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 menghebohkan 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**
   a) Mengambil data alamat wallet yang dilaporkan terlibat dalam serangan.
   b) Sumber: artikel resmi, laporan audit, dan data publik dari blockchain explorer.
2. **Analisis On-Chain**
   a) Melacak transaksi dengan ***Etherscan*** (Ethereum) atau ***block explorer*** lainnya.
   b) Menggunakan ***Breadcrumbs*** untuk visualisasi alur dana.
3. **Monitoring dan Alert**
   a) Membuat ***Etherscan Alerts*** untuk memantau aktivitas wallet.
   b) Menambahkan ***bot Telegram*** atau ***Wallet Alert*** sebagai notifikasi tambahan.
4. **Pencatatan Temuan**
   a) Menyusun laporan berupa tabel ringkasan: alamat wallet, jumlah transaksi, saldo, aktivitas terakhir.
   b) Membuat dokumentasi visual (screenshot) untuk memperkuat hasil analisis.
5. **Tools Profesional (Opsional)**
   a) Menyebutkan bagaimana hasil analisis bisa lebih dalam jika menggunakan ***Arkham Intelligence***, ***Nansen***, atau ***TRM Labs***.

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

1. Ringkasan Ksus

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**

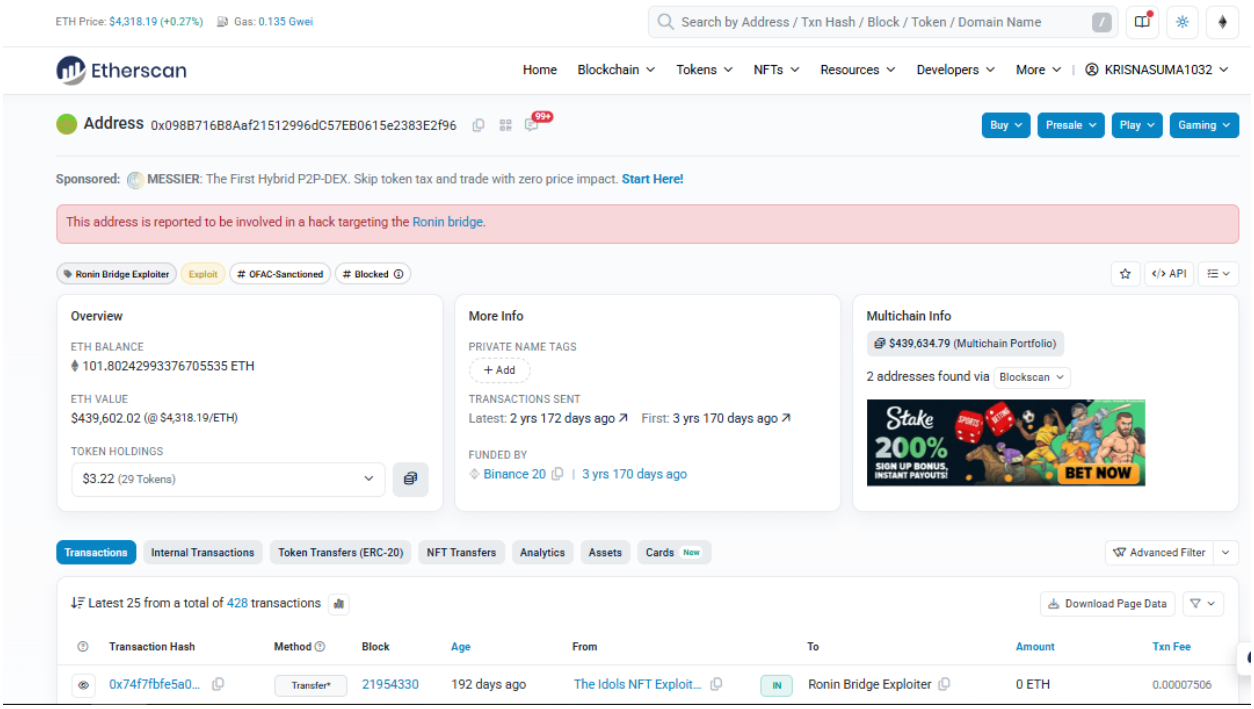
Salah satu alamat yang dikonfirmasi terlibat dalam serangan ini adalah:

