

Portofolio Analisis Crypto Forensics

(Studi Kasus Ronin Bridge Hack 2022)

A. Pendahuluan

Dalam beberapa tahun terakhir, kasus peretasan di dunia crypto semakin meningkat. Nilai kerugian yang ditimbulkan pun tidak main-main, bisa mencapai ratusan juta hingga miliaran dolar AS. Kejadian ini membuktikan bahwa industri blockchain bukan hanya tempat untuk berinvestasi, tetapi juga target empuk bagi para peretas.

Di sinilah peran *crypto forensics* menjadi penting. Analisis forensik blockchain bertujuan untuk menelusuri pergerakan dana, mengidentifikasi wallet terkait, dan memahami pola transaksi dari para pelaku. Meskipun teknologi blockchain bersifat transparan, tanpa metode analisis yang tepat, data on-chain yang sangat besar akan sulit dipahami.

Portofolio ini saya buat sebagai bukti kemampuan dalam melakukan analisis crypto forensics menggunakan kasus nyata. Saya memilih salah satu kasus besar yang sempat mengejutkan industri crypto, yaitu *Ronin Bridge Hack (2022)*. Analisis ini dilakukan menggunakan tools gratis seperti *Etherscan*, *Breadcrumbs*, dan *Wallet Alert*. Selain itu, saya juga memberikan catatan mengenai penggunaan tools profesional seperti *Arkham Intelligence* atau *Nansen*, agar pembaca memahami perbedaan tingkat analisis.

B. Metodologi

Untuk melakukan analisis, saya menggunakan beberapa langkah dasar:

1. Identifikasi Kasus dan Address Utama

- Mengambil data alamat wallet yang dilaporkan terlibat dalam serangan.
- Sumber: artikel resmi, laporan audit, dan data publik dari blockchain explorer.

2. Analisis On-Chain

- Melacak transaksi dengan *Etherscan* (Ethereum) atau *block explorer* lainnya.
- Menggunakan *Breadcrumbs* untuk visualisasi alur dana.

3. Monitoring dan Alert

- Membuat *Etherscan Alerts* untuk memantau aktivitas wallet.
- Menambahkan *bot Telegram* atau *Wallet Alert* sebagai notifikasi tambahan.

4. Pencatatan Temuan

- Menyusun laporan berupa tabel ringkasan: alamat wallet, jumlah transaksi, saldo, aktivitas terakhir.
- Membuat dokumentasi visual (screenshot) untuk memperkuat hasil analisis.

5. Tools Profesional (Opsional)

- Menyebutkan bagaimana hasil analisis bisa lebih dalam jika menggunakan *Arkham Intelligence*, *Nansen*, atau *TRM Labs*.

C. Studi Kasus (*Ronin Bridge Hack (2022)*)

1. Ringkasan Kasus

Pada Maret 2022, *Ronin Network*, sidechain yang digunakan oleh game *Axie Infinity*, mengalami peretasan besar. Peretas berhasil mencuri lebih dari **\$600** juta dalam bentuk *ETH* dan *USDC*. Insiden ini menjadi salah satu peretasan terbesar dalam sejarah crypto.

2. Analisis Address

Salah satu alamat yang dikonfirmasi terlibat dalam serangan ini adalah:

0x098B716B8Aaf21512996dC57EB0615e2383E2f96

Alamat ini sempat digunakan untuk menyalurkan dana hasil curian sebelum akhirnya dipindahkan melalui mixer seperti ***Tornado Cash***.

3. Visualisasi

a) Menggunakan ***Etherscan*** untuk melihat riwayat transaksi terakhir di wallet peretas.

ETH Price: \$4,318.19 (+0.27%) Gas: 0.135 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name

Etherscan Home Blockchain Tokens NFTs Resources Developers More KRISNASUMA1032

Address 0x098B716B8Aaf21512996dC57EB0615e2383E2f96 Buy Presale Play Gaming

Sponsored: MESSIER: The First Hybrid P2P-DEX. Skip token tax and trade with zero price impact. [Start Here!](#)

This address is reported to be involved in a hack targeting the Ronin bridge.

