

How Lazarus Group laundered \$200M from 25+ crypto hacks to fiat from 2020–2023

By

ZachXBT

Table of contents

Introduction-----3

CoinBerry, Unibright, & CoinMetro hacks-----4

Nexus Mutual founder hack-----8

EasyFi hack-----16

Bondly hack-----23

Unreported hacks-----28

MGNR and PolyPlay hacks-----30

bZx hack-----36

Steadefi and CoinShift hacks-----40

Paxful and Noones accounts-----46

Investigation results-----49

Other Incidents-----50

Acknowledgments-----54

Sources-----55

Introduction

Bluenoroff or APT38, more commonly referred to as Lazarus Group is a threat group which has been tied to the North Korean government since as early as 2009 primarily being financially motivated utilizing malware custom built for each target.

Early on, the threat group gained notoriety for cyberattacks such as [Sony Pictures Hack](#) in 2014 and \$81M [Bangladesh Bank heist](#) in 2016 and in more recent years has shifted focus to targets in the cryptocurrency industry.

Analytics firms such as [TRM](#) and [Chainalysis](#) release annual reports summarizing crypto related incidents linked to DPRK and since 2017 they estimate between \$3B to \$4.1B has been stolen.

The research in this article closely follows 25 hacks targeting companies and individuals in the cryptocurrency space spanning from August 2020 to October 2023 by tracing the movements of funds to multiple accounts identified at P2P marketplaces where Lazarus Group exchanges stolen crypto for fiat.

Victim	Date	Amount
Hobocrypt	Aug-18-2020	\$134K
FET Holder	Aug-20-2020	\$1.1M
Coinberry	Aug-24-2020	\$370K
Unibright	Sep-11-2020	\$400K
Coinmetro	Oct-6-2020	\$740K
Nexus Mutual founder	Dec-14-2020	\$8M
Indodax User	Jan-22-2021	\$2.8M
Mudge	Apr-2-2021	\$1M
EasyFi founder	Apr-19-2021	\$81M
FinNexus	May-17-2021	\$7M
Bondly Finance	Jul-14-2021	\$8.5M
LINA holder	Aug-6-2021	\$750K
TECH holder	Sep-2-2021	\$145K
mgnr.io	Oct-8-2021	\$24.1M
Polyplay	Oct-28-2021	\$1.6M
YFETH Deployer	Nov-1-2021	\$200K
bZx	Nov-3-2021	\$55M
Wonderhero	Nov-11-2021	\$1M
ANKR founder	Jan-27-2022	\$1.2M
Arthur0x	Mar-22-2022	\$1.7M
GeraCoin	Sep-7-2022	\$142K
Algorand	Oct-11-2022	\$750K
Darshan	Oct-17-2022	\$1.75M
Steadfi	Aug-7-2023	\$1.2M
Coinshift	Aug-16-2023	\$1.7M
Maverick founder	Oct-26-2023	\$8.8M

Table 0: Lazarus Group hacks from 2020–2023 covered in this article

2020—CoinBerry, Unibright, & CoinMetro Hacks

CoinBerry Incident Summary

On August 24, 2020 the Canadian crypto exchange CoinBerry stopped processing withdrawals for 12+ hrs after \$370K was drained from the Bitcoin and Ethereum hot wallets. While the exchange never publicly reported the incident, a [lawsuit](#) filed in 2022 revealed a [software bug](#) allowed 500 users to withdraw 120 BTC in 2020.

Theft address

0xA06957c9C8871ff248326A1DA552213AB26A11AE

1KcTk7kJMjYaCV3FXo5bZpjaZs2aK18ntz

Unibright Incident Summary

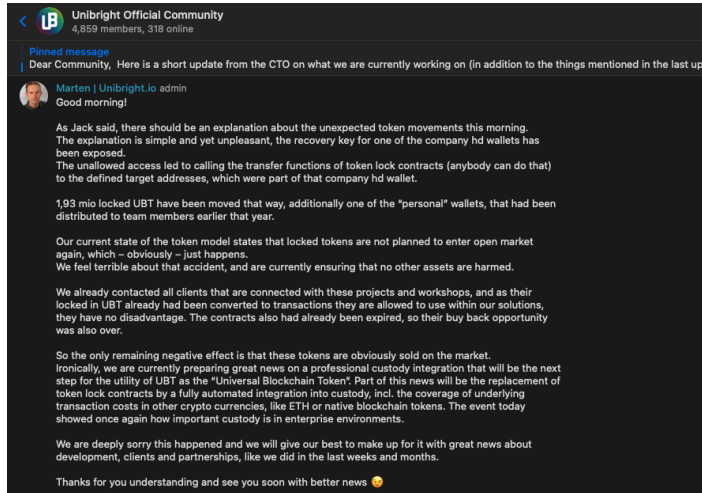
On September 11, 2020 the Unbright team noticed unauthorized transfers of \$400K from multiple wallets controlled by the team as the result of a private key compromise. The attacker immediately swapped the assets for ETH on decentralized exchanges.

Theft address

0x6C6357F30FCc3517c2E7876BC609e6d7d5b0Df43



Source: <https://twitter.com/Sjaaaakster/status/1304531302255910912>



Source: https://t.me/unibright_io/211959

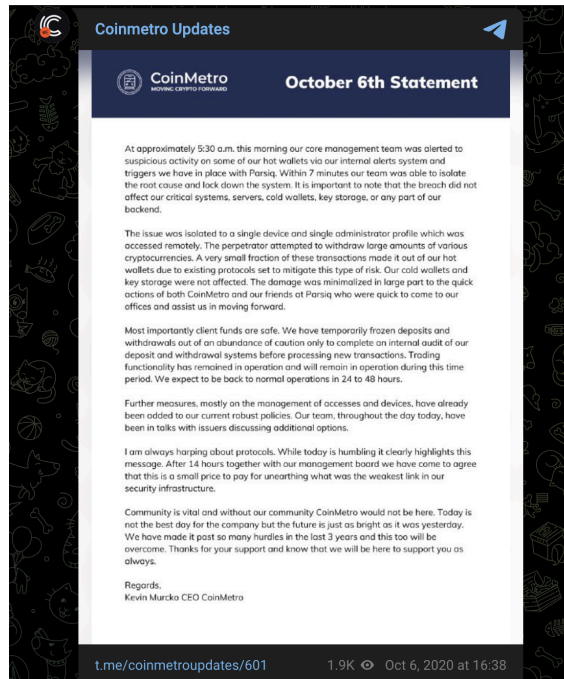
CoinMetro Incident Summary

On October 6, 2020 the CoinMetro team observed unauthorized transfers of \$750K worth of crypto assets from its hot wallets due to a security breach. As a result of the incident the Parsiq team made the decision to hard fork its token in an effort to prevent the attacker from further selling PRQ tokens and further protect user funds.

Theft address

0x044bf69ae74fcd8d1fc11da28adbad82bbb42351

1GVjvbVEYPkjCYCwJkC29t5pBWAQQd1g32



Source: <https://t.me/coinmetroudates/601>

On-chain aspects

Funds from thefts such as CoinMetro, CoinBerry, Unibright, and individuals were transferred through intermediary wallets before consolidating in 0x0864 in early January 2021.

3000 ETH was deposited to Tornado Cash by 0x0864 on January 11, 2021 beginning at 2:54 am UTC and concluding at 9:14 am UTC.

0x0864b5ef4d8086cd0062306f39adea5da5bd2603

After 1814.49 ETH was transferred from 0x0864 to 0x1031 and 17 X 100 ETH was deposited to Tornado Cash on January 11, 2021.

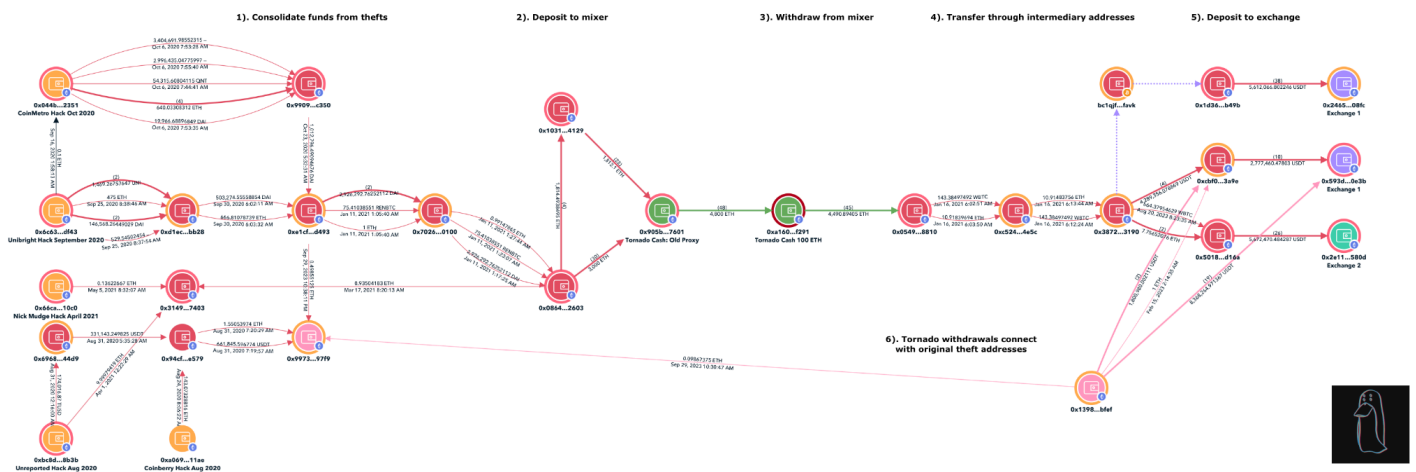
0x1031ffaf5d00c6bc1ee0978eb7ec196b1d164129

An additional 112.1 ETH was deposited to Tornado cash by 0x1031 from January 14–16, 2021.

45 X 100 ETH was withdrawn from Tornado Cash to a single address beginning on January 11, 2021 at 2:35 pm UTC and concluding on January 14, 2021 at 11:52 pm UTC.

0x05492cbc8fb228103744ecca0df62473b2858810

All Tornado Cash withdrawals for the month of January 2021 were reviewed and no additional withdrawals were found which shared similar characteristics. Additional comfort is gained with the demix as the Tornado withdrawal destination address connects back with the original theft address.



TRM forensics graph



TRM

Transfer laundered funds to P2P exchanges

Through a series of transactions, the funds sitting in 0x0549 were transferred through intermediary addresses and consolidated with funds from other Lazarus Group thefts before USDT was deposited to the P2P marketplace Paxful beginning in July 2022. In April 2023 they began using Noonex, another P2P marketplace. They continue slowly transferring USDT in batches until November 2023.

Paxful deposit address

0x246569f8b420c8d850c475c53d0d59973b3f08fc

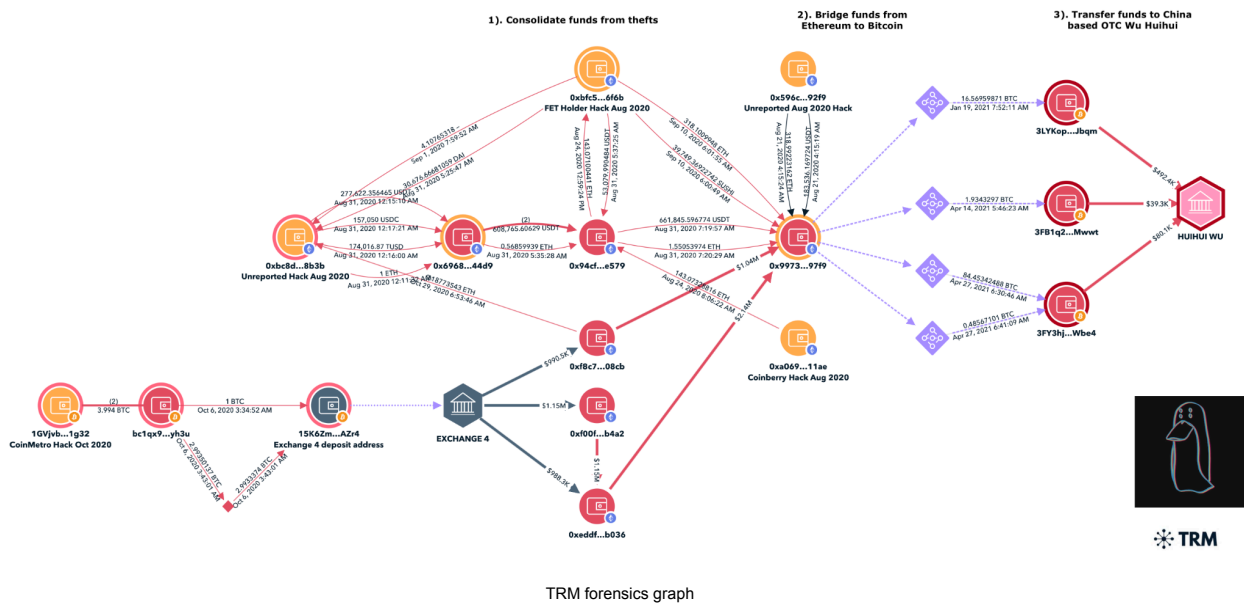
0x593dc5e1ad81667bbfc90739dd2c09c926920e3b

Noonex deposit address

0x2e1155cf5374cba058a04fd03ebd0ba19afe580d

Transfer funds from theft to OTC trader

Additionally, in 2021 multiple transfers were made from the 0x9973 address to Wu Huihui, a China-based OTC trader. In April 2023, an [indictment against Wu](#) was unsealed alleging that he facilitated payments for DPRK and he was added to the OFAC SDN list.



TRM forensics graph

WU, Huihui (a.k.a. "FAST4RELEASE"; a.k.a. "WAKEMEUPUPUP"), China; DOB 15 Dec 1988; POB Shandong, China; nationality China; Gender Male; Digital Currency Address - XBT 1986rYHckYbJpGQJy6ornuMyD2N5MTqwDt; alt. Digital Currency Address - XBT 125W5ek3DT6Zqy5S2iPt4FHQdNMcbZA3FU; alt. Digital Currency Address - XBT 1Kc6egXevyLEaeTxLFA1Zyw7GuhCN8jQtt; alt. Digital Currency Address - XBT 12w6v1qAaBc4W8h8C2Cu5SKFaKDSv3erUW; alt. Digital Currency Address - XBT 1CPJak9ZyddbawMGJPyEhCiJLXXb4sYv8N; alt. Digital Currency Address - XBT 1DJoVLgn1foJHHngduRPJvRbwpaFEKxvxd; alt. Digital Currency Address - XBT 15kZobLkD6HZgEEctz4oS2Vz21XHTnNfSg; alt. Digital Currency Address - XBT 15qyVrZvvVGvB7GWiAZ82TNcZ6QWMKu3kx; alt. Digital Currency Address - XBT 12YCFVAezkEZXYhUTyJJARkgMXiFxJgcu; alt. Digital Currency Address - XBT 1MkCnCa9agS5t6V1B15bzusBgYECB4LfWp; alt. Digital Currency Address - XBT 1NuBZQXJPYyQGfoBib8wWBDpZmbtkJa5Ba; alt. Digital Currency Address - XBT 14rjAD8ZP5xaL571cMRE98qgxxbg1S8mAN; alt. Digital Currency Address - XBT 18yWCu6agTxYqAerMxiz9sgHrK3ViezzGa; alt. Digital Currency Address - XBT 12jVCWW1ZhTLA5yVnroEJswqKwsfiZKsax; alt. Digital Currency Address - XBT 1J378PbmTKn2sEw6NBrsWVfjZLBZW3DZem; alt. Digital Currency Address - XBT 18aqbRhHupgvC9K8qEqD78phmTQQWs7B5d; alt. Digital Currency Address - XBT 16ti2EXaae5izfkUZ1Zc59HMcsdnHpP5QJ; Secondary sanctions risk: North Korea Sanctions Regulations, sections 510.201 and 510.210; Transactions Prohibited For Persons Owned or Controlled By U.S. Financial Institutions: North

Source: <https://ofac.treasury.gov/recent-actions/20230424>

December 2020—Nexus Mutual founder (Hugh Karp) hack

Incident summary

On December 14, 2020 Hugh Karp, founder of Nexus Mutual was tricked into approving a malicious transaction that [transferred out 370,000 NXM](#) (\$8.3M) after an attacker gained remote access to his computer and modified his Metamask extension.

On-chain aspects

The [post-mortem blog](#) post by Hugh Karp listed the theft addresses on Bitcoin and Ethereum.

On-chain aspects

BTC theft address

3DZTKLmxo56JXFEEDoKU8C4Xc37ZpNqEZN

ETH theft address

*0xad6a4ace6dcc21c93ca9dbc8a21c7d3a726c1fb1
0x03e89f2e1ebcea5d94c1b530f638cea3950c2e2b
0x09923e35f19687a524bbca7d42b92b6748534f25
0x0784051d5136a5ccb47ddb3a15243890f5268482
0x0adab45946372c2be1b94eead4b385210a8ebf0b*



Source: <https://x.com/hughkarp/status/1341063567408328705>

From December 16–17, 2020 the attacker deposited 137.1 BTC into the centralized mixing service ChipMixer in six deposits:

ChipMixer deposits—December 16

Deposit 1: 1 BTC deposited at 9:55 am UTC

906b3436067e48f3355f8cb5266c0055787d8cd378d3fe99e7020eecdde2ca74

Deposit 2: 5 BTC deposited at 10:09 am UTC

5ce61bc9bec2ff7a5291b48903441a39fab6df59934cf75b7cd1abee67ac8017

Deposit 3: 30 BTC deposited at 10:22 am UTC

db0cd0f1cb5bd13b9b3249e6a560aaeddbd0134d0f678220e626b20a424473ce

Deposit 4: 50 BTC deposited at 11:44 am UTC

1586fec6363ba1d6bac3056e4aee0bc0b4fefdf37f6060850b2d9168c39e6683

Deposit 5: 41.99 BTC deposited at 13:51 pm UTC

eb4854fb3ea8a3f5d87331b04bfc4daeac76343ebcbcaeff976551fadb5050cc

ChipMixer deposits—December 17

Deposit 1: 9.1 BTC deposited at 5:56 am UTC

1aa32442bfcbee3981e038d50a05885d35fd1d4ec33af5a9bd40e5d1dc88a686

Hours after the deposits, a matching amount of 136 BTC was withdrawn from ChipMixer and bridged back to Ethereum via Ren Project and consolidated with funds from other thefts.

