TRM

The First Crypto War? Assessing the Illicit Blockchain Ecosystem One Year Into Russia's Invasion of Ukraine

February 2023

When Russia invaded Ukraine on February 24, 2022, many analysts and commentators anticipated that it would become the world's first crypto war.

There were several reasons for such predictions. The offensive spurred the first major international conflict since the mainstream emergence of crypto in the 2010s. It also coincided with the top of the crypto bull run, when bitcoin and blockchain-enabled goods such as NFTs reached historic highs and maximum hype.

Second, countries of the former Soviet Union have long dominated global hacking and cybercrime activity. Both factors raised expectations that cyber warfare would play a significant role in the conflict.

Third, Ukraine's wholehearted embrace of crypto for international donations, together with fears that Western sanctions would spur a rise in crypto adoption by Russian entities seeking to evade them, also contributed to a sense of crypto's centrality to the conflict.

As the war marks its grim first anniversary, TRM Labs has focused its analysis on the state of the illicit crypto ecosystem over the past year. This report discusses how cybercriminals have adjusted their organization and tactics to adapt to the ongoing financial, political and logistical disruptions facing Europe and the wider world.

Key Findings

DNMs and High-Risk Exchanges Continue to Thrive Despite Western Crackdowns

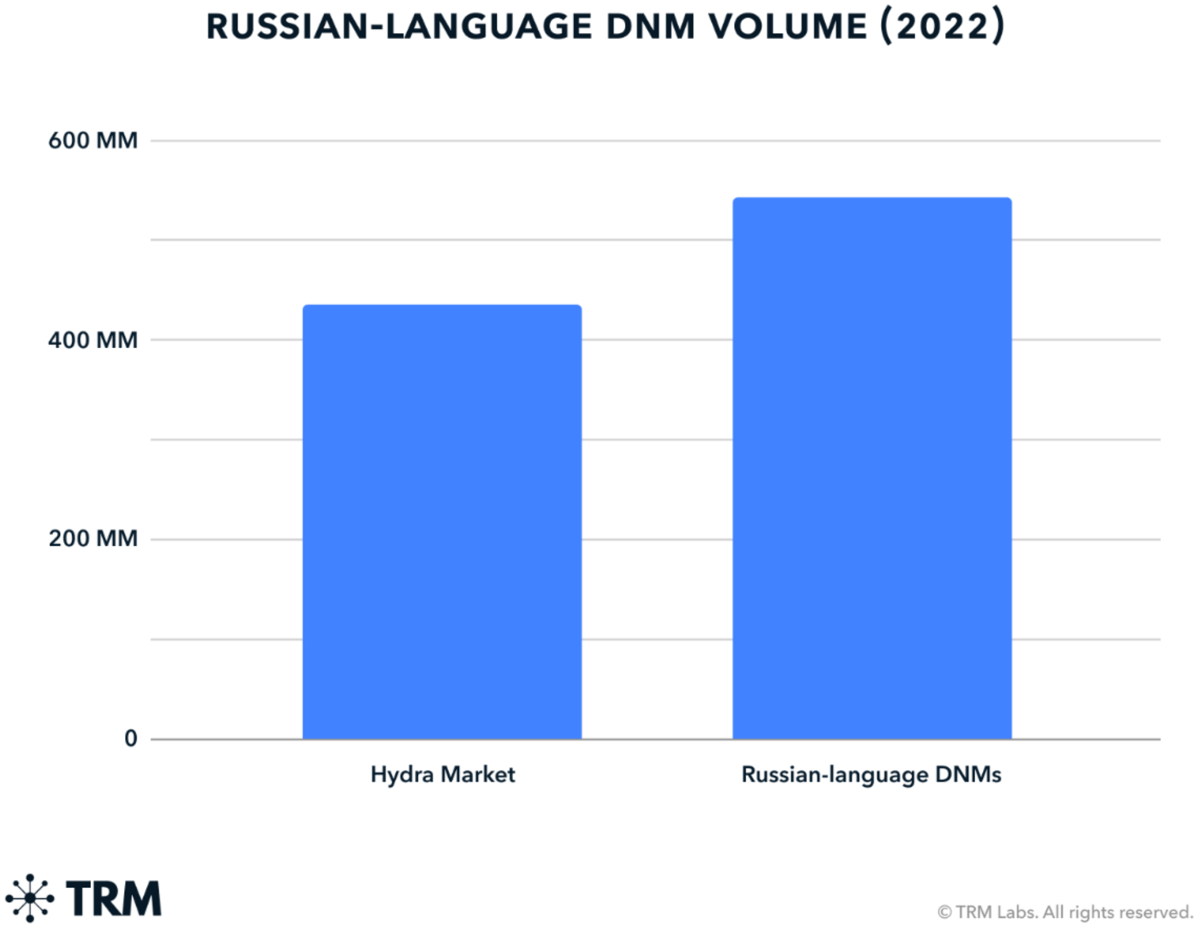
On April 5, 2022, German authorities working in conjunction with the US and Estonia, closed down Hydra Market, at the time the world's largest DNM – responsible for some EUR 1.23 billion in sales in 2020 alone.

