TRM WHITE PAPER

Why National Security and Defense Agencies Need BLOCKINT

Four ways national security agencies use blockchain intelligence to disrupt threat actors

TRMLABS.COM

Over the last few years, we've seen a move to a digital battlefield, where wars, in part, are fought in cyberspace and across blockchains. The promise of blockchain technology — cross-border value transfer at the speed of the internet for humanitarian aid, remittances, and payments — is being weaponized by malign actors who also seek to move funds for sanctions evasion, weapons proliferation, terrorist financing, ransomware, and other illicit activity.

From Russian ransomware gangs to North Korean hackers, threat actors have looked to cryptocurrencies for revenue generation, money laundering, sanctions evasion, and other illicit activity. Many of these actors perceive blockchain-based transactions to be protected from the prying eyes of regulators or law enforcement, especially for cross-border transactions. However, the reality is quite the opposite.

The native properties of public blockchains — data that is transparent, traceable, and permanent — enables government agencies to leverage **blockchain intelligence**, or **BLOCKINT**, to identify risks more readily and more effectively so they can take action against illicit actors. Not unlike conventional battlefield intelligence, the tools of blockchain intelligence capture threat activity, threat intent, and threat vulnerabilities. Through this advantage, intelligence analysts and officials can deny, degrade, and disrupt threat actors on the digital battlefield.

What is blockchain intelligence?

Blockchain intelligence (BLOCKINT) is multilayered intelligence: Raw blockchain data layered with on- and off-chain intelligence that allows national security agencies unprecedented visibility into real-time financial flows.

The nature of blockchain technology — the open and distributed ledger upon which tokens can be sent — means that each transaction is verified and logged in a shared, immutable record, along with the timestamp of the transaction and the addresses involved. This data can be used to understand connections between on-chain addresses, and can also be paired with off-chain intelligence to identify links to real-world entities. Illumination of financial flows through blockchain intelligence not only includes blockchain records, but sets the stage for expanded identification of threat actors who are hiding in plain sight.

Four key use cases for BLOCKINT in defense and security

TRM Labs provides unique BLOCKINT to national security agencies globally. Let's explore how national security agencies use TRM BLOCKINT to:

1. Identify cryptocurrency usage across countries and regions
2. Track and trace funds to investigate and disrupt illicit activity
3. Understand and disrupt disinformation and counterintelligence campaigns
4. De-anonymize ransomware and other threat actors

1. Identify cryptocurrency usage across countries and regions

BLOCKINT provides national security analysts and officials with unique data on how a threat actor is using virtual assets for revenue generation. It also provides a high-level overview of a country's cryptocurrency usage, which could provide valuable insights into the nation's overall economic health and strategy.

Below, we'll take a look at two examples — Iran and Russia — that demonstrate how cryptocurrency is generating revenue and being used by nation-state threat actors.

CASE STUDY

Iran's crypto economy

Following Iran's attack on Israel in May 2024 and the assassination of a senior Hamas leader in Iran in July 2024, we've seen new sanctions imposed and national security agencies looking to better understand Iran's use of cryptocurrencies. In this context, TRM Labs, using BLOCKINT, has analyzed Iran's crypto economy to understand how the regime utilizes digital assets.

Nobitex, Iran's largest crypto exchange, received 89% of all funds flowing to Iranian exchanges in 2023 and reported over 5.5 million users, a 28% increase from the previous year. The exchange also launched new decentralized finance (DeFi) services, including Locket Wallet and Nobidex. Despite US sanctions, TRON remains the preferred blockchain on Iranian exchanges, accounting for about 65% of incoming volumes due to its lower transaction fees and stable availability of USDT.

Approximately 70% of funds handled by Iranian exchanges in 2023 came from outside Iran, mainly from global cryptocurrency exchanges.

Iran has also been leveraging cryptocurrencies for sanctions evasion. In September 2022, Iran announced a pilot launch of the "crypto-rial," a central bank digital currency (CBDC), with further developments into 2023. Additionally, Iran and Russia have been exploring the issuance of a gold-backed cryptocurrency for cross-border transactions, operating in a special economic zone in Astrakhan, Russia. This initiative aims to facilitate international payments, bypassing traditional fiat currencies like the US dollar.

