	Banned
KYC Status	Unverified

ERMITTLUNGEN

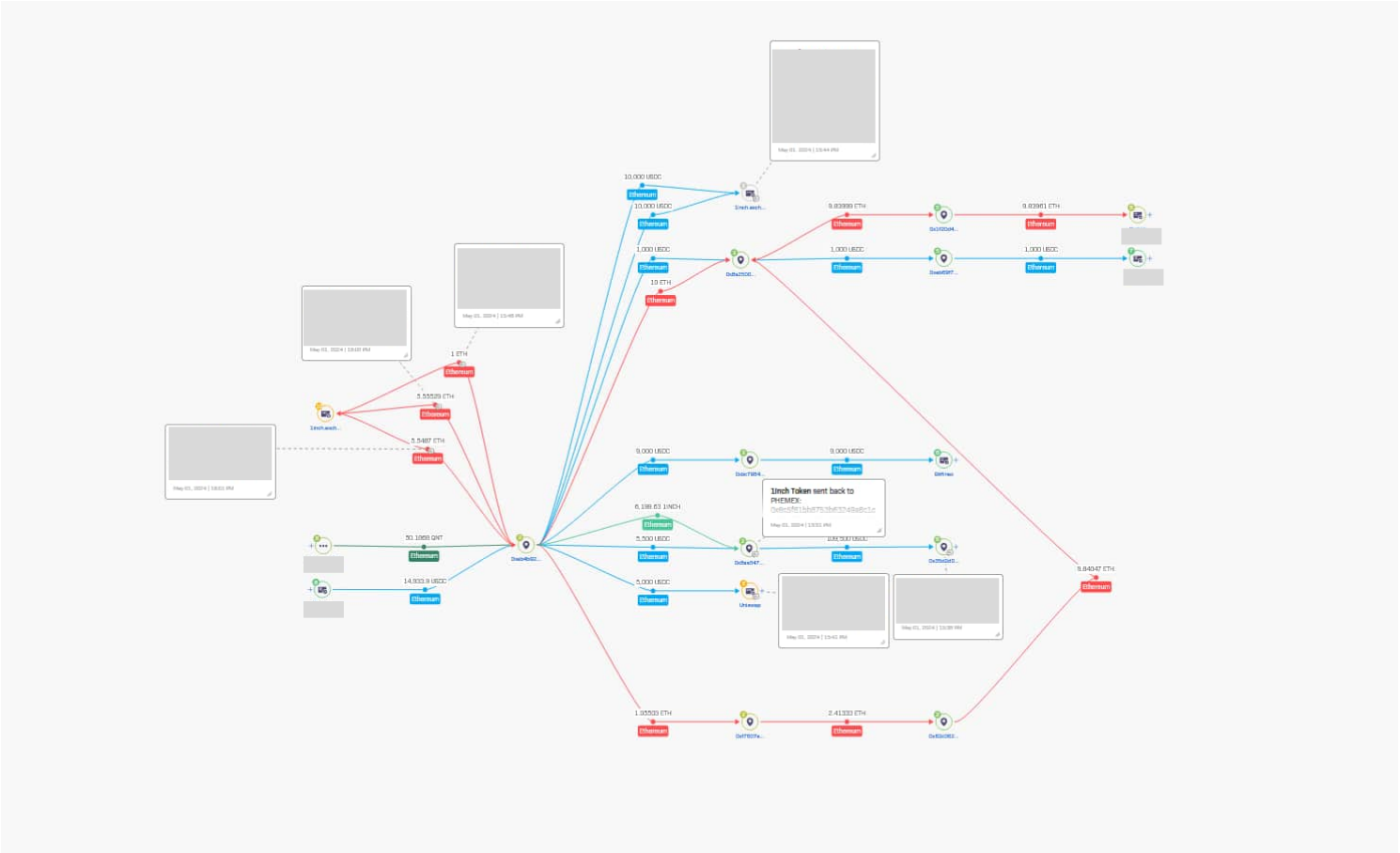
- Wir wussten, dass die BTC in andere Kryptowährungen umgewandelt worden waren
- Ein neuer Hinweis tauchte auf
- Also haben wir alle Daten zusammengetragen und eine forensische Analyse gestartet