Withdrawals consolidate 1: 4.61 BTC at 10:14 am UTC

18b9481573afb349c499ed5469ed903db5289b7946daddc1961e945b3d4d3cb7

Withdrawals consolidate 2: 5.42 BTC at 12:39 pm UTC

a88a7d86bbd780f42850472feffc626684b3df7b2f7c062e3b12009224e609d

Withdrawals consolidate 1 : 15 BTC at 12:56 pm UTC

0b6b1a990b6aab6edaef925c4af2a03f64c1a03ee98d3309f9557029af415f66

Withdrawals consolidate 2 : 60 BTC at 14:14 pm UTC

9726abb675bff14f512018a583693e815857829dc2459556938a491900638e21

Withdrawals consolidate 3 : 42 BTC at 23:33 pm UTC

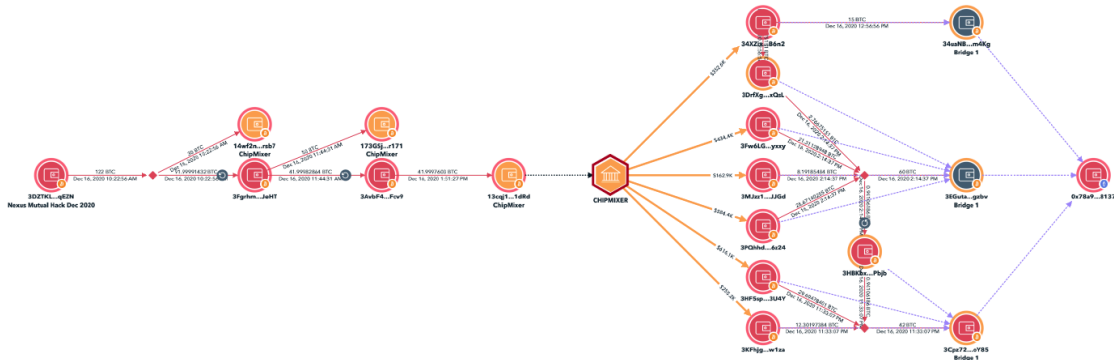
ffeb3dd56d0bde492cd08c0975edad38524f5ef003f55c258e75638044324acf

Withdrawals consolidate 4: 9.1 BTC on December 17 at 7:17 am UTC

a63eea88c4f9304e7e6c582a586b720c1dd50d671f8f6077143968eea2a3f97b

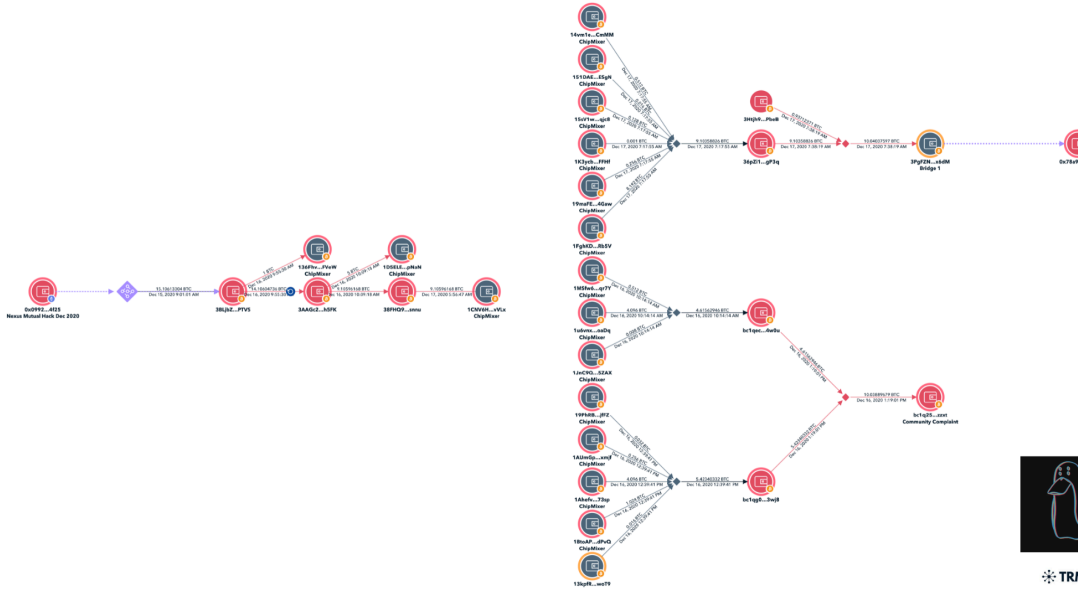
Ren Protocol ETH destination address:

0x78a9903af04c8e887df5290c91917f71ae028137



TRM

TRM forensics graph



TRM

TRM forensics graph

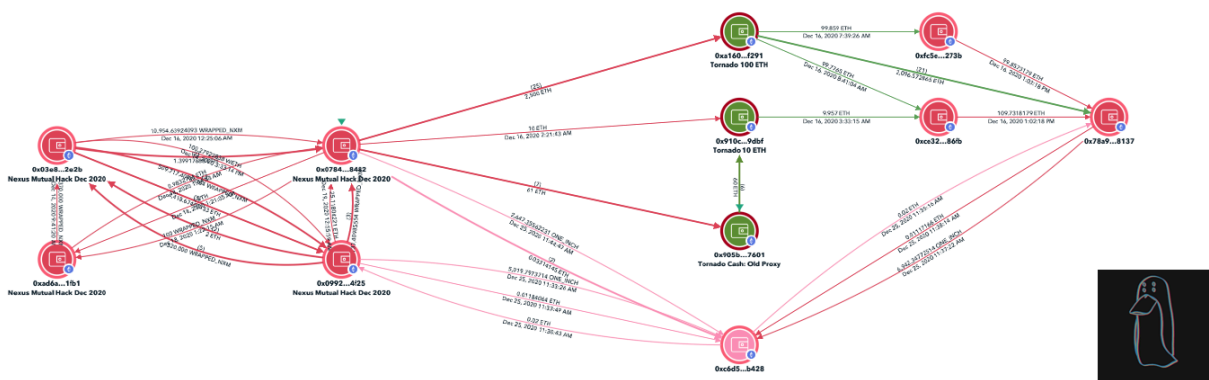
Date and Time	Transaction Hash	Amount	Address	Action
Dec-16-2020 9:55 AM UTC	906b3436067e48f3355f8cb5266c0055787d8cd378d3f99e7020eecdde2ca74	1 BTC	136FhvrVKcFjB9GhnlUw4uPoD4EXZFvW	Deposit
Dec-16-2020 10:09 AM UTC	5ce61bc9bec2ff7a5291b48903441a39fab6df59934c75b7cd1abee67ac8017	5 BTC	1D5ELEQnDCfXPAPDH5JCDwClUhtpNaN	Deposit
Dec-16-2020 10:22 AM UTC	db0cd0f1cb5bd13b9b3249e6a560aaeddbd0134d0f678220e62b20a424473ce	30 BTC	14w2nQGRfr1RT754RY8YyJkK7E2aGrb7	Deposit
Dec-16-2020 11:44 AM UTC	1586fec363ba1d6bac3056e4ae0bc0b4fedf37f6060850b2d9168c39e6683	50 BTC	173GSjx4pFaXD6KY3Hbn6YEG1WLLKmr171	Deposit
Dec-16-2020 1:51 PM UTC	eb4854fb3ea8a3f5d87331b04bfc4daeac76343ebcbcaef976551fad5050cc	41.99 BTC	13cq19PIHKFtzwnGILXS7bq1K4CG1dRd	Deposit
Dec-17-2020 5:56 AM UTC	1aa32442bfcbee3981e038d50a05885d35fd1d4ec33af5a9bd40e5d1dc88a686	9.1 BTC	1CNV6HDICL1wZLnZBPn3ZPmK6aErLcvLx	Deposit
Dec-16-2020 10:14 AM UTC	18b9481573afb349c499ed5469ed903d5289b7946daddc1961e945b3d4d3cb7	4.61 BTC	bc1qecgd8yxg2cfvju7zcmrwyg60dsa27ul4wu0	Withdrawal
Dec-16-2020 12:39 AM UTC	a88a7d86bd780f42850472fefcb626684b3df7b27c062e3b12009224e609d	5.42 BTC	bc1qg0nrdeWx68j43e702cczyvX0wmspey0n43wj8	Withdrawal
Dec-16-2020 12:56 PM UTC	006b1a990b6aab6dae9f25c4fa2a03f64c1a03ee98d3309f9557029af415f66	15 BTC	34uaNBaUF9rsxaZ3fQHNSLzm9yYpLm4Kg	Withdrawal
Dec-16-2020 2:14 PM UTC	9726abb675bf14f512018a583693e815857829dc2459556938a491900638e21	60 BTC	3EGuta87G2AZFReRBQad9eKyQwJGIPgzbv	Withdrawal
Dec-16-2020 23:33 PM UTC	f6b3dd56d0bde492cd08c0975edadd38524f5f003f5c258e75638044324acf	42 BTC	3Cpz72abcfmvtWuuRHChsZjpJUKoY85	Withdrawal
Dec-17-2020 7:17 AM UTC	a63eea88c4f9304e7e6c582a586b720c1dd50d671f8f6077143968eea2a3f97b	9.1 BTC	36pZ1XGLbs6LzJh9we44JhFR6YcVp3q	Withdrawal

Table 1: December 16–17 ChipMixer deposit and withdrawals

On the Ethereum side 2,571 ETH (25 X 100 ETH, 7 X 10 ETH, 1 X 1 ETH) was deposited into Tornado Cash from December 16–19 by theft address `0x0784051d5136a5ccb47ddb3a15243890f5268482`

Beginning just hours after deposits the `0x78a` Ren destination address started receiving withdrawals from Tornado Cash. `0x78a9903af04c8e887df5290c91917f71ae028137`

While not being a 1:1 match we can gain confidence this demix is accurate as Lazarus Group linked the post-mix address with the original theft address on December 25, 2020 reducing the effectiveness of the anonymity set as seen in the TRM graph below:



TRM forensic graph



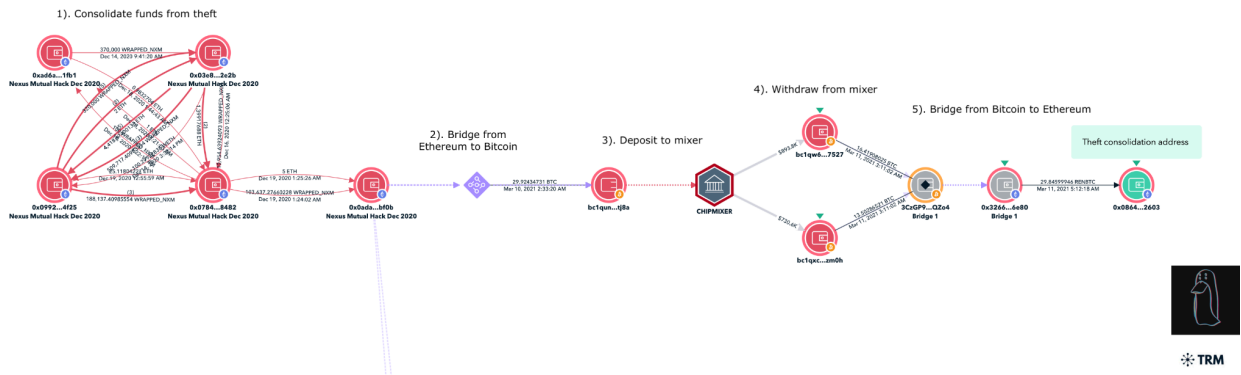
TRM

March 2021—ChipMixer Activity

In March 2021 Lazarus Group sold additional wNXM for renBTC before [bridging 89.5 renBTC](#) in total to Bitcoin via Ren Protocol and then depositing to ChipMixer

March 10th—29.98 renBTC was bridged to Bitcoin via Ren Protocol and deposited to ChipMixer in one transaction. Five hours later a matching amount of 29.92 BTC was withdrawn from ChipMixer and bridged via Ren back to Ethereum where the funds consolidated with other stolen funds in `0x0864b` from the CoinMetro hack and unreported individual hacks.

`0x0864b5ef4d8086cd0062306f39adea5da5bd2603`



TRM forensics graph

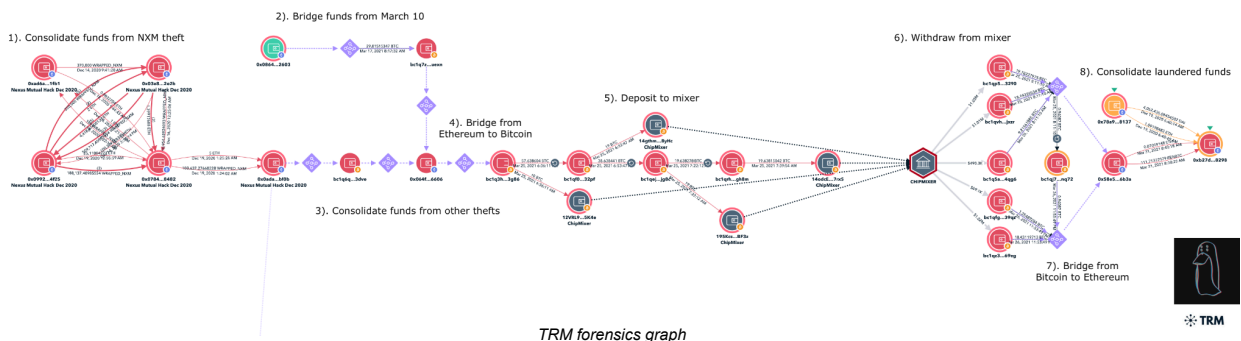
Date and Time	Transaction Hash	Amount	Address	Action
Mar-10-2021 12:48 AM UTC	713906c664b73e213408d5462232f91edce5c3002fa0ed1ed38559c6869e99a	29.92 BTC	1HHiJwMxXoTb68uefiqAtuDPWxPcACyrS	Deposit
Mar-10-2021 6:58 AM UTC	eea19d2ebf8f60adbadd9ef61b18465e3b6d16e865c91c1470515dc6553ad264	13.5 BTC	bc1qxcyp8g6j3n55n3en7c78pt0gj3fu3z7c8tzm0h	Withdrawal
Mar-10-2021 7:32 AM UTC	b4bf0af8b7ba358c515b1217900e69a32e5d27f882b2c243f5e5a10980f7e12e	16.41 BTC	bc1qw6687j3uxvgj62dylaqpqmsvzeuugs2t7527	Withdrawal

Table 2: NXM

March 20th—[13.13 renBTC was bridged](#) to Bitcoin and immediately bridged back to Ethereum via Ren Protocol and consolidates with stolen funds from the CoinMetro hack before 67.63 renBTC is bridged back to Bitcoin and four deposits were made to ChipMixer. Shortly after the deposits five withdrawals were made from ChipMixer in matching amounts adjusted for fees.

Funds were bridged via Ren from Bitcoin to Ethereum where they consolidate with the NXM batch laundered in December 2020 in 0xb27.

0xb27d40fb4a7975e6f4e6bd7f9fbf6e8d53bf8298



TRM forensics graph

Date and Time	Transaction Hash	Amount	Address	Action
Mar-25-2021 6:36 AM UTC	10183a31242ec1dafbe1a8be936388459aca6cd6b0663dd7d3da8c11053e8102	10 BTC	12VRL9vQDgV1jwoBT8r6TpxqBuLATm5K4e	Deposit
Mar-25-2021 6:53 AM UTC	b7e3010307efa20e4441e0554fcec9ebb171bc12c3aad97b703025c9156306ab	19 BTC	14gthm8HQUm4kccgwVfj41ZHdJsQfmByHc	Deposit
Mar-25-2021 7:22 AM UTC	ade08e2219126e98cb4d9d41933c4f259fc6354ac4cabe073ac4f92b69f9266d	19 BTC	195KcsMyk4QoiuXJfNRghSfQRanL56BF3z	Deposit
Mar-25-2021 7:39 AM UTC	876b41a6033b0a3031ce82325ed47239691b366129af75e7bc68728eacfd931c	19.63 BTC	14odcEaPUPNXgXd4PFVm6RqaVP4kPT7rxS	Deposit
Mar-25-2021 6:53 AM UTC	a150603622e29559fb5d68024c65f9f8786e1a0d9e41ea0f6021ae161bc098e1	9.21 BTC	bc1q5aej8zfv3zlw0wmj78yphexd5k5fnjv2i4qg6	Withdrawal
Mar-25-2021 7:22 AM UTC	64d59745f16b244a1a382a9ab7de96b03fa743c4eee2f2411e22eb8d22e21b88	19.78 BTC	bc1qp5266qlpds5y5th5cksg5v8rjq75kknw83290	Withdrawal
Mar-25-2021 7:39 AM UTC	482f1485e5816ee8cb34284cd21a0480e86619d430dd138dc85882090db281fa	18.94 BTC	bc1qvhv309xddnz5u9z485p6kv5wq9utx5fy07jxzzr	Withdrawal
Mar-26-2021 11:36PM UTC	582235a91bbb8ceea002035abc10dfdf0c2bfff3ec204649f0c4a382f00e149	18.43 BTC	bc1qz3yvqe8ftdgrgka0symfu64u3n4vice3h969eg	Withdrawal
Mar-26-2021 11:43 PM UTC	772b2a263650e240802a6e14bcdbf14a754289a4250627e35787003043654bbd	1.25 BTC	bc1qfgpkcjsxn7xc766r2k5d64z8r8lx05uynf39qz	Withdrawal

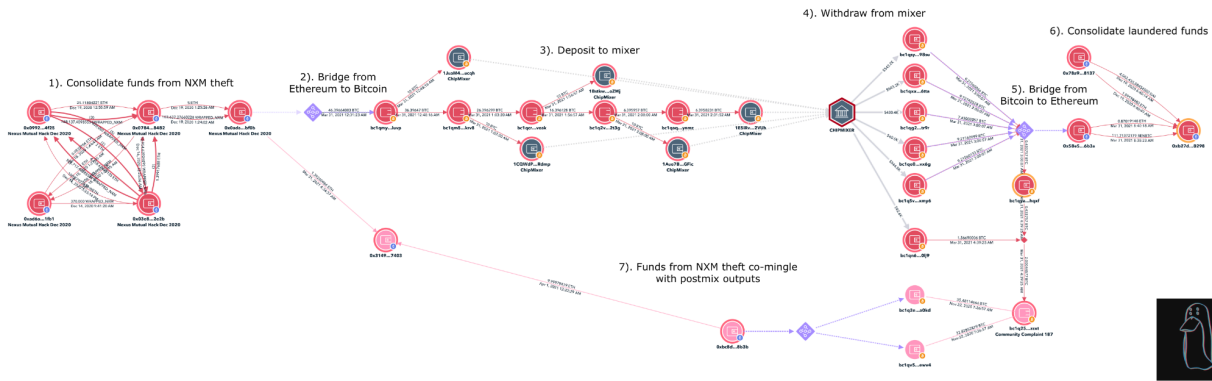
Table 3: NXM hack ChipMixer deposits and withdrawals

March 31st—46.49 renBTC was bridged to Bitcoin via Ren and five deposits were made ChipMixer. Within minutes of the deposits six addresses begin receiving withdrawals in matching amounts. Funds are bridged back to the same destination address 0x58e5 on Ethereum.