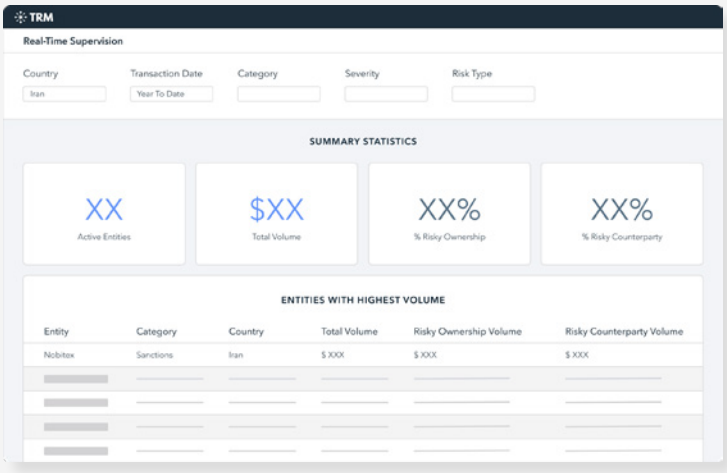
CASE STUDY

Russia's embrace of crypto to evade sanctions

According to research by TRM Labs, Russian-speaking threat actors have become a major force in international crypto crime, driving activities from ransomware to darknet markets.

In 2023, **Russian-speaking ransomware groups accounted for at least 69% of all crypto proceeds from ransomware**, exceeding USD 500 million, and **Russian-language darknet markets comprised 95% of all crypto-denominated illicit drug sales on the dark web**. Additionally, amidst global sanctions, Russia has increasingly turned to cryptocurrencies for evasion, with inflows to the Russia-based crypto exchange Garantex accounting for 82% of crypto volumes from all sanctioned entities globally. These funds have been used to purchase military equipment and critical components for Russian forces, with at least USD 85 million sent to wallets linked to Russian and Chinese entities involved in these transactions since 2021.

TRM IN ACTION



TRM Real-Time Supervision provides a simple interface to identify and manipulate risk categories for a particular country. The insights gained from Real-Time Supervision help national security and defense agencies understand how nation-states or threat actors use crypto at an aggregate level — including visibility into how much crypto flows through the region and the types of activity taking place there. For example, a defense agency interested in Iranian sanctions evasion could view the cryptocurrency flows that involve Iranian exchanges such as Nobitex or Nobidex.

2. Tracking and tracing funds to disrupt threat actors

BLOCKINT — the layering of threat intelligence on blockchain data — allows national security agencies the ability to not just understand the use of cryptocurrencies by an adversary, but also to track and trace the flow of funds to build investigations. This gives analysts a clearer operating picture of on-chain activities, and presents opportunities to disrupt illicit operations in regions of interest.

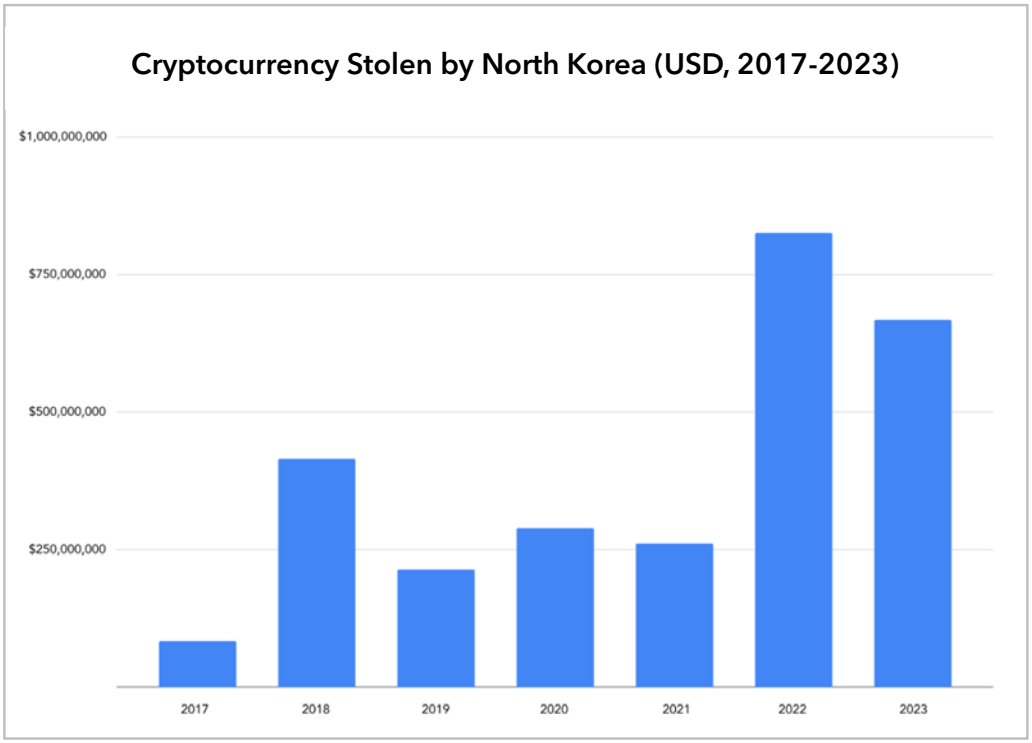
Going after sophisticated Advanced Persistent Threats (APTs) or clever non-state Malicious Cyber Actors (MCAs) requires what the former commander of US Cyber Command, Gen. Paul Nakosone, called "persistent engagement." BLOCKINT plays a key part in this engagement, as it presents decision-makers with opportunities to prevent potentially hundreds of millions of dollars flowing into the pockets of malign actors.

