Trend Research

TREND MICRO

The Russian-Speaking Underground

Dr. Fyodor Yarochkin, Vladimir Kropotov, and Robert McArdle

Contents

Published by
Trend Research

Published by
Dr. Fyodor Yarochkin, Vladimir Kropotov, and Robert McArdle

For **Raimund Genes (1963-2017)**

This paper focuses on recent key developments in the Russian-speaking cybercriminal underground, which are driven by emerging new technologies, evolving criminal business processes, and recent social and geopolitical changes.

The Russian-speaking underground's community exists and operates across multiple territories. It is probably the most formidable in terms of capacity, sophistication of attacks, geographical target distribution, and types of criminal business processes when compared to the cybercrime activities we see coming from other language communities. Additionally, it plays a significant role in major cybercrime-related news events, further cementing its influence on the global threat landscape.

With its high levels of maturity, sophistication, and status as thought leaders in the cybercrime landscape, developments in the Russian-speaking underground significantly impact the attack surface and reshape risks for businesses, governments, and even ordinary internet users, while also influencing cybercriminals from other geographical areas to adopt similar tactics. A deep understanding of these developments and trends provides valuable, actionable strategic and tactical cyber threat intelligence. Organizations can make use of these insights to strengthen their defenses and effectively protect their assets.

Among these key developments, it is important to highlight the risks introduced by new technologies, social and geopolitical changes, and the expansion of business models. The significant leverage provided by AI-exposed personally identifiable information (PII) and biometrics data by malicious actors in the underground has made it easier to generate stolen or fake digital identities. This impacts financial and government verticals and reshapes the risks and attack surface for social, ecommerce, messenger and mass media platforms.

There has been an expansion of cybercriminal operations to incorporate previously uncommon targets (such as telecoms and SS7 signaling systems), along with a greater focus on exploiting internet of things (IoT) hardware, edge devices, mobile platforms, and routers. This is further exacerbated by the fact that parts of this equipment often fall outside traditional corporate risk models, and the value of compromising them is frequently underestimated by defenders.

There have also been shifts in the priorities, scope, and use cases for bulletproof hosting services (BPH). Traditional BPH services are fading away, being replaced with other tailored solutions. Physical hosting locations are increasingly dependent on the location of the targets (for example, it is difficult to take down assets in Ukraine based on Russian requests or assets in Russia by the request of western countries).[1]

Significant changes in the financial flow and logistical operations of underground actors caused by sanctions has led to several consequences in the criminal underground. The reshipping business has reached unprecedented heights, while bitcoin has become more ingrained into the everyday underground economy. Meanwhile, normal businesses are increasingly showing interest in grey financial services to minimize business impact.

Geopolitical unrest has led to changes in the relations and trust between threat actors in different Russian-speaking countries. The red lines for threat actors in such regions have shifted significantly, with the understanding of what is "acceptable crime" expanding in scope considerably. Cybercriminals have increasingly targeted a greater number of regions, critical verticals, organizations, and asset types – which were previously largely off limits – as a result.

Changes in the local laws of countries in this region, along with new regulations on income sources, travel capabilities, and other aspects of life have caused ordinary citizens to relocate, and in doing so, have also changed the geographical distribution of the criminal actors originating from Russian-speaking countries. This has resulted in the emergence of new cyber-physical crimes in the regions where threat actors have relocated.

The growing polarization between these societies have also driven increased involvement in hacktivism. Furthermore, the convergence between threat actors from different regions and linguistic groups (e.g., Russian and Chinese-speaking criminals) has led to previously unobserved synergetic cooperation, such as collaboration between groups supporting nation-state interests (targeted espionage) and cybercriminal activities.

A deeper alignment with government interests has become more evident in the criminal underground, leading to a shift in the landscape. Some groups are using their national affiliations to protect their business models during times of conflict – for example, ransomware attacks are being propped up as attacks against enemy critical infrastructure.[2]

Criminal and nation-state groups are learning from each other, with states increasingly tapping into this ecosystem to enact their goals. For some state-focused missions, it doesn't matter who physically carried it out – whether nation-state actors, hacktivists, or financially-focused cybercriminals – as long as the results of the attack support the state's strategy. As a result, we anticipate a growing number of cases where state-backed threat actors manipulate sympathetic cybercriminal groups and hacktivists to drive them to accomplish government-aligned objectives, either knowingly or unknowingly.

These situations, trends and scenarios have a significant impact on the complexity of attacker attribution, affecting key Cyber Risk Exposure Management (CREM) procedures for governments and enterprises globally. However, combining the use of leading security platforms with the consumption of strategic intelligence resources, such as this report, plays a crucial role in addressing these concerns.

Introduction

This research is intended to highlight the major developments in the Russian-speaking underground in recent years. The Russian-speaking underground community operates across multiple countries and territories, and is considered as possessing the strongest capabilities in terms of capacity, sophistication of attacks, geographical distribution of targets, types of criminal business processes, and impact in news reporting. The spoken language and similar cultural backgrounds are seen as two major unifying factors of this wider group of threat actors. This work continues our long running efforts from our Cybercrime Underground series of publications to shed light on how these criminal underground communities operate. This publication marks a significant milestone as the fiftieth installment in the series, with a complete list available in the appendices of this document.

We have covered the Russian-speaking underground community's evolution over several previous publications, which includes the following:

- *Russian Underground 101, published in 2012*[3]
- *Russian Underground 2.0, published in 2015*[4]
- *Hacker Infrastructure and Underground Market trilogy, published in 2020*[5, 6, 7]

The significant geopolitical and economic changes that have occurred in recent times provide the perfect opportunity to once again examine how these have affected the current landscape of the Russian-speaking underground.

When discussing the Russian-speaking underground, it is crucial to distinguish between the terms *"Russian"* and *"Russian-speaking"* underground, which are often confused by many news and media outlets, or even governments. The Russian language is widely spoken and understood in many territories of the former USSR area and beyond. The language is also easily understood by speakers of other Slavic languages (Polish, Bulgarian, Chez, Serbian, Croatian), and is also a minority spoken language in some neighboring countries, such as Finland,[8] Romania, and Moldova.

The Russian-speaking underground evolved from strong technical education communities in the former USSR area, with many technically savvy individuals socializing via the FidoNet network that existed in former USSR territories before the modern internet became widely available.[9]

With the rapid expansion of the internet in the late '90s, users converged around several communities, including forums such as *"anti-chat"* and *"reversing dot net,"* and virus writing online zines (magazines) such as *"Infected voice."*[10] The larger-scale monetization of the Russian-speaking underground community began in the early '00s and generally evolved from the *"trading"* sections of existing online forums. Eventually, these sections then significantly evolved and diversified over the years into what would become the cybercriminal ecosystem. Certain external factors, such as the introduction of WebMoney and Bitcoin, the emergence of the Android ecosystem, the rise of the Web3 ecosystem and generative AI – all considerably shaped and influenced trends in the Russian-speaking underground.

Many trends that have emerged in the Russian-speaking underground are not entirely criminal in nature; they sometimes exist in a grey area that allows the participants to monetize their skills. Search engine optimization (SEO) and pharmaceutical supply businesses were, at one time, common money-making paths that existed in this gray area and generated substantial revenue for their operators.[11] Malware known as lockers were traditionally popular, however the growth and proliferation of ransomware, along with the increased scrutiny on ransomware operators from global law enforcement, has resulted in ransomware topics being less acceptable in common communication forums.

Major criminal groups within the community tend to maintain a low public profile to avoid attracting attention from law enforcement agencies with the power to disrupt their operations. For this reason, there is a common ethical boundary – often expressed as the "we do not work in RU" rule – prohibiting the targeting of the region in which the threat actors reside.

We recognize that this paper represents a substantial body of work. To enhance readability, we have divided it into two major sections for the reader's convenience:

- The core paper primarily focuses on the recent significant developments in the Russian-speaking underground that are driven by the appearance of new technologies and criminal business processes, along with recent social and geopolitical changes. Each major section begins with key takeaways, allowing readers to quickly identify and navigate to the most relevant content.
- The appendices serve as a reference, offering information and examples of sales posts and pricing for commonly available criminal services.

For readers interested in exploring additional underground trends, we recommend these key underground publications:

- *Hype vs. Reality: AI in the Cybercriminal Underground*[12]
- *Inside the Halls of a Cybercrime Business*[13]
- *The Gender-Equal Cybercriminal Underground*[14]
- *Bridging Divides, Transcending Borders: The Current State of the English Underground*[15]
- *Across the Span of the Spanish Cybercriminal Underground: Current Activities and Trends*[16]

Additionally, for those who want comprehensive knowledge on the evolution of cybercrime over the last 15 years, a complete list of all fifty publications in our *Cybercrime Underground* series can be found in the appendices.

Common Trends in the Underground

Underground activities in general, and in Russian-speaking regions in particular, seem to be evolving in cyclical patterns, with past trends resurfacing and improving as technology and society changes.

This is particularly noticeable in the approach to monetary theft:

- In the early days of cybercrime, criminals focused on stealing large amounts of money. However, such substantial theft also results in increased scrutiny and attention from authorities.[17]
- Over time, cybercriminals realized that instead of stealing US$1,000,000 from a single person, stealing US$1 from a million people would significantly reduce the chances that a victim (or law enforcement) would attempt to retrieve the stolen money.
- Threat actors also realized that good operational security (OPSEC) will allow them to target larger sums of money, while making it very difficult for law enforcement to discover their true identities.
- The proliferation of large-scale theft has led to more awareness of their risk, leading to a decline in the number of victims paying ransom or extortion demands. At the same time these massive losses has led to increased attention from law enforcement and greater collaboration and prioritization in cybercrime investigation. This has resulted in significant arrests and takedowns, as attackers are finding it more difficult to maintain OPSEC and hide their true identities.
- We've seen several global developments that have reshaped criminal business processes further in recent years. These developments are related either to changes in technologies, social behavior, or financial flows. The development of AI technologies have enabled attackers to conduct more complex attacks at scale, once again focusing on stealing smaller amounts from millions of victims. This approach helps cybercriminals stay under the radar and avoid attention of those that might pursue them.

Figure 1. Stealing a dollar from a million people still nets a criminal a million dollars – the cycle repeats itself.

In this section, we will discuss some of the other major trends affecting the cybercriminal underground in recent years. We provide concrete examples of the changes leading to these trends in later sections of this publication.

Pandemic Impact

The Covid-19 pandemic reshaped cybercriminal business processes, forcing threat actors to adapt to major shifts in social behavior of societies, as well as changes in how governments and organizations operate.

IT responses to Covid-19 boosted technologies that allow workers to work remotely in isolation, fundamentally altering the attack landscape. The business processes for many critical verticals, including telecommunications, government, and financial services, had to be rapidly changed to adapt to the new reality and ensure continuity of operations.

The key enabler for this was a switch to remote services and work-from-home (WFH) models wherever possible. The side effect of the switch was that the well-established security processes had to be quickly adapted to meet the new restrictions. Consequently, procedures such as identity verification and initial services enrollment shifted from in-person interactions to remote verification.

Such significant shifts, like the changes in IT environments, driven by widespread remote work, altered the attack surface and affected CREM procedures, especially for government, financial, and telecommunication services.

The shift to remote operations provided scaling capabilities to the attacks conducted by financially-motivated threat actors, with the number of potential targets and attack vectors increasing in parallel. Organizations have been forced to prioritize the continuity of their operations over security, leading to reduced capabilities in protect distributed assets – such as remote employees – compared to the traditional security setups, where the location of the assets were centralized or localized.

Switching to all-remote setups also provided threat actors the ability to target assets in new regions where IT services are underdeveloped, and organizations struggle to adapt to the new reality. These rapid developments introduce flaws and create opportunities for cybercriminals to attack new business models that did not exist before.

Increased Maturity on Both Defender and Attacker Sides

On the defender's side, the growing scale, variations, and measurable impact provide a deeper understanding of the value of cybersecurity for businesses and the importance of additional investments into the protection of their critical business processes.

These investments have led to an increased role of Chief Information Security Officers (CISOs) and cybersecurity teams within organizations, contributing to the increased overall maturity of the cybersecurity industry.

This has reshaped risks models for underground threat actors, raised the costs of their operations, and rendered obsolete or lowered the profitability of some criminal concepts and monetization approaches.

The growing defender maturity has forced cybercriminals to adjust their existing malicious business processes and has elevated criminal technologies and tools to a more sophisticated level.

In turn, this increase in cybercrime maturity has also resulted in an increase in cyberattack profitability. The rise in both financial resources and operational maturity has enabled threat actors to hire more experienced cybercriminal experts and deploy sophisticated tools, techniques and exploits in their attacks and campaigns.

The Emergence and Accessibility of New Technologies and Datasets

The accessibility of new technologies and datasets are enabling cybercriminals to reshape and innovate their criminal business processes.

In recent years, several significant changes affected cybercriminal underground behavior and monetization approaches:

Side Effects of the Ransomware Double Extortion Business Model and Mass Data Breaches

The scale and number of breaches and theft of sensitive information published by criminals in recent years driven by the ransomware double extortion business models has significantly transformed the criminal market.[18] It led to the exposure of PII at a global scale, with nearly all countries around the world affected. This information has become an increasingly important enabler of criminal business processes, not only for the initial profitability of extortion, but also as a requirement for emerging criminal business models centered on the creation or impersonation of identities.

Exposure of Biometrics at Scale

The unintended exposure of biometric data in social media platforms[19] is a significant yet often underestimated factor exploited by underground groups using their updated criminal business processes. It is commonly used in combination with exposed PII and accessible AI tools in criminal activities related to the creation of new identities, bypassing biometric-based 2FA and enhancing extortion and scam operations – often making use of new deepfake technologies.[20]

Accessibility of AI tools

The accessibility of AI tools has boosted criminal business processes, appearing at an opportune time when international law enforcement efforts has been affecting the dominant ransomware business model.

As AI continues to evolve, it enables criminals to combine a variety of monetizable data and revamp existing criminal operations to improve their effectivity and scale. Real time deepfake-enabled scams are also conducted over messenger apps, corporate channels, and video calling platforms.[21] AI-using underground threat actors can interact with their targets and victims in multiple languages even without prior knowledge or study. AI also enhances the precision and quality of social engineering attacks by incorporating cultural nuances specific to the victim's location, something previously impossible at scale. It enables cybercriminals to target regions that were previously beyond their ability to attack.

The Development and Rise in Popularity of Cryptocurrency and Web3 Technologies

The increasing popularity of Web3 technology, its vast scale of money flow, and the appearance of thousands of cryptocurrencies have enabled criminals to create monetize new business niches, facilitate money laundering, and incorporate Web3 and cryptocurrency assets into their business processes.

Fake non-fungible tokens (NFTs), pump-and-dump schemes, impersonation, spoofing of trusted entities for crypto scams, Ponzi schemes, and asset theft are just a few examples of potential monetization tactics.[22] Blockchain-related threats have become an entire sub-industry with its own specializations that did not exist in the past.

Further Diversification and Specialization of Underground "Professions"

We observed further diversification in the types of services offered within the criminal underground. As the ecosystem evolved largely unchecked, many threat actors developed their skills and started specializing in more precise and narrow fields of expertise delivered at greater depth.

The same trend can historically be observed in other legitimate mature markets, as their maturity and success allow for profitable sub-markets to emerge – with specialization allowing participants to gain market share. For example, in the ransomware affiliate business, we see a further breakdown of operations into distinct roles, such as "negotiators," "business analysts," and "initial access acquisition specialists," among others. We have observed similar trends in other areas of the cybercriminal ecosystem.

The outlined main global trends affected Russian-speaking and other underground ecosystems. However, the Russian-speaking underground has also undergone its own unique developments, which the next section explores in detail.

Unique Traits of the Russian-speaking Underground

Through the years, the Russian-speaking underground community has been one of the main drivers and innovators of cybercrime. While many elements of cybercrime are common across languages, differences in societal evolution in Russia compared to the West has led to unique developments and approaches that are key to understanding modern cybercrime.

Beginning in the late 1980s, and continuing for decades since, the population of ex-USSR countries had to undergo societal and economic transformations that took centuries to unfold for western societies. The various nations saw large societal shifts in values, experienced varying degrees of information and economic freedom, endured a series of financial crises and hyperinflation, and witnessed the emergence of aggressive – sometimes fraudulent – advertisement campaigns on once-trusted state-controlled mass media, all while having to deal with widespread fraud.

Being forced to bypass or fast-track many of these stages led to societies adapting quickly and developing exceptional skills for handling challenging situations, critical thinking, and creativity in approaching different problems (in some cases, surpassing the average in other regions).

Societies faced major social challenges during these stages of development. For example, individuals with multiple university or even doctoral degrees were forced to work in lower-skilled but essential industries because this provided them higher income compared to working in scientific fields. Meanwhile, there were groups of people who capitalized on opportunities (sometimes bypassing or breaking ethical and legal barriers through various levels of corruption) to build significant capital in a much shorter period of time than seen in other societies. The emergence of substantial money flows and individuals who were able to enjoy lifestyle quality standards which were far above their official incomes made these people easy targets for traditional criminals – and later, cybercriminals.

During its early stages, the rules within the Russian-speaking underground ecosystem were underdeveloped, and it was seen as normal to target assets withing the same country. The lack of available payment methods and trans-border money transfers limited the ability of threat actors to scale their crimes abroad. This challenge was overcome with the rise of Bitcoin, which became a key enabler for monetizing cybercrime on a global scale rather than being confined to regional operations.

Over time, as law enforcement capabilities improved and matured, the cybercriminal underground evolved into the regulated, ethical (albeit still criminal) and rule-based ecosystem that we see today. Currently, the Russian-speaking underground is one of the most mature in the world, with its own traits, unique skills and mindset. We describe this in detail in the succeeding sections.

Unique Skills, Mindset, and Cultural-specific Attributes

Unique cultural aspects associated with Russian-speaking society have a large influence on the pathways of the criminals entering this ecosystem and how they conduct themselves once inside it.

By witnessing the inaccessibility of a luxury lifestyle that did not align with official salaries (at the time, and while it is possible now, a university degree is often needed for this), part of the younger generation developed high expectations about their future from a very young age. The educational system in many of the countries in the region was rooted in the USSR model, in the sense that it was focused on mathematics, engineering disciplines and problem-solving skills – using pen and paper approach combined with

out-of-the-box thinking rather than access to hi-tech equipment.

Currently, many Russian speaking countries provide individuals the opportunity to obtain high school and university degrees for free. This provides an opportunity to gain skills, build a strong foundational background, and develop a mindset that fosters creative problem-solving and situational skills, all of which are important in the criminal underground.

For high-school graduates in In Russian-speaking countries, there are several career paths. Those looking for a good salary can dedicate a few years to obtaining a higher education and a formal diploma. Alternatively, those with a solid technical background could acquire all the necessary skills and get a well-paying job right after high school by participating in the cybercrime community.

The underground has a low barrier of entry. Even before graduating from school, individuals often possess enough qualifications to conduct basic activities or secure simple jobs in the underground. By spending several years in this environment, threat actors can obtain the significant experience, practical knowledge, and skills to be an important part of the underground supply chains.

By their early 20s, many threat actors – if they are studying in parallel – may have spent several years in university or obtained enough skills to have an IT-related job and formal employment. Their salary is not so important in this case, since they have alternative options for earning. However, having a job or studying allows them to avoid attention from authorities.

Another important skill developed in these societies that were shaped by rapid and significant changes over a relatively short period of time is the ability to operate under stress. Growing up in high-stress environments provide individuals with the skills to handle stressful situations, valuable traits that cybercriminals need during their operations.

In a society where people are used to being cheated repeatedly, it is normal to be highly cautious about the appearance of new people. It is necessary to show that you already belong in the community by using the appropriate slang, sharing unique underground-specific knowledge, or even providing proof of past cybercriminal activities.

Without these aspects, and given their ingrained cultural cautiousness, threat actors have significant concerns about being infiltrated by law enforcement – both local and foreign. They are quick to react to individuals who lack awareness of local traditions, culture, and language. This is reflected in cultural-specific CAPCHAs which are particularly difficult to solve for those who did not grow up in the same society. However, once trust has been established, interactions become significantly more open and transparent.

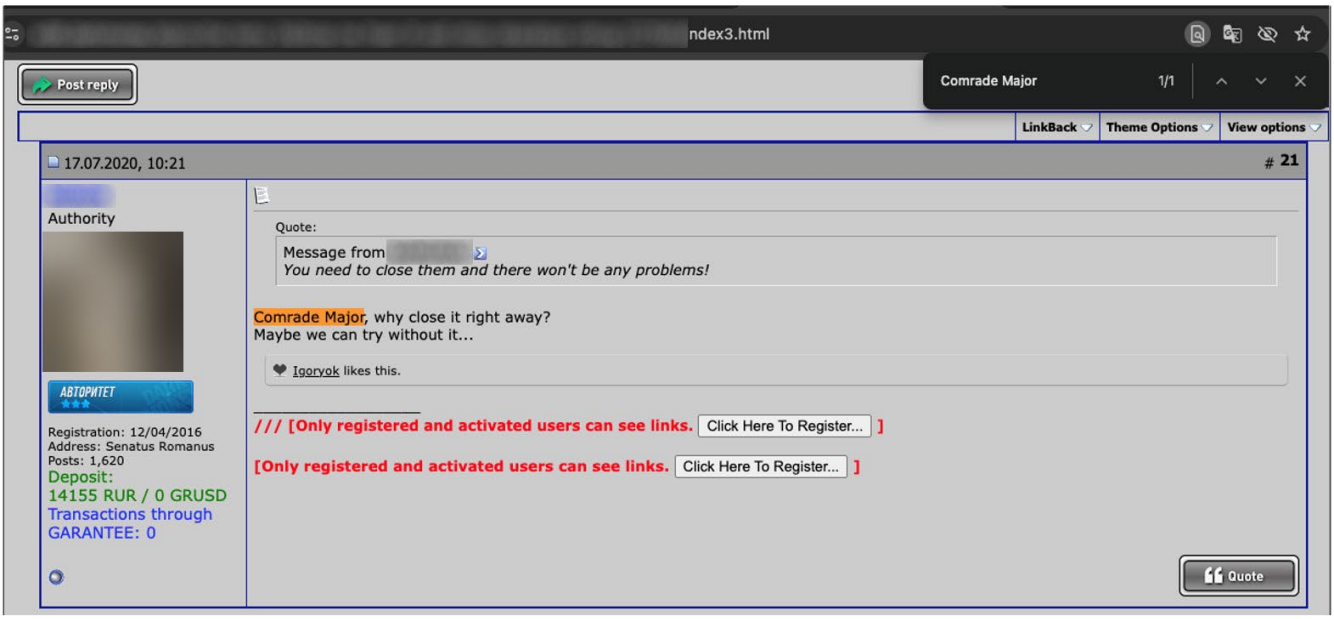


Figure 2. One forum user refers to another user as "Comrade Major", a tongue-in-cheek term of mock respect for someone assumed to be a part of law enforcement

The forum post shown in Figure 2 is based on the original actor posting comments that go against normal forum sentiments regarding the arrest of money mules. We also see this sort of behavior when individuals (who are suspected to be cybersecurity researchers) use unusual or overly formal writing styles that are out of place when compared to the typical slang used in the criminal community (in this case, the Darkmoney forum).

Such behavior reflects an "us vs them" mentality. In most of the Russian-speaking underground, there remains a polarized world view where it is seen as morally acceptable to defraud individuals from the "them" group, as opposed to the "us" group, which is seen as exploited and isolated. To integrate into the underground community, it is necessary that an individual is accepted as part of the "us" group. Recent geopolitical conflicts have only made this polarization stronger.

Control Mechanisms and Criminal Ethics

The Russian-speaking underground has very strict rules of engagement, which are ruthlessly enforced.

Nearly every platform, including shops, forums, and channels, enforce rules of engagement for their criminal users. The rules outline prohibited discussion topics – for instance, ransomware is currently banned on most forums. Another example is the restriction on certain geographical areas, such as the "don't work in RU" rule. Currently, however, the definition of this rule has become more ambiguous in today's modern reality. Furthermore, the use of duplicate accounts is commonly prohibited. This prevents actors from controlling several accounts with different nicknames that they can use to boost the reputation of their goods, tools and services.

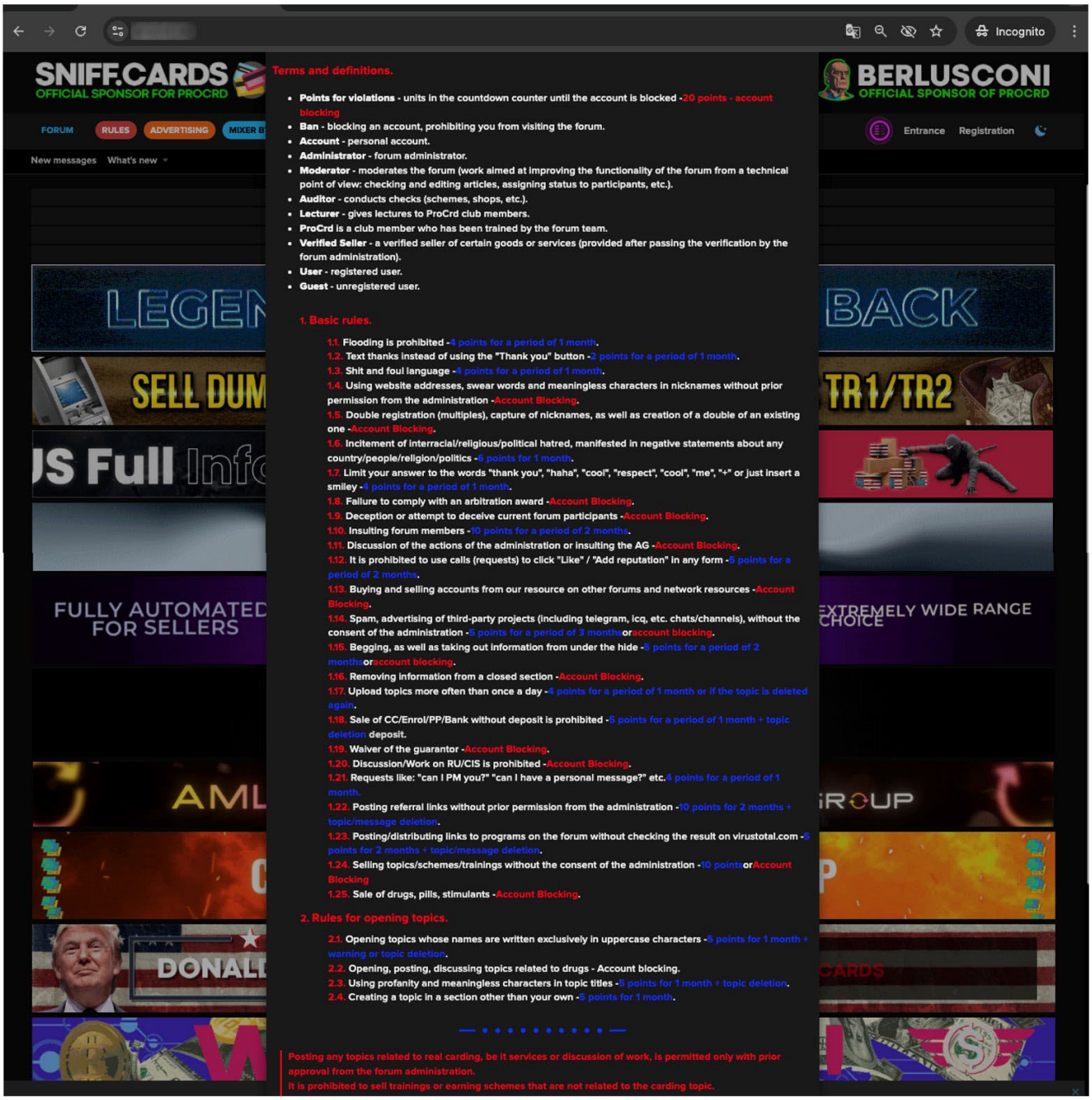


Figure 3. An example of the rules of engagement on the Procrd forum. Some rules are common across the cybercrime landscape, while others are community specific.