Date and Time	Transaction Hash	Amount	Address	Action
Mar-31-2021 12:48 AM UTC	b82c836b83e84ee96a906bd42a76107795bc8cdf22d577c673f847080550b166	10 BTC	1JuaM4E6C8n1Vcp9kSMMgqemZWiaKaucqh	Deposit
Mar-31-2021 1:03 AM UTC	e71c23cef1dc3b014951d27803ca396c809acb604786e464e969ccab2a64a3c0	19 BTC	1CQWdPFfkuT2vQnp6XPTLYsgdFXaF9Rdmp	Deposit
Mar-31-2021 1:56 AM UTC	9c35a8c46c801ee2f5d3927ab87258ed91226a1b13d9f117771aa82253452cec	19 BTC	1BstkwML5mvToR2GMpLfgQaym6fT8oZMj	Deposit
Mar-31-2021 2:08 AM UTC	95be498f585b2d908ba452b459a723a6dd5697e5a787a3bc0de3c5deb50d2619	19.63 BTC	1Aue7BX2uhRToydQkQ7HAejuKYnBLGFic	Deposit
Mar-31-2021 2:31 AM UTC	f7963b0d984901691ad71c529f641b01a67ac0d751558fc5308a60407ee1f5c8	9.21 BTC	1E5iRvZgbXaRVtACSHjRw2HmQdYgWv2VUj	Deposit
Mar-31-2021 1:03 AM UTC	a025b99d588c9200dc07ddb34c26408ea70fd8469fabab503f5651b46277675	9.21 BTC	bc1q5vzund54gmekae89ev95fca9mn7j27petxmy6	Withdrawal
Mar-31-2021 1:56 AM UTC	5bf546baf4f2775d854e74a24c0b8f1ebdfe4f62540c84eb7c051e855b274a02	1.56 BTC	bc1qn6vpyu8j6dmj8hz3xgcw2q9kcur3aeu8v30lj9	Withdrawal
Mar-31-2021 1:56 AM UTC	51825614078a40e34fdd96739ad8b2c35ee2a0e355b8588257c415798fc40ad2	9.21 BTC	bc1qe0cuv34awlt4k2sv6uteeejqgwka0ptvx6g	Withdrawal
Mar-31-2021 2:08 AM UTC	4bb509916abc7c1d3c0cedc44e3ae64cea34aca5b41baad3546c3b1b66bcf50	9.72 BTC	bc1qxxuaku5xpd8m2zrvycm39dptdydgg38ju6tta	Withdrawal
Mar-31-2021 2:31 AM UTC	eeeeae751f66ceedfad03f99e13a4979ba75a5577fd2d645f41463e0f71fe0988	9.21 BTC	bc1qsypppeefg7mtauu72lpnjq9m5c9e6elfx98su	Withdrawal
Mar-31-2021 2:56 AM UTC	1f2565af80545ee54dad6fa29c94f035a552d5073fde79753f2327668f22732f	7.43 BTC	bc1qg25pq6ujvgtdwg93q4f8mkwhkz2jf8r7gtr9r	Withdrawal

Table 4: NXM hack ChipMixer deposits and withdrawals

The accuracy of this demix can be confirmed since the withdrawal address of 1.56 BTC connects to the original NXM theft address from funds bridged via Ren in November 2020. This is highlighted in pink in the TRM graph below.



TRM forensics graph



TRM

Transfer laundered funds to P2P exchanges

In April 2021 19.96 BTC was bridged from Ethereum to Bitcoin via Ren where it was transferred to Wu Huihui, an OFAC sanctioned OTC trader.

\$11M from 0xb27 was transferred to a Bixin deposit address from May 24-July 10, 2021 .

February 2023 the remaining funds in 0xb27 were transferred to 0xcbf0 where they consolidated with funds from other thefts and were deposited to Paxful and Noones.

Bixin deposit address

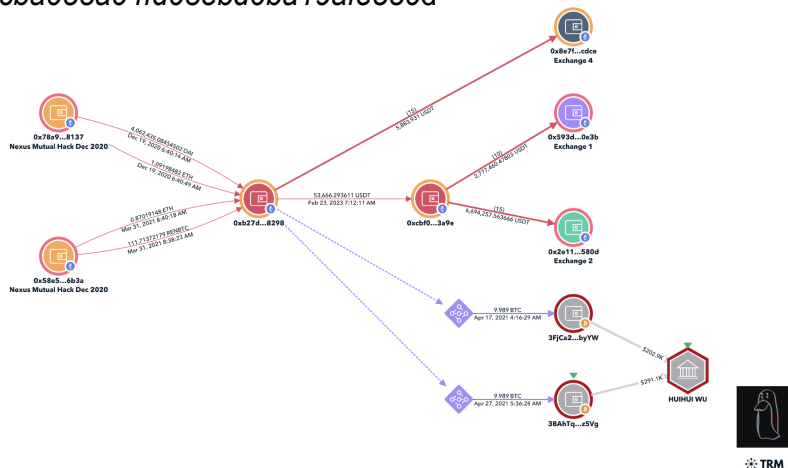
0x8e7f5d85c3587725b1188d3cc04ca814ab60cdce

Paxful deposit address

0x593dc5e1ad81667bbfc90739dd2c09c926920e3b

Noones deposit address

0x2e1155cf5374cba058a04fd03ebd0ba19afe580d



TRM

April 2021 — EasyFi founder (Ankitt Gaur) hack

Incident Summary

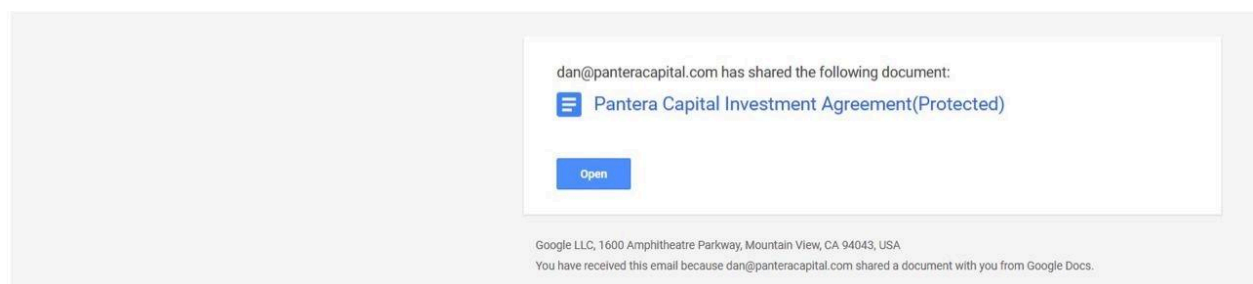
April 19, 2021 EasyFi team observed large unauthorized transfers of EASY tokens from team wallets controlled by the founder Ankitt Gaur after his device had been injected with a malicious version of Metamask allowing the attacker to [gain control of the private keys](#) resulting in \$81M stolen.



Source: <https://x.com/ankittgaur/status/1384253351492087819>

Further analysis revealed that a few days prior Ankitt Gaur had received a phishing email to his personal email address via sendgrid which appeared as if it had been sent from the Pantera Capital founder Dan.

----- Forwarded message -----
From: **Dan Morehead (via Google Drive)** <dan@panteracapital.com>
Date: Tue, Apr 13, 2021 at 11:34 AM
Subject: Pantera Capital Investment Agreement(Protected)
To: <an[REDACTED]>



Notably this type of attack resembled what happened to Hugh Karp (Nexus Mutual Founder) in December 2020.

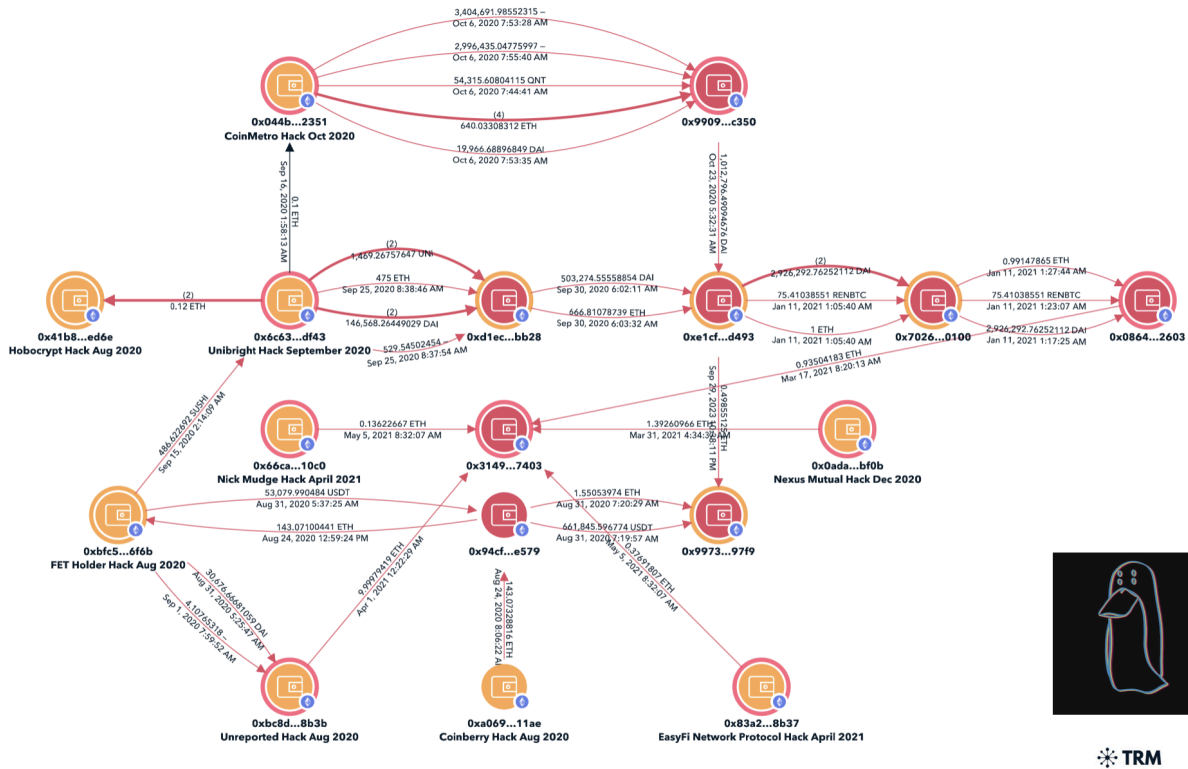
On-chain aspects

\$6M of USD/DAI/USDT of liquidity was removed from protocol pools and 2.98M EASY was transferred to 0x4371

`0x437147DA920714feC4822F0666D940945f9c972B`

The attacker can be linked to Nexus Mutual, CoinMetro, Unibright, Coinberry, and multiple individual thefts on-chain as addresses from each incident transfer ETH to 0x3149 in March-April 2021.

`0x31499e03303dd75851a1738e88972cd998337403`

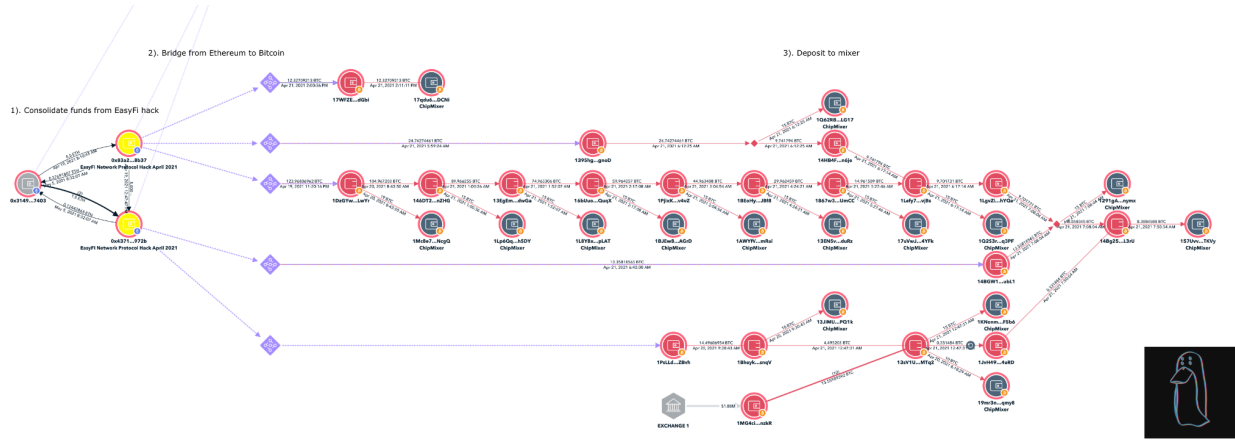


TRM

TRM forensics graph

April 2021—Laundering

From April 20–21, 2021 a total of 209.64 BTC from the theft address was bridged from Ethereum and deposited to ChipMixer from the hack.



TRM forensics graph

Date and Time	Transaction Hash	Amount	Address	Action
Apr-20-2021 8:18 AM UTC	0df5ef8a39ec334aaf98dce59d335feba0a55b133934f73253114a4469ab4c13	10 BTC	19mr3n2Skrr9ZMtrf5ePtn5ZJXvQqmy8	Deposit
Apr-20-2021 8:43 AM UTC	65e9b2deefe533d5e3f1da7b97538a8328050f6b788cd52bc26768bc0565541	19 BTC	1Mc8e7dWycuoNLRgbu3oFxn4BKvUcYncgQ	Deposit
Apr-20-2021 9:30 AM UTC	aea9a6c4e0398d5bdfdba282fa555ce5c3755744fb48d7b56887abc4157f927	10 BTC	13JiMUJSDVhvTgThbUEKV7BEN5vPkpQ1k	Deposit
Apr-21-2021 12:47 AM UTC	cdbb1e09e28705cb14c19ebbd97bbd524d5d29807c346f1474b58dd78ec5fa94	15 BTC	1KNenmdcanGi2j5SBFF2xZsJ6RiaF5b6	Deposit
Apr-21-2021 1:00 AM UTC	e6aaff241d09974595ec27668dd724254e55477f8af06490cfd06b2187d179d7	15 BTC	1Lp6QqZWuzkK9RsD9YPdeMp6Umq5UEh5DY	Deposit
Apr-21-2021 1:52 AM UTC	c521ec54e32257c3a312d2a80f26d90826273e54f8a2882e1e1d8bec71930262	15 BTC	1L8YBxVrmiN3nQsnkhGsGw9KsDh6gzpLAT	Deposit
Apr-21-2021 2:17 AM UTC	30bbdce7575f9a5620647bbe4f9c51c4bbd5d5fcec4dd597a27c3671ab52f5f1	15 BTC	1BJEwBYctHDLEWkCursEvuXEynP1a2AGrD	Deposit
Apr-21-2021 3:04 AM UTC	6fae51bbe4c5199a772d45289334bb16f959f065a7f4e03361b07f289ab62e82	15 BTC	1AWYfVjrMRrsTXF99LKMg4BSJGo6LmRui	Deposit
Apr-21-2021 4:24 AM UTC	a06efdfecff904e9896041a94f8b11f130c6582dac4268b7fa413916ee79bb44	15 BTC	13EN5vpEDBSGemM9Shk6FU3q2vqXEidurZ	Deposit
Apr-21-2021 5:27 AM UTC	b16be35f6925c39f6eefb1e146b2e9667ab9aab2128894f7d869d646d526627d	15 BTC	17uVwVJJGzQoPQj4mJjsD1Ew8eG33t4Yfk	Deposit
Apr-21-2021 6:12 AM UTC	ec9c947e39611839c1795ab72ab8a18ea1ef11916d4cef46f9a77c88428f5728	15 BTC	1Q62R8YbgckVfmWTErQKBKkJvbeVbRLG17	Deposit
Apr-21-2021 6:17 AM UTC	17c00c520aad462219d30dfb6ded265896bb76b4024a3f2f2ae549aa91a1190f	15 BTC	1Q2S3ror8DeSBz4dbcNigqgCDHbzo1q3PF	Deposit
Apr-21-2021 7:08 AM UTC	cdf62dc9d0094196d279509697c5846ec611910afb952f5f6a725e7ea30e60e5	15 BTC	1291gAWuXvgRw82pffkv56f6yRdFRLnymx	Deposit
Apr-21-2021 7:50 AM UTC	2c35ca1a04a711f89bb38d98d68b12da0c1600a71183780f19b6108ac3b4b81e	8.32 BTC	157UvvhB9G5J16XRfPXDNAazSSvHTVTKVy	Deposit
Apr-21-2021 2:11 PM UTC	7bcc87314fe7ba3ecbe2dc73d3d641d91e64bd531c2fef2a7200966f83a23175	12.32 BTC	17qdu6TgFtF5v83tgdosRSEVZRQdFDCNi	Deposit

Table 5: EasyFi hack ChipMixer deposits April 20–21, 2021

A volume and timing analysis was performed and from April 20–21, 2021 a total of 209.5 BTC was withdrawn from ChipMixer matching the amount deposited adjusted for fees. There were no other withdrawals during that period which showed similar characteristics.