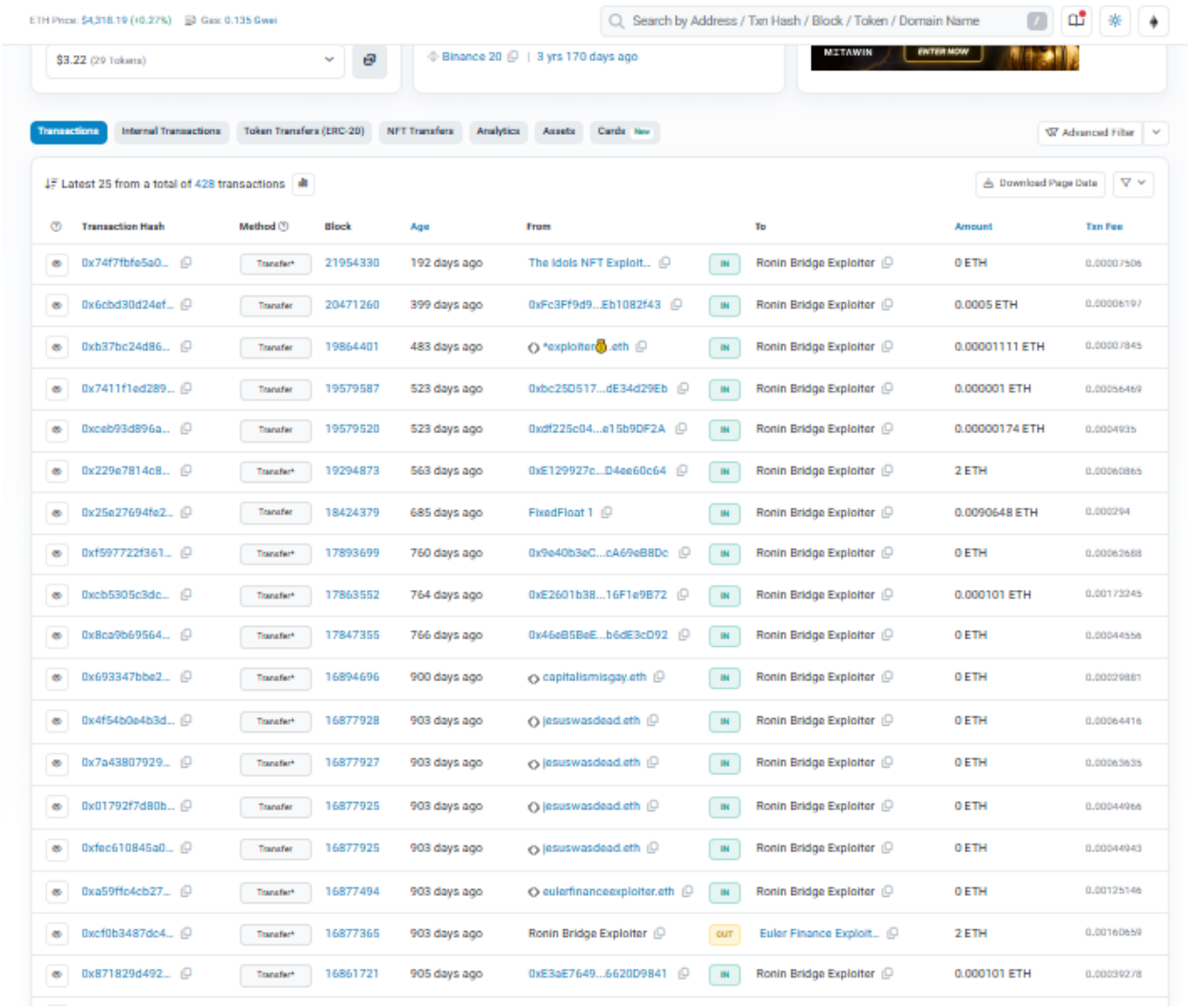
0x098B716B8Aaf21512996dC57EB0615e2383E2f96

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 tranksaksi terahkir di wallet peretas.