The rules often include control mechanisms to facilitate secure transactions between different parties in an environment rife with scams and where many actors pretend to be sellers of the same unique assets (when in fact, the true assets might be in the possession of only a few who care about their reputation). Meanwhile, others might attempt to perform social engineering and defraud the community via temporary accounts that mimic known reputable sellers from the same or other platforms, without concern for being banned.

In this toxic environment, mechanisms such as moderators, escrow services, and arbitration play a significant role in maintaining balance and upholding trust and reputations in an untrustworthy environment.

The Role and Impact of Reputation

Reputation is a key asset, with the whole criminal underground revolving around how much an individual has within the community.

In some sense, reputation functions similarly to army ranks, as actors often take the side of the individual with the higher standing in disputes, especially when factual arguments are insufficient in deciding a case. On the flip side, while reputation is hard to earn and easy to lose in real life, obtaining and keeping one's reputation is crucial for almost anyone participating in the cybercriminal underground, where the initial level of trust is nearly nonexistent and the level of concerns runs sky high. This is especially true for those who do not have the self-sufficiency to handle every part of their monetization business processes by themselves.

It can take months, or even years to build a reputation, but a single wrong decision, phrase, or deal can ruin it forever.

There are many ways to categorize the cybercriminal underground community, but by grouping members into forum/channel management and maintainers, sellers and service providers, buyers, watchers, strangers, and scammers, we can better illustrate how the value and importance of reputation vary across these groups.

For some of the groups, reputation is a necessity, for some it is beneficial but not essential, while some have no need for it whatsoever.

- For forum management (administrators, moderators, escrow services and arbitrators), it is crucial to maintain reputation and trust to keep the forum community alive.
- For sellers and service providers, reputation serves as a brand to promote and scale the monetization of their offers. As an additional measure to establish trust, financial deposits are often required by the forum or shop rules – either as a standard policy for all sellers, or as a risk mitigation measure for sellers who do not have enough reputation.
- For buyers, reputation is useful but not necessary, with the exception of specific scenarios. For example, the majority of simple, lower-cost or widely available goods, services, and tools can be purchased by actors without significant reputation. Corner cases can include the purchasing of unique services, manuals or assets, such as zero-day exploits. By selling unique assets to a reputable buyer, a seller enhances reputation. However, a valuable asset falling into the wrong hands can significantly damage its potential (for example, selling a unique and scalable fraud scheme against e-commerce companies to law enforcement or cybersecurity researchers). Buyers with low reputation can still prove their status in the community using the personal message interactions with known sellers to bypass this barrier.
- Watchers are the passive members of the community whose primarily role is to observe and satisfy their curiosity. They sometimes repost public news to increase their posts' counters, but do not actively participate in cybercriminal activities otherwise. This category often includes security researchers, law enforcement agencies, and journalists. In some cases, they must build their reputation to gain access to the hidden sections of the forums or to invite-only communities. Other examples where a boosted reputation is required involve access to restricted posts or partial content, contact information, or attached media content, which is only visible to accounts with 50+ posts on the forum.
- Strangers are like watchers, but visit the forum infrequently, engaging only in occasional activities. Reputation for these member is not a priority as long as they are able to accomplish their objectives. An example of this is a post from law enforcement notifying the community about the exposure of the identities of several actors. Normally, the account will immediately lose its reputation – however, the temporary objective is still accomplished.

- Scammers are an inevitable part of any criminal community, preying on other criminals who cannot complain to authorities without exposing their own questionable activities. Mature forums often have controls that help curb scamming activities, such as deposits or escrow services for transactions. Meanwhile less mature forums and messenger platforms are a "Wild West" for scammers, who frequently impersonate reputable sellers and service providers by replicating their posts and providing similar-looking contact details. The accounts used in such activities are only temporarily used, and losing reputation is merely considered as an expected consequence of the monetization business process.

Several factors can positively enhance member reputations and increase trust in their interactions with other representatives of the cyber-underground. These factors include: the age of the account, the quantity of posts, the number of successful deals, positive reviews and engagements, being vetted by a reputable person, and references to their reputation in other forums or communities. This latter is often why a newly registered user can almost immediately attain significant status and reputation.

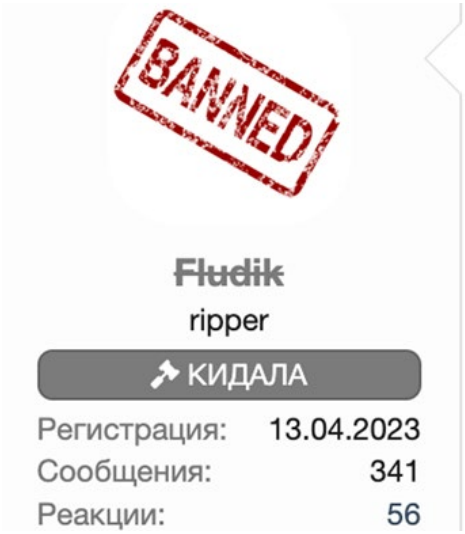


Figure 4. A "banned" tag appears instead of a personal avatar for this account due to reputation loss

At the same time, a post on a prohibited topic, providing a service or a deal with non-appropriate quality, creation of a duplicate account, PII leak related to account owner, and even rumors about connections with law enforcement agencies can disrupt reputation immediately.

Collaboration and Dominating Interests

With most cybercrime, money is the primary driving force. The key dominant interest is to maximize one's own financial flows by leveraging services provided by other community members. Collaboration in the Russian-speaking underground is a necessity to reach those goals.

Many services are structured around for-profit oriented activities, whether they are legal, existing in gray-areas, or outright illegal. To bypass the effects of this untrustworthy environment, where the real location and identities of the actors are unknown by default, mature platforms have evolved their own mechanisms based on reputation, rules and enforcement by the forum management and the community itself.

Forum interactions often emphasize respect for old-school, long-standing members, while simultaneously exploiting the naivete and immaturity of newcomers by exposing their incompetence. Successfully taking advantage of a newcomer's lack of knowledge at the right time and place is seen positively, increasing an actor's engagements and enhancing their reputation.

In most cases, collaboration is driven by pragmatism, with the primary goals being the acquisition and sharing of knowledge, deriving inspiration for new ideas, identifying potential targets, creating attacks scenarios and coming up with criminal business models.

Successful collaboration empowers criminal business processes, enhances monetization capabilities and improves the reputation of participating parties.

Due to the scale of the Russian-speaking underground and the significant time actors spend interacting with each other, collaboration is also fulfilling fundamental human psychological and self-fulfillment needs, which includes self-actualization, esteem, and belonging.[23]

While operating in high-stress environments, threat actors may seek an outlet to express their feelings, voice their concerns, and receive psychological support – which they are unable to obtain by openly admitting their crimes to normal doctors. To fulfill this niche, some forums have dedicated sections on psychological support. The appearance of such sections is an indicator of maturity, allowing the criminal members of the community to avail themselves of these services without exposing their identities.

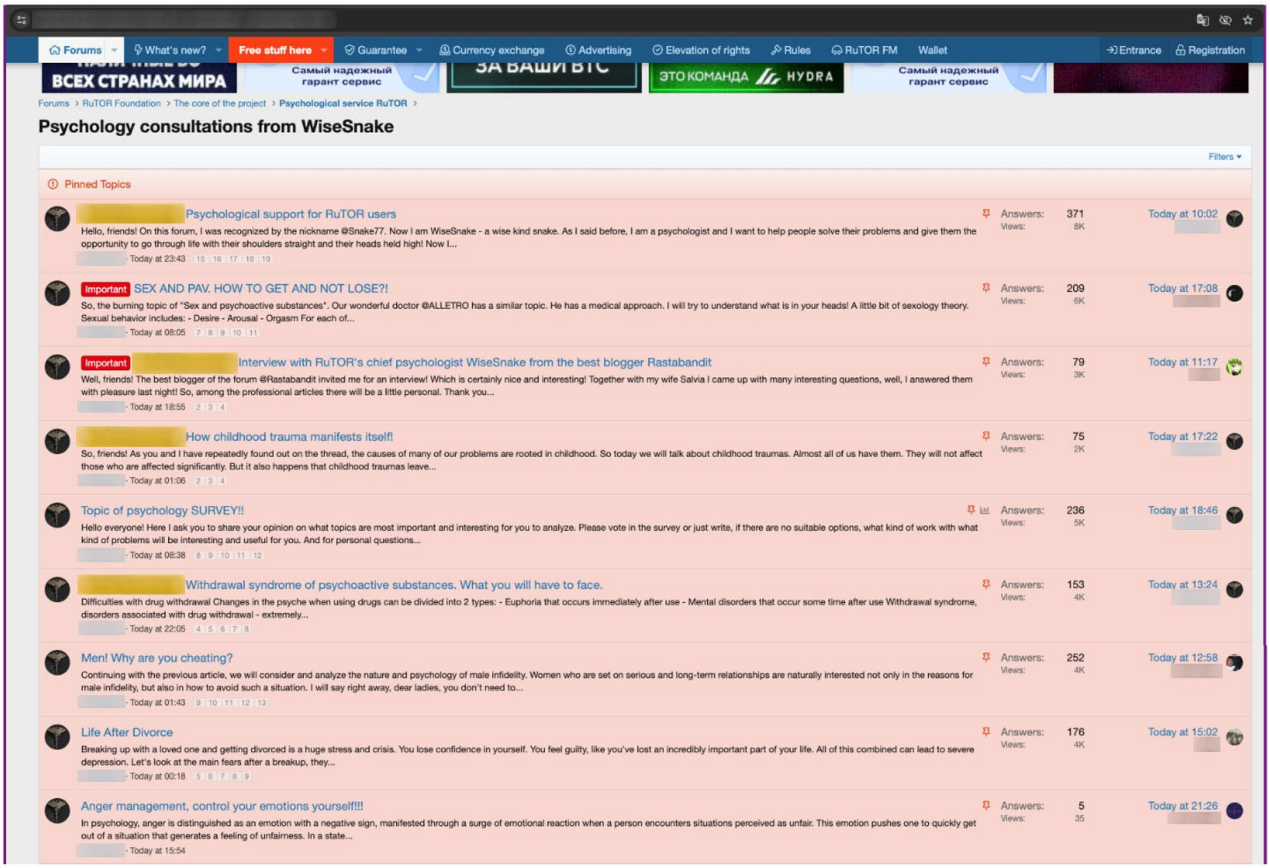


Figure 5. The psychological support section on the Rutor forum

Unique Position in the International Cybercrime Scene

The Russian-speaking underground is often regarded as the initial source of most innovations for financially motivated cybercrime. A variety of new attack techniques, scaling approaches and criminal business processes all have their roots there. Many of the attack scenarios we are witnessing now in the western world were first observed in the Russian-speaking underground years or even decades ago.

The Russian-speaking underground is comprised of a diverse mix of threat actors with different ranges of experience: teenagers, seasoned cybercriminals, organized groups that are managed as regular startups, and even experienced businesses with strict roles distribution and KPIs. Profit expectations also vary, with some actors willing to work for tens of dollars, while others expect payouts in the tens of thousands.

The market is highly competitive, offering very affordable prices for non-exclusive services. This includes exploitation and persistence tools, infrastructure and operational services. These innovations, together with the reasonable pricing that a mature competitive market naturally generates, attract increasingly greater attention from groups in other geographical locations.

It has become more common to see English language posts or messages clearly written by non-native speakers and translated into Russian, in what was traditionally Russian-speaking underground platforms. Individuals who identify as foreigners tend to be far more accepted than people who post their messages using machine translation. The linguistic artifacts in these posts suggest the presence of threat actors from different locations, such as Europe, the Americas, and China. These interactions strengthen the criminal capabilities in other countries and facilitate the scaling of cyberattacks into new regions – contributing to the globalization of cybercrime.

Pathways to Cybercrime in the Russian-speaking underground

For many aspiring criminals, cybercrime provides the right balance of quick financial gains combined with lower risks compared to traditional physical crimes.

Physical crimes leave numerous traces in the physical world. In contrast, Cyber-enabled crime (such as various scams) contain a digitalized component, while also requiring either physical interaction at certain parts of the chain or a physical presence at a particular location (e.g., for reshipping fraud).

On the other hand, cyber-dependent crimes feel safer than physical crime since all interactions can be conducted remotely using digital identities, shielding the real identity and the physical geolocation of the attacker. This makes the scaling of operation easier.

The path into cybercrime is often a tradeoff between the effort required to achieve the same financial expectations using legal means and/or the time it takes to accomplish this. Many legitimate jobs come with formal requirements, such as age, qualifications, and discipline. They can require years of investment before yielding a reasonable profit. These restrictions can be the reason why some talented teenagers turn to cybercrime.

People can also be deceived into participating in cybercrime or cyber-enabled crimes as underground actors also post their job advertisements on normal job search platforms. Software developers and money mules are often targeted using this method.

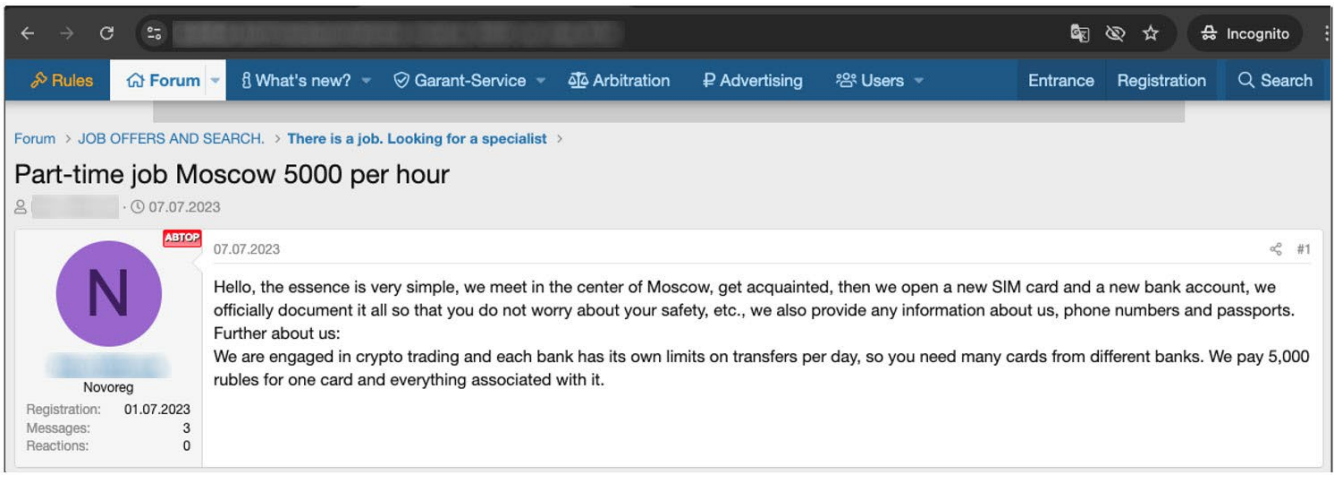


Figure 6. A money mule being hired for cryptocurrency withdrawal. The nature of the role is not fully explained applicants (Dublikat forum).

Many mature underground platforms feature dedicated options for job offers and job seekers.

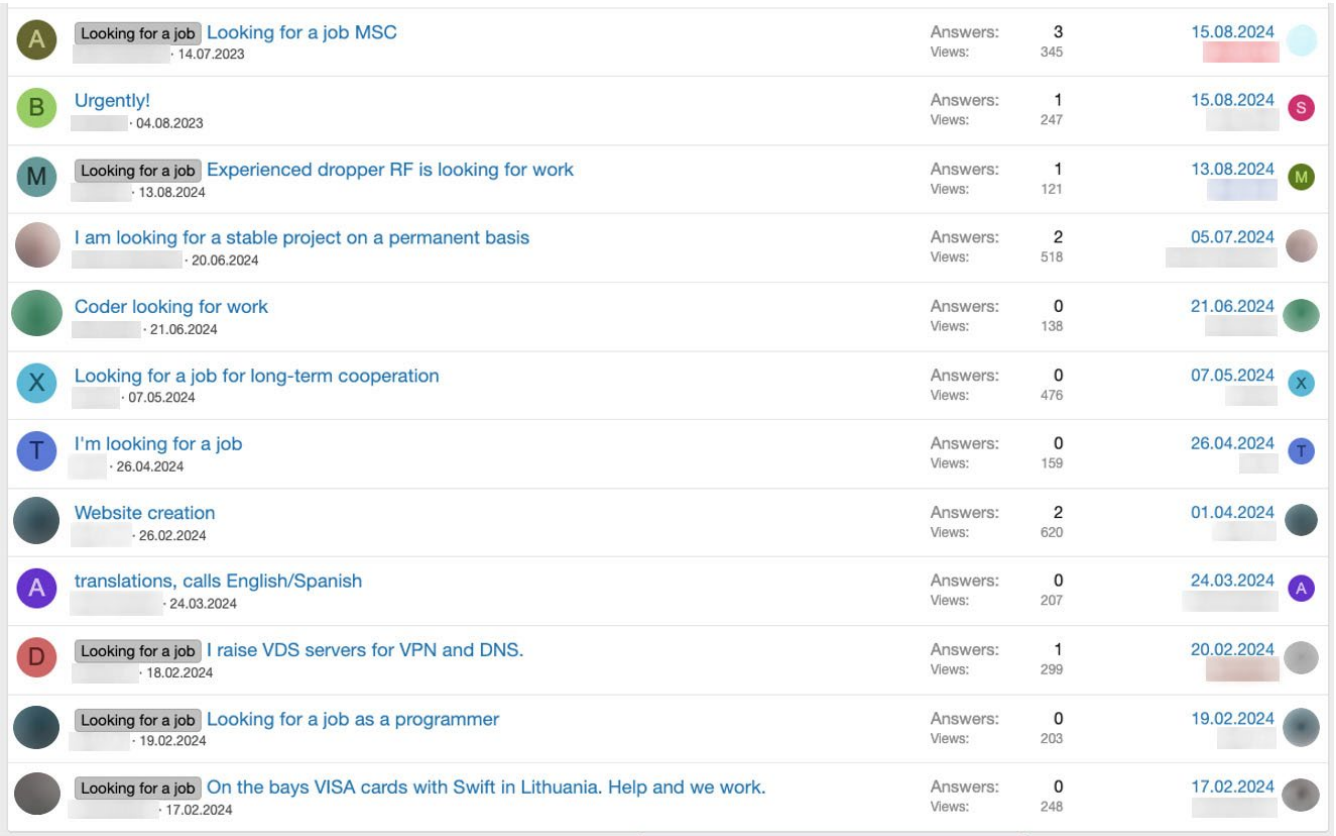


Figure 7. Examples of job requests (Rutor forum)

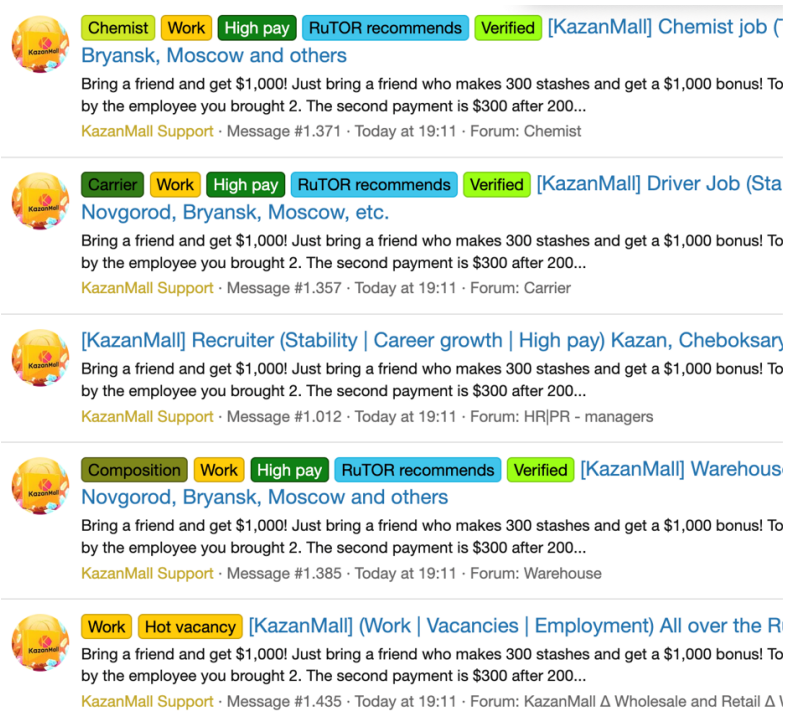


Figure 8. More examples of job requests (Rutor forum)

Job postings in the underground often indicate the level of risk involved using either specific phrasing or color-coded indicators as shorthand. For example, "green" and "white" means the job is generally safe and verified by the forum. Meanwhile, "gray" refers to questionable jobs with moderate amounts of risk, typically a minor crime or activities that can be interpreted as a crime depending on the details – but not serious enough to attract immediate attention from authorities. Finally, "Black" denotes high-risk roles that are clearly criminal in nature and will attract the attention of law enforcement. Other advertisements explicitly state the criminal nature of the job offer or contain specific key words, which serve as indicators.

Individuals can progress into cybercrime by climbing the ranks and moving up in criminal supply chains. For example, mules can advance to become scammers or even manage scam operations.

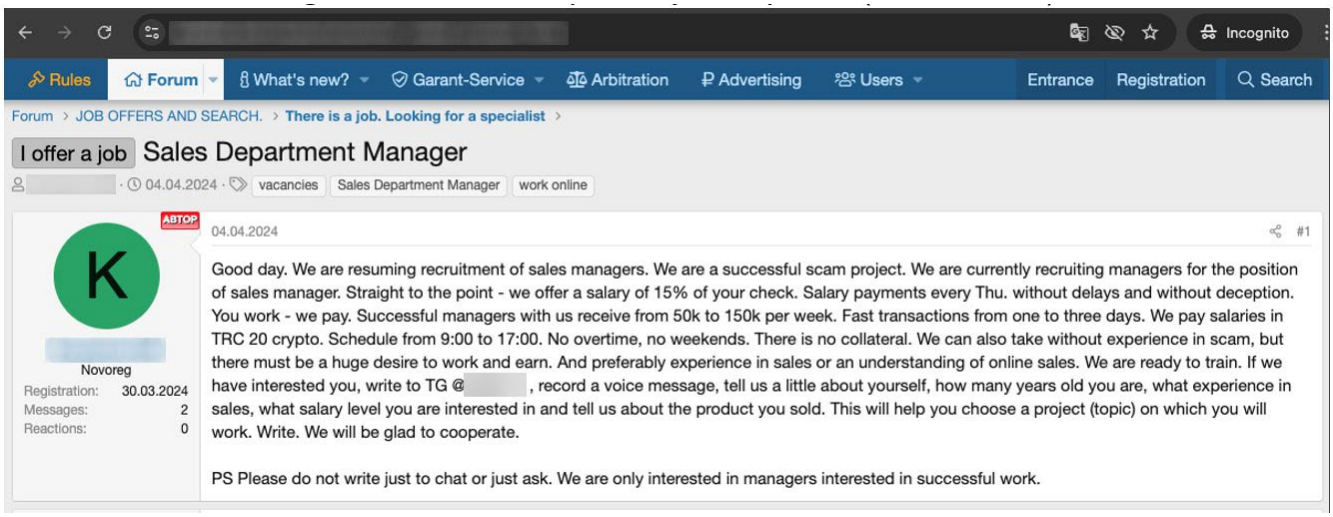


Figure 9. Job posting for a project manager position in a scam operation that outlines what the role entails (Dublikat forum)

Highlights from Key Criminal Business Processes

Most threat research focuses on tactical or operational aspects, emphasizing tactics, technique, and procedures (TTPs) and indicators of compromise (IoCs). In contrast, strategic research that offers a deeper dive into criminal business processes provides longer lasting knowledge compared to technical indicators alone.

This section highlights some of the major approaches underground threat actors are using to monetize their knowledge and bypass immature security controls.

Ransomware

Ransomware is a highly sensitive topic in Russian-speaking underground community groups. In fact, ransomware discussions are so sensitive that the topic is widely prohibited on most discussion platforms. Users even risk bans for mentioning it or posting related advertisements.