Date and Time	Transaction Hash	Amount	Address	Action
Apr-20-2021 8:35 AM UTC	84e9c14bd576f09d8523b1ed5538d6861ef692567dedb4676ad02b1954b7e907	9.21 BTC	bc1q5f1wgap0u8ur3r2sqpf50rx8rmvqzenwdmp9r	Withdrawal
Apr-20-2021 9:30 AM UTC	2bcf5353ba5d5e01bd072e54427148e7c542095d9c221cb1d7cbc786f63e91f1	18.94 BTC	bc1qtemsh0enjfpdx6043y8zrcupy6wp3e28gsae5	Withdrawal
Apr-21-2021 12:47 AM UTC	0fe006e2163f0131987c41039ae264506eb215858d047bcd3ad493a59243b	10.03 BTC	bc1q4apuzs9g7q0ffxns199vsgstg083jj7vxzsvra	Withdrawal
Apr-21-2021 1:00 AM UTC	11cfe8d9cbb7e84ebf2e2e694dbb1b519ef214cb8f7f80055640a24f3d9b4984	10.87 BTC	bc1qpvfsku20xe6k4supdzu9cuua5x8rdy0za82d	Withdrawal
Apr-21-2021 1:21 AM UTC	eb32b772e24156e20c13b5e901fc69ca87e35b5ab123805a9939d9b5bb97b387	19.08 BTC	bc1qd5h4uxl50p6f3y3hikzgv2wj33pc0fxedqdaqx	Withdrawal
Apr-21-2021 2:17 AM UTC	2d2d58ffa2948bd6e35645bb839bc65a7868a22e00efa0971187277424b57c0	0.66 BTC	bc1qfucvlt8kefld95gv4mp8fnj7pznym24tvhrtw	Withdrawal
Apr-21-2021 3:04 AM UTC	d1c8468b9984d76944869efbe9ac547b791a4ea91d9c0515dd1ca8bfbcb89165e	29.32 BTC	bc1qkgwmv0d9p6473g6kast7h0mrrpswxzrlzf65rla	Withdrawal
Apr-21-2021 3:10 AM UTC	318900de7af093d94be9b6339cf2389885dcbdd509f546c42a8cac55e58fda2	6.14 BTC	bc1q2u7n69pdzm0886gggmznyhty0af4l4nzqkdgrs	Withdrawal
Apr-21-2021 5:59 AM UTC	58fe8b12cfd85432ebee7ce41c7062f549347e5b95c38e6efe1fc2fd0e26653	10.74 BTC	bc1quzz3z2a7w6snt9he5cl4sklw64d0fyf4khrq	Withdrawal
Apr-21-2021 6:17 AM UTC	6401c5d370f6c142a7157f986d1d5f9f12533b40602b27ba69b4ba47b42c3f9	19.23 BTC	bc1qa34l4ye39u3c2k7d5dymgydq5kwjkwxhkek	Withdrawal
Apr-21-2021 6:42 AM UTC	c6f55d242f12b4651239bbbd37eb59da90aab98f782db908815785f948aa173b	10.23 BTC	bc1qctxsadq92nuqkcv5pst4jfvzfq6ngz7kxucz6p	Withdrawal
Apr-21-2021 7:29 AM UTC	04baf50a307f1a68aea193fafdfc9d863df5cb27b1955764b4f39765da03b3	19.74 BTC	bc1qk6quxamg4x4jwv0kxnpedqnlq3zwykp7u0fz0	Withdrawal
Apr-21-2021 9:33 AM UTC	fdecbb7cd43a725a4d1f3803cc3b6154bf050780e8825f03e4f0cf8b0ee631c	8.18 BTC	bc1qath2ss884adh48xrqcmz3789vmvmmwlfy8zjf	Withdrawal
Apr-21-2021 9:33 AM UTC	b1169d8b0f389662fc5c705fcc4bd19e9a0159f60c0cf60025c2c19889adf99	0.19 BTC	bc1qn5meglvhlgu9p4n3fncz4f3w5k33rsqk9ag78d	Withdrawal
Apr-21-2021 2:11 PM UTC	d32c31e751288d6f0a11a72428cd20c569c92d672f8b95f9ce2705f2b116cb	23.82 BTC	bc1q0u6nfj2q6lhzmpnhwktqzy6mzgva65rax3xwdx	Withdrawal
Apr-21-2021 2:29 PM UTC	2e1d627a1ececacc47bfd17e79ee44afa2003226ff2e6b6fd6fe8458b87928fe4	2.08 BTC	bc1qgznjavfvczl7lzkqukwtkysj27vsw8gty62tm9	Withdrawal
Apr-21-2021 2:29 PM UTC	fdec6c49b5d67c8e0880249fab1049a6da992321026b950c7165ca0f13e74b2e	10.23 BTC	bc1qsa8uxs6j8dqnx82mg97svdvdn9sr5gl68lzxax	Withdrawal

Table 6: EasyFi hack ChipMixer withdrawals

209.22 BTC from the Chipmixer withdrawals were consolidated to two addresses on April 22, 2021 and then bridged back to Ethereum using Ren protocol.

Ren bridge source transaction—

Amount: 179.47 BTC

84b7c4a2b79d454bbb1636d6d872ed367bbcf4b664193b7b8baded8675085935

Date: April 22, 2021 at 2:00 AM UTC

35TjCuKRbKcofxnKG2EkC8B66ZNXKqE1aN

Amount: 29.75 BTC

3e3b2950c72f863642db0a1bd248be3009ba65e9fa950d5a3094a7b1d7b14e2e

Date: April 22, 2021 at 2:00 AM UTC

3M8VZjtAqi51LsMuRGGY9mhPvQk5hvubvt

April 28, 2021 another batch of 6.31 renBTC was bridged to Bitcoin using Ren Protocol and then deposited to ChipMixer at 7:20 am UTC.

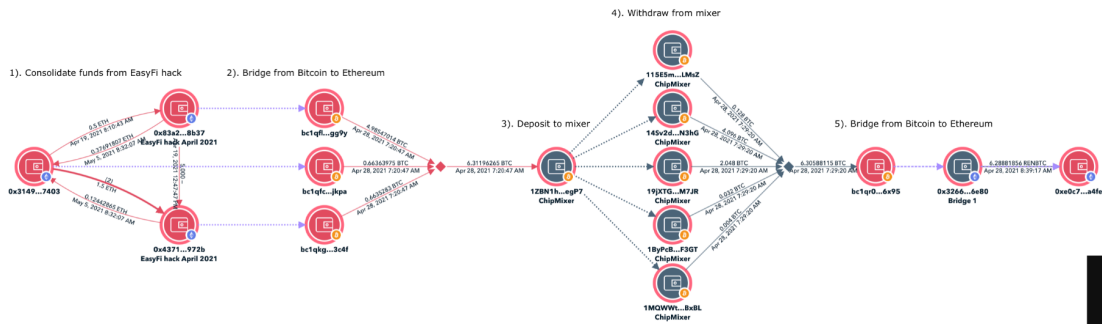
0a6f220fdc821ec1743a9a201e16a038d474b1554520e9922734e6c62628e7b2

Minutes later at 7:29 am UTC an address received 6.305 BTC from ChipMixer matching the amount deposited adjusted for fees.

4e35b2214a12f8d49cdd0100d71f7573ee47dd6a575e149eb1529285b7effff9

All funds were bridged back to Ethereum address 0xe0c7 using Ren bridge.

0xe0c79066488a15b70361ad8268d713b05944a4fe



TRM forensics graph

Transfer laundered funds to P2P exchanges:

Through a series of transactions, the funds sitting in 0xe0c7 and 0x313d were converted to DAI and wBTC, transferred through intermediary addresses, consolidate with funds from other Lazarus Group thefts, and USDT was deposited to the P2P marketplace Paxful beginning in July 2022. In April 2023 they began using Noones, another P2P marketplace. They continued slowly sending USDT in batches until November 2023.

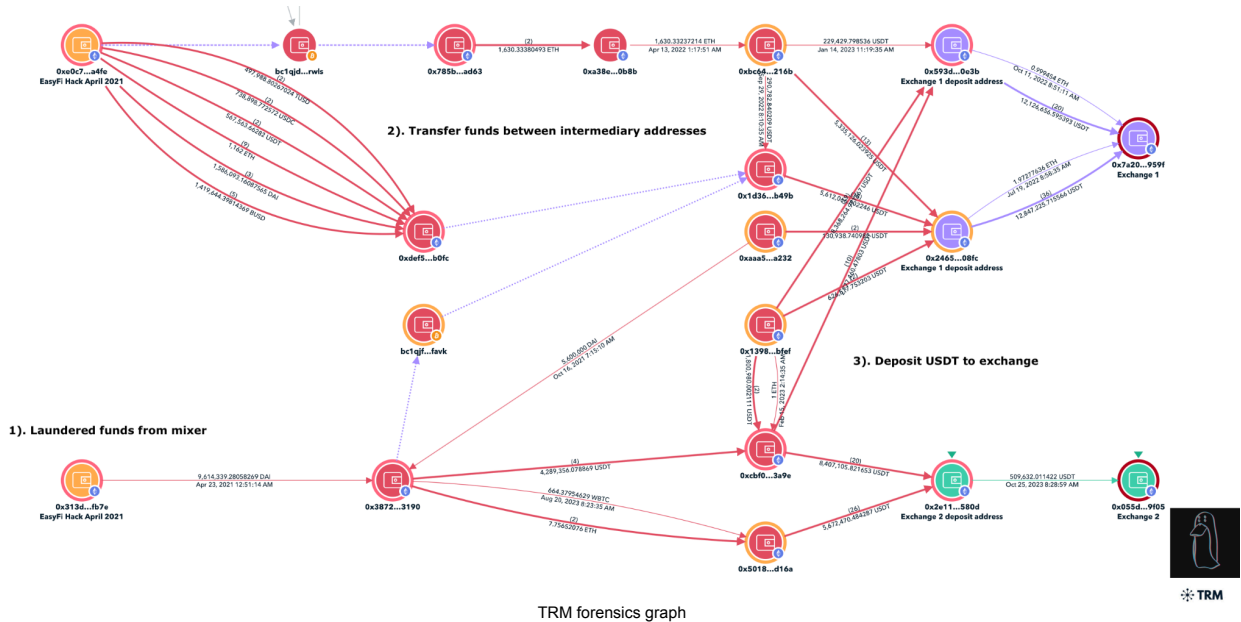
Paxful deposit address:

0x246569f8b420c8d850c475c53d0d59973b3f08fc

0x593dc5e1ad81667bbfc90739dd2c09c926920e3b

Noones deposit address:

0x2e1155cf5374cba058a04fd03ebd0ba19afe580d



July 2021—Bondly hack

Incident summary:

On July 14, 2021 Brandon Smith, CEO of Bondly Finance fell victim to an attack where the malicious actor gained access to a password account containing the recovery phrase for his hardware wallet. Soon after the [attacker transferred](#) ownership of the Bondly token contract to themselves and \$8.5M of assets belonging to the team.



Source: <https://x.com/forjofficial/status/1415543486141636612>

On-chain aspects:

The post-mortem blog post by Bondly co-founder Harry Liu highlights the theft addresses on Ethereum, BSC, and Polygon.

Ethereum, BSC, and Polygon theft address

0xc433d50dd0614c81ee314289ec82aa63710d25e8

Laundering July 2021:

Tornado Cash deposits—BSC

Through a series of transactions, 48 X 100 BNB was deposited to Tornado Cash by the attacker beginning on July 15, 2021 at 5:41 am UTC and concluded on July 16, 2021 at 6:33 am UTC.

Tornado Cash deposits—Ethereum

Through a series of transactions, 5X 100 ETH and 52 X 100,000 DAI was deposited to Tornado Cash by the attacker beginning on July 15, 2021 at 8:15 am UTC and concluding on July 16, 2021 at 2:17 am UTC. On August 11, 2021 an additional 202 ETH was deposited to Tornado Cash.

Tornado Cash withdrawals—BSC

From July 17–19th 47 X 100 BNB was withdrawn to 0x4197 on BSC. This matches the deposits 1:1 as one of the Tornado deposits was withdrawn to the depositor 0xc433.

0x419787019b991ac2c765a14467d177c6c0b05c00

Funds were then bridged from BSC to Ethereum via Multichain bridge and consolidated with the Ethereum withdrawals.

Tornado Cash withdrawals—Ethereum

From July 16–20th 35 X 100,000 DAI and 3 X 100 ETH was withdrawn to 0x365 consolidating with the 100 BNB Tornado Cash withdrawals.

0x365d2c5220989a068d8b0e95625875c55166297b

From July 22–29th 14 X 100,000 DAI and 2 X 100 ETH was withdrawn to 0xe0c7 consolidating with funds from the EasyFi hack. From August 12–23th 2 X 100 ETH was withdrawn to 0xe0c7.

0xe0c79066488a15b70361ad8268d713b05944a4fe

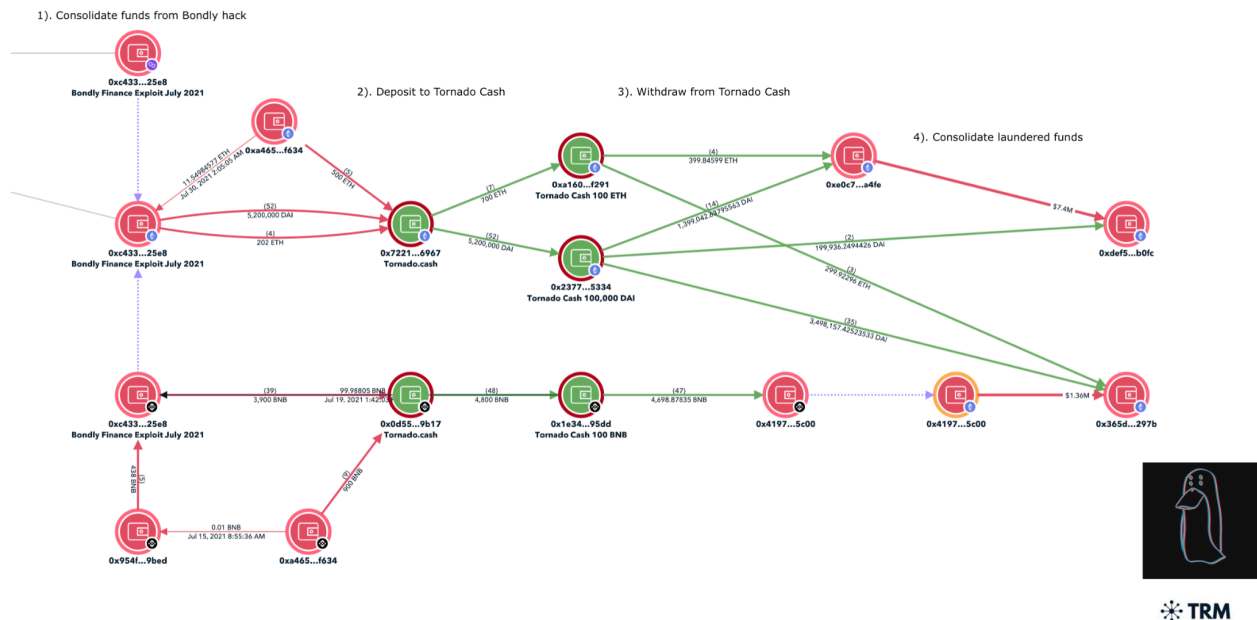
On July 24th 2 X 100,000 DAI was withdrawn to 0xdef5 which received \$7.4M from 0xe0c7 in a series of transactions.

0xdef57ccb20b1f2eaae0c64aab3280350f84cb0fc

The remaining 1 X 100,000 DAI withdrawal was made to 0x996f.

0xd7589df5c035ce5d432e5af64b13b77802b7451315f460ce1bda8a4e7c89240

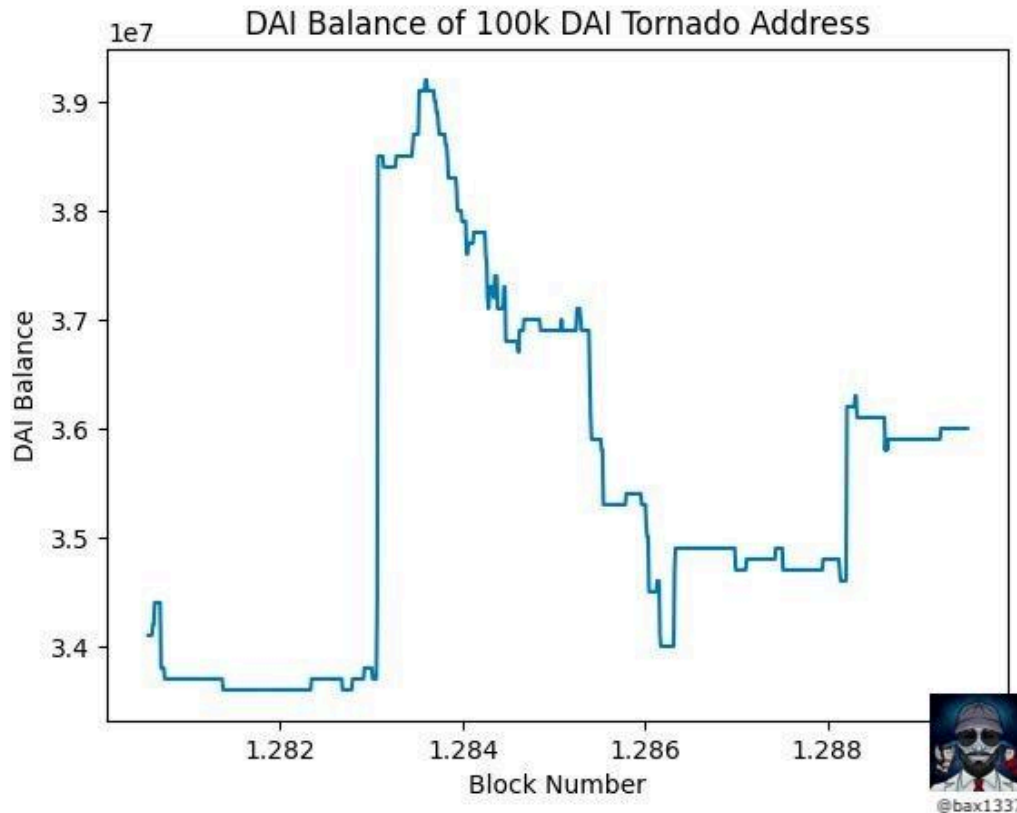
0x996f5ccbf2856137744603b382de559b78a096fc



TRM forensics graph



The Tornado Cash 100,000 DAI pool sees little activity and the 52 deposits made by the Bondly attacker increased the pool by 15% significantly reducing the effectiveness of the anonymity set. The graph below shows the cumulative balance of the 100,000 DAI pool from July 11–25, 2021 shows a sudden increase in deposits before matching withdrawals.



