

STOCKHOLMS TINGSRÄTT
Avdelning 3

INKOM: 2023-12-06
MÅLNR: B 17235-21
AKTBIL: 300

HEMLIG

2023-12-01

STOCKHOLMS TINGSRÄTT

B 17235-21



Polisen

Tilläggsprotokoll till 5000-K615323-19

Arkiv/Åkl. ex

Enhet

Nationella Operativa Avdelningen, Komplexa cyberbrott (KCB) 1 NIB NOA

Handläggare (Protokollförare)

Jim Keyzer

Undersökningsledare

Henrik Söderman

Polisens diarienummer

5000-K615323-19

HEMLIG

Åklnr

AM-74743-19

Signerat av

null

Signatör: TINGSRÄTT
Avdelning 3

Datum: 2023-12-01

2023-05-11

AKTBIL: 286

Personer i ärendet

Förtursmål Nej	Beslag	Målsägande vill bli underrättad om tidpunkt för huvudförhandlingen Nej
Ersättningsyrkanden	Tolk krävs	
Misstänkt (Efternamn och förnamn) Kronberg, Fredrik Ulf Julius		Personnummer 19830208-0778
Brott		Förhandsgodkännande enligt RB 48:10 Nej
Information om att förenklad delgivning kan komma att användas av polis och tingsrätt är överlämnad vid ett personligt sammanträffande		
Information om att tillgänglighetsdelgivning kan komma att användas av tingsrätt är överlämnad vid ett personligt sammanträffande		
Underrättad om slutförd förundersökning / utredning enligt RB 23:18a 2023-05-11, underrättelse genom vanlig delgivning		Yttrande senast (rådrum) 2023-05-26
		Resultat av slutunderrättelse
Försvare Awrohum, Kinora, förordnad 2023-04-06		
Underrättad om slutförd förundersökning / utredning 2023-05-11, skriftlig underrättelse		Yttrande senast (rådrum) 2023-05-26
		Resultat av slutunderrättelse
Misstänkt (Efternamn och förnamn) Ihrén Nironen, Adam Antti		Personnummer 19940119-7554
Brott		Förhandsgodkännande enligt RB 48:10 Nej
Information om att förenklad delgivning kan komma att användas av polis och tingsrätt är överlämnad vid ett personligt sammanträffande		
Information om att tillgänglighetsdelgivning kan komma att användas av tingsrätt är överlämnad vid ett personligt sammanträffande		
Underrättad om slutförd förundersökning / utredning enligt RB 23:18a 2023-05-11, underrättelse genom vanlig delgivning		Yttrande senast (rådrum) 2023-05-26
		Resultat av slutunderrättelse
Försvare Svantemark, Nils, förordnad 2023-04-12		
Underrättad om slutförd förundersökning / utredning 2023-05-11, skriftlig underrättelse		Yttrande senast (rådrum) 2023-05-26
		Resultat av slutunderrättelse

Misstänkt (Efternamn och förnamn) Nederman, Hampus Helge		Personnummer 19930419-2991
Brott		Förhandsgodkännande enligt RB 48:10 Nej
Information om att förenklad delgivning kan komma att användas av polis och tingsrätt är överlämnad vid ett personligt sammanträffande 2023-01-26		
Information om att tillgänglighetsdelgivning kan komma att användas av tingsrätt är överlämnad vid ett personligt sammanträffande		
Underrättad om slutförd förundersökning / utredning enligt RB 23:18a 2023-05-11, underrättelse genom vanlig delgivning		Yttrande senast (rådrum) 2023-05-26
		Resultat av slutunderrättelse
Försvare Ataseven, Metin, förordnad 2022-12-07		
Underrättad om slutförd förundersökning / utredning 2023-05-11, skriftlig underrättelse		Yttrande senast (rådrum) 2023-05-26
		Resultat av slutunderrättelse

Notering

L

Fjärde tilläggsprotokoll

Innehållsförteckning

Diariernr	Uppgiftstyp	Sida
	PM om etherumadress Kronberg	
5000-K615323-19	Protokoll Etherumadress synlig på datornskärm 'saldot'.....	4
	<i>Bilaga: Tornado cash 1</i>	
	<i>Bilaga: Tornado cash 2</i>	
	Förhör misstänkt Nironen	
	Förhör med misstänkt, Ihrén Nironen, Adam Antti	12
	IT-extraktionsprotokoll	
	<i>Misstänkt Adam Nironen</i>	
	Protokoll Extraktionsprotokoll 2023-5000-BG3418-2.....	13
	Extraktionsprotokoll krypto Nironen	
	Tjänsteanteckning Not Återställning av seeds till kryptoplånb. v. 2.....	14
	Återställning av seeds till kryptoplånböcker v. 2.....	15
	Återställning av plånböcker från beslag BG3418-1.....	19
	Protokoll Återskapade plånböcker från iPad.....	24
	IT-forensiska analysprotokoll	
	<i>Misstänkt Adam Nironen</i>	
	Protokoll Extraktionsprotokoll 2023-5000-BG3418-5.....	43
	PM fynd i iPad Nironen	
	Bildfynd i 2023-5000-BG3418-5.....	45
	Kryptospårning Nironen	
	Kryptospårning avseende återskapade plånböckerna.....	55
	230502 PM _Adam tillägg 200123 till 20424, 200925.....	71
	230510 PM _Adam tillägg Bitcoin högersida Chipmix.....	98
	230510 PM _Adam tillägg AN_77 AN_5 Chipmixer_demix.....	113
	Personalia	
	Bilaga skäligen misstänkt, Kronberg, Fredrik Ulf Julius.....	127
	Personalia, Kronberg, Fredrik Ulf Julius.....	128
	Bilaga skäligen misstänkt, Nederman, Hampus Helge.....	129
	Personalia, Nederman, Hampus Helge.....	130
	Bilaga skäligen misstänkt, Ihrén Nironen, Adam Antti.....	131



Polisen

PM**HEMLIG**
1(6)

Datum 2023-05-09

Infoklass Ej klassad

Diariennr (åberopas) 5000-K615323-19

Polismyndigheten
Nationella operativa avdelningen
Nationellt IT-Brottscentrum
Pär Landegren

Angående Ethereumadressen

0xDB7CEc67A768B1DaBB820937335a6bfadec1228a

(3 bilagor)

Bakgrund & Syfte

I samband med husrannsakan på [REDACTED] så genomfördes liveforsensik på en dator (se PM *Liveforensik stationär dator BG 136753-24*). Då uppmärksammades en flik från tjänsten zapper.fi som visade adressen för ethereumadressen 0xDB7CEc67A768B1DaBB820937335a6bfadec1228a.

I samband med husrannsakan på [REDACTED] och Banérgatan 51 har ett antal hårdvaruplånböcker för kryptovaluta av märket Ledger¹ har tagits i beslag.

Syftet med detta PM är utröna kopplingarna mellan denna adress och Fredrik Kronberg.

¹ <https://www.ledger.com/>

Polismyndigheten

2023-05-09

HEMLIG
2(6)

Dnr 5000-K615323-19

Infoklass Ej klassad

Sammanfattning & Analys

Ehtereumadressen 0xDB7CEc67A768B1DaBB820937335a6bfadec1228a har varit inloggad genom MetaMask² på flera tjänster. För att kunna vara inloggad på via MetaMask så krävs det att man har de privata nycklarna för den adress man vill logga in med. Dessa kan antingen finnas direkt i MetaMask eller i en hårdvaruplånbok. Ovan adress privata nyckel har visats befinna sig på en hårdvaruplånbok av märket Ledger.

Stakeing har genomförts från ovan adress och nycklar för att göra uttag från dessa har påträffats i **2021-5000-BG136753-24**.

Transaktioner till Mixertjänsten Tornado Cash har gjorts från ovan adress. I **2021-5000-BG136753-24** har också sk. Tornado Cash notes påträffats.

För att göra alla transaktioner och åtgärder som beskrivs ovan krävs den privata nyckeln för ovan adress. Då datorn var inloggad med ovan adress vid husrannsakan samt övrig information hittad i **2021-5000-BG136753-24** är det därför rimligt att anta att Fredrik Kronberg disponerar adressen 0xDB7CEc67A768B1DaBB820937335a6bfadec1228a.

² <https://metamask.io/>

Polismyndigheten

2023-05-09

HEMLIG

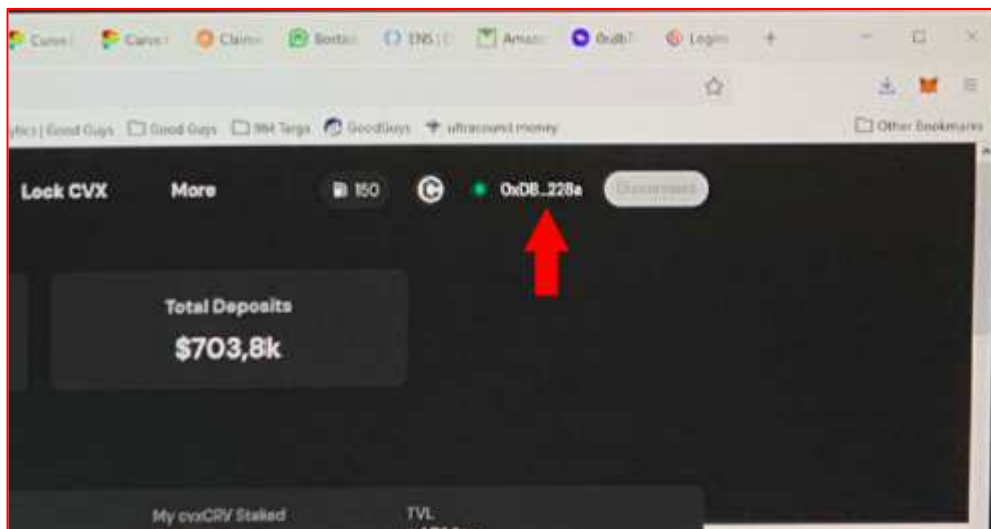
Dnr 5000-K615323-19

Infoklass Ej klassad

Resultat

Inloggad via metamask på olika tjänster

På sidan 4 i PM *Liveforensik stationär dator BG 136753-24* syns en bild som visar att en adress med första tecknen 0xDB och sista tecknen 228a är inloggad på tjänsten convexfinance³ (röd pil nedan). Samma info syns även på sidan 8 i ovan PM.



Urklipp från bild på sidan i Liveforensik stationär dator BG 136753-24

³ <https://www.convexfinance.com/>

Polismyndigheten

2023-05-09

HEMLIG

Dnr 5000-K615323-19

Infoklass Ej klassad

Nedan bild  r ett utdrag ur en film som togs ocks  vid den liveforensik som gjordes. Den visar att en ethereumadress  r inloggad p  tj nsten stakedao⁴.

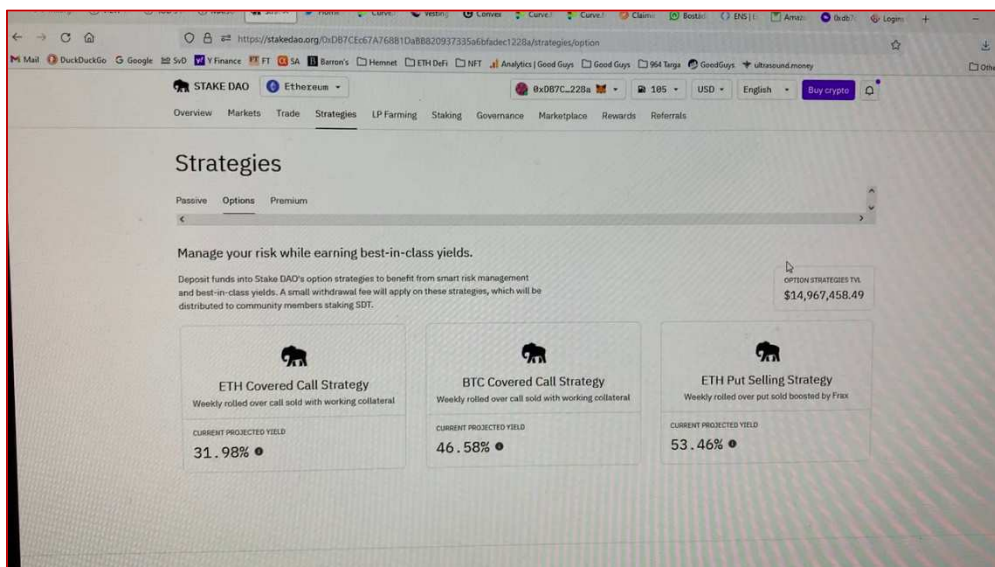
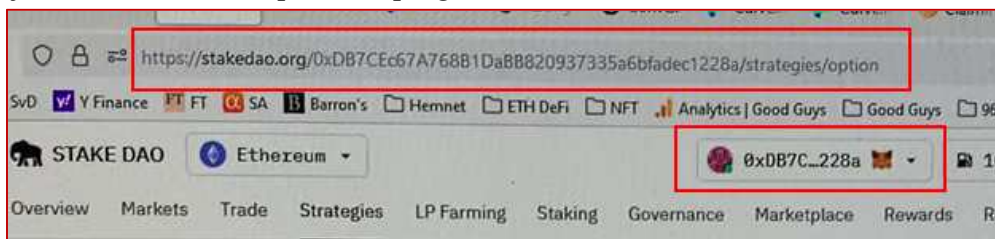


Bild fr n filmsekvens av sk rm fr n liveforensik

Ett inzoomat klipp fr n ovan bild visar att det  r adressen 0xDB7CEc67A768B1DaBB820937335a6bfadec1228a som  r inloggad p  tj nsten stakedao via pl nboksprogramvaran MetaMask.



Urklipp fr n ovan bild.

Metamask artefakter

I PM *Artefakter tillh rande MetaMask p tr ffade i 2021-5000-BG136753-24 och 2022-5000-BG118207-3* sl s det fast att i ovan n mnda beslagspunkter har det funnits en MetaMask i 2021-5000-BG136753-24 inneh llandes adressen 0xDB7CEc67A768B1DaBB820937335a6bfadec1228a kopplat till en Ledger.

⁴ <https://stakedao.org/>

Polismyndigheten

2023-05-09

HEMLIG

Dnr 5000-K615323-19

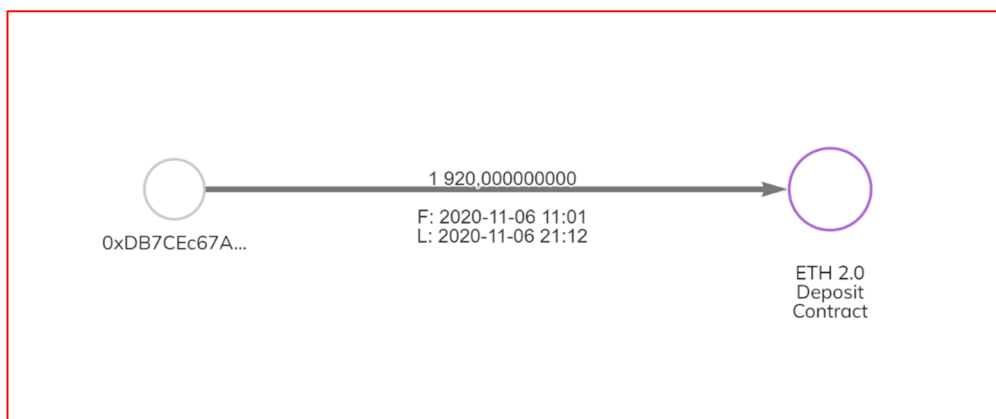
Infoklass Ej klassad

Stakeing

Ethereum-nätverket har bytt system för att godkänna nya block till blockkedjan från att lösa komplexa matematiska problem (proof of work) till att speciella noder godkänner nya block. Dessa noder måste ha en form av säkerhet i form av ether insatt (proof of stake).

En person kan alltså delta i detta nätverk genom att sätta in 32 ether till ett smart kontrakt. Därefter kan noden godkänna nya block till blockkedjan. Som ersättning för detta så erhålls delar av den transaktionsavgift som tas ut från varje transaktion. På så sätt erhålls en form av ränta på insatt kapital. Räntan är ungefär 4%. I ovan process så erhålles nycklar för att möjliggöra uttag av ev. vinst eller för att ta ut hela det stakeade beloppet.

Via blockkedjeanalys så kan man se att från adressen 0xDB7CEc67A768B1DaBB820937335a6bfadec1228a har det skickats 1920 eth till det smarta kontraktet som sköter stakeing på ethereums blockkedja. 1920 eth motsvarar alltså 60 st. noder. Transaktionsdata återfinns i bilaga 1.



Grafisk representation av insättningar till smart kontrakt.

I beslag **2021-5000-BG136753-24** återfinns de nycklar som beskrivs i tidigare stycke, dvs de nycklar som kan användas för att göra uttag från ovan noder. Då dessa kan användas för att göra uttag så är det betrakta som värdehandlingar och därför redovisas inte dessa i detta PM.

Polismyndigheten

2023-05-09

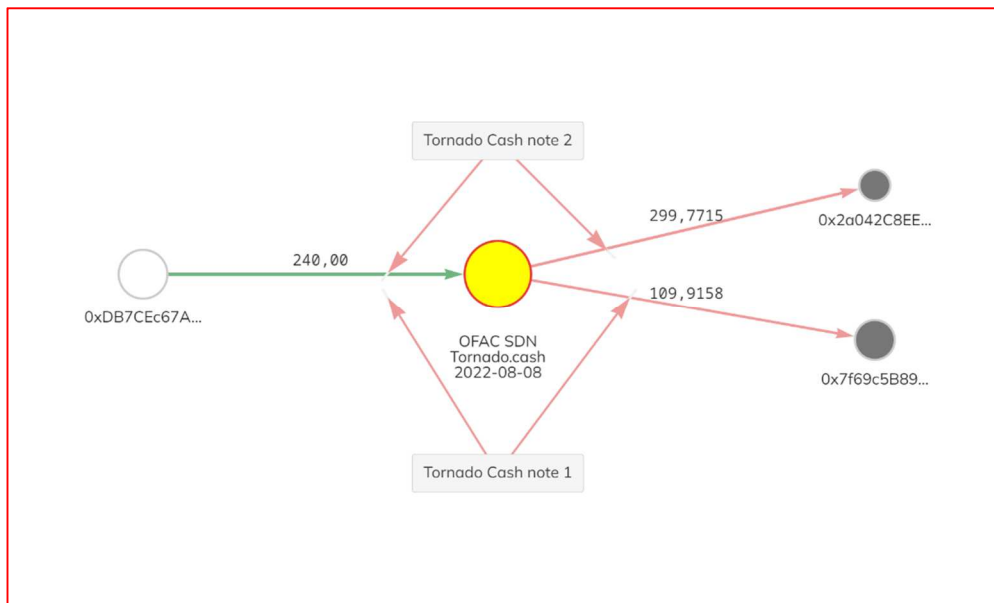
HEMLIG
6 (6)

Dnr 5000-K615323-19

Infoklass Ej klassad

Tornado Cash notes

Via blockkedjeanalys så kan man se att 0xDB7CEc67A768B1DaBB820937335a6bfadec1228a gör flera transaktioner till mixertjänsten Tornado Cash. För beskrivning om hur Tornado Cash fungerar så se **PM Tornado Cash**.



Grafisk representation av transaktioner till och från Tornado Cash

I beslag **2021-5000-BG136753-24** har två st. sk. Tornado cash notes återfunnits. Vid analys av dessa så kan man se att dessa Tornado cash notes använts för att göra transaktioner från 0xDB7CEc67A768B1DaBB820937335a6bfadec1228a till de två andra klustren som visas i ovan graf. Samtliga transaktioner finns i Bilaga 1.

Pär Landegren
Handläggare Teknisk Inhämtning

Bilagor

Bilaga1.xlsx

Tornado Cash Compliance report 1.pdf

Tornado Cash Compliance report 2.pdf



HEMLIG

Tornado.cash Compliance Report

Note

tornado-eth-100-1-0x55c3b45c95cde3ed01fb6f34ec5bdbb564464dd362461ec1dffa8850d5b655a74bc3812671507da5142ecc64e97984869bc0d1cfc9282330c1662109a1c

Deposit

100 ETH

Verified

Date

May 29, 2021 4:37 PM +UTC

Transaction

0x969609f6c1f6cc1ef443b38e49c362ebc3d606dd14a72f831d530acca4b3acce

From

0xdb7cec67a768b1dabb820937335a6bfadec1228a

Commitment

0x0363efe7659aaa4c3771e2d1e41be76484a6e765c481b493dddb23d20b591b46

Withdrawal

99.941 ETH

Verified

Relayer fee 0.059 ETH

Date

May 30, 2021 5:29 PM +UTC

Transaction

0xddaed210f6278390c953db827f2b9e1d2aeb0a7b61aef969445e9b712c34ceaf

To

0x7f69c5b893e04111640a209dd3d292a03850a668

Nullifier Hash

0x142ec3463ef5cb55b7f47428f2f01663b8ad0433a4ed1a5aa22afcb3a6cd7dde



Warning

This Compliance Report is for informational purposes only. You should confirm the validity of this report by using Tornado's Compliance Tool (<https://tornadocash.eth.link/compliance>) or via any other cryptographic software that can compute and verify the information contained herein (the "Tornado Compliance Tool"). Any discrepancies between information found in this report and provided by the above tool indicate that the information in this report may be inaccurate and/or fraudulent. THE COMPLIANCE REPORT IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OF THE TORNADO.CASH COMPLIANCE TOOL BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THIS COMPLIANCE REPORT.



HEMLIG

Tornado.cash Compliance Report

Note

tornado-eth-100-1-0xe4c9f2a27ea0d38dcfc6280f7f460ffd7f6ca5c1ad0b4fc25c41a8aeb6e9b774044b1cac0a332c5e606e1ed48e86f4224fb389136579340eb273be5b54c4

Deposit

100 ETH

Verified

Date

Nov 8, 2021 10:18 AM +UTC

Transaction

0xaab6a65d203180d766189c5c51fea699f0e621917c2a7
be965aa8400a57d9496

From

0xdb7cec67a768b1dabb820937335a6bfadec1228a

Commitment

0x2956c3a65684f59785da44da5edc846cde9efce6a577d
abdfa323d44b402af02

Withdrawal

99.919 ETH

Verified

Relayer fee 0.081 ETH

Date

Nov 8, 2021 6:03 PM +UTC

Transaction

0x40b24156b4af3fa00c1625f6ee23f6ad92b299d188b2d
8fe81cbe7021c81c7df

To

0x2a042c8ee907a4712bf54463de7c4ed4c4b87671

Nullifier Hash

0x2e2e6d0c77da92a136c52de3627c787a357544c6fcf4d
27e811995c17869cec1



Warning

This Compliance Report is for informational purposes only. You should confirm the validity of this report by using Tornado's Compliance Tool (<https://tornadocash.eth.link/compliance>) or via any other cryptographic software that can compute and verify the information contained herein (the "Tornado Compliance Tool"). Any discrepancies between information found in this report and provided by the above tool indicate that the information in this report may be inaccurate and/or fraudulent. THE COMPLIANCE REPORT IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OF THE TORNADO.CASH COMPLIANCE TOOL BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THIS COMPLIANCE REPORT.



Polisen

HEMLIG

12

Förhör

Signerat av

Signerat datum

Enhet

Nationella Operativa Avdelningen, Komplexa cyberbrott (KCB) 1 NIB NOA

Diariernr

5000-K615323-19

Hörd person

Ihrén Nironen, Adam Antti

Personnummer

19940119-7554

Den hörde är

Misstänkt

ID Styrkt

Ja

Sätt

Känd av Insp Keyzer

Ställning till misstänkt - målsägande - vittne

Tolk

Språk

Anledning till förhör / Misstankar som misstänkt har underrättats om

Synnerligen grovt narkotikabrott, Fullbordat, Gärningsman

Underrättad om misstanke

2023-01-09

Ytterligare information om anledning till förhör

Fortsatta förhör i ärendet

Underrättad om rätt till försvarare

Godtar den försvarare som rätten förordnar

Försvarare/ombud önskas

Advokat Nils Svantemark

Försvarare/ombud närvarande

Ja

Förhørsledare

Jim Keyzer

Förhørsdatum

2023-04-26

Förhör påbörjat

14:15

Förhör avslutat

Förhørsplats

Häktet Kronoberg

Typ av förhör

RB 23:6

Förhörssätt

Ljudbandsförhör

Förhörsvittne

Utskrivet av

NJ

Berättelse



Polismyndigheten
NOA
Nationellt It-brottscentrum, It-forensik
106 75 STOCKHOLM

Datum
2023-05-02

Diarienummer
K615323-19
5800/49376-21

HEMLIG

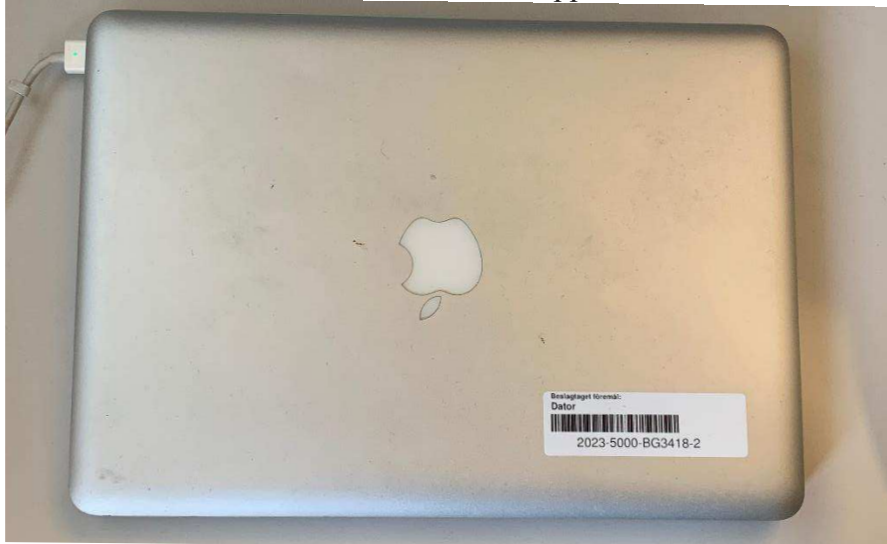
Extraktionsprotokoll avseende beslag 2023-5000-BG3418-2

Inledande uppgifter

Undersökningen begärd av: Kammaråklagare Henrik Söderman
Anledning till undersökningen: Extrahering av information
Ansvarig it-forensiker: Viktor Näsman
Tid för undersökningen: Undersökningen påbörjades den 9 februari 2023

Sammanfattning

Beslaget var en Macbook av tillverkaren Apple.



Datorn var krypterad och dekrypteringsförsök utfördes. Då det korrekta lösenordet inte påträffades gick det inte att utföra någon analys.

Viktor Näsman
It-forensiker



Polisen

HEMLIG

14

Tjänsteanteckning

Not Återställning av seeds till kryptoplånb. v. 2

Signerad av

Signerad datum

Enhet

Nationella Operativa Avdelningen, Komplexa cyberbrott (KCB) 1 NIB NOA

Diariernr

5000-K615323-19

Uppgiftslämnare

Keyzer, Jim

Datum

2023-05-08

Tid

14:52

Beslag verkställt

Nej

Material för analys

Nej

Mottaget

Mottaget datum

Tid

Sätt på vilket uppgift lämnats

Upprättad av

Jim Keyzer

Uppgiften avser

KORRIGERING/TILLÄGG

Uppgift

OBS: ett PM med väsentligen samma innehåll som dokumentet nedan har tidigare distribuerats med tilläggsprotokoll 3. Dock saknades redovisning av en transaktion i det PM, varför det kompletta och korrekta underlaget istället läggs in i tilläggsprotokoll 4.

/JK



Polisen

PM**HEMLIG**
1(4)

Datum 2023-05-08

Infoklass Ej klassad

Diariennr (åberopas) 5000-K615323-19

Polismyndigheten
Nationella operativa avdelningen
Nationellt IT-Brottscentrum
Pär Landegren

Återställning av plånböcker från beslag BG3418-5

(2 bilagor)

Bakgrund & Syfte

I forensisk undersökning av beslag BG3418-5 har påträffats vad som bedöms vara ett antal återställningsfraser till plånböcker innehållandes kryptovaluta. Totalt har det påträffats 3 återställningsfraser till monero, 1 återställningsfras till Bitcoin Cash och 33 st återställningsfraser till Bitcoin.

Syftet med detta PM är att redovisa resultatet av återställning av dessa plånböcker.

Plånböckerna är benämnda med ett löpnummer från den forensiska rapport samt första och sista ordet i återställningsfrasen.

Resultat

Moneroplånböcker

Samtliga moneroplånböcker har återställts i programvaran Feather¹.

Plånboken 1 jogger vessel

Plånboken innehåller transaktionsdata och ett kvarvarande saldo på 3.672330953449 xmr. Transaktionsdata har exporterats ut ur plånboken och bifogas som bilaga till detta PM.

Plånboken 2 trolling tamper

Plånboken innehåller inga transaktioner

Plånboken 4 eavesdrop ruined

Plånboken innehåller inga transaktioner

¹ <https://featherwallet.org/>

Polismyndigheten

2023-05-08

HEMLIG
2(4)

Dnr 5000-K615323-19

Infoklass Ej klassad

Bitcoin Cash-Plånbok

Plånboken 131 recycle cupboard

Plånboken har återställts i programvaran Electron Cash² och innehöll inga transaktioner.

Bitcoinplånböcker

Samtliga plånböcker har återställts i programvaran Electrum³ om inget annat redovisas. Om transaktioner har återfunnits har adresser innehållandes transaktioner exporterats ut och redovisats i bilaga 2.

Plånboken 99 section flat

Plånboken har återställts i Programvaran Wasabi Wallet⁴ och innehöll inga transaktioner.

Plånboken 5 object divorce

Plånboken har ett kvarvarande saldo på 0,00023549 BTC

Plånboken 9 staff alert

Plånboken har inget kvarvarande saldo.

Plånboken 16 tumble dizzy

Plånboken innehåller inga transaktioner

Plånboken 18 pull company

Plånboken har inget kvarvarande saldo.

Plånboken 20 able maple

Plånboken har ett kvarvarande saldo på 0,00060831 BTC.

Plånboken 26 detail spread

Plånboken innehåller inga transaktioner

Plånboken 27 napkin cash

Plånboken har inget kvarvarande saldo.

Plånboken 29 section vacant

Plånboken har ett kvarvarande saldo på 0,00008632 BTC

² <https://electroncash.org/>

³ <https://electrum.org/>

⁴ <https://wasabiwallet.io/>

Polismyndigheten

2023-05-08

HEMLIG
3(4)

Dnr 5000-K615323-19

Infoklass Ej klassad

Plånboken 42 card then

Plånboken har ett kvarvarande saldo på 0,00008632 BTC.

Plånboken 44 purity offer

Plånboken har inget kvarvarande saldo.

Plånboken 45 never beyond

Plånboken har inget kvarvarande saldo.

Plånboken 48 fee correct

Plånboken har inget kvarvarande saldo.

Plånboken 53 accident grain

Plånboken har inget kvarvarande saldo.

Plånboken 54 cabbage episode

Plånboken hade ett återstående saldo på 1,0177615 BTC. Beslag av dessa redovisas i annat pm.

Plånboken 65 unaware purse

Plånboken hade ett återstående saldo på 0,00041618 BTC. Beslag av dessa redovisas i annat pm.

Plånboken 69 prefer anchor

Plånboken har ett återstående saldo på 0,00018537 BTC.

Plånboken 72 ill cave

Plånboken har ett återstående saldo på 0,00026389 BTC.

Plånboken 77 original curious

Plånboken har inget kvarvarande saldo.

Plånboken 78 enough brick

Plånboken har ett återstående saldo på 0,00099057 BTC.

Plånboken 80 harbor pudding

Plånboken har ett återstående saldo på 0,00093775 BTC.

Plånboken 86 cereal shiver

Plånboken har inget kvarvarande saldo.

Polismyndigheten

2023-05-08

HEMLIG
4(4)

Dnr 5000-K615323-19

Infoklass Ej klassad

Plånboken 89 strategy dentist

Plånboken har ett återstående saldo på 0,00438866 BTC.

Plånboken 91 note sound

Plånboken har ett återstående saldo på 0,00012159 BTC.

Plånboken 93 eyebrow sunset

Plånboken har ett återstående saldo på 0,00094803 BTC.

Plånboken 97 tomorrow rather

Plånboken har ett återstående saldo på 0,00040499 BTC.

Plånboken 100 put sniff

Plånboken har inget kvarvarande saldo.

Plånboken 104 drastic honey

Plånboken har ett återstående saldo på 0,00052480 BTC

Plånboken 120 belt pigeon

Plånboken har ett återstående saldo på 0,00043250 BTC

Plånboken 140 scatter solar

Plånboken har inget kvarvarande saldo.

Pär Landegren

Handläggare Teknisk Inhämtning

Bilagor

Bilaga 1 – Monerotransaktioner

Bilaga 2 – Adresser i återställda Bitcoinplånböcker



Polisen

PM**HEMLIG**
1(5)

Datum 2023-05-05

Infoklass Ej klassad

Diariennr (åberopas) 5000-K615323-19

Polismyndigheten
Nationella operativa avdelningen
Nationellt IT-Brottscentrum
Pär Landegren

Återställning av plånböcker från beslag BG3418-1

(1 bilaga)

Bakgrund & Syfte

I forensisk undersökning av beslag BG3418-1 har påträffats vad som bedöms vara ett antal återställningsfraser till plånböcker innehållandes kryptovaluta.

Syftet med detta PM är att redovisa resultatet av återställning av dessa plånböcker.

Plånböckerna är benämnda med första och sista ordet i återställningsfrasen.

Om transaktioner har återfunnits har adresser innehållandes transaktioner exporterats ut och redovisats i bilaga 1.

Resultat

Bitpay wallet

Plånböckerna har återställts i programvaran Bitpay wallet¹.

Plånboken clog long

Plånboken innehåller inga transaktioner

Plånboken era police

Plånboken har ett kvarvarande saldo på 0,0015687 BTC

Pi wallet epand gravity

Plånboken har ej återställts då inloggning krävs för samt att det bedöms inte ha bäring på ärendet.

¹ <https://bitpay.com/wallet/>

Polismyndigheten

2023-05-05

HEMLIG
2(3)

Dnr 5000-K615323-19

Infoklass Ej klassad

Electrum plunge mind

Plånboken har återställts med programvaran Electrum². Plånboken innehåller inga transaktioner.

Defiwallet

Plånböckerna har återställts med programvaran Crypto.com Defi wallet³

Plånboken picture vehicle

Plånboken innehöll inga transaktioner.

Plånboken universe arena

Plånboken har ett kvarvarande saldo på 0,00003841 BTC

Breadwallet coconut axis

Plånboken har återställts i programvaran Electrum och har ett kvarvarande saldo på 0,00032062 BTC

CakeWallet

Dessa återställningsfraser är samma som avhandlas för Monero i PM

Återställning av plånböcker från beslag BG3418-5 och kommer därför inte redovisas i detta PM.

Incognito Wallet

Plånboken har återställts med programvaran Incognito wallet. Plånboken innehåller inga Bitcoin-transaktioner. Den innehåller transaktioner för PRV-token men de bedöms inte ha någon bäring på ärendet.

CoinBase Wallet

Plånböckerna har återställts i Coinbase Wallet⁴.

Plånboken claim shuffle

Plånboken innehöll inga transaktioner.

Plånboken fiber grain

Plånboken innehöll inga transaktioner.

Plånboken unveil author

Plånboken innehöll inga transaktioner.

² <https://electrum.org/>

³ <https://crypto.com/eea/defi-wallet>

⁴ <https://www.coinbase.com/wallet>

Polismyndigheten

2023-05-05

HEMLIG
3(3)

Dnr 5000-K615323-19

Infoklass Ej klassad

CoPay Wallet lab husband

Plånboken har återställts i Bitpay wallet⁵ och innehöll inga transaktioner

AtomicWallet

Plånböckerna har återställts i Atomic wallet⁶.

Plånboken bottom walk

Plånboken innehöll inga transaktioner.

Plånboken satisfy you

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken unaware dawn

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken wrist genius

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken quality robust

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken boring absorb

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken bounce pencil

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken lend empty

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken second grocery

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken repeat loyal

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

⁵ <https://bitpay.com/wallet/>

⁶ <https://atomicwallet.io/>

Polismyndigheten

2023-05-05

HEMLIG
4(3)

Dnr 5000-K615323-19

Infoklass Ej klassad

Plånboken spatial transfer

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken glory quick

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken noble punch

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken moment inmate

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken cream april

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken wall ride

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken index rack

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken cause hundred

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken prefer airport

Återställningsfrasen var ogiltig och därför kan ingen plånbok återskapas.