Ronin Bridge Exploiter Exploit # OFAC-Sanctioned # Blocked

Overview

ETH BALANCE
101.80242993376705535 ETH

ETH VALUE
\$439,602.02 (@ \$4,318.19/ETH)

TOKEN HOLDINGS
\$3.22 (29 Tokens)

More Info

PRIVATE NAME TAGS
+ Add

TRANSACTIONS SENT
Latest: 2 yrs 172 days ago First: 3 yrs 170 days ago

FUNDED BY
Binance 20 3 yrs 170 days ago

Multichain Info

\$439,634.79 (Multichain Portfolio)

2 addresses found via Blockscan

Stake 200% SIGN UP BONUS. INSTANT PAYOUTS! BET NOW

Transactions Internal Transactions Token Transfers (ERC-20) NFT Transfers Analytics Assets Cards New

Advanced Filter

Latest 25 from a total of 428 transactions

Download Page Data

Transaction Hash	Method	Block	Age	From	To	Amount	Txn Fee
0x74f7fbfe5a0...	Transfer*	21954330	192 days ago	The Idols NFT Exploit...	Ronin Bridge Exploiter	0 ETH	0.00007506

ETH Price: \$4,318.19 (+0.27%) Gas: 0.135 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name

\$3.22 (29 Tokens)

Binance 20 | 3 yrs 170 days ago

METAWIN ENTER NOW

Transactions Internal Transactions Token Transfers (ERC-20) NFT Transfers Analytics Assets Cards New

Advanced Filter

Latest 25 from a total of 428 transactions

Download Page Data

Transaction Hash	Method	Block	Age	From	To	Amount	Txn Fee
0x74f7fbfe5a0...	Transfer*	21954330	192 days ago	The Idols NFT Exploit...	Ronin Bridge Exploiter	0 ETH	0.00007506
0x6cbd30d24ef...	Transfer	20471260	399 days ago	0xFc3F9d9...Eb1082f43	Ronin Bridge Exploiter	0.0005 ETH	0.00006197
0xb37bc24d86...	Transfer	19864401	483 days ago	*exploiter.eth	Ronin Bridge Exploiter	0.00001111 ETH	0.00007845
0x7411f1ed289...	Transfer	19579587	523 days ago	0xbcc250517...dE34d29E6	Ronin Bridge Exploiter	0.000001 ETH	0.00006469
0xceb93d896a...	Transfer	19579520	523 days ago	0xdf225c04...e15b9DF2A	Ronin Bridge Exploiter	0.00000174 ETH	0.0004935
0x229e7814c8...	Transfer*	19294873	563 days ago	0xE129927c...D4ee60c64	Ronin Bridge Exploiter	2 ETH	0.00060865
0x25e27694fe2...	Transfer	18424379	685 days ago	FixedFloat 1	Ronin Bridge Exploiter	0.0090648 ETH	0.000294
0xf597722f361...	Transfer*	17893699	760 days ago	0x9e40b3eC...cA69e88Dc	Ronin Bridge Exploiter	0 ETH	0.00063688
0xcbb5305c3dc...	Transfer*	17863552	764 days ago	0xE2601b38...16F1e9B72	Ronin Bridge Exploiter	0.000101 ETH	0.00173245
0x8ca9b69564...	Transfer*	17847355	766 days ago	0x46e85BeE...bde3c092	Ronin Bridge Exploiter	0 ETH	0.00044356
0x693347bbe2...	Transfer*	16894696	900 days ago	*capitalismisgay.eth	Ronin Bridge Exploiter	0 ETH	0.00029881
0x4f54b0e4b3d...	Transfer*	16877928	903 days ago	*jesuswasdead.eth	Ronin Bridge Exploiter	0 ETH	0.00064416
0x7a43807929...	Transfer*	16877927	903 days ago	*jesuswasdead.eth	Ronin Bridge Exploiter	0 ETH	0.00063635
0xd01792f7d80b...	Transfer	16877925	903 days ago	*jesuswasdead.eth	Ronin Bridge Exploiter	0 ETH	0.00044966
0xfec610845a0...	Transfer	16877925	903 days ago	*jesuswasdead.eth	Ronin Bridge Exploiter	0 ETH	0.00044943
0xa59ffc4cb27...	Transfer*	16877494	903 days ago	*eulerfinanceexploiter.eth	Ronin Bridge Exploiter	0 ETH	0.00125146
0xcfb0b3487dc4...	Transfer*	16877365	903 days ago	Ronin Bridge Exploiter	Euler Finance Exploit...	2 ETH	0.00160659
0x871829d492...	Transfer*	16861721	905 days ago	0xE3aE7649...6620D9841	Ronin Bridge Exploiter	0.000101 ETH	0.00039278