CASE STUDY

North Korean cyber actors steal and launder crypto at unprecedented speed and scale

Over the last five years, North Korea has attacked the crypto ecosystem at unprecedented speed and scale. Nearly USD 3 billion worth of cryptocurrency has been lost to Pyongyang-linked threat actors between 2017 and 2023. **In 2023, hackers tied to North Korea stole approximately USD 700 million in cryptocurrency**, according to research by TRM Labs – over a third of all funds stolen in crypto attacks last year, despite an approximately 20% reduction from the USD 850 million haul in 2022. **On average, hacks perpetrated by North Korea in 2023 resulted in ten times more losses than those perpetrated by other actors.**

In its 2023 Annual Threat Assessment, the US Intelligence Community expressed concern that North Korea's "cyber program continues to adapt to global trends in cybercrime by conducting cryptocurrency heists, diversifying its range of financially motivated cyber operations, and continuing to leverage advanced social engineering techniques."



Sophisticated threat actors like North Korea's Lazarus Group exploit blockchain technology to maximize their financial gains while simultaneously hiding their tracks – through on-chain money laundering techniques such as chain-hopping, the use of mixing services, performing cryptocurrency swaps, and sometimes even leveraging Non-Fungible Tokens (NFTs).

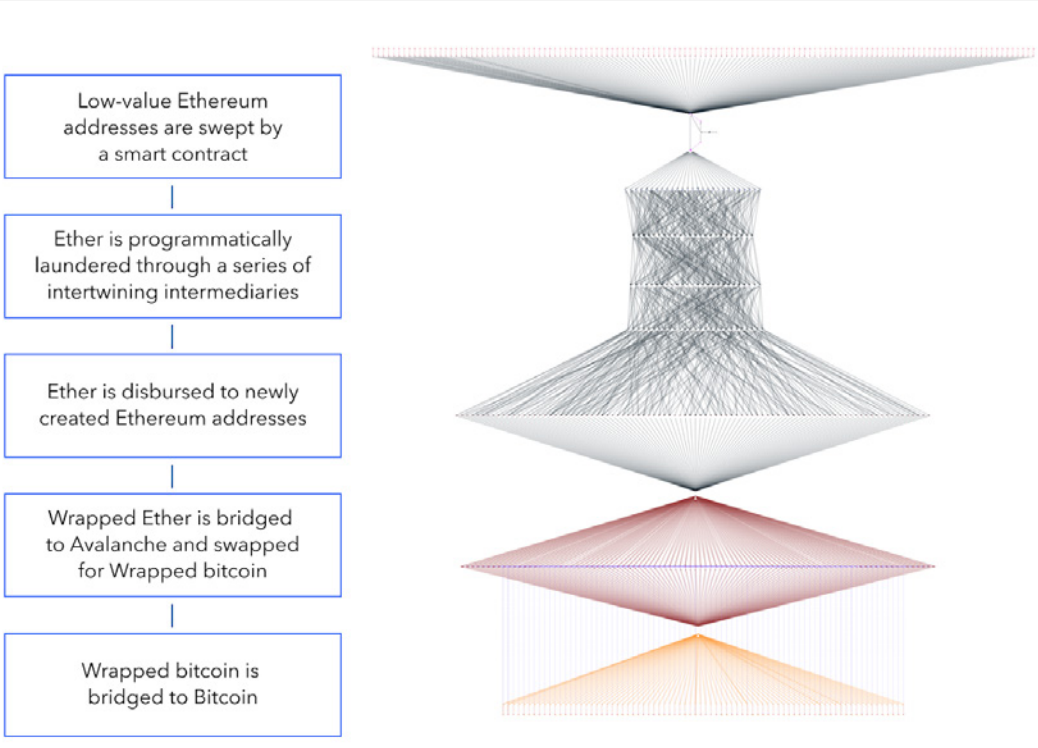
BLOCKINT allows investigators to follow hacked and stolen funds across blockchains and, in many cases, through obfuscation techniques like mixers in order to disrupt the off-ramping of funds.