Plånboken diesel shoulder

Plånboken innehöll inga transaktioner

Polismyndigheten

2023-05-05

HEMLIG
5(3)

Dnr 5000-K615323-19

Infoklass Ej klassad

Pär Landegren
Handläggare Teknisk Inhämtning

Bilagor

Bilaga 1 – Adresser i återställda Bitcoinplånböcker



Polisen

PM**HEMLIG**
1 (19)

Datum 2023-05-10

Diariennr (åberopas)

Polismyndigheten
Utredningsenheten
Nationellt it-brottscentrum
Teknisk inhämtning
Max Ståhl

5000-K615232-19

Analys av återskapade plånböcker med löpnummer 91, 97, 104 och 120, från beslag 2023-5000-BG3418-5.

Syfte

Syftet med detta PM är att beskriva de kryptofinansiella observationer och analyser som gjorts i ärendet gällande Adam Nironens löneplånböcker som identifierats med hjälp av återställningsfraser från beslag av Adam Nironens ipad.

Bakgrund

En återställningsfras är en värdehandling vilken ger tillgång till värdet och för att kunna genomföra transaktioner i plånboken.

Analyserade plånböcker är återskapade utav återställningsfraser från Adam Nironens ipad.¹

I detta PM finns en detaljerad analys per plånbok för:

- 2020-08-24 löpnummer 91
- 2020-05-25 löpnummer 97
- 2020-07-24 löpnummer 104
- 2020-06-25 löpnummer 120

Plånböcker som tar emot jämn insättning på lönedatum benämns löneplånböcker

¹ För information om hur återskapandet gått till se PM Analys svar från Coinbase, H. N.

Sammanfattning

I detta PM analyseras fyra återskapade plånböcker, som hittas i beslaget av Adam Nironens ipad.

Alla fyra har hanterats på liknande sätt genom att de har tagit emot jämna summor på datum 24:e eller 25:e i månaden. Efter att plånböckerna tagit emot en summa BTC så genomförs transaktioner till mixertjänsten Chip-mixer fem-sex gånger under perioden av en månad tills det att plånboken är tom.

De inkommande transaktionerna kan i två fall (löpnummer 91 och 97) härledas till att ha sitt ursprung i vad som liknar säkerhetsinbetalningar tillhörande FS3. Denna analys är baserad på att säkerhetsinbetalningar har vid andra tillfällen använts av admin för FS3 för att göra löneutbetalningar till moderatorerna Hund, Regnskog och Lakritsfisk. Dessa två plånböcker tar emot lön för utifrån denna analys.

För mer information om löneutbetalningar och säkerhetsinbetalningar se,

- PM Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen
- PM Kryptospårning av löneutbetalningar - Moderator Regnskog
- PM Löneutbetalning Lakritsfisk Kryptospårning
- PM Säkerhetsinbetalningar från säljare till admin Flugsvamp 3.0
- PM Analys av Bitcoinflöde till och från marknadsplatsen Flugsvamp 3.0

De övriga två (löpnummer 104 och 120) har inkommande transaktioner som inte kan kopplas till säkerhetsinbetalningar. De inkommande transaktionerna kan inte heller kopplas till moderatorerna Regnskog och Lakritsfisk. Det har inte varit möjligt att göra en tydlig analys av de inkommande transaktionerna till plånböckerna med löpnummer 104 och 120. Det går inte att säga att det har varit lön som betalats ut till dessa två plånböcker.

Tillvägagångssätt

Plånböckerna har återskapats och analyserats baserat på:

- varifrån krypto till plånboken kommer ifrån
- när och hur mycket som emottagits
- hur plånboken hanterats

Gröna pilar - Har använts för att tydliggöra lönetransaktion

Polismyndigheten

2023-05-10

HEMLIG
3 (19)

Blåa pilar - Representerar växel vilket innebär att kluster som är samman-kopplade med blå pilar tillhör samma plånbok.

Lila pilar - FS3 relaterade transaktioner

Bilderna i detta PM ligger med som bilagor i större format.

Resultat

Nedan presenteras de återskapade plånböckerna separat.

Löneplånbok 20-08-24, löpnummer 91

Summering

Återskapad plånbok 200824 med återställningsfras från Adam Nironens ipad.²

Här är antagande avseende lön från FS3 baserat på:

- att insättningen av bitcoin var jämn och genomfördes på lönedatum
- värdet stämmer med övriga löneinsättningar
- plånboken är återskapad med återställningsfras från Adam Nironen
- plånboken tar emot en transaktion som kommer från kluster som tar emot transaktioner som liknar säkerhetsinbetalningar i storlek.
- plånbokens användning av Chipmixer, standardförfarande för moderator Hund och för de återskapade plånböckerna från Adam Nironen

² Återskapad plånbok med återställningsfras(note....sound) från Adam Nironens ipad med löpnummer 91. Beslag 2023-5000-BG3418-5.

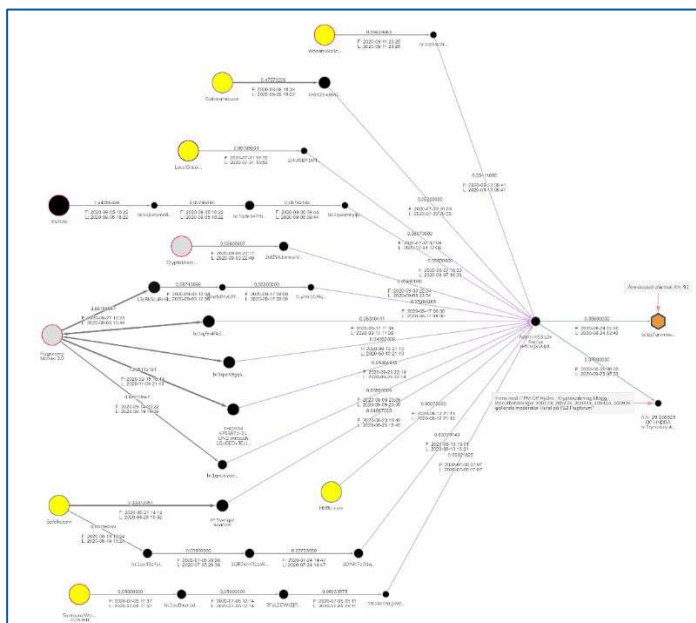


Bild 1 Transaktioner som liknar säkerhetsinbetalningar skickas vidare till plånbok AN 091

Tabell: Transaktionsdata

74b5e1ad571a88ccf76c04062498017c223f4556e4d9de6c8be3f2bd5ed67d35

Datum	Belopp BTC	Belopp SEK (ca)	Mottagande bitcoin address
200824	0,35	36 157	bc1q7qrvnawm7vk92j6g5jw3a50s5eyw5w0qcfzkpl

Fem av sex transaktioner gjorda med plånbokens adresser har gått till mixer-tjänsten Chipmixer. Vid återskapande av plånboken fanns ett saldo på 0,00012159 BTC.

Datum	Belopp BTC	Belopp SEK	Destination
2020-08-24	0,09	9 297	Chipmixer
2020-08-30	0,053	5 374	Chipmixer
2020-09-01	0,047	4 849	Chipmixer
2020-09-13	0,07	6 326	Chipmixer
2020-09-20	0,05	4 800	Chipmixer
2021-07-30	0,039	14 096	Okänd

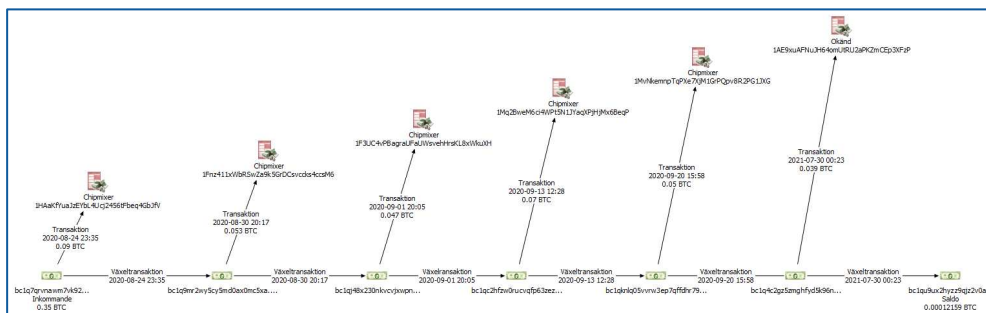


Bild 2 Hantering av krypto i plånbok AN 91

Löneplånbok 20-05-25, löpnummer 97

Summering

Återskapad plånbok 200525 med återställningsfras från Adam Nironens
ipad.³

Här är antagande avseende lön från FS3 baserat på:

- att insättningen av bitcoin var jämn och genomfördes på lönedatum
- värdet stämmer med övriga löneinsättningar
- Har kopplingar till FS3, bedömt genom möjliga säkerhetsinbetalningar; lila pilar med ca 0,052 BTC ca 5000 SEK under perioden
- plånboken är återskapad med återställningsfras från Adam Nironen
- plånbokens användning av Chipmixer liknar hanteringen av BTC som moderator Hund och för de övriga återskapade plånböckerna

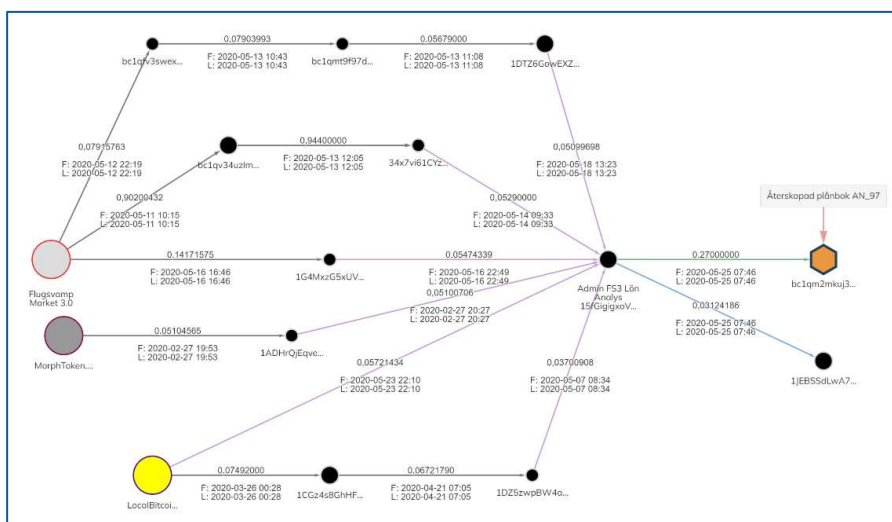


Bild 3 Transaktioner som liknar säkerhetsbetalningar skickas vidare till plånbok AN 097

³ Återskapad plånbok med återställningsfras(tomorrow....rather) från Adam Nironens ipad med löpnummer 97. Beslag 2023-5000-BG3418-5.

Tabell: Transaktionsdata

f62b04cbf8c093f279f6bf5f68d8f83e504c05a9e6d6027ef95e0656a936111d

Datum	Belopp BTC	Belopp SEK (ca)	Mottagande bitcoin address
200525	0,27	23 312	bc1qm2mkuj33z20gaee2zc9v9n06gg893yd9cy0tzd

Samtliga fem transaktioner gjorda med plånbokens adresser har gått till mixertjänsten Chipmixer. Vid återskapande av plånboken fanns ett saldo på 0,00040499 BTC.

Datum	Belopp BTC	Belopp SEK	Destination
2020-05-25	0,06	5 180	Chipmixer
2020-06-04	0,07	6 403	Chipmixer
2020-06-05	0,05	4 422	Chipmixer
2020-06-07	0,05	4 465	Chipmixer
2020-06-19	0,039	3 382	Chipmixer

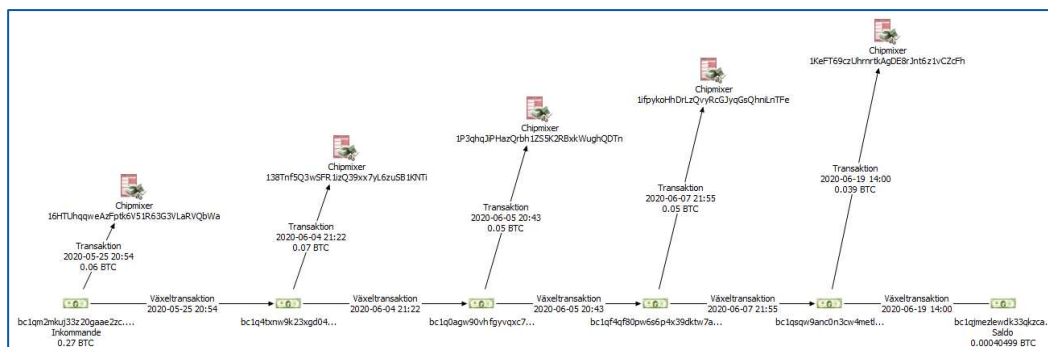


Bild 4 Hantering av krypto i plånbok AN_97

Löneplånbok 20-07-24, löpnummer 104

Summering

Återskapad plånbok 200724 med återställningsfras från Adam Nironens ipad.⁴

Här är antagande avseende lön från FS3 baserat på:

- att insättningen av bitcoin var jämn och genomfördes på lönedatum
- värdet stämmer med övriga löneinsättningar

⁴ Återskapad plånbok med återställningsfras(drastic...honey) från Adam Nironens ipad med löpnummer 104. Beslag 2023-5000-BG3418-5.

- plånboken är återskapad med återställningsfras från Adam Nironen
- plånbokens användning av Chipmixer och FS3, standardförfarande för moderator Hund och för de återskapade plånböckerna

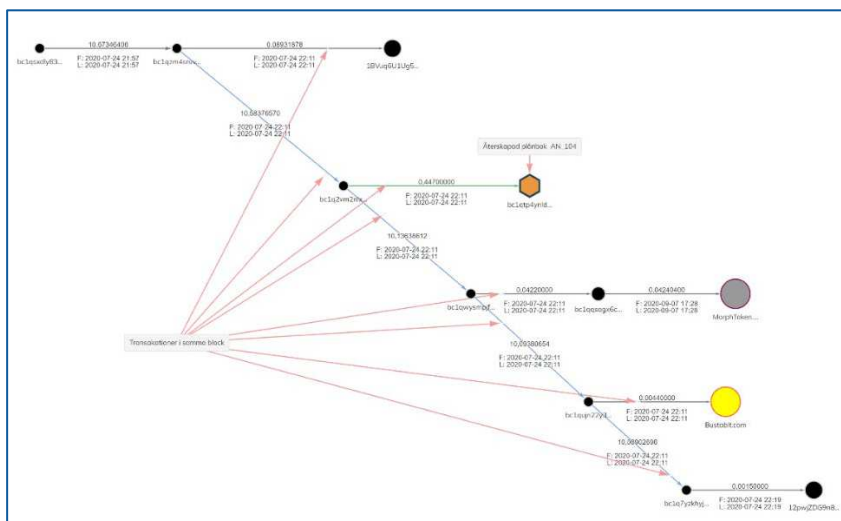


Bild 5 Plånbok som skickar till AN_104 skickar till olika okända mottagare i samma block

Tabell: Transaktionsdata

680905b5022f8dc5c559bf746b9bb5f882e8faf9e0879a6a3198123a38598ca6

Datum	Belopp BTC	Belopp SEK (ca)	Mottagande bitcoin address
200724	0,4470	37 828	bc1qtp4ynld8kfdcdwzav77tkxsxfry6g6zafr0lj

Fem av sex transaktioner gjorda med plånbokens adresser har gått till mixer-tjänsten Chipmixer. Vid återskapande av plånboken fanns ett saldo på 0,00052480 BTC.

Datum	Belopp BTC	Belopp SEK	Destination
2020-07-25	0,111	9 531	Chipmixer
2020-07-27	0,09	8 710	Chipmixer
2020-07-28	0,062	5 934	Chipmixer
2020-07-28	avgift (0,00037029)	35	Internt i plånboken
2020-08-04	0,082	8 012	Chipmixer
2020-08-18	0,10	10 394	Chipmixer

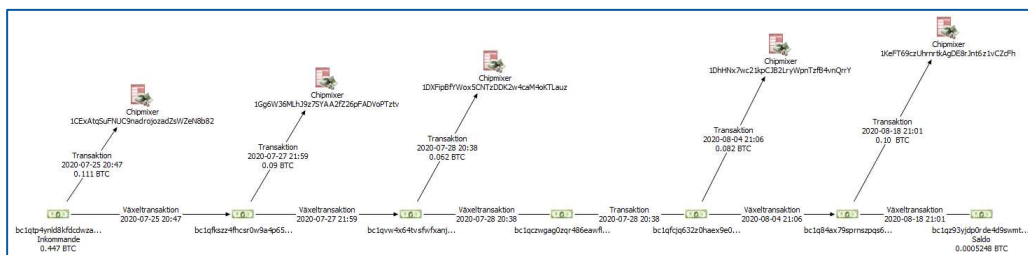


Bild 6 Hantering av krypto i plånbok AN_104

Löneplånbok 20-06-25, löpnummer 120

Summering

Återskapad plånbok 200625 med återställningsfras från Adam Nironens ipad.⁵

Här är antagande avseende lön från FS3 baserat på:

- att insättningen av bitcoin var jämn och genomfördes på löndatum
- värdet i SEK stämmer med övriga löneinsättningar
- plånboken är återskapad med återställningsfras från Adam Nironen
- plånbokens användning av Chipmixon och FS3, standardförfarande för moderator Hund och för de återskapade plånböckerna

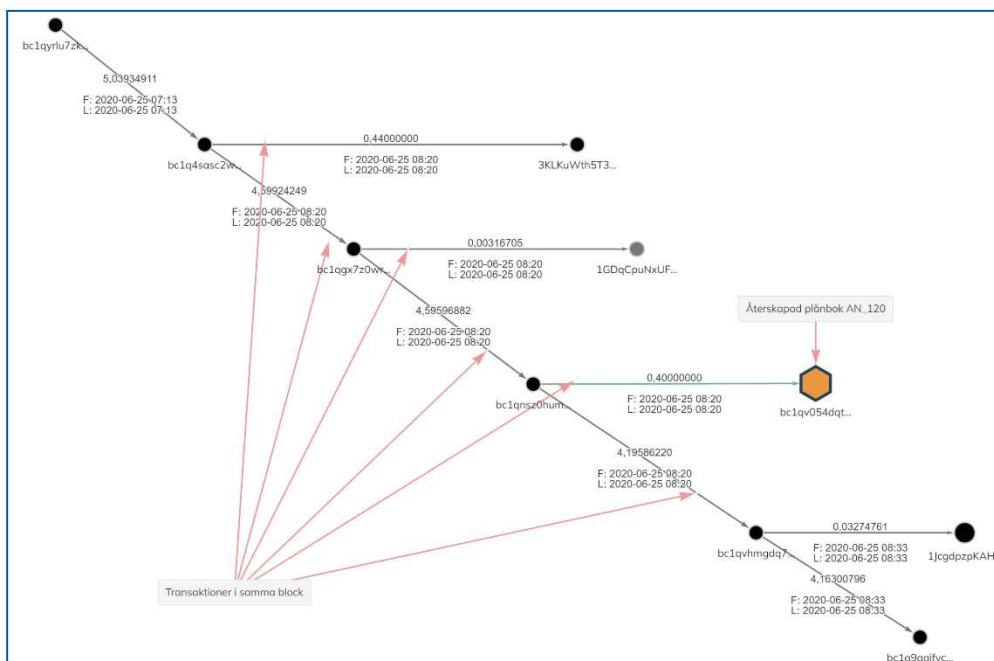


Bild 7 Plånbok som skickar till AN_120 skickar till olika okända mottagare i samma block

⁵ Återskapad plånbok med återställningsfras(belt...pigeon) från Adam Nironens ipad med löpnummer 120. Beslag 2023-5000-BG3418-5.

Polismyndigheten

2023-05-10

HEMLIG

Tabell: Transaktionsdata

daf8bbbf28f92e9d6b5ba23a7e9f2c01220ee6f645c28fd4dda460c2983d0356

Datum	Belopp BTC	Belopp SEK (ca)	Mottagande bitcoin address
200625	0,40	34 677	bc1qv054dqt9wcjfl84az6v5vrfy2hl40xdu2zd3wp

Samtliga sex transaktioner gjorda med plånbokens adresser har gått till mixertjänsten Chipmixer. Vid återskapande av plånboken fanns ett saldo på 0,0004325 BTC.

Datum	Belopp BTC	Belopp SEK	Destination
2020-06-25	0,06	5 201	Chipmixer
2020-06-26	0,066	5 639	Chipmixer
2020-07-05	0,069	5 835	Chipmixer
2020-07-06	0,045	3 937	Chipmixer
2020-07-14	0,07	5 945	Chipmixer
2020-07-20	0,089	7 359	Chipmixer

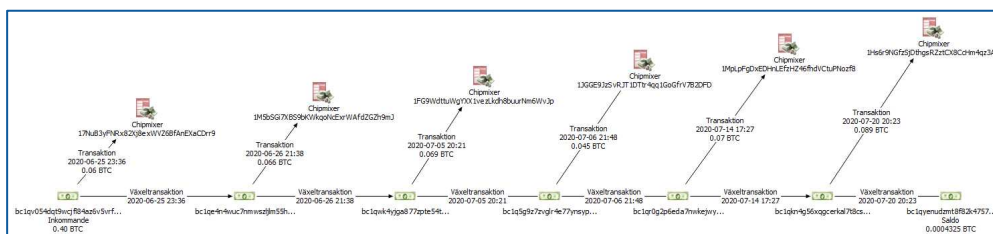


Bild 8 Hantering av krypto i plånbok AN_120

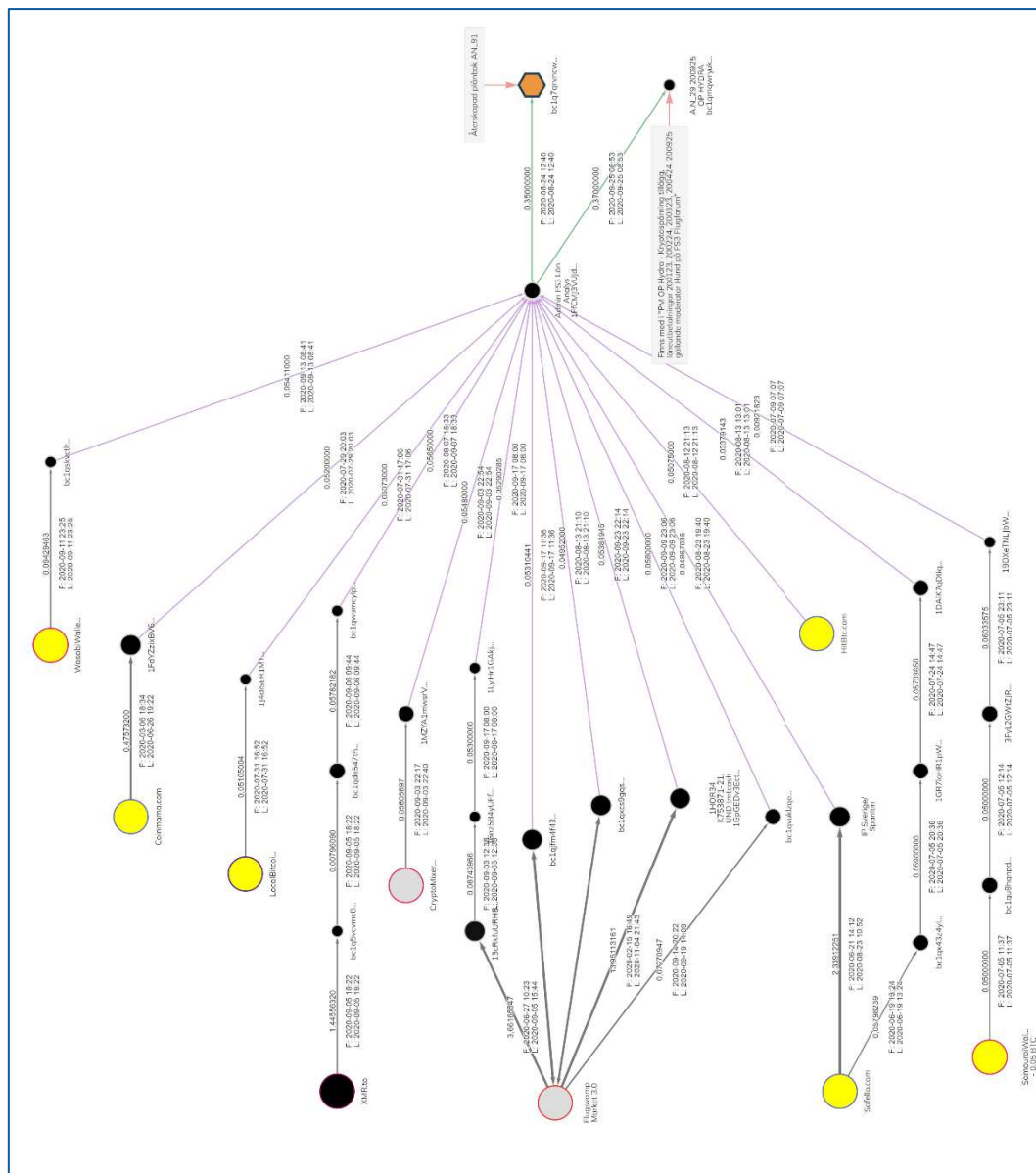
Handläggare

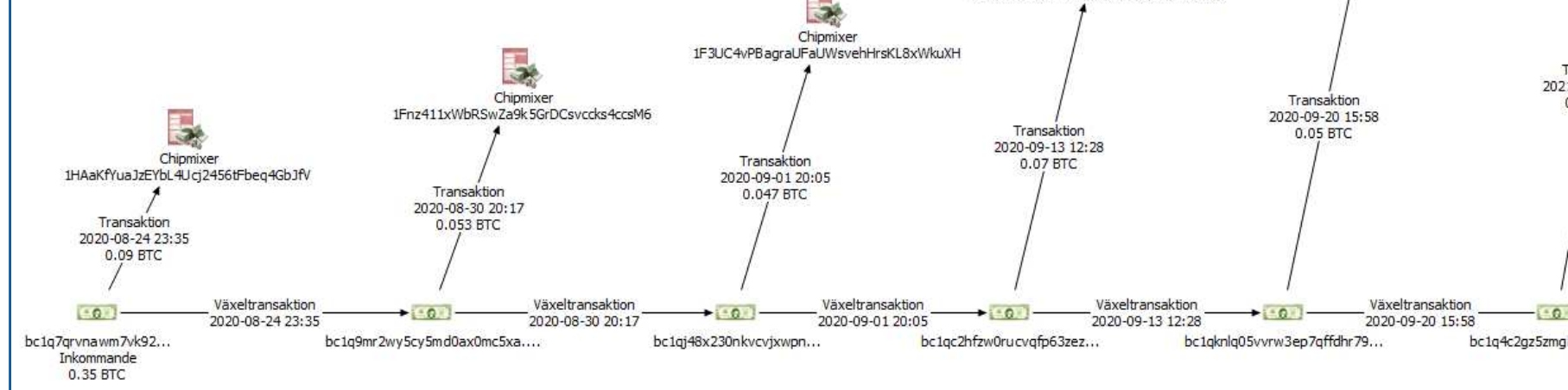
Max Ståhl

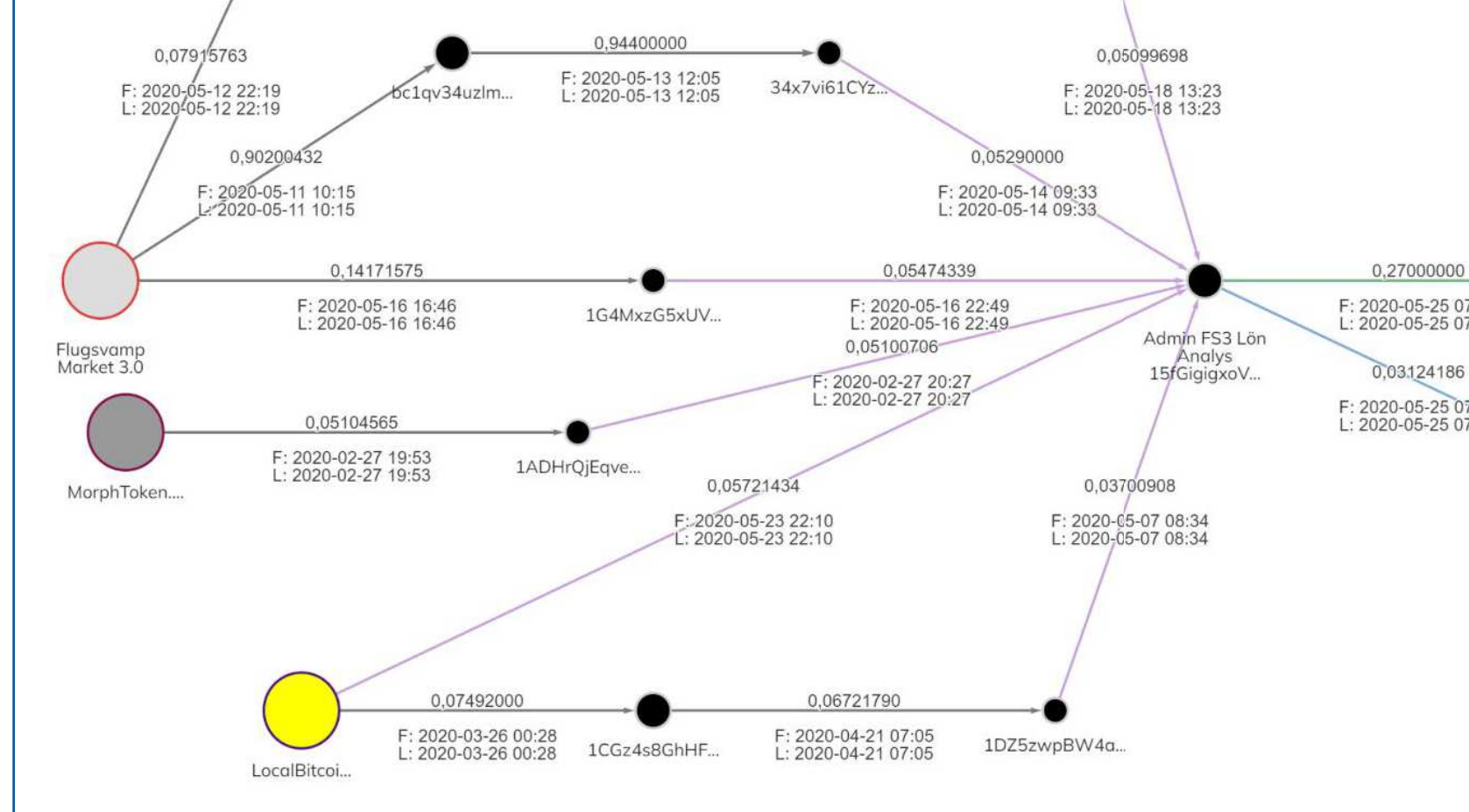
Bilaga 1-8: Bilder från PM i större format

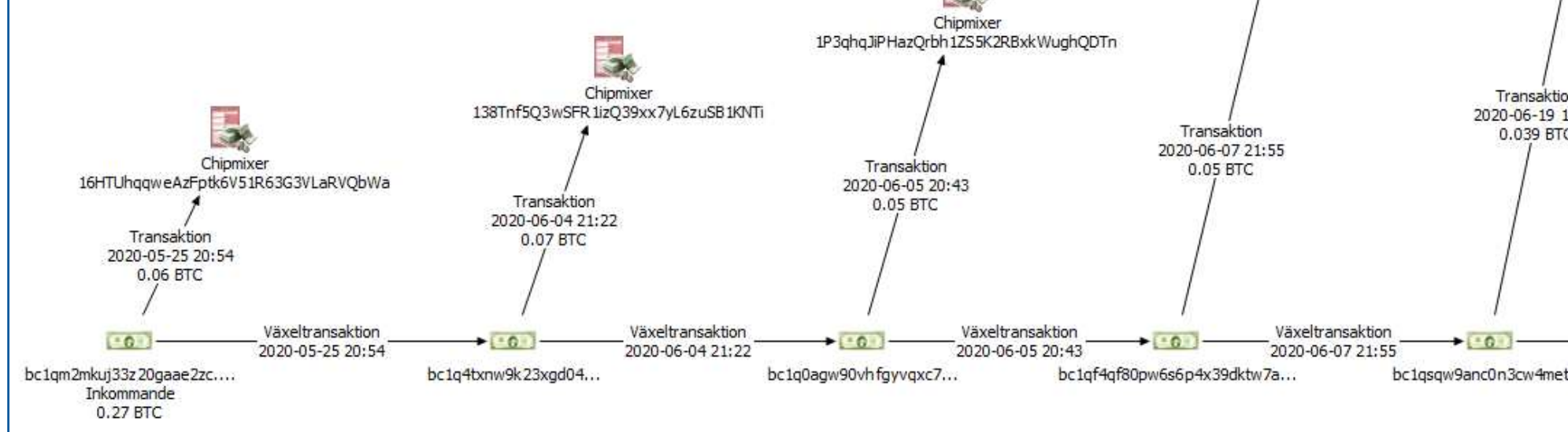
Bilaga 9: Adresser och transaktioner i återskapade plånböcker

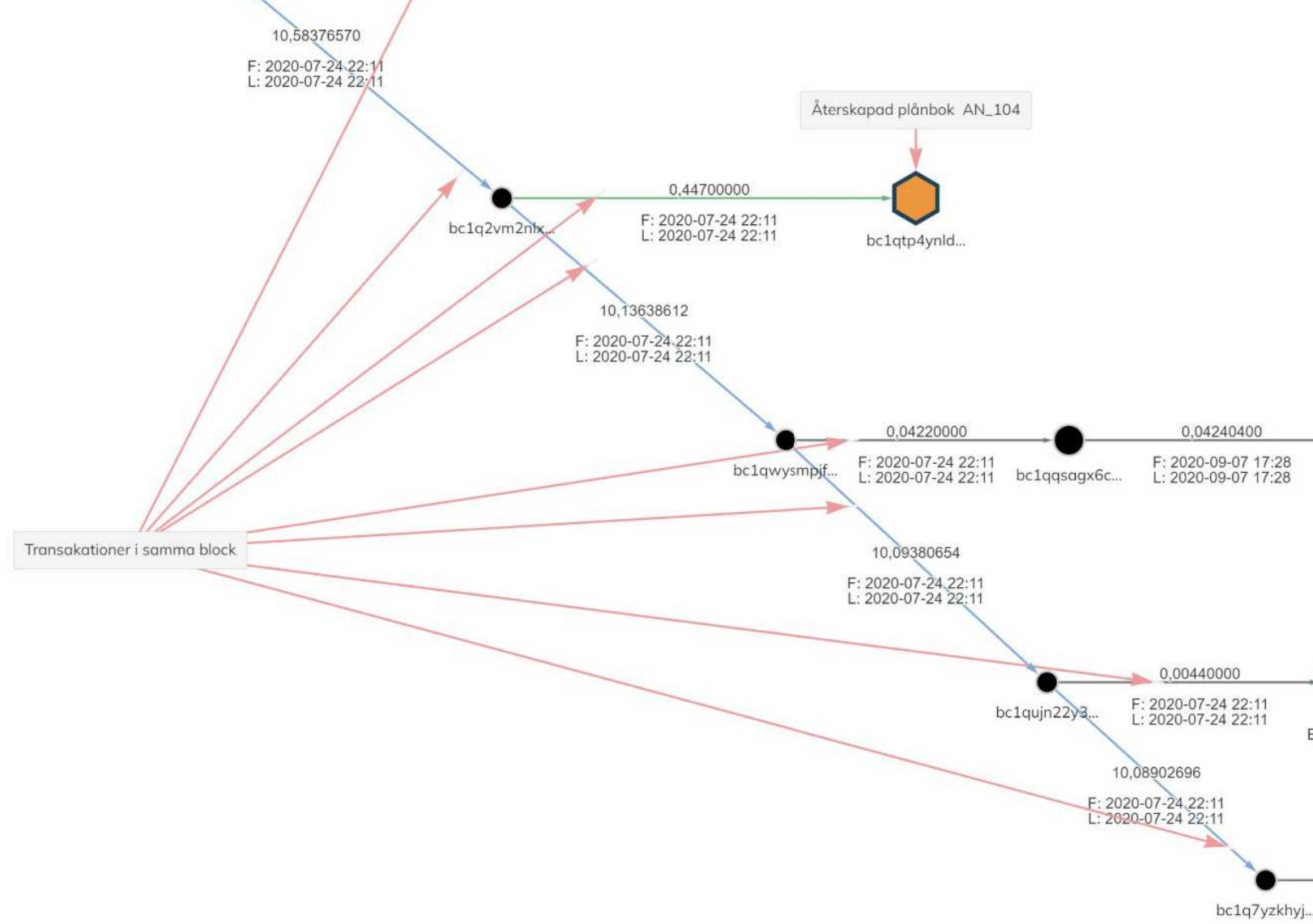
Transaktioner som liknar säkerhetsinbetalningar skickas vidare till plånbok
AN 091