This was not always the case – ransomware discussions were much more common in the past. However, heightened scrutiny from international law enforcement due to ransomware has led to most communities steering clear of the topic to avoid unwanted attention. As a result, most of the ransomware-related discussions on these forums are swiftly shut down by moderators, as seen in the following screenshot:

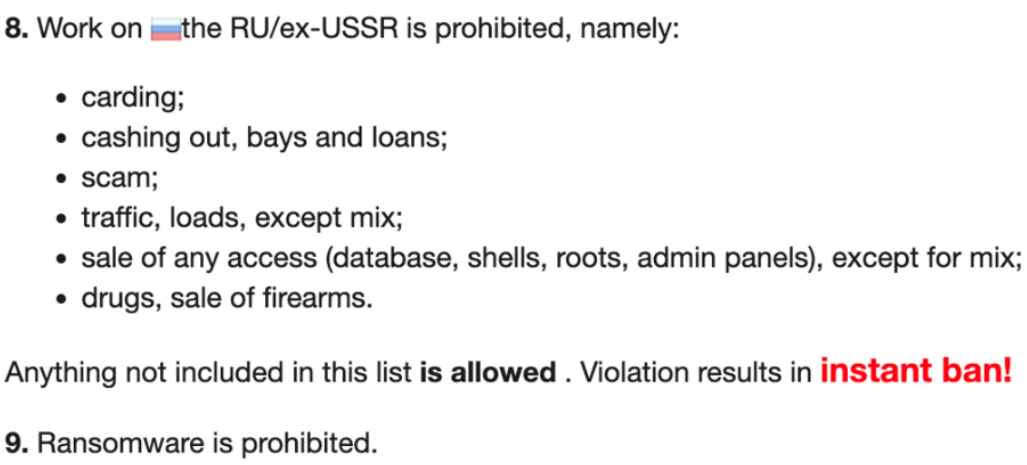


Figure 10. A section of forum rules explaining the restrictions on ransomware discussions

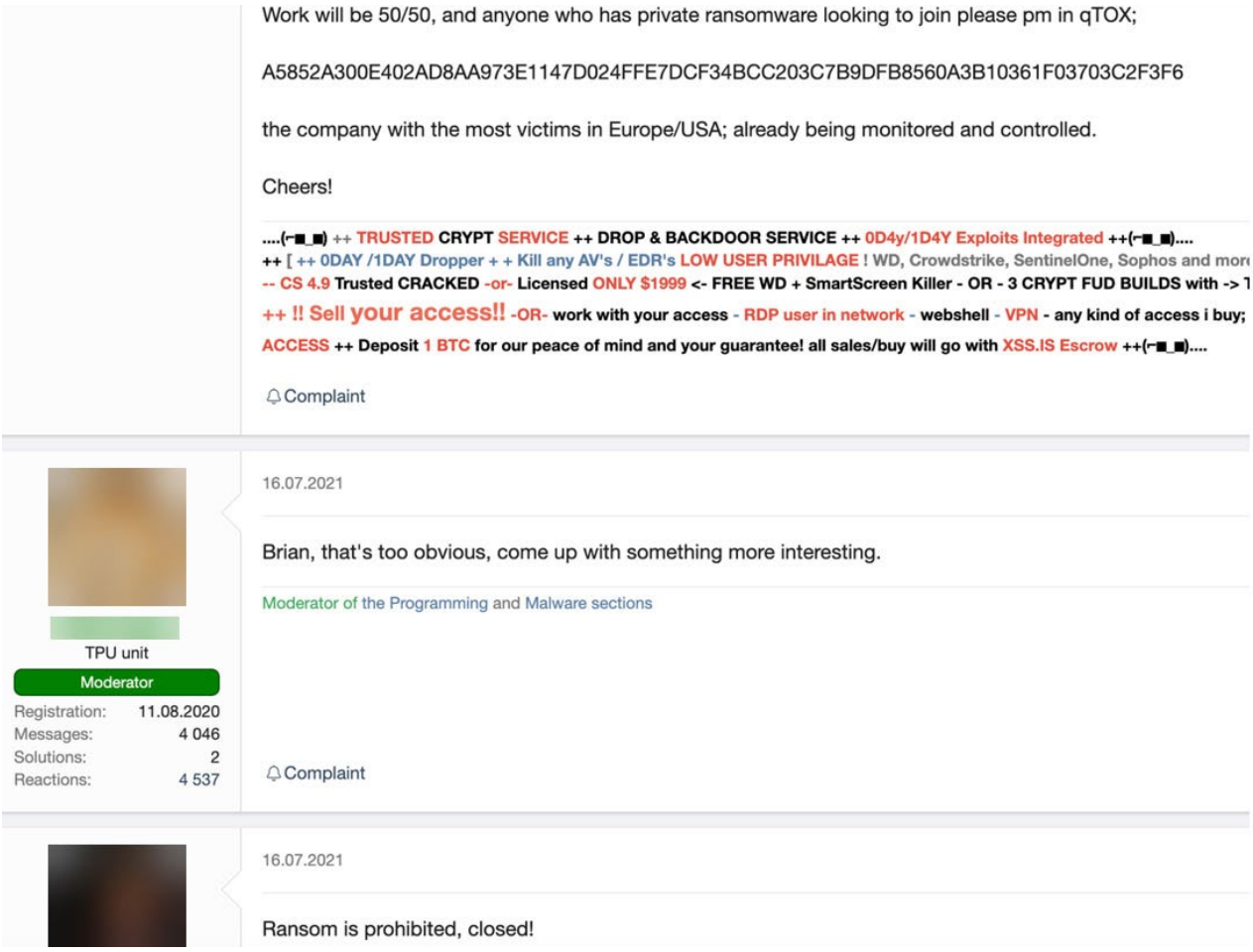


Figure 11. A thread closed by a moderator due to the discussion of ransomware

However, the number of recent source code leaks from some ransomware groups have created ample opportunities for newer threat actors to quickly develop new variants. Additionally, supporting parts of the ecosystem, such as Initial Access Brokers selling access to compromised organizations, are still readily available. In most cases, they avoid discussions of the final ransomware payloads.

It is also interesting to see how the ransomware ecosystem generally influenced the approach used by Russian-speaking cybercriminal operations. What began as plain extortion evolved into double-extortion, victim shaming, and purely destructive attacks where ransomware is used, not for financial gains, but to cause damage to businesses. At each point, the overall cybercrime ecosystem responded by supplying key supporting services, such as the need for strong bulletproof hosting to support leak sites.

Many of the ransomware groups operate as affiliate programs and rely on services from the underground ecosystem. For example, access broker listings are highly sought after by ransomware operators.

Due to the massive impact of ransomware attacks, the general sentiment in non-ransomware-related discussion groups is that these attacks are too bold, loud and attention-grabbing (even while generating a significant amount of money for the authors). As a result, many platforms enforce strict policies banning any business communication that could be linked to ransomware operations. However, this does not stop ransomware groups and members of affiliate programs to from purchasing services and goods on regular trading platforms, or even from hiring and covertly recruiting new team members.

Scams

A common-translated motto in the Russian-speaking scam business is "An easy mark is not a mammoth; they will never go extinct."

This is why the word "mammoth" and related visuals are widely popular among the Russian-speaking scammer community. In addition, many slang terms originated from this reference.

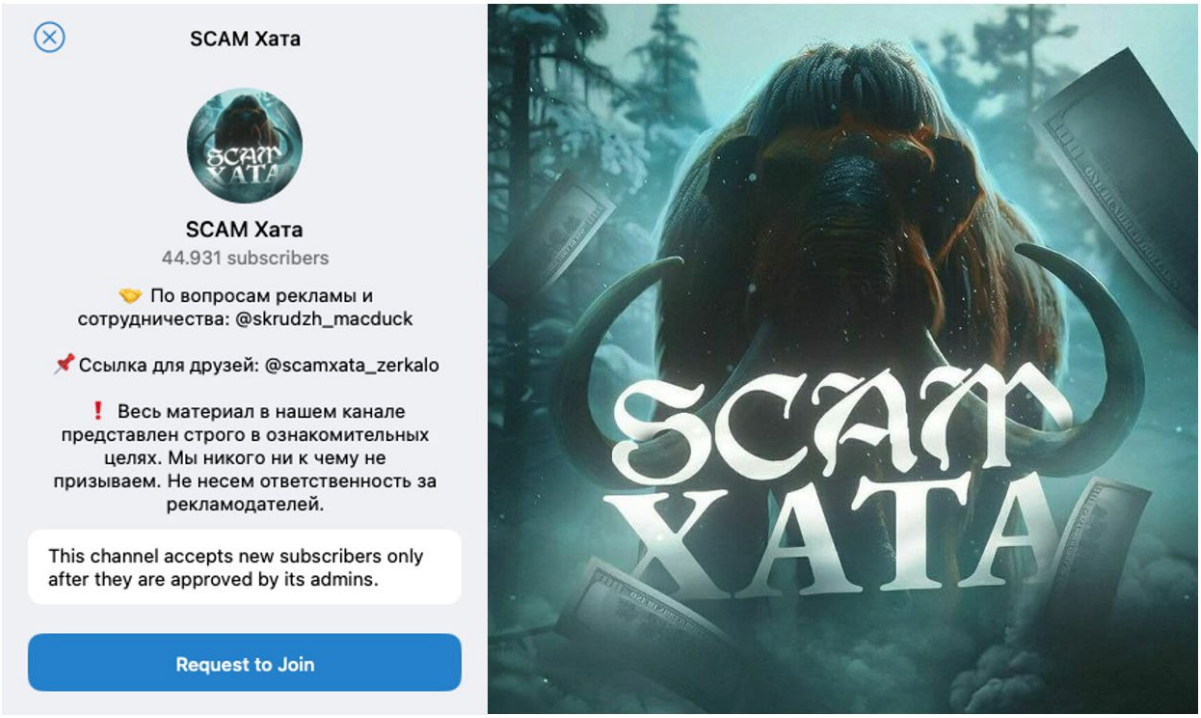


Figure 12. Scam-focused telegram channel. Note the Mammoth imagery.

Established scam groups operate with structured organizations that have defined roles and highly automated processes to conduct operations at scale. Telegram is a commonly used platform for organizing and running these operations, offering several useful tools to support these groups. Criminal business models in this area have a variety of roles, including:

- Business owners, who are responsible for top-down investments and resource distribution.
- Administrators, who oversee the creation and operation of telegram channels, bots, creation of accounts and technical support.
- Developers, who support and create scamming tools and implement automation.
- Financial operations groups, who manage the use of funds from stolen credit cards and accounts, and handle cash-out processes.
- Callers, who conduct social engineering and psychological operations, which includes calling technical support to unlock accounts and funds, and performing shipping fraud.
- Finally, there are ordinary workers who interact with the victims and force them to provide sensitive information, which can be leveraged for monetization.

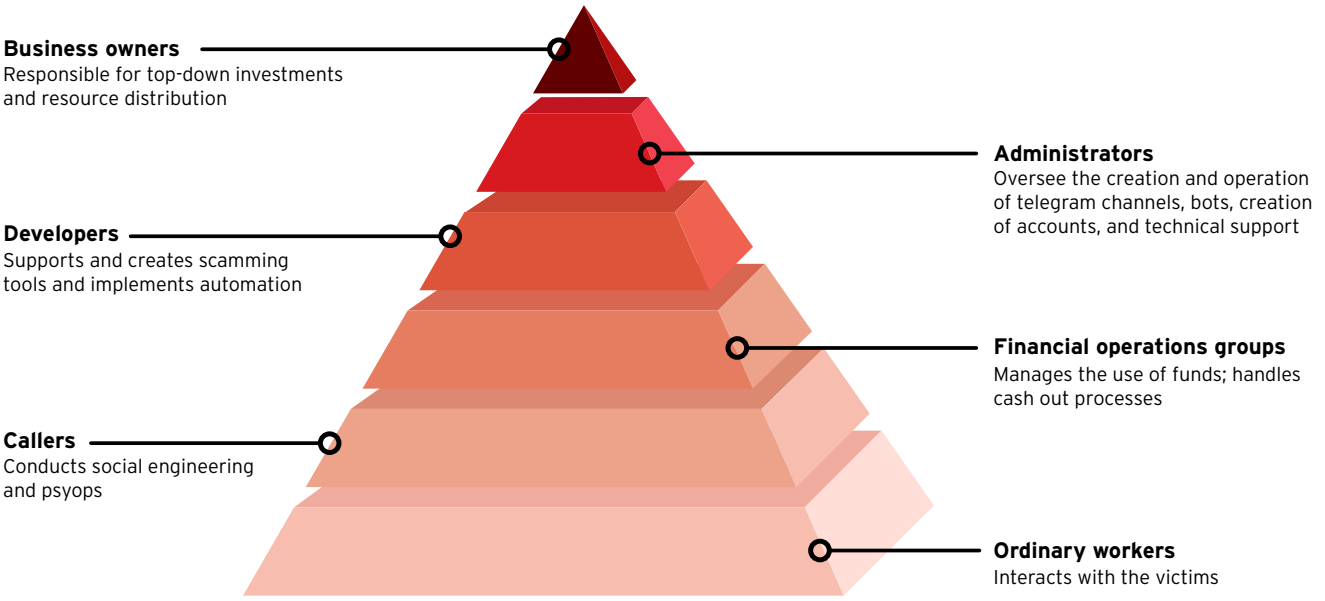


Figure 13. An example of a business hierarchy within a scam operation

Detailed descriptions of the technical workings of criminal business processes are typically tailored to the specific targeted platform whose users are being scammed and its geographical location. This is because the same targeted platform can have different languages, currencies, security and regulation policies, and cultural nuances – all of which need to be considered by criminals. Figure 14 shows an example of a list of available manuals, showcasing various targeted countries and platforms, along with guides on how to scam their users.

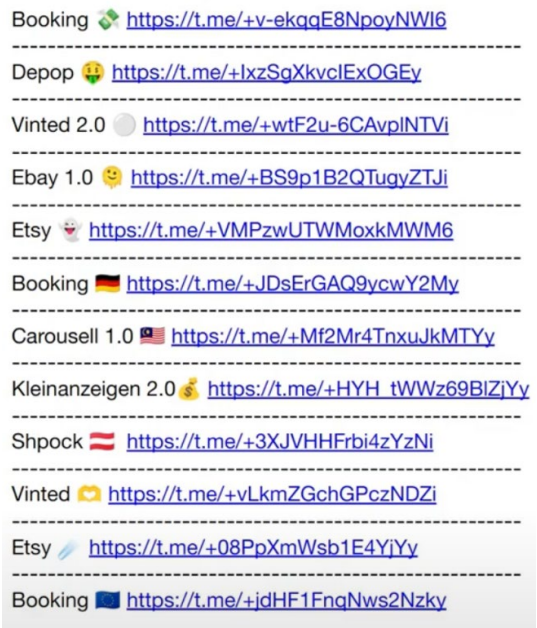


Figure 14. E-commerce fraud tutorials

(Source: the presentation "Scam as a Service Powered by Telegram" by Aurimas Rudinskis).[24]

For example, consider an advertisement for a manual targeting the *Kleinanzeigen* platform (a popular German classifieds portal). This guide details methods for using brute-force attacks to create and exploit accounts at scale, how to bypass 2FA, and more.

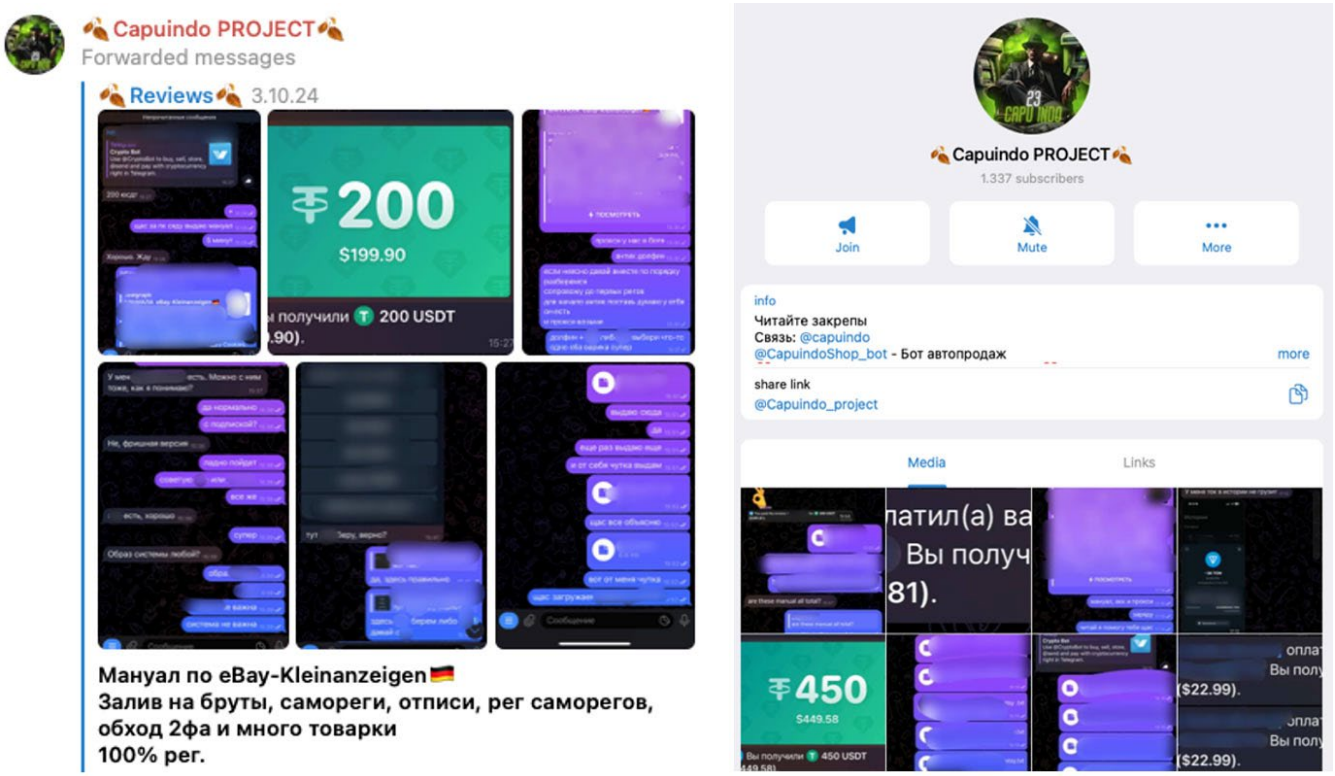


Figure 15. Kleinanzeigen monetization tutorial

Figure 15 shows a Kleinanzeigen tutorial on how to monetize this popular bulletin board for used goods in Germany, through brute forcing accounts (left), along with a corresponding Telegram channel (right).

Various specialized Telegram bots are utilized at different stages of common scams. For example, bots automate the sale of necessary accounts for the targeted services. Parser bots scrape content from legitimate targeted service marketplaces to mimic recent advertisement posts on those platforms. Furthermore, there are also services related to identity provision, which produces realistic-looking IDs tailored to match those from a targeted country.

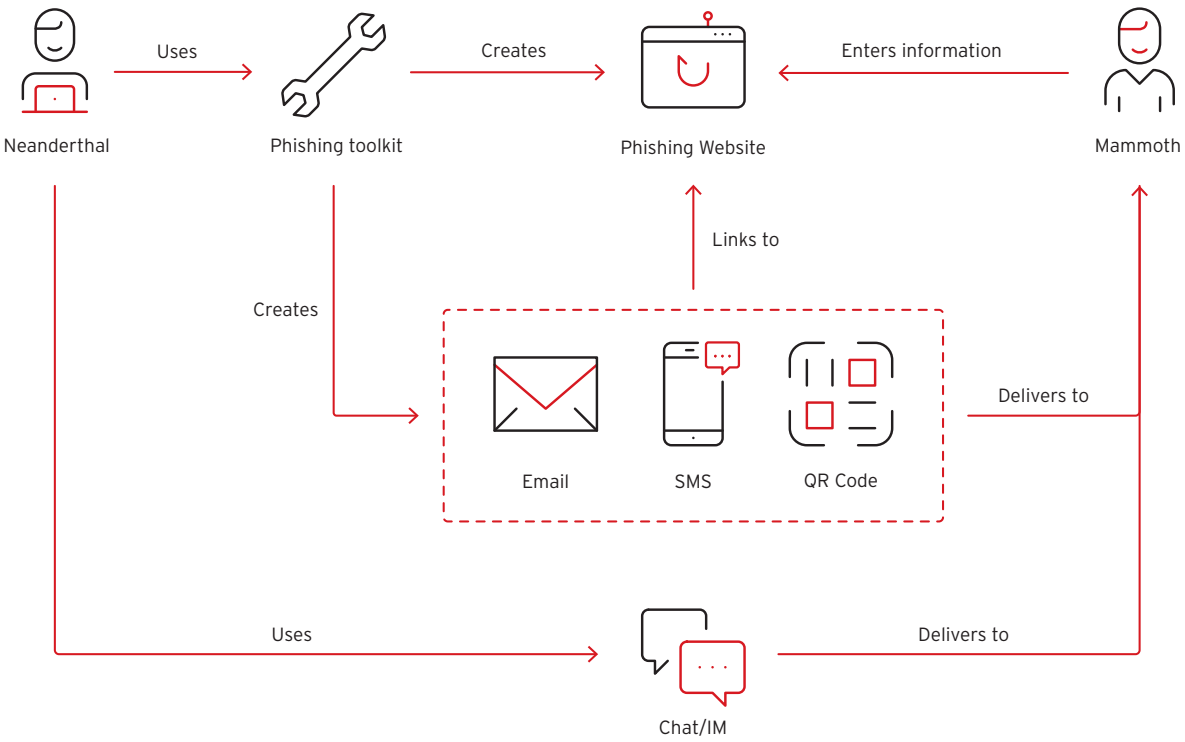


Figure 16. Example of a business process. "Neanderthal" is a term used by scammers to refer to themselves, originating from the idea of them being "Mammoth shepherds."

Most of the revenue from scam operation business models typically goes to the ordinary workers who interact with victims, earning them between 40% and 70% of the revenue. For other participants, including people responsible for financial operations, support, mentors, and callers, it is normal to see between 5% and 10% of the income.

Phishing

Phishing encompasses various specializations, depending on the type of information that needs to be collected. It can be used to target accounts on social media platforms, messaging apps, and public email services, as well as infiltrate corporations, governments, and e-commerce platforms. Additionally, phishing campaigns may be used to collect personal information, biometric data, credit card details, payment information, and a wide range of other sensitive data.

While other global underground communities focus on selling phishing kits, Russian-speaking communities are known for developing them. This has created a niche market with special employment opportunities for individuals skilled in cloning banking sites to support phishing kits.

As a result, phishing campaigns are often adapted to the targeted platforms or individuals. They can take the form of a mass campaign aimed at collecting as much information as possible from a wide range of victims, or more targeted in nature to extract sensitive information from a particular victim.

The Russian-speaking underground offers a number of services, tools, and in-depth guidelines on how to conduct phishing operations. In the following screenshot (Figure 17), the author posted a series of detailed guides covering various aspects of phishing, including the creation of phishing sites and dynamic phishing templates (Phishlets).

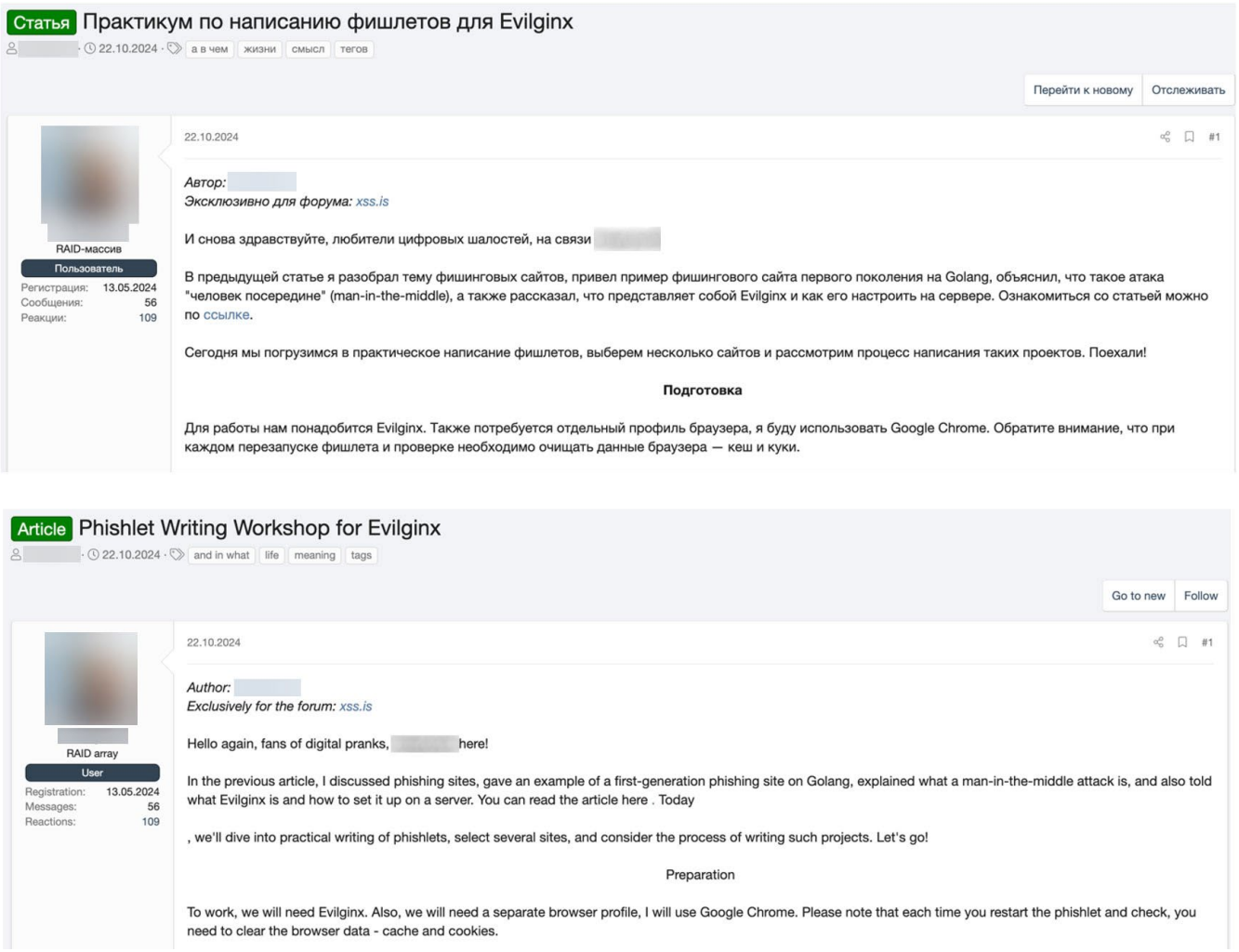


Figure 17. An example of phishing operation guides posted on the "XSS" forum (top) and the translated message (bottom)

Phishing operations can involve emails with custom templates, customized web sites that mimic targeted platforms, as well as channels and groups in social media and messenger platforms. They may also leverage voice calls and messenger services (via telecom or messenger platforms), or QR-codes to create visibility gaps in security systems.

The Russian-speaking underground provides all the necessary components required to conduct phishing campaigns, along with developer services for customized implementations tailored to specific needs and requirements. For example, the screenshot shown in Figure 18 features an advertisement on the "Procrd" forum offering website development and cloning services.