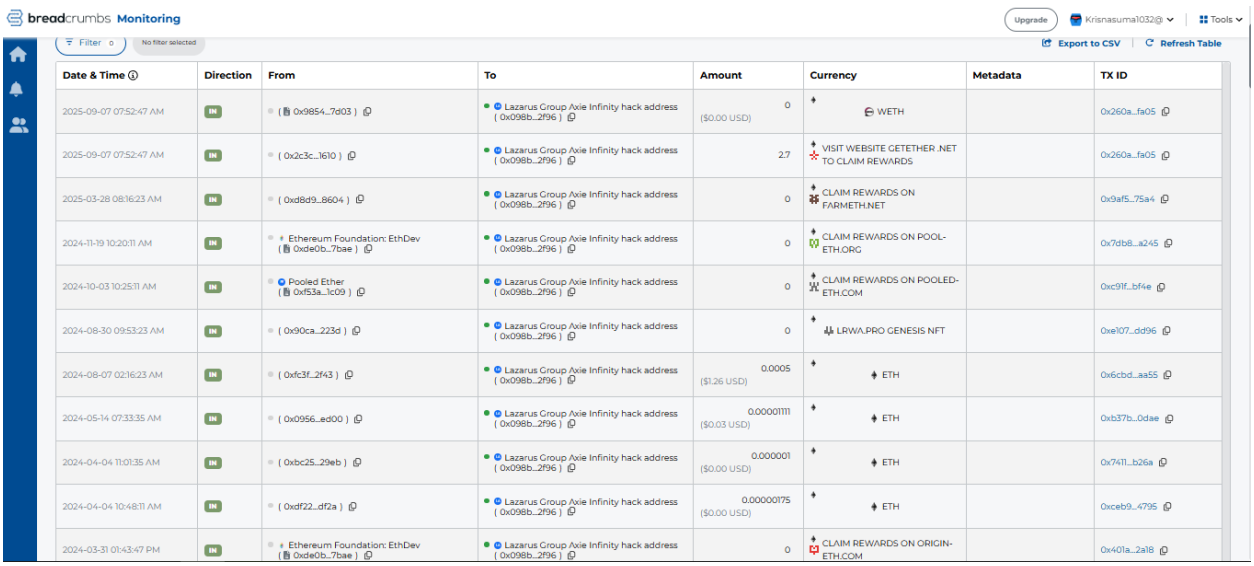




Sumber: https://etherscan.io

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.



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.

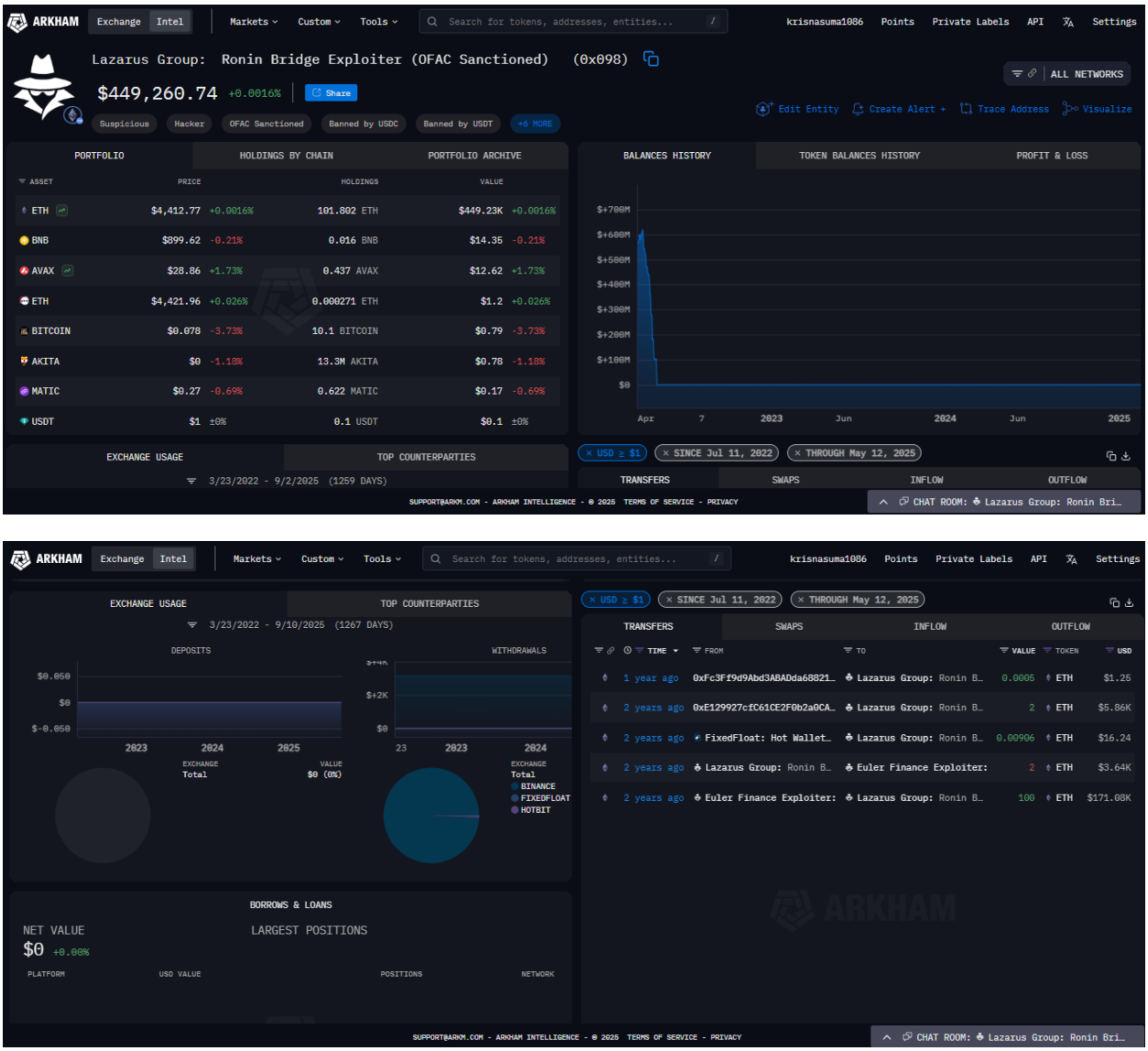
Hasil monitoring melalui ***Breadcrumbs*** menunjukkan bahwa sebagian besar transaksi yang masuk ke dompet tersebut berupa nilai sangat kecil seperti ***0.00005* ETH**, token tidak bernilai dengan label ***$0 USD***, maupun transaksi yang berisi pesan promosi atau phishing seperti "***VISIT WEBSITE GETETHER.NET 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 kerterkaitan 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 (± $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.