TRM IN ACTION

TRM Forensic's **Graph Visualizer** employs behavioral Signatures® such as automated identification of peel chains and cross-chain swaps to save time and provide a seamless cross-chain investigative experience.

For example, in the 2023 Atomic Wallet hack, DPRK hackers stole approximately USD 100 million worth of cryptocurrency across seven blockchains and then laundered it using a range of complex techniques – including the use of automated software programs, mixers, and cross-chain swaps.

Despite the heist's complexity, TRM's BLOCKINT enabled investigators to follow the assets, identify the threat actors, and seize the illicit funds – including those stolen and laundered by North Korea.



3. Understanding and disrupting disinformation and counterintelligence campaigns

Adversaries and allies alike seek to use cryptocurrency to recruit assets and fund espionage and disinformation operations. Cryptocurrency source payments are likely an attractive option for these governments due to the fact that transactions are quick, discreet, and allow their spies to cash out in their home country's currency.

In counterintelligence operations, however, BLOCKINT has the potential to identify foreign intelligence agents and disinformation networks earlier in the investigative process. The blockchain's immutability, coupled with address attribution, leaves a trail that cannot be hidden in the same way fiat currency's trail can.

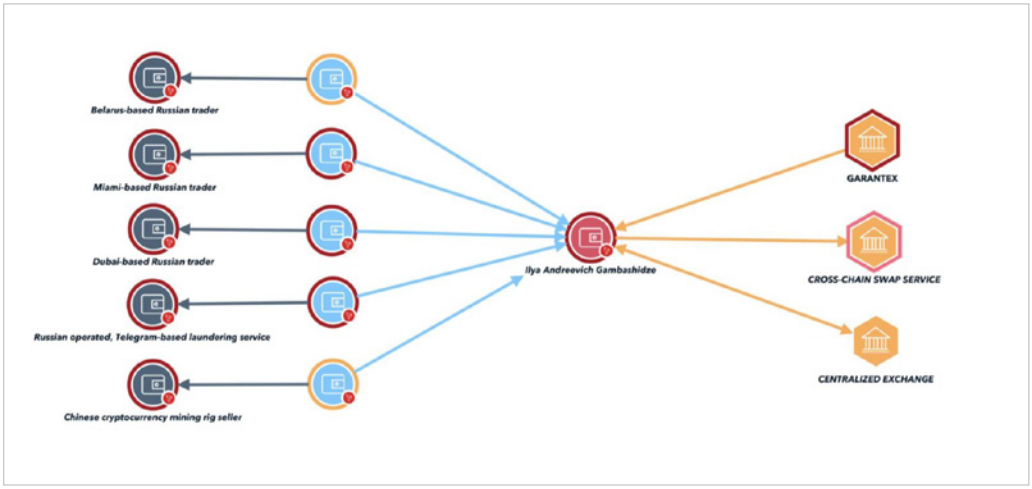
CASE STUDY

Tracking Russia's disinformation campaign on the blockchain

In 2024, more voters globally than ever in history will head to the polls. At least 64 countries (plus the European Union), representing a combined population of about 49% of the people in the world, are set to hold national elections — the results of which, for many, will prove consequential for years to come. And with elections come election interference and disinformation campaigns. However, we are seeing national security agencies use BLOCKINT to disrupt these efforts.