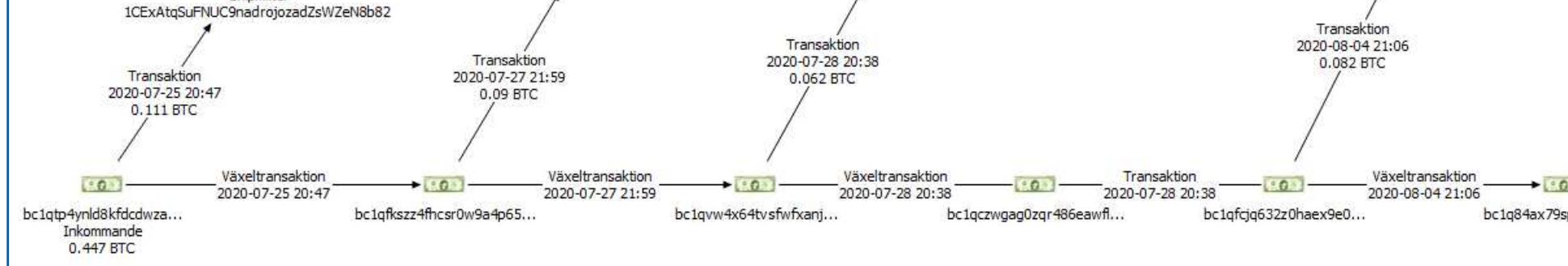


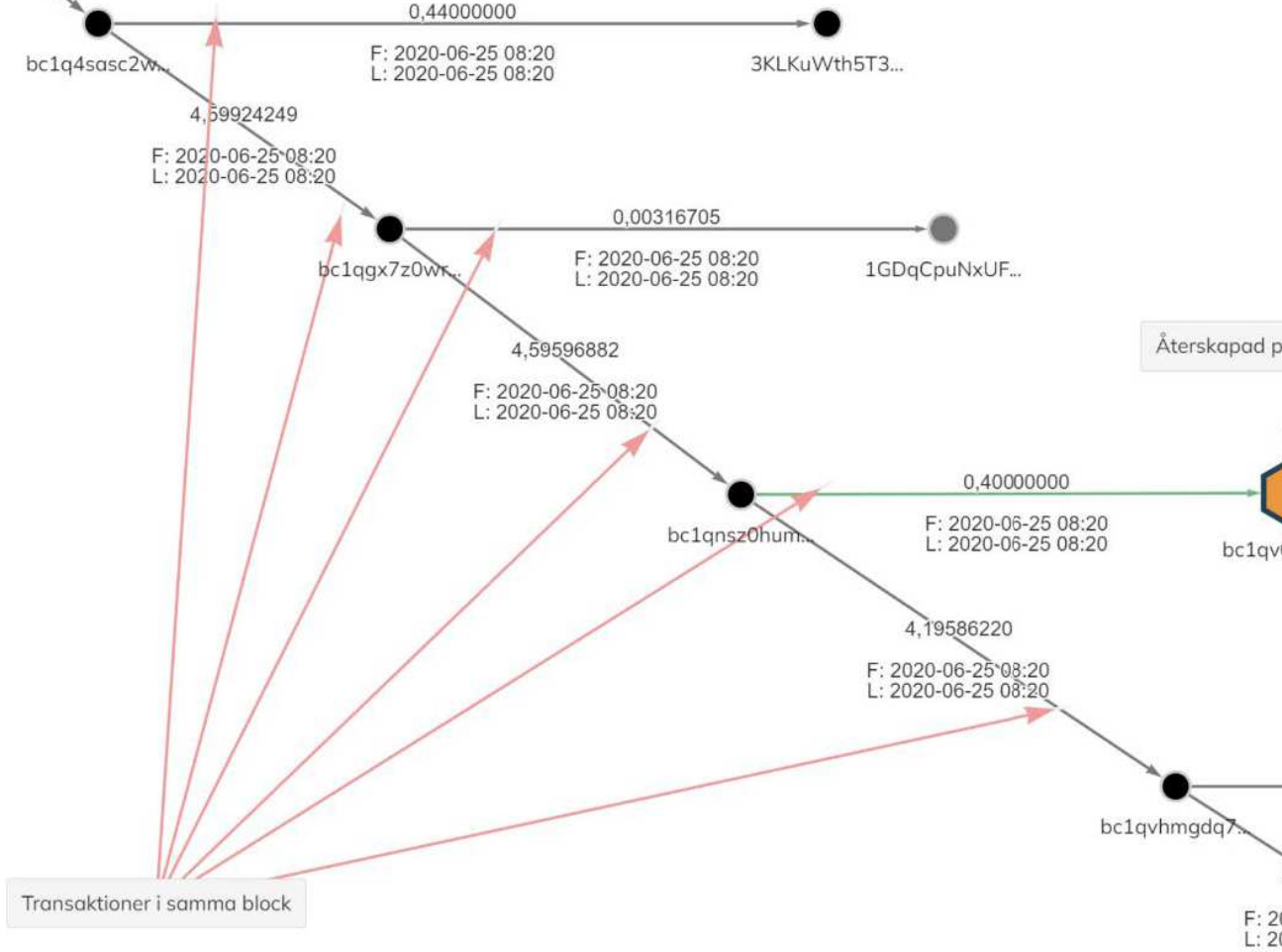


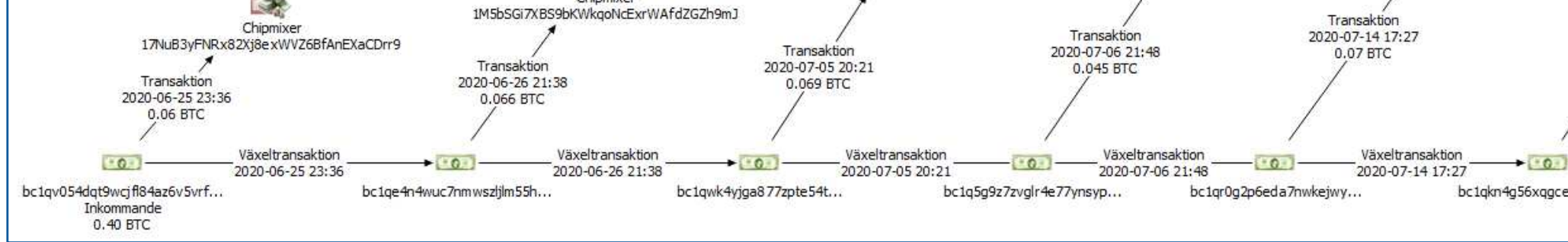












Bilaga 9: Adresser och transaktioner i återskapade plånböcker

Adresser i återskapad plånbok med löpnummer 91

bc1q7qrwnawm7vk92j6g5jw3a50s5eyw5w0qcfzkpl
bc1q9mr2wy5cy5md0ax0mc5xapl7n74e3fxw5a06ce
bc1qj48x230nkvcvjxwpnuxv8r584wc4z2kh2dyatj
bc1qc2hfw0rucvqfp63zezgr4htahjq7hclvceum
bc1qkn1q05vvrw3ep7qffdhr79n0eyzq3rwrvshwcs
bc1q4c2gz5zmghfyd5k96nzffztvyjmjn6hllnnpnmw
bc1qu9ux2hyzz9qjz2v0asz0h2k22jjz4ts9xuagw7

Analyserade transaktioner gjorda av plånbok med löpnummer 91

71480eba94b5cb5e7d9fc8d14f17eb17b5feb62c457580096e6a9c4903d6bea3
daf6fedf897d0ea5c35d21f926624b88f3205c30ce01c4ffc4b2869fbfad31db
6809b6bba5122386913fdbc468bfc8cba2dd9b0da1f8f207329f1997f8036e31
ec8592447c77e9ff07022a0ec69df336a363351704558f9544613da7352da081
9d2ce930e40fd194a003501e07598793ef17cd01a3213f805f7c7e6381cdcc9d
62a9d32b41a4e9c3524e11d50cbee4a1b789a3cde3649a16a7c747fc43e526f5

Adresser i återskapad plånbok med löpnummer 97

bc1q0agw90vhfgyvqxc78wf7cdvwl5f6hXu0uwza07
bc1q4txnw9k23xgd0497y8m0qeuzydsds9v84wfsar
bc1qf4qf80pw6s6p4x39dktw7adv2dndmszfkmv92c
bc1qjmezlewdk33qkzca095wd2mp2jt49sf5clqeps
bc1qm2mkuj33z20gaae2zc9v9n06gg893yd9cy0tzd
bc1qsqw9anc0n3cw4metlnxce5ym3e5jk592lh2ykv

Analyserade transaktioner gjorda av plånbok med löpnummer 97

8ad3ac795403a0adf2fe0f43c9efec1df3771b8648c59daf9043a369e52e1456
7989b5970cc34f1841683d0f141bf7fb9405ba15f5b568b9b277ad58be0c9780
c58bab4c49faa4b2ce399aeb6938d9938d13ee5be9e66ee155510cfdbd9edad9
3a1a269de0c4a9b2f99ecd788d292a33aacdcc40c6f32f4a1d68289f514f912b
26d4c84e89864cefd0d3a85548c1f38efe62596abaca5a05da8fee6a58f1474f

Adresser i återskapad plånbok med löpnummer 104

bc1q84ax79sprnszpq56yhlakj26jmm15fyke5zh7s
bc1qczwgag0zqr486eawflmk0nk8r6mcgrp3v4w4m2
bc1qfcjq632z0haex9e0qeq9w4qxy0eqkt07sttey9
bc1qfkszz4fhcsr0w9a4p65y3r8hzhcgwu99xkkrl5
bc1qtp4ynld8kfdcdwzav77tkxsxfry6g6zafr0ljk
bc1qv4x64tvsfwfxanjza5h3wutgn4flxqharreug
bc1qz93yjdpo0rde4d9swmter2fv72y70hn97mxz698

Polismyndigheten

2023-05-10

HEMLIG
19 (19)

Analyserade transaktioner gjorda av plånbok med löpnummer 104

4d869757d01326c58f966b2d106e20cafecfdfa6e3dc2116dce14fc6412460ad
26fab363c1fbd1df4bf7ba943ddf520b7bbce1f8d2d7641279db402064e4b6ca
866a3e189c0839a6413f4180da48fc9a003796d80c764174559580c51a7cb205
9f3a3fbf47d26c4ae589afd999eb925dd27f70c75889890c1a99e0fbd370a1d5
e72f42375f54fae5ec4d829d3e184f8972f4940f72dcf790738c9cd253d25178
b931b39d9fca0a5be470a0dc23d14126e6a8577853b9f4089a703dbdf983a65a

Adresser i återskapad plånbok med löpnummer 120

bc1qv054dqt9wcjfl84az6v5vrfy2hl40xdu2zd3wp
bc1qe4n4wuc7nmwszljlm55hj88qutqd2wvvj9pa97
bc1qwk4yjga877zpte54td9tlvzyy43pnhgcl0l7m7
bc1q5g9z7zvglr4e77ynsyppc7kf7ntmkcu8fz0w6v
bc1qr0g2p6eda7nwkejwya5gchcrn82nv49apqruc
bc1qkn4g56xqgcercal7t8csz2e7lwq7m3np4nac3j
bc1qyenudzmt8f82k4757ue6x0e4z9za4rwetc6nfe

Analyserade transaktioner gjorda av plånbok med löpnummer 120

f1fa22a3f5bd02767d0af1ed47948395cfd5c5d91a26c569228909e15b5b3789
ff8f08e580110c32de98c49c712274a9b0191fc11a2b9203b6226012c7035492
88fdab13a6be5b03058e3eb4bafd8f3ca89b7e3d2572235e207a0dac03fd5546
96f8cf74ee0c106028c64ea53255aac982c9d4643b1c0f7427d72d7921aabf5c
65490b7a0277963b6295d9416cd533603587aba09db112792983f8284f0c06fa
075b53f7796cbb8d04ea6c461d98d6b6758122111f2dd75c2ff9d0b3173a40a3



Polismyndigheten
NOA
Nationellt It-brottscentrum, It-forensik
106 75 STOCKHOLM

Datum
2023-05-05

Diarienummer
K615323-19
5800/49376-21

HEMLIG

Extraktionsprotokoll avseende beslag 2023-5000-BG3418-5

Inledande uppgifter

Undersökningen begärd av: Kammaråklagare Henrik Söderman

Anledning till undersökningen: Extrahering av information

Ansvarig it-forensiker: Viktor Näsman

Tid för undersökningen: Undersökningen påbörjades den 19 januari 2023

Beskrivning av material

Tillverkare och modell:	iPad Air 1.gen (A1475)
IMEI:	358532050098995
SIM-kort:	☒ Ja ☐ Nej
Operatör:	Comviq
ICCID:	89462048009063416169
Minneskort:	☐ Ja ☒ Nej
Övrig information:	-

Fotografier



Åtgärd

Enheten har extraherats på information. Informationen har bearbetats i it-forensisk programvara för att kunna analyseras av utredare. Analyserbart material har överlämnats till utredare.

Materialförteckning

Gods

Beslagsnummer	Beskrivning	Platsbeskrivning	Tillvarataget av
2023-5000-BG3418-5	iPad Air 1.gen (A1475)	I andra lådan uppi från i byrå, sovrum. Avstängd	Forensiker

Viktor Näsman
It-forensiker



PM

HEMLIG
1 (10)

Datum 2023-05-10

Infoklass Ej klassad

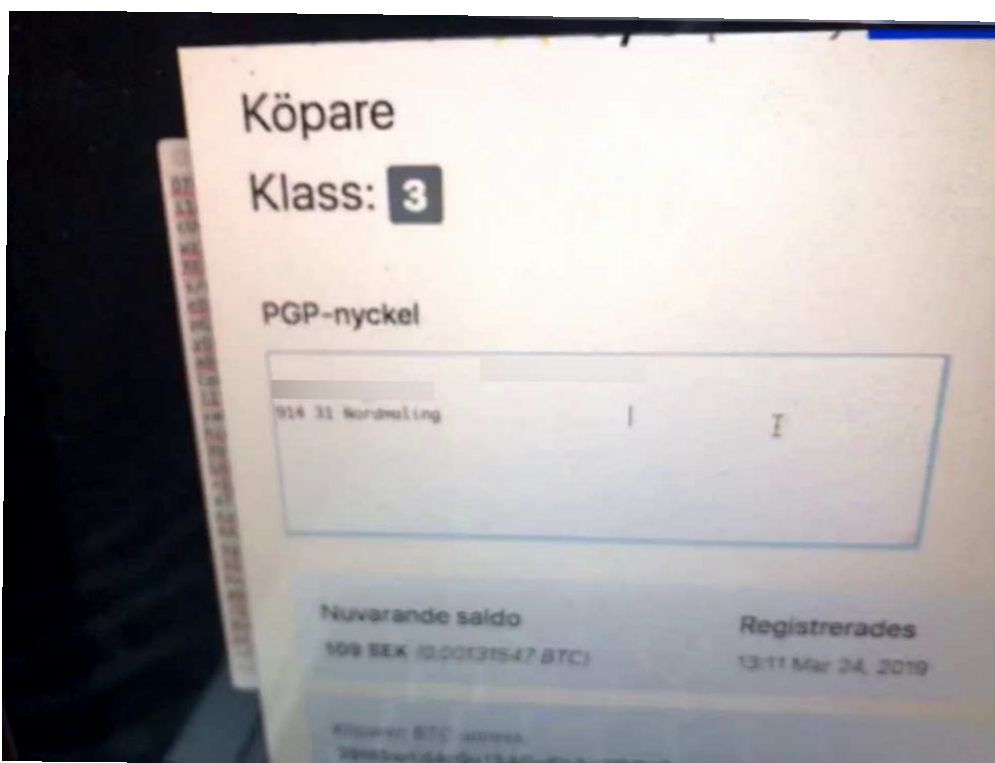
Diariennr (åberopas) 5000-K615323-19

Polismyndigheten
Nationella operativa avdelningen
Nationellt IT-Brottscentrum
Pär Landegren

Bildfynd i 2023-5000-BG3418-5

Bakgrund & syfte

I beslaget 2023-5000-BG3418-5, en ipad, så har en film hittats. Ur den denna film har en bildruta exporterats ut. Filmen har filnamnet *22296F86-EA5A-481B-BD9A-686CA7F1621A.medium.MOV* och är skapad 2020-01-06 14:51:39 (UTC+0). Filmen visar en skärm som i sin tur visar vad som kan vara Flugsvamp 3.0. Bilden innehåller ett namn och adress som är maskerat i denna bild.



Bildruta ur filmen 22296F86-EA5A-481B-BD9A-686CA7F1621A.medium.MOV

I utredningen har det via Noas Underättelseavdelning framkommit uppgifter om att en uppgiftslämnare har inkommit med information om en s.k admin-panel till marknadsplatsen Flugsvamp 3.0. Adminpanelen är ett gränssnitt för att sköta administrationen på marknadsplatsen och innehåller bla uppgifter

Polismyndigheten

2023-05-10

HEMLIG
2 (10)

Dnr 5000-K615323-19

Infoklass Ej klassad

om registrerade konton (både köpare och säljare), uttag av bitcoin och annat. Denna information har överlämnats till utredningen (se underättelsenotis Överföring av underrättelseinformation till utredning). Information från Adminpanelen har sparats ner vid 5 olika tillfällen 2019-01-22, 2019-01-24, 2019-01-28, 2019-01-30, 2019-02-14

Mellan perioden 2019-01-11 och 2021-10-28 har Flugsvamp 3.0 skrapats¹. Se PM ***Skrapningar av Flugsvamp 3.0 och Flugforum.***

Syftet med detta PM är att utreda om materialet på filmen kommer från den publika delen (dvs inloggad som köpare) av Flugsvamp 3.0 eller om det kan komma från någon form av admin- eller supportfunktion.

Sammanfattning och analys

I beslaget 2023-5000-BG3418-5, en ipad, har en film hittats som visar vad som bedöms INTE vara ”Min Profil”-sida för en vanlig köpare utan mer troligtvis någon sorts admin- eller kundtjänstfunktion för att administrera ett specifikt köparkonto.

Denna funktionalitet har inte varit öppen för vanliga köpare utan bara för admin eller av admin utsedd personal.

Resultat

När man är inloggad som köpare på Flugsvamp 3.0 finns det en sida som heter ’Min Profil’ som visar ens PGP-nyckel. Ingen skrapning finns att tillgå från det aktuella datumet (2020-01-06). Skrapningar från 2020-01-05 och 2020-01-07 finns dock att tillgå och nedan är skärmdumpar av dessa sidor.

¹ sparat ner en hel kopia av hemsidan

Polismyndigheten

2023-05-10

HEMLIG
3 (10)

Dnr 5000-K615323-19

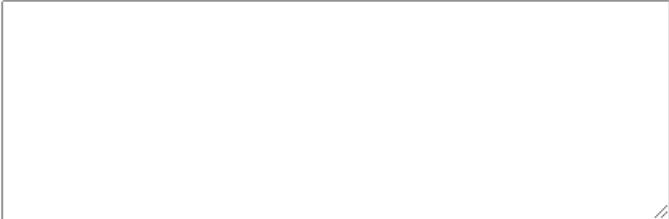
Infoklass Ej klassad

Min Profil

Stealth-mode är avstängt

Aktivera**konto1** *Inga omdömen*Klass: **1**

PGP-nyckel

Ändra

Dölj all historik

Dölj all historik fram tills nu. Det som döljs är dina insättningar, färdiga ordrar och avbrutna ordrar.

Dölj historik

[Klicka här](#) för att komma till sidan för affiliateinkomster. Programmet är på paus och går ej längre att använda för nya användare.

Skärmdump av 'Min Profil' från 2020-01-05

Polismyndigheten

2023-05-10

HEMLIG
4 (10)

Dnr 5000-K615323-19

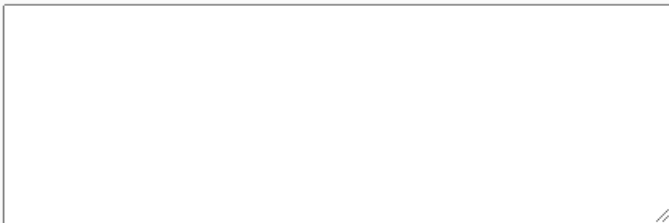
Infoklass Ej klassad

Min Profil

Stealth-mode är avstängt

Aktivera**isidor** *Inga omdömen*Klass: **1**

PGP-nyckel

Ändra

Dölj all historik

Dölj all historik fram tills nu. Det som döljs är dina insättningar, färdiga ordrar och avbrutna ordrar.

Dölj historik

[Klicka här](#) för att komma till sidan för affiliateinkomster. Programmet är på paus och går ej längre att använda för nya användare.

Skärmdump av 'Min Profil' från 2020-01-07

Som syns på bilder är det ingen skillnad i information som visas förutom att det är olika användarnamn som syns på bilderna då olika användarnamn har använts vid respektive skrapningstillfälle.

Polismyndigheten

2023-05-10

HEMLIG
5 (10)

Dnr 5000-K615323-19

Infoklass Ej klassad

Nedan visas en skärmdump från admin-panelen från administrationen av en användare. Värt att notera är att det här materialet från admin-panelen sparades ned i pdf-format vilket påverkar att textrutan ser lite annorlunda ut. Materialet skärmdumpen är tagen på är från 2019-02-14

PyrexTrill ★ 5/5 (1 st) Skicka meddelande

Köpare

Klass: 3

PGP-nyckel

Version: GnuPG v1

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBFwf19IBCADGPuuY5xvujNBm0jgD/S+Ty0swFK2Dgx4WdML0hdSoG08uyL1Y
MBD+JsDorqD7rbY4Zt/C183E4k8dDlp2opmBoMwZ4MKX1crwN5LSV2csQ09ZBbQ
k2Y1umg2+DFbxrvC0Rgj/7vY8qcKQIMp89mhLbxA81e/0rxqxL3rvCokDjfn5m1m
UCV8Goks8kNmZWg9tfpMykAZKt91TPV7FBbZaJaIOy0Le+a2Vre3wVrvCpy1nJM
xvJZYxq/0gDj3Wwet1PyHCL3a9p1bf7h2cUQsNwJfXln2/qY7hhT0Czbrm9K9056

Nuvarande saldo

18 SEK (0.00054649 BTC)

Registrerades

10:41 Dec 19, 2018

Senast inloggad

10:22 Feb 14, 2019

Orderhistorik

Aktiva beställningar

Produkt	Säljare	Kostnad	Orderdatum	Autosläpps	Orderstatus
<u>Ksalol 1mg</u> 10 st	<u>kavajman</u>	100 SEK (0.00301488 BTC)	Feb 13, 2019 14:27	Feb 21, 2019 12:37	Skickad 12:37 Feb 14, 2019
<u>Ksalol 1 mg i Blister! WOW PRIS!</u> 15 st	<u>Medicinmannen</u>	105 SEK (0.00311231 BTC)	Feb 13, 2019 07:36	Feb 20, 2019 08:39	Skickad 08:39 Feb 13, 2019
<u>Buprenorfin 8mg</u> 1 st	<u>plskan</u>	210 SEK (0.00627166 BTC)	Feb 12, 2019 17:23	Feb 19, 2019 22:34	Skickad 22:34 Feb 12, 2019

296.7 mm

Skärmdump av adminpanelen

Polismyndigheten

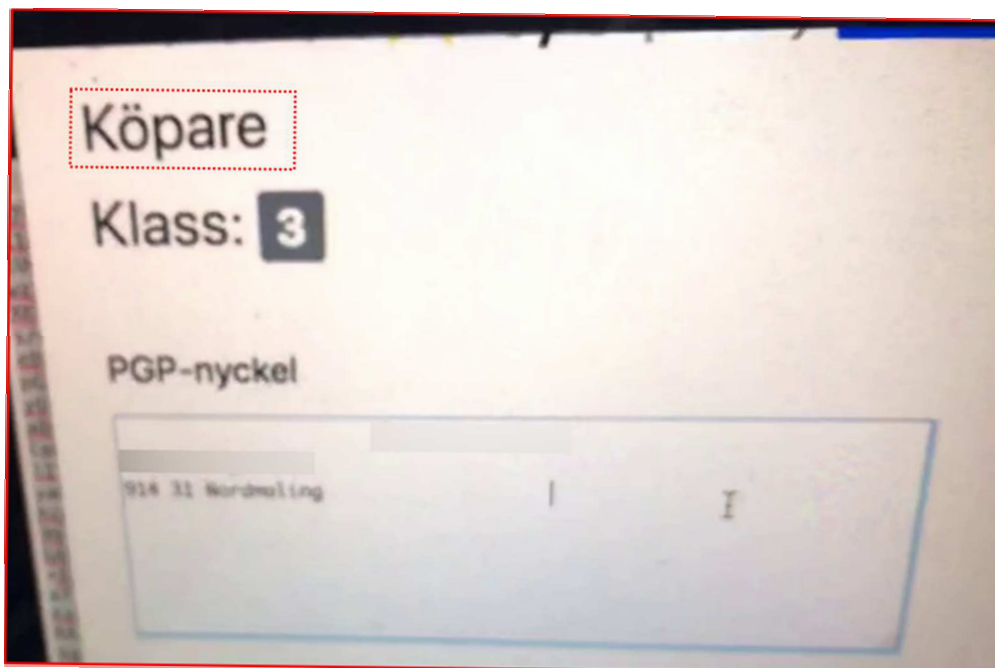
2023-05-10

HEMLIG
6 (10)

Dnr 5000-K615323-19

Infoklass Ej klassad

Jämför man överdelen i den hittade bilden och bilden från skrapningen ser man att det skiljer sig mellan bilderna. Direkt över Klass: så står det på det i skrapade materialet användarnamnet och i fyndet så står det istället Köpare (markerad med röd streckad linje) samt bredvid PGP-Nyckel finns det en grön knapp med texten Ändra(markerad med röd streckad linje).

*Urklipp från skrapning**Urklipp från fynd*

Polismyndigheten

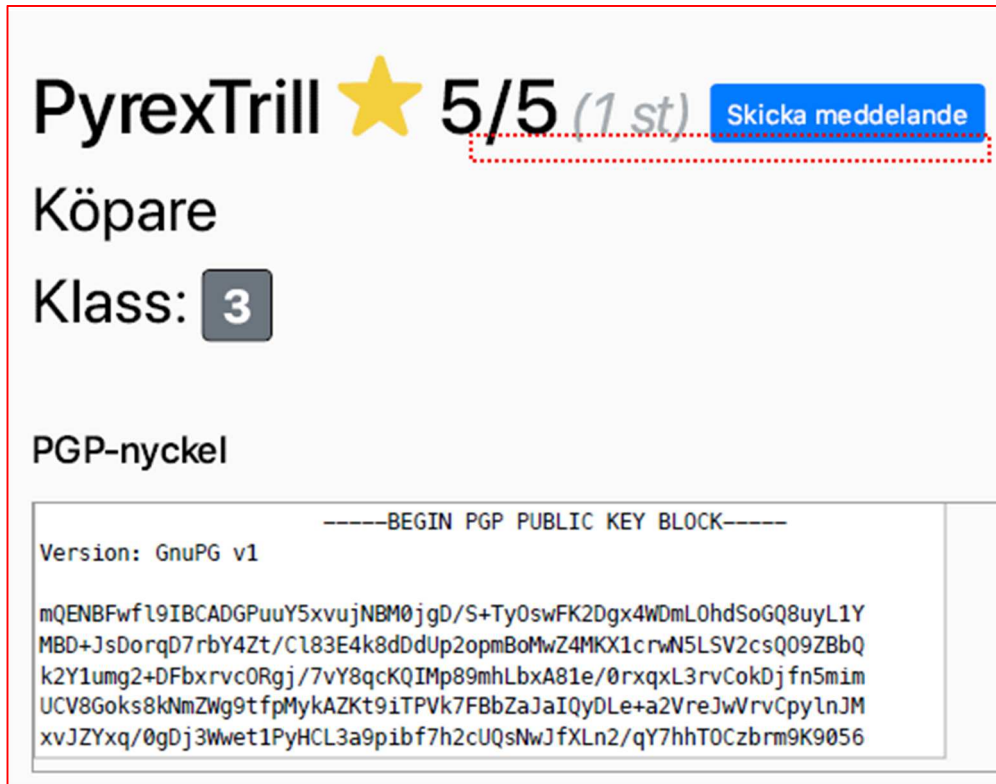
2023-05-10

HEMLIG

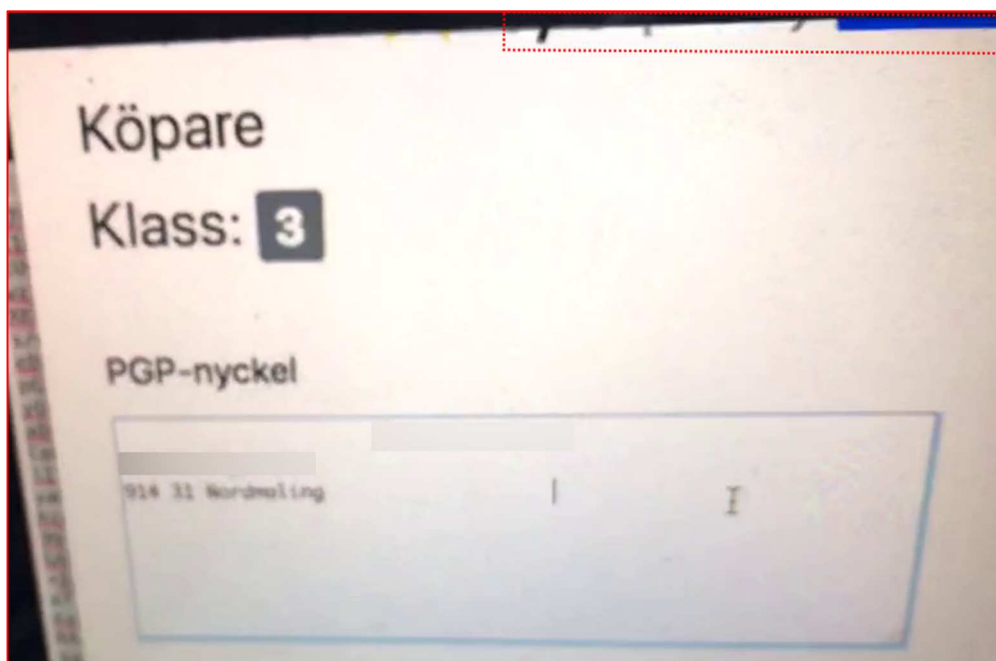
Dnr 5000-K615323-19

Infoklass Ej klassad

Jämför istället överdelen av bilden från adminpanelen med den hittade bilden så stämmer dom mer överens. Det finns ingen grön knapp med texten Ändra, ordet Köpare står direkt över klass. Det röda pickade markeringen i bilderna visar på att vad ses i den nedre bilden stämmer över ens med tecknet /, tecknen () samt den blå knappen skicka.



Urklipp från adminpanelen



Urklipp från fynd

Polismyndigheten

2023-05-10

HEMLIG
9 (10)

Dnr 5000-K615323-19

Infoklass Ej klassad

Jämför man istället sidan från adminpanelen så ser man att informationen om Nuvarande saldo samt registrerades finns med (markerade med röd streckad linje). I klippet från adminpanelen finns det också information om aktiva beställningar och i klippet från fyndet finns det information om vad som skulle kunna vara köparens BTC-adress. Denna skillnad skulle kunna bero på att klippet från adminpanelen är från 2019-02-14 och utveckling skulle kunna ha skett därifrån eller att man har skapat en liknande vy för en kundtjänstfunktion med annan information.

PGP-nyckel

Version: GnuPG v1

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFwf191BCADGPuuy5xvujNBm0jgD/S+TyOswFK2Dgx4WdMLohdSoG08uyL1Y
MBD+JsDorgD7rbY4Zt/C183E4k8ddUp2opmBoMwZ4MOK1cruN5LSV2csQ09ZBbQ
k2Y1umg2+0FbxrvC0Rgj/7vY8qcKQIMp89mhLbxA81e/0rxqxL3rvCokDjfn5eim
UCV8Goks8KnmZwg9tftMykAZKt91TPvk7FBbZaJaI0y0Le+a2VreJwVrvCpylnJM
xvJZYxq/0gdj3Wwet1PyHCL3a9p1bf7h2cUQsNwJfXln2/qY7hhT0Czbrm9K9056

Nuvarande saldo	Registrerades	Senast inloggad
18 SEK (0.00054649 BTC)	10:41 Dec 19, 2018	10:22 Feb 14, 2019

Orderhistorik

Aktiva beställningar

Produkt	Säljare	Kostnad	Orderdatum	Autosläpps	Orderstatus
Ksalol1mg	kavajman	100 SEK	Feb 13, 2019	Feb 21,	Skickad
10 st		(0.00301488 BTC)	14:27	2019 12:37	12:37 Feb 14, 2019

Urklipp från adminpanelen

PGP-nyckel

914 11 Nordmaling

I

Nuvarande saldo	Registrerades
109 SEK (0.00131547 BTC)	13:11 Mar 24, 2019

Urklipp från fynd

Polismyndigheten

2023-05-10

HEMLIG
10 (10)

Dnr 5000-K615323-19

Infoklass Ej klassad

Pär Landegren

Handläggare Teknisk Inhämtning



Polisen

PM1 (16) **HEMLIG**

Datum

2023-05-11

Diariennr (åberopas)

5000-K615323-19

Polismyndigheten
Utredningsenheten
Nationellt it-brottscentrum
Teknisk inhämtning
Anette Berglund

OP Hydra - Kryptospårning avseende återskapade plånböckerna AN_80, AN_18, AN_44 och AN_48 på höger sida om Chipmixer samt kopplingar till plånböckerna 190725, 190824 och 190924

Syfte

Syftet med detta PM är att beskriva de kryptofinansiella observationer och analyser som gjorts i ärendet gällande Adam Nironen(940119-7554) och hans kopplingar till moderator Hund avseende plånböckerna AN_80, AN_18, AN_44 och AN_48.

Nationella operativa avdelningen

2023-05-10

Innehåll

Syfte	1
Bakgrund.....	3
Underlag.....	3
Vad är Flugsvamp Market 3.0 (FS3)	4
Flugforum, lön, moderatorer och användare.....	4
Vad var Chipmixer.....	4
Om spårning av kryptovalutor	4
Om redovisade kryptospårningsgrafer	6
Dagskurs för att omvandla bitcoin (BTC) till SEK	7
Källor	7
Sammanfattning	8
Tillvägagångssätt	8
Analys av transaktioner.....	8
Användning av Chipmixer.....	10
Övergripande.....	10
Summerande beskrivning hur det går till.....	10
Återanvändning av samma för användaren unika Chipmixeradress.....	11
Resultat	12
Återskapade plånböcker AN_18, AN_80, AN_44, AN_48 tillhörande på höger sida om Chipmixer	12
Demixning av två insättningsadresser till Chipmixer	14

Bakgrund

En återställningsfras är en värdehandling vilken ger tillgång till värdet och för att kunna genomföra transaktioner i plånboken.

Analyserade plånböcker i detta PM är återskapade utav återställningsfraser från Adam Nironens ipad.¹ samt baserade på svar från kryptotjänsten BitPay.com

Då Chipmixer i stor utsträckning har använts för att dölja härkomsten har analys gjorts avseende demixing där det i detta PM är plånbok från Adam Nironens ipad med löpnummer 18 och 80 som är i fokus.

Demixingen är probabilistisk då kopplingen gjorts genom att matcha tid och summa in och ut ur Chipmixer, ej genom att följa transaktioner genom blockkedjan.

Löneplånböckerna 19-07-25, 19-08-24, 19-09-24 samt 19-11-24 finns analyserade i ”PM Krypto-spårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen”.