Frankfurt's Public Prosecutor's Office Central Office for Combating Cybercrime (ZIT) and the German Federal Criminal Police Office (BKA) seized Hydra servers and over EUR 23 million worth of bitcoin. That same day, Hydra was sanctioned by OFAC. OFAC also sanctioned Garantex, a Russian crypto exchange accused of processing transactions linked to Hydra and other illicit sources. However, its servers were not disrupted.

"Our actions send a message today to criminals that you cannot hide on the darknet or their forums", the State Department announced in a press release, "and you cannot hide in Russia or anywhere else in the world."

Hydra's shutdown resulted in a significant short-term hit to the crypto-based illicit drugs trade. However, ten months on, the Russian-language DNM ecosystem appears to have sprung back to life, with the emergence of more than a dozen new marketplaces.

TRM research shows that while total DNM sales volumes remain lower year-on-year than in 2021, indications point to a robust recovery. Globally, DNMs amassed a quarter more volume from May to December 2022 than they had between January and April, when Hydra Market was still active.



By the end of 2022, the explosion of new DNMs that fought to take Hydra's place saw a major consolidation, with just four players responsible for 80% of market share. Notably, all were Russian-language DNMs.

Overall, Western sanctions and law enforcement action appears to have had little impact on DNMs. They enjoyed several periods of sustained growth, between April-July 2022 and October-December. In fact, December 2022 was the most successful month for the Russian-language DNMs, which amassed more than USD 130 million in sales.

A similarly robust picture emerges when it comes to Russian high risk exchanges. TRM defines high risk exchanges as having more than one of the following characteristics:

- Minimal KYC controls
- A history of illicit on-chain and off-chain activity
- Located in unregulated or unsupervised jurisdictions

- Facilitate cash transactions

High-risk exchanges, or those with little to no KYC or AML controls, process up to 90 times more illicit crypto volume than non high-risk exchanges. Almost all Russian exchanges (95%) are considered high risk, according to the above definition – a figure that has remained largely unchanged since the outbreak of the war.

Garantex, the Russian high risk exchange sanctioned by OFAC in April 2022, posted USD 18.36 billion in volume between February 2022 and February 2023, more than double its previous annual figure of USD 7.76 billion..

Russia-linked Ransomware Gangs Restructured, Possibly to Avoid Potential Sanctions

Facing increased scrutiny from Western law enforcement (including the threat of sanctions), Russian-speaking ransomware operators have attempted to increase their anonymity through changes in on-chain behavior.

TRM's analysis of on-chain transactions, open source reporting, and proprietary information found that two major syndicates, LockBit and Conti, restructured their activities, likely to avoid sanctions by Western countries.

Conti, one of the most prolific syndicates, shut down its original operation and rebranded into at least three smaller groups: Black Basta, BlackByte and Karakut, the last of which was formerly a side project run by Conti operators.

