Russian Language Cybercriminal Forums – Analyzing The Most Active And Renowned Communities

By Oleg

Published: 2024-02-08 · Archived: 2026-04-05 22:27:54 UTC

Chapter III. Exploring and comparing prominent Russian language cybercriminal forums.

Welcome to the third part of this series of OSINT investigations about the Russian language cybercriminal ecosystem and forums. In the first Chapter, we explored the origins of this ecosystem and uncovered how Russian language cybercriminal forums (RLCF) appeared, evolved and the current state they are in. In the second Chapter we assessed the “underground” nature of RLCF and of their economic functioning.

Today I would like to discover with you what I believe to be the most prominent RLCF and analyze their place in the wider Russian speaking cybercriminal ecosystem. We will try to assess the sizes of the audiences of the most prominent RLCF and identify what kind of "goods and services" are being traded on these forums.

If you have missed the previous Chapters do not hesitate to read them because many methodological concepts, such RLCF categories or their levels of activity are explained there and are indispensable for the understanding of this Chapter.

If you wish to discover the full list of the 94 studied RLCF, you can find it here.

Insights of the third Chapter:

- Currently, reputable RLCF are the primary platforms for threat actors engaging in commercial activities or seeking to purchase goods and services from other threat actors they do not trust. Although Telegram plays a significant role for cybercriminals, it faces inherent limitations, such as the absence of a trustworthy escrow and arbitration system.
- Despite the different nature of the studied RLCF, like carding or drug selling forums, there are notable similarities and connections between these communities. Common elements include the presence of bulletproof hosters and anonymous cryptocurrency exchange services, which link the entire ecosystem.
- While some RLCF boast massive communities, overall the number of highly skilled and proficient threat actors is relatively small, likely numbering in the several thousand. Conversely, RLCF focused on low-level fraud schemes, basic carding technics, or drug sales tend to attract larger communities.
- The Russian speaking cybercriminal ecosystem is well structured, with major communities gathering different types of threat actors:
    - “XSS” and “Exploit” stand as the core of the high-level cybercriminal underground focusing on hacking and malware. The reputation of “Exploit” has nevertheless suffered from repeated rumors about its control by law enforcement. The majority of threat actors present on these forums usually target non-Russian speaking countries.
    - “LolzTeam” is a learning place for wannabe cybercriminals and more importantly a workforce pool for infostealer distribution. However, the aggressive monetization policy implemented by moderators of this forum since the spring of 2023 has had a negative impact on the standing of this RLCF and has reduced the presence of infostealer Malware as a Service (MaaS).
    - "WWH-Club" is a large market specializing in carding services and is known as an educational hub for this illicit craft. Like "LolzTeam", albeit for different reasons, the monetization policy of “WWH-Club”'s staff has led to discontent among threat actors. They complain on other forums because access to arbitration is restricted to users with paid membership plan. Users of this forum target both Russian speaking countries and the rest of the world.
    - Fraud-oriented RLCF like "DarkMoney" or "Probiv" share similarities with other RLCF, as they attract threat actors specializing in fake document and financial fraud services. However, the

quantity and quality of these services are more extensive. Additionally, threat actors on these forums often target their own countries (former Soviet Union).

- Drugs-focused RLCF like "RuTor" primarily operate within the former Soviet republics and promote relatively low-level content from a technical perspective. Interestingly, "RuTor"'s staff encouraged its community to engage in carding attacks to help them earn money and even opened in 2022 a dedicated section with tutorials about carding and other fraud schemes.

I) Telegram – the new frontier for Russian speaking threat actors?

Before delving into an examination of major RLCF with high activity, let me recount an illustrative incident involving two renowned RLCF and a Telegram channel belonging to a MaaS. This incident underscores the enduring significance of prominent RLCF as public arenas for cybercriminal communication and collaboration. Despite Telegram's recent emergence as a vital tool in the cybercriminal landscape due to its leniency towards illicit activities[1], it cannot replace RLCF in the foreseeable future.