Sumber: <https://etherscan.io>

Berdasarkan hasil monitoring menggunakan *Etherscan*, ditemukan sebuah alamat dompet yang telah ditandai secara resmi dengan peringatan *“This address is reported to be involved in a hack targeting the Ronin bridge”*. Hal ini menegaskan bahwa alamat tersebut berhubungan langsung dengan peretasan besar pada *Ronin Bridge (kasus Axie Infinity)*. Dari data yang terlihat, dompet ini terakhir aktif sekitar 192 hari yang lalu, namun masih menyimpan saldo sebesar *101,80 ETH (senilai ± \$439.000)* serta 29 token lain dengan nilai kecil (*sekitar \$33,22*). Riwayat transaksi menunjukkan terdapat 428 transaksi, di mana sebagian besar aktivitas terbaru hanyalah mikro-transfer (*dusting*) dalam jumlah sangat kecil, spam token, atau bahkan transaksi nol (*0 ETH*). Pola ini umum terjadi pada alamat yang sudah terkenal di komunitas, karena sering menjadi target kiriman spam ataupun *dusting attack*. Meski begitu, fakta bahwa dompet ini masih memegang aset dalam jumlah besar memperlihatkan bahwa hasil eksploitasi masih tersimpan di dalamnya. Keunggulan keterbukaan blockchain membuat alamat ini mudah dilacak oleh publik melalui label resmi di *Etherscan*, sehingga dapat membantu komunitas dan pihak berwenang dalam mengidentifikasi serta mencegah upaya pencucian aset ke bursa. Untuk investigasi lebih lanjut dan mendalam, analis profesional biasanya menggunakan platform khusus seperti *Chainalysis*, *Arkham Intelligence*, atau *Nansen* untuk menelusuri potensi aliran dana lebih detail, termasuk pergerakan ke *mixer*, *DEX*, atau juga *cross-chain bridge* yang sulit diidentifikasi dengan tools gratis.

b) Menggunakan **Breadcrumbs**, alur transaksi terlihat berpindah dari wallet utama ke beberapa alamat lain.

Date & Time	Direction	From	To	Amount	Currency	Metadata	TX ID
2025-09-07 07:52:47 AM	IN	(0x9854...7a03)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0 (\$0.00 USD)	WETH		0x260a...fa05
2025-09-07 07:52:47 AM	IN	(0x2c3c...3610)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	2.7	VISIT WEBSITE GETETHER.NET TO CLAIM REWARDS		0x260a...fa05
2025-03-28 08:16:23 AM	IN	(0xd8d9...B604)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0	CLAIM REWARDS ON FARMETH.NET		0x9af5...75a4
2024-11-19 10:20:11 AM	IN	Ethereum Foundation: EthDev (0x0d0b...7bae)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0	CLAIM REWARDS ON POOL-ETH.ORG		0x7db8...a245
2024-10-03 10:25:11 AM	IN	Pooled Ether (0x53a...1c09)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0	CLAIM REWARDS ON POOLED-ETH.COM		0xc9f...bf4e
2024-08-30 09:53:23 AM	IN	(0xd0ca...223d)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0	LRWA.PRO GENESIS NFT		0xe07...d096
2024-08-07 02:16:23 AM	IN	(0xfc3f...2f43)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0.0005 (\$1.26 USD)	ETH		0x6cbd...a555
2024-05-14 07:33:35 AM	IN	(0xd956...ad00)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0.00001111 (\$0.03 USD)	ETH		0xb37b...0dae
2024-04-04 11:01:35 AM	IN	(0xbc25...29eb)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0.0000001 (\$0.00 USD)	ETH		0x7411...b26a
2024-04-04 10:48:11 AM	IN	(0xdf22...df2a)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0.00000175 (\$0.00 USD)	ETH		0xcce9...4795
2024-03-31 01:43:47 PM	IN	Ethereum Foundation: EthDev (0x0d0b...7bae)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0	CLAIM REWARDS ON ORIGIN-ETH.COM		0x401a...2a18
2023-08-26 05:16:23 PM	IN	Milady (0x5a0...25a5)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0	HAPPYBIRTHDAYBEACH.COM		0x2e33...9ea3
2023-08-07 10:08:35 PM	IN	(0xe260...9e72)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0.000101 (\$0.18 USD)	ETH		0xc653...7a1d
2023-07-29 01:40:23 PM	IN	(0x0085...408c)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	58,006,827.6	MOMO		0xf070...8c74
2023-07-07 10:26:35 AM	IN	(0x7ef4...7c49)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	78,211,261.85	MILADY2.0		0xc7e8...48a5
2023-05-21 11:16:47 AM	IN	(0x7ef4...7c49)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	92,192,877.86	SCAT		0x72b0...cad8
2023-03-23 09:27:11 AM	OUT	Lazarus Group Axi Infinity hack address (0x098b...2f96)	(0xf995...5ccc)	0	WETH		0x0a6e...2238
2023-03-23 09:26:23 AM	OUT	Lazarus Group Axi Infinity hack address (0x098b...2f96)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0	WETH		0x64e3...4ded
2023-03-22 01:02:23 AM	OUT	Lazarus Group Axi Infinity hack address (0x098b...2f96)	Euler Finance exploit (0xb66c...95db)	2 (\$3,488.88 USD)	ETH		0xcfb0...ceae
2023-03-19 08:18:47 PM	IN	(0xe3ae...9841)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0.000101 (\$0.18 USD)	ETH		0x8718...ef2b
2023-03-19 08:05:47 PM	IN	(0xe3ae...9841)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	0.00000001 (\$0.00 USD)	ETH		0x2ea8...efb2
2023-03-17 11:48:23 AM	IN	Euler Finance exploit (0xb66c...95db)	Lazarus Group Axi Infinity hack address (0x098b...2f96)	100 (\$167,379.25 USD)	ETH		0x202a...d457
2022-08-15 11:06:09 AM	OUT	Lazarus Group Axi Infinity hack address (0x098b...2f96)	(0xd30...b5b7)	9	CASH		0x513d...1164