Plånböcker som tar emot jämn insättning på lönedatum benämns löneplånböcker annars är de benämnda med löpnummer knutet till återställningsfras.

I följande avsnitt presenteras utökad bakgrundsinformation då dokumentet innehåller detaljer som kräver viss insikt i bl.a. Flugsvamp 3, kryptovalutor och spårning av dessa samt den illegala mixer-tjänsten Chipmixer² som nu är nedtagen.

Underlag

Plånböcker kopplade till Adam Nironen som får en jämn insättning på lönedatum är bildligt placerade på vänster sida om Chipmixer och plånböcker som Adam Nironen använder för att ta emot krypto(chips) från Chipmixer, presenteras på höger sida om Chipmixer.

På vänster sida om Chipmixer är plånböcker kopplade till Adam Nironen som tar emot bitcoin från FS3/FS3 admin och skickar in till Chipmixer.

På höger sida om Chipmixer är kluster/plånböcker som tar emot krypto från Chipmixer, dvs efter mixning där vi genom svar från kryptotjänster identifierat kluster tillhörande Adam Nironen samt genom återskapade plånböcker från återställningsfraser från Adam Nironens ipad och mobil.

Detta gäller generellt förutom för den plånbok som tar emot en jämn insättning 2019-06-25(44)³ från plånbok tillhörande FS3 admin men som även kopplas till Adam Nironen genom svar från kryptotjänstleverantörer.

¹ Namngivningen på plånböcker är dels baserad på datum för inkommande jämn insättning på lönedatum dels beroende på löpnummer på återställningsfras.

² En kortare beskrivning av Chipmixer finns under rubriken ”Tillvägagångssätt”.

³ Denna löneplånbok 190625 har även återskapats med återställningsfraser från Adam Nironens ipad med löpnummer(44). Plånboken sätter även in till Chipmixer.

Vad är Flugsvamp Market 3.0 (FS3)⁴

FS3 var en svensk internetmarknadsplats för primärt narkotika som existerade mellan 2018.12.17 och 2021.10.30. Under marknadsplatsen livstid kunde användare skapa konton på sidan och använda dessa för att köpa eller sälja produkter på sidan. Marknadsplatsen användes via anonymiseringstjänsten TOR och all handel skedde med kryptovalutan bitcoin (BTC).

Flugforum, lön, moderatorer och användare⁵

På själva Flugsvamp Market 3.0 fanns ingen plattform för diskussion. Till detta ändamål fanns i stället internetforumet *Flugforum* där det också fanns ansvarig admin-roll och moderator-roller.

En moderators arbetsuppgift på en plattform är generellt att bistå med hanteringen av det dagliga arbetsflödet på plattformen.

För sin arbetsinsats erhöll sidans moderatorer lön från administratören (FS3 admin) av Flugsvamp Market 3.0⁶. Moderatorkontot "Hund" var en av de moderatorer som erhöll lön från administratören.

Vad var Chipmixer

Chipmixer var en av många mixertjänster som används för att dölja och anonymisera härkomsten av krypto.⁷

Då kryptovalutor är spårbara genom den öppna blockkedjan kan mottagare av kryptovaluta i vissa fall se var pengarna härstammar ifrån. Denna möjlighet nyttjas av t.ex. kryptoväxlingsföretag i syfte att detektera pengar som härstammar från marknadsplatser för handel med vapen/narkotika/barnövergreppsmaterial, it-brottsvinster eller andra icke önskvärda källor.

För att dölja den ursprungliga källan till sina kryptovalutor finns därför s.k. *mixertjänster*. Syftet med en mixertjänst är att försvåra *spårningen* av kryptovalutor genom att dölja den ursprungliga källan till pengarna från framtida mottagare.

Generellt fungerar de flesta mixertjänster genom att användare skickar in sina kryptovalutor i mixertjänsten varpå pengarna efter en tid skickas ut av tjänsten till en nyskapad adress/plånbok som användaren får tillgång till. Under processen har pengarna rörts ihop med andra användares kryptovalutor, vilket döljer den initiala källan till pengarna. Den nya källan till pengarna blir således mixertjänsten.

I detta PM är Chipmixer relevant då Chipmixer användes genomgående för att anonymisera och dölja varifrån kryptovaluta kommer ifrån.

Om spårning av kryptovalutor

Transaktioner med kryptovalutor fungerar genom en så kallad *blockkedja*. En blockkedja är en (oftast) publik databas på internet där samtliga transaktioner med en kryptovaluta registreras.

Kortfattat innebär det att samtliga bitcointransaktioner som någonsin ägt rum finns helt öppet publicerade på internet. Det som framgår om transaktionerna i blockkedjan är bl.a. vilka datum, adresser och belopp som förekommer i transaktionerna, dock inte vem de inblandade bitcoinadresserna *tillhör*.

⁴ Se PM Rapport Beskrivning Flugsvamp 3.0

⁵ Se avsnitt avseende Hund i huvudprotokollet under Roller och aktivitet på Flugforum och Marknadsplatsen

⁶ Information från den privata/dolda delen av Flugforum.

⁷ Mer info avseende Chipmixer finns under rubrik "Tillvägagångssätt".

Nationella operativa avdelningen

2023-05-10

För att kunna spåra transaktioner med kryptovalutor behöver man således komplettera transaktionsinformationen från de öppna blockkedjorna med *kunskap* om vem som äger respektive kryptoadresser. Det finns idag flera analysverktyg för kryptospårning som besitter stora mängder information om använda kryptoadresser och dess ägare, vilket gör det möjligt att visualisera samt genomföra spårningar av transaktioner.

Kryptospårningen som redovisas i detta PM baseras därmed på öppen information från blockkedjan kombinerat med kännedom om kryptoadresser från ett eller flera etablerade kryptospårningsverktyg. Spårningsverktyg har ägarkännedom om vissa (men inte alla) kryptoadresser, därför kan vissa transaktioner spåras till olika identifierbara entiteter såsom olika kryptotjänster, där växling från kryptovalutor till fiatvaluta eller andra kryptovalutor har ägt rum. Dessa tjänster kan i sin tur ha ytterligare information om sin kund som brukat tjänsten, i form av ytterligare transaktionsinformation eller annan data.

Avseende ägandet av specifika kryptoadresser i *privata kryptoplånböcker*, vilka lagras lokalt i telefoner/datorer hos användare, är dessa oftast okända för kryptospårnings-verktyg då privata kryptoplånböcker generellt är anonyma, såvida adresserna i dessa inte blivit kända för den utredande analytiker som vilket är fallet vid till exempel återställning av en kryptoplånbok.

När man pratar om kryptovaluta används ofta termer som kryptoadresser, plånböcker, privata och publika nycklar, återställningsfraser och kluster. Nedan återges en snabb förklaring till dessa termer:

- Kryptovalutor skickas till och från en eller flera adresser. Med en **kryptoadress** avses således en specifik kryptoadress som använts för att skicka eller ta emot kryptovaluta.
- Kryptoadresser kan vara långa och jobbiga att hantera manuellt. Därför hanteras betalningar och adresshantering ofta via **kryptoplånböcker**. En plånbok är oftast en programvara/telefonapp vars syfte är att agera lagringsplats för en eller flera kryptoadresser, samt möjliggöra betalningar med dessa adresser.
- En kryptoadress består i regel av två delar; en privat och en publik nyckel. Den **publika nyckeln** är själva kryptoadressen och kan lämnas ut till andra om man önskar ta emot betalningar till adressen i fråga.
- Den **privata nyckeln** används till att signera utbetalningar från den motsvarande publika nyckeln. Oftast hanterar plånböckerna detta åt användarna. Den privata nyckeln kan också betraktas som en värdehandling då man med hjälp av denna kan förbruka de pengar som finns på den tillhörande adressen.
- En kryptoplånbok kan skapa många kryptoadresser (och privata nycklar) åt användaren. Dessa kan lagras uteslutande i plånboken i fråga, som i sin tur kan lagras t.ex. i en dator eller mobiltelefon. Skulle enheten gå sönder så skulle pengarna också gå förlorade vilket inte vore säkert.

Därför erhåller användare ofta en s.k. **återställningsfras** till plånboken vid skapandet av plånboken. En sådan fras består oftast av 1-25 ord i en specifik ordning. Med hjälp av dessa ord kan åtkomsten till samtliga adresser i plånboken återskapas i en annan plånbok. Därför betraktas även återställningsfraser som värdehandlingar.

- **Ett kryptokluster** är en term som används vid visualisering av kryptospårning och avser två eller flera kryptoadresser som bedömts hanteras av samma kontrollerande entitet. Dessa bedömningar sker dels automatiskt av kryptospårningsverktyg och baseras då på öppen information från blockkedjan. Om en kryptobetalning görs från t.ex. fyra bitcoinadresser samtidigt, vilket är vanligt, kan man dra slutsatsen att adresserna kontrolleras av samma betalande entitet som styr över samtliga adresser privata nycklar. Adresserna kan då visualiseras som en (1) grafisk entitet istället för fyra separata adresser. *En plånbok består oftast av flertal kluster i verktyget som ännu inte automatiskt identifierats höra samman.*

Klustring kan också utföras manuellt av kryptoanalytikern. Manuell klustring skapas genom kryptoanalys – antingen mot bakgrund av vetskap om att två eller flera adresser hör ihop, eller mot kryptoanalytikerns bedömning om att två eller flera adresser hör ihop baserat på hur adresserna interagerat tekniskt på blockkedjan. För mer info se ”PM Spårning av kryptovaluta och kluster”.

Ovanstående har applicerats då information avseende adressernas ägande har funnits i Flugforum, genom hemlig dataavläsning, och i enheter kopplade till Adam Nironen där till exempel återställningsfraser påträffats⁸.

Om redovisade kryptospårningsgrafer

I detta PM presenteras utförd kryptoanalys som bilder/grafer från kryptospårningsverktyg. Dessa bilder visualiserar kryptoflöden som ägt rum mellan olika adresser och adresskluster. Bilderna av vissa spårningar kommer även med som bilagor för att kunna läsas i detalj. Nedan förklaras innehållet i dessa grafer:

- Graferna i detta PM ska generellt läsas från vänster till höger, med vissa undantag. Transaktionerna sker alltid i pilarnas riktningar. I grafer representeras kluster av bl.a. ringar som symboliserar t.ex. marknadsplatser, mixertjänster och växeltjänster för kryptovalutor. Då det är relevant med specifik adress har detta valts ut och presenterats med en hexagon.
- En pil mellan kluster representerar en eller flera transaktioner som gått i pilens riktning. Ovanpå pilarna kan olika datum redovisas, t.ex. ”F: <datum> L: <datum>”. F och L står i dessa fall för ”first” resp. ”last”, dvs. första och sista gången transaktioner har skett mellan adresserna i fråga.
- Transaktionspilarna kan ha olika färg i grafer; generellt gäller följande legend:
 - Gröna pilar representerar generellt löneutbetalningar
 - Blåa pilar representerar växel på transaktioner. Växel sker på grund av överskottet som tillhör betalande plånbok.
 - Röda pilar representerar transaktioner till/från Chipmixer
 - Lila pilar representerar transaktioner till/från FS3
 - Turkosa pilar är endast pilar med tillhörande kommentarer
- Vid en bitcointransaktion töms de betalande adresserna på saldo, den överblivna växeln kan åka tillbaka till den *betalande adressen*, eller till *en av plånboken nyskapad adress*. Detta

⁸ Gul lapp i Adam Nironens plånbok samt från beslagsnummer: 2023-5000-BG3418-1(mobil), 2023-5000-BG3418-5(ipad).

hanteras oftast automatiskt av kryptoplånboken. Detta kan leda till grafer där en och samma plånbok består av flera adresskluster i kryptoanalysprogrammet.

I de fall växeladresser tillhörande samma plånbok har detekterats har växeladresserna visualiserats med blå pilar i graferna. Det innebär att kluster som i bilderna är kopplade med blå pilar enligt växelanalys tillhör samma plånbok.

- Tider i graferna

Tiderna visade i graferna är i UTC vilket innebär:

CET – Svensk vintertid = UTC +1 timme

CEST – Svensk sommartid = UTC + 2 timmar

Tiden som är specificerad på respektive transaktionspil är när transaktionen konfirmerades. Detta sker ca var 10:e minut. I dokumentet har därför generellt skrivits ”i stort sett samtidigt” när transaktioner har samma tidsstämpel.

Dagskurs för att omvandla bitcoin (BTC) till SEK

Kurs som använts genomgående i detta PM är baserad på dagskursen för respektive transaktion. Då värdet på krypto är fluktuerande över dag och tid är detta ett ungefärligt värde. Kursen har inhämtats från kryptoväxlingsföretaget Coinbase.

För att få dagskursen så kan nedan URL användas, där man byter ut datumet till den dag man är intresserad av.

<https://api.coindesk.com/v1/bpi/historical/close.json?start=2021-10-29&end=2021-10-29¤cy=SEK>

Källor

I analysen har följande källor primärt givit underlag till information avseende tillhörighet av krypto-adresser och beteenden:

- Rapport Beskrivning Flugsvamp 3.0
- PM Återställning av plånböcker från beslag BG3418-5⁹
- PM Återställning av plånböcker från beslag BG3418-1¹⁰
- PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen
- Information från kryptoväxlare och kryptotjänster

⁹ PM gällande återställning av kryptoplånböcker från Adam Nironens ipad

¹⁰ PM gällande återställning av kryptoplånböcker från Adam Nironens mobil

Nationella operativa avdelningen

2023-05-10

Sammanfattning

De återskapade plånböckerna AN_18, AN_80, AN_44 och AN_48 är sammanlänkade och får sina bitcoin direkt eller indirekt från Chipmixer där AN_44 är identifierad till Adam Nironen genom svar från kryptoväxlare och AN_48 är kopplad till FS3 adress som nyttjas av Adam Nironen

AN_48 är genom insättningsadress till FS3 kopplad till löneplånbok 190725. Inga andra insättningar sker till denna FS3 adress.

Adam Nironen har genom tillgång till återställningsfraserna ägande till alla ovan nämnda plånböcker.

Genom probabilistisk demix kan man koppla de till moderator Hund tillhörande och bekräftade löneplånböckerna 190824 och 190924 till plånböckerna AN_80 och AN18.

Tillvägagångssätt

Analys har gjorts baserat på tillgänglig information i ärendet. Där kopplingar funnits till olika etablerade kryptotjänster har dessa kontaktats i syfte att erhålla ytterligare kundinformation.

När man får ägarkännedom om en (1) adress analyseras adressen i ett analysverktyg. I detta fall har växelanalys genomförts i stor utsträckning.

I detta PM har adresser analyserats baserat på återskapade plånböcker från återställningsfraser från Adam Nironens ipad och mobil¹¹.

För att kunna överföra ett värde från en kryptoadress måste användaren ha tillgång till den privata nyckeln som tillhör adressen. Den privata nyckeln genereras när adressen skapas.

Detta innebär att en utgående transaktion från en plånbok kan **endast** göras om man har tillgång till de privata nycklarna för adressen i plånboken.

En plånboks samtliga kryptoadresser kan återskapas med en återställningsfras som består av ett antal ord i en viss ordning. Detta kan jämföras med ett kassaskåp vilken endast kan öppnas och hanteras av den som har nyckeln dvs återställningsfrasen. I ärendet har flera sådana återställningsfraser beslagtagits vilka använts för att återskapa frasernas tillhörande kryptoplånböcker med tillhörande adresser. När man återskapar en kryptoplånbok får man tillgång till all historik samt kontroll över de kryptovalutor som finns i plånboken. Separata PM finns skrivna om dessa¹².

Analys av transaktioner

Generellt kan sägas att det finns väldigt många mixertjänster, växeltjänster och betaltjänster tillgängliga för att hantera kryptovaluta. Analys har därför gjorts för att se mönster i vilka tjänster som använts av löneplånböckerna vid mottagande av lön samt vad Adam Nironen använt, där Chipmixer, BitRefill, BitPay, Crypto.com, ChangeNow, CoinGate samt insättningsadresser på FS3 köpkonto varit viktiga. Utöver det har även en oidentifierad tjänst¹³ använts av både moderator Hund och Adam Nironen.

¹¹ Se under rubrik: "Källor"

¹² Se under rubrik: Källor

¹³ 3NxTrm9XgYY6Tk~

Nationella operativa avdelningen

2023-05-10

När man överför värden från en bitcoinadress till annan så skapas en växel med överskottet som aningen skickas till en ny adress eller så sätts växeln tillbaka till den adressen som skickade.

I de fall det skapas en ny växeladress med överskottet på betalningen, tillhör även den till samma plånbok/ägare som skickade transaktionen.

Bitcoinadresser som bedömts tillhöra samma plånbok genom växelanalys är i alla grafer sammanlänkade med blå transaktions pilar dvs vilka representerar växeln. Flera av dessa plånböcker har sedermera kunnat verifieras genom återskapade plånböcker med återställningsfraser från hemlig dataavläsning, gul lapp i Adam Nironens plånbok samt från Adam Nironens ipad. I detta PM har endast plånböcker analysretas.

I nedanstående exempel kan man baserat på växelanalys, följ blåa pilar, bedöma att adresserna bc1q4xyrzs~, bc1qylv2ke3~och bc1q3zffsqk~ tillhör samma plånbok.

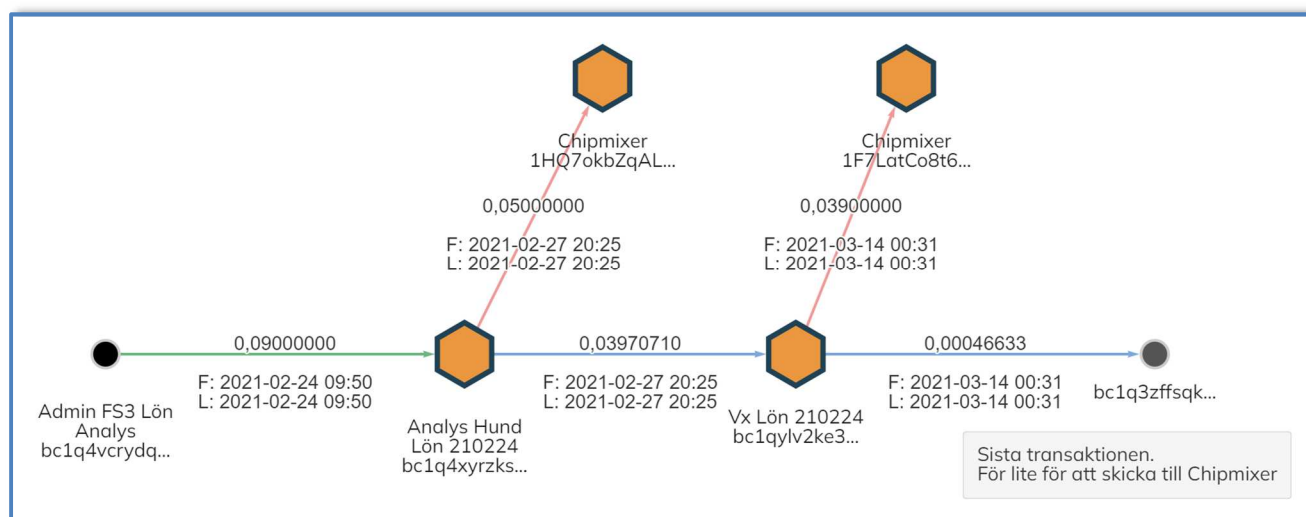


Bild 1 Exempel på tydliggörande av växelanalys baserat på transaktioner på blockkedjan

Användning av Chipmixer

Övergripande

I denna utredning gällande Adam Nironen och moderator Hund har mixertjänsten *Chipmixer* påträffats frekvent.

I och med det har det även lagts fokus på att probabilistiskt identifiera dessa transaktioner genom Chipmixer. Probabilistiskt innebär att man endast kan göra en bedömning om att transaktioner genom Chipmixer hör ihop genom att matcha med summa och tid som ingångsvärden så länge man inte har tillgång till underlag från Chipmixer. Man kan alltså inte följa transaktionen genom blockkedjan.

Chipmixeradressen och sessionsid(sessiontoken) genereras då man startar en mixing session mot Chipmixer. Dessa är unika för dig och är sammankopplade. Det sessionsid man får är en värdehandling vilken används för att få tillgång till de för dig nya bitcoins av motsvarande värde som du satt in. Leverans från Chipmixer dvs. de privata nycklarna till de nya bitcoinadresserna, totalt med samma värde som insättningen, kommer i specifika valörer, så kallade chips¹⁴. Dessa är förgenererade och minimivärdet på ett chips är 0,001 BTC.

Sessionen är aktiv i sju dagar, därefter har du inte längre access till informationen till de privata nycklarna eller kan sätta in BTC till Chipmixeradressen och få något tillbaka.

När mixningen är klar efter ca 15-30 min så använder du ditt unika och tillfälliga sessionsid som kan användas i sju dagar, för att få access till de privata nycklarna till chipsen.

Summerande beskrivning hur det går till

Nedan följer en summerande beskrivning om hur ”mixingen” går till hos Chipmixer:

- Användaren går in på darknet på Chipmixers hemsida och påbörjar en mixing.
- När man påbörjar en ”mixning” erhåller användaren en egen unik sessions-ID på Chipmixers websida, vilket kan jämföras med ett mycket långt lösenord. Man blir informerad att spara denna textsträng för att kunna använda den i kommande skede. **Utan sin egna temporära unika session-ID får man inte tillgång till de mixade pengarna och förlorar sina insatta pengar.** Denna sessions-ID är ingen cookie utan sparas genom att markera den på websidan och spara den.
- Användaren sparar sin sessions-ID. Då dessa Ids är långa är det sannolikt att de sparas på den enhet där man får dem. Exempel på en sessions-ID:
ha5YqpyLZwhXBTm7dCGUu5PZsMLmM9Jm
- Användaren erhåller en egen unik insättningsadress till Chipmixer som är en bitcoinadress och som fungerar som användarens tillfälliga ”kontonummer” hos tjänsten. Denna egna, unika och tillfälliga bitcoinadressen som skapas av Chipmixer för insättning av pengar är aktiv under 7 dagar.
Detta innebär att man har sju dagar på sig att hämta resultatet efter insättning och mixing. Normalt använder man sessionen och adressen för en (1) insättning till Chipmixer, vilket är vad som står på Chipmixers hemsida.

¹⁴ Av Chipmixer förskapade bitcoin med fasta värden varav det lägsta är 0,001 BTC

Nationella operativa avdelningen

2023-05-10

- Användaren går därefter in i sin kryptoplånbok och skickar vald jämn summa bitcoin över 0.001BTC från plånboken till sin unika tillfälliga bitcoin-adress på Chipmixer.
- Chipmixer har ett förråd av s.k. ”chips”; tidigare skapade och sparade kryptoadresser med saldo. Dessa kommer i fasta jämna valörer varav den minsta är 0.001 BTC. Från detta förråd matchas värdet av det man satt in och användaren får tillgång till de privata nycklarna till dessa nya bitcoin-adresser.
- Användaren går in på Chipmixers websida och lägger in sitt sessions-ID för att se om mixningen är klar. Detta kan ta ca 15-30 min eller mer.
- När användaren fått tillgång till de nya privata nycklarna från Chipmixer kan pengarna från dessa adresser flyttas vidare. Detta bör ske skyndsamt då även Chipmixer har tillgång till de privata nycklarna i fråga.

Den som mixar sina bitcoins genom Chipmixer får således en egen, unik och tillfällig insättningsadress till Chipmixer när mixningen inleds.

Återanvändning av samma för användaren unika Chipmixeradress

Denna metod med att återanvända adress och sessions-ID inom 7 dagar är något som det inte informeras om på Chipmixers hemsida, utan är helt odokumenterad.

Det har testats för att se att och hur det fungerar.

Moderator Hunds och Adam Nironens gemensamma återanvändning av unik Chipmixer insättningsadress har därför kunnat användas för att knyta ihop ägande av kluster till Piraten, Hund och Adam Nironen.

Återanvändning av insättningsadress fungerar enligt följande. Så länge sessionen är aktiv, vilket är 7 dagar, kan man sätta in ytterligare bitcoin till samma unika Chipmixer adress och återfå resultatet (dvs. mixade bitcoins med motsvarande värde) genom att återanvända samma sessions-ID. **Utan sessions-ID får man inte tillgång till det mixade resultatet och förlorar det som är insatt.**

Återanvändning innebär att man bara behövt gå in i sin egen plånbok, återanvända den unika insättningsadressen från förra insättningen och därefter hämta det mixade resultatet med sitt redan tillgängliga tillfälliga och unika sessions-ID.

Nationella operativa avdelningen

2023-05-10

Resultat

Återskapade plånböcker AN_18, AN_80, AN_44, AN_48 tillhörande på höger sida om Chipmixer

Bägge återskapade plånböckerna AN_80 och AN_18 får sina respektive första transaktioner från Chipmixer¹⁵.

Plånbok AN_18 töms till plånbok AN_80.

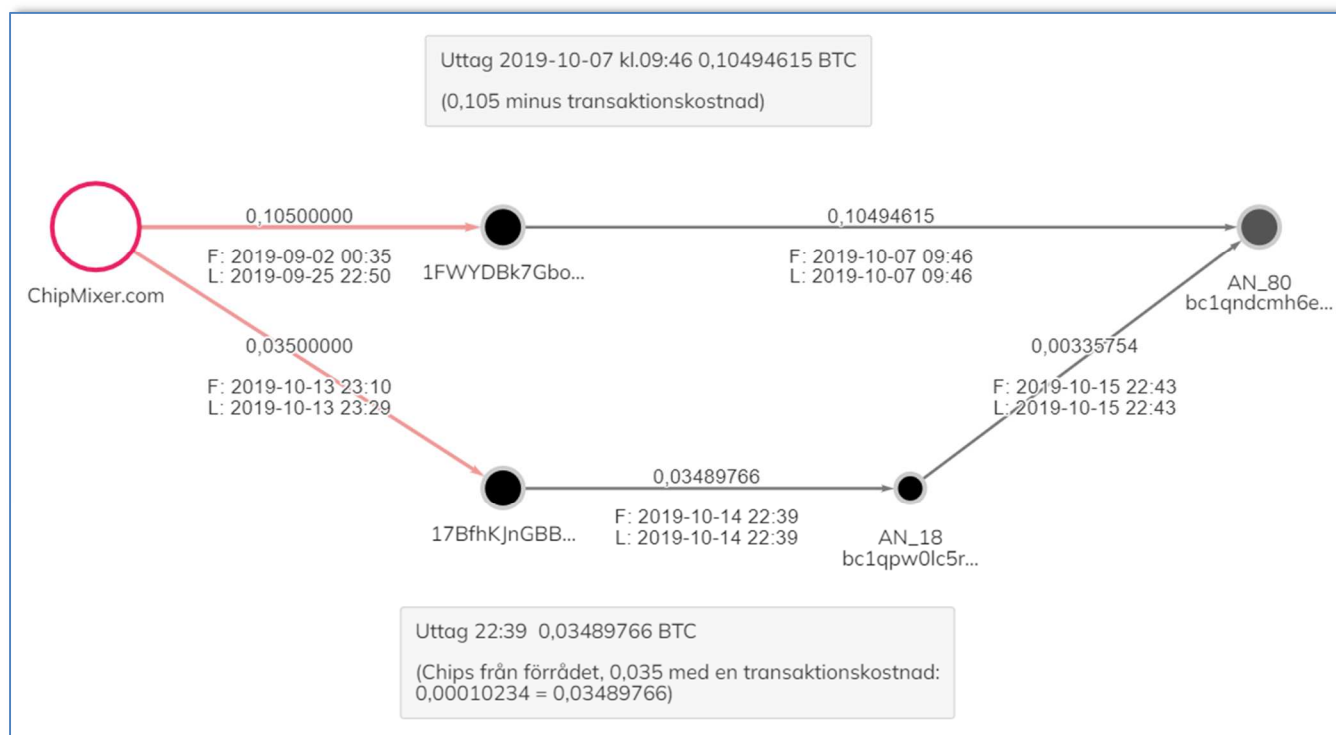


Bild:

AN_80 töms till plånbok AN_44 identifierad till Adam Nironen.
AN_44(Adam Nironen) skickar bitcoin till plånbok AN_48.

Plånbok AN_48 sätter in på FS3 köpkonto med adress 38bf6UWS5Z5X7vxN-tWRN4iHBkj9HhW28WG till vilken även löneplånboken 190725, bedömt tillhörande Adam Nironen, sätter in. Inga andra insättningar sker till denna FS3 adress.

Plånbok AN_48 sätter även in till FS3 insättningsadress 34eo9PB4gm9tbzovo7WZFQuEiGw1Bm5cd6 knuten till Adam Nironen..

Nedan bild visar i sin helhet hur AN_80, AN_18, AN_44 och AN_48 hänger ihop med Adam Nironen knuten till både AN_44 och samt till FS3 adressen 34eo9PB4gm9tbzovo7WZFQuEiGw1Bm5cd6.

Adam Nironen har genom tillgång till återställningsfraserna ägande till alla nämnda plånböcker

¹⁵ Se underlag för demixing i PM

Nationella operativa avdelningen

2023-05-10

Den används okända tjänsten 3NxTrm9X~ nyttjas

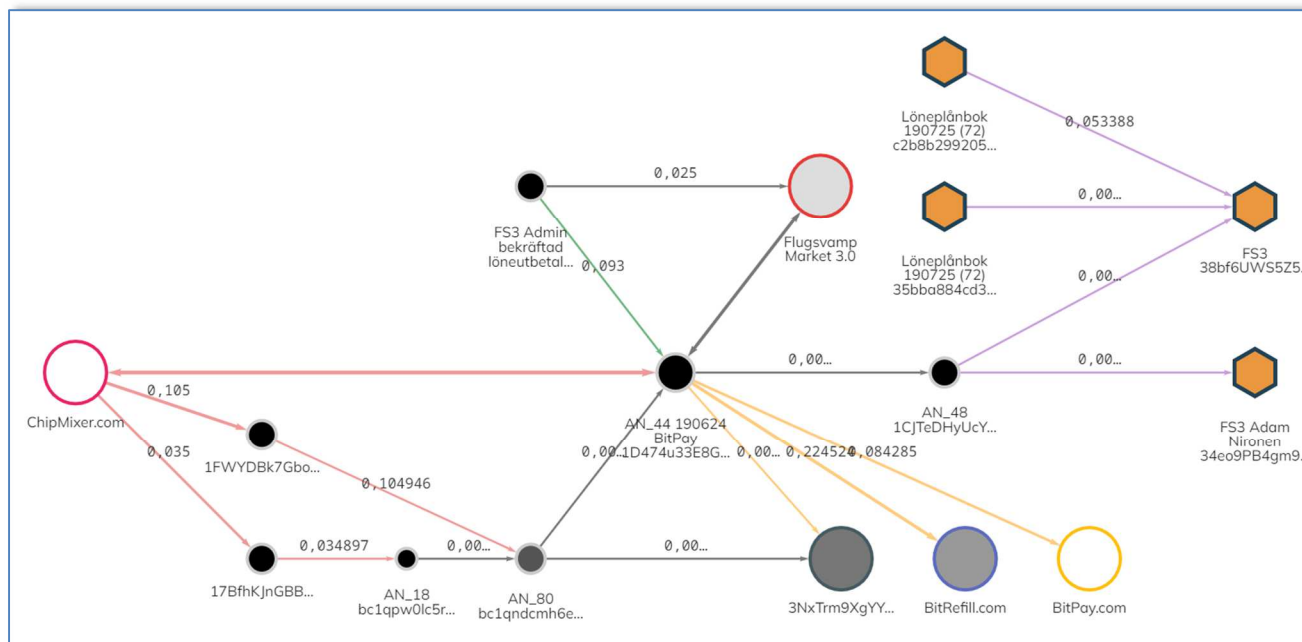


Bild: Transaktioner mellan återskapade plånböcker samt insättning till FS3 från löneplånbok 190725

Nationella operativa avdelningen

2023-05-10

Demixning av två insättningsadresser till Chipmixer**Blå ruta 1 och 2**

Från de **återskapade löneplånböckerna 190824(93) samt 190924(86)** varav bägge är bekräftade att tillhöra moderator Hund görs tre insättningar till den för användaren unika och och tillfälliga Chipmixeradressen 17K3HxvHogqGSHU4kRo7L9XJMVSt5fawTJ.

2019-10-07 09:03 med 0,04 BTC
2019-10-07 09:21 med 0,04 BTC
2019-10-07 09:33 med 0,025 BTC
Summa: 0,105 BTC

Bägge löneplånböckerna är återskapade med återställningsfraser från Adam Nironens ipad.

Blå ruta 3 och 4

Möjlig leverans från Chipmixer i bilden, är chips till ett värde av 0,105 BTC när de hämtas från Chipmixer

2019-10-07 09:46 hämtas chips till ett värde av 0,105 BTC till plånboken AN_80, återskapad med återställningsfras med löpnummer 80 från Adam Nironens ipad.

Grön ruta 1 och 2

Från den **återskapade löneplånboken 190924(86)** vilken är bekräftad att tillhöra moderator Hund görs en insättning till den för användaren unika och tillfälliga Chipmixeradressen 14yARaK4e39zB6d9oXsXVZPiZfAfh2WuQs

2019-10-14 22:06 med 0,035 BTC

Grön ruta 3 och 4

Möjlig leverans från Chipmixer i bilden, är chips till ett värde av 0,035 BTC när de hämtas från Chipmixer

2019-10-14 22:39 hämtas chips till ett värde av 0,035 BTC till plånboken AN_18 återskapad med återställningsfras med löpnummer 18 från Adam Nironens ipad.