Tornado Cash 100,000 DAI pool balance from Jul-11-2021 to Jul-25-2021

In June 2022 \$4.9M laundered from hacks such as Nexus Mutual, EasyFi, and Bondly was transferred to two Binance deposit addresses:

0x27a9d7d17d72a5a67115dbf381b121b51d8b5dd8

0xabef0df725ef5d2f0354c59ea3ccb161abc11515

Transfer laundered funds to P2P exchanges

Through a series of transactions, the funds sitting in 0xe0c7 and 0x365d were transferred through intermediary addresses and consolidate with funds from other Lazarus Group thefts such as EasyFi and the Nexus Mutual founder before USDT was deposited to the P2P marketplace Paxful beginning in July 2022. In April 2023 they began using Noones, another P2P marketplace. They continue slowly sending USDT in batches until November 2023.

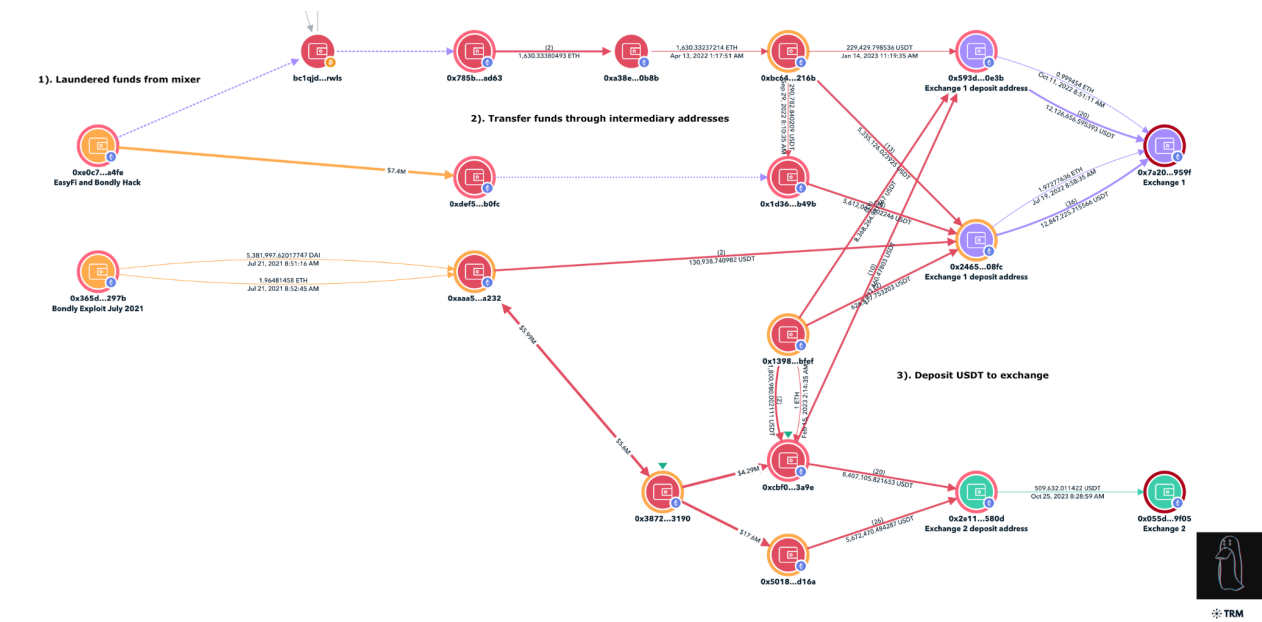
Paxful deposit address:

0x246569f8b420c8d850c475c53d0d59973b3f08fc

0x593dc5e1ad81667bbfc90739dd2c09c926920e3b

Noones deposit address:

0x2e1155cf5374cba058a04fd03ebd0ba19afe580d



TRM forensics graph

August and September 2021—Unreported Hacks

August and September 2021 saw multiple individuals hacked for \$2M likely due to private key compromise. Indicators of the thefts include on-chain connections to known hacks such as FinNexus, assets transferred out from victims wallets and immediately sold for ETH, and activity in victims wallets stopped after transfers were made.

Theft address

0x5271b379f3e1954e20791142d734596a3de28efd

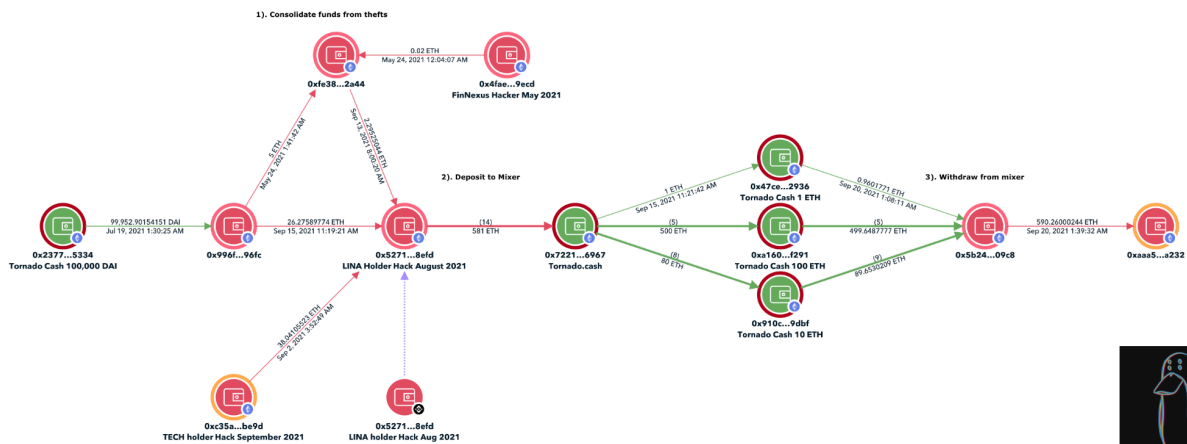
0xc35a06d02471acc48e552e99d8b860bac73cbe9d

0x40d7b7A55dd51ee94A9a4788311e39CB362Fe1Ea

Funds from the multiple thefts consolidated in 0x5271 before 581 ETH was deposited to Tornado Cash on September 15, 2021 beginning at 10:13 am UTC.

591 ETH was withdrawn from Tornado Cash to a single address on September 20, 2021 beginning at 12:20 am UTC.

0x5b24da735fd5835ec5afb5abf9f3e89270e609c8



TRM

TRM forensics graph

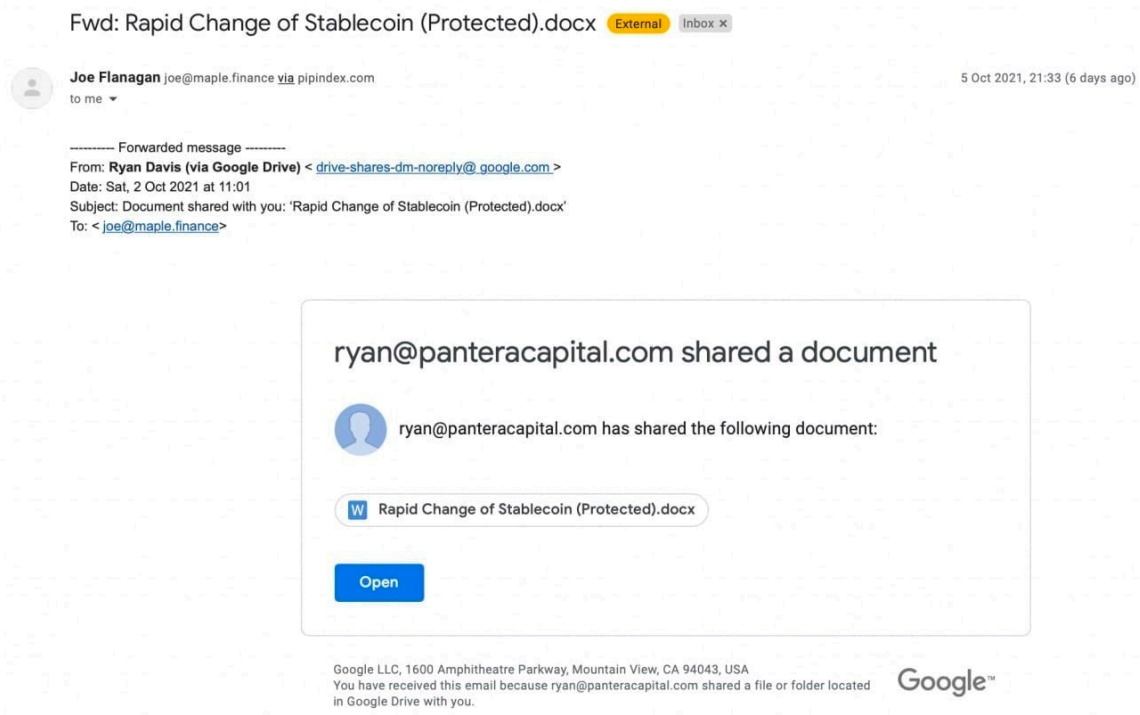
October 2021 — MGNR and PolyPlay Hack

MGNR hack incident summary:

On October 8, 2021 the trading firm mgnr.io had \$24M worth of assets drained from their wallets as the result of a private key compromise. [In a deleted post on X \(formerly Twitter\) the team](#) shared they had been targeted in a sophisticated cyber attack after receiving a Pantera Capital phishing email via SendGrid similarly to Ankitt Gaur from EasyFi. The team noted that private keys to hot wallets had been temporarily shared between multiple team members.



Source: https://web.archive.org/web/20211014032211/https://twitter.com/mgnr_io/status/1448489258029703168/



Phishing email

MGNR hack on-chain aspects

[A blog post by the user CryptoCat](#) in January 2022 revealed addresses from the theft by detailing mgnr.io wallets which sold Maple Finance tokens on October 8, 2021. The author mistakenly attributes the actions to the team instead of the hack.

Theft address:

0x57737d6f8ea0099c30c96754a436e46d4dd3fa80

MGNR hack October 2021 laundering

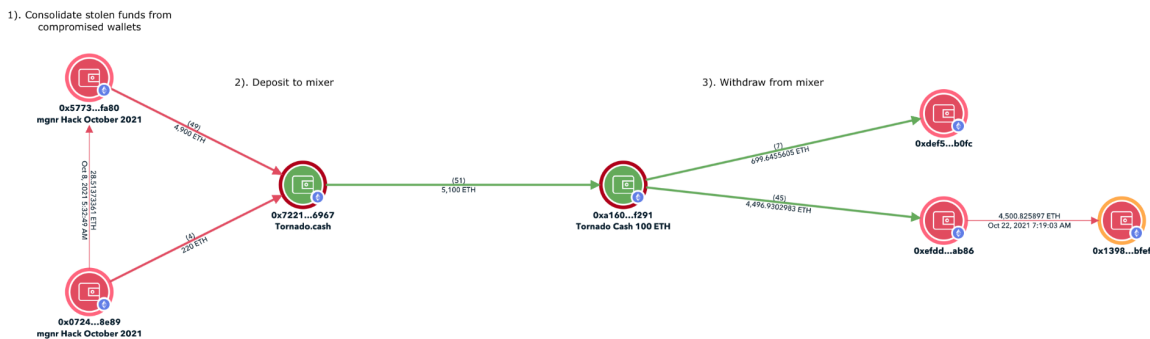
All assets from compromised mgnr.io wallets on EVM chains were bridged and swapped before being consolidated into 0x577 where the attacker deposited 4900 ETH from the incident to Tornado Cash beginning on October 8, 2021 at 4:37 am UTC and concluding on October 12, 2021 at 6:16 am UTC. Another address connected to the attacker deposited 210 ETH to Tornado Cash during this period.

A few days after 0xdef5 which received \$4.3M from the EasyFi and Bondly hacks earlier in the year received 700 ETH from Tornado Cash.

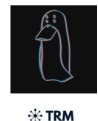
0xdef57ccb20b1f2eaae0c64aab3280350f84cb0fc

Another address 0x1398 received 4500 ETH from Tornado Cash which previously had received \$15.2M from the EasyFi and Bondly hacks earlier in the year.

0x1398db28ca00d9f943355d6b57ab28a61110bfef



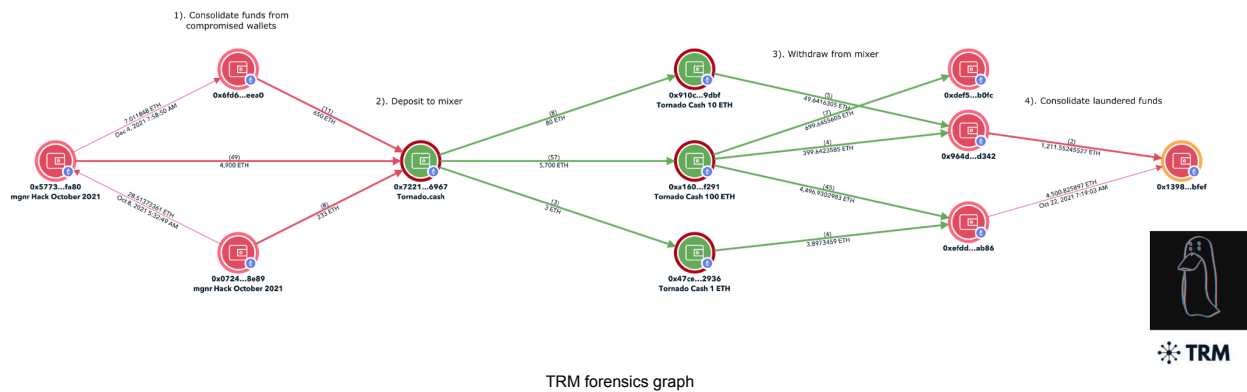
TRM forensics graph



While 1 X 100 ETH withdrawal is missing from the Tornado Cash demix for the 100 ETH pool there were no other withdrawals during that period which showed similar characteristics.

MGNR hack January 2022 laundering

On January 14, 2022 another 6 X 100 ETH and 5 X 10 ETH from an address connected to the theft was deposited to Tornado Cash. Just 24 hours later 4 X 100 ETH and 5 X 10 ETH was withdrawn to 0x964 before being transferred to 0x1398 further strengthening the demix due to the multiple denominations withdrawn over a sustained period of time.



TRM forensics graph

Transfer laundered funds to P2P exchanges

Through a series of transactions, the funds sitting in 0xdef, 0x964, and 0xefdd were transferred through intermediary addresses and consolidate with funds from other Lazarus Group hacks such as EasyFi, Bondly, and the Nexus Mutual founder before USDT was deposited to the P2P marketplace Paxful beginning in July 2022. In April 2023 they began using Noones, another P2P marketplace. They continue slowly sending USDT in batches until November 2023.

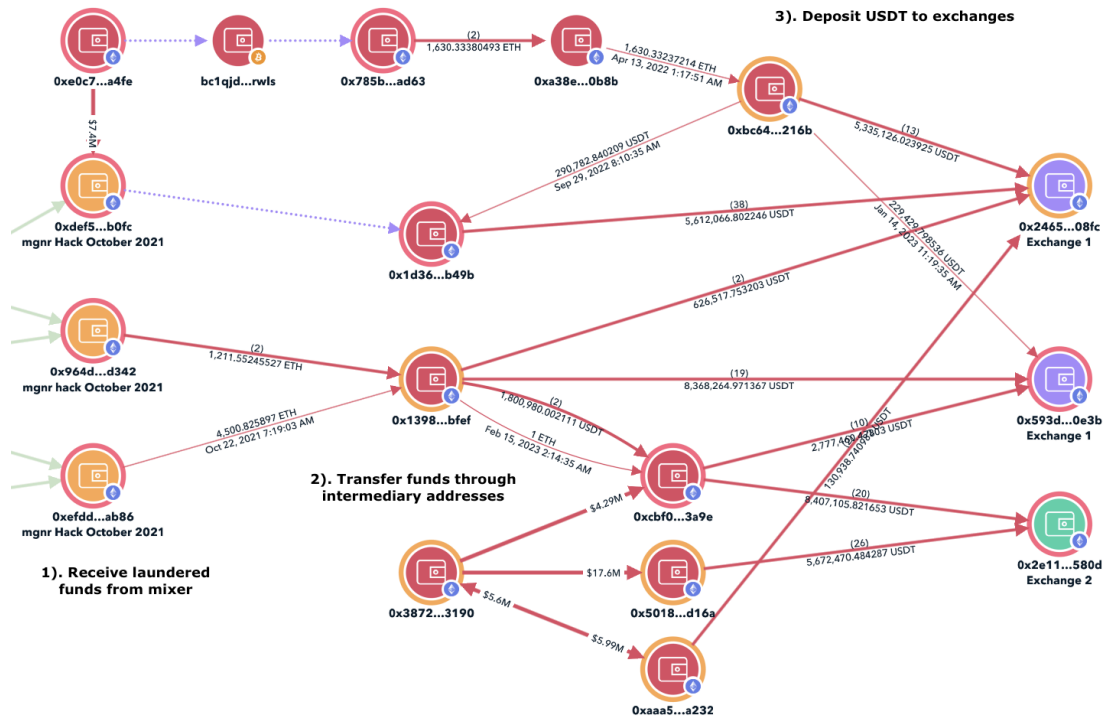
Paxful deposit address:

0x246569f8b420c8d850c475c53d0d59973b3f08fc

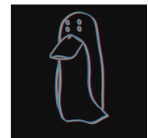
0x593dc5e1ad81667bbfc90739dd2c09c926920e3b

Noones deposit address:

0x2e1155cf5374cba058a04fd03ebd0ba19afe580d



TRM forensics graph



TRM

PolyPlay Incident Summary

October 28, 2021 in a series of transactions, multiple wallets controlled by the PolyPlay team saw unauthorized transfers of \$1.6M indicating a private key compromise. In a deleted post on X (formerly Twitter) the PolyPlay team shared the wallet address of the attacker and a Binance listing phishing email they received.

PolyPlay Official @PolyPlayCoin · 1h
 PolyPlay was hacked this morning by @binance @cz_binance @Teddy_Lin

Through a fake exchange listing email. This profile has been on LinkedIn for a long time with numerous high level executives in his connection list.

16 replies, 24 retweets, 62 likes

PolyPlay Official @PolyPlayCoin · 58m
 0x0040c81b7de0953e5b9fc056700479cace1b7500

The hackers wallet

@binance @cz_binance your lack of customer service and action against fake profiles has led to coins being manipulated.

You need to start providing proper customer service and avenues to reach out. @BinanceChain

willingness and contribution to social impact. A TXID will be generated afterwards that will be attached to your project to signify that your team is now a part of the Binance ecosystem.