Sumber: <https://monitor.breadcrumbs.app>

Dari gambar monitoring dashboard **Breadcrumbs** didapatkan bahwa alamat dompet yang dikaitkan dengan Lazarus Group (Ronin Bridge Hack) masih aktif tercatat di blockchain. Dari Etherscan, alamat ini sudah ditandai sebagai reported address involved in hack sehingga publik dapat mengidentifikasinya dengan jelas.

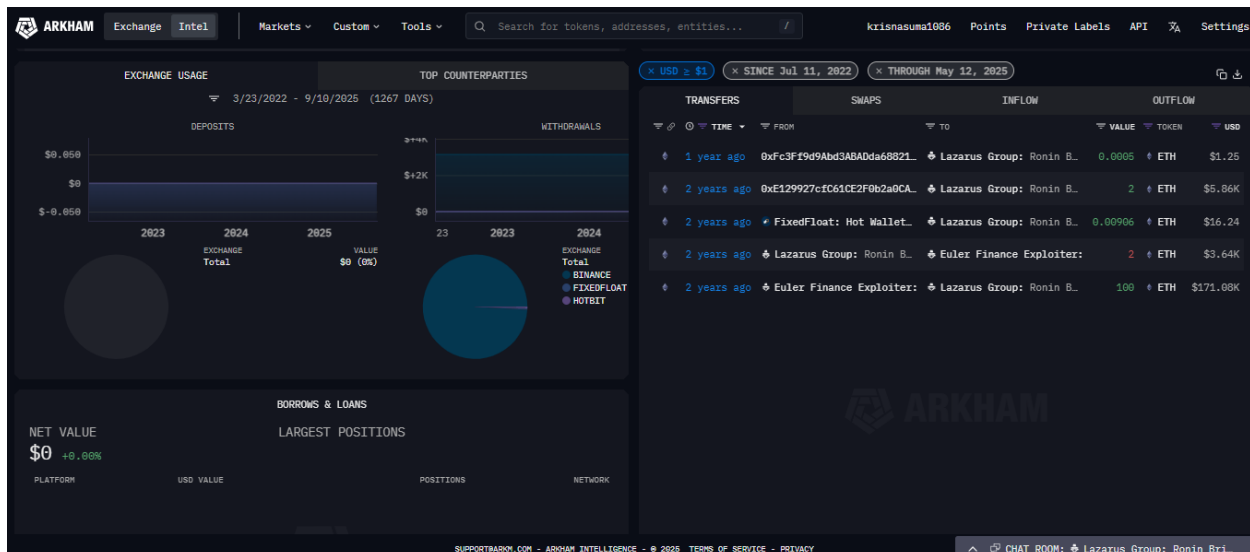
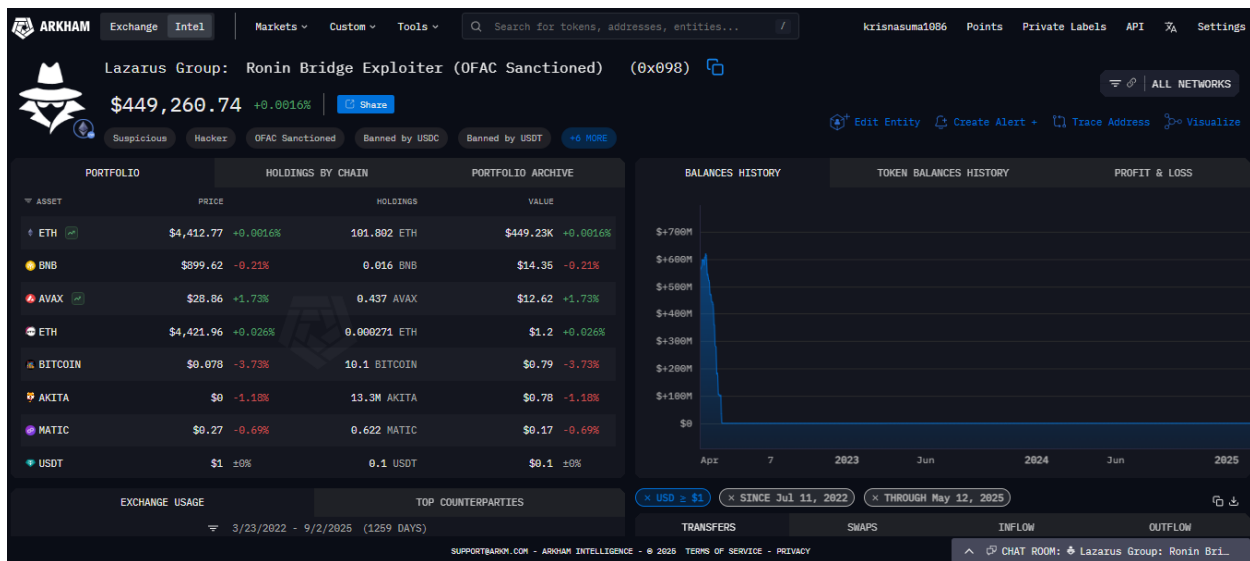
Hasil monitoring melalui **Breadcrumbs** menunjukkan bahwa sebagian besar transaksi yang masuk ke dompet tersebut berupa nilai sangat kecil seperti **0.00005 ETH**, token tidak bernilai dengan label **\$0 USD**, maupun transaksi yang berisi pesan promosi atau phishing seperti **“VISIT WEBSITE GETETHER.NET TO CLAIM REWARDS”**, **“CLAIM REWARDS ON FARMETH.NET”**, dan **“CLAIM REWARDS ON ORIGIN-ETH.COM”**. Pola ini menandakan bahwa wallet hasil hack sering menjadi target spam karena statusnya yang sudah dikenal luas di komunitas.

Bagi seorang analis forensik, penting untuk membedakan antara noise berupa spam transaksi atau phishing token dengan data relevan berupa transfer aset signifikan dalam jumlah

besar. Dari hasil observasi dua gambar, tidak ditemukan pergerakan besar terbaru dan mayoritas aktivitas hanyalah spam.

Kasus ini juga menunjukkan keunggulan keterbukaan teknologi blockchain. Meskipun aset diretas sejak lama, alur transaksi masih bisa dimonitor secara publik menggunakan **Etherscan** maupun **Breadcrumbs**. Namun, untuk investigasi yang lebih dalam seperti melacak aliran dana ke mixer, exchange, atau cross-chain bridge, dibutuhkan penggunaan tools profesional seperti Arkham Intelligence, Chainalysis, atau Nansen yang mampu memberikan analisis lebih detail hingga menghubungkannya dengan identitas di dunia nyata.

