How we proved North Korea's blockchain malware campaign

By ana.lobzhanidze

Published: 2025-12-17 · Archived: 2026-04-05 18:47:33 UTC

When malware lives on servers, law enforcement can seize them. When it's hosted on domains, registrars can take them down. But when threat actors embed malware directly in blockchain transactions, they create something unprecedented: infrastructure that's permanent, globally distributed, and impossible to remove.

North Korean threat actors have done exactly that. In Parts 1-3 of this investigation series, Ransom-ISAC documented the technical sophistication of Cross-Chain TxDataHiding, a technique for embedding malware payloads and command-and-control instructions in blockchain transactions. The malware analysis was groundbreaking. But it left one critical question unanswered: who's behind it?

Part 4 answers that question. Crystal Intelligence proved North Korean attribution by doing something traditional blockchain forensics doesn't: we followed the money backward.

(Read the technical analyses: Part 1, Part 2, Part 3.)

The attribution challenge

Traditional malware attribution relies on infrastructure fingerprinting: server configurations, domain registration patterns, hosting provider choices, IP addresses. But when the infrastructure IS the blockchain itself, those indicators vanish. Blockchain transactions are pseudonymous. Anyone can post data. The technical signatures tell you what happened, not who did it.

This is where financial intelligence becomes essential. While malware analysis reveals the technique, financial forensics reveals the threat actor.

Following the money backward

Traditional blockchain forensics starts with stolen cryptocurrency and traces where it goes: through mixers, across chains, into exchanges. Crystal reversed the approach.

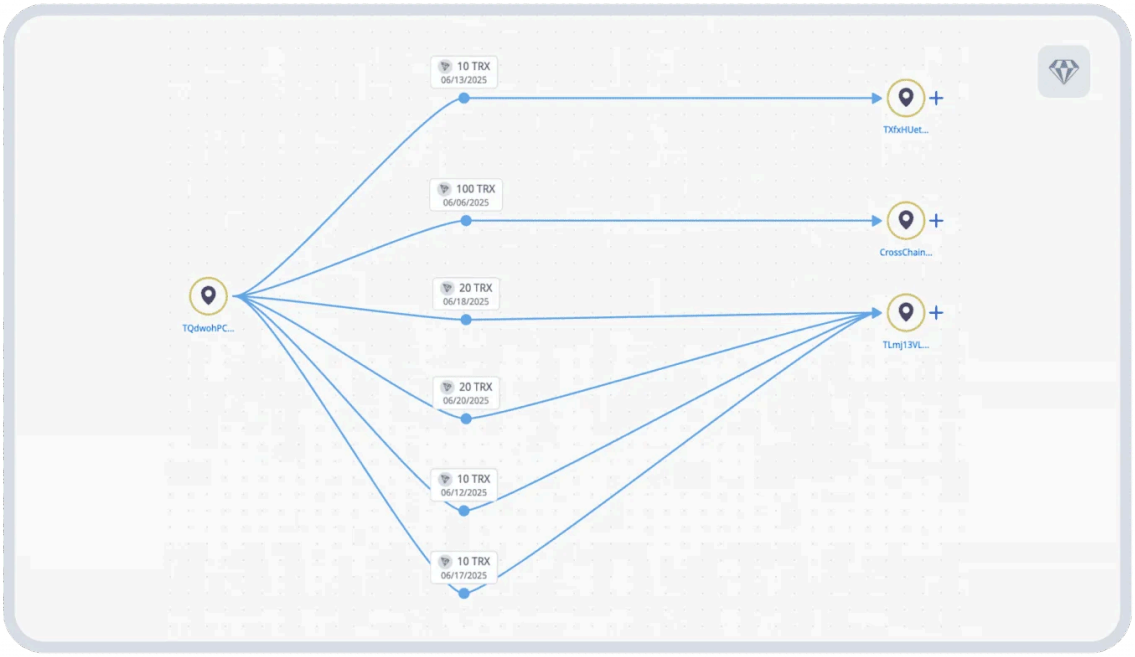
We started with the wallets posting malware transactions and asked: where did their operational funding come from?