Thanks for your kind gesture, kindly find the official Bitcoin wallet attached to your project for donation to our Binance charity foundation.

bc1qehfrdrpp5zmp7n4w74me8jk3s5c45uh748taxw

Best Regards,

Binance Listing Team.

www.binancelisting.com

Malta



On Thu, 28 Oct 2021 at 2:54 AM Claudiu wrote:

Website is PolyPlay.net

Source: <https://web.archive.org/web/20211028211901/https://twitter.com/PolyPlayCoin/status/1453833668196249605>

On-chain aspects:

Theft Address

0x0040c81b7de0953e5b9fc056700479cace1b7500

350 ETH from the incident was then deposited to Tornado Cash on November 8, 2021 and 320 ETH was withdrawn 90 minutes later to an address connected to other Lazarus Group hacks. Funds were later deposited to Paxful and Noones accounts.

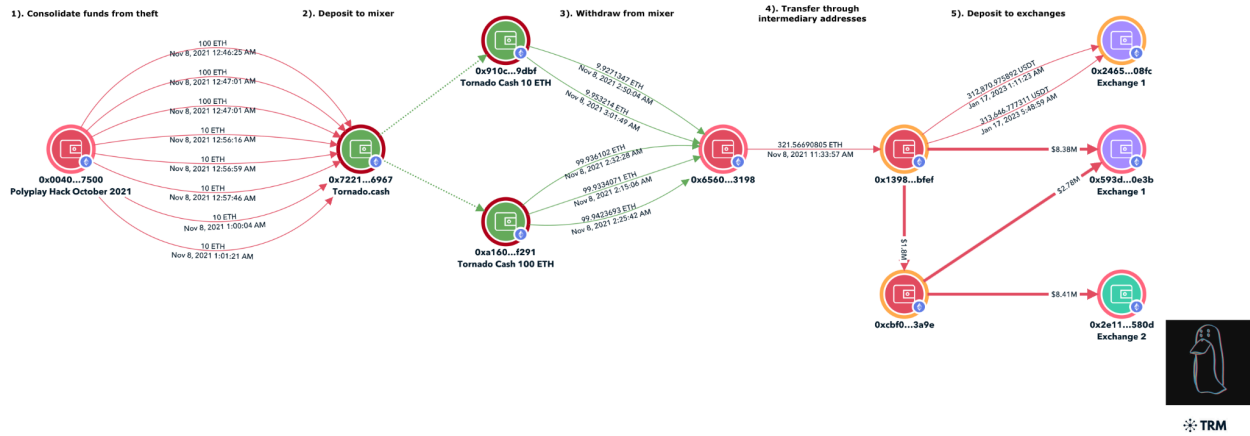
Paxful deposit address:

`0x246569f8b420c8d850c475c53d0d59973b3f08fc`

`0x593dc5e1ad81667bbfc90739dd2c09c926920e3b`

Noones deposit address:

`0x2e1155cf5374cba058a04fd03ebd0ba19afe580d`



TRM forensics graph

November 2021—bZx Hack

Incident Summary

On November 3, 2021 the lending protocol bZx had \$55M drained on the BSC and Polygon deployments after a bZx developer fell victim to a phishing attack after running a script on his personal computer granting the malicious actor access to their private keys.

In a [post mortem update](#) the bZx core team shared that they worked with Kaspersky to analyze the incident and reached the conclusion it was likely Lazarus Group as their security team had analyzed prior attacks carried out by the group finding similarities in the tools and phishing email received.



bZx - Fulcrum & Torque (on ETH/B...
@bZxHQ

Follow

An hour ago it appears that the private key controlling the Polygon and BSC deployments was compromised, leading to loss of funds. The Ethereum deployment is under DAO control and not impacted. We will provide further updates soon.

5:44 AM - 5 Nov 2021

21 Retweets 42 Likes

Source: <https://web.archive.org/web/20211105125919/https://twitter.com/bZxHQ/status/1456603269355094021>

Fwd : Pantera Capital Investment Agreement(Protected) ▶



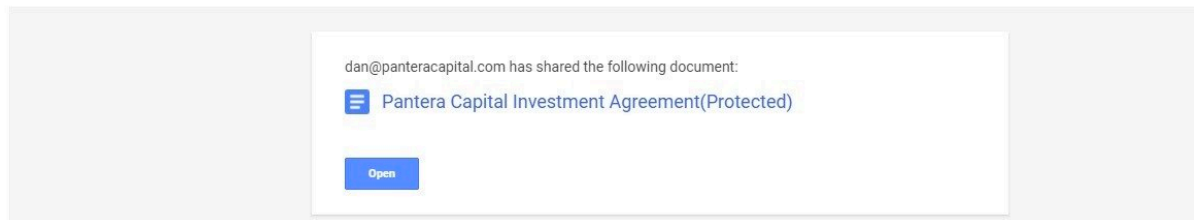
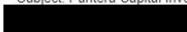
Kyle Kistner via sendgrid.net
to me ▾

5:45 PM (3 hours ago)


Can you give me your thought on this agreement>

----- Forwarded message -----

From: Dan Morehead (via Google Drive) <dan@panteracapital.com>
Date: Tue, May 4, 2021 at 11:34 AM
Subject: Pantera Capital Investment Agreement(Protected)



dan@panteracapital.com has shared the following document:

 Pantera Capital Investment Agreement(Protected)

[Open](#)

Phishing email

On-chain aspects

A [preliminary post-mortem](#) published by the bZx team shared wallet addresses involved with the hack.

Theft addresses

0x74487eed1e67f4787e8c0570e8d5d168a05254d4

0xafad9352eb6bcd085dd68268d353d0ed2571af89

0x0ACC0e5faA09Cb1976237c3a9aF3D3d4b2f35FA5

0x967bb571f0fc9ee79c892abf9f99233aa1737e31

0x6abcA33faeb7deb1E61220e31054f8d6Edacbc81

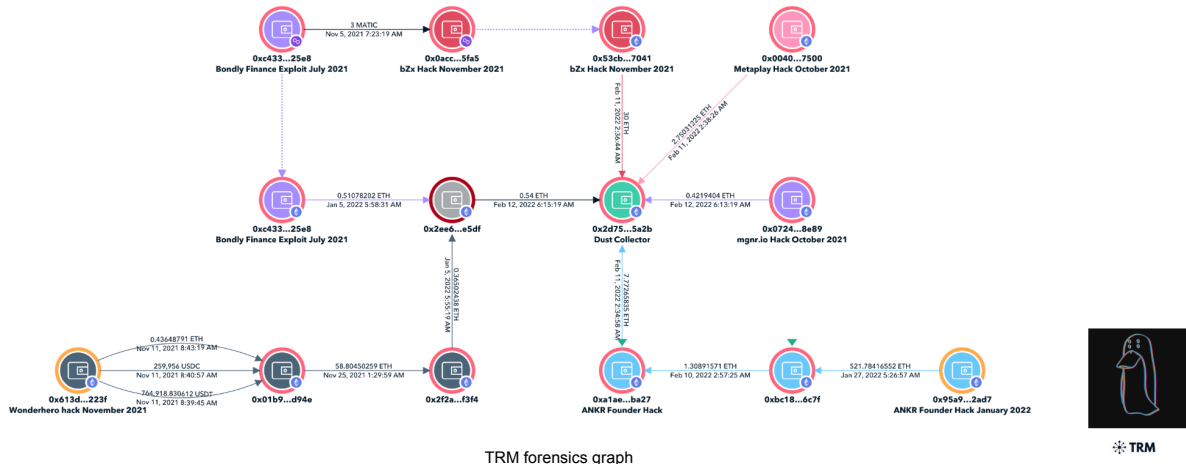
0x1ae8840ceaef6eec4da1b1e6e5fcf298800b46e6

Connections between theft addresses

The Bondly attacker was directly connected to the bZx hack from November 2021 as the 0xc43 theft address funded one of the addresses used by the bZx attacker on Polygon as well transferred funds on Ethereum to an intermediary address which received funds from another address involved in the bZx hack listed in the post-mortem blog post. Notably both attacks also share similar characteristics in the sense as the hacker gained access to a password and manipulated the protocols smart contracts after.

On-chain the incident is also connected to other hacks such as mgnr.io, Polyplay, Wonderhero and ANKR founder as dust leftover in theft addresses was swept to a single address in February 2022.

0x2d7554062664050294640891a122019a68ac5a2b



bZx hack laundering

Tornado Cash deposits

- 8600 ETH from the theft was deposited to Tornado Cash from November 15–18, 2021 by 0x20d9
- 2360 ETH from the theft was deposited to Tornado Cash on December 13, 2021 by 0x20d9

Tornado Cash withdrawals:

- 4100 ETH likely from the theft was withdrawn to 0x7c6 from December 3–10, 2021.

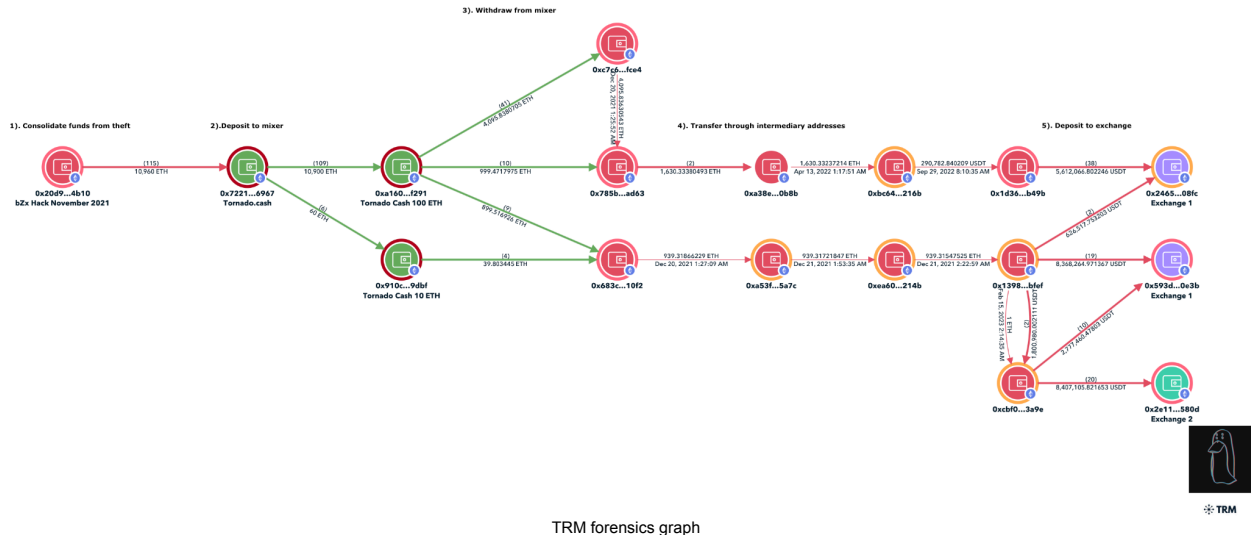
0xc7c6d42875fd091faa16ad0225f587158f47fce4

- 940 ETH likely from the theft was withdrawn to 0x683 on December 18, 2021

0x683c3d42325ca1beb2475f443c916832f0bd10f2

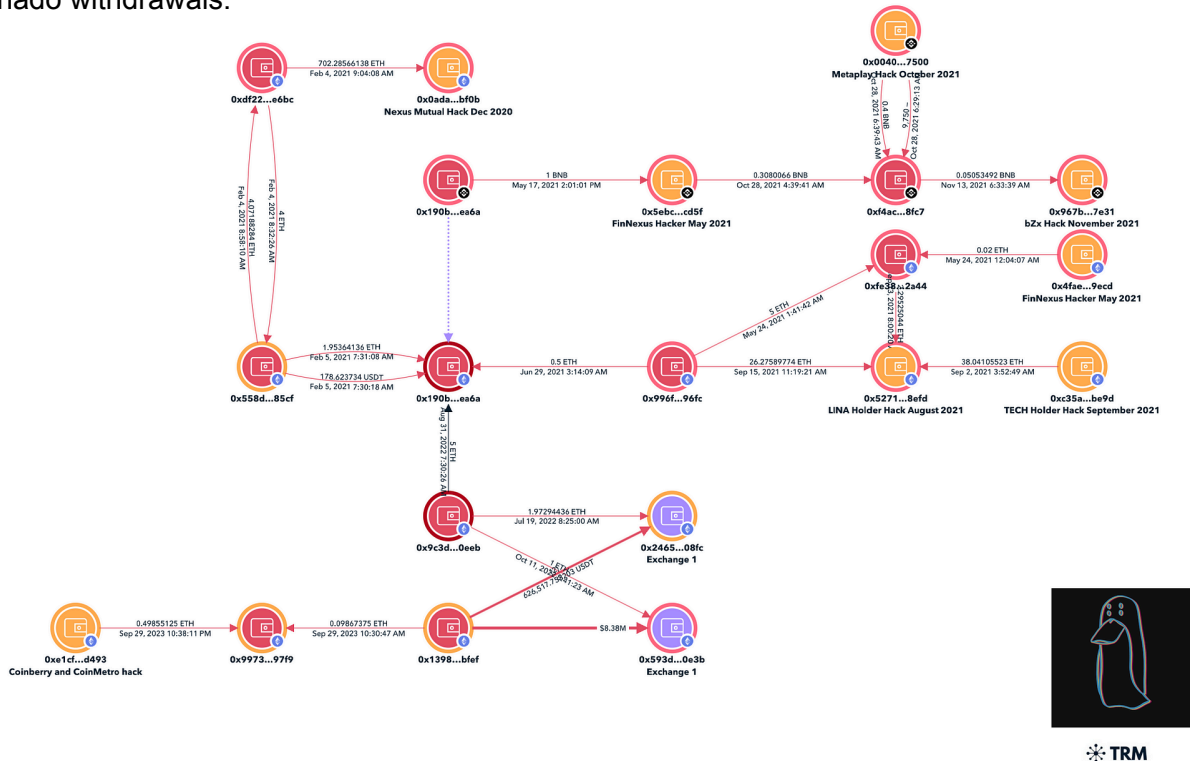
- 1000 ETH likely from the theft was withdrawn to 0x785b on December 23, 2021.

Reviewed all Tornado withdrawals 400 ETH or more from November 15—December 31, 2021 and no other withdrawals during this period shared similar characteristics of laundering patterns from other Lazarus Group thefts.



Post-Mix connections to theft addresses

While only a partial demix of 6,400 ETH from the hack comfort is gained as on-chain the Paxful deposit addresses 0x2465 and 0x593d are connected to Coinberry, CoinMetro, Nexus Mutual, FinNexus, PolyPlay, bZx hacks linking the original theft addresses from multiple incidents to the Tornado withdrawals.



August 2023—Stedefi & CoinShift Hacks

Stedefi Incident summary

On August 7, 2023 the Steadefi team made a post on X (formerly Twitter) informing the community its deployer wallet had been compromised and an attacker had transferred ownership of all lending and strategy vaults to an address the attacker controlled, allowing them to drain \$1.2M of users assets.

A [recent DPRK report published by the United Nations](#) from March 2024 revealed a Steadefi team member had been in contact with someone on Telegram pretending to work at a fund named “Spirit Blockchain Group” where the attacker sent a malicious file disguised as a presentation for their investment fund which the Steadefi team member downloaded.



Source: <https://x.com/stedefi/status/1688619454178144264>



Source: https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports_S/2024/215 7 March 2024

Steadefi On-Chain Aspects

In a post on X (formerly Twitter) the Steadefi team shared the wallet of the attacker.

Theft address:

0x9cf71f2ff126b9743319b60d2d873f0e508810dc

Coinshift Incident Summary

While no public statements have been made about the incident, due to the sudden transfers of assets from multisig wallets tied to the founder on which were sold immediately August 16, 2023 it is likely the founder was a victim of a private key compromise.

Coinshift On-Chain Aspects

Theft address:

0x979ec2af1aa190143d294b0bfc7ec35d169d845c

0x68c4a151d436ec1c5448d225a97bd19cce4dfed0

0xbcd5b968a79a04bf2bb942a449f10c20a7121ed8

0x4c7c2b39e3d642d452adfca632939a60b1baacf7

August 2023 Laundering:

624.3 ETH was deposited to Tornado Cash by 0xe10d from the Steadefi hack in August 2023.

900 ETH was deposited to Tornado Cash by 0x68c4 from the Coinshift hack in August 2023.

Further evidence that the attacks were done by the entity is shown through the overlap between deposits made to the Tornado Cash 100 ETH pool within minutes of each other by the Steadefi and Coinshift attacker on August 23, 2023.

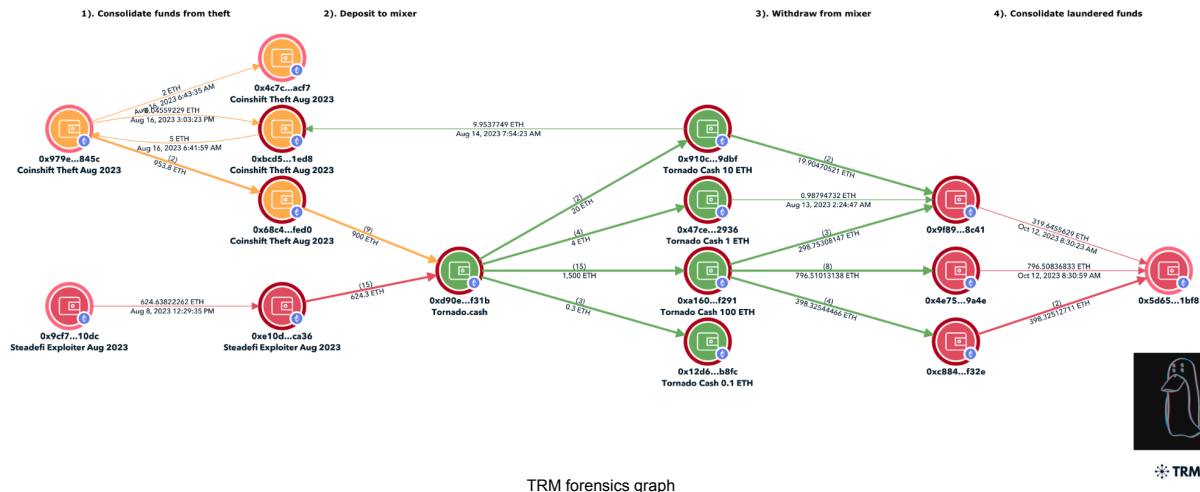
The table below shows 15 X 100 ETH deposited to the Tornado Cash 100 ETH pool from both incidents.