- c) Menggunakan **Arkam Intelligence(Free)** untuk menandai siapa pemiliknya, monitoring aliran dana keluar masuk dan hingga kemungkinan keterkaitan dengan wallet lain



Sumber: <https://intel.arkm.com>

Berdasarkan hasil monitoring menggunakan Arkham Intelligence, ditemukan alamat dompet yang secara resmi ditandai sebagai milik Lazarus Group, aktor siber yang terlibat dalam peretasan besar Ronin Bridge (Axie Infinity hack) dan telah masuk daftar sanksi OFAC. Hingga September 2025, dompet ini masih menyimpan aset senilai sekitar \$449.260, dengan saldo utama 101,80 ETH (\pm \$449.000), sementara sisanya berupa token kecil seperti BNB, AVAX, BTC,

MATIC, AKITA, dan USDT dengan nilai yang tidak signifikan. Riwayat transaksi mencatat 428 aktivitas, mayoritas berupa dusting (mikro-transfer) dan spam token, dengan transaksi besar terakhir yakni transfer 100 ETH (~\$171.000) dari Euler Finance Exploiter ke dompet Lazarus. Beberapa interaksi juga tercatat dengan layanan pihak ketiga seperti FixedFloat, Binance, dan Hotbit. Aktivitas terakhir terpantau lebih dari 192 hari lalu, menunjukkan dompet relatif dorman meski masih menyimpan aset besar. Dengan status publik sebagai alamat hasil hack yang terkena sanksi, dompet ini otomatis terblokir di sebagian besar bursa resmi, namun tetap berisiko digunakan untuk pencucian aset melalui mixer atau cross-chain bridge. Analisis ini menegaskan bahwa penggunaan tools blockchain forensik profesional seperti Chainalysis, Arkham Intelligence Pro, atau Nansen penting untuk melacak alur dana lebih dalam dan menghubungkannya dengan entitas di dunia nyata.

d) Dana kemudian diarahkan ke mixer untuk menyulitkan pelacakan lebih lanjut.