We identified addresses paying transaction fees for malware-containing transactions across Binance Smart Chain, TRON, Aurora, and Ethereum. Then we traced their funding sources backward through cross-chain bridges, swap services, and layered transactions. The infrastructure funding patterns revealed something traditional forward-tracing would never catch: multi-year operational planning.

> "***Traditional blockchain forensics traces stolen funds forward. We reversed it: starting with operational wallets and tracing funding backward revealed connections invisible to standard***

> ***methods.***“

– Nick Smart, Chief Intelligence Officer, Crystal Intelligence



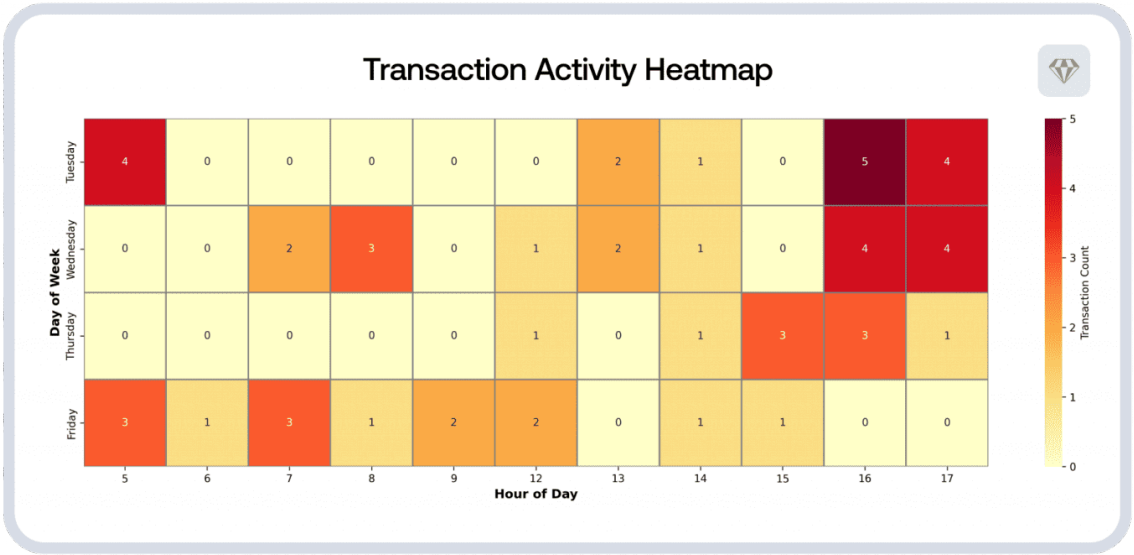
Above: Visualization showing cross-chain transaction flow from TQdwohPCWqqfCUaCispyV1NaUZ1HgiJPUy to multiple addresses Source: Crystal Expert