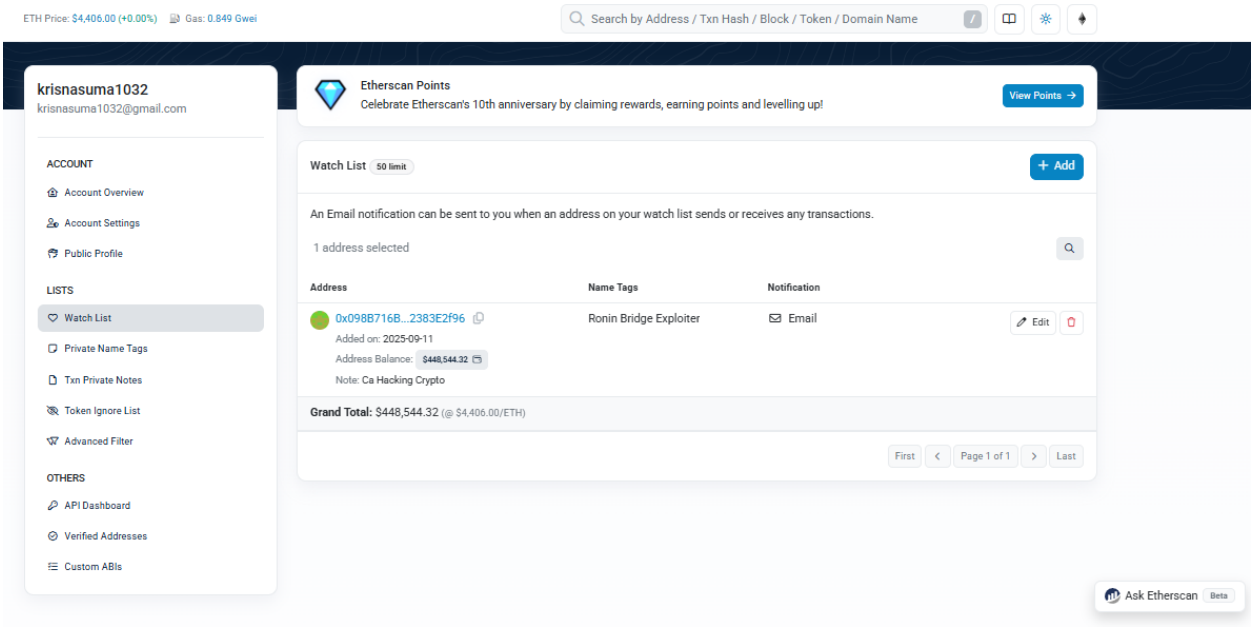
d) Dana kemudian diarahkan ke mixer untuk menyulitkan pelacakan lebih lanjut.