Figure 18. Website creation and cloning services that support phishing (Procrd forum)

Account Brute-forcing

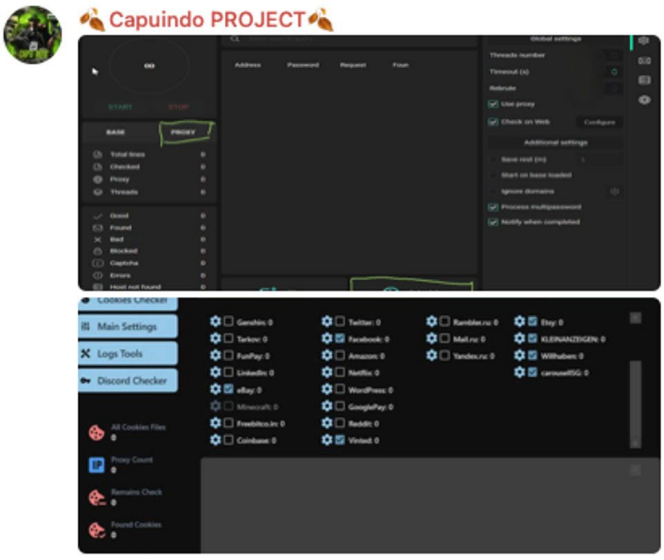
Account brute-forcing is a valuable part of several important underground supply chains. It feeds into the access-as-a-service,[25] proxy supply, hosting,[26] and abuse of marketing and advertisement campaigns while also influencing operational supply chains, depending on the type and locations of the accounts being targeted.[27]

For example, compromised SOHO routers and other IoT devices are often used as proxies, while access to assets in corporate environments can facilitate ransomware attacks, data exfiltration, phishing campaigns, spamming, business email compromise (BEC), and even industrial espionage operations. Meanwhile hijacked medial accounts can be exploited for phishing, influence operations, or even stock market manipulation.

The screenshot in Figure 19 is from a Telegram channel offering training on conducting brute-force operations, showcasing the interface of the tools used. Alongside educational resources, the package includes all the necessary tools and data.

"Cloud of logs" is a popular underground service that provides daily, weekly, or monthly paid access to the data harvested by numerous infostealers. The data is typically stored on cloud storage platforms and allows attackers to sift through unsorted

information in search of valuable credentials, authenticated cookies, and other sensitive information. The package shown in Figure 19 also includes access to a "cloud of logs" platform as an extended offering.[28]



Web3 Asset Monetization

Web3 technologies, such as NFTs, the metaverse, blockchain platforms (Ethereum, Solana, Polkadot, etc.), decentralized finance (DeFi), and decentralized autonomous organizations (DAOs), have gained considerable popularity in recent years. Web3 funding has reached $9.043 billion, though performance varies across different sectors.[29]

Due to the unique combination of high value assets that are often controlled by people who lack an understanding of security risks and the technical complexities of the ecosystem,[30] Web 3 has become a prime target for criminals.[31]

A screenshot from the XSS forum (Figure 20) highlights the scale of these operations, with a single team claiming to have earned US$300,000 in October 2023 alone. Additionally, the actor behind the post mentions having just six months of experience. It also references the platforms (Twitter, Discord, TikTok, Instagram, and Threads) used to carry out the operations, along with information related to the number competitor teams in the market.

The caption itself reflects the slang associated with these types of scams, where "hairy ones" refer to the victims ("mammoths").

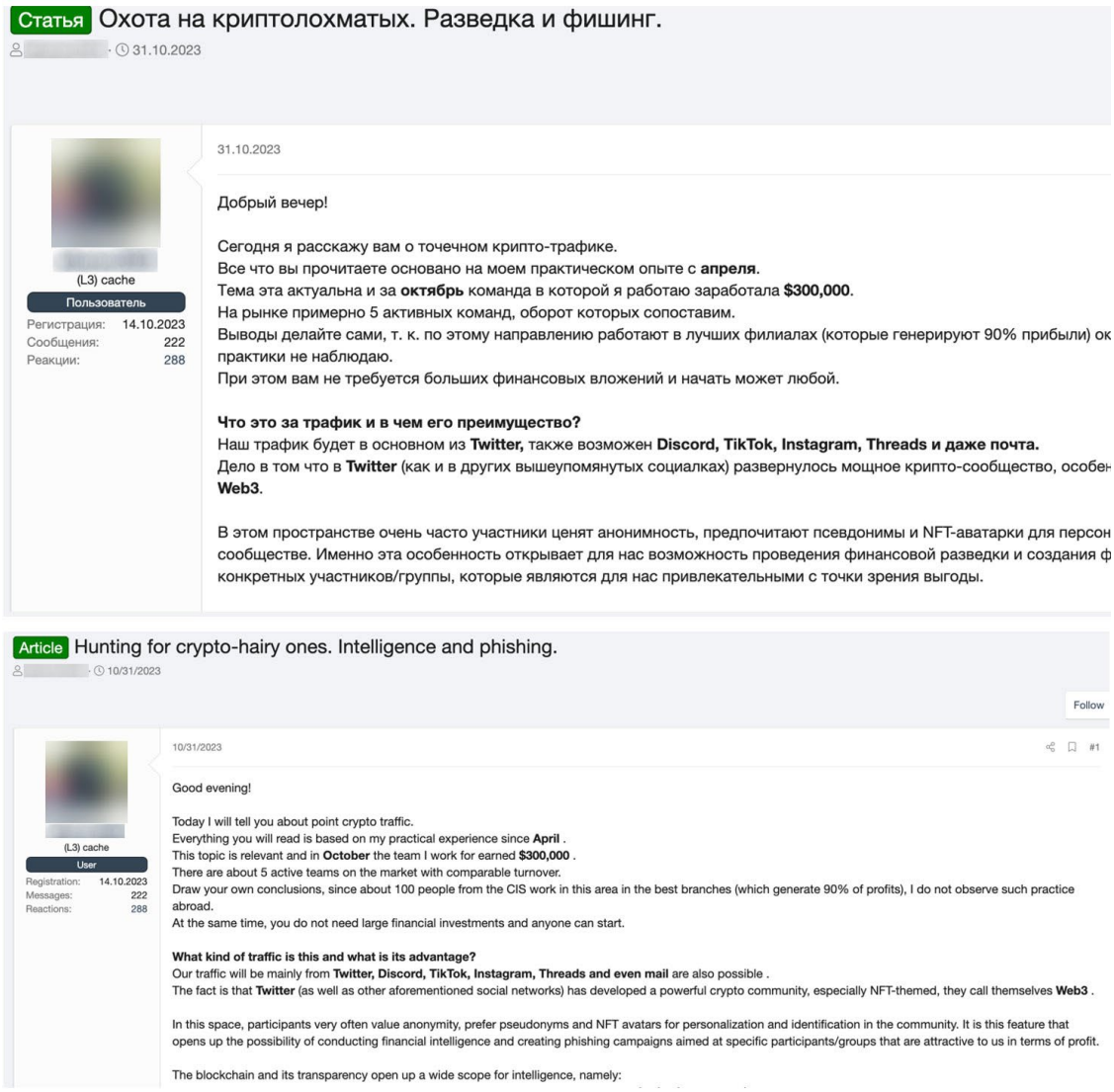


Figure 20. Web3 asset monetization manual (XSS forum)

One such scam process operates as follows:

- The attackers first gains possession of accounts on Twitter (X), Discord and/or other social media platforms that are neither too old, nor too new – typically 1-3 years old with prior relevant activity. The attackers prioritize verified accounts to increase trust levels.
- Since Discord is widely used within the Web3 community, a Discord account is necessary for interactions with the victim.
- The attackers use compromised corporate mail accounts to enhance trust.
- The goal of the attackers is to create a credible-looking online presence, using verified accounts with a large number of relevant followers and activities. To achieve this, the attackers use automation with the accounts to generate a high volume of relevant posts, comments, and engagements with real influencers. Some influencers may blindly follow back, significantly boosting the trust levels of the attacker-owned accounts in the process.

- The attackers use a combination of automation software, bots, and third-party services alongside manual efforts to efficiently scale their operations.
- Once the infrastructure is in place and ready to operate, the attackers identify a target via the *Drops, Tops* and *Trending* sections on the OpenSea Website.[32]
- The attackers then collect information on Web3 asset owners (e.g., NFT holders), including their interests, contacts, and habits using Open-Source Intelligence (OSINT) techniques.
- The attackers use social engineering techniques to impersonate the original project (e.g., announcing and promoting an online event), which redirects visitors to sites designed to trick them into downloading software that will drain their Web3 assets.

Intelligence Gathering and Privacy-related Services

There are several use cases for cybercrime actors to conduct intelligence gathering and deanonymization. Threat actors not only gather additional data on assets and potential targets, but they can also themselves be victims of other underground criminals or individuals impersonating them. As a result, some actors seek intelligence to understand their adversaries.

The Russian-speaking underground offers a very high level of privacy and intelligence gathering services, often limited only by the buyer's budget and a few operational red lines. These red lines typically involve cases in which providing such data can attract a significant amount of law enforcement attention due to geopolitical implications – for example, when journalists or investigators attempt to leverage underground services.[33] The risk of retaliation from a target with the capability to fight back is another consideration (which can involve revenge on both the original target and the service they used for the attack).

The ability to provide such advanced services relies on deep technical knowledge of the technologies, methods, and places needed to collect such information, along with access to critical parts of the human intelligence (HUMINT) gathering infrastructure (that is, intelligence coming from human sources) – for example, access to city surveillance systems or leaked government and commercial databases (which includes pivotable PII). By combining these data sources, attackers can offer underground services such as mapping phone numbers to the name on a government issued IDs.

Technical capabilities are not the only basis for obtaining such intelligence gathering services. It also relies on the threat actor's ability to find insiders within government, telecom, and financial institutions who often play critical roles in such services. Figure 21 shows an example of a job posting for government, financial institution, and telecom insiders published on the *Dublikat* forum.

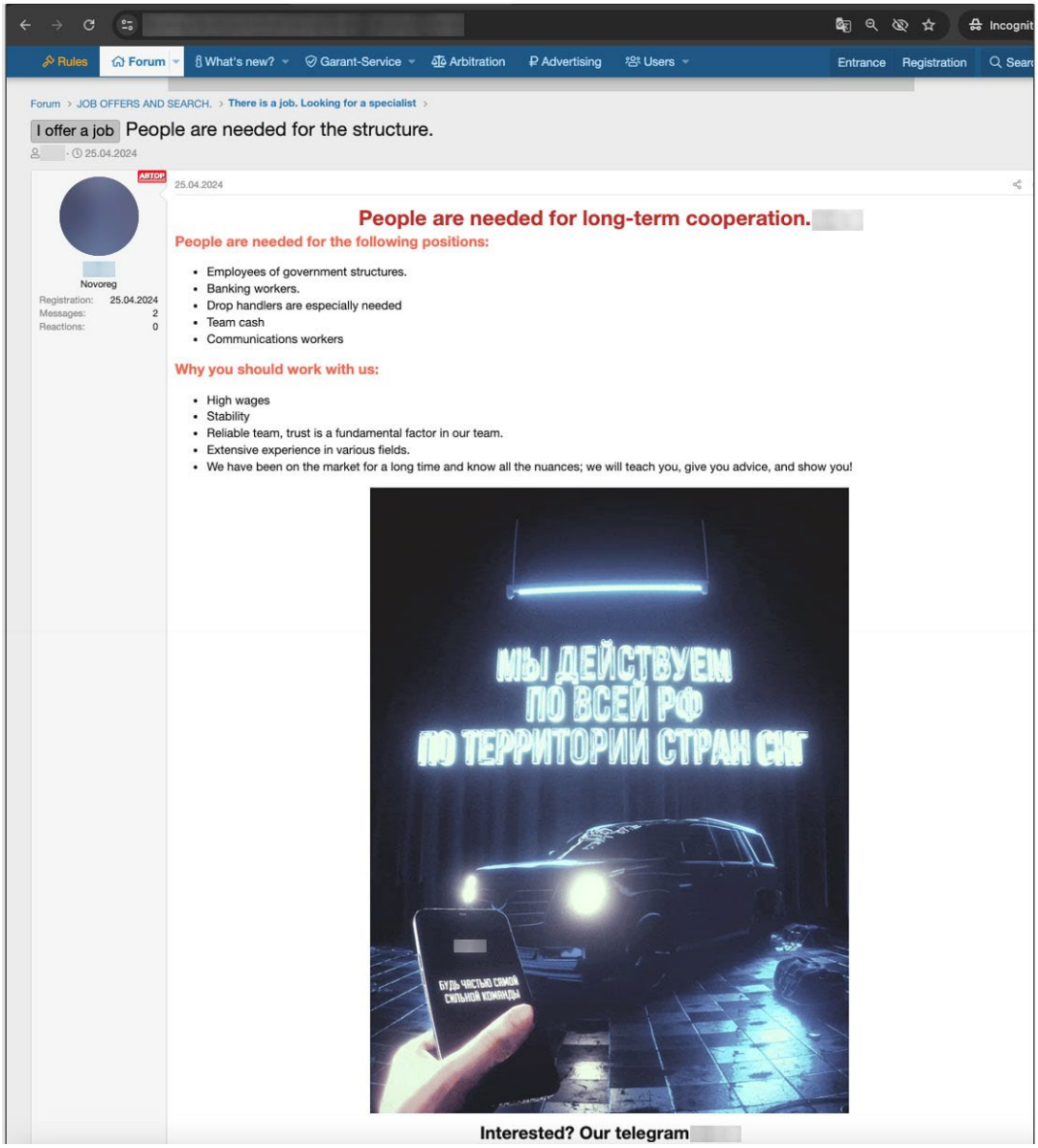


Figure 21. An insider job posting published on the "Dublikat" forum

The services offered can include verification of information in law enforcement databases, tracking recent flight and travel details, accessing banking statements, confirming the presence of residence permits and assets in a particular country or region, and providing other sensitive information.

Figure 22. An example of a HUMINT service offering that claims to have access to information from government institutions. The starting price for these services start at US$500 (XSS forum).

In regions with highly advanced surveillance systems, it is not surprising to see services offering HUMINT capabilities based on biometric data and image recognition.

The advertisement in Figure 23 showcases the ability to map a face to a real identity or track the location of an individual using cameras in Moscow and St. Petersburg. A simple photo or a full name with a date of birth can serve as a starting pivot point.

The prices for such services typically range between US$100 and US$1,000, although special requests are priced on a case-by-case basis.

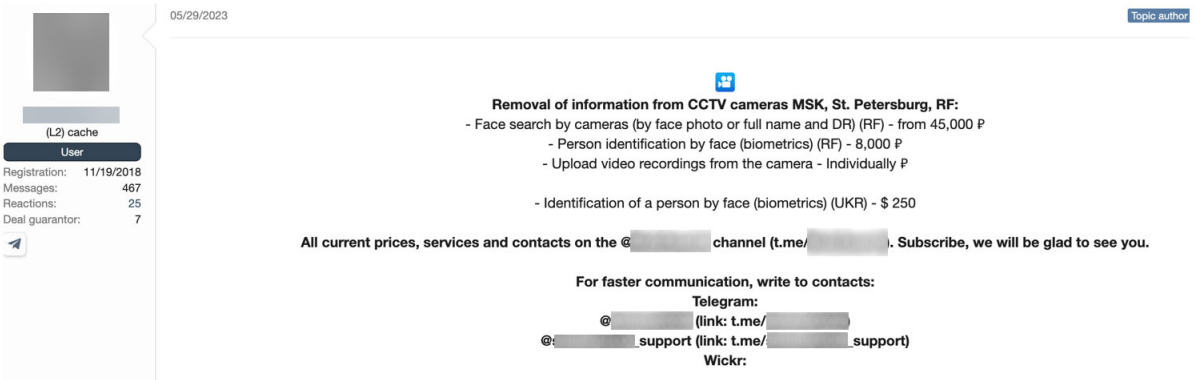


Figure 23. An example of a biometric-based HUMINT service in the underground

Modern telecoms possess extensive visibility and HUMINT capabilities, making telecom-based services an integral part of underground intelligence operations.

Offers in the underground often include mapping real identities and phone numbers, interaction details (including calls and SMS), the tracking of their approximate locations over time, and determining their current location (often called "Flash"). The prices for such services normally range between US$100 and US$1,000, with the ability to identify personal details on targets acting as a baseline for various other criminal business models, including extortion and impersonation.

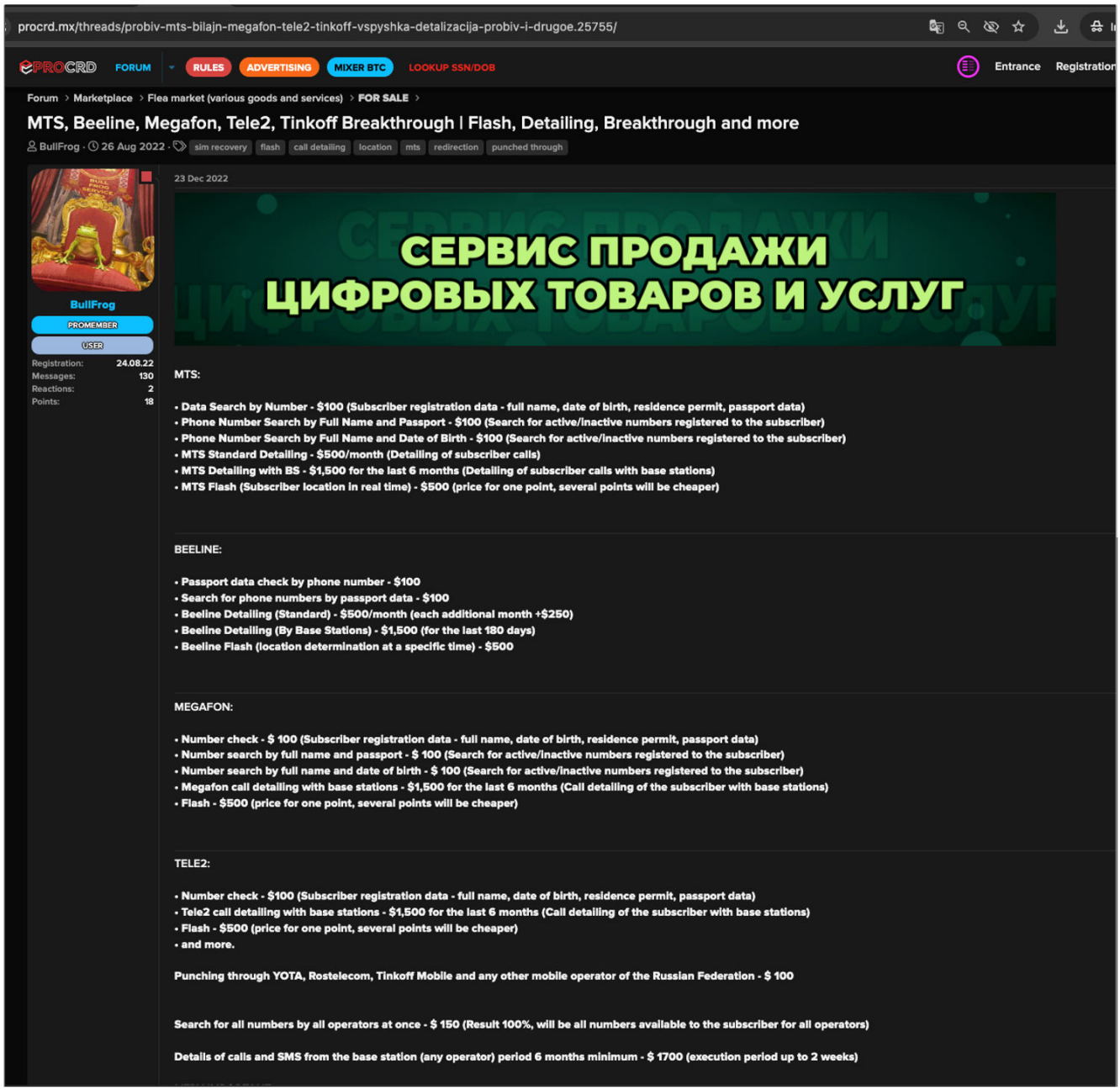


Figure 24. An example of a telecom-based intelligence gathering service being offered in the underground (Procrd forum)

Synergy of Cyber and Physical Domains

Guns, drugs, and other prohibited substances are well-known commodities that are sold within the underground ecosystem. There is a growing synergy between physical and cybercrime groups, as physical crime groups increasingly recognize the value of high-tech crime to scale and enhance their operations.

The screenshot in Figure 25, which shows an individual promoting a "violence-as-a-service" operation is seeking to hire a PHP backend developer, is an example of this synergy.

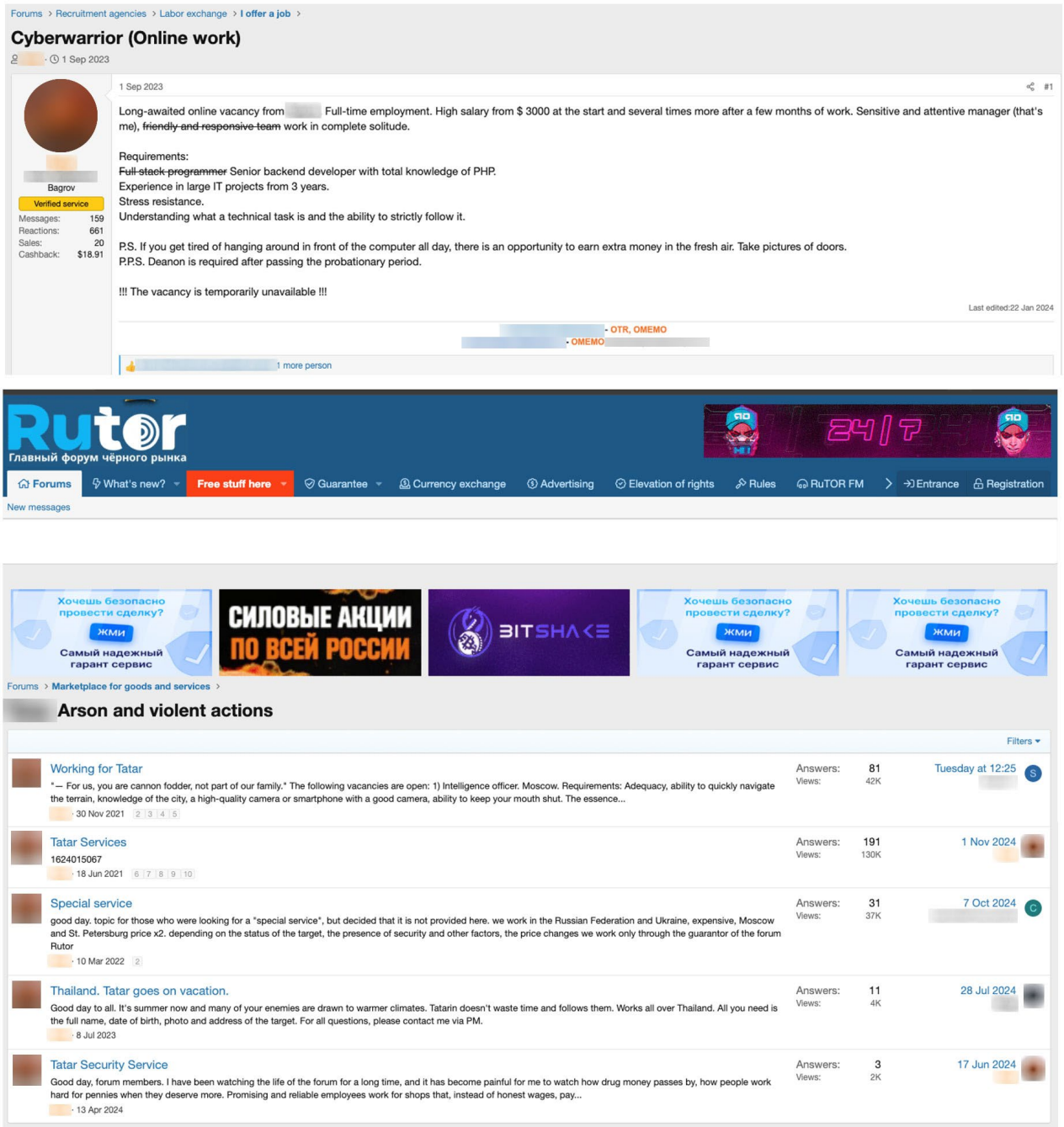


Figure 25. Job offerings for a senior backend developer posted by an actor (top) who also provides physical violence services (bottom)

Violence as Crime Services

One trend that we have observed within the Russian-speaking underground over the past few years is the rise of demand and offers for violence-as-a-service activities.

The likely reasons for the increased supply and demand for such services include geopolitical unrest, economic instability, and increased national state-aligned interest in this field. These services often incorporate OSINT and HUMINT services as a part of their operations.

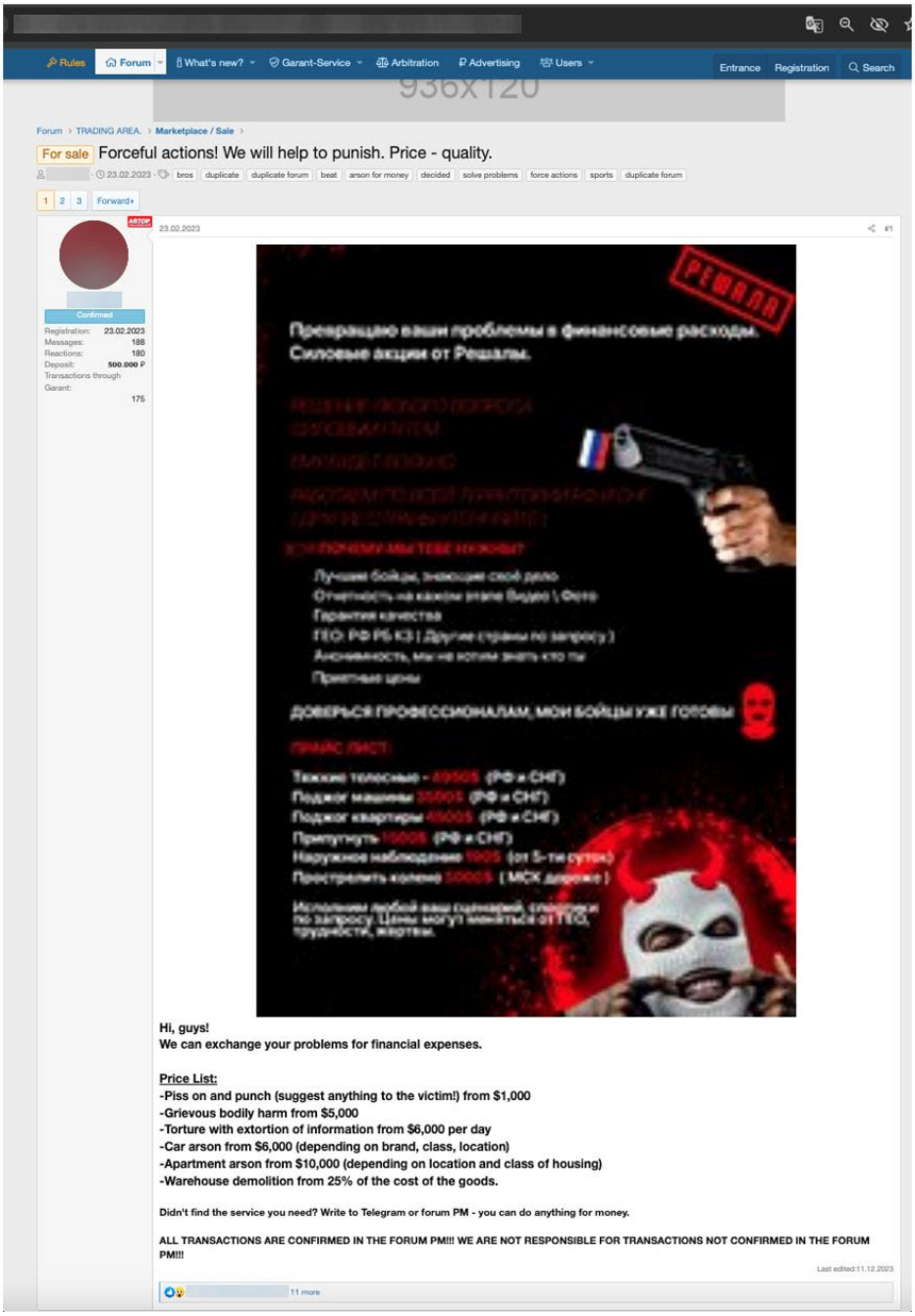


Figure 26. Physical violence-as-a-service offering (Dublikat forum)

The prices for physical violence actions often start at several thousand US dollars and can range up to tens of thousands.