ERMITTLUNGEN



AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

ERMITTLUNGEN



AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

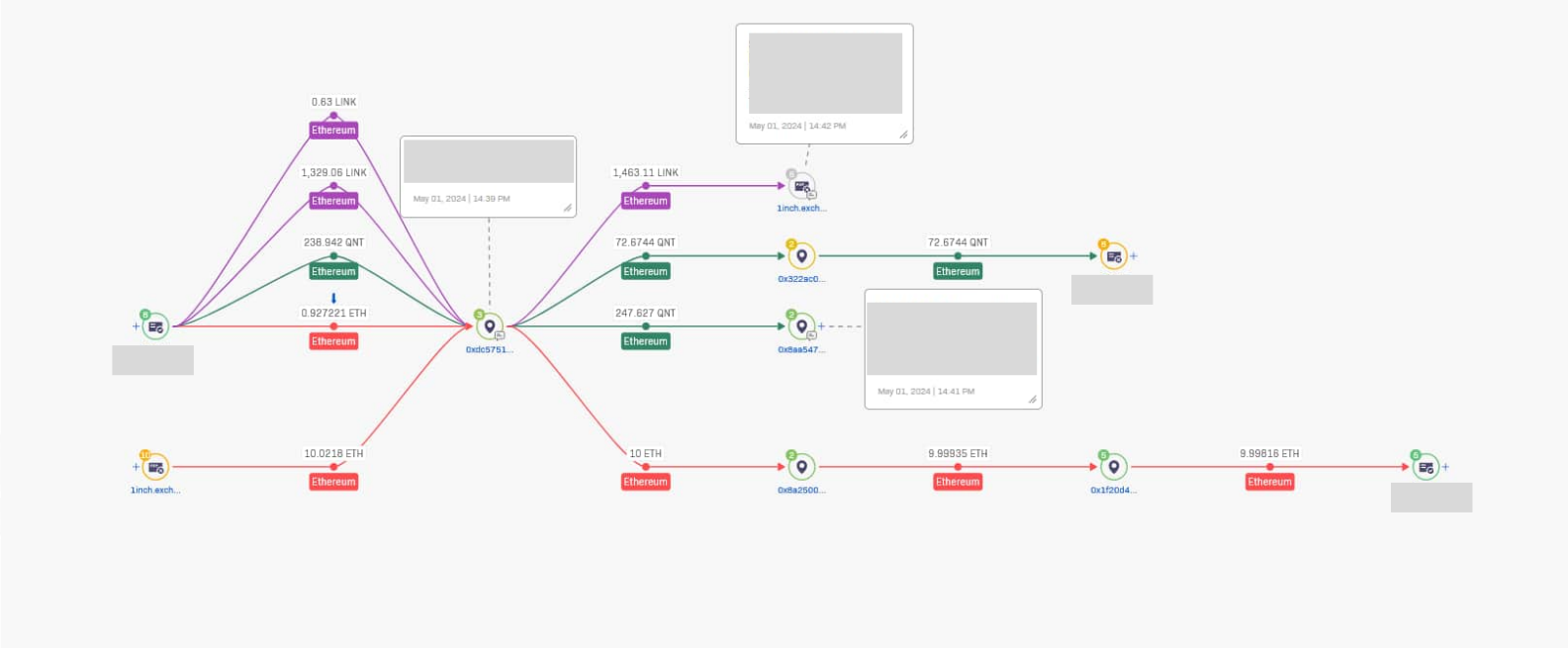
ERMITTLUNGEN

After 5 years, we made the difficult decision to shut down AlgoExplorer on January 31st, 2024 due to lack of funding.

We are deeply grateful for the journey we've shared with you all.

AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

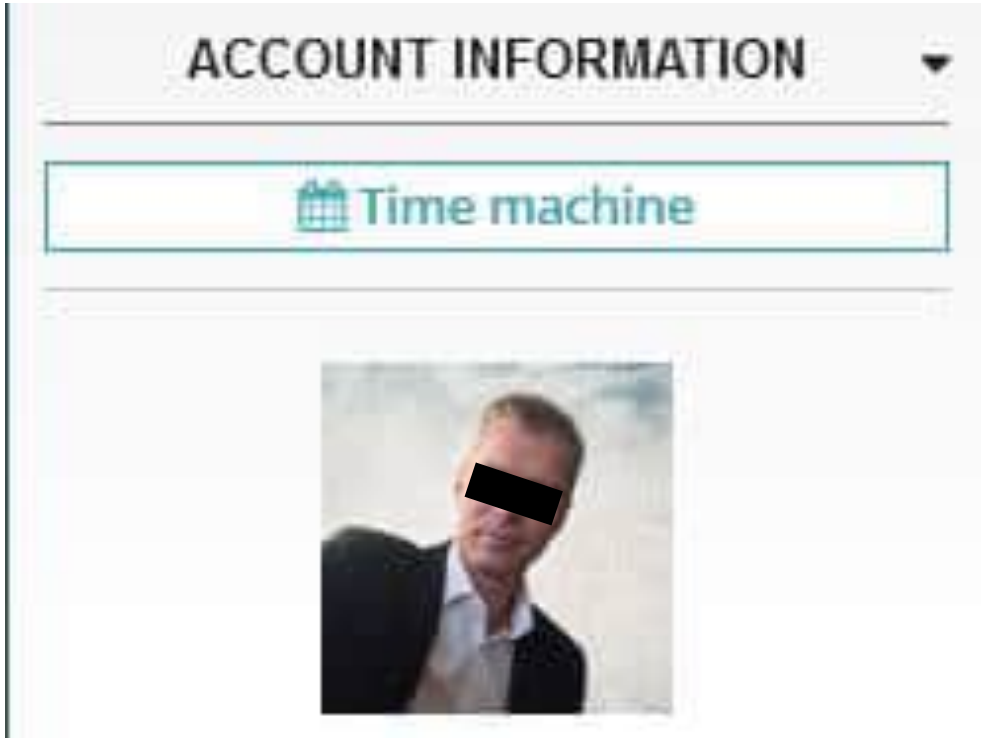
ERMITTLUNGEN



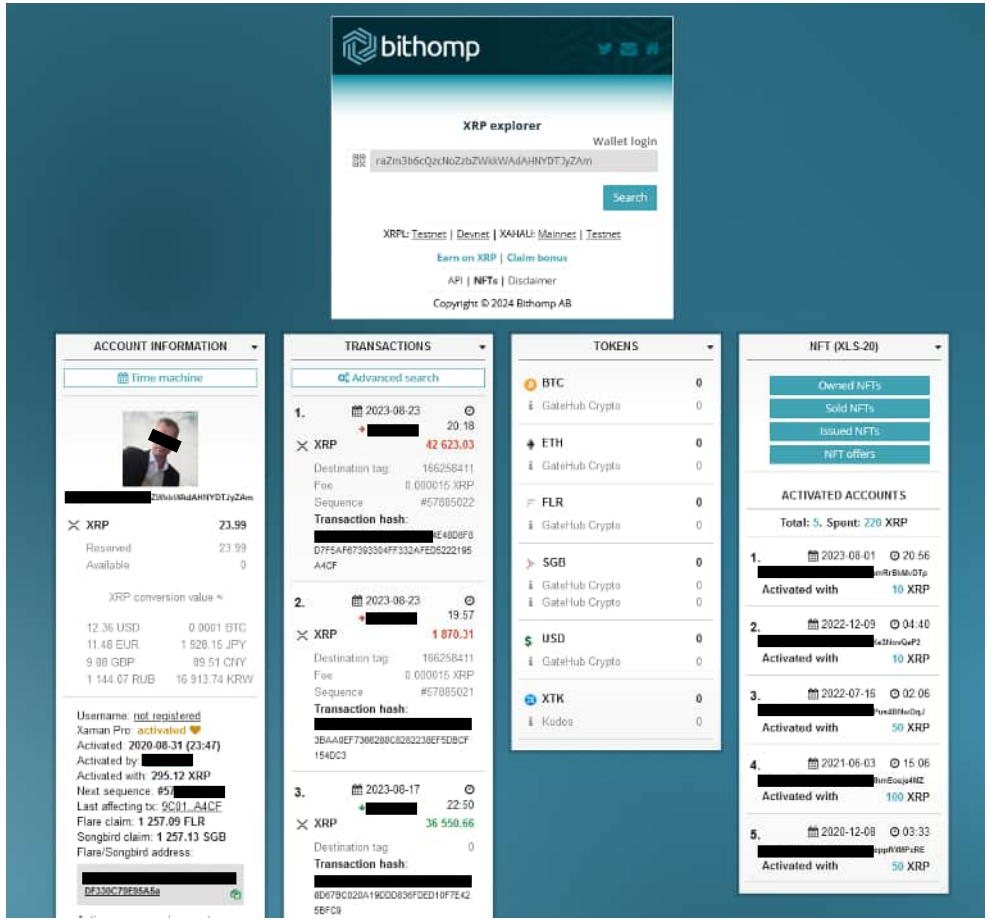
ERMITTLUNGEN

- Es war eine zeitaufwändige und intensive Suche
- Teilweise wurden die Kryptowährungen in andere Währungen umgewandelt und zurück auf die ursprünglichen Plattformen gesendet
- In einigen Fällen wurden die Transaktionen unauffindbar
- Einige Transaktionsflüsse konnten noch nicht grafisch dargestellt werden und mussten mithilfe eines Blockchain-Explorers verfolgt werden
- Einige Vermögenswerte wurden an Plattformen in anderen Ländern gesendet, was unterschiedliche Gesetze und Verfahren bedeutete
- Neue Informationsanfragen mussten gestellt werden. Es folgten weitere Woche des Wartens