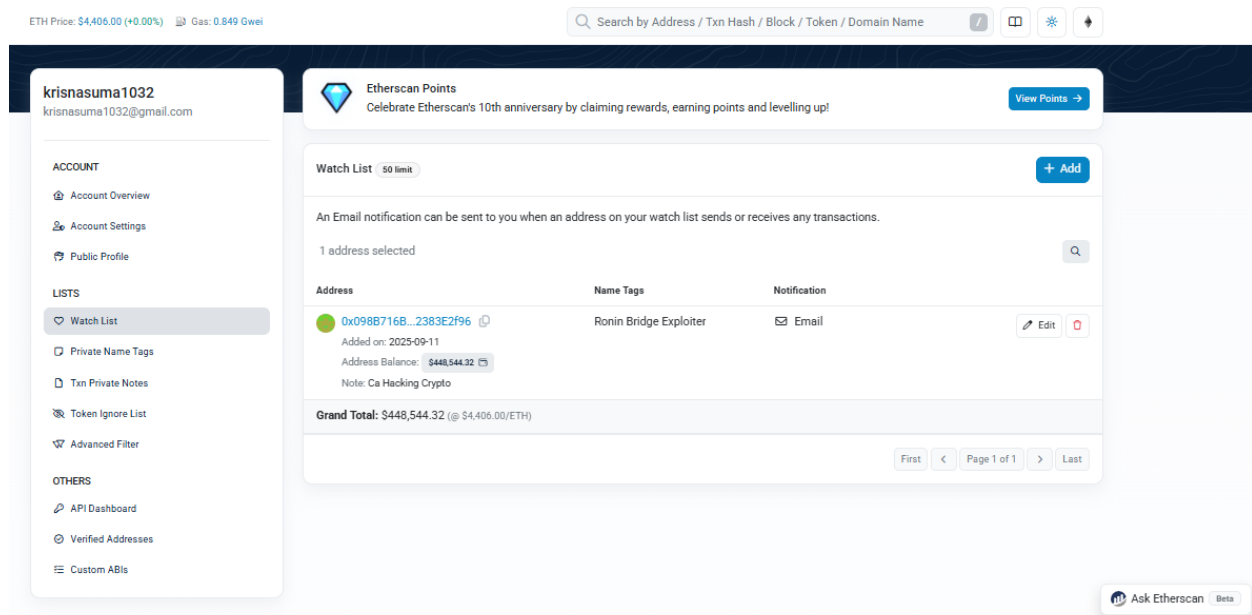


Sumber: <https://intel.arkm.com/visualizer/entity>

Untuk melihat aliran dana menuju mixer, saya menggunakan fitur visualisasi gratis di Arkham. Berdasarkan hasil tersebut, terlihat pola khas penggunaan mixer di mana node pusat merupakan kontrak Tornado.Cash (10 ETH Pool) yang berfungsi sebagai sarana obfuscation atau penyamaran transaksi. Secara garis besar, dana hasil eksploitasi maupun transaksi terkait pertama kali masuk (inflow) ke alamat Tornado Cash, lalu bercampur dengan ribuan ETH lain dari pengguna berbeda dalam proses mixing yang memutus hubungan langsung antara pengirim dan penerima. Setelah itu, dana keluar (outflow) ke berbagai alamat baru yang lebih bersih (fresh wallets), sebelum akhirnya ditukar melalui DEX, CEX, atau digunakan kembali dalam ekosistem kripto. Pola ini mengindikasikan bahwa pelaku menggunakan mixer Tornado Cash sebagai langkah utama untuk menyembunyikan jejak transaksi. Untuk analisis lebih detail mengenai alamat tujuan setelah keluar dari Tornado, pencarian dapat dilanjutkan menggunakan fitur search by entity di Arkham agar setiap alamat yang terhubung bisa diidentifikasi lebih spesifik.