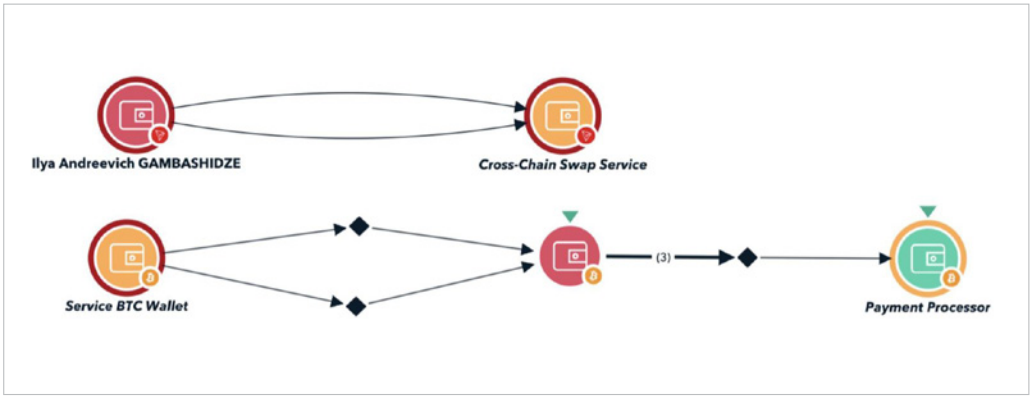
On March 20, 2024, the US Treasury's OFAC sanctioned two individuals and two entities for their roles in a Russian disinformation campaign, including attempts to impersonate legitimate media outlets. The sanctions targeted Russian national Ilya Andreevich Gambashidze and his company, the Social Design Agency (SDA), as well as Nikolai Aleksandrovich Tupikin and his company, Structura LLC, for spreading pro-Russian messaging through fake websites, videos, and social media accounts. This campaign, conducted in October 2022, involved over 60 websites impersonating legitimate news sources.

In its sanctions designation, OFAC included a number of cryptocurrency addresses belonging to Gambashidze, including two TRON (TRX) addresses: TMGLqRQ4twjW8wJhVH1mQR7nUThpGHUsN3 and TEFph7dZoUN5233cGEzF6XFwRpjPF8fQDS.



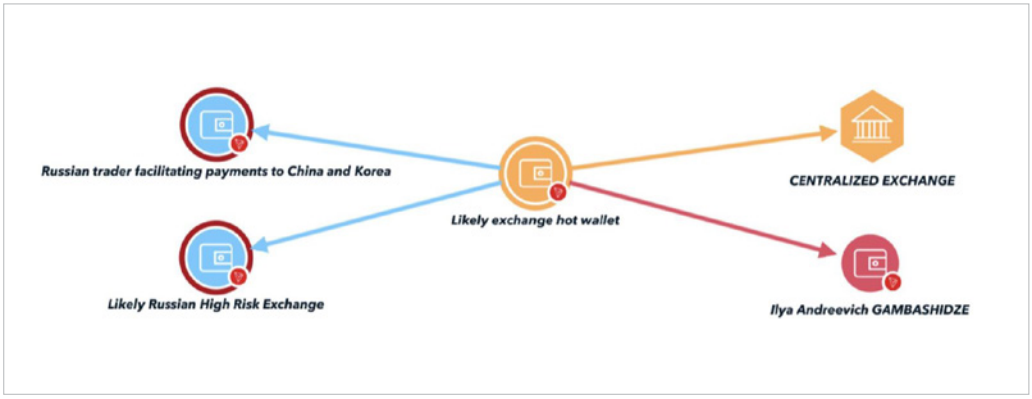
TRM's Graph Visualizer showing movement of funds in and out of an address (TMGLq) associated with Gambashidze

By using BLOCKINT, investigators were able to identify that the first address (TMGLq) was active between April 2022 and March 2024. The vast majority of the funds received by the address came from the sanctioned Russian exchange Garantex. TRM Labs traced several payments through the cross-chain swap service, including one made to a Bitcoin wallet that paid a US-based payment processor — a potential method of paying for internet infrastructure.



The TMGLq address converts USDT into BTC via a cross-chain swap service

The second address (TEFph) was only active between February and March 2024. It appears the vast majority of funds were sent from a hot wallet likely associated with an exchange that has also made significant transfers to other Russian cryptocurrency traders, exchanges, and services.



