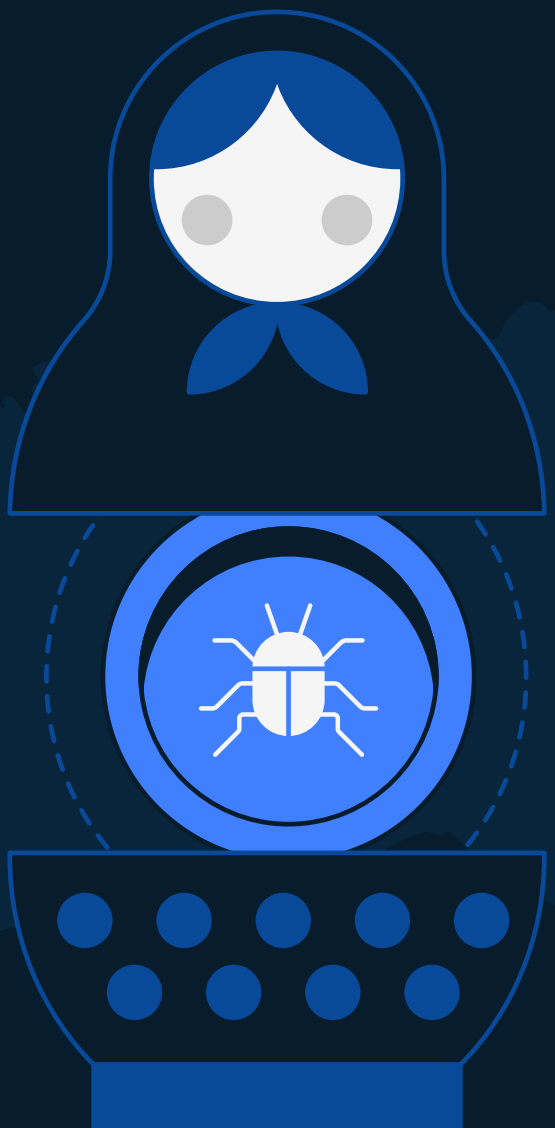
TRM

Comrades in Crime

Exploring the Russian-speaking illicit crypto ecosystem



TRMLABS.COM

The rise of Russian-speaking crypto criminals

From ransomware groups to illicit marketplace operators, Russian-speaking threat actors have become a ubiquitous force in international crypto crime.

Due to the online nature of crypto transactions and widespread use of privacy tools, it is often difficult to confirm whether these actors are in fact based in Russia or have ties to the government. Yet whatever their location, TRM research shows that these groups and individuals — united by their use of the Russian language — play an outsized role in most types of crypto-enabled cybercrime.

Russian-speaking threat actors from across the former Soviet Union consistently drive most types of crypto-enabled cybercrime, from ransomware to illicit crypto exchanges and darknet markets.

- **Ransomware:** Russian-speaking ransomware groups accounted for at least 69% of all crypto proceeds from ransomware in 2023, exceeding USD 500 million
- **Darknet markets:** Russian-language darknet markets comprised 95% of all crypto-denominated illicit drug sales on the dark web in 2023
- **Sanctions:** Inflows to just one Russia-based crypto exchange, Garantex, accounted for 82% of crypto volumes belonging to all sanctioned entities internationally

There are certain exceptions to the dominance of Russian-speaking crypto crime: North Korea remains the world's hacking superpower, responsible for stealing close to USD 1 billion in cryptocurrency in 2023, while Asia-based criminals appear to lead in scams and investment fraud. However, Russian-speaking threat actors are unique in the breadth of their malign activity.