Nationella operativa avdelningen

2023-05-10

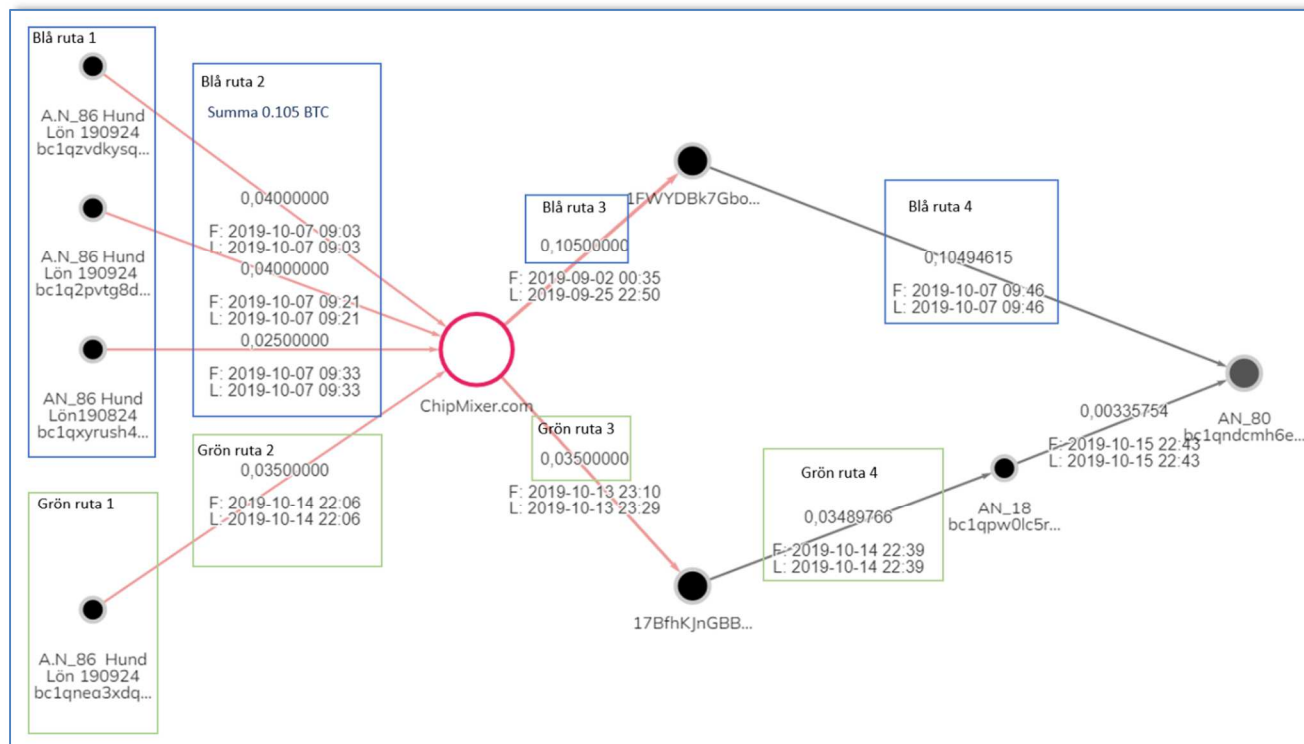
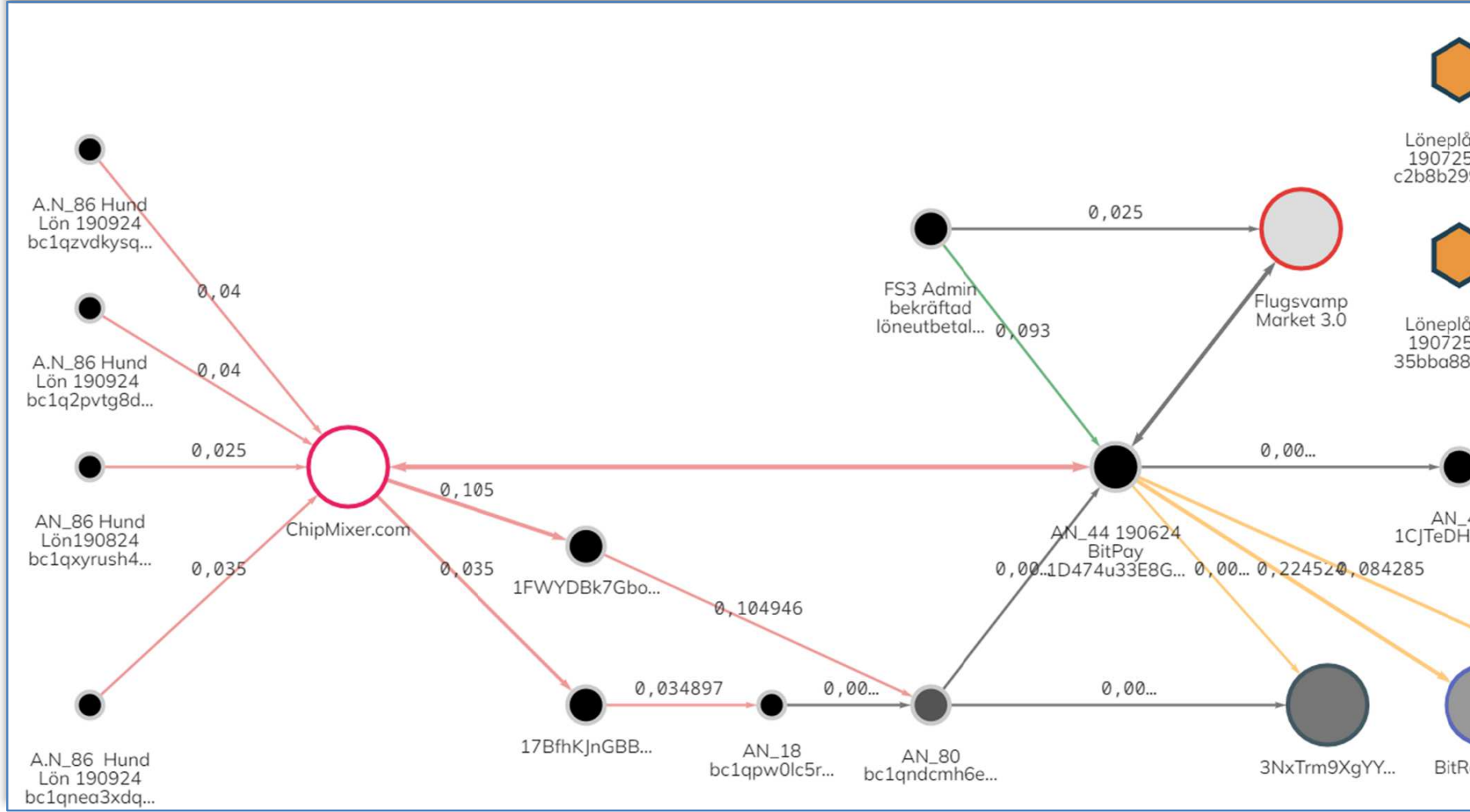


Bild: Demixning genom Chipmixer

Den möjliga demixing utgår ifrån de till moderator Hund bekräftade löneplånböckerna 190824 samt 190924 och vilket är ett ytterligare underlag gällande Adam Nironen som moderator Hund.

Nationella operativa avdelningen

2023-05-10





Polisen

PM

1 (27) **HEMLIG**

Datum

2023-05-07

Diariernr (åberopas)

5000-K615323-19

Polismyndigheten
Utredningsenheten
Nationellt it-brottscentrum
Teknisk inhämtning
Anette Berglund

PM OP Hydra - Kryptospårning löneutbetalningar 20-01-23, 20-02-24, 20-03-23, 20-04-24, 20-09-25 gällande moderator Hund på FS3.

Syfte

Syftet med detta PM är att beskriva de kryptofinansiella observationer och analyser som gjorts i ärendet gällande Adam Nironen(Adam) och hans kopplingar till moderator-kontot Hund, FS3 och FS3 admin gällande de ytterligare löneplånböcker med löpnummer 65, 89, 20, 69, 29 som identifierats med hjälp av återställningsfraser från beslag av Adam Nironens ipad.

Innehåll

Syfte	1
Bakgrund.....	3
Säkerhetsinbetalningar - depositioner.....	3
Källor	3
Sammanfattning	3
Tillvägagångssätt	5
Resultat	6
Säkerhetsinbetalningar - depositioner.....	6
Likartad hantering av inkomst	6
Löneplånbok 20-01-23, Koppling moderator Hund och Adam Nironen(65)	7
Summering.....	7
Grafisk presentation av utbetalningen till plånboken baserat på blockkedjan.....	7
Grafisk presentation av alla transaktioner i plånboken baserat på blockkedjan	8
Löneplånbok 20-02-24 Koppling moderator Hund och Adam Nironen(89).....	10
Summering.....	10
Grafisk presentation av utbetalningen till plånboken baserat på blockkedjan.....	10
Grafisk presentation av alla transaktioner i plånboken baserat på blockkedjan	11
Löneplånbok 20-03-23 Koppling moderator Hund och Adam Nironen(20)	13

Nationella operativa avdelningen

2023-05-11

Summering.....	13
Grafisk presentation av utbetalningen till plånboken baserat på blockkedjan.....	13
Grafisk presentation av alla transaktioner i plånboken baserat på blockkedjan	14
Grafisk presentationer av lönen i sitt sammanhang baserat på blockkedjan	16
Löneplånbok 20-04-24 Koppling moderator Hund och Adam Nironen(69)	18
Summering.....	18
Grafisk presentation av utbetalningen till plånboken baserat på blockkedjan.....	18
Grafisk presentation av alla transaktioner i plånboken baserat på blockkedjan	18
Grafisk presentation av utbetalningen i ett sammanhang baserat på blockkedjan.....	21
Löneplånbok 20-09-25 Koppling moderator Hund och Adam Nironen(29)	22
Summering.....	22
Grafisk presentation av utbetalningen till plånboken baserat på blockkedjan.....	22
Grafisk presentation av alla transaktioner i plånboken baserat på blockkedjan	23
Grafisk presentation av utbetalningen i ett sammanhang baserat på blockkedjan.....	25

Bakgrund

En återställningsfras är en värdehandling vilken ger tillgång till värdet och för att kunna genomföra transaktioner i plånboken.

Analyserade plånböcker är återskapade utav återställningsfraser från Adam Nironens ipad.¹

I detta PM finns en detaljerad analys per löneplånbok för:

- 2020-01-23 löpnummer 65
- 2020-02-24 löpnummer 89
- 2020-03-23 löpnummer 20
- 2020-04-24 löpnummer 69
- 2020-09-25 löpnummer 29

Dessa plånböcker finns även med i övergripande resultat samt i sammanfattningen i ”PM Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen”.

Plånböcker som tar emot jämn insättning på lönedatum benämns löneplånböcker.

Säkerhetsinbetalningar - depositioner

För att skapa ett säljarkonto på FS3 krävs en säkerhetsinbetalning.

Från Flugforumdumpen finns information avseende säkerhetsbetalningar². Initialt var kostnaden 3000 SEK vilket sedan höjdes till 5000 SEK och sedan vidare till 7500 SEK.

Säkerhetsinbetalningar skedde till bitcoinadresser som börjar med 1 sk. 1-adresser.

Källor

- PM OP Hydra - Kryptospårning löneutbetalningar
- PM Säkerhetsinbetalningar från säljare till admin Flugsvamp 3.0
- PM OP Hydra - Analys av Bitcoinflöde till och från marknadsplatsen Flugsvamp 3.0
- PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen.

Sammanfattning³

Det skapas en ny plånbok för mottagande av varje utbetalning vilket stämmer överens med alla andra plånböcker utom den första löneplånboken 190625 vilken även tar emot en ojämn summa direkt från FS3⁴.

¹ Namngivningen på plånböcker är baserad på datum för inkommande jämn insättning på lönedatum

² PM Säkerhetsinbetalningar från säljare till admin Flugsvamp 3.0 samt OP Hydra - Analys av Bitcoinflöde till och från marknadsplatsen Flugsvamp 3.0

³ Se PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen.

Nationella operativa avdelningen

2023-05-11

Alla återskapade plånböcker mottager en jämn insättning på lönedatum som första transaktion vilka stämmer överens i tid och storlek i SEK med övriga löneutbetalningar från FS3 admin till moderator Hund.

Löneplånbok 200323, 200424 är kopplade till FS3 genom möjliga säkerhetsinbetalningar.

Löneplånboken 200925 är kopplad till FS3 och FS3 admin då den utbetalningsplånboken mottager säkerhetsinbetalningar.

Löneplånbok 200224 återanvänder Chipmixer-adress vilket är en odokumenterad metod som identifierats i samband med moderator Hund och plånböcker kopplade till Adam Nironen.

Samtliga analyserade plånböcker hanterar inkommande jämn insättning på lönedatum på likartat sätt såsom moderator Hund hanterar det och såsom återskapade löneplånböcker kopplade till Adam Nironen hanterar det:

- En plånbok per mottagen jämn insättning på lönedatum
- Genom separata transaktioner skicka värden genom Chipmixer och i vissa fall insättningar till FS3
- Lämnar det i plånboken som understiger minimum-belopp för att skickas genom Chipmixer.

Nationella operativa avdelningen

2023-05-11

Tillvägagångssätt

Plånböckerna har återskapats och analyserats baserat på:

- varifrån krypto till plånboken kommer ifrån
- när och hur mycket som emottagits
- hur plånboken hanterats

Då information avseende säkerhetsinbetalningar funnits på flugforum och dessa använts för utbetalning av lön till moderatorer inkluderas viss analys av dessa med koppling till plånböckerna.

Växelanalys har applicerats vilket stämt överens med vilka adresser som tillhör respektive löneplånbok efter återskapande.

- Grön pil** - Använts för att tydliggöra en lönetransaktion
- Blå pil** - Representerar växel vilket innebär att kluster som är sammankopplade med blå pilar tillhör samma plånbok.
- Röd pil** - Transaktioner till Chipmixer
- Lila pil** - FS3 relaterade transaktioner

Nationella operativa avdelningen

2023-05-11

Resultat

Säkerhetsinbetalningar - depositioner

De plånböcker som gör jämna insättningar på lönedatum till plånböckerna 200323, 200424 emottar flertal insättningar som bedöms vara säkerhetsinbetalningar.

Den FS3 plånbok som betalar ut en jämn utbetalning på lönedatum till löneplånboken 200925 tar emot insättningar till bekräftade säkerhetsinbetalningsadresser.

Urklipp från Flugforum avseende säkerhetsbetalningar

admin
Administratör
Registrerad: 2018-12-27
Inlägg: 822
IP address logged
☒ Email

2019-10-09 14:03:20
#335
Vi har problem med säljare som inte sköter sina affärer som de ska. Detta tar upp en hel del tid och arbete från vår sida med dispyter som skall hanteras och kunder vars ordrar aldrig blir skickade, så vi måste göra det lite svårare att börja sälja på FS för att förhoppningsvis öka kvaliteten på de som säljer och ge en känsla av att ett säkarkonto på FS är värdefullt och bör hanteras därefter.

Som första steg:

Ny säljare måste skicka bild på hela sitt varulager med lapp som inkluderar dagens datum och säljarnamn.
Säljarsäkerheten höjs från och med nu till 5000kr (uppdaterar detta i information till säljare om en stund)

Har du en förslag på lämplig tjänst dit nya säljare skall ladda upp bilden som vi kan använda för alla? Har inte riktigt tid att skapa en egen funktion för det just nu.

I övrigt kan vi hålla allt som det är med krav på förklaring om pgp osv.

Vad tycker du om detta?

Offline
:: Rapportera :: Ta bort :: Ändra :: Citera

Bild 1

Likartad hantering av inkomst

Alla analyserade plånböcker i detta PM hanterar inkommande jämn insättning på lönedatum på likartat sätt såsom moderator Hund hanterar dem och såsom plånböcker kopplade till Adam hanterar det dvs genom att skicka värden genom Chipmixer och i vissa fall görs insättningar till FS3 köpkonto samt lämna det i plånboken som understiger minimum-belopp för att skickas genom Chipmixer.

Löneplånbok 20-01-23, Koppling moderator Hund och Adam Nironen(65)Summering

Återskapad plånbok 20-01-23(65) med återställningsfras från Adam Nironens ipad.⁵

Här är antagande avseende lön från FS3 baserat på:

- att insättningen av bitcoin var jämn och genomfördes på lönedatum
- värdet i SEK stämmer med övriga löneinsättningar⁶
- plånboken är återskapad med återställningsfras från Adam Nironen
- plånbokens användning av Chipmixer och FS3, standardförfarande för moderator Hund och för de återskapade plånböckerna

Tabell: Transaktionsdata för

ea0eb69023b9d761eecd514d7cf8783e1f5d07621b245fcfcf6efd6820192fab

Datum	Belopp BTC	Dagskurs	Belopp SEK (ca)	Mottagande bitcoin address
20-01-23 19:54	0,375	79990.0246	29 996	bc1q9dvv4jrj0rhrwgtytd79vk58plsqwemvdf6wx4

Grafisk presentation av utbetalningen till plånboken baserat på blockkedjan

En jämn utbetalning i BTC från analys FS3 admin skedde 2020-01-23 till plånboken med 0,375 BTC vilket vid tillfället motsvarade ca 29 996 SEK. (grön pil)

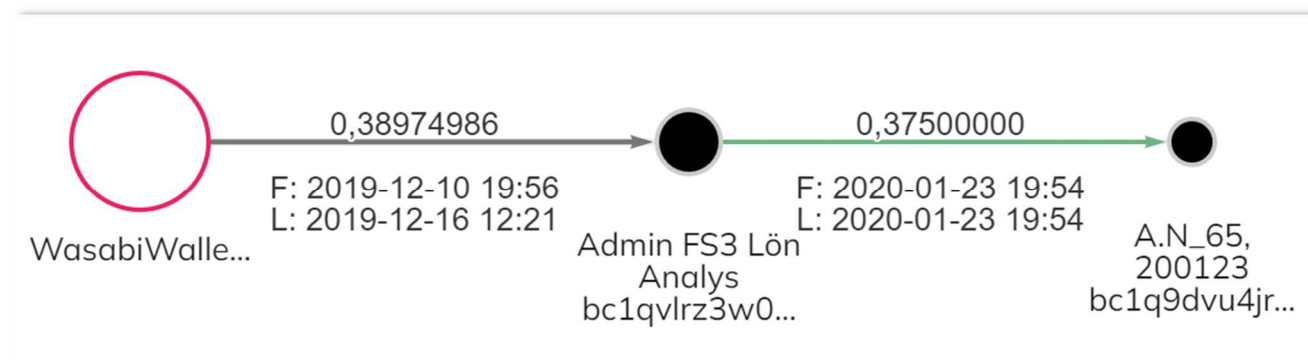


Bild 2

⁵ Återskapad plånbok med återställningsfras(unaware-pursue) från Adam Nironens ipad med löpnummer 65. Beslag 2023-5000-BG3418-5.

⁶ Se löner i PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen.

Nationella operativa avdelningen

2023-05-11

Grafisk presentation av alla transaktioner i plånboken baserat på blockkedjan

Lönen överförs genom flertal insättningar genom Chipmixer(röda pilar).

Flertal insättningar sker till FS3 köpkonto med insättningsadress 3P89QvZQUniN-jHw3yJMRCVqbThp5Po7Svt (lila pilar)

Insättning på FS3 köpkonto görs i syfte att handla på FS3. En köpare kan inte själv ta ut insatta medel från ett FS3 köpkonto⁷.

På grund av antalet transaktioner har plånboken uppdelats i två rader. Följ den långa blå pilen vilket är växeln på insättning till FS3.

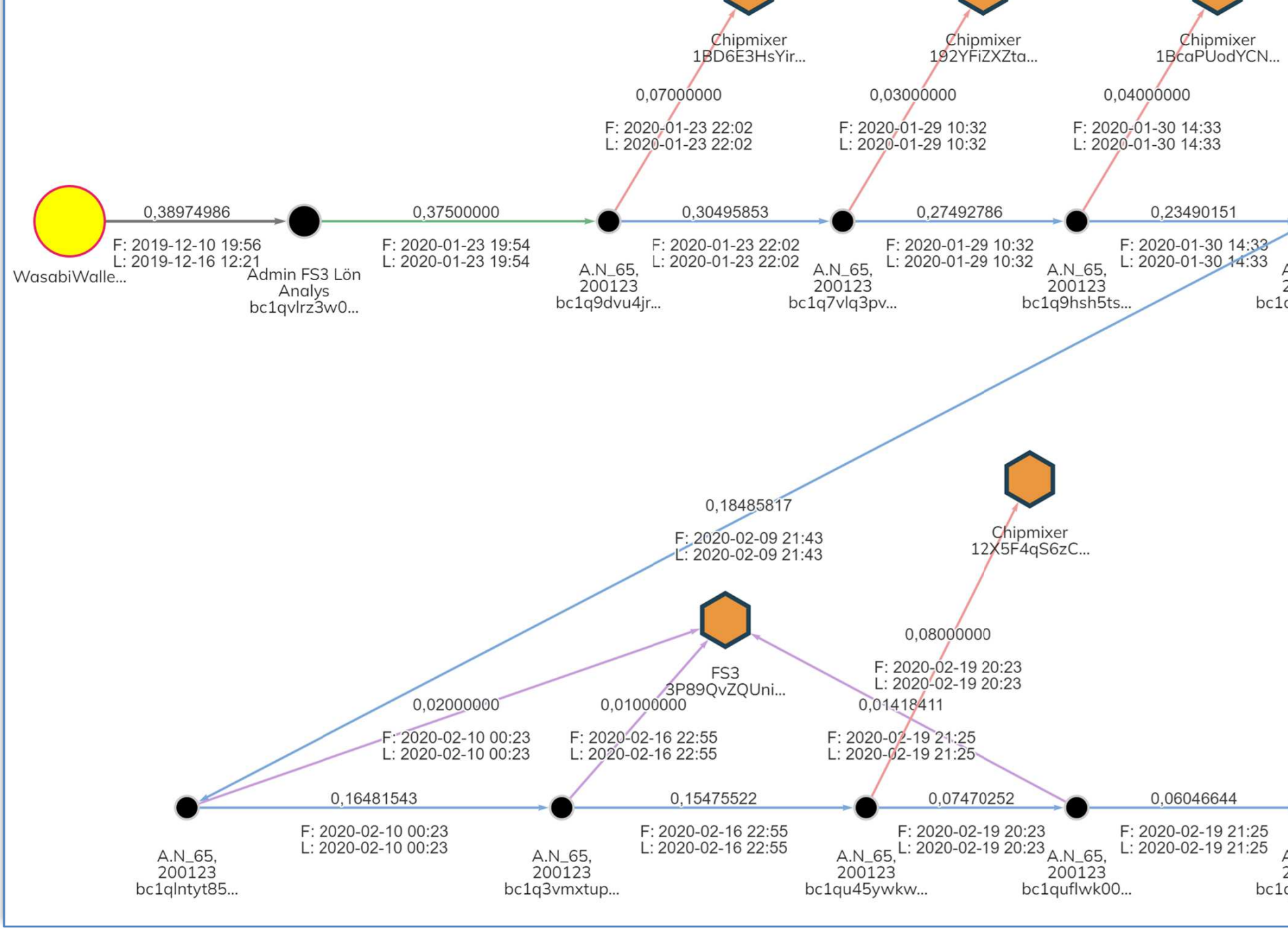
Alla kluster sammankopplade med blå pilar tillhör samma plånbok

Börja läs transaktionerna i plånboken från vänster. Starta från den svarta cirkeln och följ den gröna pilen vilket är första transaktionen in i plånboken.

⁷ Se PM Rapport Beskrivning Flugsvamp 3.0

Nationella operativa avdelningen

2023-05-11



Löneplånbok 20-02-24 Koppling moderator Hund och Adam Nironen(89)Summering

Återskapad plånbok 200224 med återställningsfras från Adam Nironens ipad.⁸

Här är antagande avseende lön från FS3 baserat på:

- att insättningen av bitcoin var jämn och genomfördes på lönedatum
- värdet i SEK överensstämmer med övriga löneinsättningar⁹
- plånboken är återskapad med återställningsfras från Adam Nironen
- plånbokens användning av Chipmixer och FS3, standardförfarande för moderator Hund och för de återskapade plånböckerna från Adam Nironen
- Återanvändning av Chipmixeradress 1Pc2YXtm23R9aBwsWQG7Bum6xft8Q2PwRh

Tabell: Transaktionsdata för

53c4dd372d6dfdf3266399d1191150f23750ce697ad807a52232082070c35f91

Datum	Belopp BTC	Dagskurs	Belopp SEK (ca)	Mottagande bitcoin address
20-02-24 08:05	0,32	94085.4043	30 107	bc1q7ajnxvq0pufegh06cqy3dqk6pmuvy8wul0nlfid

Grafisk presentation av utbetalningen till plånboken baserat på blockkedjan

En jämn utbetalning i BTC skedde 2020-02-24 till plånboken med 0,32 BTC vilket vid tillfället motsvarade ca 30 107 SEK, grön transaktions pil.



Bild 4

⁸ Återskapad plånbok med återställningsfras(strategy-dentist) från Adam Nironens ipad med löpnummer 89. Beslag 2023-5000-BG3418-5.

⁹ Se löner i PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen.

Nationella operativa avdelningen

2023-05-11

Grafisk presentation av alla transaktioner i plånboken baserat på blockkedjan

Lönen överförs genom flertal insättningar genom Chipmixer(röda pilar).

Insättning sker till FS3 köpkonto med insättningsadress 3BESAYT4uWVgPym-KqzBqncqnfBQQanPc4 som även tar emot insättningar från Chipmixer. (lila pilar)

Insättning på FS3 köpkonto görs i syfte att handla på FS3. En köpare kan inte själv ta ut insatta medel från ett FS3 köpkonto¹⁰.

På grund av antalet transaktioner har plånboken uppdelats i två rader. Följ den långa blå pilen vilket är växeln på insättning till FS3.

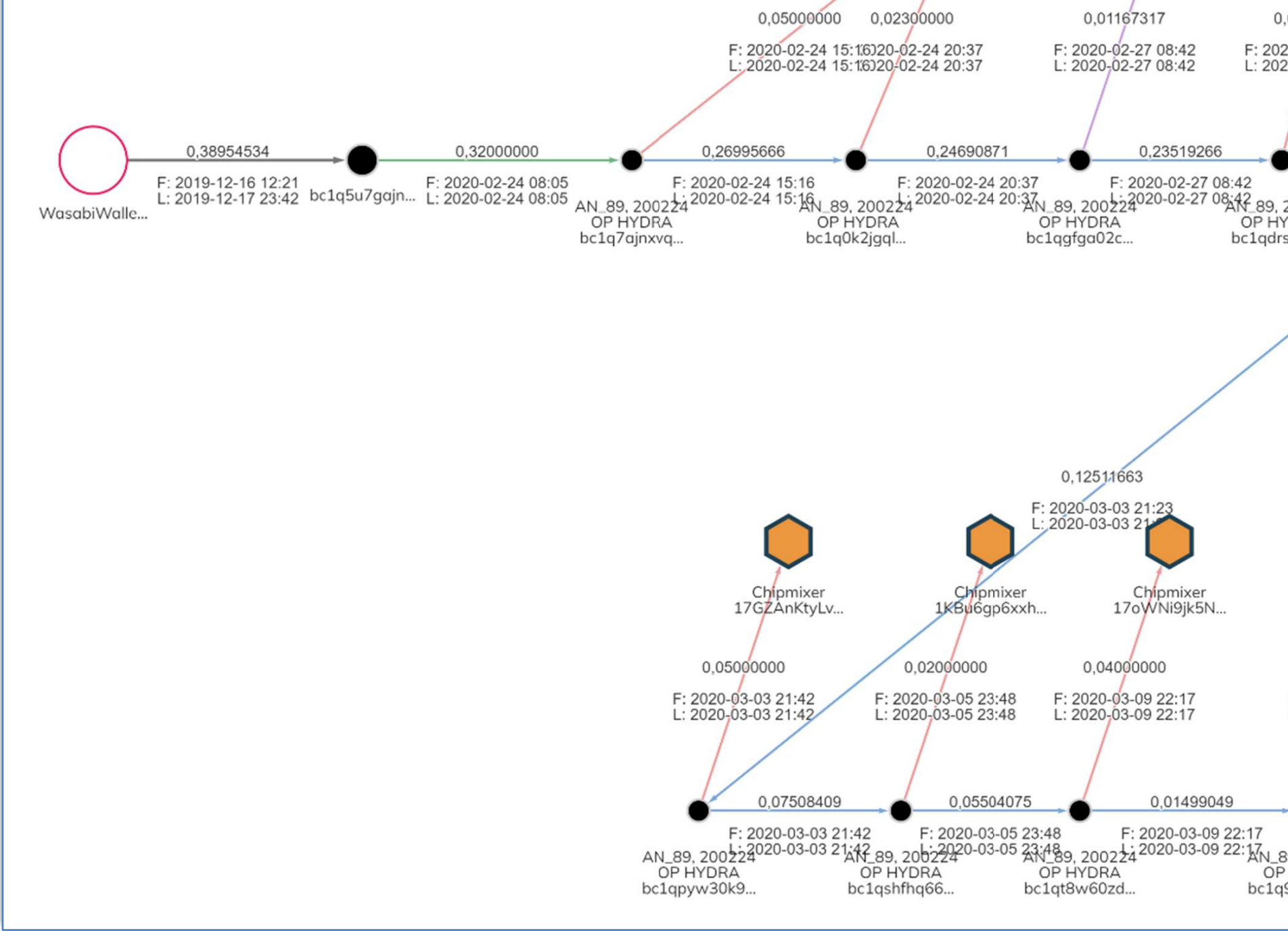
Alla kluster sammankopplade med blå pilar tillhör samma plånbok

Börja läs transaktionerna i plånboken från vänster. Starta från den svarta cirkeln och följ den gröna pilen vilket är första transaktionen in i plånboken.

¹⁰ Se PM Rapport Beskrivning Flugsvamp 3.0

Nationella operativa avdelningen

2023-05-11



Löneplånbok 20-03-23 Koppling moderator Hund och Adam Nironen(20)Summering

Återskapad plånbok 200323 med återställningsfras från Adam Nironens ipad.¹¹

Här är antagande avseende lön från FS3 baserat på:

- att insättningen av bitcoin var jämn och genomfördes på lönedatum
- värdet i SEK överensstämmer med övriga löneinsättningar¹²
- plånboken är återskapad med återställningsfras från Adam Nironen
- plånbokens användning av Chipmixer, standardförfarande för moderator Hund och för de återskapade plånböckerna från Adam Nironen
- Har kopplingar till FS3, bedömt genom möjliga säkerhetsinbetalningar; svarta pilar med ca 0,06 BTC, ca 5000 SEK under perioden 2020-01-12 till 2020-03-08

Tabell: Transaktionsdata för

936185ed82e7b694097132e307117798e53d2d5caa3afdc39c6f73b681d905c6

Datum	Belopp BTC	Dagskurs	Belopp SEK (ca)	Mottagande bitcoin address
20-03-23 13:01	0,53	67054.6698	35 539	bc1q88w7jw8mvd4my2l6w7rny6geu86ksk8we098hv

Grafisk presentation av utbetalningen till plånboken baserat på blockkedjan

En jämn utbetalning i BTC skedde 2020-03-23 till plånboken med 0,53 BTC vilket vid tillfället motsvarade ca 35 539 SEK.

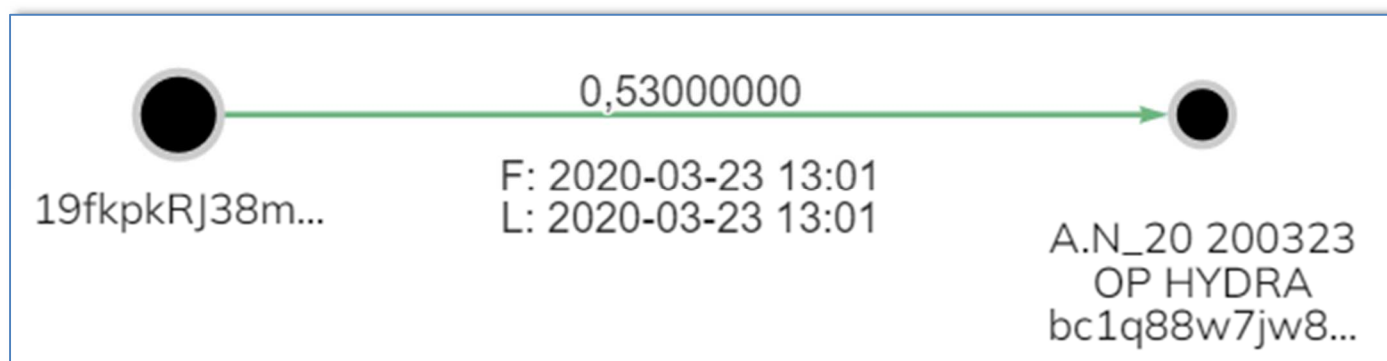


Bild 6

¹¹ Återskapad plånbok med återställningsfras(able-maple) från Adam Nironens ipad med löpnummer 20. Beslag 2023-5000-BG3418-5.

¹² Se löner i PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen.

Nationella operativa avdelningen

2023-05-11

Grafisk presentation av alla transaktioner i plånboken baserat på blockkedjan

Lönen överförs genom flertal insättningar genom Chipmixer(röda pilar).

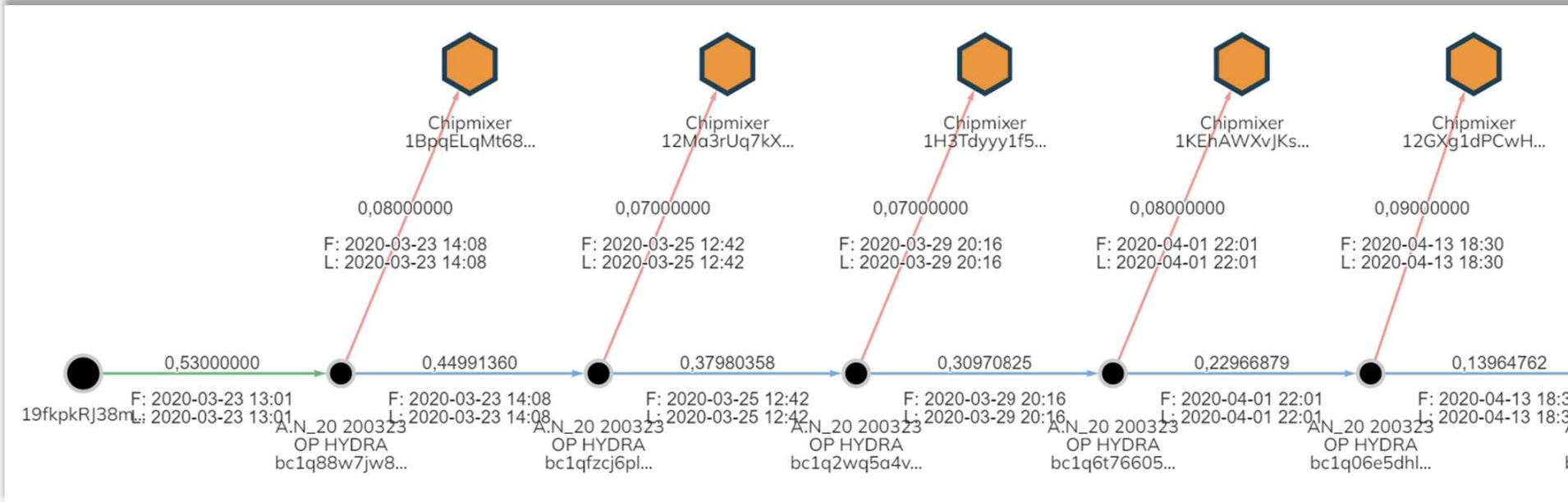
Följ den långa blå pilen vilket är växeln på insättning till Chipmixer.

Alla kluster sammankopplade med blå pilar tillhör samma plånbok

Börja läs transaktionerna i plånboken från vänster. Starta från den svarta cirkeln och följ den gröna pilen vilket är första transaktionen in i plånboken.

Nationella operativa avdelningen

2023-05-11



Nationella operativa avdelningen

2023-05-11

Grafisk presentationer av lönen i sitt sammanhang baserat på blockkedjan

De lila pilarna representerar möjliga säkerhetsinbetalningar på ca 5000 SEK vilka FS3 admin bedöms använda för utbetalning¹³.

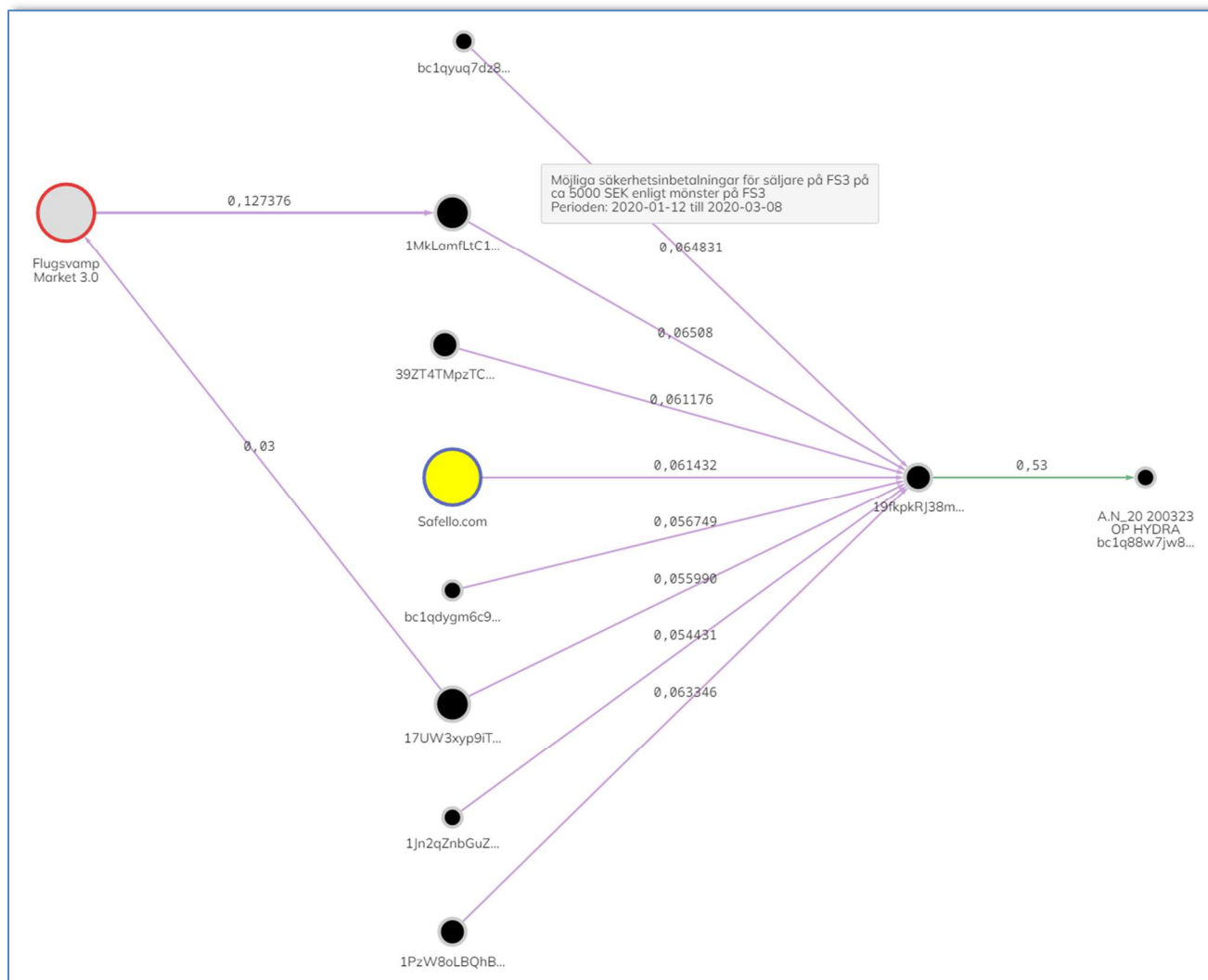


Bild 8

Nedan är en transaktion från ovan bild, den andra uppfifrån som får 0,1273619 BTC och som analyserats separat. Efter det som är en möjlig säkerhetsinbetalning 2020-03-23 13:01 på 0,06508000, så får klustret ut ojämna summor från FS3 med start 2020-01-24 22:17 vilket överensstämmer med säljaruttag.