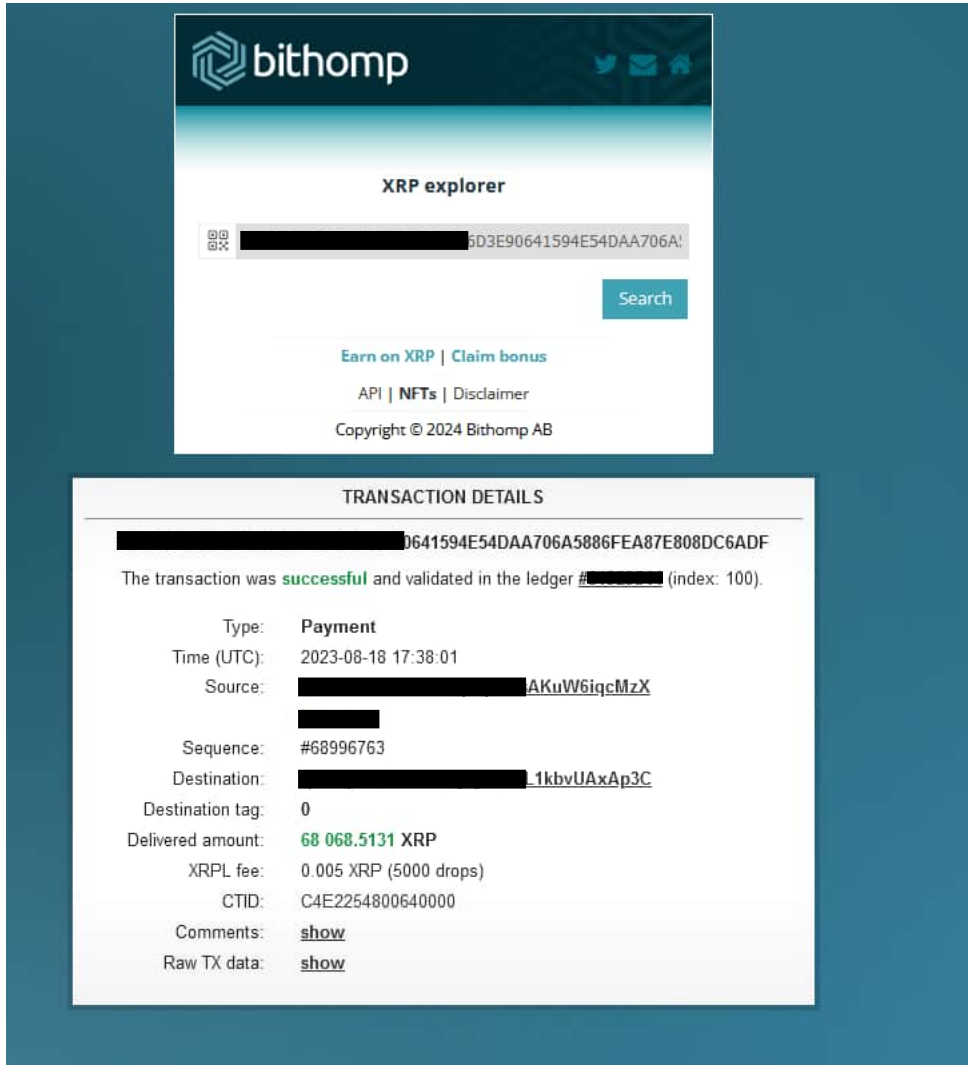
ERMITTLUNGEN



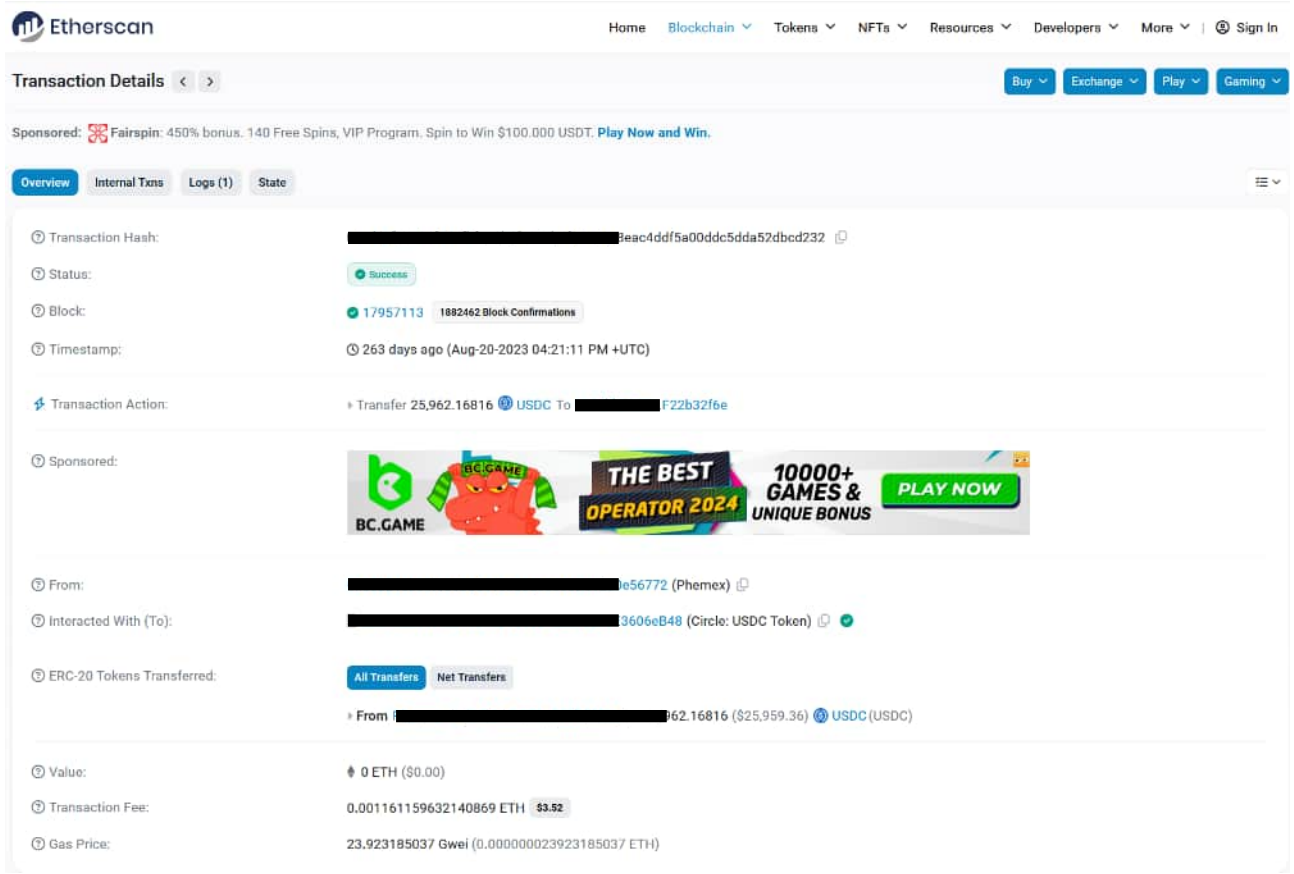
ERMITTLUNGEN



ERMITTLUNGEN



ERMITTLUNGEN



AKTUELLER STATUS

- Plötzlich war es da, das entscheidende Beweisstück, nach dem wir monatelang gesucht hatten
- Da wir bereits wussten, wer die Person auf dem Bild war, mussten wir nun unsere Ergebnisse beweisen
- Wir schlossen die forensische Analyse ab, leiteten die Ergebnisse an die Polizei von Miami weiter
- Es kam zu erneuten Informationsanfragen, und plötzlich: verifizierte Konten, die auf den Namen des Verdächtigen registriert waren