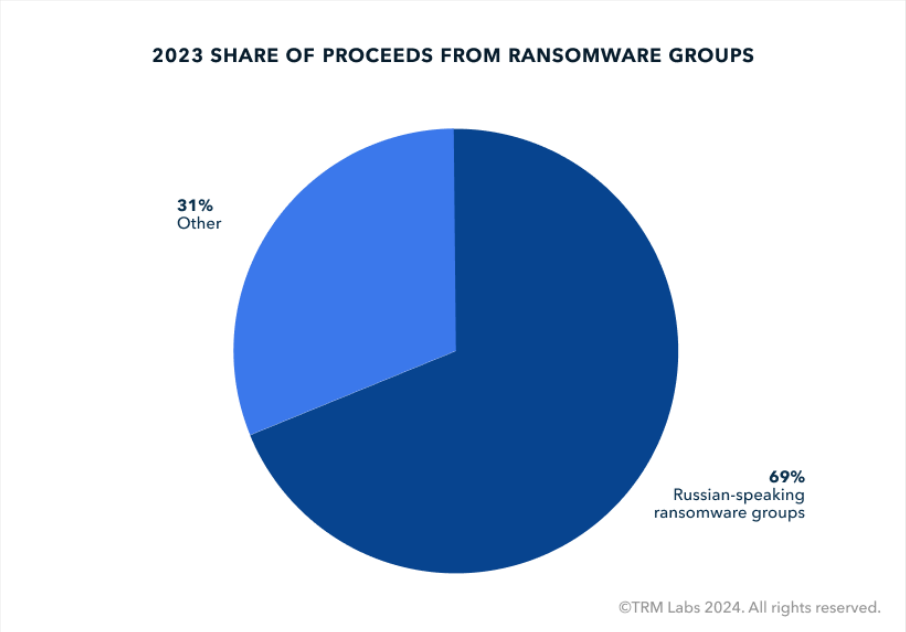
Some Russian-speaking threat actors hold links to the Kremlin and have been actively using crypto to procure foreign equipment for the Russian war effort. Over the past three years, over USD 85 million has been sent to wallets used by Russian and Chinese entities involved in this type of procurement and cross-border trade.

This report brings together blockchain data collected and analyzed by TRM Labs to document the broad range of crypto crime committed by Russian-speaking threat actors.

Russian-speaking groups lead the world in ransomware

Ransomware is a type of malicious software that encrypts a victim's files or data, rendering them inaccessible. The attacker then demands a ransom, usually in cryptocurrency, in exchange for the decryption key. Ransomware has become a significant threat to individuals, businesses, and even governments, with high-profile attacks on critical healthcare and infrastructure facilities.

Russian-speaking ransomware groups accounted for at least 69% of all ransomware proceeds in 2023, which exceeded USD 500 million. Lockbit and ALPHV/Black Cat – the two largest operators in 2023 and both Russian-speaking – together posted attack revenues of at least USD 320 million.



Ransomware groups also sometimes sell their proprietary malware to affiliates or other threat actors as part of a cybercrime business model called "ransomware as a service," or RaaS. This may involve a licensing agreement, subscription service, flat fee, or profit sharing – which allows for rapid distribution and increased attack frequency.

LockBit was one of the most prolific ransomware groups in the world until it was disrupted in 2024 through an international law enforcement operation. The group, whose future remains unclear even though it survived the disruption, operated a RaaS model to conduct thousands of attacks and extort victims for large ransom payments in cryptocurrency.

Lockbit's victims in 2023 included Boeing and the UK's postal operator, Royal Mail. Lockbit posted 43 gigabytes of hacked data online after Boeing reportedly refused to pay a USD 200 million ransom. The Royal Mail also did not pay its ransom of USD 80 million for the 44 gigabytes of data stolen by Lockbit.