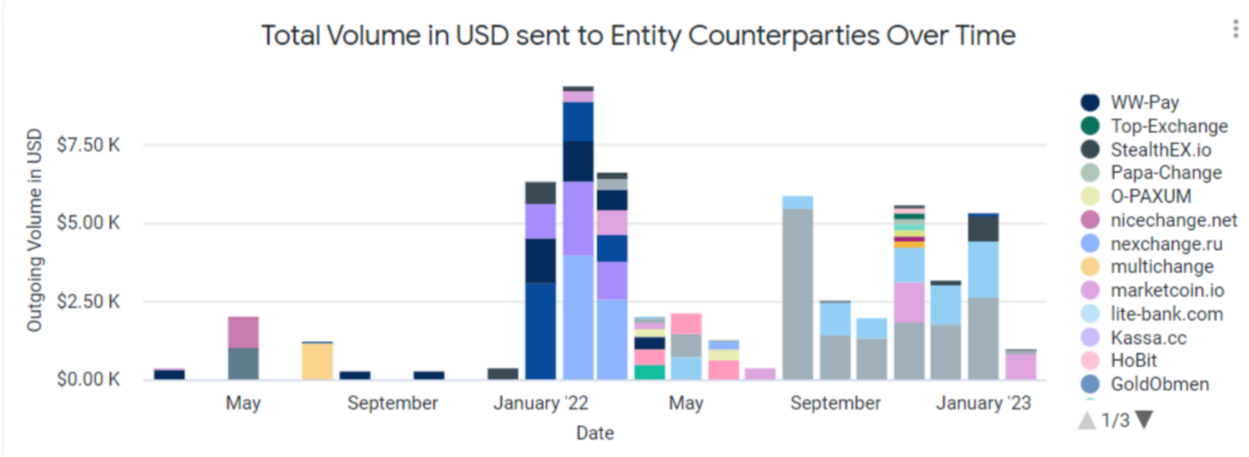
Data on LockBit suggests the group has rebranded since the invasion of Ukraine. On June 27, 2022, LockBit announced LockBit 3.0, stating that their activities were apolitical and the group is focused on monetary gain.

LockBit published the following statement on February 27, 2022: "Our community consists of many nationalities of the world, most of our pentesters are from the CIS including Russians and Ukrainians, but we also have Americans, Englishmen, Chinese, French, Arabs, Jews, and many others in our team. Our programmers developers live permanently around the world in China, the United States, Canada, Russia and Switzerland."

A LockBit representative also stated on July 24, 2022, in an interview with Red Hot Cyber that it does not support Russia. LockBit's claim that it had no intention to purposely attack Western countries may have been motivated by the possibility of Western sanctions against Russian entities. Moreover, LockBit stated that it had prohibited attacks against entities related to critical infrastructure, probably to minimize the risk of law enforcement attention and potential sanctions.

Entities Linked to Child Sexual Abuse Material (CSAM) Flocked to Russian High-Risk Exchanges and Darknet Markets (DNMs)

TRM research identified a sharp spike in the volume of funds sent by CSAM-linked entities to Russia-based high-risk exchanges between December 2021 and March 2022.



On the day of the invasion, CSAM entities were found to have sent at least USD 3,700 to Russian high-risk exchanges, of which USD 3,500 went to Nexchange.ru.

Although USD 3,700 may seem like a small amount, it is potentially highly significant. This is because the figure represents only those cases where a CSAM entity sends funds directly to an address controlled by Nexchange.ru. CSAM entities usually seek to avoid such direct exposure to exchange addresses for anonymisation purposes, as evidenced by a lack of almost any such transactions observed in the months prior to the war.

One hypothesis for the sudden appearance of such direct exposure is that CSAM actors may have rushed to launder and cash out the proceeds of crime, possibly to obtain liquidity ahead of a full-scale international war and any ensuing economic shocks.

Yet while direct money movements between CSAM actors and Russian high risk exchanges peaked in February 2022, they remained a significant presence for the rest of the year. In total, approximately USD 57,000 were sent by CSAM entities to Russian High-Risk Exchangers in 2022. Such sustained activity may suggest a longer-term shift in the relationship between CSAM groups and Russian exchanges.