4. Monitoring

- a) Saya membuat Etherscan Alert untuk wallet ini sehingga jika ada transaksi baru, sistem akan mengirim email notifikasi.

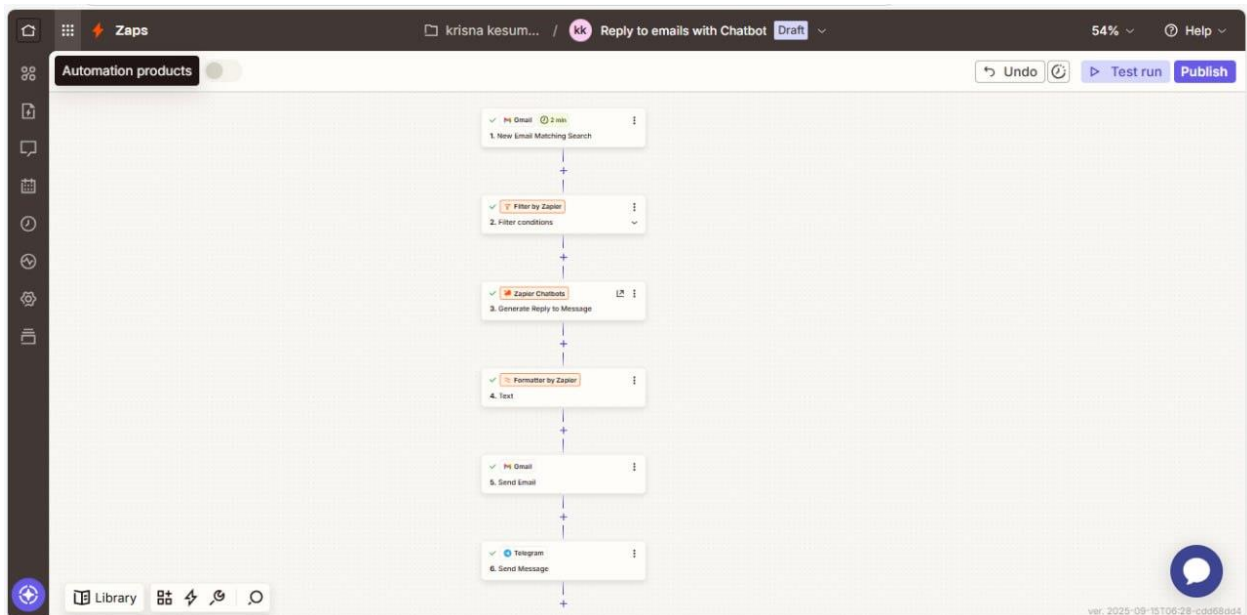


Sumber: <https://etherscan.io/myaddress>

Berdasarkan gambar di atas, saya membuat atau menggunakan fitur dari **Etherscan Alert** dengan menambahkan alamat wallet target ke dalam **Watchlist**. Dengan mengaktifkan opsi **Email Notification**, setiap transaksi masuk atau keluar dari wallet tersebut otomatis dikirim ke email saya. Cara ini memudahkan pemantauan aktivitas wallet secara real-time tanpa harus membuka explorer secara manual, dan notifikasi juga bisa diteruskan ke **Telegram** agar lebih cepat diakses melalui perangkat mobile.

- b) Untuk menambahkan variasi, saya juga menghubungkan alert tersebut dengan bot Telegram menggunakan **Ai Agent Zapier (Free)**. Dengan begitu, aktivitas wallet bisa dipantau secara real-time.