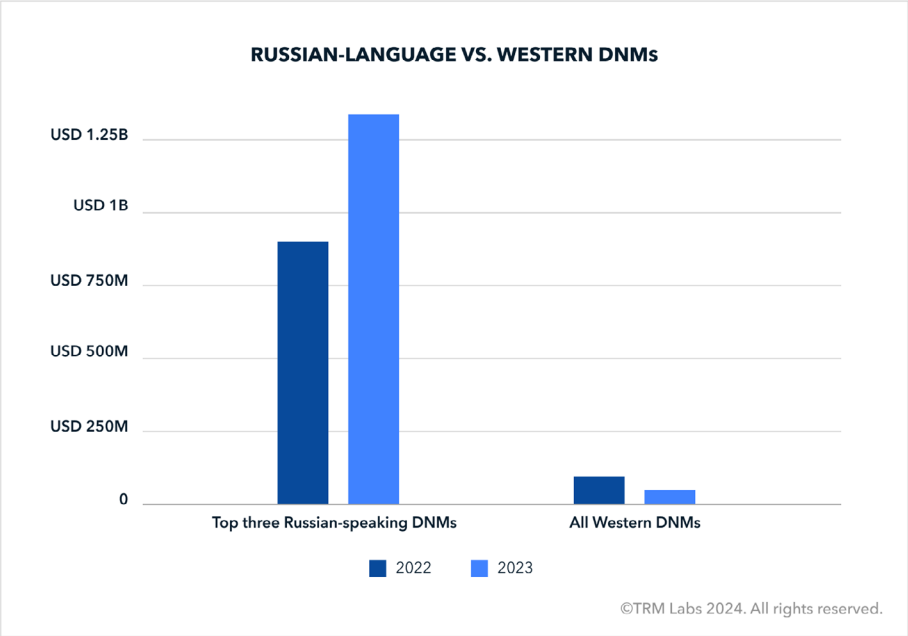
BlackCat/ALPHV, also a RaaS group, uses a sophisticated ransomware strain written in the Rust programming language, which enhances its efficiency and makes it more difficult to analyze. Its significance lies in its use of advanced double and triple extortion tactics, impacting high-profile sectors such as healthcare and critical infrastructure.

In 2023, BlackCat/ALPHV attacks targeted MGM Resorts and Henry Schein, a Fortune 500 distributor of dental and medical supplies that also provides practice management software and solutions for the healthcare industry.

Russian-language darknet markets monopolize crypto-denominated drug sales

Russian-language darknet markets (DNMs) represent 95% of all crypto-denominated dark web drug sales globally. DNMs are multi-vendor online illicit global commerce platforms that mainly sell illicit drugs. An established form of transnational organized crime, DNMs combine anonymization networks and cryptocurrencies with encryption technologies.

Kraken Market, the world's largest DNM in 2024, is a Russian-language marketplace. **The three largest Russian-language DNMs handled USD 1.4 billion in cryptocurrency in 2023, around one-third higher than in 2022.** By contrast, the entire Western DNM ecosystem handled less than USD 100 million in 2023, around a fifth less than in 2022.



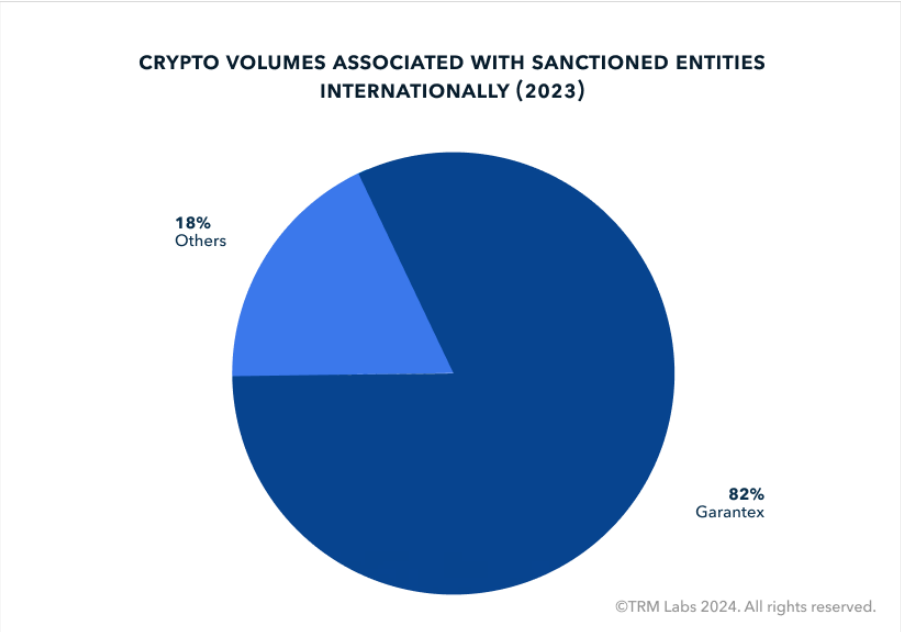
In North America, Western Europe, and Australia, drugs bought on DNMs are generally mailed to customers. By contrast, Russian-language DNMs serving the former Soviet space use dead drops as part of the *zakladka* or "stash" system.