Russian-Language DNMs Used as Money Laundering Mixers

It is possible that Russia's political and economic estrangement from the West has fuelled perceptions that the country is a friendly jurisdiction for criminals seeking to evade Western law enforcement. Indeed, TRM research has also noted an increase in the use of Russian dark net markets (DNMs) - whose main purpose is selling illicit drugs to customers in former Soviet countries - as money laundering tools by international criminal groups (this phenomenon is discussed elsewhere in this report).

Russian-language DNMs frequently function as quasi-mixers, commingling funds from customers, vendors, sales, marketplace commissions and other sources. Their escrow systems process payments by merging different sets of coins from different origins. When withdrawing funds from the marketplace, the original tokens deposited by a user will have been replaced with different coins of a similar value (minus the withdrawal commission). Russian-language DNMs also allow users to exchange deposited funds both into cash via dead-drops as well as into digital wallets. This breaks the trail linking user deposits to purchases, withdrawals, and other exfiltration avenues, allowing malicious actors to use Russian-language DNMs for laundering purposes.

TRM data shows there is a variety of threat actors laundering funds through these DNMs, especially cybercrime services, shops selling stolen credit card data and personally identifiable information (PII) – also known as carding/PII or fraud shops – as well as independents who run their own marketplaces where they are sole vendors. Funds originating from ransomware, investment schemes, violent extremism, scams and CSAM were also seen being laundered through these DNMs.

To add an additional layer of security and break the blockchain trail, some threat actors then withdraw the funds from these DNMs and send them to dedicated mixers, gambling services, decentralized finance projects, and various payment services.

Hackers Take Sides, But Dark Net Markets Stay Neutral

Much has been written about the apparent schism provoked by the war within the Russian-speaking cybercriminal community, which comprises nationals of both Russia and Ukraine as well as other nearby states with divergent views of Moscow's politics.

However, TRM research found that the conflict appears to have had a greatly uneven impact, with some categories of cybercrime much more likely than others to exhibit divisions along political lines. Hacking groups have been the most vocal in taking sides, while DNMs appear largely to have steered clear of overt partisanship.

Russia's invasion of Ukraine saw the political alignment of several Russian-speaking hacking groups. Several publicly pledged loyalty to Russia or Ukraine and began accepting cryptocurrency donations to fund their operations and raise money for military equipment.

Known as *hacktivists*, these groups conduct high-profile attacks against targets – including critical infrastructure – located on the territory of their declared enemies. Common operations include DDoS attacks, which target websites by overloading them with requests. Although such attacks don't affect the confidentiality or integrity of the targeted data, they pose a significant threat to victims' day-to-day operations and often result in financial and reputational losses. Other nefarious activities include breaching networks to steal sensitive data and defacement attacks, where hackers break into a website's code and tamper with its images and text.

Two of the largest and most prominent hacktivist groups to emerge from the conflict are the pro-Russian KillNet and pro-Ukrainian Dump Forums. Both claim to be composed of volunteers fighting for the national interests of each country without being directly affiliated with any government.

KillNet

KillNet is a pro-Russian group that actively supports Russia's war in Ukraine and Moscow's wider geopolitical agenda. First observed at the end of 2021 acting as a DDoS attacker for hire, following the invasion KillNet pledged loyalty to the Russian state and began to use crypto to raise funds for the Russian war effort. It also began targeting government entities and critical infrastructure in countries opposing the invasion, through DDoS attacks against Lithuania, Poland, Japan, Norway, the Czech Republic, Moldova, and the US, among others.

KillNet uses its channel on the Telegram app (with nearly 100,000 followers as of February 2023) to solicit cryptocurrency donations. KillNet solicits donations in BTC, Monero, USDT, and Ethereum and has cashed funds out on Eastern European high-risk exchanges with weak Know-Your-Customer (KYC) requirements.