Payments to and from the second address (TEFph) associated with Gambashidze

CASE STUDY
Using BLOCKINT to disrupt espionage operations

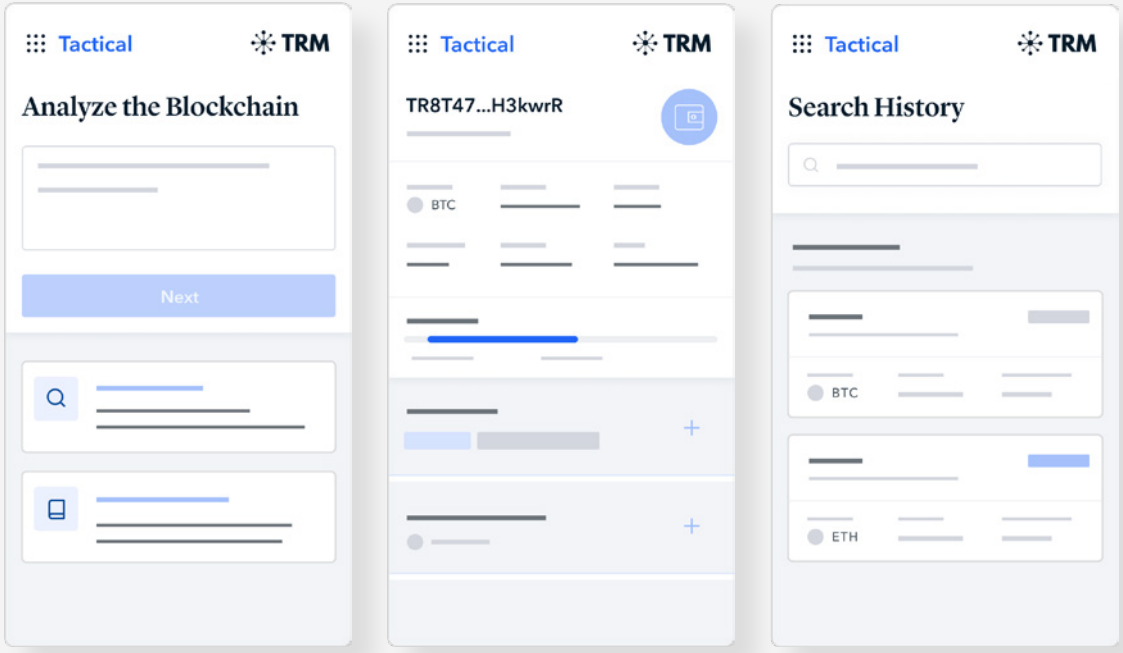
In November 2022, US nuclear engineer Jonathan Toebbe and his wife Diana were sentenced to 18 and 21 years in prison, respectively, for attempting to pass secret nuclear propulsion technology to a third country. In their exchanges with FBI agents posing as foreign officials, the couple requested payment in the Monero privacy coin.

Similarly, in October 2022, the US Department of Justice (DOJ) released a complaint alleging two Chinese intelligence officers made source payments to an individual they believed to be a mole within the DOJ team handling the Huawei prosecution. The intelligence officers sent approximately USD 61,000 across several payments in bitcoin to this alleged mole, in exchange for details about "witnesses, trial evidence, and potential new charges to be brought against Huawei," according to the complaint.

When payments are made in cryptocurrencies, analysts use BLOCKINT. These "breadcrumbs" on the blockchain help them identify and track payments in order to isolate transactions, connect them to dates and times, identify centralized or decentralized financial services involved, and correlate datasets with internal collections to potentially discover new access points to their targets.

TRM IN ACTION

TRM Tactical is a mobile-first BLOCKINT product that helps assets and operators triage artifacts found in the field to determine if they are associated with a person or organization of interest, and if they should be retained.



National security and defense agencies can also use **TRM BLOCKINT API** to ingest enriched blockchain data into their systems. This allows them to correlate blockchain intelligence with other sources of counterintelligence — empowering them to make mission-critical decisions with the most complete data set possible.

4. De-anonymizing ransomware actors

While blockchain addresses are pseudonymous, they are not unattributable. BLOCKINT allows national security and defense agencies to identify patterns of behavior associated with specific addresses linked to real world entities through on-chain analysis, off-chain data, and behavioral analysis.