Victim	Date and Time	Transaction Hash	Amount	Address	Action
Steadefi	Aug-12-2023 8:27 AM UTC	84e9c14bd576f09d8523b1ed5538d6861ef692567dedb4676ad02b1954b7e907	100 ETH	0xe10d4a5bd440775226c7e1858f573e379d0aca36	Deposit
Steadefi	Aug-13-2023 1:50 AM UTC	0xc79f37d9a938374dbe58985942809e27a7efeaefdba0bd96b03df4e5eb573b6b3	100 ETH	0xe10d4a5bd440775226c7e1858f573e379d0aca36	Deposit
Steadefi	Aug-14-2023 8:38 AM UTC	0xbca24a3413040aae23734be6e55914623741fb5c808a81aa3d1d4d37185c0984	100 ETH	0xe10d4a5bd440775226c7e1858f573e379d0aca36	Deposit
Steadefi	Aug-14-2023 8:39 AM UTC	0x7b6228e5f0b743ea3c8373d0e319828db3125ec9527d3c17c33da4203225d38b	100 ETH	0xe10d4a5bd440775226c7e1858f573e379d0aca36	Deposit
Steadefi	Aug-23-2023 3:02 PM UTC	0xcaaf7423e4913275d743a3654dfcd5d0c0a263774609b9f91c9ce2037f9cfc1	100 ETH	0xe10d4a5bd440775226c7e1858f573e379d0aca36	Deposit
Steadefi	Aug-23-2023 3:03 PM UTC	0xae6c879f0073ef92527f10dced067d22ebfb1d1bdb342cc8a087ebb3b9ad643c	100 ETH	0xe10d4a5bd440775226c7e1858f573e379d0aca36	Deposit
Coinshift founder	Aug-23-2023 3:06 PM UTC	0x4350fd8e07054313fcd4a4d0367975bad1dfc217750c0a9ba65d609ac218298	100 ETH	0x68c4a151d436ec1c5448d225a97bd19cce4dfd0	Deposit
Coinshift founder	Aug-23-2023 3:06 PM UTC	0xe1f199fed6223634f2e9785114dd9aeca9ed3ba4639b5123cdabc9884c8db	100 ETH	0x68c4a151d436ec1c5448d225a97bd19cce4dfd0	Deposit
Coinshift founder	Aug-23-2023 3:07 PM UTC	0x057272ac9f1b9f90f802b1845bd1190c1f2a86c80588b94c60216945a63d3d77	100 ETH	0x68c4a151d436ec1c5448d225a97bd19cce4dfd0	Deposit
Coinshift founder	Aug-23-2023 3:08 PM UTC	0xc19f6e22279a945e2aee06af5a74ce9c1366a5d060f3a203b8f66f8389cbfeef	100 ETH	0x68c4a151d436ec1c5448d225a97bd19cce4dfd0	Deposit
Coinshift founder	Aug-23-2023 3:08 PM UTC	0xf156df23d5e362746327265983bfc77eea8394992d0c98ae64678dc81c7276a0e	100 ETH	0x68c4a151d436ec1c5448d225a97bd19cce4dfd0	Deposit
Coinshift founder	Aug-24-2023 6:24 AM UTC	0xea23678f217f6d5521fa4b724f417bbb204cc173dd6d4e91783f016f71ec4865	100 ETH	0x68c4a151d436ec1c5448d225a97bd19cce4dfd0	Deposit
Coinshift founder	Aug-24-2023 6:29 AM UTC	0x8305049c3f307dd2cd39db53bd7d1fd5a09f96e828d10937d774e4239f55d	100 ETH	0x68c4a151d436ec1c5448d225a97bd19cce4dfd0	Deposit
Coinshift founder	Aug-24-2023 6:49 AM UTC	0xb1b2cd6625d2dd48a64e31f2de34526c1bc87b93ce381ba33564d3366db7742b	100 ETH	0x68c4a151d436ec1c5448d225a97bd19cce4dfd0	Deposit
Coinshift founder	Aug-24-2023 6:50 AM UTC	0x815b4c6078dba652d9a1433038e1a7b84e622e0762150ea5cab3f30b7531a37	100 ETH	0x68c4a151d436ec1c5448d225a97bd19cce4dfd0	Deposit

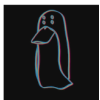
Table 7: Steadefi & Coinshift Tornado Cash 100 ETH deposits

Within 24 hrs of the deposits to the Tornado Cash 100 ETH pool, matching amounts were withdrawn to three addresses and later consolidated to a single address on October 12, 2023.

0x5d65aeb2bd903bee822b7069c1c52de838f11bf8



TRM forensics graph



TRM

Date and Time	Transaction Hash	Amount	Address	Action
Aug-13-2023 1:35 AM UTC	0x499dae0411931bdb396a704894ac824f434e7b4c6f8828a8872db151a0fa7dd8	100 ETH	0xc884cf2fb3420420ed1f3578eaeecbde53468f32e	Withdrawal
Aug-14-2023 1:02 AM UTC	0x6c7c233bd39ddfd920e0b04ac23a935c19be332a46e0d82cf75f43eb4ac209a2	100 ETH	0x4e75c46c299ddc74bac808a34a778c863bb59a4e	Withdrawal
Aug-16-2023 3:26 PM UTC	0xb589962b62c59ed2e8c5977ba614ce94bfc9d107015ad67a1e9391122a03e849	100 ETH	0xc884cf2fb3420420ed1f3578eaeecbde53468f32e	Withdrawal
Aug-17-2023 11:36 PM UTC	0xf23aa066bbaaac2cd34b850791314d6a070148e1fb4440cad1d5a8ceb4e811b	100 ETH	0xc884cf2fb3420420ed1f3578eaeecbde53468f32e	Withdrawal
Aug-24-2023 5:30 AM UTC	0xa23628410e99c908ebd3839e7d928f72b7a896c80714f3e1e1321f057f573a2c	100 ETH	0xc884cf2fb3420420ed1f3578eaeecbde53468f32e	Withdrawal
Aug-24-2023 6:02 AM UTC	0xbf61cd7e50303f602220e28298d6f98b211073d42d8245dd3c20e910d3be191	100 ETH	0x9f8941cd7229aa3047f05a7ee25c7ce13cbb8c41	Withdrawal
Aug-24-2023 6:17 AM UTC	0xae4f5a05724f045f7bcc720c9f88ddab5dd024e08b8f04ebe8789cd4bfd542a0	100 ETH	0x9f8941cd7229aa3047f05a7ee25c7ce13cbb8c41	Withdrawal
Aug-24-2023 6:30 AM UTC	0x7c89734cb0003b0cfea8a5f2422d2357a07f4ac5634f5cbb1d13653c0a93313	100 ETH	0x4e75c46c299ddc74bac808a34a778c863bb59a4e	Withdrawal
Aug-24-2023 6:34 AM UTC	0x8f93ea6db99d8a4a979931b7adb61551d1077aba33611e4b7092d25899824ea7	100 ETH	0x4e75c46c299ddc74bac808a34a778c863bb59a4e	Withdrawal
Aug-24-2023 6:45 AM UTC	0x750daa582a682be4d1912c6a87d49e954d89900a1eac0cf124a6c295f1700914	100 ETH	0x4e75c46c299ddc74bac808a34a778c863bb59a4e	Withdrawal
Aug-24-2023 6:58 AM UTC	0x6cdb391b2f3cc82129bbe38bcee21c33d7701e92135c167192f4bb2e6ccdbf0	100 ETH	0x4e75c46c299ddc74bac808a34a778c863bb59a4e	Withdrawal
Aug-26-2023 12:28 AM UTC	0x05ed749eab53d1111867ca646a8cd2e10128cf19392a007e3489ced182f5646d	100 ETH	0x4e75c46c299ddc74bac808a34a778c863bb59a4e	Withdrawal
Aug-26-2023 12:30 AM UTC	0x95f09f1eea597fcff5910fa0ca00194d0989b472c8afec8f42da8a184045145a	100 ETH	0x4e75c46c299ddc74bac808a34a778c863bb59a4e	Withdrawal
Aug-26-2023 12:55 AM UTC	0x015cd6b0209fef494cec051248a43f88784f8a246633df430ec813f0f86375eb	100 ETH	0x9f8941cd7229aa3047f05a7ee25c7ce13cbb8c41	Withdrawal
Aug-26-2023 2:38 AM UTC	0xac714a7159996e756d44f544333b19e05f4eb9eec23855330b15c24268f614dc	100 ETH	0x4e75c46c299ddc74bac808a34a778c863bb59a4e	Withdrawal

Table 8: Steadefi and Coinshift Tornado Cash 100 ETH withdrawals

Transfer laundered funds to P2P exchange accounts:

Through a series of transactions, the funds sitting in 0x5d were converted to USDT, transferred through intermediary addresses and deposited to P2P marketplaces Paxful and Noones in November 2023. The Paxful deposit address 0x2465 has been reused for other Lazarus Group hacks such as EasyFi, Bondly, and Nexus Mutual.

Paxful deposit address:

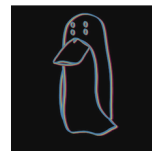
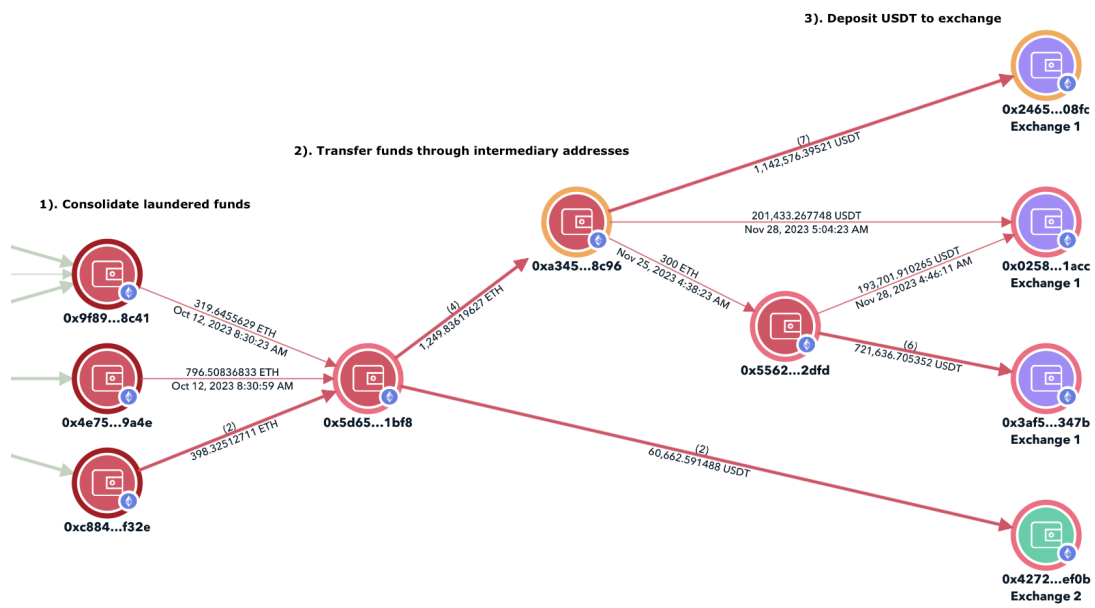
0x246569f8b420c8d850c475c53d0d59973b3f08fc

0x0258c2af4fe694df026cca55d17febd5b361acc

0x3af55ab7edbca175f80f3a7ddeac5dabf611347b

Noones deposit address:

0x4272200ef626d409e9bac681aa0efdb653a9ef0b



TRM

TRM forensics graph

Paxful and Noones accounts receive \$44M from Lazarus Group hacks through July 2022– November 2023

Paxful deposit address

\$12.8M deposits from July 2022—November 2023

0x246569f8b420c8d850c475c53d0d59973b3f08fc

\$12.1M total deposits from January 2023—November 2023

0x593dc5e1ad81667bbfc90739dd2c09c926920e3b

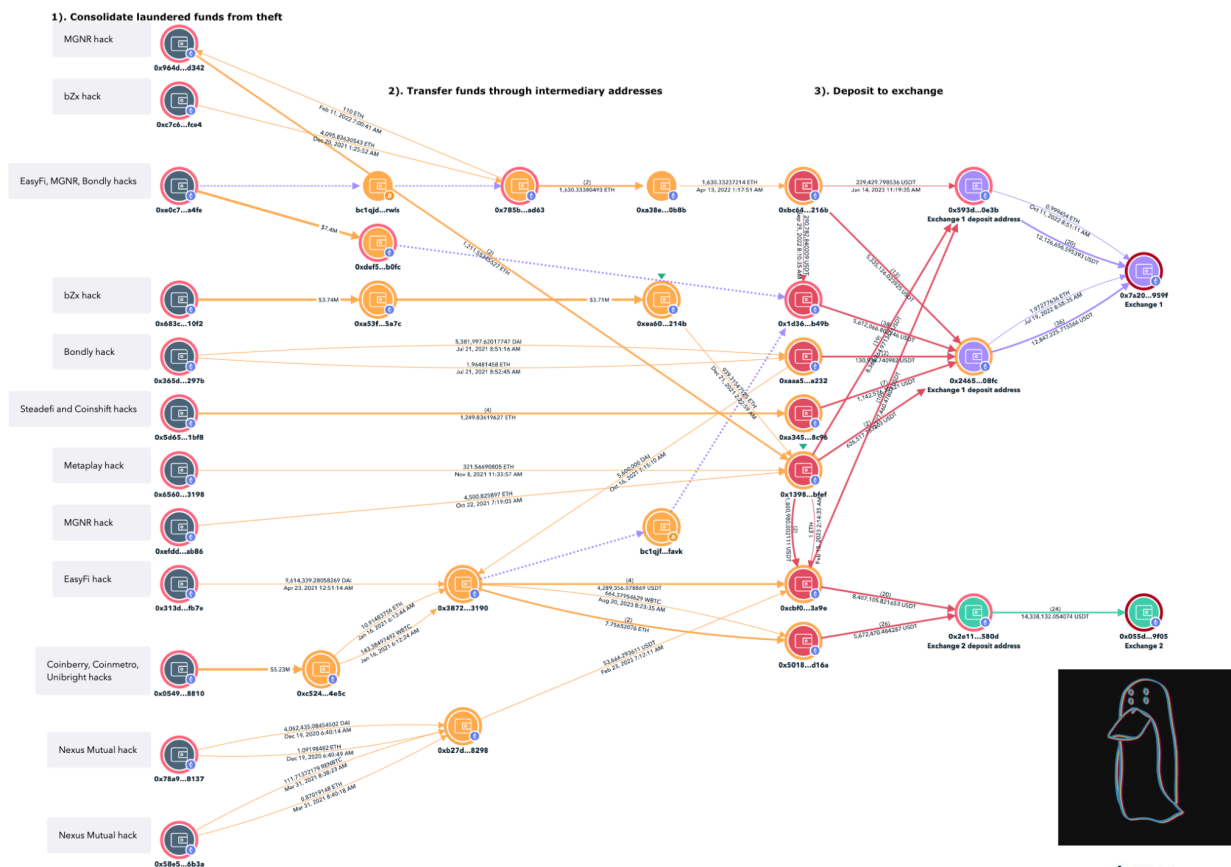
Noones deposit address

\$14.3M total deposits from April 2023—November 2023

0x2e1155cf5374cba058a04fd03ebd0ba19afe580d

November 25, 2023 Lazarus group began using new Paxful and Noones deposit addresses.

[Full list can be found here.](#)



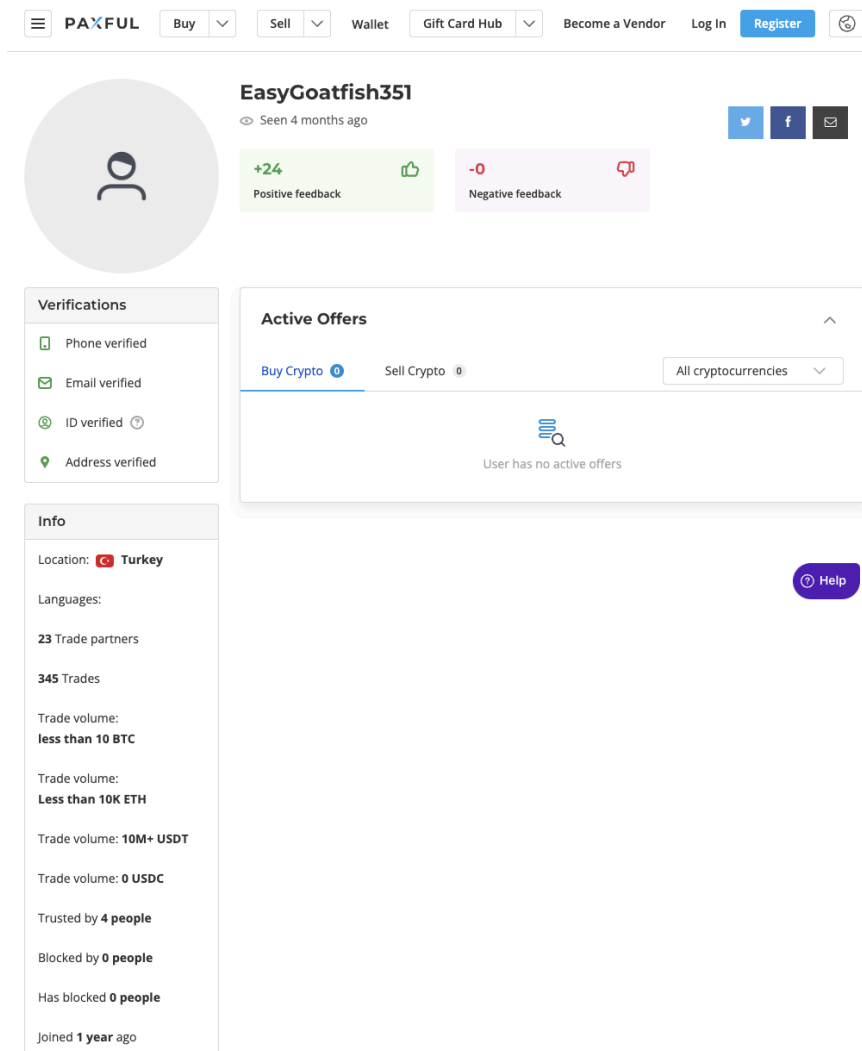
Converting \$44M to fiat on P2P marketplaces Paxful and Noones

OSINT analysis was conducted and I identified two users which were active on Paxos and Noones and displayed trading volume consistent with the amount deposited from the hacks.

EasyGoatfish351

FairJunco470

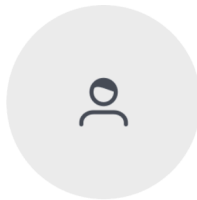
The timing of activity on these accounts further matches the deposit. Very few other accounts on Paxful and Noones showed similar levels of trading volume. Taken together, it is very likely that these were the accounts being used.