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.

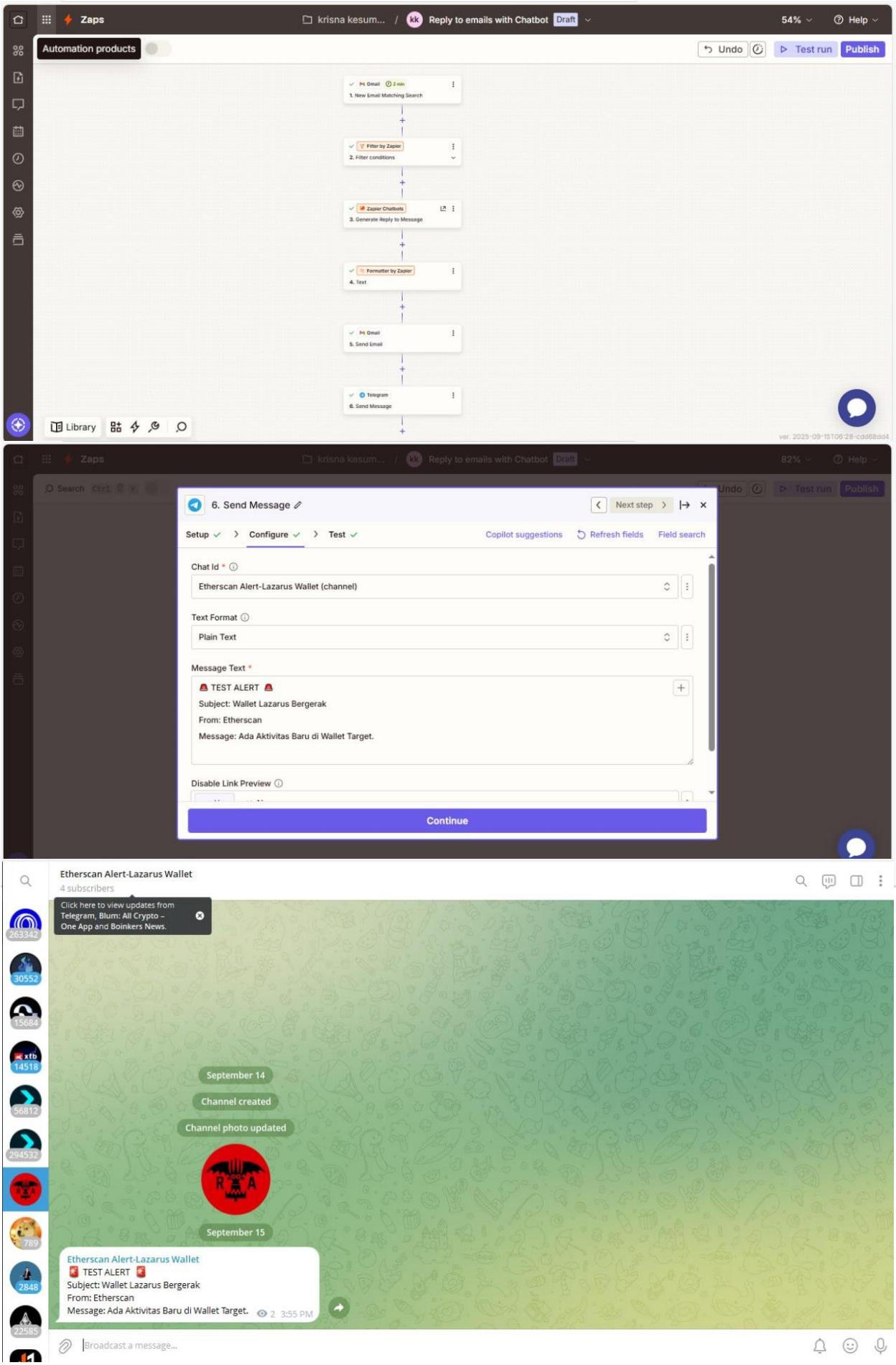


Sumber: https://etherscan.io/myaddress

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.



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