Alongside physical actions, we have observed offers focused on using psychological pressure on the victim, including harassing calls, SIM card blocking, and other similar tactics. The screenshot in Figure 27 shows that the topic has accumulated 10,000 views and six pages of discussions.

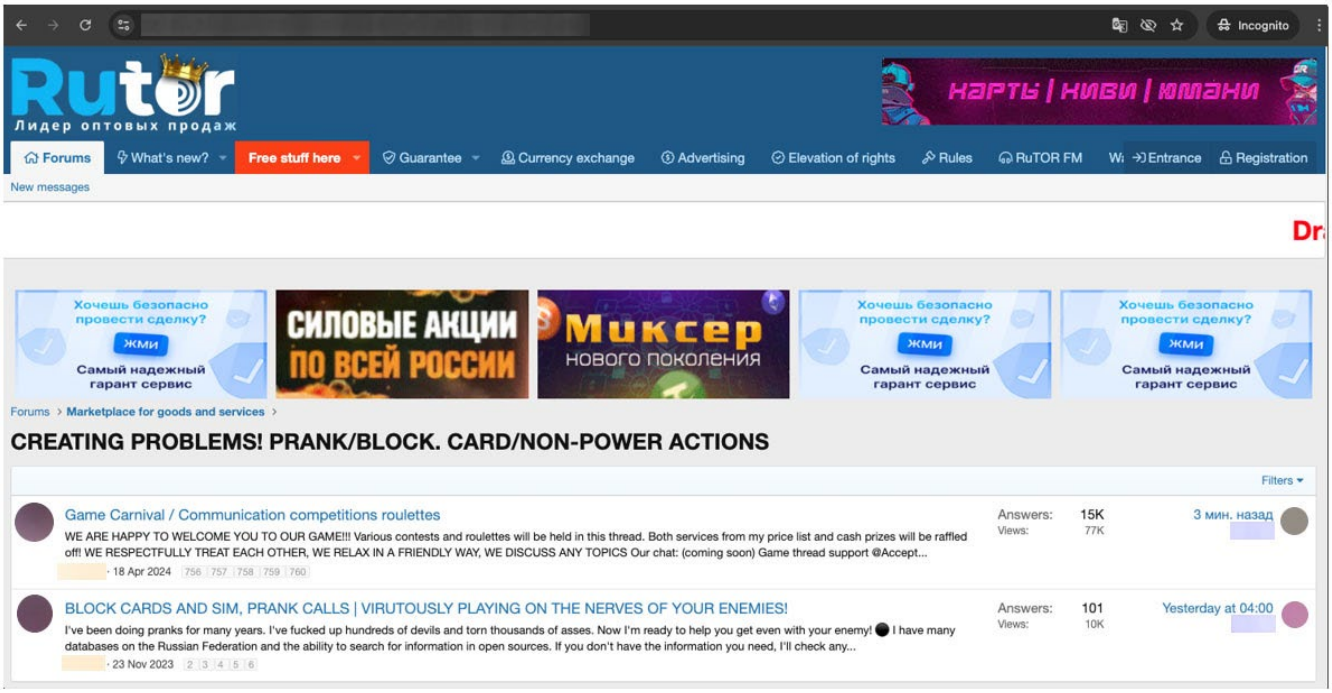


Figure 27. "Nonviolent" psychological operations (psyops) services being offered in the underground (Rutor forum)

Car-related Underground Activities

Several factors drive the growing interest in cars among the cybercriminal community.

For example, disruptions in supply chains, particularly due to sanctions in Russia, have limited even dealer access to vendor-supplied diagnostic tools and software. In addition, some car owners have a high demand for tuning, feature enablement, and car diagnostics, but find that official routes to achieve these are limited. This creates a gap that criminals and underground services can fill.

The second factor that can potentially drive car-related underground activities further is the demand for spare parts that official suppliers cannot fulfill. As a result, cars may be stolen and dismantled to meet spare part demands.

Yet another reason for the growth in car crime services is the increasing connectivity of nearly every modern vehicle, which opens up significant possibilities for new monetization schemes. The ability to remotely control cars, including opening doors and tracking car locations, can enhance other criminal activities such as intelligence gathering and mule services. The following screenshot (Figure 28), which is taken from the *Rutor* forum, illustrates activity within just one car-related subsection.

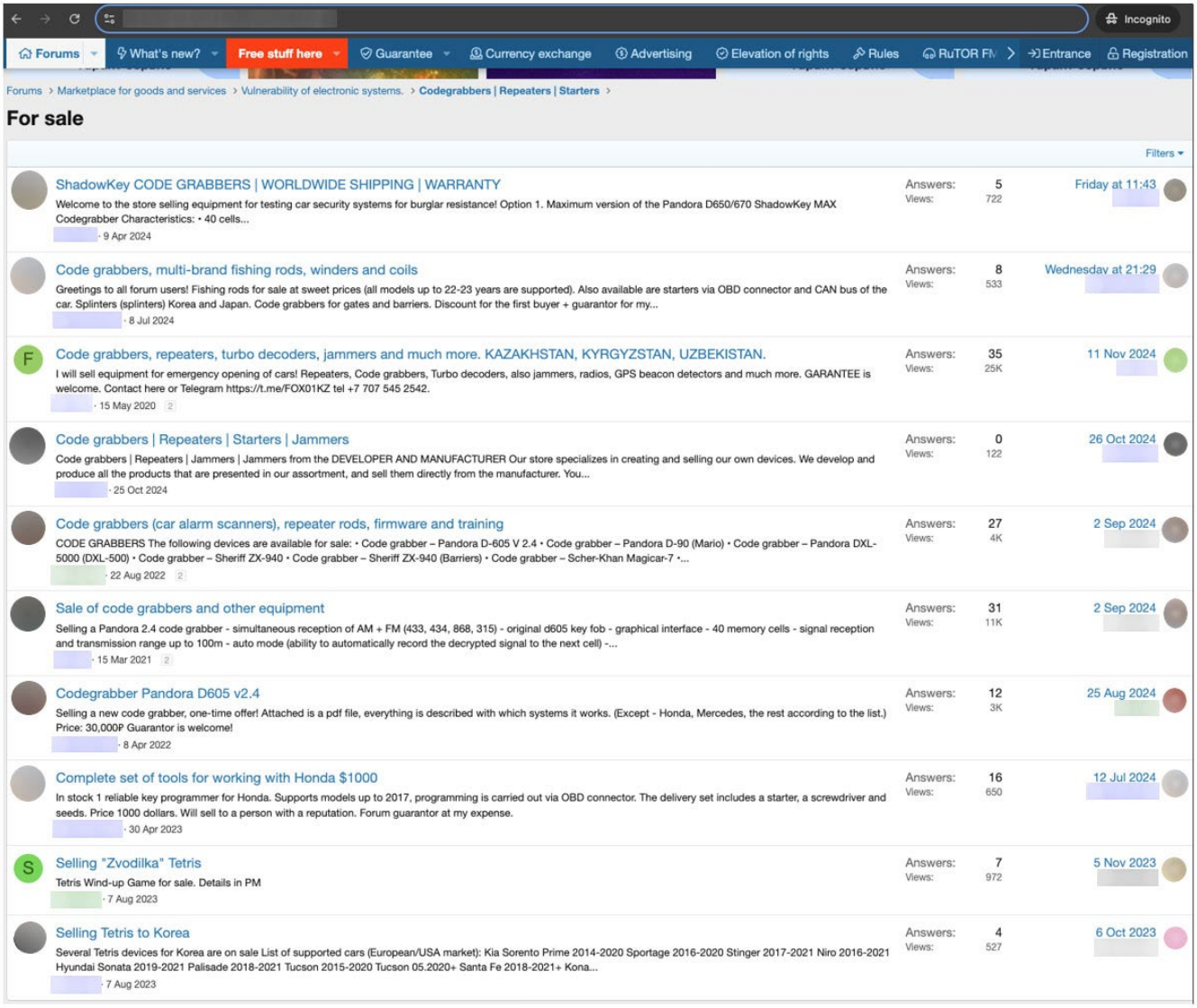


Figure 28. Examples of car-related tools and services (Rutor forum)

Influence of Geopolitical Events in the Underground

Recent geopolitical events have significantly affected the Russian-speaking underground, triggering changes in the rules of engagement, including the geographical areas and critical verticals deemed "acceptable to target."

These include not only the war between Russia and Ukraine but also the Nagorno-Karabakh conflict, elections in Georgia, and unrest in several other ex-USSR states. The geopolitical unrest reshaped ties and trust both between and within cybercriminal groups and communities. It also exposed the support particular sides were providing, which can indicate the origin or the physical location of the underground actors.

Changes in trust between countries lead to the polarization of economic and military alliances. Prioritization of military supply chains and imposed sanctions result in shifts in digital, physical, and financial supply chains, ultimately influencing underground activities.

This section highlights key changes in threat actor behavior, criminal business processes, and the prioritization of monetization options influenced by recent geopolitical events.

Changes in the Rules of Engagement

The underground phrase "Do not work in RU" is a common agreement among criminals to avoid targeting victims within Russia — however, the term has never referred exclusively to Russia. By default, it encompasses Russian-speaking countries or former USSR territories.

Later, depending on interpretation, the Baltic countries were excluded, aligning the defined areas with the Commonwealth of Independent States (CIS). While the rule itself is fairly universal, it has various exclusions triggered by the chokepoints in different criminal business processes and necessary activities within Russian-speaking areas.

Money mules, money laundering, and intelligence collection services have long been available on Russian-speaking underground communication platforms but require some level of involvement within Russian-speaking countries to function. Figure 29 shows an example of a payment processing service in both Russia and Ukraine.

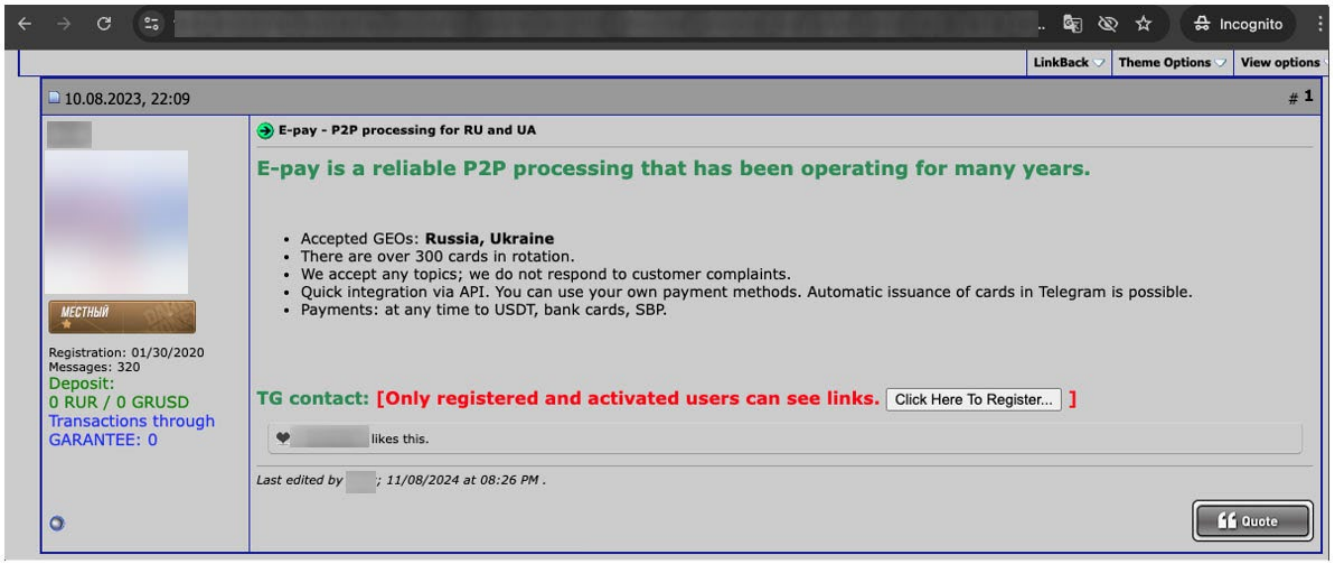


Figure 29. Payment processing service operating in both Russia and Ukraine (DarkMoney forum)

In general, the rule remains in place for many underground platforms today, though some tolerate posts that potentially target either Russia, Ukraine, or other countries in the region. There are ongoing discussions in most underground communities on the long-term consequences for those who break this rule.

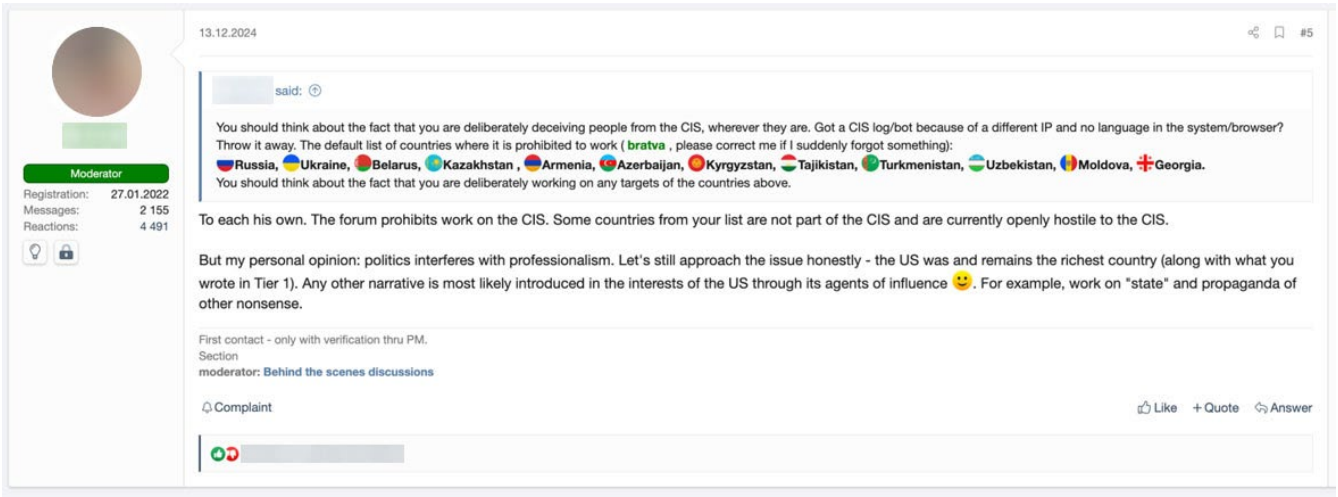


Figure 30. Discussion of "targeting" Russian-speaking countries (translated)

Recent Targeting Changes in Russia and Ukraine

One of the main reasons why the "Do not work in RU" rule has remained in place for so long was the fear of attracting local law enforcement. However, recent geopolitical events in the region, particularly the war between Russia and Ukraine, have led many criminals to believe that the likelihood of such law enforcement collaboration has decreased significantly.

This lower risk, combined with the motivation to harm the perceived enemy, has led to a rise in instances where this rule is broken. As an example, the following screenshot (Figure 31) shows a request to buy a Hidden Virtual Network Computing (HVNC) or stealer malware that works in Russia was posted on the Rutor forum, which tolerates such posts.

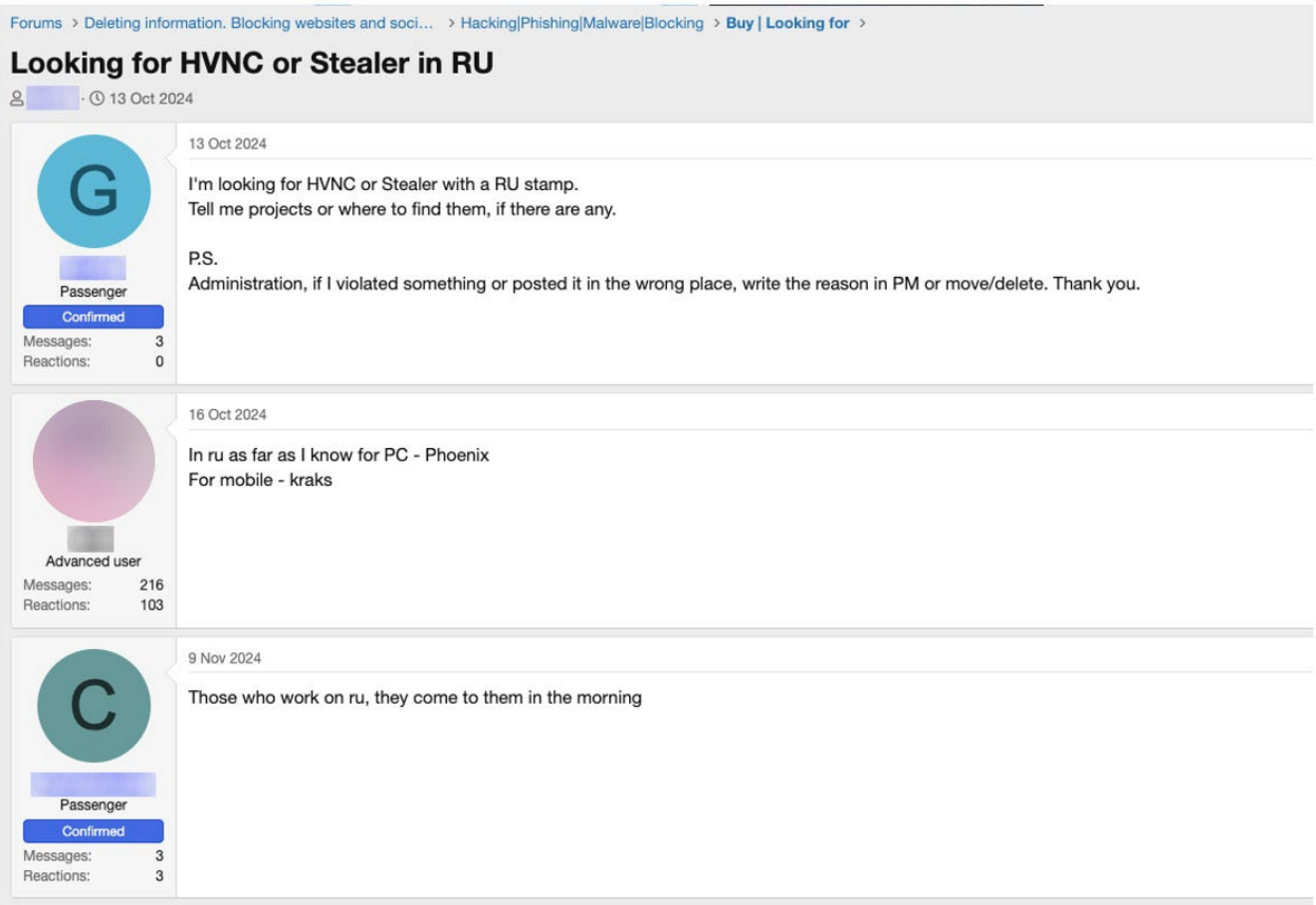


Figure 31. A request for HVNC or stealer malware compatible with Russia on the Rutor forum

Alongside malware, other services that are an important part of the cybercrime underground supply chains are advertised with explicit claims of their suitability for implementing criminal business processes in a particular region. Figure 32 shows an example of a proxy service offer designed to target Russia with spam campaigns.

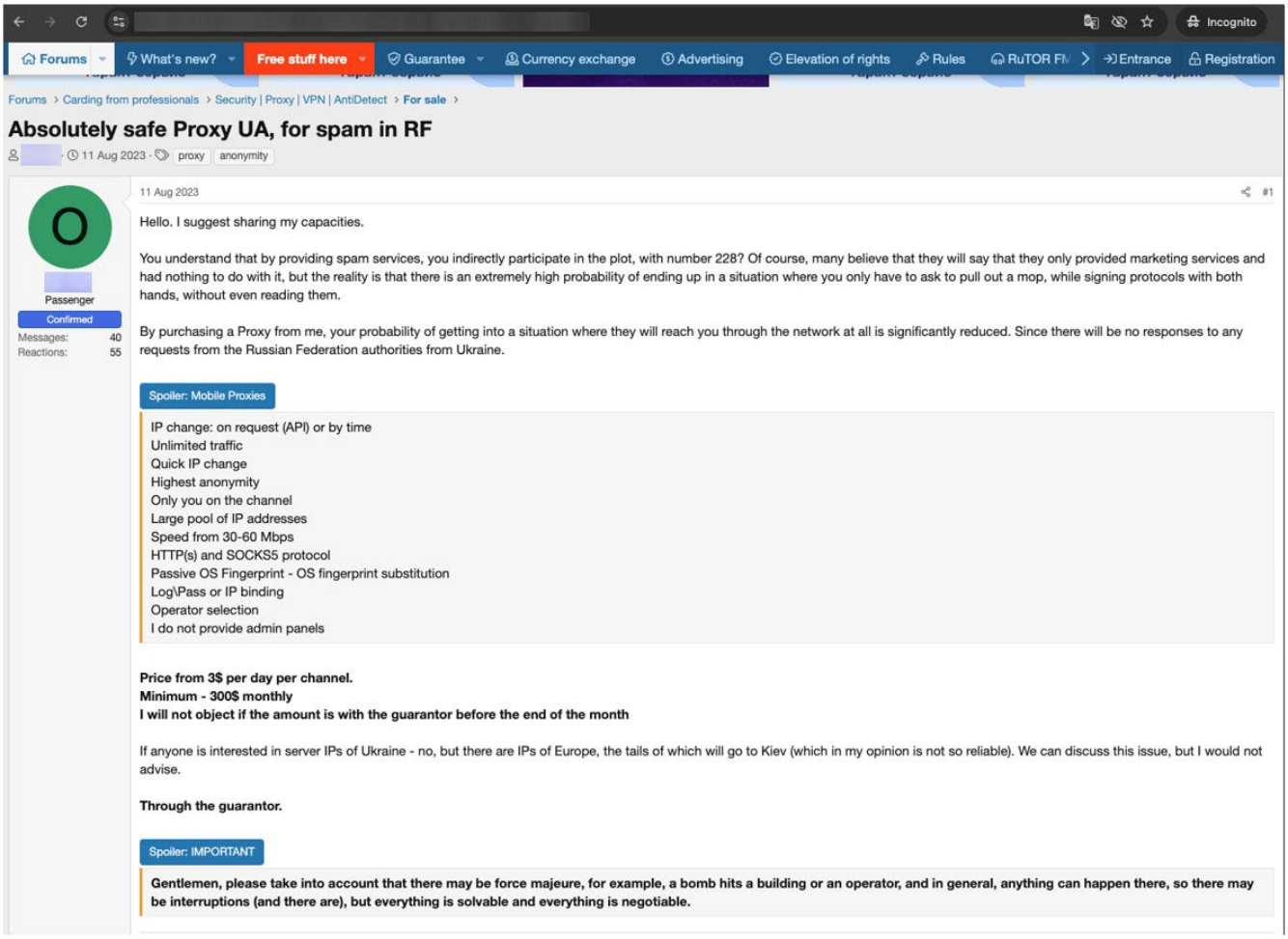


Figure 32. Ukraine-based proxies offered for targeting the Russian Federation (Rutor Forum)

The separation of loyalties has also impacted recruitment processes in the underground. Job proposals targeting Russian-speaking regions are appearing more frequently in these communities. Figure 33 shows an example of a job posting for a scam team that targets RU (Russia in this context), posted on the Gerki forum in February 2024, with a low entry barrier (training expected to take just a few hours).

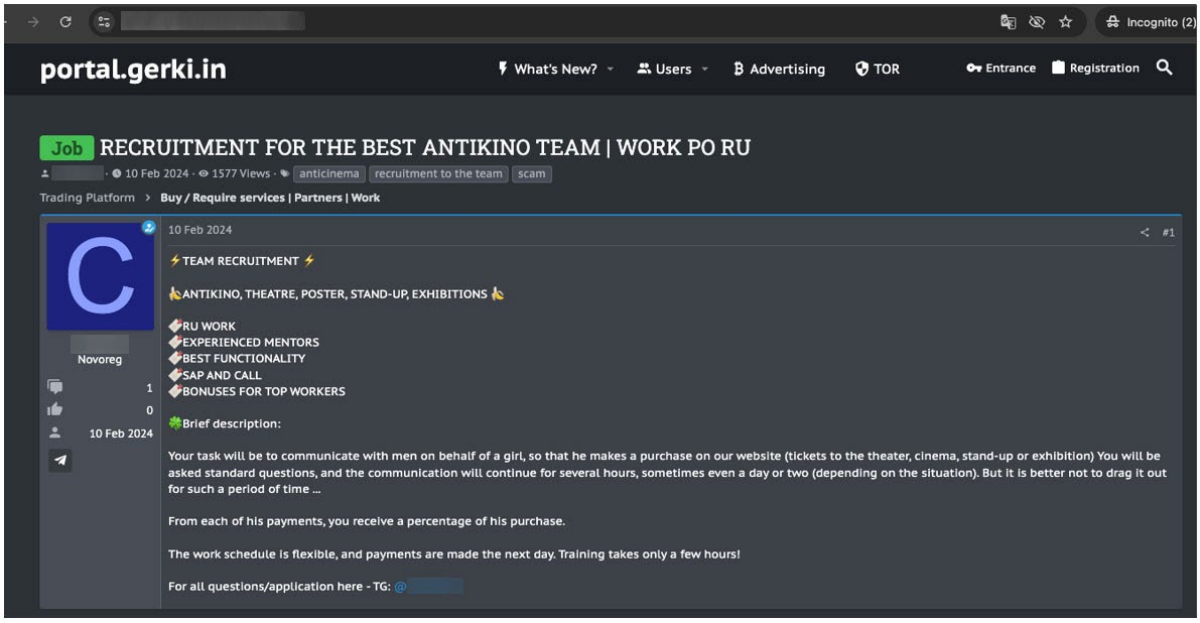


Figure 33. Job posting to conduct scams in Russia (Gerki forum)

Ukraine is also targeted in similar ways and on a comparable scale. Figure 34 shows an example of a job offer for a female, Ukrainian-speaking individual for explicitly-claimed criminal activity (referred to with the common criminal slang "black project"). The job requires interaction with potential victims via calls and messengers in Ukrainian, with a starting salary of US$2,000 per month.