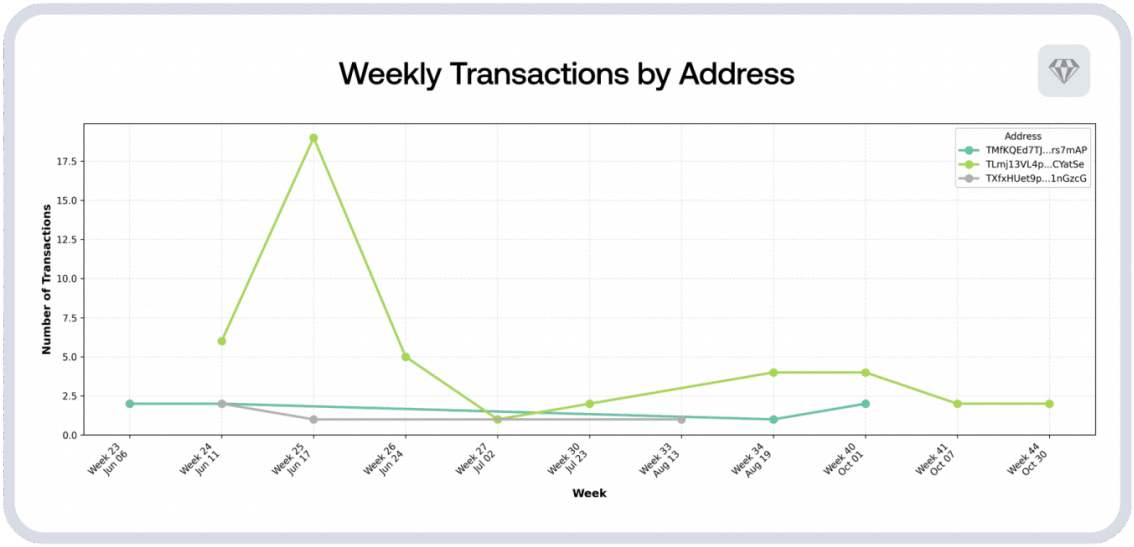
What the financial trail revealed

Some infrastructure wallets had been dormant since 2021. Not months, but years. They held funds, waiting, before sudden activation in 2024-2025 for malware operations. This isn’t opportunistic cybercrime. It’s strategic nation-state planning.

The operational funding moved across multiple blockchains using bridges and swap services, demonstrating sophisticated understanding of blockchain monitoring gaps. Between October 2024 and April 2025, funds flowed through legitimate services in patterns that looked normal in isolation but revealed operational discipline when analyzed comprehensively.

Transaction timing showed weekday activity during standard working hours. Operations began in early June 2025 and continued through November with rotating command-and-control servers. The behavioral patterns were consistent, methodical, disciplined.



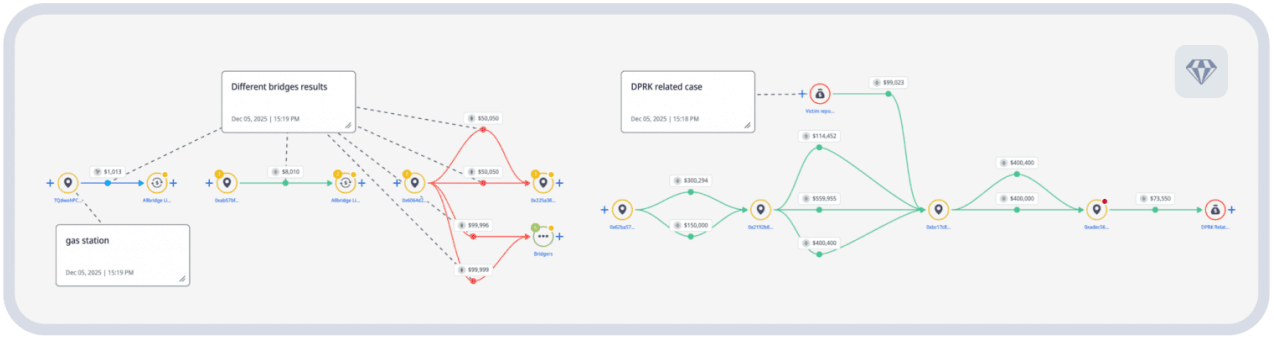


Above: Temporal analysis heatmap showing transaction activity by day of week and hour, plus weekly transactions chart showing activity patterns from June through November 2025

Then we found the smoking gun: direct financial connections to known North Korean operations.