Let's journey back to February 2023 to revisit a misadventure that happened to one of the most renowned MaaS, namely, the Raccoon Stealer[2]. Since its launch, the group of cybercriminals developing this malware relies on Telegram for purposes including conducting transactions and providing customer support. Much like other clients of this MaaS, an individual operating under the alias "hash_attack" opted to initiate contact with the Raccoon Stealer's team through Telegram. This engagement was aimed at procuring advertising space for "hash_attack"'s bruteforce service on the exclusive Telegram channel belonging to the Raccoon Stealer.

However, this business transaction took an unfortunate turn, resulting in a discord between "hash_attack" and the Raccoon team. Frustrated by the situation, "hash_attack" decided to take a confrontational stance by publicizing the dispute on one of the RLCF where he was present. Although, "hash_attack" had accounts on the majority of RLCF such as “XSS”, “WWH-Club” or “BHF”, where Raccoon Stealer’s representatives were also present, the threat actor choose to open an arbitration thread on “Exploit”, which highlights the trust of this cybercriminal in this community to help him solve his problem.

Figure 1. The threat actor “hash_attack” opened an arbitration thread against Raccoon Stealer on Exploit.

"hash_attack" raised allegations against the Raccoon team, claiming that they failed to refund him 3,000 dollars following a disagreement concerning an advertising arrangement. Although the monetary value involved in this dispute may appear relatively inconsequential in comparison with the revenues generated by this successful MaaS, the moderators of the "Exploit" forum deemed the refusal to return the funds as a potential scam attempt. Consequently, they took the step of banning the "raccoonstealer" account from their forum.

In a rapid sequence of events, the administration of the "XSS" forum, which maintains a cooperative relationship with "Exploit" and even shares at least two moderators in common with this RLCF, chose to follow suit by banning "raccoonstealer"'s account from their platform as well. This chain reaction underscores the

interconnectedness of some cybercriminal forums. After this harsh punishment Raccoon Stealer's staff decided to give back the 3,000 dollars to "hash_attack" but could not recover their accounts on these two prominent RLCF.

On February 15, 2023, the prominent threat actor "Stallman", who is the current administrator of the ransomware-centric forum "RAMP", initiated a discussion on the "Exploit" forum in support of the Raccoon Stealer team. Prior to this incident, "Stallman" has publicly endorsed Raccoon Stealer on multiple occasions, professing it to be his preferred information-stealing malware. In a personal effort to assist Raccoon Stealer in regaining access to both "Exploit" and "XSS", "Stallman" advocated on their behalf. Nevertheless, even this intervention proved ineffective in achieving the desired outcome.

Figure 2. The threat actor Stallman opened a thread on Exploit to ask its administration to lift the ban of raccoonstealer's account.

Raccoon Stealer's reputation took a clear hit, as new accusations followed both on "XSS" and "Exploit". Several users claimed that Raccoon Stealer is stealing crypto wallet's information from the logs of its own customers and sending them directly to the developers of this malware, depriving thereby the cybercriminals who have purchased this MaaS from a source of income. Without a presence on these forums, the Raccoon team was not able to defend itself against these accusations.

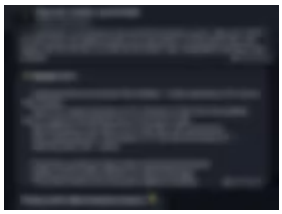

Figure 3. Raccoon Stealer continued to operate and sell their malware on Telegram even after the ban on XSS and Exploit in February 2023.

Eventually, after suffering a six-month absence from "XSS" and "Exploit", Raccoon Stealer was allowed to return to these RLCF after making a deposit of 1 BTC (around 25,000 dollars in August 2023) on each forum[3]. It is necessary to note that although some newspapers published somewhat misleading titles announcing the "return" of Raccoon Stealer after the end of the ban, this MaaS never stopped operating. Its development continued, and it was always possible to purchase a subscription via its official Telegram channel. Thereby, the decision of the Raccoon team to accept the conditions of these RLCF suggests that a presence on these platforms is of substantial importance for MaaS and other advanced threat actors.

Figures 4 and 5. “raccoonstealer” was allowed to return to “XSS” and “Exploit” in August 2023 after the group made a deposit of 1 BTC on each of these forums. Auto translated from Russian.

These events underscore several noteworthy aspects that elucidate why, despite the emergence of Telegram and its popularity among threat actors, RLCF continue to be indispensable for conducting illicit activities.