¹³ Se rubrik: Säkerhetsinbetalningar

Nationella operativa avdelningen

2023-05-11



Bild 9

Löneplånbok 20-04-24 Koppling moderator Hund och Adam Nironen(69)Summering

Återskapad plånbok 200424 med återställningsfras från Adam Nironens ipad.¹⁴

Här är antagande avseende lön från FS3 baserat på:

- att insättningen av bitcoin var jämnt avrundad och genomfördes på lönedatum
- värdet stämmer med övriga löneinsättningar¹⁵
- insättningen kan spåras från FS3
- plånboken är återskapad med återställningsfras från Adam Nironen
- har kopplingar till FS3, bedömt genom möjliga säkerhetsinbetalningar; svarta pilar under perioden 2020-01-29 till 2020-04-17
- plånbokens användning av Chipmixer, standardförfarande för moderator Hund och för de återskapade plånböckerna från Adam Nironen

Tabell: Transaktionsdata för

901cd885aa3ba53ab493fd03b706b084a4a6fac5794482682552d4cb1fb0e350

Datum	Belopp BTC	Dagskurs	Belopp SEK (ca)	Mottagande bitcoin address
20-04-24 17:46	0,49	75629,7249	37 059	bc1qa2rm2wd8yqt2slgqp36wq9ggmrcc9ztke3q7c

Grafisk presentation av utbetalningen till plånboken baserat på blockkedjan

En jämn utbetalning i BTC skedde 2020-04-24 17:46 till plånboken med 0,49 BTC vilket vid tillfället motsvarade ca 37 059 SEK. **Grön transaktionspil**

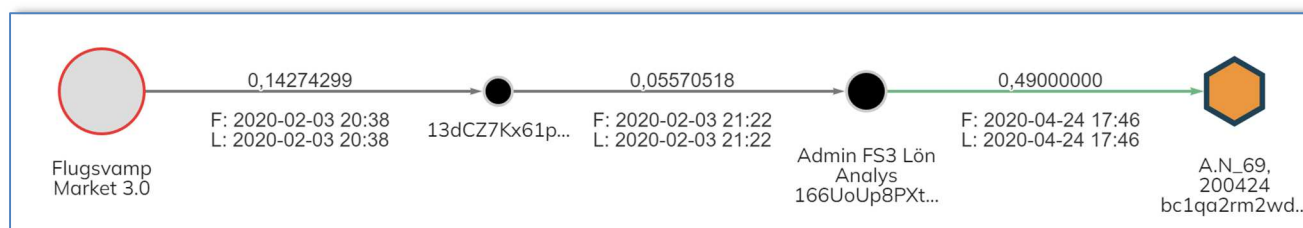


Bild 10

Grafisk presentation av alla transaktioner i plånboken baserat på blockkedjan

Lönen mixas och överförs genom flertal insättningar genom Chipmixer(röda pilar).

Alla kluster sammankopplade med blå pilar tillhör samma plånbok

¹⁴ Återskapad plånbok med återställningsfras(prefer-anchor) från Adam Nironens ipad med löpnummer 69. Beslag 2023-5000-BG3418-5.

¹⁵ Se löner i PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen.

HEMLIG

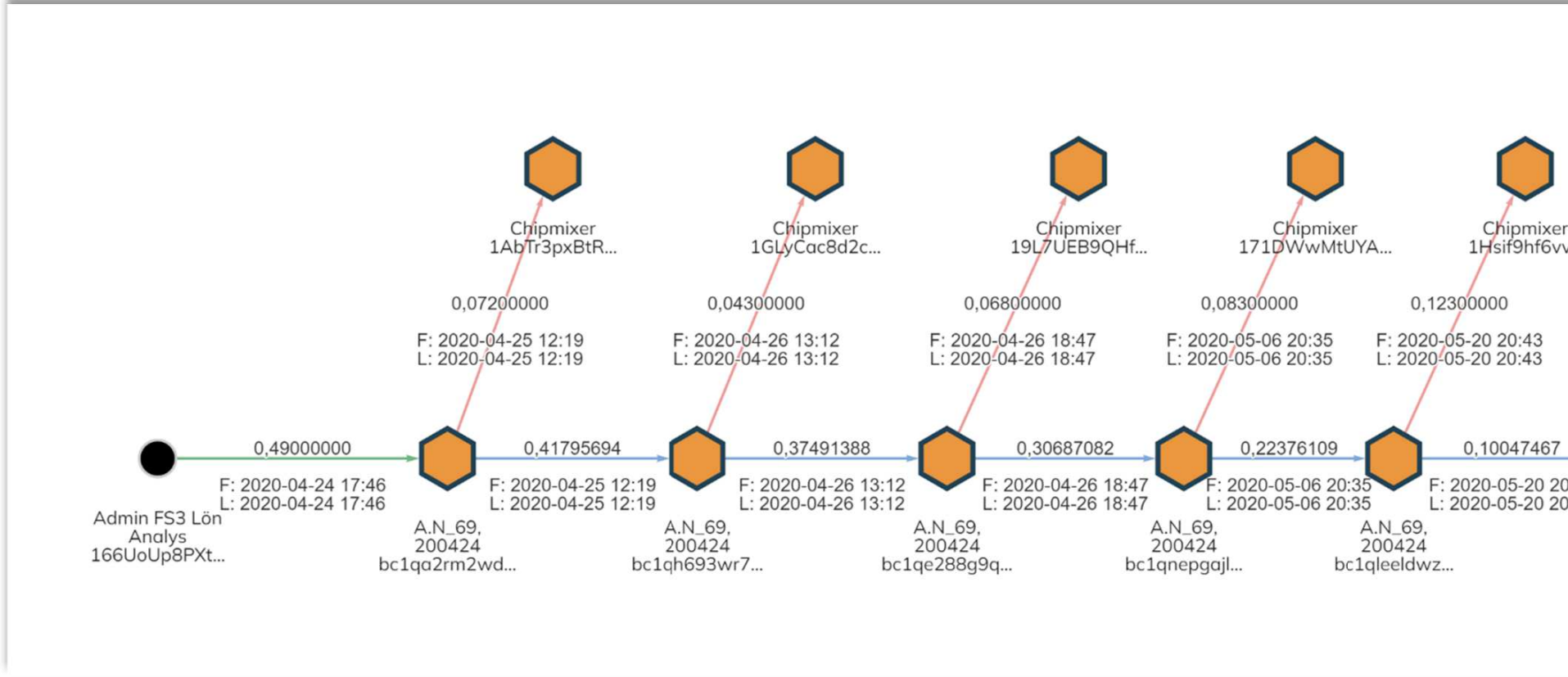
Nationella operativa avdelningen

2023-05-11

Börja läs transaktionerna i plånboken från vänster. Starta från den svarta cirkeln och följ den gröna pilen vilket är första transaktionen in i plånboken.

Nationella operativa avdelningen

2023-05-11



Grafisk presentation av utbetalningen i ett sammanhang baserat på blockkedjan

De lila pilarna representerar möjliga säkerhetsinbetalningar på ca 5000 SEK vilka FS3 admin bedöms använda för utbetalning¹⁶.

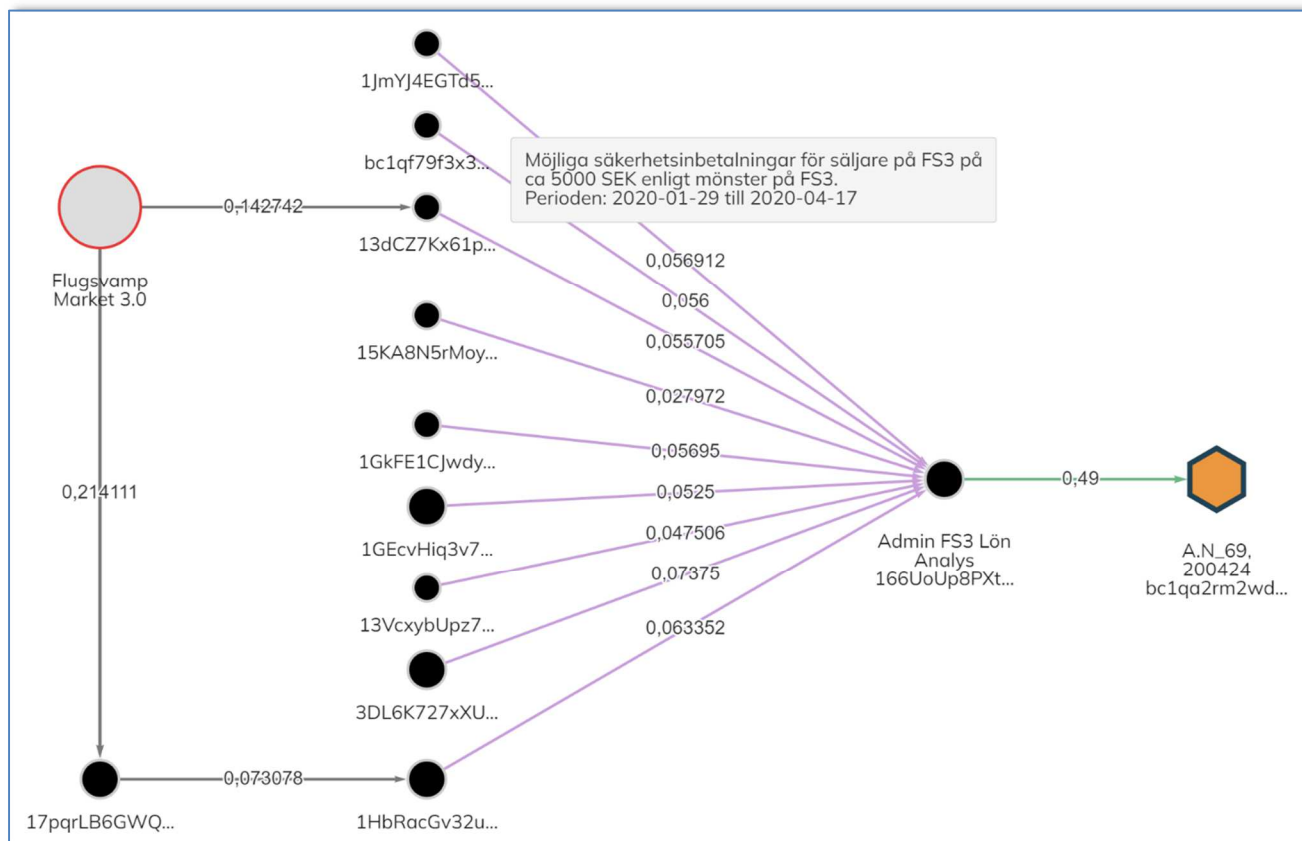


Bild 12 Bedömt säkerhetsinbetalningar

¹⁶ Se rubrik: Säkerhetsinbetalningar

Nationella operativa avdelningen

2023-05-11

Löneplånbok 20-09-25 Koppling moderator Hund och Adam Nironen(29)Summering

Återskapad plånbok 200925 med återställningsfras från Adam Nironens ipad.¹⁷

Här är antagande avseende lön från FS3 admin är baserat på:

- att insättningen av bitcoin var jämn och genomfördes på lönedatum
- värdet stämmer med övriga löneinsättningar¹⁸
- plånboken är återskapad med återställningsfras från Adam Nironen
- plånboken tar emot säkerhetsbetalningar för att öppna säljare-konto på FS3.
- plånbokens användning av Chipmixer, standardförfarande för moderator Hund och för de återskapade plånböckerna från Adam Nironen

Tabell: Transaktionsdata för

121b1b8031f21f3de195e4e2e4b23320130d81976bc2d90d68d24c1a8cc691da

Datum	Belopp BTC	Dagskurs	Belopp SEK (ca)	Mottagande bitcoin address
20-09-25 08:53	0,37	94230,3895	34 865	bc1qmqwryuk94vaj63nntfu5gkcmur86ujywlwzqy4

Grafisk presentation av utbetalningen till plånboken baserat på blockkedjan

En jämn utbetalning i BTC skedde 2020-09-25 08:53 till plånboken med 0,37 BTC vilket vid tillfället motsvarade ca 34 865 SEK.

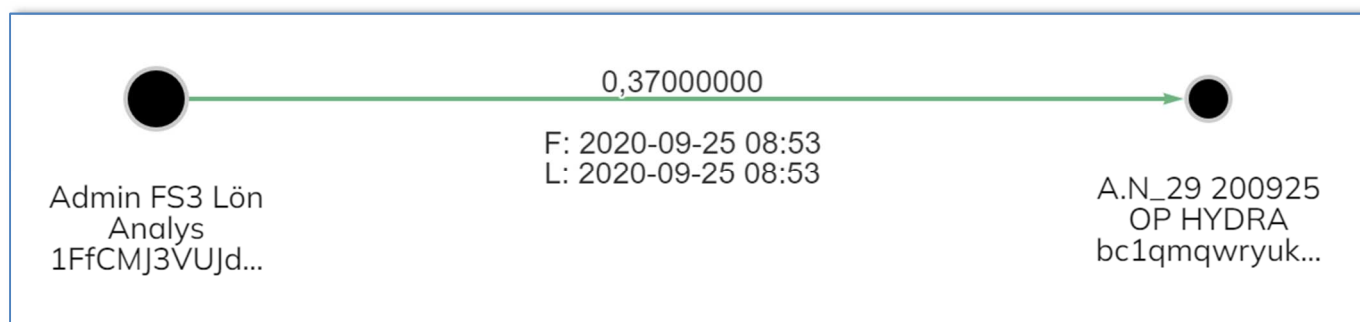


Bild 13 Ubetalning av lön från FS3 admin

¹⁷ Återskapad plånbok med återställningsfras(section-vacant) från Adam Nironens ipad med löpnummer 29. Beslag 2023-5000-BG3418-5.

¹⁸ Se löner i PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen.

Nationella operativa avdelningen

2023-05-11

Grafisk presentation av alla transaktioner i plånboken baserat på blockkedjan

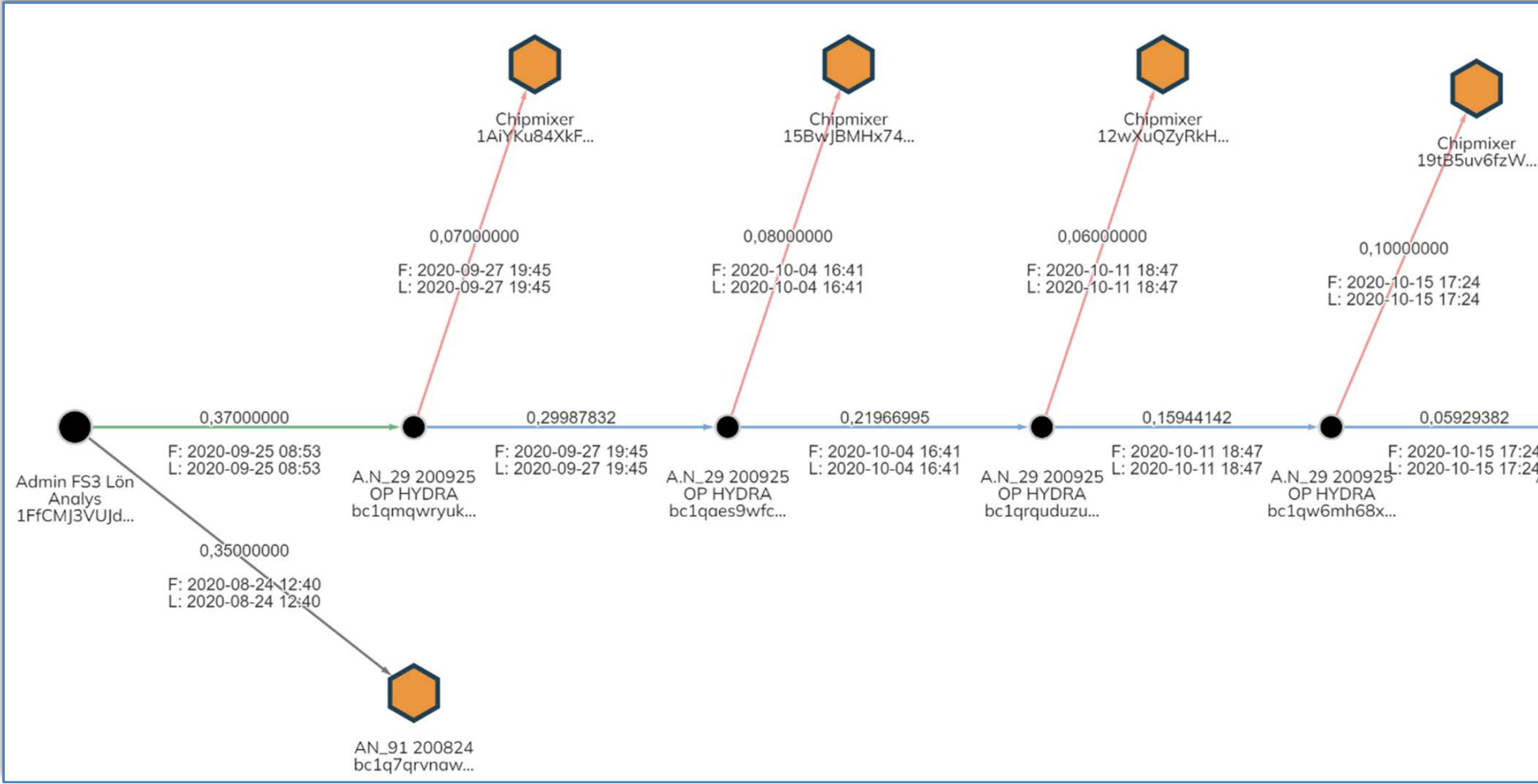
Lönen överförs genom flertal insättningar genom Chipmixer(röda pilar).

Alla kluster sammankopplade med blå pilar tillhör samma plånbok

Börja läs transaktionerna i plånboken från vänster. Starta från den svarta cirkeln och följ den gröna pilen vilket är första transaktionen in i plånboken.

Nationella operativa avdelningen

2023-05-11



Nationella operativa avdelningen

2023-05-11

Grafisk presentation av utbetalningen i ett sammanhang baserat på blockkedjan

Bekräftade säkerhetsinbetalningar till FS3 plånbok som betalar ut en jämn insättning på lönesdatum till löneplånboken 200925

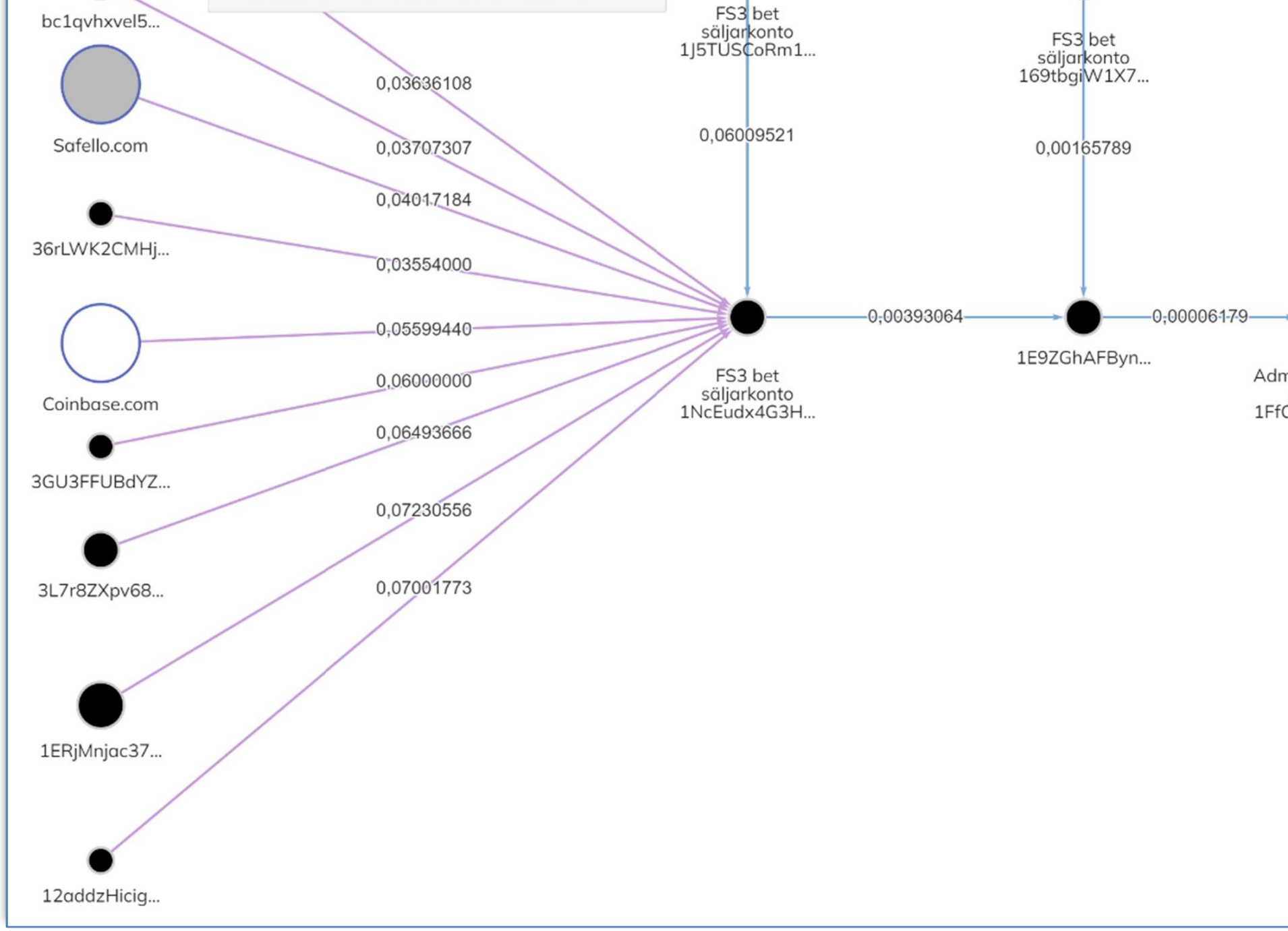
Det kluster som gör en jämn utbetalning på lönedatum till löneplånbok 200925 får insättningar från kluster kopplade till FS3 genom

- bekräftade säkerhetsinbetalningsadresser.¹⁹
- mottagande av växel på en jämn utbetalning på lönedatum. (blå pil)

¹⁹ PM Säkerhetsinbetalningar från säljare till admin Flugsvamp 3.0 samt OP Hydra - Analys av Bitcoinflöde till och från marknadsplatsen Flugsvamp 3.0

Nationella operativa avdelningen

2023-05-11



HEMLIG

Nationella operativa avdelningen

2023-05-11



Polisen

PM1 (15) **HEMLIG**

Datum

2023-04-27

Diariennr (åberopas)

5000-K615323-19

Polismyndigheten
Utredningsenheten
Nationellt it-brottscentrum
Teknisk inhämtning
Anette Berglund

OP Hydra - Kryptospårning avseende återskapade plånböcker på höger sida om Chipmixer

Syfte

Syftet med detta PM är att beskriva de kryptofinansiella observationer och analyser som gjorts i ärendet gällande Adam Nironen(940119-7554) och hans kopplingar över tid efter mottagande av bitcoin från Chipmixer.

Alla återskapade plånböcker från beslag är inte inkluderade utan summeringen är primärt baserat på svar från kryptotjänster samt växelanalys.

Innehåll

Syfte	1
Bakgrund.....	3
Vad är Flugsvamp Market 3.0 (FS3)	3
Flugforum, lön, moderatorer och användare.....	3
Löneplånbok	3
Tillgängliga löneadresser från Flugforum för moderator Hund	3
Allmänt användare Piraten.....	3
Vad var Chipmixer.....	3
Om spårning av kryptovalutor	4
Om redovisade kryptospårningsgrafer	5
Dagskurs för att omvandla bitcoin (BTC) till SEK	6
Källor	7
Sammanfattning	8
Tillvägagångssätt	8
Analys av transaktioner.....	8
Användning av Chipmixer.....	10

Nationella operativa avdelningen

2023-05-10

Övergripande.....	10
Summerande beskrivning hur det går till.....	10
Återanvändning av samma för användaren unika Chipmixeradress.....	11
Resultat	12
Övergripande Adam Nironen.....	12
Summering av transaktioner till och från kluster identifierade till Adam Nironen	12
Bilagor.....	15

UTKAST

Bakgrund

I detta avsnitt presenteras utökad bakgrundsinformation då dokumentet innehåller detaljer som kräver viss insikt i bl.a. Flugsvamp 3, kryptovalutor och spårning av dessa samt mixertjänsten Chipmixer¹.

Vad är Flugsvamp Market 3.0 (FS3)²

FS3 var en svensk internetmarknadsplats för primärt narkotika som existerade mellan 2018.12.17 och 2021.10.30. Under marknadsplatsen livstid kunde användare skapa konton på sidan och använda dessa för att köpa eller sälja produkter på sidan. Marknadsplatsen användes via anonymiseringstjänsten TOR och all handel skedde med kryptovalutan bitcoin (BTC).

Flugforum, lön, moderatorer och användare³

På själva Flugsvamp Market 3.0 fanns ingen plattform för diskussion. Till detta ändamål fanns i stället internetforumet *Flugforum* där det också fanns ansvarig admin-roll och moderator-roller.

En moderators arbetsuppgift på en plattform är generellt att bistå med hanteringen av det dagliga arbetsflödet på plattformen.

För sin arbetsinsats erhöll sidans moderatorer lön från administratören (FS3 admin) av Flugsvamp Market 3.0⁴. Moderatorkontot "Hund" var en av de moderatorer som erhöll lön från administratören.

Löneplånbok

Benämningen löneplånbok används där plånboken mottagit ett jämnt belopp på lönedatum.

Tillgängliga löneadresser från Flugforum för moderator Hund

Genom tillgång under viss tid till den privata delen av Flugforum har utredningen tagit del av Hunds löneadresser för augusti, september och samt till viss del i oktober 2019 samt mars, april, september och oktober år 2021. Dessa definieras som bekräftade.

Allmänt användare Piraten

I utredningen har det framkommit behov av att göra kryptoanalys gällande Adam Nironen och dennes kopplingar till FS3 användarkonto Piraten.

Vad var Chipmixer

Chipmixer var en av många mixertjänster som används för att dölja och anonymisera härkomsten av krypto.⁵

Då kryptovalutor är spårbara genom den öppna blockkedjan kan mottagare av kryptovaluta i vissa fall se var pengarna härstammar ifrån. Denna möjlighet nyttjas av t.ex. kryptoväxlingsföretag i syfte att detektera pengar som härstammar från marknadsplatser för handel med vapen/narkotika/barnövergreppsmaterial, it-brottsvinster eller andra icke önskvärda källor.

¹ En kortare beskrivning av Chipmixer finns under rubriken "Tillvägagångssätt".

² Se PM Rapport Beskrivning Flugsvamp 3.0

³ Se avsnitt avseende Hund i huvudprotokollet under Roller och aktivitet på Flugforum och Marknadsplatsen

⁴ Information från den privata/dolda delen av Flugforum.

⁵ Mer info avseende Chipmixer finns under rubrik "Tillvägagångssätt".

För att dölja den ursprungliga källan till sina kryptovalutor finns därför s.k. *mixertjänster*. Syftet med en mixertjänst är att försvåra *spårningen* av kryptovalutor genom att dölja den ursprungliga källan till pengarna från framtida mottagare.

Generellt fungerar de flesta mixertjänster genom att användare skickar in sina kryptovalutor i mixertjänsten varpå pengarna efter en tid skickas ut av tjänsten till en nyskapad adress/plånbok som användaren får tillgång till. Under processen har pengarna rörts ihop med andra användares kryptovalutor, vilket döljer den initiala källan till pengarna. Den nya källan till pengarna blir således mixertjänsten.

I detta PM är Chipmixer relevant då Chipmixer användes genomgående för att anonymisera och dölja varifrån kryptovaluta kommer ifrån.

Om spårning av kryptovalutor

Transaktioner med kryptovalutor fungerar genom en så kallad *blockkedja*. En blockkedja är en (oftast) publik databas på internet där samtliga transaktioner med en kryptovaluta registreras.

Kortfattat innebär det att samtliga bitcointransaktioner som någonsin ägt rum finns helt öppet publicerade på internet. Det som framgår om transaktionerna i blockkedjan är bl.a. vilka datum, adresser och belopp som förekommer i transaktionerna, dock inte vem de inblandade bitcoinadresserna *tillhör*.

För att kunna spåra transaktioner med kryptovalutor behöver man således komplettera transaktionsinformationen från de öppna blockkedjorna med *kunskap* om vem som äger respektive kryptoadresser. Det finns idag flera analysverktyg för kryptospårning som besitter stora mängder information om använda kryptoadresser och dess ägare, vilket gör det möjligt att visualisera samt genomföra spårningar av transaktioner.

Kryptospårningen som redovisas i detta PM baseras därmed på öppen information från blockkedjan kombinerat med kännedom om kryptoadresser från ett eller flera etablerade kryptospårningsverktyg. Spårningsverktyg har ägarkännedom om vissa (men inte alla) kryptoadresser, därför kan vissa transaktioner spåras till olika identifierbara entiteter såsom olika kryptotjänster, där växling från kryptovalutor till fiatvaluta eller andra kryptovalutor har ägt rum. Dessa tjänster kan i sin tur ha ytterligare information om sin kund som brukat tjänsten, i form av ytterligare transaktionsinformation eller annan data.

Avseende ägandet av specifika kryptoadresser i *privata kryptoplånböcker*, vilka lagras lokalt i telefoner/datorer hos användare, är dessa oftast okända för kryptospårnings-verktyg då privata kryptoplånböcker generellt är anonyma, såvida adresserna i dessa inte blivit kända för den utredande analytikern vilket är fallet vid till exempel återställning av en kryptoplånbok.

När man pratar om kryptovaluta används ofta termer som kryptoadresser, plånböcker, privata och publika nycklar, återställningsfraser och kluster. Nedan återges en snabb förklaring till dessa termer:

- Kryptovalutor skickas till och från en eller flera adresser. Med en **kryptoadress** avses således en specifik kryptoadress som använts för att skicka eller ta emot kryptovaluta.
- Kryptoadresser kan vara långa och jobbiga att hantera manuellt. Därför hanteras betalningar och adresshantering ofta via **kryptoplånböcker**. En plånbok är oftast en programvara/telefonapp vars syfte är att agera lagringsplats för en eller flera kryptoadresser, samt möjliggöra

betalningar med dessa adresser.

- En kryptoadress består i regel av två delar; en privat och en publik nyckel. Den **publika nyckeln** är själva kryptoadressen och kan lämnas ut till andra om man önskar ta emot betalningar till adressen i fråga.
- Den **privata nyckeln** används till att signera utbetalningar från den motsvarande publika nyckeln. Oftast hanterar plånböckerna detta åt användarna. Den privata nyckeln kan också betraktas som en värdehandling då man med hjälp av denna kan förbruka de pengar som finns på den tillhörande adressen.
- En kryptoplånbok kan skapa många kryptoadresser (och privata nycklar) åt användaren. Dessa kan lagras uteslutande i plånboken i fråga, som i sin tur kan lagras t.ex. i en dator eller mobiltelefon. Skulle enheten gå sönder så skulle pengarna också gå förlorade vilket inte vore säkert.

Därför erhåller användare ofta en s.k. **återställningsfras** till plånboken vid skapandet av plånboken. En sådan fras består oftast av 1-25 ord i en specifik ordning. Med hjälp av dessa ord kan åtkomsten till samtliga adresser i plånboken återskapas i en annan plånbok. Därför betraktas även återställningsfraser som värdehandlingar.
- **Ett kryptokluster** är en term som används vid visualisering av kryptospårning och avser två eller flera kryptoadresser som bedömts hanteras av samma kontrollerande entitet. Dessa bedömningar sker dels automatiskt av kryptospårningsverktyg och baseras då på öppen information från blockkedjan. Om en kryptobetalning görs från t.ex. fyra bitcoinadresser samtidigt, vilket är vanligt, kan man dra slutsatsen att adresserna kontrolleras av samma betalande entitet som styr över samtliga adresser privata nycklar. Adresserna kan då visualiseras som en (1) grafisk entitet istället för fyra separata adresser. *En plånbok består oftast av flertal kluster i verktyget som ännu inte automatiskt identifierats höra samman.*

Klustring kan också utföras manuellt av kryptoanalytikern. Manuell klustring skapas genom kryptoanalys – antingen mot bakgrund av vetskap om att två eller flera adresser hör ihop, eller mot kryptoanalytikerns bedömning om att två eller flera adresser hör ihop baserat på hur adresserna interagerat tekniskt på blockkedjan. För mer info se ”PM Spårning av kryptovaluta och kluster”.

Ovanstående har applicerats då information avseende adressernas ägande har funnits i Flugforum, genom hemlig dataavläsning, och i enheter kopplade till Adam Nironen där till exempel återställningsfraser påträffats⁶.

Om redovisade kryptospårningsgrafer

I detta PM presenteras utförd kryptoanalys som bilder/grafer från kryptospårningsverktyg. Dessa bilder visualiserar kryptoflöden som ägt rum mellan olika adresser och adresskluster. Bilderna av vissa spårningar kommer även med som bilagor för att kunna läsas i detalj. Nedan förklaras innehållet i dessa grafer:

⁶ Gul lapp i Adam Nironens plånbok samt från beslagsnummer: 2023-5000-BG3418-1(mobil), 2023-5000-BG3418-5(ipad).

- Graferna i detta PM ska generellt läsas från vänster till höger, med vissa undantag. Transaktionerna sker alltid i pilarnas riktningar. I grafer representeras kluster av bl.a. ringar som symboliserar t.ex. marknadsplatser, mixertjänster och växeltjänster för kryptovalutor. Då det är relevant med specifik adress har detta valts ut och presenterats med en hexagon.
- En pil mellan kluster representerar en eller flera transaktioner som gått i pilens riktning. Ovanpå pilarna kan olika datum redovisas, t.ex. "F: <datum> L: <datum>". F och L står i dessa fall för "first" resp. "last", dvs. första och sista gången transaktioner har skett mellan adresserna i fråga.
- Transaktionspilarna kan ha olika färg i grafer; generellt gäller följande legend:
 - Gröna pilar representerar generellt löneutbetalningar
 - Blåa pilar representerar växel på transaktioner. Voxel sker på grund av överskottet som tillhör betalande plånbok.
 - Röda pilar representerar transaktioner till/från Chipmixer
 - Lila pilar representerar transaktioner till/från FS3
 - Turkosa pilar är endast pilar med tillhörande kommentarer
- Vid en bitcointransaktion töms de betalande adresserna på saldo, den överblivna växeln kan åka tillbaka till den *betalande adressen*, eller till *en av plånboken nyskapad adress*. Detta hanteras oftast automatiskt av kryptoplånboken. Detta kan leda till grafer där en och samma plånbok består av flera adresskluster i kryptoanalysprogrammet.

I de fall växeladresser tillhörande samma plånbok har detekterats har växeladresserna visualiserats med blå pilar i graferna. Det innebär att kluster som i bilderna är kopplade med blå pilar enligt växelanalys tillhör samma plånbok.

- Tider i graferna

Tiderna visade i graferna är i UTC vilket innebär:

CET – Svensk vintertid = UTC +1 timme

CEST – Svensk sommartid = UTC + 2 timmar

Tiden som är specificerad på respektive transaktionspil är när transaktionen konfirmerades. Detta sker ca var 10:e minut. I dokumentet har därför generellt skrivits "i stort sett samtidigt" när transaktioner har samma tidsstämpel.