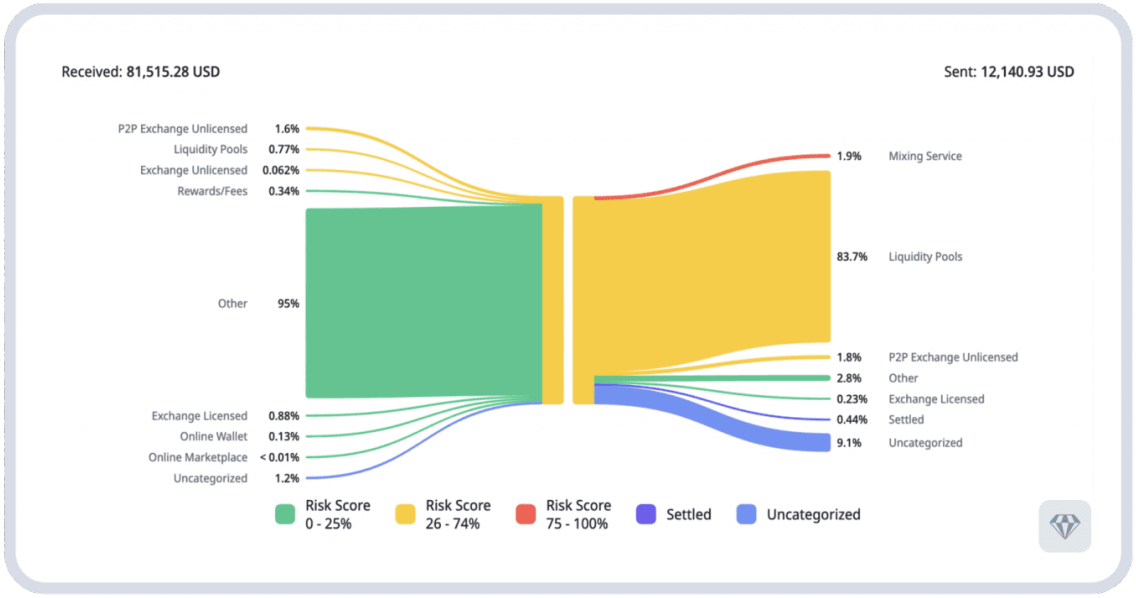
Operational wallets linked to addresses involved in documented DPRK cryptocurrency thefts, including the Bybit theft, the largest cryptocurrency theft to date. The financial flows connected to known hubs for North Korean laundering operations: Huione, Xinbi Guarantee, and BlackU. These aren’t circumstantial similarities. They’re direct financial relationships.

One operational wallet was accessed via IP address 188.43.33.249 in Vladivostok, Russia—geolocating to the site of the former US Consulate. This aligns perfectly with known DPRK internet routing through TransTeleCom infrastructure established in 2017, when North Korea diversified its internet access through Russia.



Above: Bridging activity showing fund flows eventually connecting to DPRK theft addresses. Source: Crystal Expert

The full scope of financial flows revealed significant operational funding:



Above: Fund flow showing received vs. sent funds breakdown: $81,515.28 through various sources flowing to destinations including Mixing Service (1.9%), Liquidity Pools (83.7%), and other services. Source: Crystal Expert

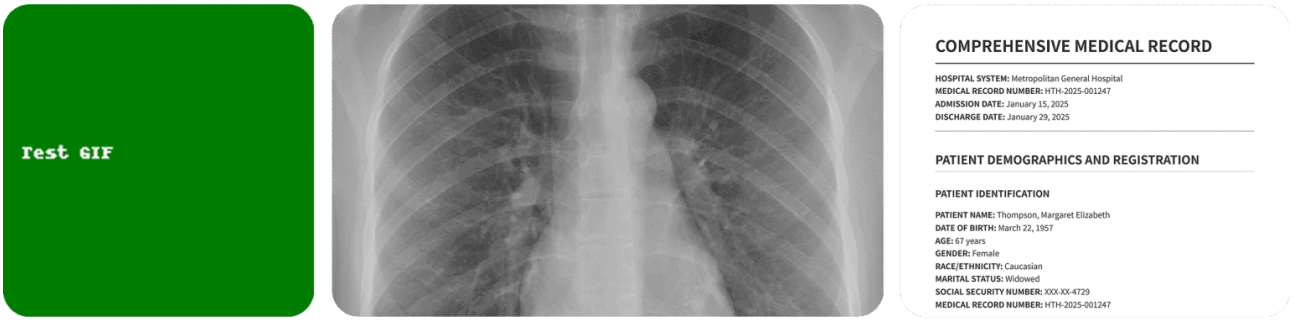
They’re not just using this technique; they’re perfecting it

But financial patterns weren’t the only unusual discovery.