While mail deliveries generally take several days to arrive, dead drops can occur within minutes. Such efficiency has led DNM vendors operating over Tor and Telegram to displace street dealers as the main source of illegal drugs in Russia. Russian-language DNM vendors also source significant volumes of synthetic drug precursors from Chinese manufacturers.

For more information about the role of Chinese drug precursor manufacturers in the international synthetic drugs trade, read TRM's recent report here.

One Russia-based crypto exchange comprised almost all of the world's sanctioned crypto volume

Garantex, a Russia-based crypto exchange sanctioned by OFAC in April 2022, accounted for 82% of crypto volumes associated with all sanctioned entities internationally in 2023. These include crypto exchanges as well as individuals subject to US and international sanctions regimes.



At least some of this volume represents cryptocurrency sent by Russian-speaking actors to sanctioned Chinese manufacturers to purchase military equipment and critical components used by Russian forces in Ukraine. This equipment includes commercial UAVs, anti-UAV equipment, thermal optics, integrated circuits (ICs), GPS modules, and tantalum capacitors critical to production of Russian weapons systems.

Since 2021, at least USD 85 million has been sent to wallets linked to both Russian and Chinese entities involved in the manufacturing, transport, and sale of military and dual use equipment and critical components.

Not all this volume, which is likely to rise as more entities are discovered and attributed, relates to sanctioned assets: it may also include the sale of other goods not related to the war effort as part of the wider cross-border trade between Russia and China settled using cryptocurrency.

Blockchain intelligence catches up with Russian-speaking crypto criminals

When it comes to crypto crime, Russian and Russian-speaking cyber threat actors are rarely out of the news. From Colonial Pipeline and the Democratic National Convention, to the British Library and Royal Mail, they have been responsible for some of the most high-profile ransomware attacks in recent years.

And even beyond the headlines, the Russian-speaking cyber ecosystem is the dominant force behind other types of crypto-denominated illicit commerce, from DNMs to sanctioned exchange transactions. Some threat actors are directly involved in procuring military equipment for Russian forces fighting in Ukraine.

Several factors – historical, regulatory, and normative – may help explain the apparent disproportionate involvement of Russian-speaking actors in crypto-denominated cybercrime. The fall of the Soviet Union left a highly skilled Russian-speaking workforce with limited legitimate economic opportunities. This, coupled with a lack of stringent regulatory frameworks and enforcement mechanisms in many successor states, created a relatively low-risk environment for cybercrime. A shared language and background may also have helped cybercrime actors to forge ties across various former Soviet countries as well as diaspora communities in the West – creating strong network effects.

Because they are active across the former Soviet Union (and beyond) and employ a range of measures to frustrate detection by law enforcement, disrupting Russian-speaking criminals is a difficult and time-consuming task. However, blockchain intelligence tools allow investigators to collect significant insights into their modi operandi and amass vital clues about the location of the physical infrastructure they use.

The disruption of major groups such as Lockbit and Hydra, at the time the world's largest DNM, shows the power of international law enforcement cooperation underpinned by blockchain data. As the threat landscape evolves, TRM Labs will continue to innovate its market-leading tools in the service of creating a safer financial system for billions of people.