Dagskurs för att omvandla bitcoin (BTC) till SEK

Kurs som använts genomgående i detta PM är baserad på dagskursen för respektive transaktion. Då värdet på krypto är fluktuerande över dag och tid är detta ett ungefärligt värde. Kursen har inhämtats från kryptoväxlingsföretaget Coinbase.

För att få dagskursen så kan nedan URL användas, där man byter ut datumet till den dag man är intresserad av.

<https://api.coindesk.com/v1/bpi/historical/close.json?start=2021-10-29&end=2021-10-29¤cy=SEK>

Nationella operativa avdelningen

2023-05-10

Källor

I analysen har följande källor primärt givit underlag till information avseende tillhörighet av krypto-adresser och beteenden:

- Rapport Beskrivning Flugsvamp 3.0
- PM Återställning av plånböcker från beslag BG3418-5⁷
- PM Återställning av plånböcker från beslag BG3418-1⁸
- PM Adam Nironen beslag Bitpay plånbok
- PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen
- Information från kryptoväxlare och kryptotjänster

⁷ PM gällande återställning av kryptoplånböcker från Adam Nironens ipad

⁸ PM gällande återställning av kryptoplånböcker från Adam Nironens mobil

Sammanfattning

Från Chipmixer hämtar Adam Nironen ett stort antal chips, dvs fasta värden av bitcoin, till ett värde av ca 713 676 SEK under perioden 2019-06-23 till 2022-12-22.

En insättning från FS3 admin på lönedatum går direkt till en återskapad löneplånbok AN_44 190624 som är identifierad till Adam Nironen genom kontakt med kryptoväxlare.

En ojämn insättning går direkt från FS3 till denna plånbok.

Avseende plånböcker på höger sida om Chipmixer har Adam Nironen använt överföringarna från Chipmixer till olika sammanhang såsom insättning till Crypto.com till vilket han kopplat ett betalkort, gjort köp genom tjänsterna BitPay och BitRefill samt växlat genom CoinGate och ChangeNow samt nyttjat en okänd tjänst⁹ som även moderator Hund nyttjat.

Tillvägagångssätt

Analyser har gjorts baserat på tillgänglig information i ärendet. Där kopplingar funnits till olika etablerade kryptotjänster har dessa kontaktats i syfte att erhålla ytterligare kundinformation.

När man får ägarkännedom om en (1) adress analyseras adressen i ett analysverktyg. I detta fall har växelanalys genomförts i stor utsträckning.

I detta ärende har adresser påträffats på Flugforum, underlag via hemlig dataavläsning, i svar från kryptoväxlingsföretag, återställningsfraser på en gul lapp i Adam Nironens plånbok samt ett stort antal återställningsfraser mm i beslag av ipad och mobil.

För att kunna överföra ett värde från en kryptoadress måste användaren ha tillgång till den privata nyckeln som tillhör adressen. Den privata nyckeln genereras när adressen skapas.

Detta innebär att en utgående transaktion från en plånbok kan **endast** göras om man har tillgång till de privata nycklarna för adressen i plånboken.

En plånboks samtliga kryptoadresser kan återskapas med en återställningsfras som består av ett antal ord i en viss ordning. Detta kan jämföras med ett kassaskåp vilken endast kan öppnas och hanteras av den som har nyckeln dvs återställningsfrasen. I ärendet har flera sådana återställningsfraser beslagtogs vilka använts för att återskapa frasernas tillhörande kryptoplånböcker med tillhörande adresser. När man återskapar en kryptoplånbok får man tillgång till all historik samt kontroll över de kryptovalutor som finns i plånboken. Separata PM finns skrivna om dessa¹⁰.

Analys av transaktioner

Generellt kan sägas att det finns väldigt många mixertjänster, växeltjänster och betaltjänster tillgängliga för att hantera kryptovaluta. Analys har därför gjorts för att se mönster i vilka tjänster som använts av löneplånböckerna vid mottagande av lön samt vad Adam Nironen använt, där Chipmixer, BitRefill, BitPay, Crypto.com, ChangeNow, CoinGate samt insättningsadresser på FS3 köpkonto

⁹ 3NxTrm9XgYY6Tk~

¹⁰ Se rubrik i detta PM: Källor

Nationella operativa avdelningen

2023-05-10

varit viktiga. Utöver det har även en oidentifierad tjänst¹¹ använts av både moderator Hund och Adam Nironen.

När man överför värden från en bitcoinadress till annan så skapas en växel med överskottet som antingen skickas till en ny adress eller så sätts växeln tillbaka till den adressen som skickade.

I de fall det skapas en ny växeladress med överskottet på betalningen, tillhör även den till samma plånbok/ägare som skickade transaktionen.

I stor utsträckning har växelanalys legat till grund för skapande av vilka bitcoinadresser som tillhör samma plånbok och därmed samma ägare.

Bitcoinadresser som bedömts tillhöra samma plånbok genom växelanalys är i alla grafer sammanlänkade med blå transaktions pilar dvs vilka representerar växeln. Flera av dessa plånböcker har sedermera kunnat verifieras genom återskapade plånböcker med återställningsfraser från hemlig dataavläsning, gul lapp i Adam Nironens plånbok samt från Adam Nironens ipad.

I nedanstående exempel kan man baserat på växelanalys, följ blåa pilar, bedöma att adresserna bc1q4xyrzs~, bc1qylv2ke3~ och bc1q3zffsqk~ tillhör samma plånbok.

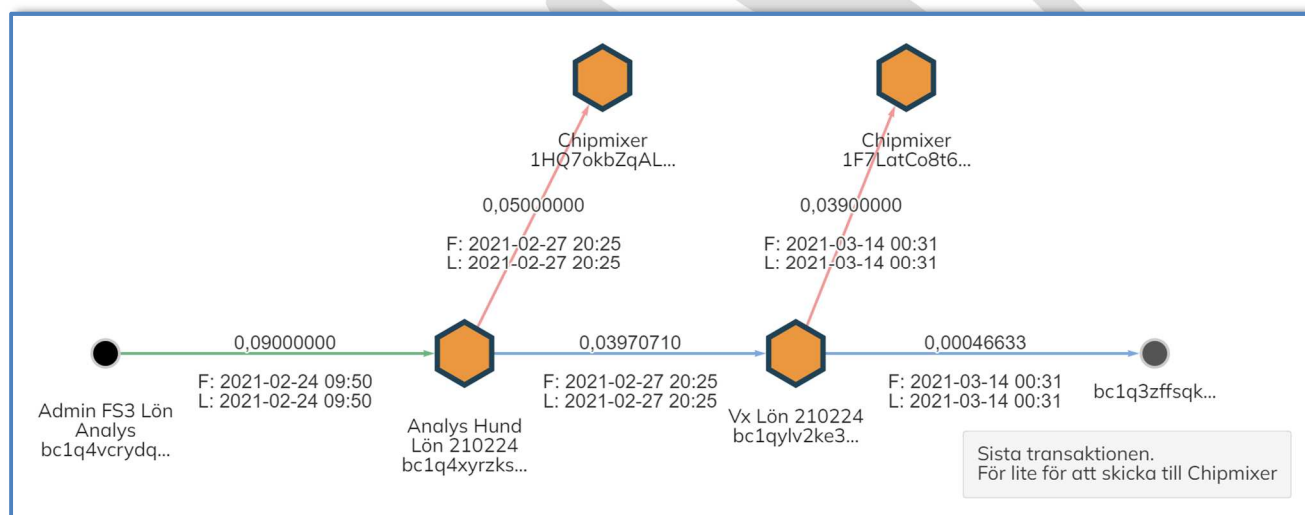


Bild 1 Exempel på tydliggörande av växelanalys baserat på transaktioner på blockkedjan

¹¹ 3NxTrm9XgYY6Tk~

Användning av Chipmixer

Övergripande

I denna utredning gällande Adam Nironen och moderator Hund har mixertjänsten *Chipmixer* påträffats frekvent.

I och med det har det även lagts fokus på att probabilistiskt identifiera dessa transaktioner genom Chipmixer. Probabilistiskt innebär att man endast kan göra en bedömning om att transaktioner genom Chipmixer hör ihop genom att matcha med summa och tid som ingångsvärden så länge man inte har tillgång till underlag från Chipmixer. Man kan alltså inte följa transaktionen genom blockkedjan.

Chipmixeradressen och sessionsid(sessiontoken) genereras då man startar en mixing session mot Chipmixer. Dessa är unika för dig och är sammankopplade. Det sessionsid man får är en värdehandling vilken används för att få tillgång till de för dig nya bitcoins av motsvarande värde som du satt in. Leverans från Chipmixer dvs. de privata nycklarna till de nya bitcoinadresserna, totalt med samma värde som insättningen, kommer i specifika valörer, så kallade chips¹². Dessa är förgenererade och minimivärdet på ett chips är 0,001 BTC.

Sessionen är aktiv i sju dagar, därefter har du inte längre access till informationen till de privata nycklarna eller kan sätta in BTC till Chipmixeradressen och få något tillbaka.

När mixningen är klar efter ca 15-30 min så använder du ditt unika och tillfälliga sessionsid som kan användas i sju dagar, för att få access till de privata nycklarna till chipsen.

Summerande beskrivning hur det går till

Nedan följer en summerande beskrivning om hur ”mixingen” går till hos Chipmixer:

- Användaren går in på darknet på Chipmixers hemsida och påbörjar en mixing.
- När man påbörjar en ”mixning” erhåller användaren en egen unik sessions-ID på Chipmixers websida, vilket kan jämföras med ett mycket långt lösenord. Man blir informerad att spara denna textsträng för att kunna använda den i kommande skede. **Utan sin egna temporära unika session-ID får man inte tillgång till de mixade pengarna och förlorar sina insatta pengar.** Denna sessions-ID är ingen cookie utan sparas genom att markera den på websidan och spara den.
- Användaren sparar sin sessions-ID. Då dessa Ids är långa är det sannolikt att de sparas på den enhet där man får dem. Exempel på en sessions-ID:
ha5YqpyLZwhXBTm7dCGUu5PZsMLmM9Jm
- Användaren erhåller en egen unik insättningsadress till Chipmixer som är en bitcoinadress och som fungerar som användarens tillfälliga ”kontonummer” hos tjänsten. Denna egna, unika och tillfälliga bitcoinadressen som skapas av Chipmixer för insättning av pengar är aktiv under 7 dagar.
Detta innebär att man har sju dagar på sig att hämta resultatet efter insättning och mixing. Normalt använder man sessionen och adressen för en (1) insättning till Chipmixer, vilket är vad som står på Chipmixers hemsida.

¹² Av Chipmixer förskapade bitcoin med fasta värden varav det lägsta är 0,001 BTC

Nationella operativa avdelningen

2023-05-10

- Användaren går därefter in i sin kryptoplånbok och skickar vald jämn summa bitcoin över 0.001BTC från plånboken till sin unika tillfälliga bitcoin-adress på Chipmixer.
- Chipmixer har ett förråd av s.k. ”chips”; tidigare skapade och sparade kryptoadresser med saldo. Dessa kommer i fasta jämna valörer varav den minsta är 0.001 BTC. Från detta förråd matchas värdet av det man satt in och användaren får tillgång till de privata nycklarna till dessa nya bitcoin-adresser.
- Användaren går in på Chipmixers websida och lägger in sitt sessions-ID för att se om mixningen är klar. Detta kan ta ca 15-30 min eller mer.
- När användaren fått tillgång till de nya privata nycklarna från Chipmixer kan pengarna från dessa adresser flyttas vidare. Detta bör ske skyndsamt då även Chipmixer har tillgång till de privata nycklarna i fråga.

Den som mixar sina bitcoins genom Chipmixer får således en egen, unik och tillfällig insättningsadress till Chipmixer när mixningen inleds.

Återanvändning av samma för användaren unika Chipmixeradress

Denna metod med att återanvända adress och sessions-ID inom 7 dagar är något som det inte informeras om på Chipmixers hemsida, utan är helt odokumenterad.

Det har testats för att se att och hur det fungerar.

Moderator Hunds och Adam Nironens gemensamma återanvändning av unik Chipmixer insättningsadress har därför kunnat användas för att knyta ihop ägande av kluster till Piraten, Hund och Adam Nironen.

Återanvändning av insättningsadress fungerar enligt följande. Så länge sessionen är aktiv, vilket är 7 dagar, kan man sätta in ytterligare bitcoin till samma unika Chipmixer adress och återfå resultatet (dvs. mixade bitcoins med motsvarande värde) genom att återanvända samma sessions-ID. **Utan sessions-ID får man inte tillgång till det mixade resultatet och förlorar det som är insatt.**

Återanvändning innebär att man bara behövt gå in i sin egen plånbok, återanvända den unika insättningsadressen från förra insättningen och därefter hämta det mixade resultatet med sitt redan tillgängliga tillfälliga och unika sessions-ID.

Resultat

Övergripande Adam Nironen

Plånböcker kopplade till Adam Nironen som får en jämn insättning på lönedatum är bildligt placerade på vänster sida om Chipmixer och plånböcker som Adam Nironen använder för att ta emot krypto(chips) från Chipmixer, presenteras på höger sida om Chipmixer.

Återskapade löneplånböcker kopplade till Adam Nironen tar emot bitcoin på vänster sida om Chipmixer, från FS3/FS3 admin och skickar in till Chipmixer.

Kluster och plånböcker på höger sida om Chipmixer, dvs efter mixning, har identifierats tillhöra Adam Nironen genom kontakt med olika växeltjänster samt genom återskapade plånböcker från Adam Nironens ipad och mobil.

Detta gäller generellt förutom för den plånbok som tar emot en jämn insättning 2019-06-25(44)¹³ från plånbok tillhörande FS3 admin men som även kopplas till Adam Nironen genom svar från kryptotjänstleverantörer dvs finns både på höger och vänster sida.

Avseende plånböcker på höger sida om Chipmixer har Adam Nironen använt överföringarna från Chipmixer till olika sammanhang såsom insättning till Crypto.com till vilket han kopplat ett betalkort, köp genom tjänsterna BitPay och BitRefill samt växlade genom CoinGate och ChangeNow.

Summering av transaktioner till och från kluster identifierade till Adam Nironen

I nedanstående tabeller ges en överblick över summor från Chipmixer till Adam Nironen och därefter vad Adam Nironen gjort med inkomna bitcoin från Chipmixer. Inkluderat är även en jämn insättning i bitcoin på lönedatum från plånbok tillhörande FS3 admin samt ojämns insättning direkt från FS3 till samma plånbok.

Tabell: BTC från Chipmixer till kluster tillhörande Adam Nironen¹⁴ genom kontakt med kryptotjänster samt växelanalys och delvis även återskapade plånböcker då de har överlappat.

Från ¹⁵	Till	Summa mottaget ca (SEK)	Antal transakt- ioner	Period
Från Chipmixer	Adam Nironen ¹⁶	713 676	232	2019-06-23 till 2022-12-22
Från FS3	Adam Nironen	3 408	1	2019-06-03
Från FS3 admin	Adam Nironen	9 534	1	2019-06-24

Summorna från FS3 och FS3 admin beror på löneplånbok AN_44 190624, som mottager jämn insättning på lönedatum från FS3 admin, används av Piraten, tar emot ojämns insättning direkt från FS3, är identifierad till Adam Nironen genom svar från växlare samt är återskapad med återställningsfras från Adam Nironens ipad.

¹³ Denna löneplånbok 190624 har även återskapats med återställningsfras från Adam Nironens ipad med löpnummer(44). Plånboken sätter även in till Chipmixer.

¹⁴ Inkluderar även två återskapade plånböcker, AN_44 från ipad och coinbasewallet (coconut -axis) från mobilen vilka identifierats till Adam Nironen genom svar från kryptotjänster

¹⁵ Måste hämtas från Chipmixer.com med de sessionsid som genererades tillsammans med respektive insättningsadress

¹⁶ Kluster identifierade till Adam Nironen genom kontakt med tjänster såsom kryptoväxlare mm.

Nationella operativa avdelningen

2023-05-10

Tabell: BTC från Adam Nironen till olika tjänster

Från ¹⁷	Till	Summa mot - taget (ca SEK)	Antal transak- tioner	Period
Adam Nironen	Bitrefill.com	347 001	145	2020-03-23 till 2023-01-03
Adam Nironen	Crypto.com	135 146	50	2020-06-19 till 2022-08-08
Adam Nironen	BitPay.com	92 082	26	2019-08-25 till 2021-06-29
Adam Nironen	CoinGate.com	81 807	42	2021-01-02 till 2022-07-31
Adam Nironen	ChangeNow.com	7 340	4	2020-06-05 till 2022-06-25
Adam Nironen	Chipmixer.com	22 626	7	2019-06-26 till 2021-07-13
Adam Nironen	3NxTrm9XgYY~	374	3	2019-06-26 till 2010-09-03
Adam Nironen	BitcoinPay.com	176	1	2019-09-12
Adam Nironen	FS3	19 658	21	2019-06-17 till 2021-09-05
Nedtagande av Chipmixer ¹⁸	Seized Assets – State of Hessen	14 009	35	2023-03-15
	Summa	720 219		

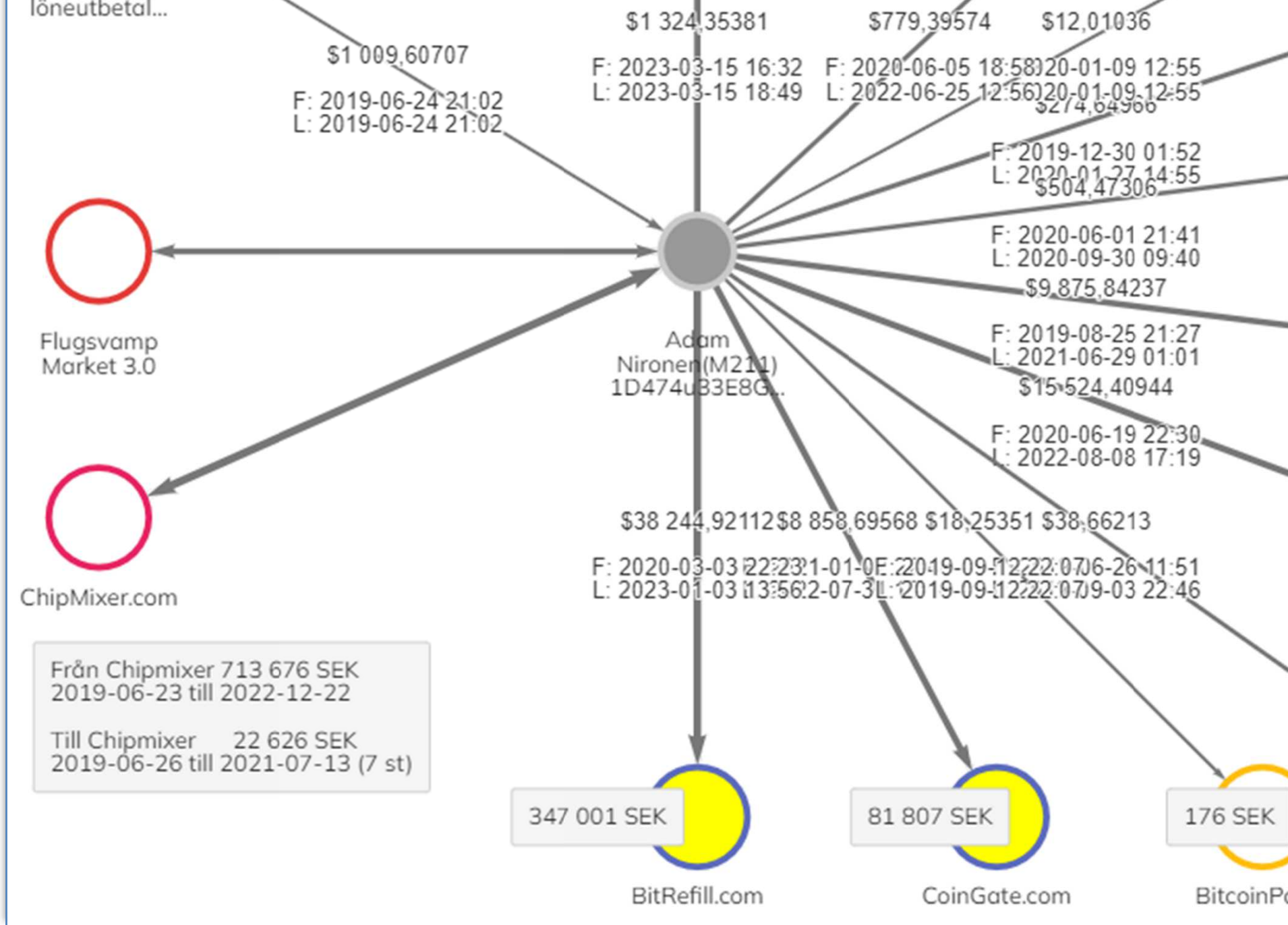
Nedan är en översiktsbild gällande ovanstående tjänster som kluster, identifierade till Adam Nironen, har interagerat med enligt blockkedjan.

¹⁷ Kluster identifierade till Adam Nironen genom kontakt med tjänster såsom kryptoväxlare mm.

¹⁸ Vid nedtagande av den illegala mixertjänsten Chipmixer beslagtogs de värden som Chipmixer fortfarande hade access till genom tillgång till de privata nycklarna därav Seized Assets – State of Hessen.

Nationella operativa avdelningen

2023-05-10



Nationella operativa avdelningen

2023-05-10

Bilagor

- 1 Bilaga_till 3Nx.xlsx
- 2 Bilaga_till BitcoinPay_com.xlsx
- 3 Bilaga_till BitPay_com.xlsx
- 4 Bilaga_till Bitrefill_com.xlsx
- 5 Bilaga_till Coingate.xlsx
- 6 Bilaga_till CoinGate_com.xlsx
- 7 Bilaga_till Crypto_com.xlsx
- 8 Bilaga_till S3.xlsx

Adam_Hund_Piraten_Löneadresser.xlsx



Polisen

PM1 (14) **HEMLIG**

Datum

2023-05-07

Diariennr (åberopas)

5000-K615323-19

Polismyndigheten
Utredningsenheten
Nationellt it-brottscentrum
Teknisk inhämtning

PM OP Hydra - Kryptospårning löneutbetalningar och demixing avseende de återskapade plånböckerna 190725(72), 100824(93), 190924(86), 191124(45) samt AN_77 gällande moderator Hund och Adam Nironen.

Syfte

Syftet med detta PM är att beskriva de kryptofinansiella observationer och analyser som gjorts i ärendet gällande Adam Nironen(Adam) och hans kopplingar till moderator Hund och FS3 gällande den ytterligare plånboken med löpnummer 77 som identifierats med hjälp av återställningsfraser från beslag av Adam Nironens ipad.

Innehåll

Syfte	1
Bakgrund.....	2
Källor	2
Sammanfattning	2
Tillvägagångssätt	3
Resultat	4
Transaktion avseende inhämtade chips från Chipmixer till plånbok AN_77	4
Inkommande transaktioner till plånbok AN_77 från kluster identifierade till Adam Nironen.....	4
Utvecklad plånbok AN_77 bc1q9e60p2c med plånbokens alla transaktioner	6
Förenklad och sammanslagen plånbok AN_77 med utvalda transaktioner	7
Transaktion från plånbok AN_77 till FS3 3CyXtW4YGZ2N~ i ett sammanhang	8
Transaktion från plånbok AN_77 och AN_5 till Chipmixeradress 14GneXpHZYxrzw~	9
Demixning av insättning till Chipmixer	10
Chipmixer insättningsadress med sessiontoken/id.....	10
Demix av två insättningsadresser.....	11
Demix samt plånboken i sin helhet.....	13

Bakgrund

En återställningsfras är en värdehandling vilken ger tillgång till värdet och för att kunna genomföra transaktioner i plånboken.

Analyserade plånböcker i detta PM är återskapade utav återställningsfraser från Adam Nironens ipad.¹ samt baserade på svar från kryptotjänsten BitPay.com

Då Chipmixer i stor utsträckning har använts för att dölja härkomsten har analys gjorts avseende demixing där det i detta PM är plånbok från Adam Nironens ipad med löpnummer 77 som är i fokus.

Demixingen är probabilistisk då kopplingen gjorts genom att matcha tid och summa in och ut ur Chipmixer, ej genom att följa transaktioner genom blockkedjan.

Löneplånböckerna 19-07-25, 19-08-24, 19-09-24 samt 19-11-24 finns analyserade i ”PM Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen”.

Plånböcker som tar emot jämn insättning på lönedatum benämns löneplånböcker annars är de benämnda med löpnummer knutet till återställningsfras.

Källor

- PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen.
- Återställning av plånböcker från beslag BG3418-5
- Svar från kryptoväxlare BitPay
- Bild på Chipmixeradress 17b6TsaM8FKmAK3XMtcRLhdbKQWJBjMdtU samt tillhörande-sessionid/token²

Sammanfattning

Denna plånbok får insättningar Chipmixer och från kluster identifierade till Adam Nironen genom BitPay samt sätter in till FS3 köpkonto med insättningsadress 3CyXtW4YGZ2NL1s~.

Denna FS3 insättningsadress nyttjas endast av Adam Nironen samt plånböcker som återskapats från Adam Nironens ipad varav en plånbok bedöms fått lön i rollen som moderator Hund.

Det har probabilistisk gjorts en demixing från följande återskapade löneplånböcker³: 190725, 190824⁴, 190924 samt 191124, genom Chipmixer och ut till återskapade plånbok, AN_77 bc1q9e60p2c.

¹ Namngivningen på plånböcker är dels baserad på datum för inkommande jämn insättning på lönedatum dels beroende på löpnummer på återställningsfras.

² Se avsnitt ”Sammankoppling av ägande genom insättning till Chipmixer” i PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen”. I beslag från Adam Nironens ipad kan man se en bild från Chipmixer med insättningsadress och tillhörande sessionid (token). Bild: 2023-5000-BG3416-5 1AE27E09-FF67-417D-AEDD-C5258E83D2FF.JPG

³ Se PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen.

⁴ Löneplånböckerna 190824 och 190924 är bekräftade löneplånböcker tillhörande moderator Hund.

Nationella operativa avdelningen

2023-05-11

Användning av den odokumenterade metoden att återanvända den för användaren unika och tillfälliga Chipmixeradressen såsom moderator Hund samt Adam Nironen identifierats göra.

Återanvändning av Chipmixeradress sammankopplar de återskapade plånböckerna AN_77 och AN_5 dessutom är de bägge återskapade med återställningsfraser från Adam Nironens ipad.

Ovanstående tyder på att Adam Nironen är moderator Hund.

Tillvägagångssätt

Plånböckerna och identifierade kluster har analyserats med fokus på:

- varifrån krypto till plånboken kommer ifrån och vart det tar vägen
- när och hur mycket som emottagits
- vad har skickats till Chipmixer från redan identifierade löneplånböcker till plånböcker identifierade på höger sida om Chipmixer.

Blå pilar - Representerar växel vilket innebär att kluster som är sammankopplade med blå pilar tillhör samma plånbok.

Nationella operativa avdelningen

2023-05-11

Resultat

Transaktion avseende inhämtade chips från Chipmixer till plånbok AN_77

2019-09-25 kl 01:31 hämtas chips från Chipmixer till ett värde av 0,04 BTC vilket efter transaktionskostnad blir 0,03992114 BTC och läggs i plånboken AN_77 bc1q9e60p2c~ vilket är första transaktionen till plånboken.

Datomet 2019-09-10 23:53 är irrelevant för analysen då det härrör sig från när chipsen⁵ skapades.

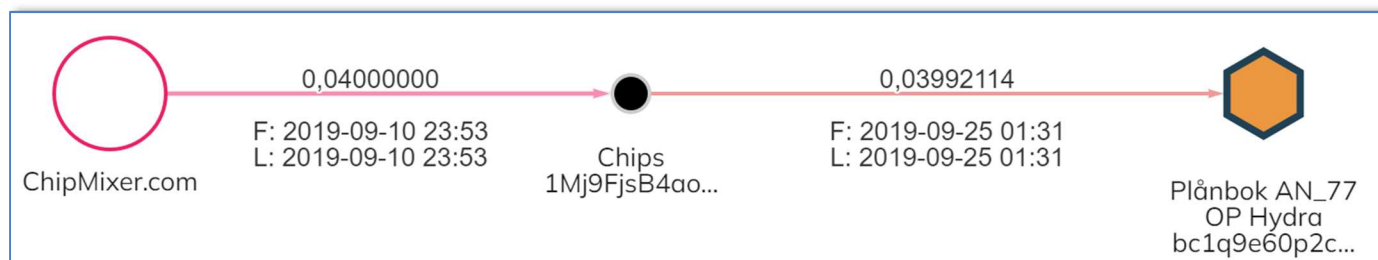


Bild: Inkommande transaktion från Chipmixer till plånbok AN_77

Inkommande transaktioner till plånbok AN_77 från kluster identifierade till Adam Nironen

Denna återskapade plånbok emottar även tömningar från andra plånböcker identifierade till Adam Nironen⁶.

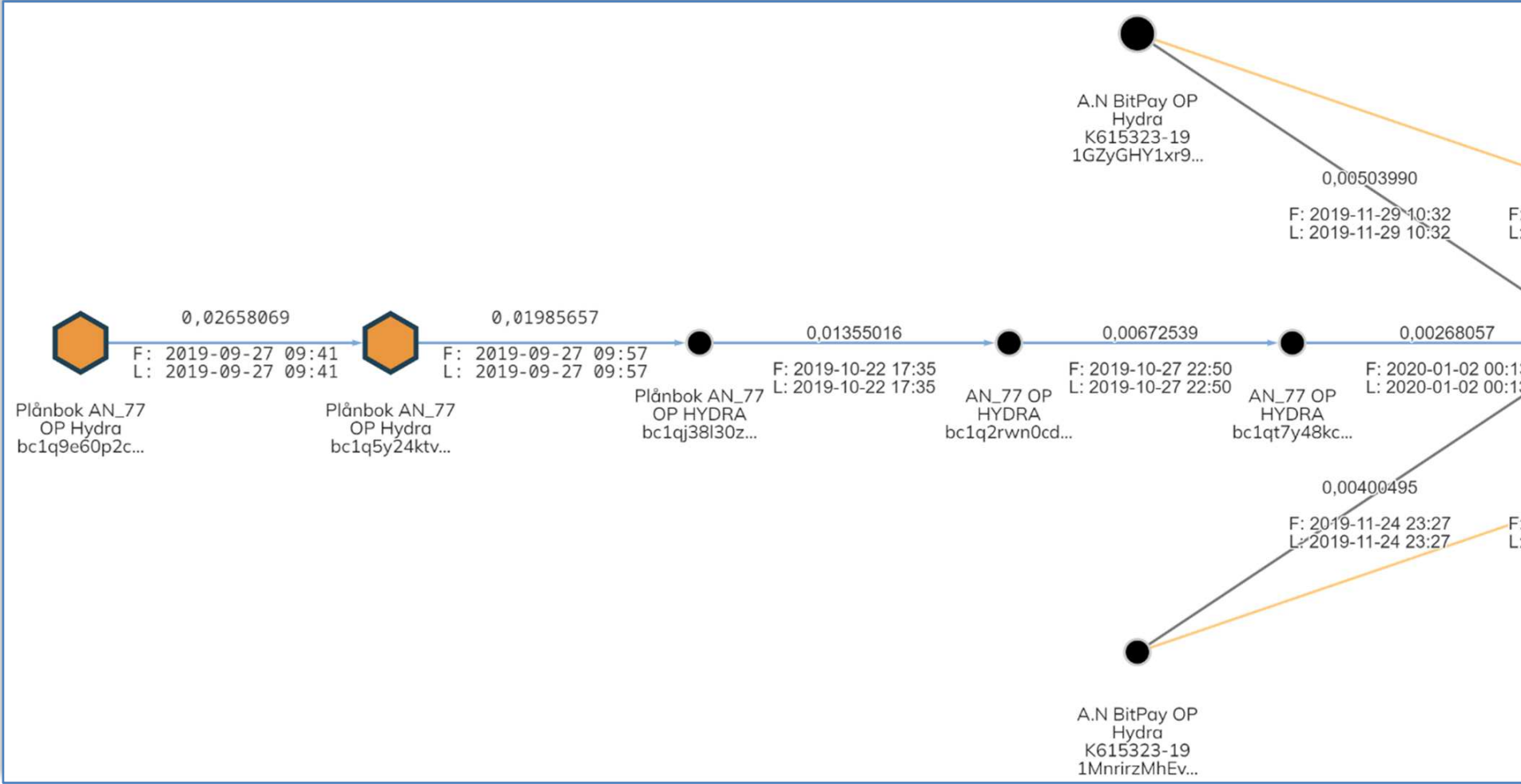
Efter respektive insättning till BitPay töms dessa två plånböcker till AN_77 genom två insättningar 2019-11-29 10:32 samt 2019-11-24 23:27.

⁵ Av Chipmixer förskapade fasta värden av bitcoin som finns i deras "förråd" av bitcoin

⁶ Identifierade genom svar från BitPay.com

Nationella operativa avdelningen

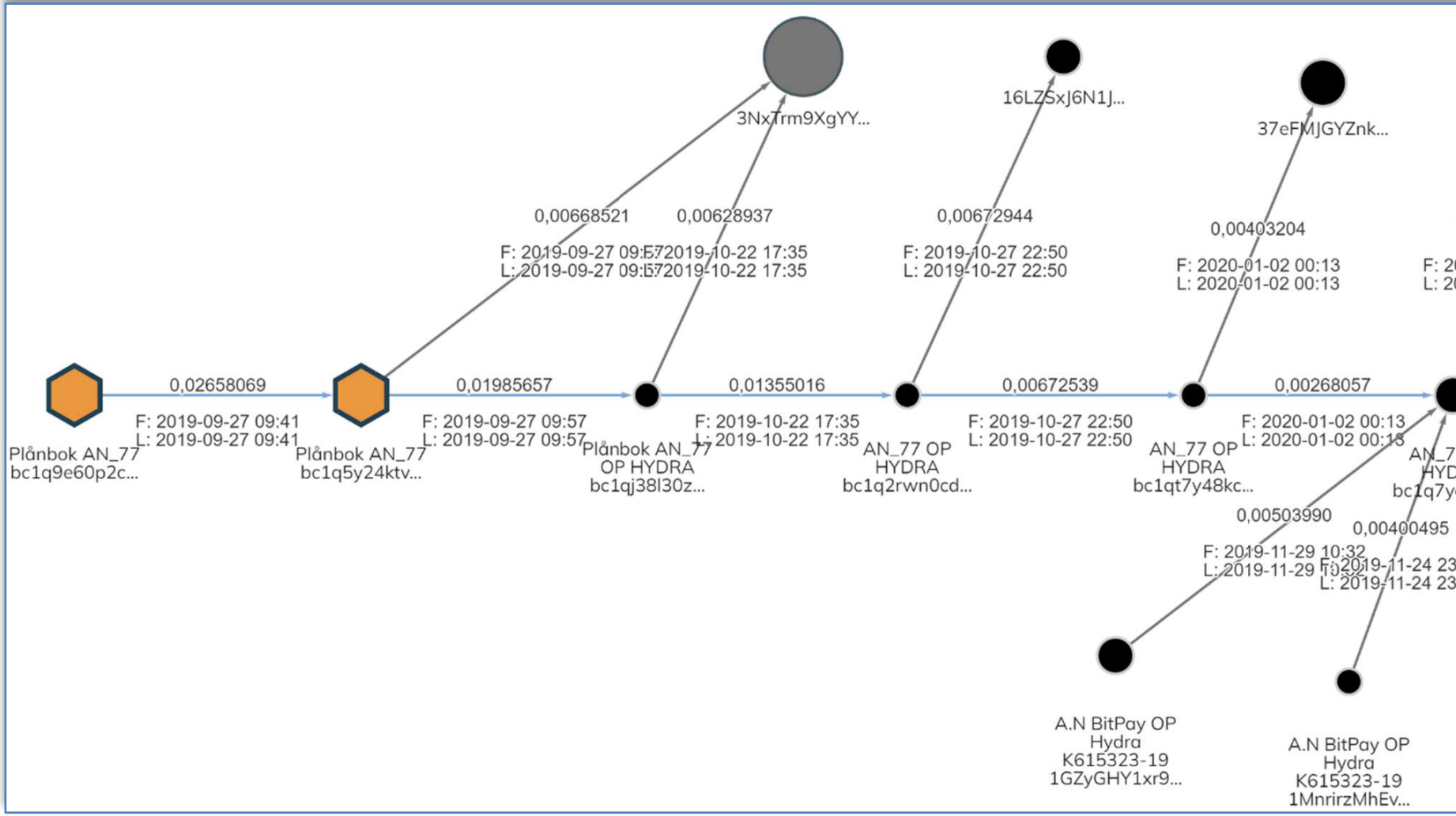
2023-05-11



Nationella operativa avdelningen

2023-05-11

Utvecklad plånbok AN_77 bc1q9e60p2c med plånbokens alla transaktioner



Förenklad och sammanslagen plånbok AN_77 med utvalda transaktioner

Plånbok AN_77 med alla tillhörande adresser sammanslagna i ett kluster med inkommande transaktioner samt tre av de viktigaste utgående transaktionerna från plånboken.