AKTUELLER STATUS

- Die Verbindungen auf der Blockchain zwischen den gestohlenen BTC, den umgetauschten Kryptowährungen und den Konten des Hauptverdächtigen waren klar
- Ein internationaler Haftbefehl wurde aufgrund der Fluchtgefahr und der Gefahr der Beweisvernichtung erlassen
- Aktuell sitzt der Verdächtige in U-Haft
- Von den gestohlenen 50 BTC sind aktuell knapp 35 sichergestellt

SCHUTZMAßNAHMEN

- **Zugriffsrechte bei Mitarbeiterwechsel entziehen:** Wenn Mitarbeiter das Unternehmen verlassen oder ihre Position wechseln, sollten ihre Zugriffsrechte auf Systeme und Daten sofort widerrufen werden. Statistisch betrachtet, sind etwa 75 % der Datendiebstähle auf ehemalige Mitarbeiter zurückzuführen, die noch Zugang zu sensiblen Informationen hatten. Dies hilft, unerlaubten Zugriff nach der Beendigung des Arbeitsverhältnisses zu verhindern

- **Verifizierter Firmenaccount bei regulierter & lizensierter Kryptobörse**: Unternehmen, die mit Kryptowährungen arbeiten, sollten verifizierte Konten bei regulierten Börsen erstellen. Das ermöglicht eine bessere Nachverfolgung von Transaktionen und bietet Schutz vor Betrug und Diebstahl. Regulierungen stellen sicher, dass Börsen Sicherheitsstandards einhalten, was das Risiko von unbefugtem Zugriff und Missbrauch verringert.

- **Multi-Faktor-Authentifizierung (MFA) aktivieren:** Die Implementierung von MFA auf allen wichtigen Accounts und Systemen schützt vor unberechtigtem Zugriff, selbst wenn Zugangsdaten kompromittiert wurden. MFA reduziert das Risiko, da die meisten Cyberangriffe auf einfache Passwortdiebstähle abzielen.

SCHUTZMAßNAHMEN

- **Regelmäßige Schulungen für Mitarbeiter:** Da ein Großteil der Cyberangriffe durch Phishing oder Social Engineering gelingt, sollten regelmäßige Schulungen für Mitarbeiter durchgeführt werden, um sie über aktuelle Bedrohungen und Sicherheitsrichtlinien aufzuklären. Dies stärkt die "menschliche Firewall" und hilft, Angriffe frühzeitig zu erkennen.

- **Software und Systeme regelmäßig aktualisieren:** Unternehmen sollten darauf achten, alle genutzten Programme und Betriebssysteme stets auf dem neuesten Stand zu halten. Updates enthalten oft wichtige Sicherheitspatches, die Schwachstellen schließen, welche von Hackern ausgenutzt werden könnten.

- **Notfall- und Backup-Strategien entwickeln:** Ein Notfallplan und regelmäßige Backups sind essenziell, um auf Datenverluste oder Cyberangriffe schnell zu reagieren. Dies ermöglicht eine schnelle Wiederherstellung und minimiert Ausfallzeiten im Falle eines Angriffs.

- **Zulieferer-Sicherheitsbewertungen durchführen:** Da Angriffe oft über die Lieferkette erfolgen, sollten Unternehmen die IT-Sicherheitsstandards ihrer Lieferanten überprüfen und Sicherheitsanforderungen im Vertrag festlegen. So kann verhindert werden, dass Schwachstellen bei Dritten das eigene Unternehmen gefährden.

AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

Q&A

Quellen

- https://www.pwc.at/de/dienstleistungen/wirtschaftspruefung/cybersecurity/europaeische-nis-2-richtlinie-implikationen-fuer-unternehmen-und-institutionen.html
- www.bitkom.org/EN/List-and-detailpages/Press/German-business-losses-more-than-220-billion-euros-per-year
- https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
- https://www.bka.de/EN/CurrentInformation/AnnualReports/annualreports_node.html

AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

TRUST THROUGH TRANSPARENCY

AIO FORENSICS
BLOCKCHAIN INTELLIGENCE

VIELEN DANK

A|Q FORENSICS GmbH
0043 (0) 676 5135 748

office@aq-forensics.com
www.aq-forensics.com

Roith 6 | A-5145
Neukirchen an der Enknach

A|Q FORENSICS
BLOCKCHAIN INTELLIGENCE