BLOCKINT also allows agencies to trace the origin and destination of funds on the blockchain, identify clusters of addresses controlled by the same entity or connected entities, and uncover networks of transactions that can lead to the identification of threat actors. This becomes especially valuable when attempting to map out vast cybercriminal ecosystems made up of infrastructure-as-a-service (IaaS) providers, mixers, initial access brokers, and countless other services sold on darknet forums. Non-state MCAs in safe havens like Russia illustrate this concept well.

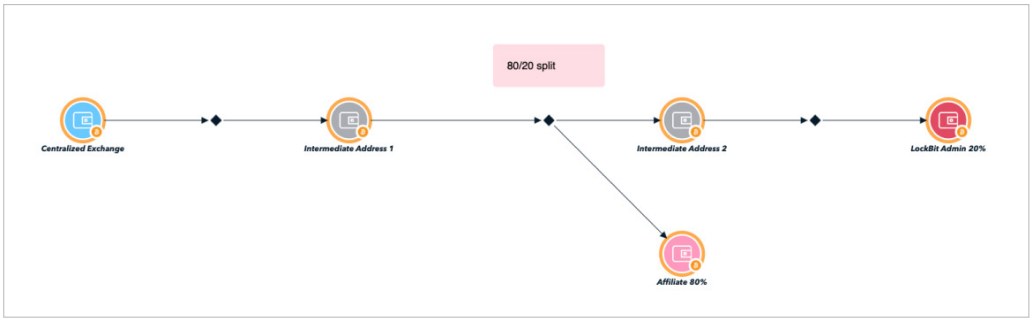
CASE STUDY

US and UK authorities take down ransomware group Lockbit using BLOCKINT

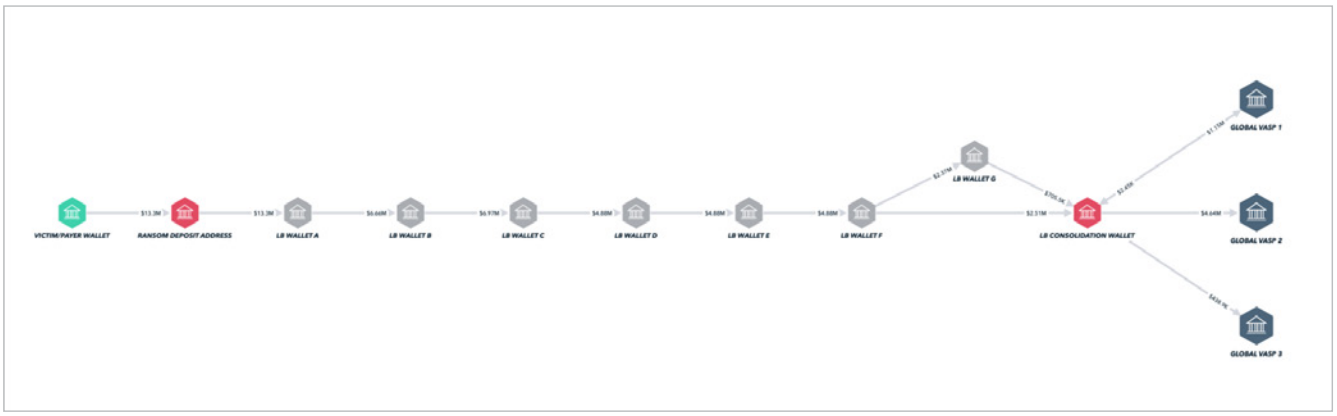
In February 2024, the UK's National Crime Agency, the US DOJ, the FBI, and Europol announced the disruption of the notorious ransomware group LockBit and the takedown of its associated website infrastructure. LockBit, which used a Ransomware-as-a-Service model, attacked various critical infrastructure sectors globally, extorting over GBP 160 million (USD 200 million) in bitcoin between 2022 and its takedown. The group, responsible for over 2,000 confirmed attacks, have had an estimated economic impact that could exceed USD 8 billion in disrupted operations and costs.

LockBit used bitcoin as the primary cryptocurrency used to facilitate ransom payments. But with the evolution of LockBit 3.0, the group has introduced privacy enhanced payment options such as ZCash for both collecting from victims and paying its affiliates.