The blockchain analysis revealed something unexpected: unusual data embedded in transactions that had nothing to do with malware operations. Medical records. Chest X-rays. Legal documents. Audio files. None connected to actual attacks.

This is testing. Threat actors systematically experimenting with different file types, sizes, and encoding methods to understand what blockchain networks accept and how data persists across different chains. They’re not just deploying a technique—they’re actively developing it.

The presence of these artifacts raises intriguing questions. Some researchers have speculated whether such embedded data could function as a modern ‘numbers station’—a method intelligence agencies use to communicate with agents overseas through broadcasts of encoded data that appear meaningless to observers. While DPRK is known to operate traditional numbers stations, whether these blockchain artifacts serve a communication function remains uncertain. What’s clear is systematic experimentation with the technique’s capabilities.



Above: Examples of unusual artifacts embedded in blockchain transactions – medical records, chest X-rays, legal documents, and test images used for systematic testing of file types and encoding methods.

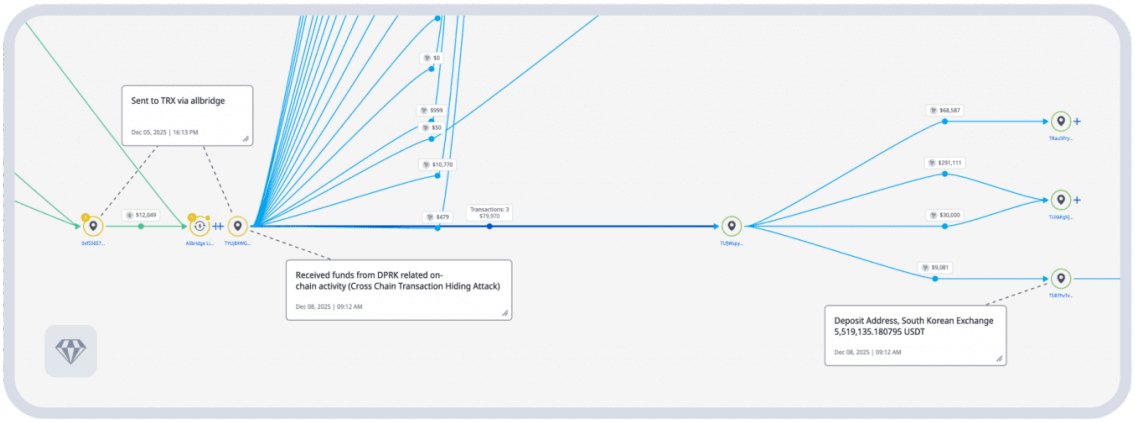
Why this changes everything

This represents Phase 3 in North Korean cryptocurrency operations.