Plånboken hämtar chips från Chipmixer identifierade till Adam Nironen samt skickar transaktioner till:

- den okända tjänsten 3NxTrm9XgYY~
- till Chipmixer med adress 14GneXpHZYx~ som även plånbok AN_5 skickar till.
- FS3 med insättningsadress 3CyXtW4YGZ2~
- samt ett par andra tjänster ej i bild.

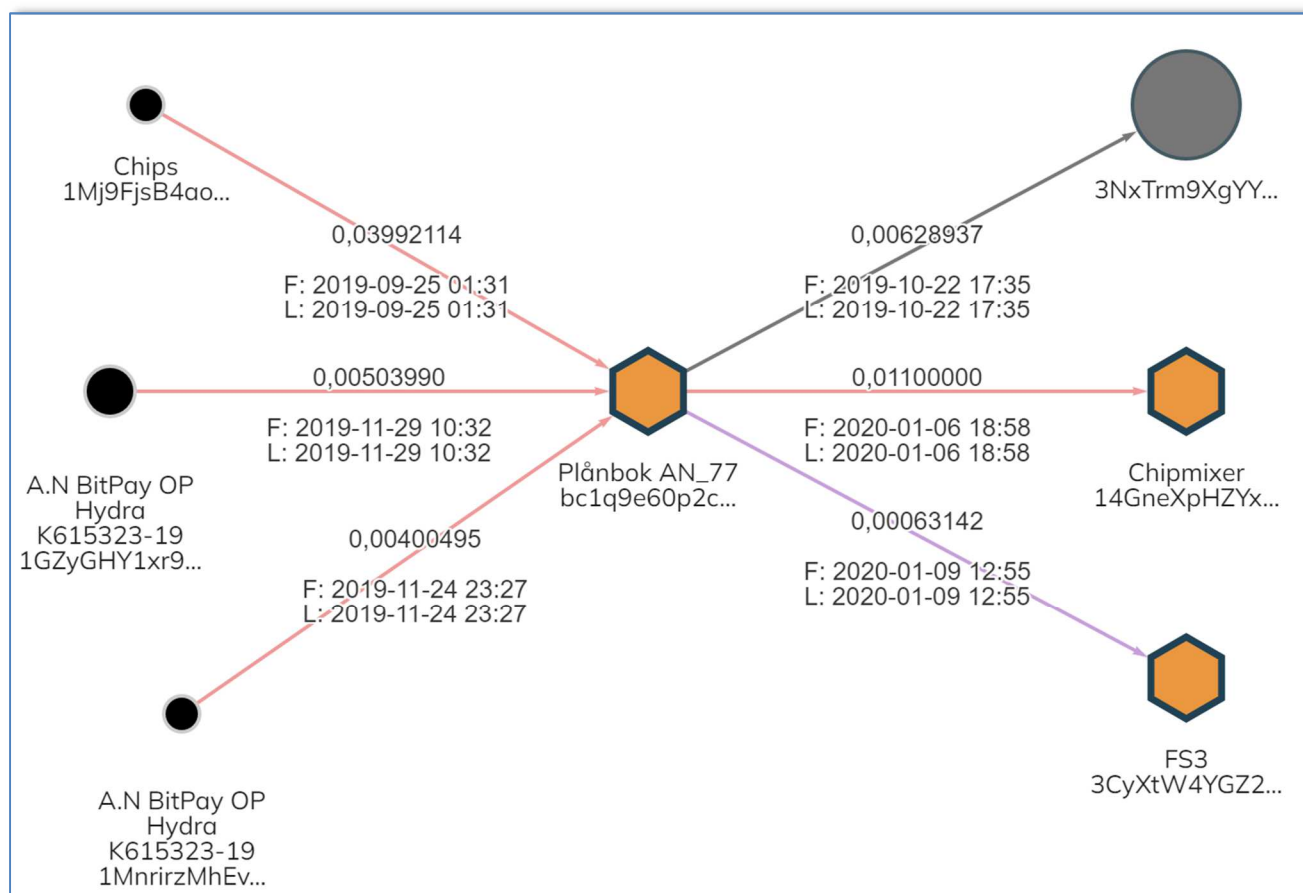


Bild: Transaktioner in och ut från återskapade plånbok AN_77

Nationella operativa avdelningen

2023-05-11

Transaktion från plånbok AN_77 till FS3 3CyXtW4YGZ2N~ i ett sammanhang

Plånbok AN_77 töms genom insättning till köpkonto på FS3 med insättningsadress 3CyXtW4YGZ2NL1sAJC1s5DU7h3h7qcbXQS

Denna FS3 insättningsadress har endast insättningar från andra återskapade plånböcker från Adam Nironens ipad varav två bedömt är knutna till lön till moderator Hund, samt från ett kluster identifierat till Adam Nironen genom BitPay.

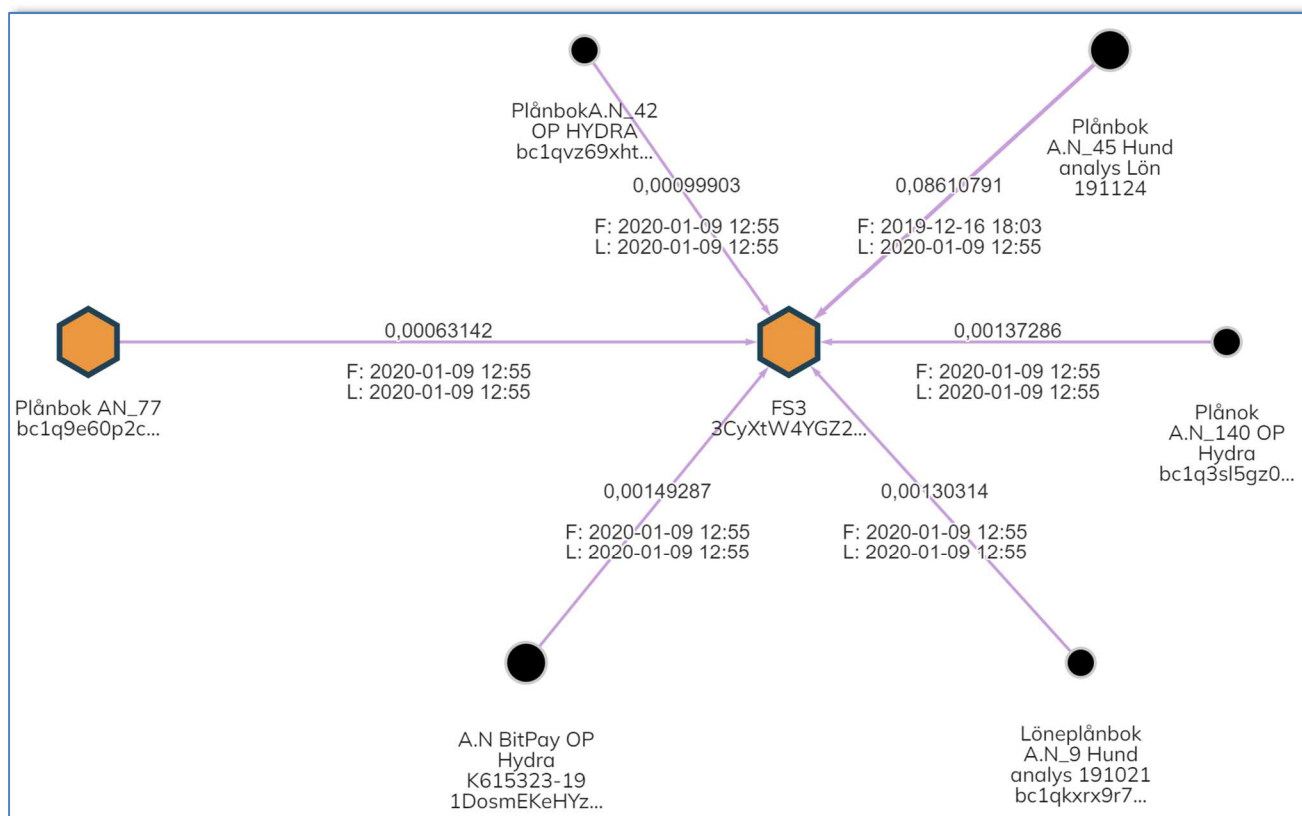


Bild: Alla transaktioner till FS3 insättningsadress 3CyXtW4YGZ2N~

Nationella operativa avdelningen

2023-05-11

Transaktion från plånbok AN_77 och AN_5 till Chipmixeradress 14GneXpHZYxrzw~

Här sker en återanvändning av Chipmixeradress 14GneXpHZYxrzw~ vilket vi sett i samband med moderator Hund samt Adam Nironen.

Återanvändning av Chipmixeradress 14GneXpHZYxrzw~ sker från två återskapade plånböcker⁷.

Från återskapade plånbok AN_77 skickas 2020-01-06 0,011 BTC till Chipmixeradress 14GneXpHZYxrzw~.

Till denna för användaren unika och tillfälliga adress 14GneXpHZYxrzw~ sätts det även in 2020-01-06 0,137 BTC från den återskapade plånboken AN_5 med adress bc1qf5lj724v6kca2pktrg0vyr3uxgdc54lx2ceqqk.

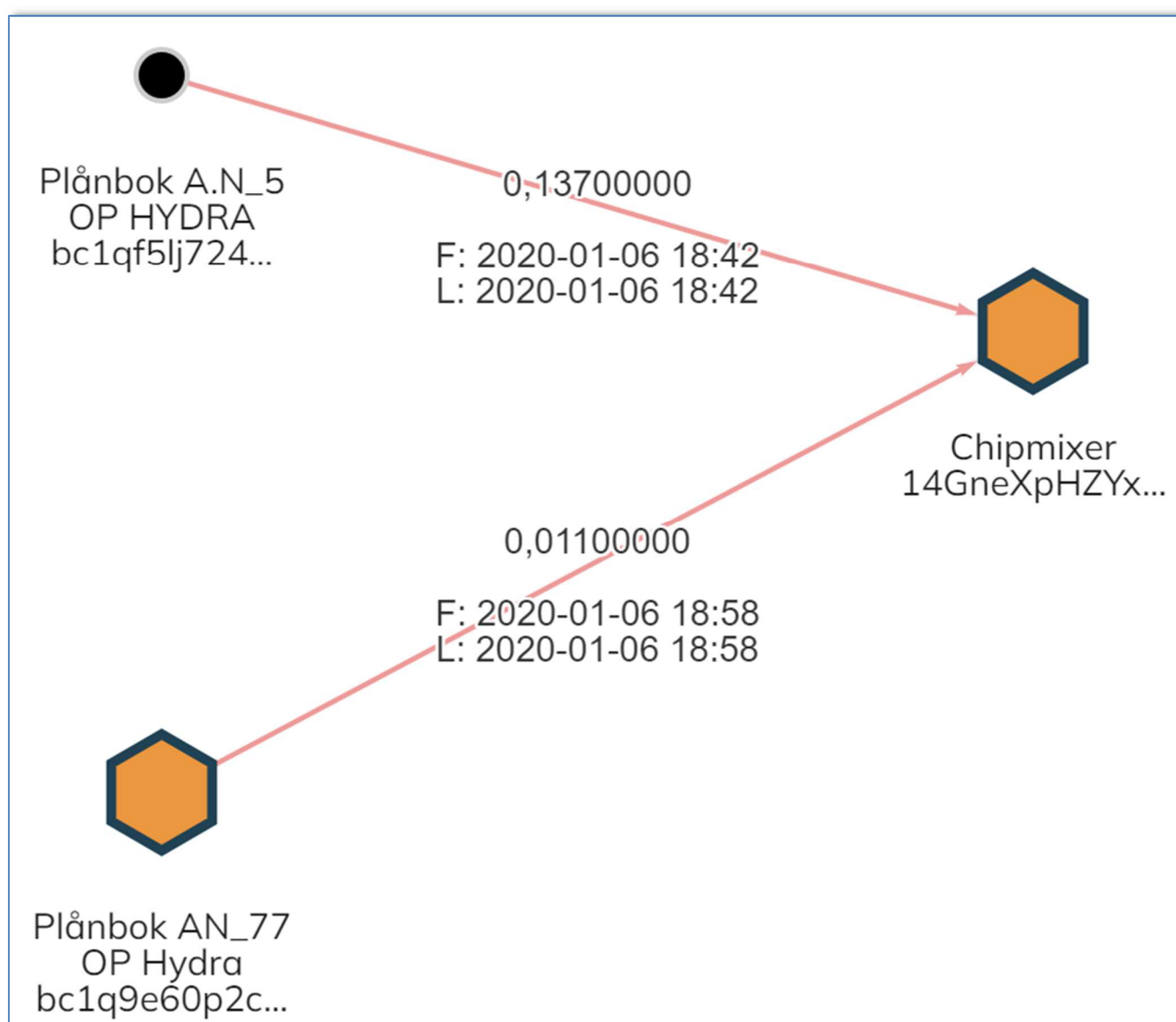


Bild: Återanvändning av Chipmixeradress

⁷ Återställningsfraser från Adam Nironens ipad med löpnummer 5 respektive 77.

Nationella operativa avdelningen

2023-05-11

Demixning av insättning till Chipmixer**Chipmixer insättningsadress med sessiontoken/id⁸**

Följande bild med insättningsadress och tillhörande session token/id till Chipmixer har påträffats på Adam Nironens ipad⁹.

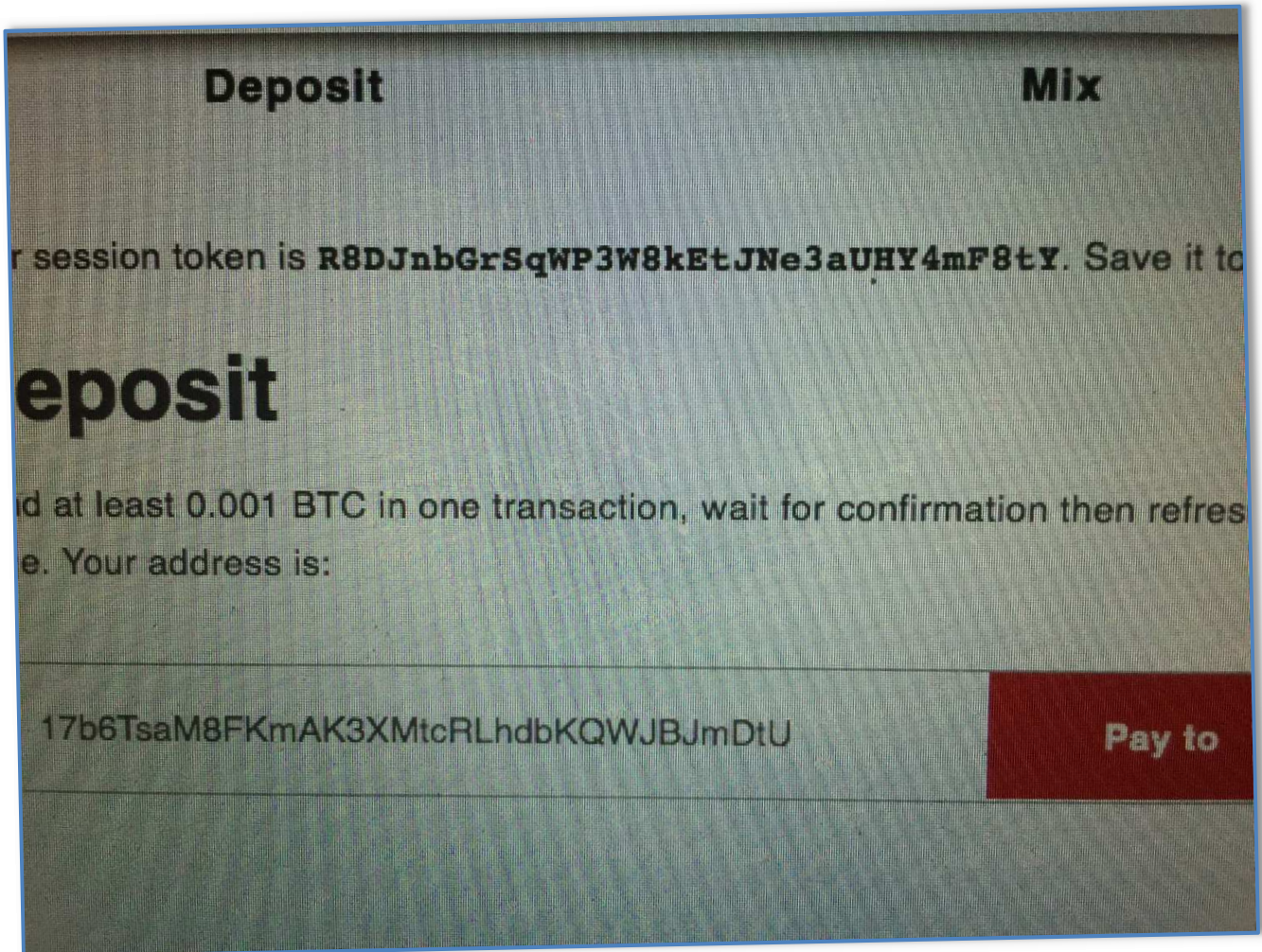


Bild: Chipmixer insättningsadress med sessiontoken (sessionid)

⁸ Se avsnitt "Sammankoppling av ägande genom insättning till Chipmixer" i PM OP Hydra - Kryptospårning löneutbetalningar gällande moderator Hund på FS3 Flugforum samt användare Piraten med tillhörande kopplingar till Adam Nironen.

⁹Bild: 2023-5000-BG3416-5 1AE27E09-FF67-417D-AEDD-C5258E83D2FF.JPG

Demix av två insättningsadresser

Blå ruta 1 och 2

Från de **tre återskapade löneplånböckerna 190725, 190824, 190924** varav två av dessa är bekräftade¹⁰ tillhöra moderator Hund genom flugforum görs tre insättningar till den för användaren unika och tillfälliga Chipmixeradressen 17b6TsaM8FKmAK3XMtcRLhdbKQWJBjMdU

2019-09-25 01:18 med 0,02 BTC

2019-09-25 01:18 med 0,01 BTC

2019-09-25 01:18 med 0,01 BTC

Summa 0,04 BTC

Alla tre löneplånböckerna är återskapade med återställningsfras från Adam Nironens ipad. Chipmixer insättningsadressen tillsammans med sessionid finns fotad i beslag¹¹.

Blå ruta 3 och 4

Möjlig demix från Chipmixer i bilden, är chips till ett värde av 0,04 BTC när de hämtas från Chipmixer

2019-09-25 01:31 hämtas chips¹² till ett värde av 0,04 BTC till en plånbok AN_77, återskapad med återställningsfras med löpnummer 77 från Adam Nironens ipad.

Grön ruta 1 och 2

Från **återskapade löneplånboken 191124 (45)** görs två insättningar till Chipmixeradressen 16UjLH9ex1oXeTe1bv5SK65iXR48NGBumq

2019-11-26 22:18 med 0,055 BTC

2019-11-28 01:51 med 0,01 BTC

Grön ruta 3 och 4

Möjlig leverans från Chipmixer i bilden, är chips till ett värde av 0,065 BTC när de hämtas från Chipmixer

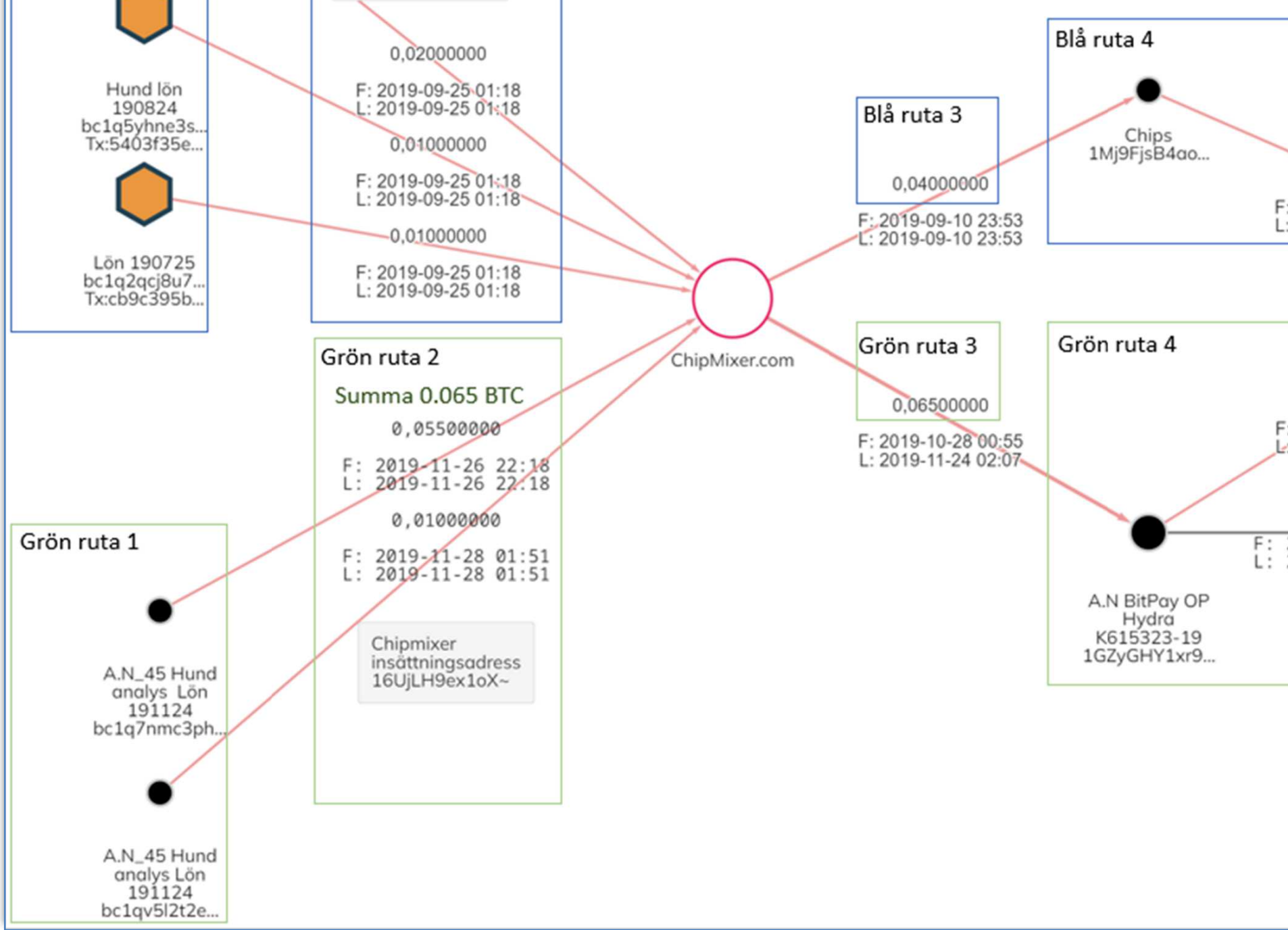
2019-11-28 02:09 med 0,05947700 BTC kopplad till Adam Nironen

2019-11-29 10:32 med 0,00503990 BTC till en återskapad plånbok från ipad med löpnummer 77

¹⁰ 190824, 190924

¹¹ Bild: 2023-5000-BG3416-5 1AE27E09-FF67-417D-AEDD-C5258E83D2FF.JPG

¹² Av Chipmixer förskapade fasta värden av bitcoin



Demix samt plånboken i sin helhet

Blå ruta 1 och 2

Tre löneplånböcker, 190725, 190824, 190924 varav två av dessa dessutom är bekräftade¹³ genom flugforum tillhörande moderator Hund sätter tillsammans in **0,04 BTC 2019-09.25 kl 01:18** till den för användaren unika och tillfälliga Chipmixer adressen 17b6TsaM8FKm~.

Alla tre löneplånböckerna är återskapade med återställningsfras från Adam Nironens ipad. Chipmixer insättningsadressen tillsammans med sessionid finns fotad i beslag¹⁴.

Blå ruta 3 och 4

Klockan **2019-09-25 01:31 hämtas chips¹⁵ till ett värde av 0,04 BTC** till en plånbok AN_77, åter-skapad från Adam Nironens ipad med löpnummer 77.

Till denna plånbok, AN_77, töms två kluster identifierade till Adam Nironen.

Lila ruta 1

Plånbok AN_77 töms genom insättning till köpkonto på FS3 som endast har insättningar från andra återskapade plånböcker från Adam Nironens ipad samt ett kluster identifierat till Adam Nironen genom BitPay.

Grön ruta 1 och 2.

Två kluster från löneplånbok 191124 sätter tillsammans in **0,065 BTC** genom två insättningar varav den senare sker **2019-11-28 kl 01:51** till den för användaren unika och tillfälliga Chipmixer adressen 16UjLH9ex1oX~

Löneplånboken 191124 är återskapad med återställningsfras från Adam Nironens ipad med löpnummer 45.

Grön ruta 3 och 4.

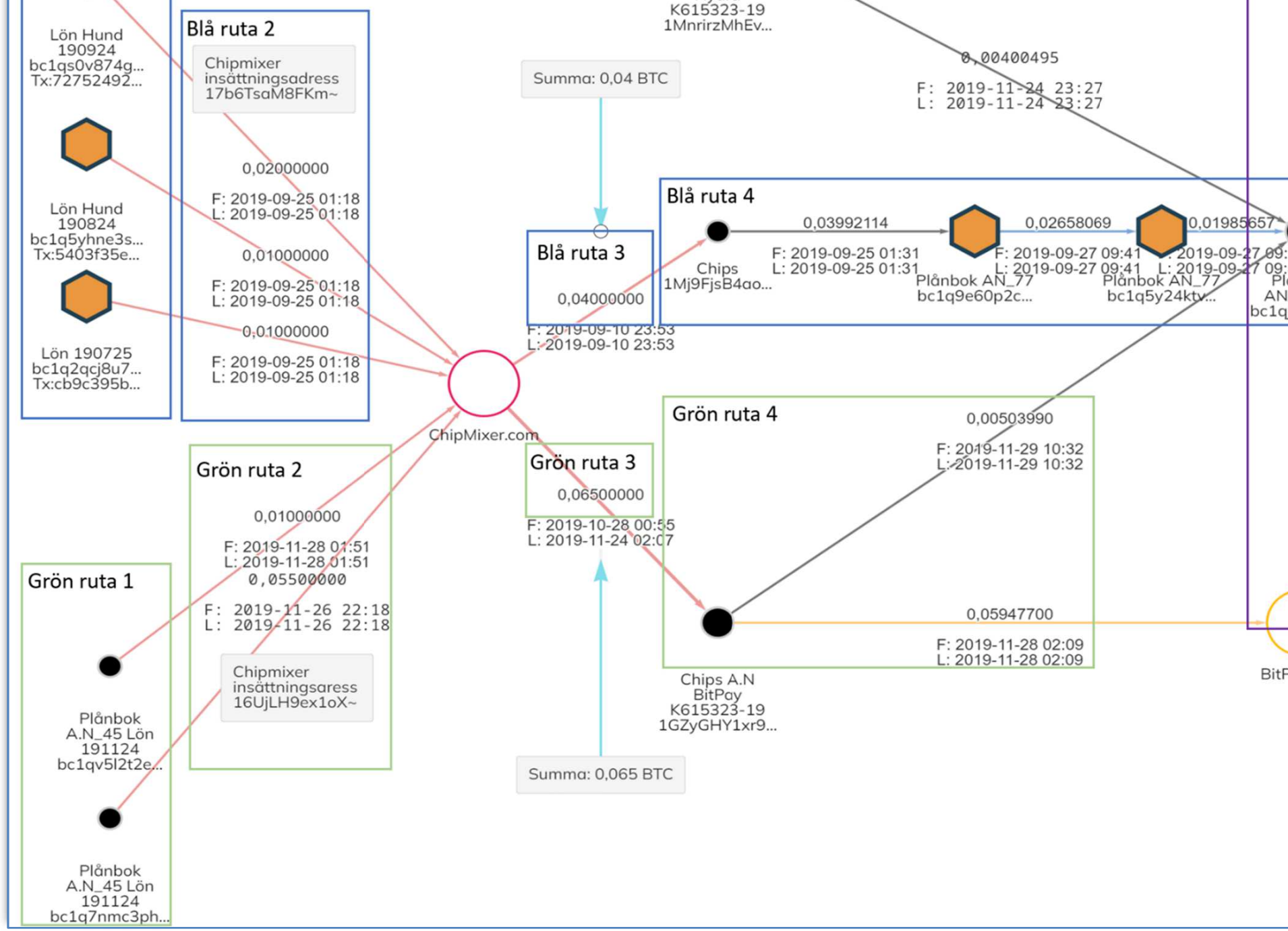
Klockan **2019-11-28 02:09 hämtas chips till ett värde av 0,65¹⁶** genom insättning till BitPay varav det därefter töms dagen efter 2019-11-20 10:32 med en överföring till den återskapade plånboken med löpnummer 77.

¹³ 190824, 190924

¹⁴ Bild: 2023-5000-BG3416-5 1AE27E09-FF67-417D-AEDD-C5258E83D2FF.JPG

¹⁵ Av Chipmixer förskapade fasta värden av bitcoin

¹⁶ $0,00503990 + 0,05947700 = 0,0645169$ BTC





Polisen

HEMLIG

127

Bilaga - Skäligen misstänkt

Enhet

Nationella Operativa Avdelningen, Komplexa cyberbrott (KCB) 1 NIB NOA

Diariernr

5000-K615323-19

Skäligen misstänkt person

Kronberg, Fredrik Ulf Julius

Personnr

19830208-0778

Identifierad

Ja

Kontroll sätt

Annat

Kommentar

Känd av utredare

Personalia och dagsbottsuppgift

Utskriftsdatum
2023-05-22

Namn Kronberg, Fredrik Ulf Julius		Personnummer 19830208-0778	
Tilltalsnamn Fredrik	Kallas för	Öknamn	Kön Man
Födelseförsamling Oscar	Födelselän Stockholms län	Födelseort utland	
Medborgarskap Sverige	Hemvistland	Telefonnr 0709998098: Mobiltelefon	
Postadress [REDACTED] [REDACTED]			
Folkbokföringsort [REDACTED]			
Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)			
Utbildning			
Yrke / Titel			
Arbetsgivare		Telefonnr	
Anställning (nuvarande och tidigare)			
Arbetsförhet och hälsotillstånd			
Kompletterande uppgifter			
Uppgiven inkomst 150000	Bidrag 0	Hemmavarande barn under 18 år	
Försörjningsplikt		Skulder 0	
Förmögenhet			
Kontroll utförd			
Taxerad inkomst		Taxeringsår	
Taxeringskontroll utförd av		Datum - -	



Polisen

HEMLIG

129

Bilaga - Skäligen misstänkt

Enhet

Nationella Operativa Avdelningen, Komplexa cyberbrott (KCB) 1 NIB NOA

Diariens

5000-K615323-19

Skäligen misstänkt person

Nederman, Hampus Helge

Personnr

19930419-2991

Identifierad

Ja

Kontrollsätt

Nationellt ID-kort

Kommentar



Polisen

HEMLIG

130

Personalia och dagsbottsuppgift

Utskriftsdatum
2023-05-22

Namn Nederman, Hampus Helge		Personnummer 19930419-2991	
Tilltalsnamn Hampus	Kallas för	Öknamn	Kön Man
Födelseförsamling Långbro	Födelselän Örebro län	Födelseort utland	
Medborgarskap Sverige	Hemvistland	Telefonnr	
Postadress Stånggatan 6 D 703 46 Örebro			
Folkbokföringsort Örebro			
Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)			
Utbildning			
Yrke / Titel			
Arbetsgivare		Telefonnr	
Anställning (nuvarande och tidigare)			
Arbetsförhet och hälsotillstånd			
Kompletterande uppgifter			
Uppgiven inkomst 100000	Bidrag 0	Hemmavarande barn under 18 år 0	
Försörjningsplikt		Skulder 0	
Förmögenhet 0			
Kontroll utförd Taxerad inkomst 86500		Taxeringsår 2020	
Taxeringskontroll utförd av PA Patrich Kung		Datum 2022-03-22	



Polisen

HEMLIG

131

Bilaga - Skäligen misstänkt

Enhet

Nationella Operativa Avdelningen, Komplexa cyberbrott (KCB) 1 NIB NOA

Diariennr

5000-K615323-19

Skäligen misstänkt person

Ihrén Nironen, Adam Antti

Personnr

19940119-7554

Identifierad

Ja

Kontrollsätt

Annat

Kommentar

Genom utredning fastställt



Polisen

HEMLIG

Underrättelse/Delgivning jml RB 23:18a

Enhet

Nationella Operativa Avdelningen, Komplexa cyberbrott (KCB) 1 NIB NOA

Ärende

Diariennr

5000-K615323-19

Underrättad av

Keyzer, Jim

Gärning

Synnerligen grovt narkotikabrott Fullbordat, Stockholm Stockholm, mellan 2018-12-17 och -

Berörd person

Personnr

19930419-2991

Efternamn

Nederman

Förnamn

Hampus Helge

Underrättelsesätt

Underrättelse genom vanlig delgivning

Delgiven info. om ev. förenklad delgivning

2023-01-26

Datum utsänd

2023-05-11

Yttrande senast (rådrum)

2023-05-26

Notering

Resultat av slutunderrättelse

Information gällande erinran

Försvare

Namn

Ataseven, Metin

Underrättelsesätt

Skriftlig underrättelse

Datum utsänd

2023-05-11

Yttrande senast (rådrum)

2023-05-26

Notering

Resultat av slutunderrättelse

Information gällande erinran

**HEMLIG**

Underrättelse/Delgivning jml RB 23:18a

Enhet

Nationella Operativa Avdelningen, Komplexa cyberbrott (KCB) 1 NIB NOA

Ärende

Diariennr

5000-K615323-19

Underrättad av

Siklosi, Göran

Gärning

Bokföringsbrott Fullbordat, Stockholm Stockholm, mellan 2019-12-12 00:00 och 2021-08-25 00:00

Grovt penningtvättsbrott Fullbordat, [REDACTED] mellan 2019-12-12 och 2021-08-25

Synnerligen grovt narkotikabrott Fullbordat, Stockholm Stockholm, mellan - och 2021-11-09

Berörd person

Personnr

19830208-0778

Efternamn

Kronberg

Förnamn

Fredrik Ulf Julius

Underrättelsesätt

Underrättelse genom vanlig delgivning

Datum utsänd

2023-05-11

Yttrande senast (rådrum)

2023-05-26

Notering

Resultat av slutunderrättelse

Information gällande erinran

Försvare

Namn

Awrohum, Kinora

Underrättelsesätt

Skriftlig underrättelse

Datum utsänd

2023-05-11

Yttrande senast (rådrum)

2023-05-26

Notering

Mejlat

Resultat av slutunderrättelse

Information gällande erinran



Polisen

HEMLIG

Underrättelse/Delgivning jml RB 23:18a

Enhet

Nationella Operativa Avdelningen, Komplexa cyberbrott (KCB) 1 NIB NOA

Ärende

Diariernr

5000-K615323-19

Underrättad av

Siklosi, Göran

Gärning

Synnerligen grovt narkotikabrott Fullbordat, Stockholm Stockholm, mellan 2019-06-02 och -

Berörd person

Personnr

19940119-7554

Efternamn

Nironen

Förnamn

Adam Antti

Underrättelsesätt

Underrättelse genom vanlig delgivning

Datum utsänd

2023-05-11

Yttrande senast (rådrum)

2023-05-26

Notering

Resultat av slutunderrättelse

Information gällande erinran

Försvare

Namn

Svantemark, Nils

Underrättelsesätt

Skriftlig underrättelse

Datum utsänd

2023-05-11

Yttrande senast (rådrum)

2023-05-26

Notering

Mejlat

Resultat av slutunderrättelse

Information gällande erinran