Berdasarkan gambar di bawah ini, saya telah membuat otomatisasi menggunakan **Zapier AI Agent** yang terhubung dengan **Gmail** dan **Telegram**. Sistem ini saya rancang khusus untuk memantau notifikasi dari Etherscan pada wallet Lazarus yang saya watchlist. Alurnya, setiap kali terjadi pergerakan di wallet Lazarus, **Etherscan** akan mengirimkan email notifikasi. Setelah itu **Gmail** menyaringnya melalui label khusus, kemudian Zapier menangkap email tersebut dan otomatis meneruskan pesan ke **Telegram Channel** melalui bot. Hasil pengujian menunjukkan bahwa alert sudah berhasil muncul di channel sebagai contoh output bot. Dengan demikian, notifikasi hanya akan terkirim jika benar ada aktivitas pada address Lazarus. Dokumentasi bukti setup, Screenshot konfigurasi **Zapier** (step **Gmail** trigger ke **Telegram** action) dan Screenshot **Telegram Channel** dengan alert bot aktif.



6. Send Message

Setup > Configure > Test

Chat Id *

Etherscan Alert-Lazarus Wallet (channel)

Text Format

Plain Text

Message Text *

TEST ALERT

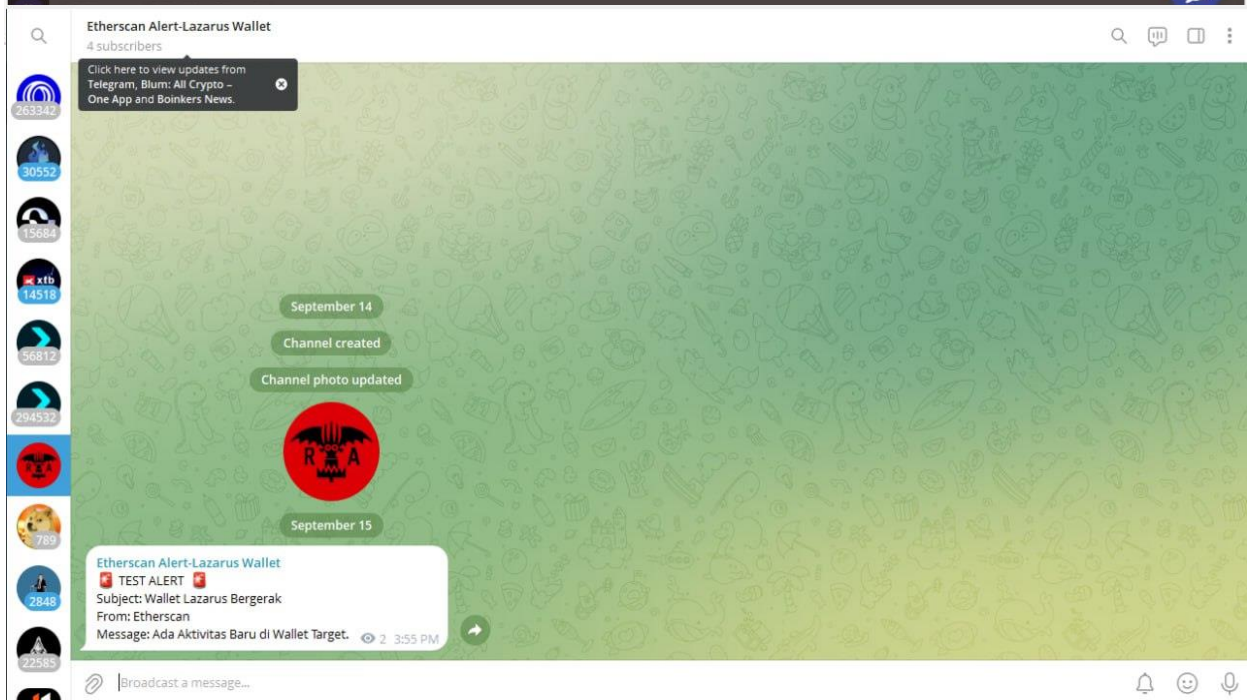
Subject: Wallet Lazarus Bergerak

From: Etherscan

Message: Ada Aktivitas Baru di Wallet Target.

Disable Link Preview

Continue



Sumber: <https://zapier.com> dan <https://web.telegram.org>