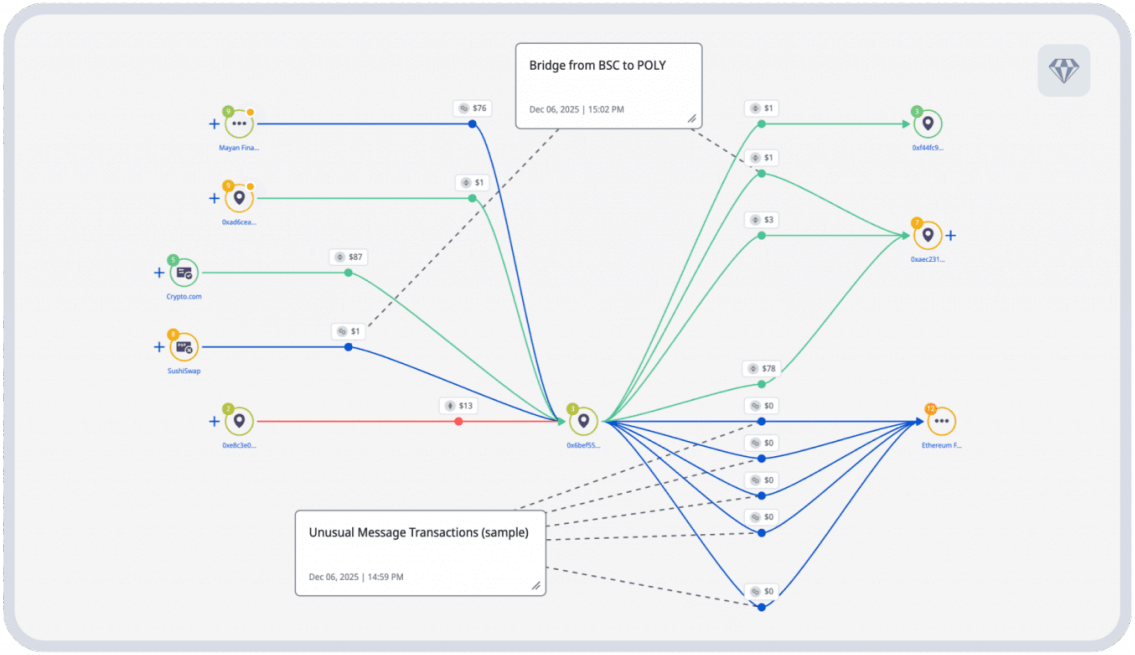
- Phase 1 (2016-2020) focused on theft – direct exchange hacks and DeFi exploits.
- Phase 2 (2020-2024) focused on laundering – sophisticated obfuscation using mixers, bridges, and layered transactions.
- Phase 3 (2025-present) focuses on building permanent operational infrastructure ON blockchains.

The implications ripple across industries. Security teams monitoring emails, websites, and servers can’t see threats living on blockchains. Compliance teams watching for suspicious transaction patterns miss infrastructure funding that looks normal. The crypto industry faces a fundamental challenge: the same properties that make blockchains valuable – permanence, censorship resistance, global accessibility – make them attractive for adversary infrastructure.

And this technique will spread. What North Korea demonstrates today, other nation-state actors and cybercriminal groups will adapt tomorrow.



Above: Figure showing wallet relationships and connections to South Korean exchanges and DeFi services. Source: Crystal Expert



Above: Unusual on-chain artifacts. Figure visualization of polygon transactions with unusual message-encoded data and different bridging methods being tested. Source: Crystal Expert

Building on emerging research

This research builds on emerging understanding of blockchain-based malware techniques. In 2023, Mandiant documented ‘etherhiding’—hiding malicious code in blockchain data. Crystal’s investigation reveals the broader operational picture: not just isolated techniques, but systematic infrastructure development, cross-chain distribution, multi-year planning, and verified attribution to specific nation-state actors through financial forensics.

When threat actors build infrastructure on blockchains, financial intelligence becomes essential to attribution. This investigation demonstrates that permanent, blockchain-based malware infrastructure is no longer theoretical—it’s operational. And proving attribution requires following the money, not just analyzing the code.

—

About this investigation

This is Part 4 of the Cross-Chain TxDataHiding investigation series, produced in collaboration between Crystal Intelligence and Ransom-ISAC.

Read the full series:

- Part 1: Novel tradecraft and C2 infrastructure
- Part 2: Malware payload analysis
- Part 3: Infrastructure fingerprinting and attribution
- Part 4: Financial intelligence and blockchain forensics (this post)

Contributors: Nick Smart (Chief Intelligence Officer, Crystal Intelligence), Andrii Sovershennyi (Senior Analyst, Crystal Intelligence), François-Julien Alcaraz, Yashraj Solanki, Tammy Harper, and Ellis Stannard.

Access the investigation: Crystal Expert users can view detailed blockchain analysis and visualizations at expert.crystalintelligence.com

Find out how Crystal Intelligence's investigation, compliance, and advisory solutions can help your organization negotiate the evolving crypto regulation landscape by booking a demo here.