TRM research found that crypto addresses attributed to KillNet received around USD 280,000 over 2022. By February 2023, KillNet's total traced cryptocurrency donations reached nearly USD 310,000. The group has claimed to use these funds to purchase and deliver military and other equipment to Russian forces fighting in Ukraine. Its official Telegram page contains photos that appear to show special forces soldiers taking delivery of night vision goggles; other photos show a rocket emblazoned with the words "We are KillNet", an ostensible note of thanks from the troops. TRM research has found no on-chain corroboration of links between KillNet and the Russian military.

Over the past two months, KillNet claimed numerous cyber attacks against Western targets, including the UK and US healthcare sectors. This led the US Health Sector Cybersecutiry Coordination Center to issue a warning to healthcare sector companies identifying KillNet activity as "a threat to government and critical infrastructure organizations including healthcare." Most recently, KillNet took credit for a network failure that disrupted dozens of flights operated by the German airline Lufthansa, even as the airline blamed an accidentally severed cable.

Dump Forums

Founded in May 2022, the pro-Ukrainian Dump Forums is among the most visible hacktivist groups combating Russian interests. Like KillNet, it is staffed by Russian-speaking individuals (the Russian language is not an indicator of nationality as most Ukrainian citizens can speak both languages fluently). The Dump Forums attack arsenal includes DDoS attacks, breaching and leaking of sensitive data as well as defacement attacks.

The group's Telegram account has around 10,000 followers; it also uses an eponymous online discussion forum. Dump Forums has claimed attacks against Russian state institutions including Gazprombank, the Federal Tax Service, the postal service, the Federal Security Service (FSB), and others. As with KillNet, such claims are rarely independently corroborated.

Dump Forums demands ransom payments in cryptocurrency. Most recently, in January 2023, Dump Forums claimed to have stolen data from Russia's Ministry of Construction and Housing and threatened to leak it unless the ministry transferred an unspecified amount of cryptocurrency. On-chain investigation by TRM found no evidence that any ransom payment was made to date to the specific wallet address provided by Dump Forums. In total, other wallet addresses publicly posted by Dump Forums were found to have received over USD 21,000.

Russian-Language DNMs Prioritize Commerce Over Politics

Questions of loyalties regarding the war in Ukraine do not seem to have had a significant impact on Russian-speaking DNMs. That is not to say that individual DNMs have not been linked to other illicit actors with clear political sympathies.

For example, the DNM Solaris voiced support for the Russian government and formed a partnership with KillNet. Nearly $50,000 was sent directly to KillNet from an address associated with Solaris in October 2022, while KillNet claimed to conduct cyberattacks against RuTor, a forum that provided support to Solaris competitor OMG!OMG! Market. According to the message, RuTor then paid $15,000 USD to KillNet to stop the DDoS attack. On-chain analysis by TRM corroborates these claims.

However, although OMG!OMG! Market and the RuTor forum are perceived as pro-Ukraine, they have not banned Russian vendors. Meanwhile, their shared support for Putin's invasion did not prevent Kraken, another ostensibly pro-Russian DNM, from attacking Solaris Market.

It is possible that the lack of political alignment among Russian-language DNMs reflects the highly-fragmented DNM landscape since the elimination of Hydra market, in which challenger DNMs are engaged in a constant struggle for commercial supremacy and market share (similar strife occurred amongst Western DNMs in the early 2010s in the wake of the takedown of SilkRoad by US law enforcement).

Conclusion

One year since the start of Russia's full-scale invasion of its neighbor, the war in Ukraine continues to exact an enormous toll. Thousands of lives have been destroyed as vital food and economic infrastructure, European security and the future of the established international order itself remain in jeopardy.

Unfortunately, the war does not appear to have had a similarly disruptive effect on international criminal networks operating in the crypto ecosystem. On the contrary, as illustrated by our findings relating to the use of Russian DNMs and high risk exchanges by CSAM entities and other illicit actors, the conflict appears to have led criminals to embrace Russia as a safe haven outside the reach of Western sanctions and law enforcement, and the breakdown in coordination between Moscow and Washington on cybercrime matters in the wake of the war appears to have emboldened a host of international malicious actors.