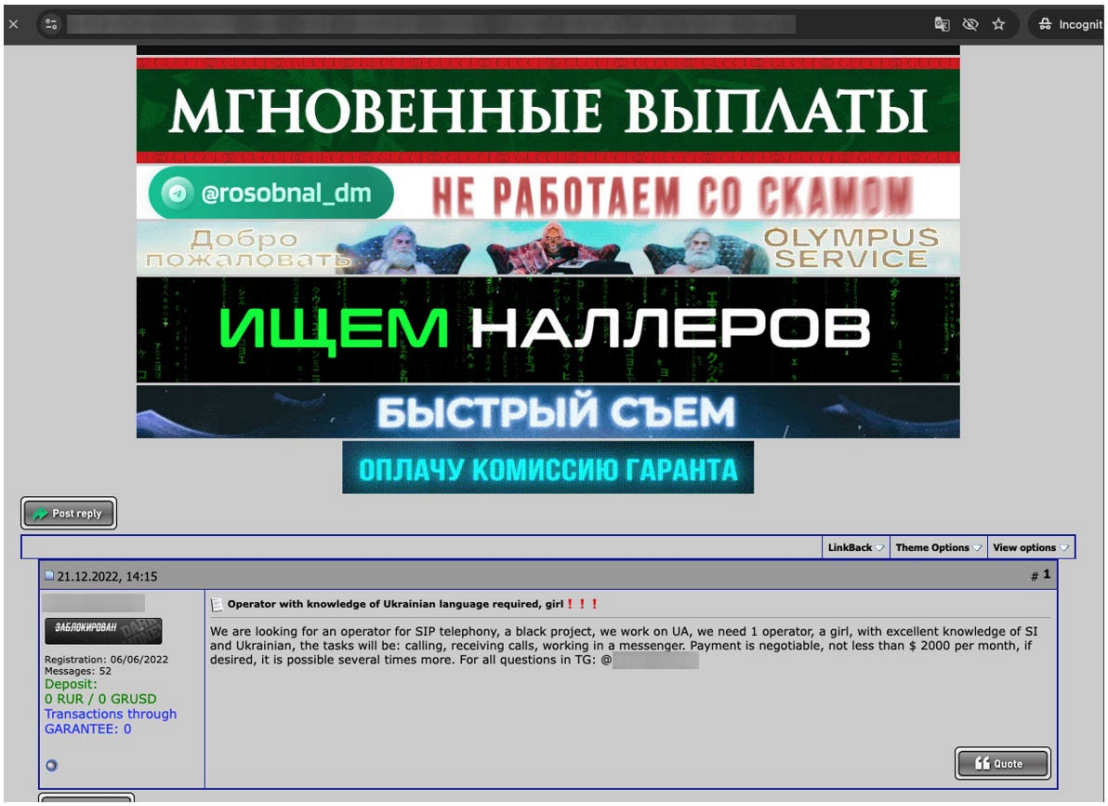


Figure 34. A recruitment post for a scam that targets Ukraine (Darkmoney Forum)

Alignment with Government Objectives

By leveraging attacker services on the underground, government-aligned threat actors are often capable not just of achieving their goals, but also maintain a level of deniability, as the actions and damage are carried out by third parties.

This also allows them to blend in with the more financially motivated campaigns of the same criminal service providers. Geopolitical unrest further increases pressure on nation-state-aligned actors, as their objectives shift rapidly and the deadlines to conduct operations become dramatically tighter. This shortens the preparation window for their operations, driving them to seek alternative ways to achieve their goals.

Underground services are one option for providing such resources, and it is not surprising to see the traces of national-state interest groups increasing both in underground conversations and in the tools observed with their kill chains.

At the same time, the presence of such actors can raise a red flag within the underground community, as seen with the reactions in the following screenshot (Figure 35). In this case, the request to conduct operations is restricted to border regions currently contested in the war – which is very unusual for normal criminal behavior.

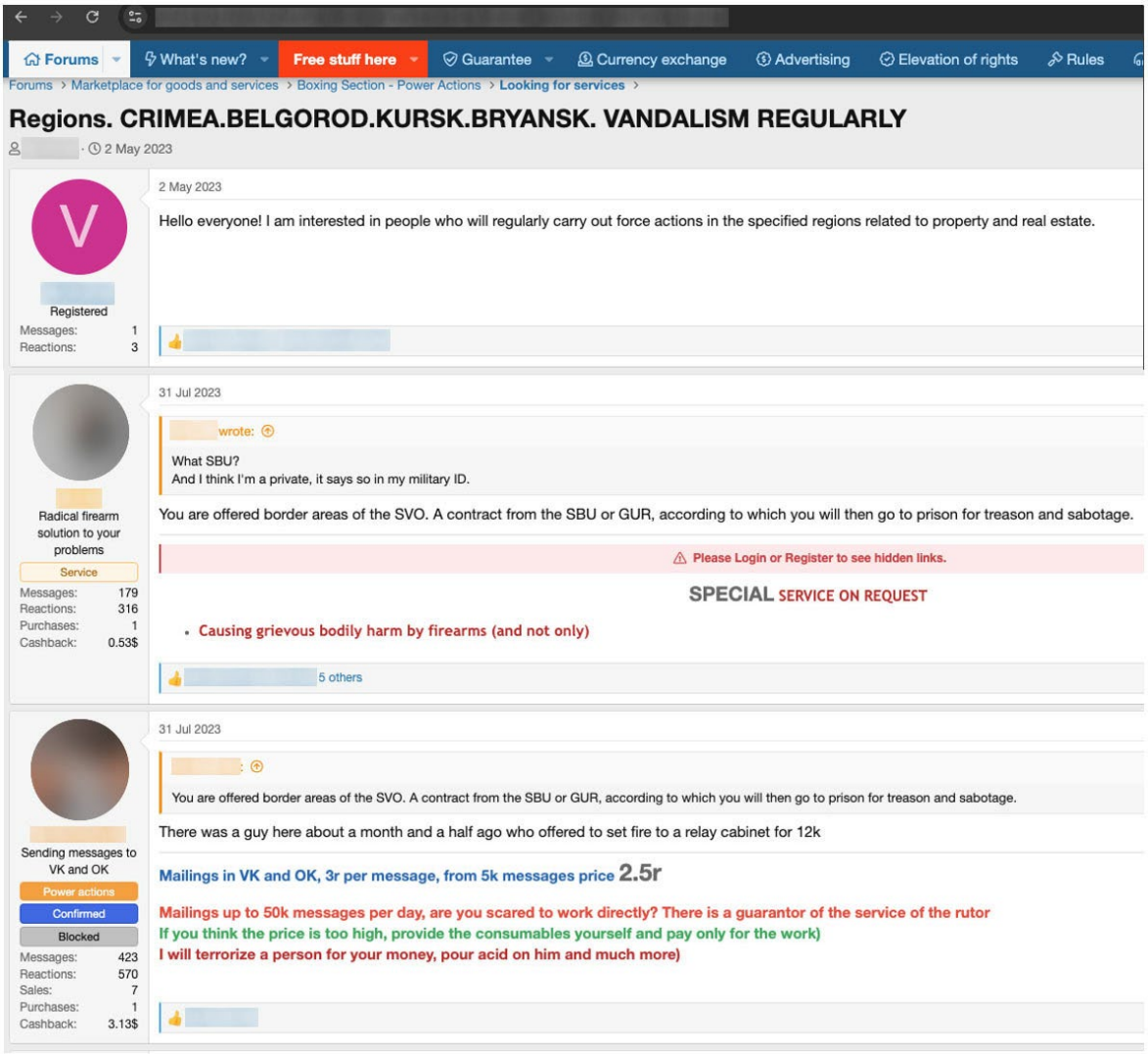


Figure 35. A request for violent actions near the Ukraine-Russian border (Rutor forum)

Rise of Hacktivism

Separate from financial criminal motivations or nation state espionage, hacktivism — ideologically motivated hacking — offers an opportunity for both criminal and nation-state groups to advance their differing goals.

For example, it can be used to justify the actions of ransomware groups, whether against particular geographical regions or against specific verticals (e.g., military or government. Additionally, by influencing the targets of hacktivist operations or pretending to participate in them, such groups can conceal their real actions by diverting defender focus.

There have been several cases where criminal groups took sides in ongoing conflicts, aligning their actions with hacktivist ideals rather than financial ones. We explored this in depth in our paper "Understanding Hacktivists: The Overlap of Ideology and Cybercrime".[34]

The rise of hacktivism is an expected behavior during geopolitical unrest. This trend creates additional opportunities for criminal and nation-state groups to exploit such attacks even against organizations outside the main conflict. The adaptation of criminal business processes to leverage or incorporate hacktivist actions can lead to significant changes of the attack surface for the defending organization, requiring adjustments to mitigation procedures.

Reshaping of Ties and Trust Relationships

Significant geopolitical events in the region, including several kinetic conflicts, disrupt ties and trust relationships at the same level. Actors — depending on their geolocation, mindset, priorities, and self-discipline — tend to choose one of two paths: either taking sides and breaking away from previous partnerships or prioritizing criminal monetization over the ongoing conflict and maintaining the status quo.

Even in this second category, however, changes are inevitable, driven by the macro environment in which they live. For example, cash-out options in Russia have changed due to the sanctions, and criminals now find some previously trusted underground services they relied on to now be untrustworthy – leading to disruptions in their business. Some actors have physically relocated to European, Asian, and American countries, where they have begun interacting with the local community and adapting their knowledge to the local environment.

These processes have lowered entry barriers for foreigners to request or offer services in the Russian-speaking underground, expanding underground service coverage into these new geographical regions.

In the following screenshot (Figure 36), taken from the Darkmoney forum, we see a discussion about preferred countries for relocating (where it is considered "safe" to continue business).

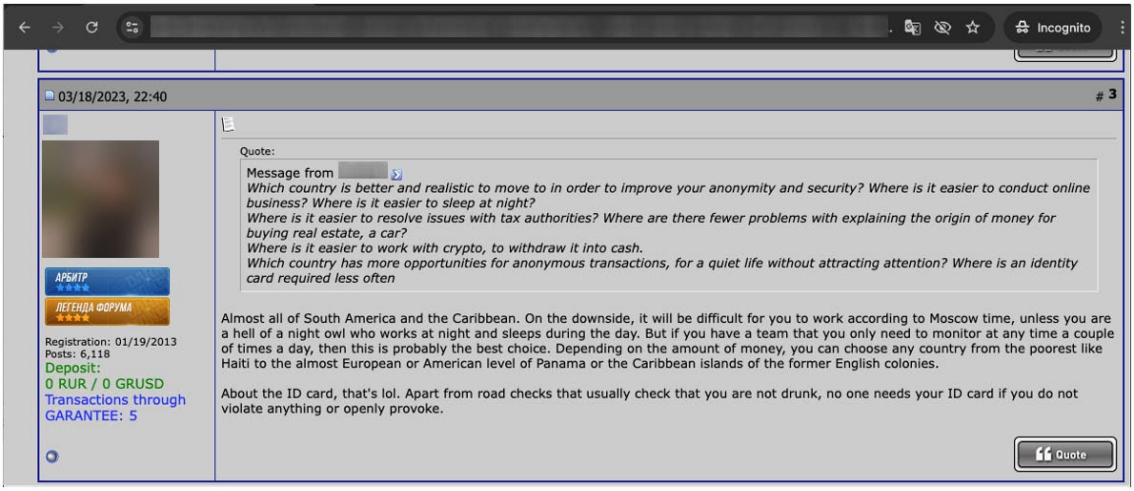


Figure. 36 A thread on relocation options (Darkmoney forum)

Synergy with the Chinese-speaking Community

In recent years, there has been an increased presence of non-Russian speaking members in Russian-speaking forums.

The origins of other participants vary, but we have observed a significant increase of Chinese-speaking individuals collaborating with members of Russian-speaking forums. There are several factors that indicate a Chinese-speaking origin: some users post messages in Chinese, while in other cases, image metadata contains Chinese text. Some forum participants also openly disclose their origins.

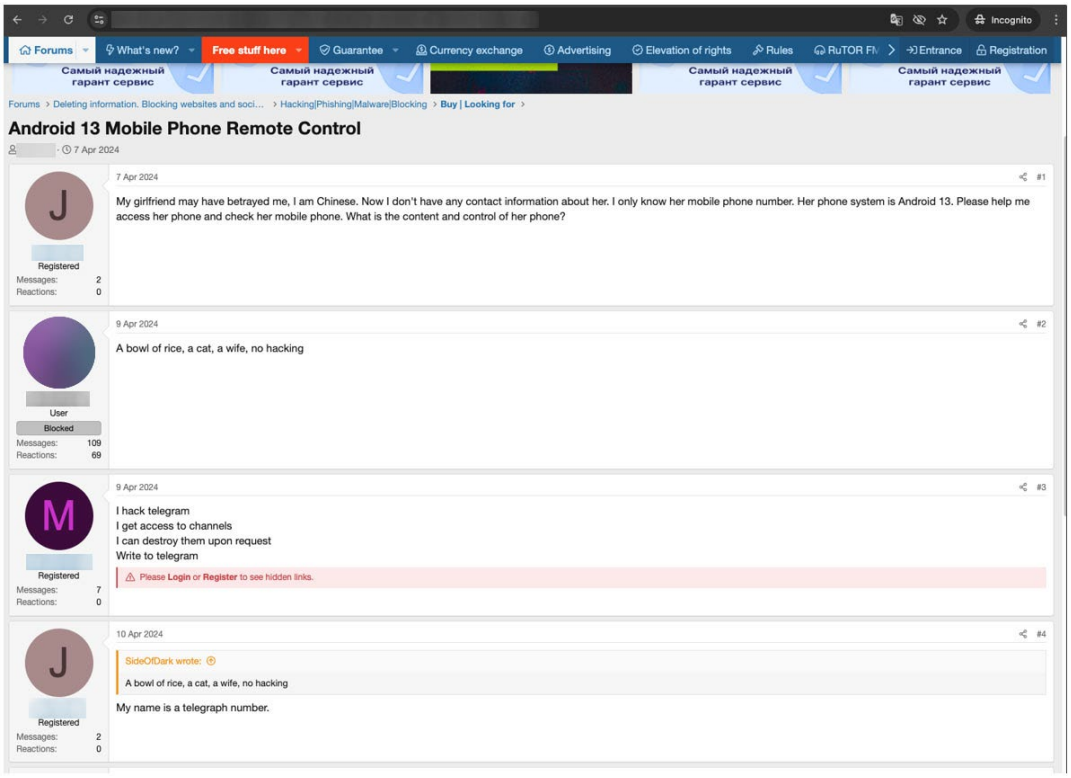


Figure 37. A request from a Chinese-speaking person on a Russian-language forum (Rutor forum)

This evolution of collaboration has led to several notable trends:

- Chinese-speaking criminal groups frequently act as initial access brokers for compromised companies worldwide, selling access to compromised assets and data on Russian forums.
- These groups often seek resources on Russian-speaking forums, including purchasing vulnerabilities, exploit code, or requesting the development of malicious software.
- They have also been observed recruiting individuals to conduct offensive operations.

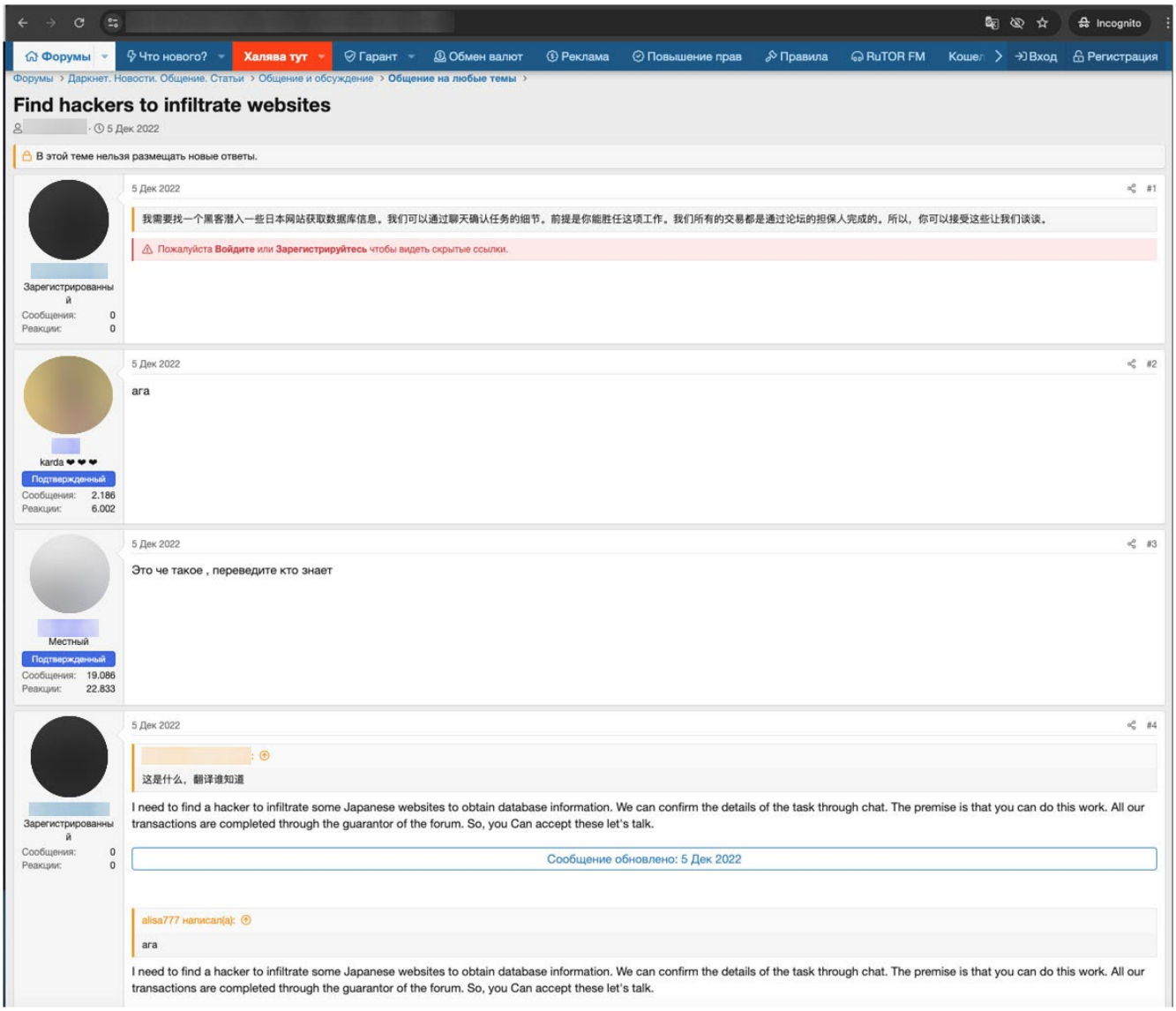


Figure 38. Request from a Chinese-speaking member to infiltrate Japanese website databases (Rutor forum)

Spillover of the Russian-speaking Cybercrime Scene into the EU

Many individuals, especially from Ukraine and Russia, have relocated or considered relocating abroad in recent years.

Alongside ordinary people, members of the cybercrime underground have expressed interest in relocation. Indicators of such demand can be seen among the job postings in the underground. For example, the following post on the Rutor forum indirectly suggests the existence of a service facilitating illegal Ukrainian border crossings:

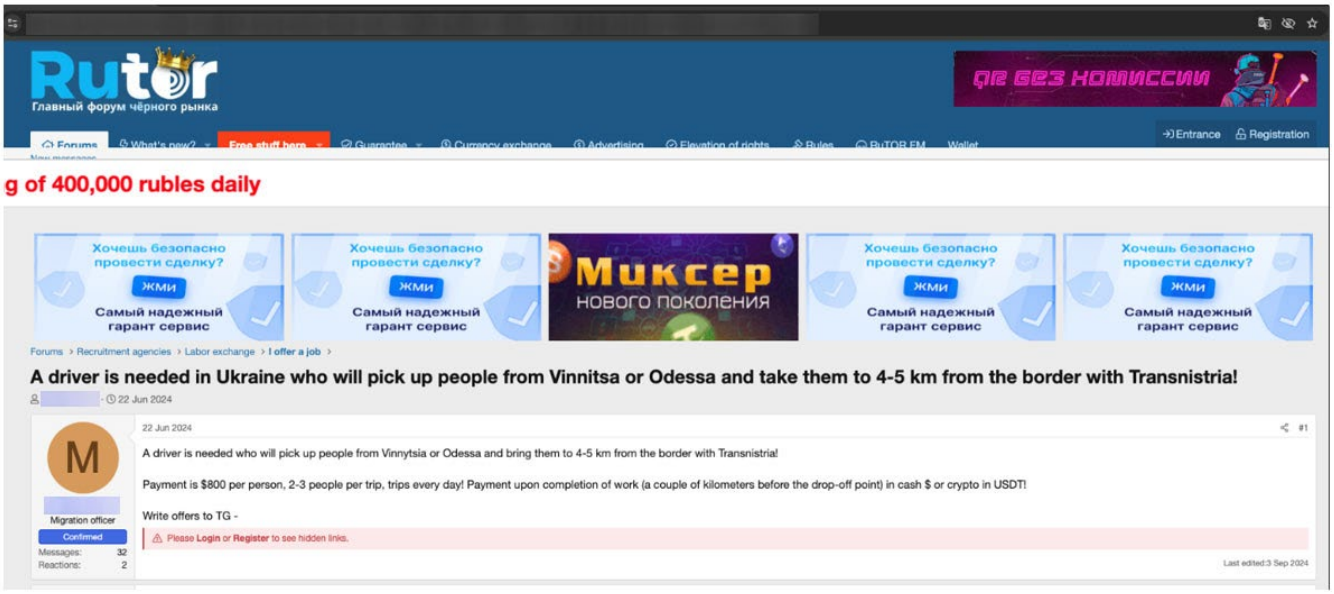


Figure 39. A job offer for a driver for human trafficking operations (Rutor forum)

Along with relocation, underground actors are bringing their habits and applying their knowledge to these new locations. They are introducing and adapting criminal business processes, including those requiring a physical presence in the area.

For example, the advertisement in Figure 40 offers violent actions and surveillance services in both the CIS and Europe, posted on a Russian-speaking underground forum. Such services were less common in the past, indicating a growing availability of local assets available to carry them out. The range of services may attract not only cybercriminals, but also nation-states looking to cause disruption in this region.

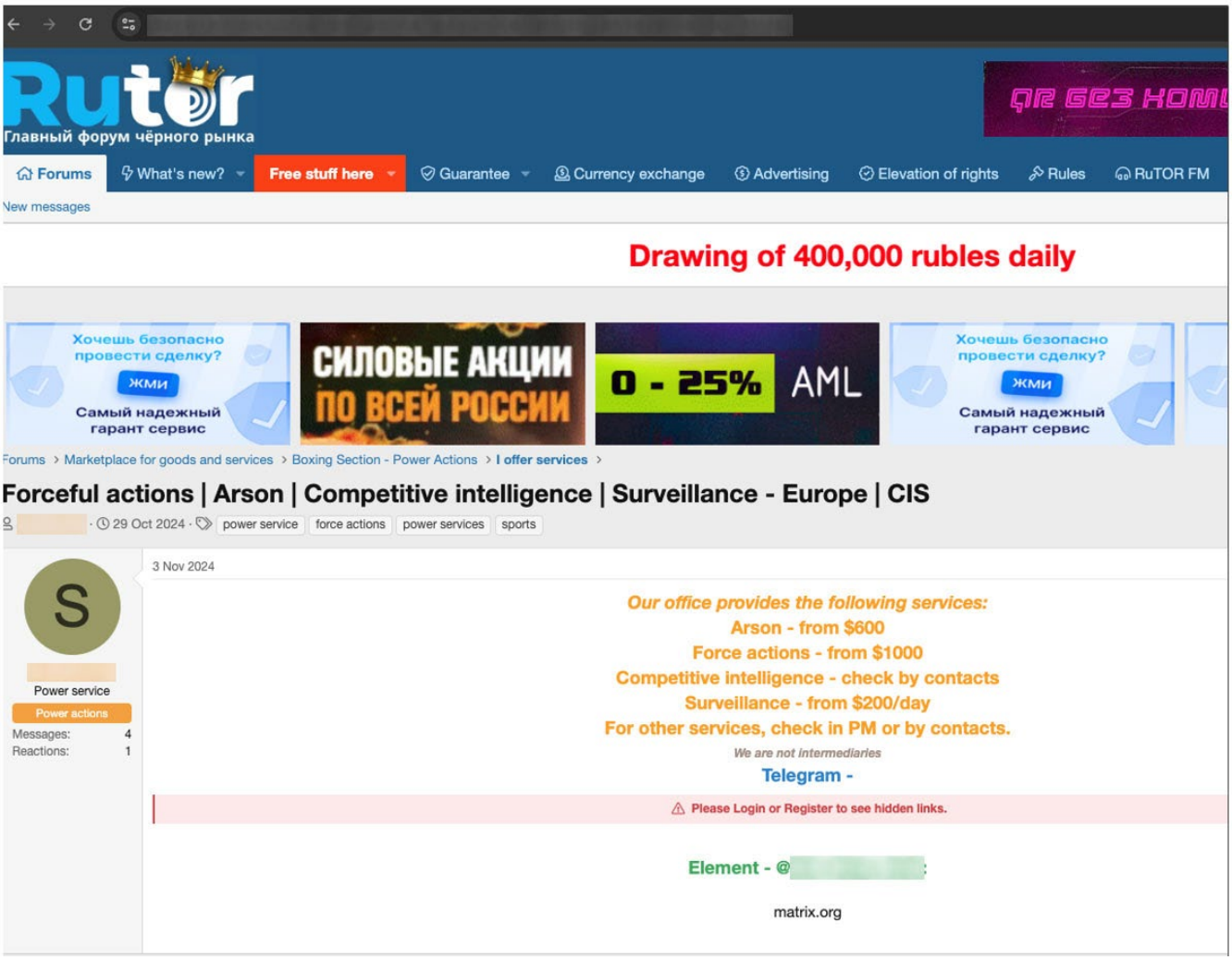


Figure 40. An offer to conduct violent actions in Europe (Rutor forum)

Another advertisement is related to calling activities targeting German-speaking countries. The proposed salary is €2,000 per month, with weekly payments, and working hours from 9 AM to 5 PM in Berlin.