The screenshot shows the Paxful user profile for 'EasyGoatfish351'. The profile includes a header with navigation links (Buy, Sell, Wallet, Gift Card Hub, Become a Vendor, Log In, Register) and a user profile card with a placeholder avatar, name, and social media links. Below the profile card are two boxes: 'Verifications' and 'Active Offers'. The 'Verifications' box lists: Phone verified, Email verified, ID verified, and Address verified. The 'Active Offers' box shows 'Buy Crypto' and 'Sell Crypto' buttons, a dropdown for 'All cryptocurrencies', and a message 'User has no active offers'. To the right of the 'Active Offers' box is a purple 'Help' button. Below the profile card is an 'Info' section with the following details:

- Location: Turkey
- Languages:
- 23 Trade partners
- 345 Trades
- Trade volume: less than 10 BTC
- Trade volume: Less than 10K ETH
- Trade volume: 10M+ USDT
- Trade volume: 0 USDC
- Trusted by 4 people
- Blocked by 0 people
- Has blocked 0 people
- Joined 1 year ago

Screenshot from Paxful



FairJunco470

Seen 6 months ago



+9 Positive feedback

-0 Negative feedback

Verifications

- Phone verified
- Email verified
- ID verified
- Address verified

Active Offers

Buy Crypto 0 Sell Crypto 0 All cryptocurrencies

User has no active offers

Info

Location: Belgium

Languages:

14 Trade partners

263 Trades

Trade volume: 0 BTC

Trade volume: 0 ETH

Trade volume: 10M+ USDT

Trade volume: 0 USDC

Trusted by 7 people

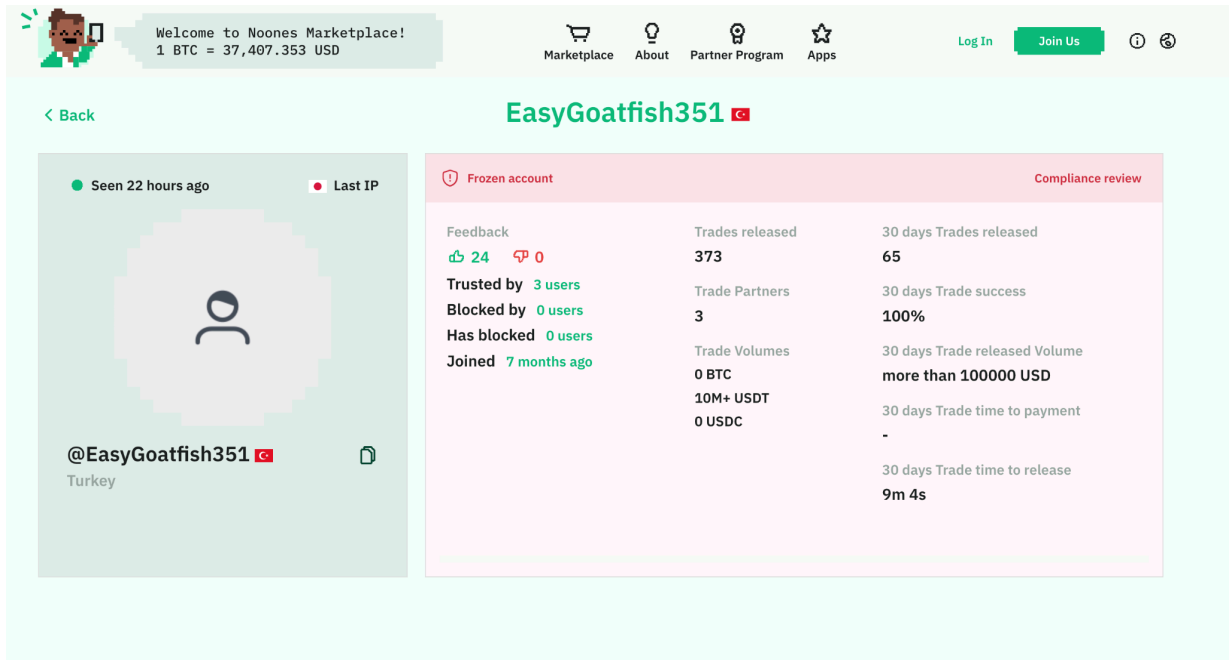
Blocked by 0 people

Has blocked 0 people

Joined 1 year ago

Help

Screenshot from Paxful



Screenshot from Noones

Additionally, the hot wallet outflows for Noones and Paxful were analyzed and no matching crypto withdrawals of similar volumes were observed, indicating USDT was likely being exchanged for bank transfers or cash after deposits were made to the site.

Historically Lazarus Group [has used Chinese OTC traders](#) to convert crypto to fiat.

Results of the investigation

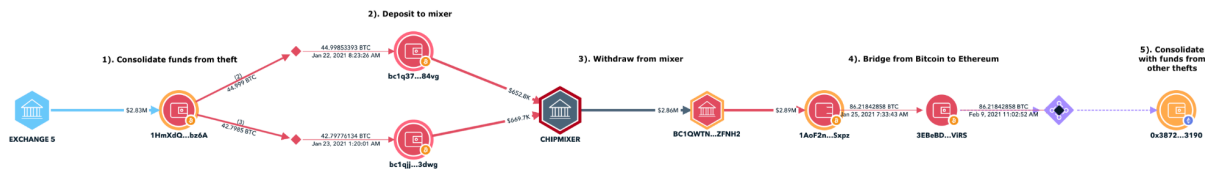
At the time of this article 374K USDT was blacklisted by Tether in November 2023 and an undisclosed amount was frozen at centralized exchanges in Q4 2023.

- *0x5018CF5F48A09C46b4833890cC2cF0df2533D16A*

3 of 4 stablecoin issuers have blacklisted an additional \$3.4M sitting in a group of addresses. This article will be updated after the 4th follows suit.

Other connected incidents

Exchange user hack—January 2021



TRM

Source address: 1HmXdQx3TCVibvjPAp3BrR7awbe6Gtbz6A

Arthur0x hack—March 2022

Arthur @Arthur_0x

Found out the likely root cause for the exploit, it's a targeted social engineering attack. Received a spear-phishing email that really seems to be sent by one of our portco with content that seems like general industry-relevant content.

They are likely targeting all crypto peep

Forwarded message

From: Jehan Chu (via Google Drive) <@jehanchu@kenetic.capital>
 Date: Sat, 12 March 2022 at 11:01
 Subject: Document shared with you: 'A Huge Risk of Stablecoin (Protected).docx'
 To: <@jehanchu@kenetic.capital>

jehan@kenetic.capital shared a document

jehan@kenetic.capital has shared the following document:

A Huge Risk of Stablecoin (Protected).docx

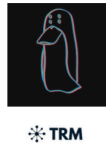
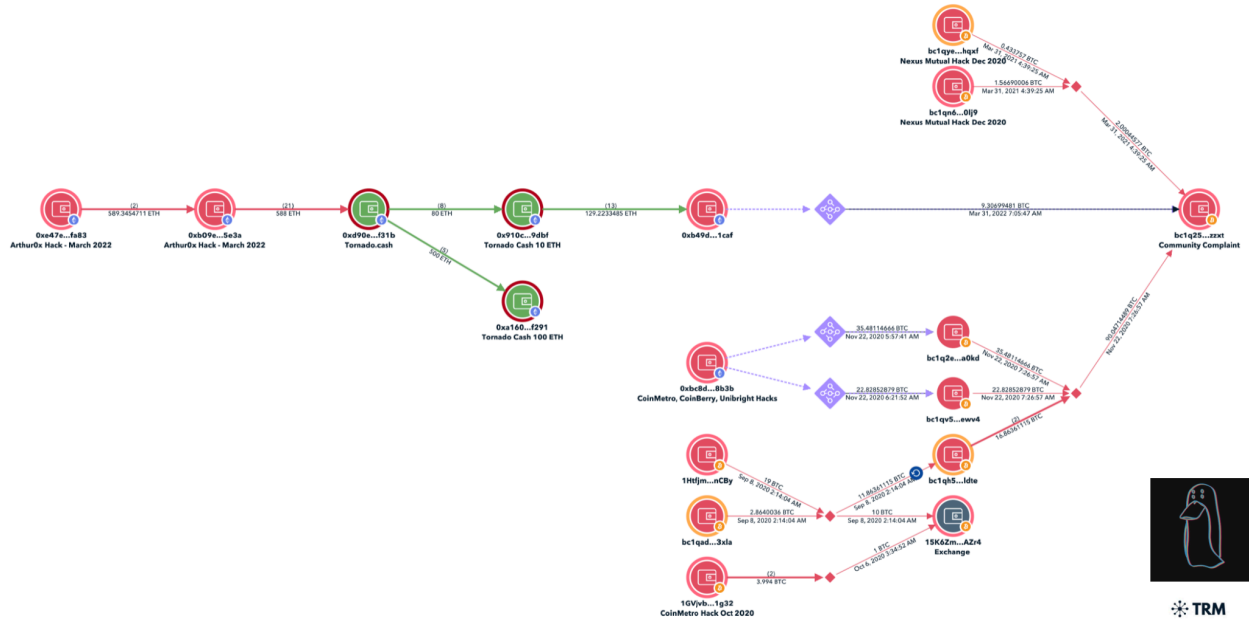
[Open](#)

Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
 You have received this email because jehan@kenetic.capital shared a file or folder located in Google Drive with you.

7:16 AM · Mar 22, 2022

642 Reposts 257 Quotes 2,055 Likes 268 Bookmarks

Source: https://twitter.com/Arthur_0x/status/1506167899437686784



Source address:0xb09e66b66b7daa35699496ff560e1034990e5e3a

Geracoin & Darshan hack—September & October 2022



Dear GERA holders,

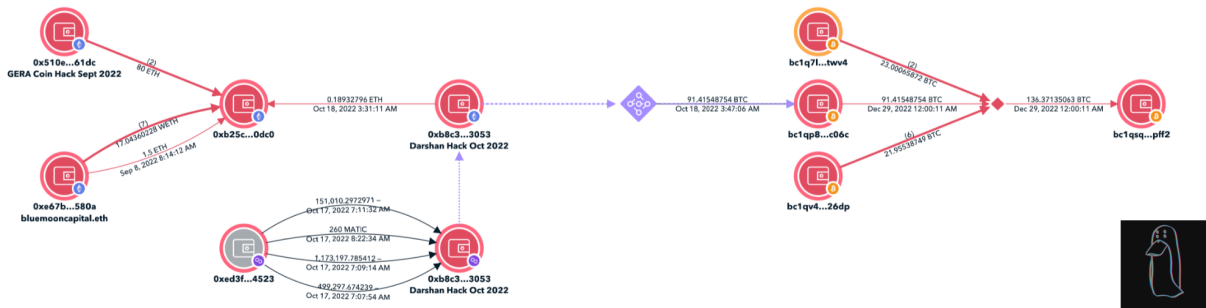
It has come to our attention that the GERA token's security has been compromised due to a private key leak. Hackers transferred ownership of the GERA token's smart contract deployer to another address: "0x510E4d61663bE6a24D600AaF90F892dd8c8C61dC".



3:43 PM · Sep 7, 2022

6 Reposts 5 Quotes 14 Likes

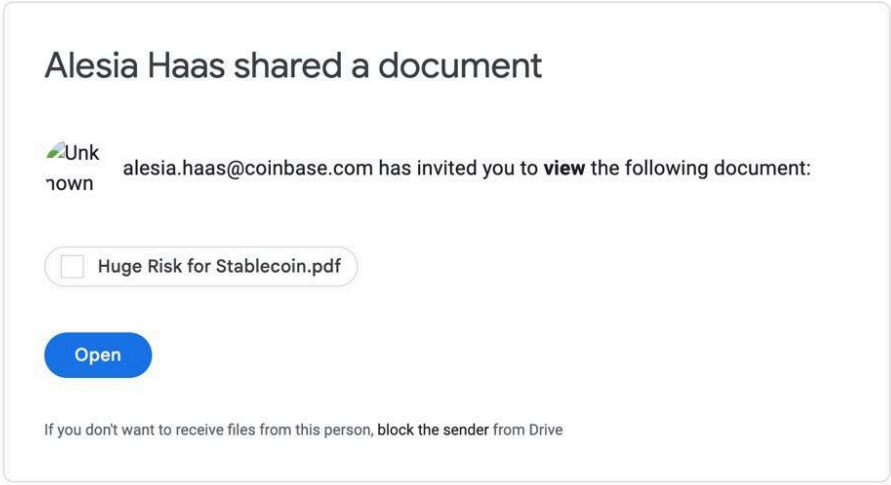
Source: <https://twitter.com/GeraCoin/status/1567538962410995713>



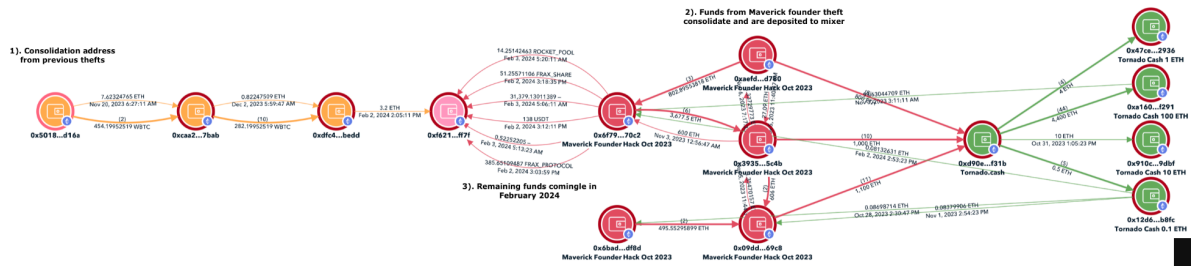
Source address: 0xb25caeb548c40c564d2067a69a913cae14750dc0

Maverick Founder hack—October 2023

----- Forwarded message -----
 From: ██████████ (via Google Docs) <drive-shares-dm-noreply@google.com>
 Date: Tue, May 23, 2023 at 08:38 AM
 Subject: Document shared with you: "Huge Risk for Stablecoin.pdf"
 To: <██████████>



Phishing email



TRM

Source address: 0x6f79657e33ff6816349c81e2e9852d76b39370c2

A special thanks to

- Taylor Monahan from Metamask
- Symbiotic from Binance Security Team
- Nick Bax from Five I's
- Nick Carlsen from TRM Labs

for their contributions and guidance with the investigation.

Sources

Chainalysis Crypto hacks 2024

<https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/>

Chainalysis crypto hacks 2022

<https://www.chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/>

The All-Purpose Sword: North Korea's Cyber Operations and Strategies 2019

https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf

TRM crypto hacks 2023

<https://www.trmlabs.com/post/north-korean-hackers-stole-600-million-in-crypto-in-2023>

Bangladesh Bank Heist - Kaspersky

https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies

CoinBerry

<https://www.quadrigainitiative.com/casestudy/nothinghappenedatcoinberry.php>

<https://www.coindesk.com/business/2022/09/08/canadian-crypto-exchange-coinberry-files-lawsuit-against-50-users-after-losing-120-btc/>

Unibright Jack Tweet

<https://twitter.com/Sjaaaakster/status/1304531302255910912>

Unibright Telegram post

https://t.me/unibright_io/211959

CoinMetro

<https://medium.com/parsiq/transcript-the-crazy-story-behind-the-coinmetro-hack-72091b6f07b8>

<https://web.archive.org/web/20201101073137/https://blog.parsiq.net/coinmetro-hack-poloniex-and-next-steps/>

<https://t.me/coinmetroudates/601>

US vs 280 cryptocurrency accounts

<https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges>

Wu Huihui, Chinese OTC trader

<https://home.treasury.gov/news/press-releases/jy1435>

<https://www.justice.gov/opa/pr/north-korean-foreign-trade-bank-representative-charged-crypto-laundering-conspiracies>

CoinMetro Hack archive

<https://web.archive.org/web/20201101073137/https://blog.parsiq.net/coinmetro-hack-poloniex-and-next-steps/>

Unibright Hack

<https://github.com/tayvano/lazarus-bluenoroff-research/blob/main/hacks-and-thefts/Unibright.md>

Hugh Karl (Nexus Mutual Founder) Tweet

<https://x.com/hughkarp/status/1341063567408328705>

Nexus Mutual Hack Blog Post

https://medium.com/@hugh_karp/nxm-hack-update-72c5c017b48

Kaspersky Bluenoroff Research

<https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/>

EasyFi Hack Blog Post

<https://medium.com/easify-network/easyfi-security-incident-pre-post-mortem-33f2942016e9>

EasyFi Incident Post

<https://x.com/ankittgaur/status/1384253351492087819>

Bondly Post-Mortem

<https://forj.medium.com/bondly-attack-july-14th-2021-postmortem-beb7cf02e9ba>

<https://medium.com/mantra-dao/bondly-exploit-how-it-unfolded-on-zenterest-postmortem-d8120d8d784b>

Bondly Incident Post

<https://x.com/forjofficial/status/1415543486141636612>

MGNR Tweet archive

https://web.archive.org/web/20211014032211/https://twitter.com/mgnr_io/status/1448489258029703168/

MGNR Wallets Blog Post

<https://cryptocatvc.medium.com/mgnr-io-maple-finance-7e70241e5f4>

PolyPlay Tweet archive

<https://web.archive.org/web/20211028211901/https://twitter.com/PolyPlayCoin/status/1453833668196249605>

bZx Incident Post archive

<https://web.archive.org/web/20211105125919/https://twitter.com/bZxHQ/status/1456603269355094021>

bZx Post-Mortem Archive

<https://web.archive.org/web/20211111211421/https://bzx.network/blog/post-mortem-update>

<https://web.archive.org/web/20211105225627/https://bzx.network/blog/preliminary-post-mortem>

Stedefi X Post

<https://x.com/stedefi/status/1688619454178144264>

United Nation DPRK report (S/2024/215 7 March 2024)

https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

Paxful and Noones Chainabuse Report

<https://www.chainabuse.com/report/8f714069-47da-471b-b3e6-95b0c1dd8329?context=browse-all>

Tayvano Lazarus Bluenoroff Github

<https://github.com/tayvano/lazarus-bluenoroff-research>

Arthur0x X/Twitter Thread

https://twitter.com/Arthur_0x/status/1506167899437686784

GeraCoin X/Twitter post

<https://twitter.com/GeraCoin/status/1567538962410995713>