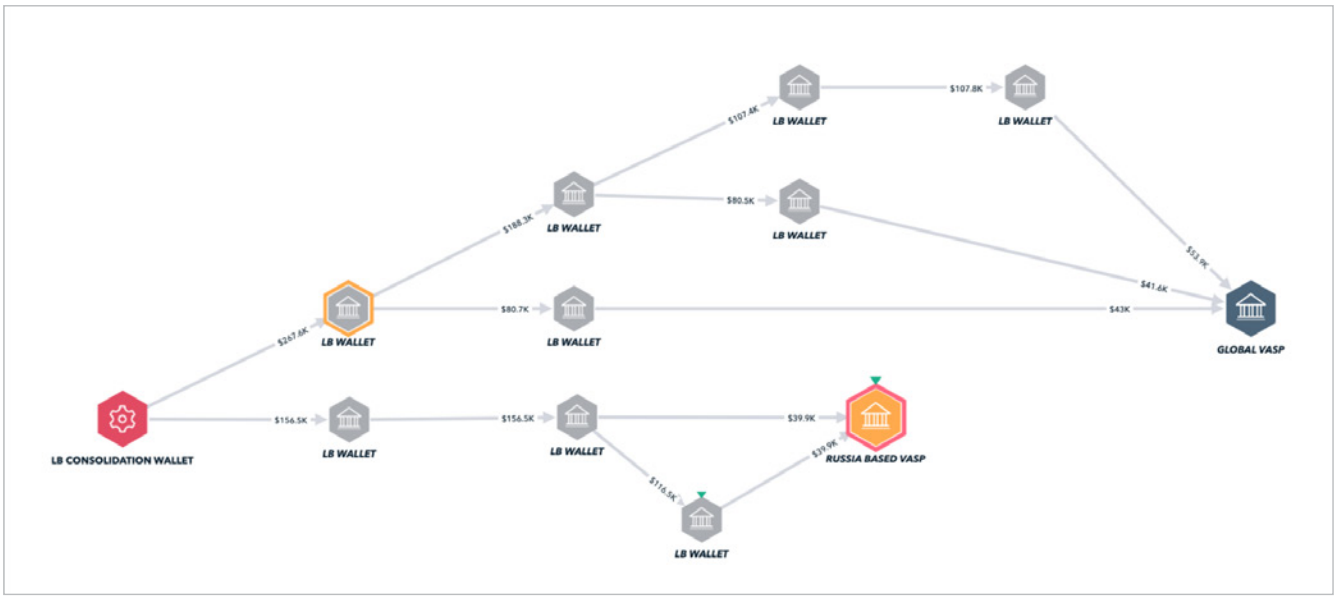
On-chain analysis of LockBit activity highlights the group's operating structure, where victims' initial ransom payments undergo a financial split: 80% goes to the LockBit affiliate, and 20% goes to LockBit's administrators. LockBit operators have subsequently used Wasabi 2.0 to mix funds, and multiple non-custodial exchanges and centralized VASPs in the United States and Asia to launder victim funds.



TRM graph showing initial ransom payments and 80/20 financial split between LockBit affiliates and administrators



TRM graph showing laundering of a USD 13 million ransom payment across multiple VASPs



TRM graph showing laundering of ransom proceeds using multiple smaller cashouts on multiple VASPs

With robust BLOCKINT, these relationships and networks become clearer and more easy to visualize. Analysts can also begin piecing together recurring payments for infrastructure or VPNs, identify patterns (like cuts paid out to developers), correlate advertised prices for exploits with cryptocurrency payments, and so on.

TRM IN ACTION

TRM Blockchain Intelligence Platform helps defense analysts and intelligence agencies monitor on-chain activities to identify potential threats to national security. TRM has unique attribution on PRC, Russia, Iran, and DPRK, established through:

- A dedicated team of threat hunters who actively collect primary source evidence
- Extensive open source intelligence from scanning more than 300 million web pages, dark web forums, paste sites, sanctions sites, Telegram, and more
- Proprietary clustering from advanced data science and machine learning

BLOCKINT has never been more mission-critical

As threat actors increasingly turn to cryptocurrencies to fund their activities, it has never been more critical for defense and national security agencies to invest in blockchain intelligence.

From following terrorist financing, to preventing money laundering and disrupting illicit weapons programs, BLOCKINT helps defense and national security teams develop a more complete operating picture of the threat landscape in their region – and ultimately enables intelligence community members to advance their mission in accordance with national strategies and priorities.