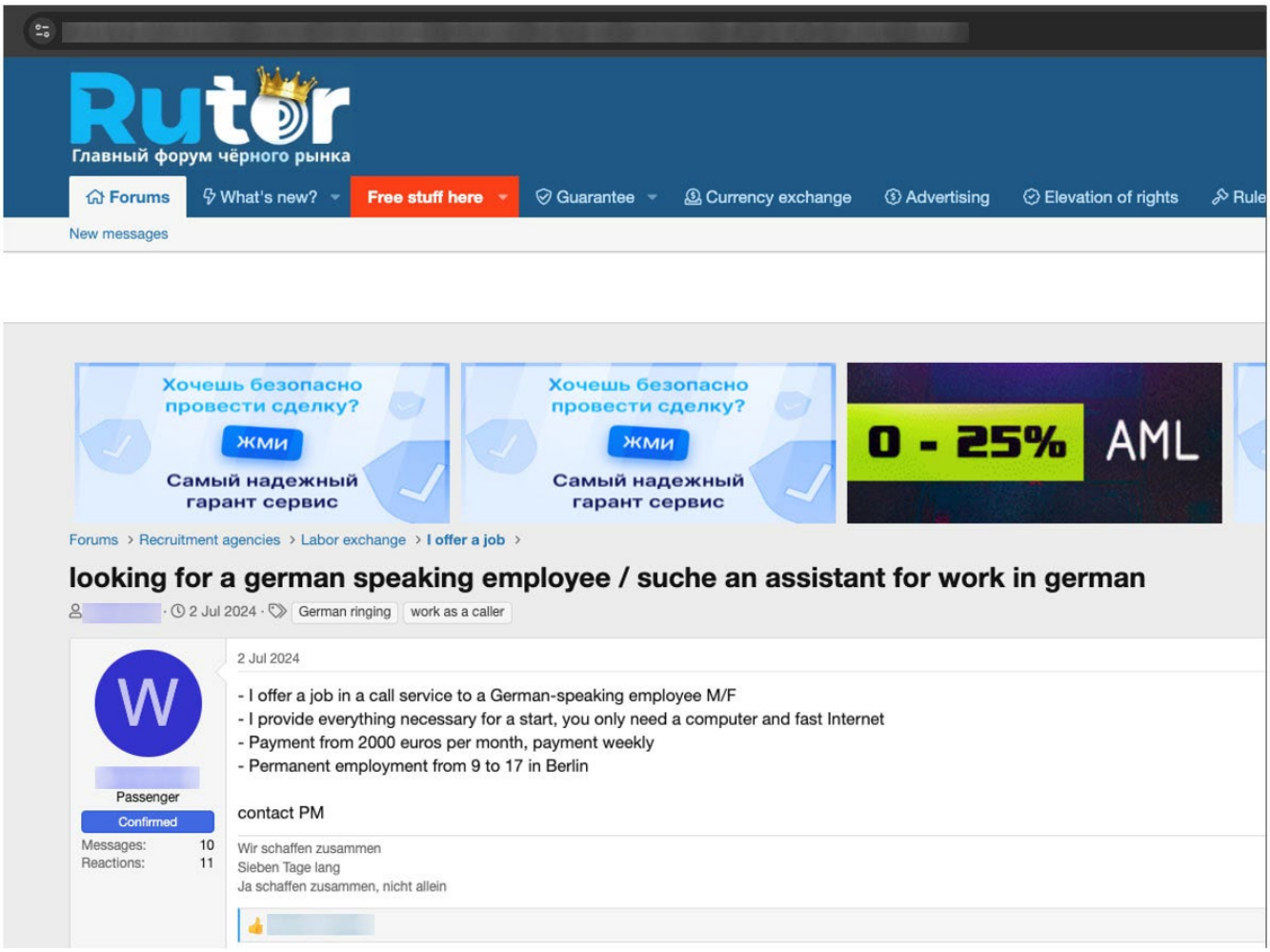


Figure 41. A request for German speaker to carry out call fraud, who also is a member of the Russian-speaking cybercrime underground (Rutor Forum)

We also observed an increase in advertisements for money laundering and withdrawal services offered in Ukraine and the European Union (but not in Russia) by the same actor. According to the description, both money mules and shell companies in the EU and Ukraine are involved in this actor's business process.

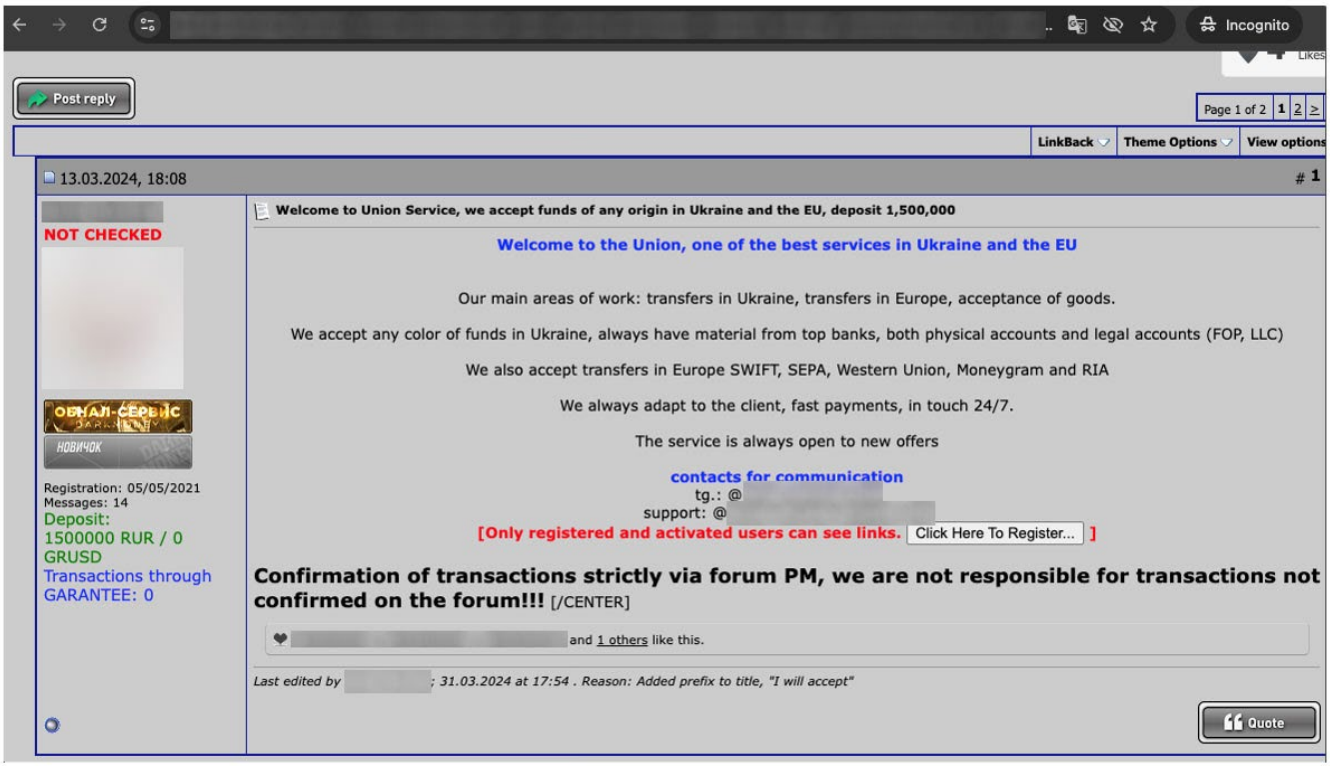


Figure 42. A money laundering offer available in Ukraine and the EU, but not in Russia

Reshaping of Digital, Physical, and Financial Supply Chains

Along with trust and ties, geopolitical unrest significantly affected digital, physical, and financial supply chains. The key driver of this disruption is the significant changes in logistics caused by imposed sanctions and business decisions to withdraw from affected regions.

Sanctions targeting business entities and individuals have also increased demand in the region for goods with limited supplies. With restrictions on official suppliers, underground actors are capitalizing on this market and integrating it into their business processes.

Sanctions are regularly discussed in relation to supply chains, with some logistics services advertising the delivery of sanctioned items. The example in Figure 43 features an advertisement offering shipping from USA and Germany within 14 days. The actor also explicitly mentions collaboration with the carding and staffing community to deliver their goods.

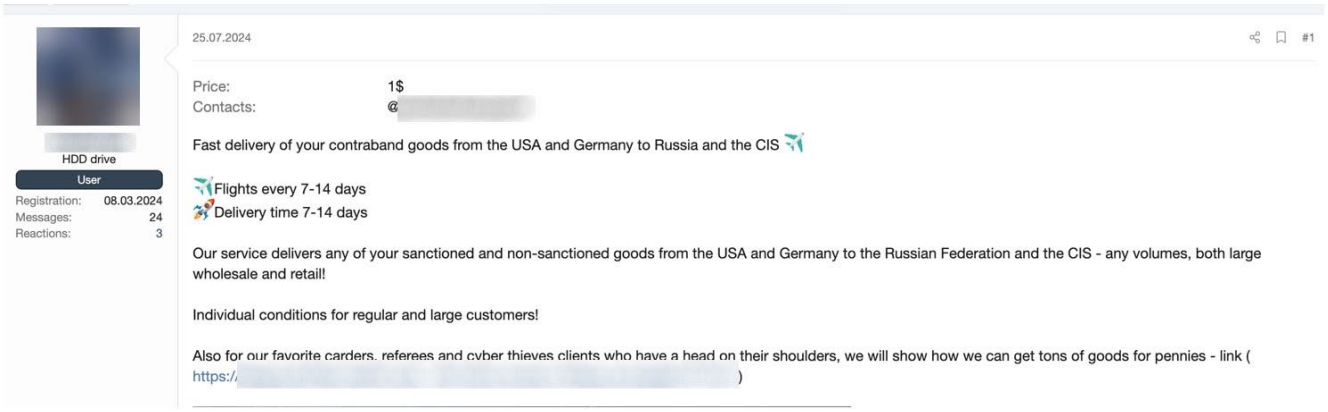


Figure 43. Delivery service for goods to bypass sanctions

We observed another actor advertising products shipped from eBay and Amazon, mostly focusing on IT equipment such as cell phones, tablets, and laptops – many of which are already available in their local stock. Other actors are capable of delivering other hard-to-obtain items, such as drones. Those deliveries are often part of the monetization schemes for stolen credit card or e-commerce accounts, as the prices offered to customers are lower than the official item prices on e-commerce platforms.

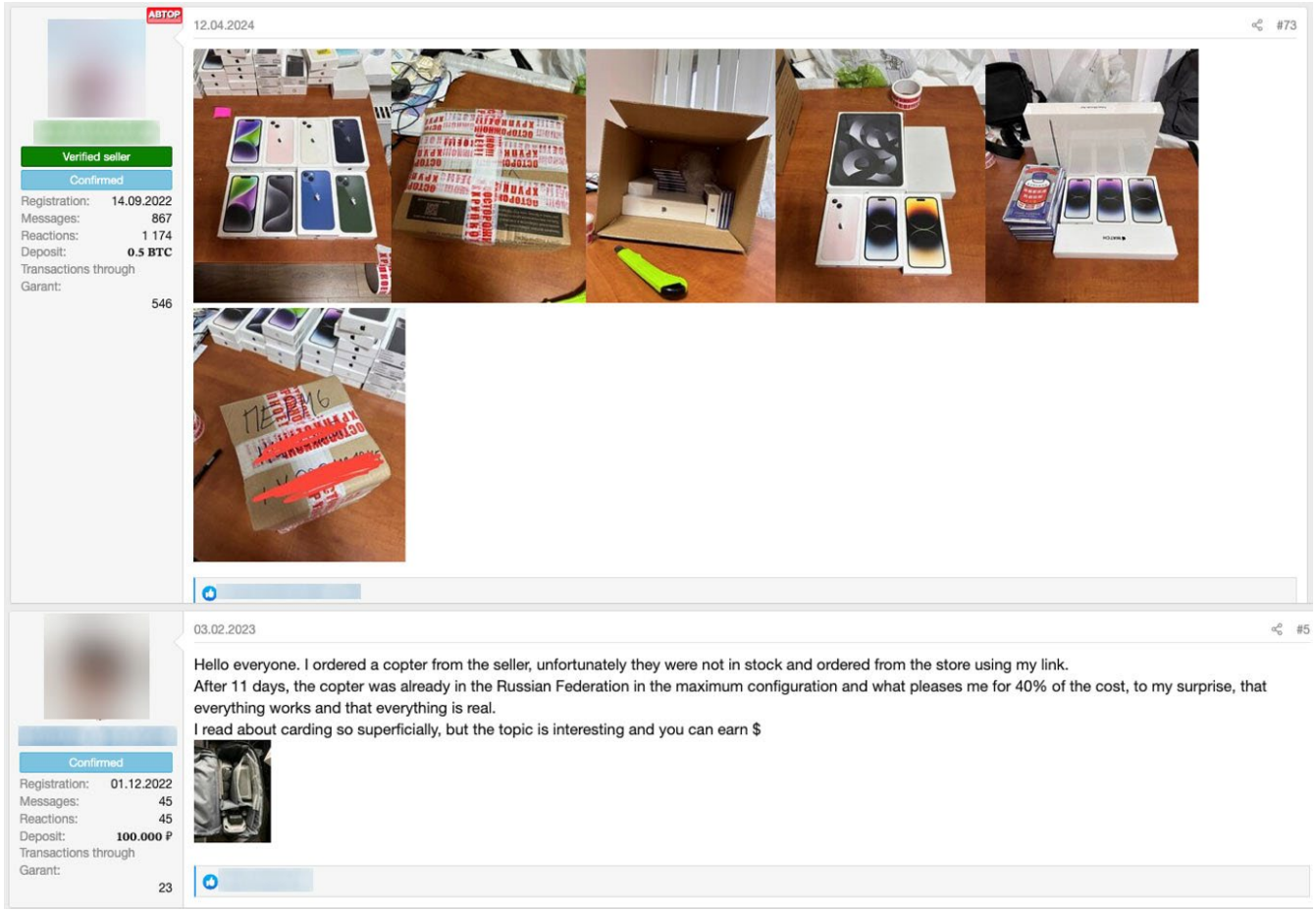


Figure 44. Examples of items shipped from eBay and Amazon to Russia through an underground service

Since traveling between CIS countries is easier for Russian citizens compared to the European Union (where a visa is often required) a significant number of those who left Russia have relocated to nearby countries. This has reshaped financial flows and increased demand for money transfers to countries like Uzbekistan, Kyrgyzstan, and Kazakhstan – countries that were not previously as popular for such services.

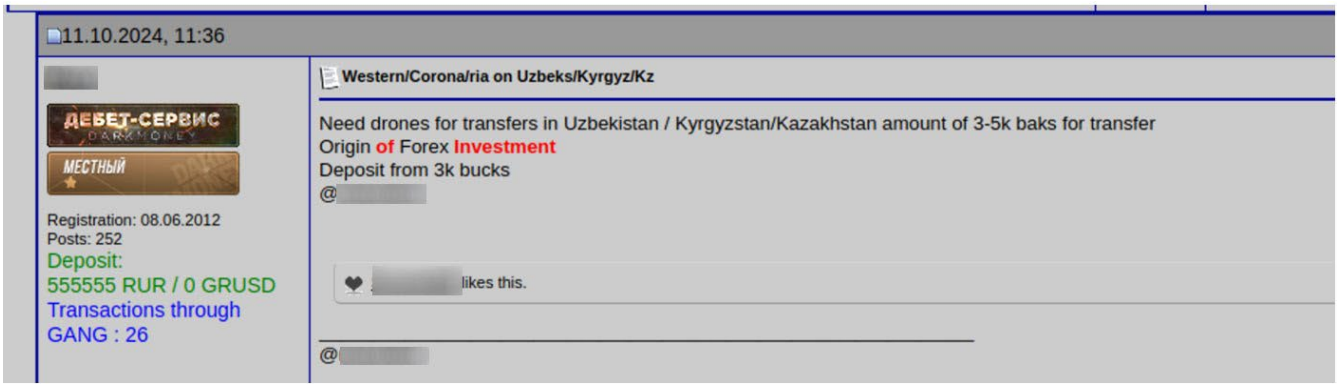


Figure 45. An actor recruiting mules (referred to as "drones") in Uzbekistan, Kyrgyzstan, and Kazakhstan due to the growing demand of such services in the region (DarkMoney forum)

Money flows between Russia and many foreign countries are largely disrupted due to the sanctions. As a result, legal business entities are turning to the underground to facilitate financial transfers abroad. The following example (Figure 46) highlights a discussion about the growing demand of these types of underground financial services.

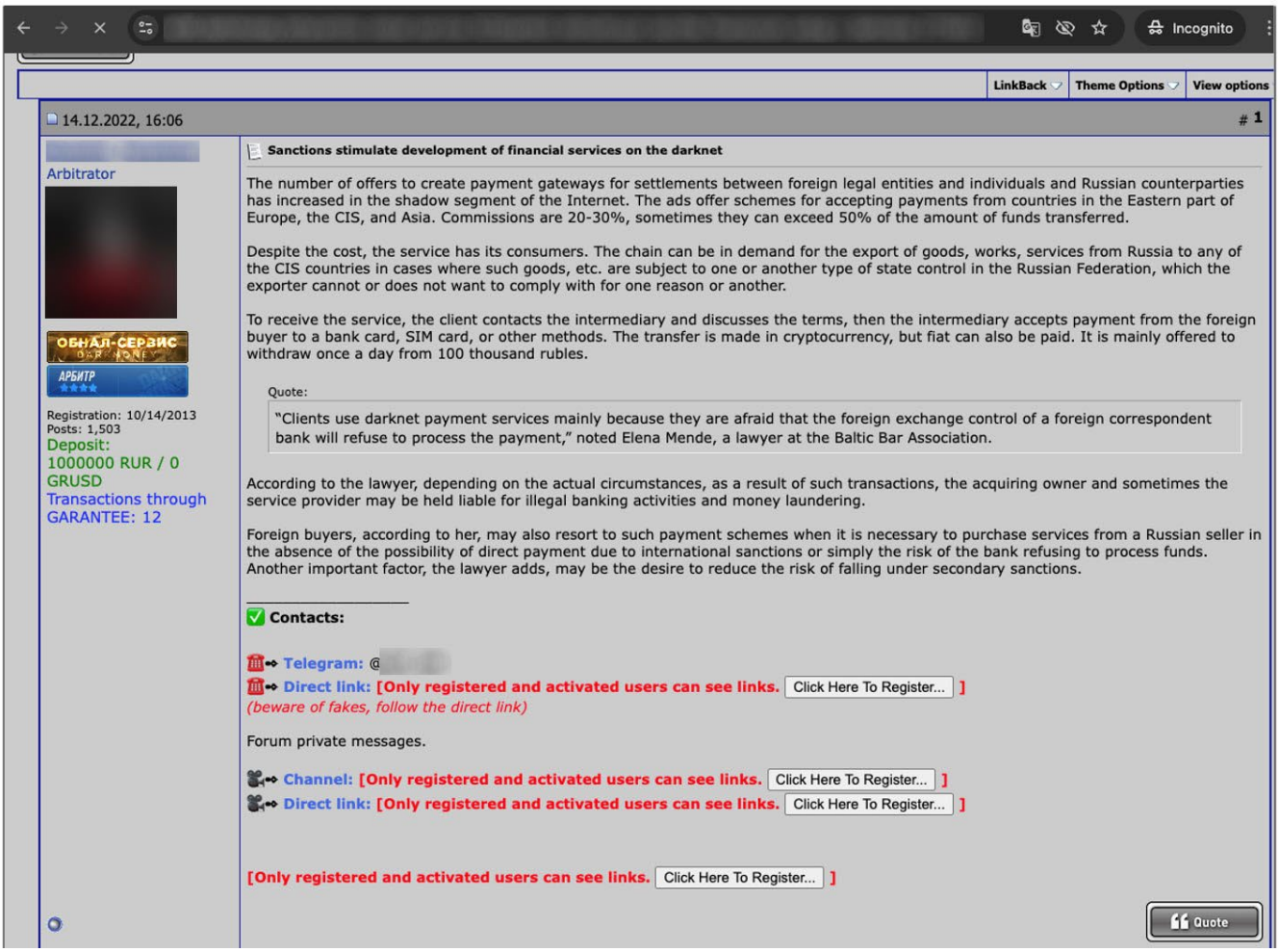
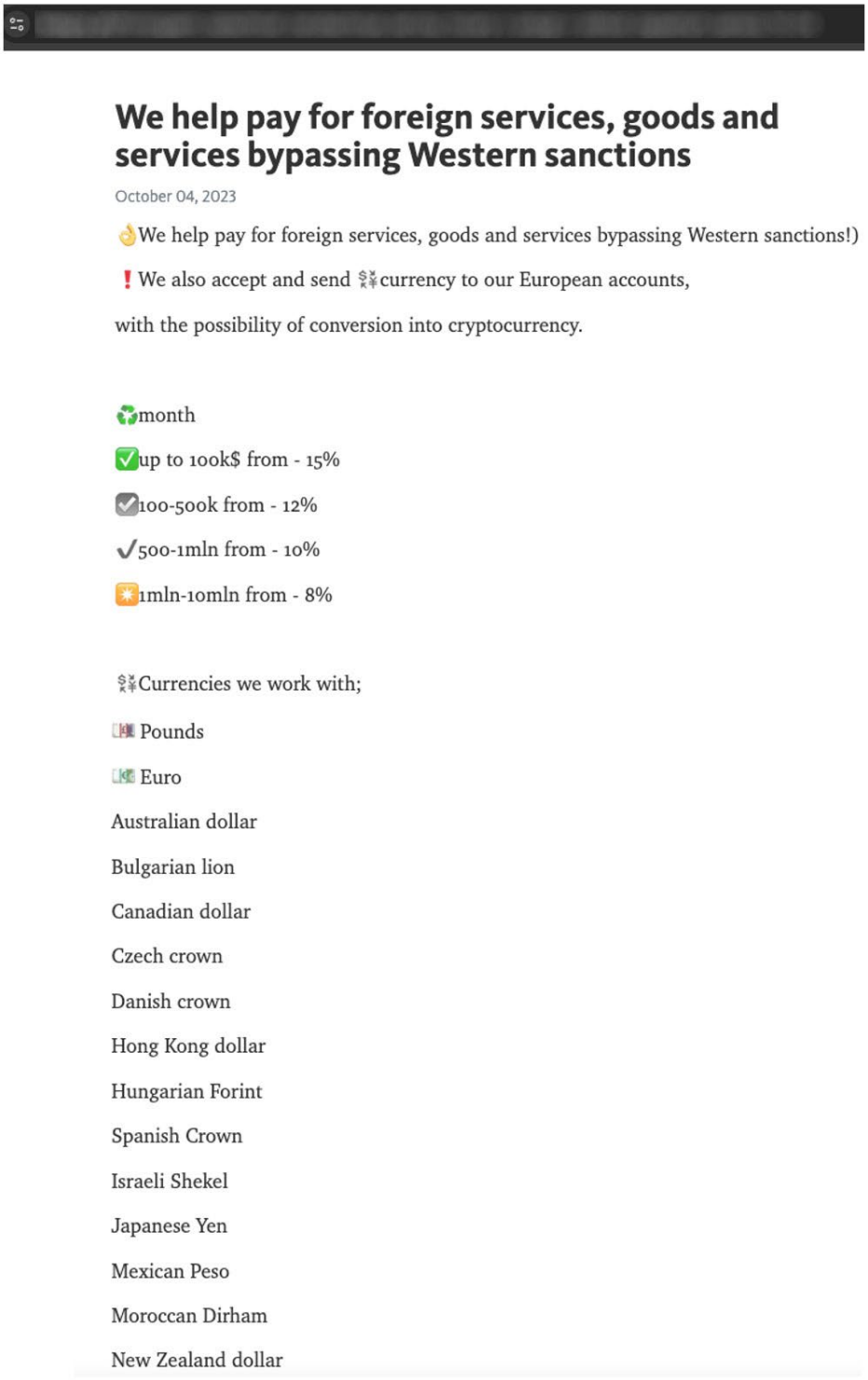


Figure 46. A discussion on how sanctions are driving demand for dark market services (DarkMoney forum)

Services that assist with sanction bypass payments appear quite scalable and widely available. The example in Figure 47 illustrates the interest rates for these services ranging from 8% to 15%, depending on the scale of financial operations provided to a particular customer per month. The volume tiers are split into several categories, starting at below US$100,000 and going up to US$10,000,000. A list of supported currencies, including nearly 30 popular ones, is also provided. The advertisement explicitly states assistance in bypassing Western sanctions.



We help pay for foreign services, goods and services bypassing Western sanctions

October 04, 2023

👌We help pay for foreign services, goods and services bypassing Western sanctions!)

❗We also accept and send 💱currency to our European accounts,

with the possibility of conversion into cryptocurrency.

♻️month

✅up to 100k$ from - 15%

☑️100-500k from - 12%

✔️500-1mln from - 10%

🔆1mln-10mln from - 8%

💱Currencies we work with;

🇬🇧 Pounds

🇪🇺 Euro

Australian dollar

Bulgarian lion

Canadian dollar

Czech crown

Danish crown

Hong Kong dollar

Hungarian Forint

Spanish Crown

Israeli Shekel

Japanese Yen

Mexican Peso

Moroccan Dirham

New Zealand dollar

Figure 47. A service offering for organizing payments and bypassing Western sanctions (Telegram)

The Effects of OPSEC and counter-OPSEC on Attacker Attribution

The attribution of cybercriminals can be highly complex. The counteroffensive to attribution for these criminals is strong OPSEC. We have observed that OPSEC techniques and related services have significantly improved over the years.

These have evolved from traditional bulletproof hosting to fully anonymized workstations with full-disk encryption and multi-hop exit traffic paths.

Law enforcement has been proactive in taking action against cybercriminals. This extends beyond arrests to include infrastructure takedowns and psychological operations aimed at creating mistrust and paranoia among involved individuals.

For example, we have observed an interesting dynamic where law enforcement actions such as forum posts trigger a process of self-reflection and recommendations for future improvements in the development of criminal toolkits.

Figure 48 provides an illustrative example. During Operation Magnus (which disrupted the Redline and Meta infostealer families), law enforcement posted references to usernames recovered from systems they had successfully taken down:

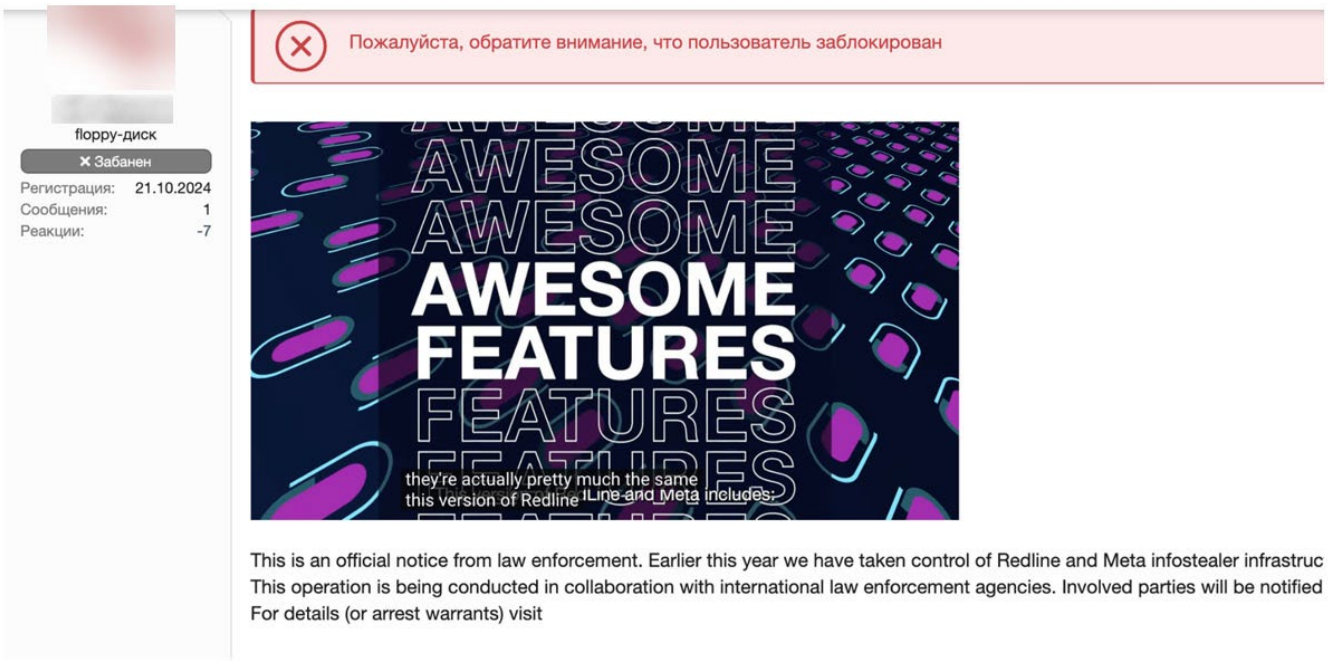


Figure 48. A post from a law enforcement-controlled account "OP_Magnus" to the XSS forum

This prompted a self-reflective response from the community that included several recommendations on how to make future tool development be less prone to analysis and disclosure.

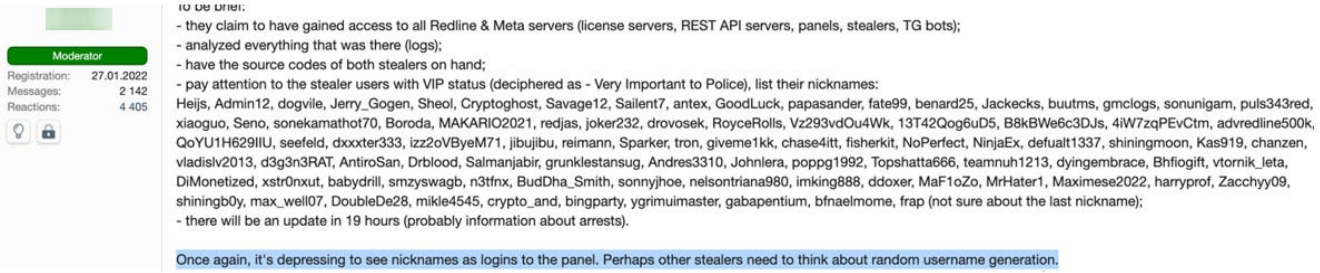


Figure 49. A response by a forum member with self-reflecting analytical comments

OPSEC needs are frequently addressed via specific services such as dedicated hosts with encrypted filesystems, traffic mixers, and VPNs for exit traffic. Various tools, such as mptcp, Whonix and multiple VPNs, are popular solutions for network traffic and anonymization.

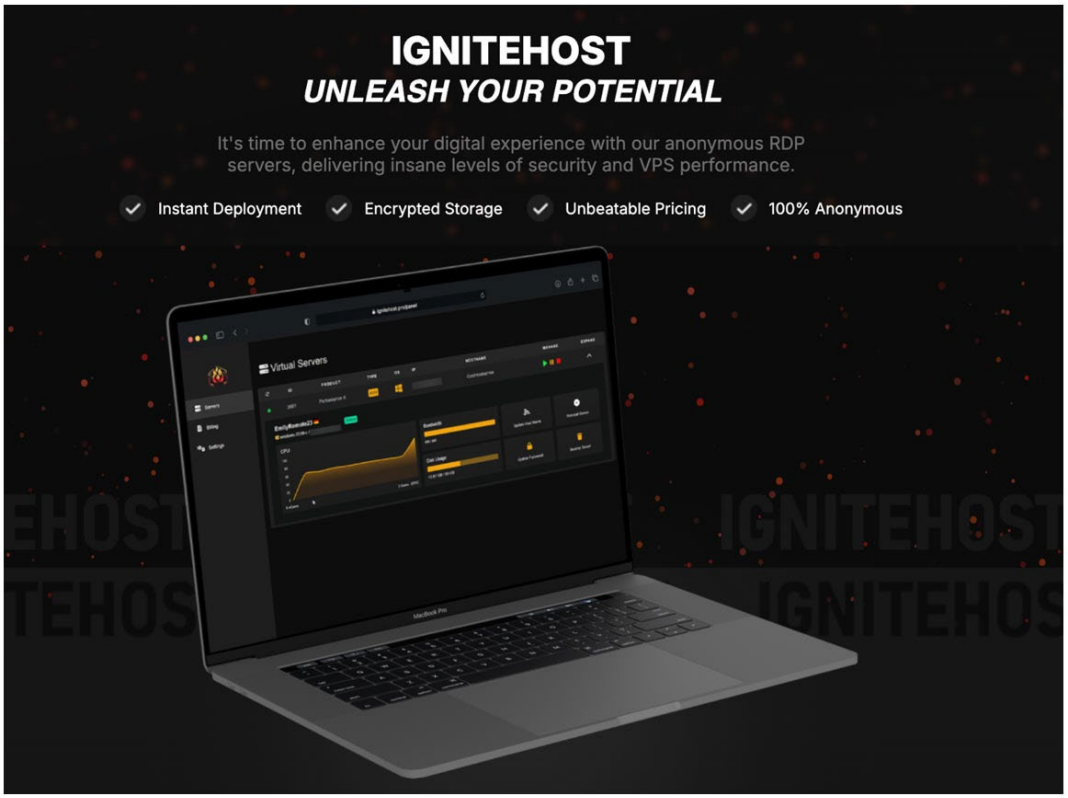


Figure 50. An example of an offering for a highly secure "in-cloud" environment that offers a high level of anonymity for the user

With that said, personal OPSEC is equally important. A recent arrest of the actor using the handle "Wazawaka" serves as a clear sign that even cybercriminals operating in former USSR areas that claim to avoid targeting victims in this region can still face arrest by local law enforcement if they neglect personal operational security.[35]

"Wazawaka" generally ignored OPSEC considerations and never particularly tried to hide his identity, believing he was safe as long as he didn't attack Russian targets. However, his recent arrest proved otherwise, showing that avoiding local crimes is not enough to ensure a cybercriminal's freedom – strong OPSEC is still essential. This lesson has been repeatedly seen in several recent cases, prompting many groups to adapt their strategies accordingly.[36]

Another significant challenge for cybercriminals is infiltration of the groups by security researchers or disgruntled competitors. One of the most notable cases was "Contileaks," where years of internal communication from the Conti Ransomware group were leaked by a security researcher.[37]

OPSEC also needs to account for insider threats. There have been a number of instances where members of a criminal group have disclosed internal group operations as an act of revenge for disagreements or have hacked rival groups to undermine potential competitors.

Many criminal groups who have evolved to a senior professional level prefer to work, partner, or hire only from trusted sources. Even within these groups, a significant level of anonymity and discretion is maintained to ensure that a single "rotten apple" doesn't compromise the whole group.

Impact of Takedowns

Conducting public takedowns has been widely popularized by international law enforcement and private security firms as a seemingly effective means of combating cybercrime. A takedown, in essence, is a coordinated takeover and disablement of attacker infrastructure, though it does not always produce the expected results.

The takedown process is usually followed by PR and media campaigns aimed at promoting and amplifying the effectiveness of such actions. But how effective are these operations in reality?

In many cases, attacker infrastructure is often disposable. Given the level of automation used by threat actors, it often takes only a few days for them to recover and rebuild their infrastructure. Unless the takedown process is coordinated with disabling the human element (the actual criminal group), the attackers often simply learn from their mistakes and reconstruct a new environment – one that would normally address any of the issues that were potentially identified during the takedown process.

For this reason, modern law enforcement actions have evolved to not only disrupt infrastructure but also damage the brand of the criminal group and its services. Furthermore, seized infrastructure is used to gather intelligence, allowing law enforcement closer to attribution and the arrest of the individuals involved.

Arguably, when attacker infrastructure is identified and accessible to those with legal authority, it may be more beneficial to monitor its internal data over a period of time to continuously predict and prevent the cybercrime group's impact over a prolonged timeframe. This debate between intelligence gathering vs. disruption operations remains a balancing act, as law enforcement have to factor for the harm caused by ongoing crimes during monitoring as opposed to future crimes they may prevent based through gathered intelligence.

Effects on Attacker Attribution

Attribution in today's world is becoming increasingly difficult. For years, we have observed false flag activities, such as malicious software samples intentionally embedding Russian or other language words to mislead researchers and point them in the wrong direction.

With the development of AI technologies and proliferation of automated translation, attempting to deceive researchers trying performing attribution based on language is becoming increasingly difficult.

That said, general techniques can still be applied. When analyzing online conversations, it is often possible to link local events in specific regions to the potential physical location of the actors. Certain regional linguistic nuances, ideological expressions, or political associations can also help build a more confident profile of a threat actor's background.

How Changes in the Underground Affect Individuals and Businesses

Effect Risks and Mitigations for Internet Users

The recent changes in the Russian-speaking underground, along with the emergence of new technologies utilized by underground threat actors has increased the risks for ordinary people to be successfully targeted. We highlight some of these key changes for awareness:

- Technologies like AI allow the attackers to target internet users more precisely, using more attractive and well-prepared lures that incorporate local languages and cultural aspects.
- The appearance of high-resolution media, which includes biometric data, on social media platforms has made it easier for cybercriminals to impersonate individuals. When combined with leaked personal information – obtained via breaches or cyberattacks – and enhanced by AI, new opportunities for attackers have emerged. This involves the creation of highly convincing digital identities that can be used to conduct actions such as opening financial accounts on behalf of unsuspecting individuals.
- Criminals are also implementing complex, yet scalable monetization processes that target people across several forms of media and combining attack techniques to exploit a variety of human weaknesses simultaneously. For example, many evolved scams and fraud schemes contact victims and their relatives via messenger platforms, emails, calls, and SMS to improve the efficiency of such attacks.[38] Similar techniques are employed by hacktivism-driven actors, who are able to persuade their targets to conduct hacktivist actions on their behalf.
- Geopolitical unrest has led to the physical migration of underground actors, who are now starting to apply their knowledge and experience for implementing and adopting criminal business processes to their new environments. These new regions, which were previously unfamiliar with such scams, are often unprepared or less resistant (similar to the introduction of a new predator into an ecosystem). Reshipping fraud is a popular example of this trend.

A two-pronged approach – leveraging cutting edge security and anti-scam technology, while simultaneously enhancing awareness and the ability to spot cybercrime fraud red flags during the early stages of attacks – is key to minimizing the risk of successful attacks on ordinary internet users.

Effects on Cyber Risk Exposure Management (CREM) for Businesses and Governments

The combination of increased maturity, new financial capabilities, reshaped ties and ethical boundaries, closer international collaboration, deeper synergy, and the integration of cybercrime with nation-state-backed groups has significantly altered the cyber risk surface for organizations.

In doing so, it continues to challenge traditional defenses, leading to a more risk-driven approach to attack surface defense.

- Increased maturity and financial capabilities enable criminals to implement new and sophisticated monetization schemes that leverage more advanced tools, vulnerabilities, and exploits.

- Reshaped cultural ties and closer international collaboration have led to the appearance of attacker capabilities and criminal business processes that were previously unseen among actors from a particular geographical region.
- Changes in ethical boundaries have expanded the range of targets to include critical sectors and geographical locations that were considered off-limits in the past.
- The polarization of societies and geopolitical unrest can provoke new campaigns against business and government assets. A government decision or even a controversial claim from a company can turn organizations (including others in their industry) into the targets of criminal, hacktivist, state-sponsored, or hybrid attacks. For example, in August 2024, the French multinational insurance corporation AXA was targeted by hacktivists in response to the arrest of Pavel Durov.[39]
- Evidence of deeper synergy between groups with nation-state-aligned interests and cybercrime groups have been observed in underground forum interactions and in the traces of attacks in-the-wild. One example of such a collaboration occurs when a group aligned with the interests of a nation state, after completing its own mission on a target, resells access to a criminal ransomware operator. This can distract security teams with a more visible but unrelated security incident unless they have the maturity to handle these types of hybrid attacks. Conversely, the reverse can also occur, where a nation-states purchases access to sensitive targets that had previously been compromised by cybercriminal groups with financial motivations.

It is crucial for governments and businesses to employ a strong combination of leading security defense platforms, advanced threat intelligence, and human knowledge on strategic shifts in the threat landscape into their CREM procedures to address these ongoing changes. This is particularly important when dealing with the increased sophistication, capabilities, maturity, and synergy between criminal groups from different geographical regions and those aligned with nation-state interests.

Conclusion

Criminal communities are constantly evolving, particularly in Russian-speaking regions. The key drivers of this evolution are emerging technologies, new criminal business processes, and recent social and geopolitical changes.

Staying informed of these developments is important for businesses and governments, as most modern cyberattacks originate from, or have their roots in the Russian-speaking criminal underground. This thriving community acts as a hub where criminals can develop and monetize new attacks. The shifts we have observed are especially relevant for companies seeking to defend themselves from ransomware attacks, phishing attempts, scams, and innovative new cyberattacks. Understanding the enemy is the first part of defending against them.

The last few years have brought significant economic, geopolitical and technological changes that have left a significant imprint on how the underground community has evolved. The proliferation of Web3 technologies and cryptocurrencies has fueled a massive boom in services that support this ecosystem, including cash-out platforms and cryptocurrency mixers. Many legitimate online platforms operate exclusively with cryptocurrencies, leading to the emergence of a new market for phishing toolkits tailored specifically to address this cryptocurrency niche.

The significant changes in the geopolitical situation, particularly the introduction of sanction controls, have stimulated the criminal ecosystem. In particular, the sector of the cybercrime underground that provides services to bypass these restrictions – from online staffing services to financial system components – has become increasingly well -developed.

Conflicts such as the Russia-Ukraine war and unrest in former USSR states have redefined which regions and sectors are considered fair game for attacks. Previously, the "Do not work in RU" rule broadly covered Russian-speaking nations, but interpretations have evolved, excluding some areas while still enforcing restrictions for criminal operations that require Russian-speaking infrastructure, such as money laundering and intelligence collection.

The changing geopolitical landscape, combined with a reduction in law enforcement intervention, has led to a rise in violations of this rule. Cybercriminals and underground service providers are increasingly targeting both Russia and Ukraine, as seen in the growing number of job postings and malware offerings aimed at these regions.

Government-aligned threat actors and hacktivist groups have taken advantage of the underground market for their own objectives. State-affiliated actors seek to exploit criminal services for cyber operations, blending in with financially motivated attacks. Hacktivist movements have also gained momentum, using cyberattacks to further ideological or political agendas. These shifts have disrupted trust relationships within underground communities, forcing criminals to reconsider alliances and business strategies. Sanctions and financial restrictions have further complicated criminal operations, leading some cybercriminals to relocate to new regions, thereby broadening the reach of the underground market. These developments illustrate how geopolitical instability reshapes cybercrime, making it more unpredictable and intertwined with state-driven agendas.

Bulletproof hosting, as we knew it, no longer exists. While hosting services remain widely available in the underground, we have observed the appearance of multiple alternative solutions, including residential proxies, "secure workstation on the dark web," traffic mixers, reverse proxying, and other options that focus on addressing some of the bulletproof hosting needs of their criminal user base.

Information leaks driven by ransomware double extortion business models are widely monetized in combination with unintentionally exposed biometric data on social media and the emerging use of generative AI to create digital identities – both of real people and even nonexistent ones. These identities are then used for financial and cryptocurrency fraud, alongside extortion schemes.

The synergy between different cybercriminal linguistic groups and threat actors from non-cybercrime backgrounds is becoming increasingly evident. We have observed collaborations between actors aligned with nation-states interests and ransomware groups, allowing for the exchange of tradecraft and malware tooling. This trend is partially driven by economic changes in other regions, and partly by advancements in the ability to communicate naturally across different linguistic and cultural groups due to the development of automatic translation and AI tools.

Finally, the rapid development of AI technologies has significantly influenced the evolution of tools and services in the criminal underground, including the automation of search engine optimization (SEO) tools, fake news, disinformation toolkits. and more.[40]

A deep understanding of developments in the cybercriminal underground enables us to integrate this strategic and tactical threat intelligence into awareness programs and CREM, while also helping improve the cyber defense capabilities of governments, businesses, and ordinary individuals. The pace at which the modern underground evolves has significantly intensified, but so too have the innovations of organizations dedicated to preemptively defending against it.

Endnotes

1 Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin. (Sept. 3, 2024). *Trend Micro*. "UNWIRED: Understanding the Unforeseen Risks in Evolving Communication Channels." Accessed on Mar. 17, 2025, at: Link.

2 Ravie Lakshmanan. (Oct. 19, 2024). *The Hacker News*. "Crypt Ghouls Targets Russian Firms with LockBit 3.0 and Babuk Ransomware Attacks." Accessed on Mar. 17, 2025, at: Link.

3 Max Goncharov. (2012). *Trend Micro*. "Russian Underground 101." Accessed on Mar. 17, 2025, at: Link.

4 Max Goncharov. (2015). *Trend Micro*. "Russian Underground 2.0." Accessed on Mar. 17, 2025, at: Link.

5 Mayra Fuentes, Feike Hacquebord, Stephen Hilt, Ian Kenefick, Vladimir Kropotov, Robert McArdle, Fernando Mercês, and David Sancho. (2020). *Trend Micro*. "Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them." Accessed on Mar. 17, 2025, at: Link.

6 Vladimir Kropotov, David Sancho, and Fyodor Yarochkin. (2020). *Trend Micro*. "The Hacker Infrastructure and Underground Hosting: An Analysis of Ransomware Campaigns, Phishing, and Web Injects." Accessed on Mar. 17, 2025, at: Link.

7 Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin. (2020). *Trend Micro*. "The Hacker Infrastructure and Underground Hosting: Cybercrime Modi Operandi and OpSec." Accessed on Mar. 17, 2025, at: Link.

8 Wikipedia contributors. (n.d.). *Wikipedia*. "Russians in Finland." Accessed on Mar. 17, 2025, at: Link.

9 Randy Bush. (1992). *FidoNet*. "Randy Bush INET92 Paper." Accessed on Mar. 17, 2025, at: Link.

10 DosWorld. (n.d.). *GitHub*. "Infected.Voice." Accessed on Mar. 17, 2025, at: Link.

11 Brian Krebs. (June 13, 2011). *Krebs on Security*. "Organization Chart Reveals ChronoPay's Links to Shady Internet Projects." Accessed on Mar. 17, 2025, at: Link.

12 David Sancho and Vincenzo Ciancaglini. (Aug. 15, 2023). *Trend Micro*. "Hype vs. Reality: AI in the Cybercriminal Underground." Accessed on Mar. 17, 5, at: Link.

13 Vladimir Kropotov, David Sancho, and Fyodor Yarochkin. (April 3, 2023). *Trend Micro*. "Inside the Halls of a Cybercrime Business." Accessed on Mar. 17, 2025, at: Link.

14 Mayra Rosario Fuentes. (Feb, 28, 2023). *Trend Micro*. "The Gender-Equal Cybercriminal Underground." Accessed on Mar. 17, 2025, at: Link.

15 Stephen Hilt and Mayra Rosario Fuentes. (Jan. 7, 2025). *Trend Micro*. "Bridging Divides, Transcending Borders: The Current State of the English Underground." Accessed on Mar. 17, 2025, at: Link.

16 David Sancho and Mayra Rosario Fuentes. (Jan. 30, 2025). *Trend Micro*. "Across the Span of the Spanish Cybercriminal Underground: Current Activities and Trends." Accessed on Mar. 17, 2025, at: Link.

17 Federal Bureau of Investigation. (Jan. 31, 2014). *FBI*. "A Byte Out of History: $10 Million Hack, 1994-Style." Accessed on Mar. 17, 2025, at: Link.

18 Mayra Fuentes, Feike Hacquebord, Stephen Hilt, Ian Kenefick, Vladimir Kropotov, Robert McArdle, Fernando Mercês, and David Sancho. (2020). *Trend Micro*. "Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them." Accessed on Mar. 17, 2025, at: Link.

19 Craig Gibson, Vladimir Kropotov, Philippe Z Lin, Robert McArdle, and Fyodor Yarochkin. (Oct. 18, 2022). *Trend Micro*. "Leaked Today, Exploited for Life: How Social Media Biometric Patterns Affect Your Future." Accessed on Mar. 17, 2025, at: Link.

20 Vladimir Kropotov, Fyodor Yarochkin, Craig Gibson, and Stephen Hilt. (Sept. 27, 2022). *Trend Micro*. "How Underground Groups Use Stolen Identities and Deepfakes." Accessed on Mar. 17, 2025, at: Link.

21 Craig Gibson and Josiah Hagen. (June 28, 2023). *Trend Micro*. "Virtual Kidnapping: How AI Voice Cloning Tools and ChatGPT Are Being Used to Aid Cybercrime and Extortion Scams." Accessed on Mar. 17, 2025, at: Link.

22 Fyodor Yarochkin, Vladimir Kropotov, and Jay Liao. (Jan. 18, 2023). *Trend Micro*. "'Payzero' Scams and the Evolution of Asset Theft in Web3." Accessed on Mar. 17, 2025, at: Link.

23 Northwestern Oklahoma State University. (n.d.). *Northwestern Oklahoma State University*. "Maslow's Hierarchy of Needs." Accessed on Mar. 17, 2025, at: Link.

24 Aurimas Rudinskis. (Oct. 24, 2024). *Hack.lu 2024*. "Scam as a Service Powered by Telegram." Accessed on Mar. 17, 2025, at: Link.

25 Trend Micro. (Nov. 30, 2021). *Trend Micro*. "Investigating the Emerging Access-as-a-Service Market." Accessed on Mar. 17, 2025, at: Link.

26 Trend Micro. (Sept. 2, 2020). *Trend Micro*. "Hacker Infrastructure and Underground Hosting 101: Where Are Cybercriminal Platforms Offered?" Accessed on Mar. 17, 2025, at: Link.

27 Vladimir Kropotov and Fyodor Yarochkin. (Sept. 28, 2017). *Trend Micro*. "Business Process Compromise and the Underground's Economy of Coupon Fraud." Accessed on Mar. 17, 2025, at: Link.

28 Vladimir Kropotov and Fyodor Yarochkin. (Nov. 16, 2020). *Trend Micro*. "Cybercriminal 'Cloud of Logs': The Emerging Underground Business of Selling Access to Stolen Data." Accessed on Mar. 17, 2025, at: Link.

29 RootData. (Feb. 5, 2024). *RootData*. "RootData 2023 Web3 Research Report and Annual Rankings." Accessed on Mar. 17, 2025, at: Link.

30 David Sancho. (June 30, 2022). *Trend Micro*. "The Crypto-Monetized Web: A Forward-Looking Thought Experiment." Accessed on Mar. 17, 2025, at: Link.

31 Fyodor Yarochkin, Vladimir Kropotov, and Jay Liao. (Jan. 18, 2023). *Trend Micro*. "'Payzero' Scams and the Evolution of Asset Theft in Web3." Accessed on Mar. 17, 2025, at: Link.

32 OpenSea. (n.d.). *OpenSea*. "Collection Stats." Accessed on Mar. 17, 2025, at: Link.

33 The Moscow Times. (Jan. 19, 2021). *The Moscow Times*. "Russian Police Officer Suspected of Leaking Navalny Poisoners' Data." Accessed on Mar. 17, 2025, at: Link.

34 David Sancho. (Feb. 4, 2025). *Trend Micro*. "Understanding Hacktivists: The Overlap of Ideology and Cybercrime." Accessed on Mar. 17, 2025, at: Link.

35 Antoniuk, D. (Dec. 2, 2024). *The Record*. "Ransomware suspect Wazawaka reportedly arrested by Russia." Accessed on Mar. 19, 2025, at: Link.

36 Daryna Antoniuk. (Feb. 22, 2024). *The Record*. "Russia arrests three alleged SugarLocker ransomware members." Accessed on Mar. 17, 2025, at: Link.

37 Zack Whittaker. (Feb. 28, 2022). *TechCrunch*. "Conti ransomware gang's internal chats leaked online." Accessed on Mar. 17, 2025, at: Link.

38 Craig Gibson and Josiah Hagen. (June 28, 2023). *Trend Micro*. "Virtual Kidnapping: How AI Voice Cloning Tools and ChatGPT Are Being Used to Aid Cybercrime and Extortion Scams." Accessed on Mar. 17, 2025, at: **Link**.

39 David Sancho. (Feb. 4, 2025). *Trend Micro*. "Understanding Hacktivists: The Overlap of Ideology and Cybercrime." Accessed on Mar. 17, 2025, at: **Link**.

40 Trend Micro. (June 13, 2017). *Trend Micro*. "Fake News and Cyber Propaganda: The Use and Abuse of Social Media." Accessed on Mar. 17, 2025, at: **Link**.