- Major RLCF are a source of legitimacy and lead generation: The decision made by Raccoon Stealer to invest nearly $50,000 to regain access to "XSS" and "Exploit" offers a compelling insight into the importance of these platforms for cybercriminals. Establishing a presence on prominent RLCF not only grant legitimacy but also serves as a prime source for lead generation. Threat actors seeking to offer services, distribute malware, or secure employment, recognize the pivotal role of these forums.

- Major RLCF ensure security of transactions: Another crucial aspect to consider is that Telegram currently lacks a credible escrow system (for more details about the escrow system see Chapter II). Consequently, threat actors and MaaS vendors seeking secure transactions often prefer to conduct their business through reputable forums that offer escrow services.

- The longevity of major RLCF allows them to acquire and maintain a reputation: The reputation and (supposed) integrity of major RLCF, cultivated over time and through a proven track record, stand as a pivotal differentiator with other RLCF and also Telegram groups and channels.

Although prominent RLCF are essential to the Russian speaking cybercriminal ecosystem, we will discover that not all major RLCF are equal. They occupy distinct niches, gather different types of threat actors, and vary in reputation and trustworthiness within the ecosystem. Understanding these distinctions is crucial for comprehending the dynamics of the cybercriminal landscape.

The Russian language cybercriminal ecosystem exhibits a well-structured framework, characterized by the diverse audience and services prevalent on each forum. Our analysis will scrutinize the unique roles played by these forums, providing valuable insights into their significance within this intricate landscape.

II) Key Russian language cybercriminal forums and their role in the ecosystem.

You may legitimately ask how exactly one can assess the role of a RLCF and compare it with another one, or how to determine which forums are the most prominent in their own area of specialization?

To address this question, I suggest utilizing objective indicators, such as the level of activity, the type and quantity of “goods and services” that can be found on these forums, along with more qualitative assessments like the community reputation or the technical expertise of the userbase. To conduct this analysis, I preselected 8 highly active and qualitative forums from 5 categories (see the methodology in the first Chapter – categories: Cybercrime, Fraud, Carding, Other/Cybercrime and Drugs. Programming cybercriminal forums are excluded because none is presently highly active).

Expanding the excerpt of studied RLCF to communities with a small userbase and lower activity, provided they housed highly skilled threat actors, as exemplified by the ransomware-focused forum "RAMP”, was also an option. However, I ultimately decided against this approach due to the niche nature of these communities. For

instance, “RAMP”, with an annual active userbase of approximately 300 members who posted slightly over 3,000 messages in 2023, serves as an illustration of the limited scope and engagement within such forums.

III) Quantitative analysis – how big is the user base of major RLCF?

To assess the “active user base” of major RLCF my first idea was to count members that have posted at least one message in 2023. This approach is, of course, questionable as some forum users can be active only in private messages and would thus be excluded from my assessment. Furthermore, a single person can have several accounts and write messages from each one of them.

An alternative idea was to rely on the official forums’ statistics, namely the counting of registered accounts during 2023. After exploring this assessment method, it appeared that it can be even more unreliable in some cases. For instance, during the first half of 2023 the RLCF “Exploit” conducted a spring cleaning by deleting around 30,000 accounts, which then represented over one third of the total number of registered members.

I choose to cut the Gordian knot by selectively using both methods while remaining consistent and trying to provide a reliable assessment of the activity of each studied RLCF.

Communities from within the Cybercrime, Carding and Fraud, categories, like "XSS", "WWH-Club" or “DarkMoney”, presented in the Table 2, are comparatively much smaller than the RLCF from the Other/Cybercrime and Drugs categories, such as "LolzTeam" and "RuTor", presented in Table 3. Thereby, in Table 2 the size of the community was assessed via a counting of active users that have published at least one message in 2023. On the contrary, counting active users on forums with audiences exceeding several hundreds of thousands of active users, that are present in Table 3, was technically challenging and I decided to rather count the number of new accounts registered in 2023. The magnitude of the discrepancy in the userbase sizes between the major RLCF from Table 2 and Table 3 is so significant that this difference of datasets is in fact almost irrelevant.

The results I've uncovered closely resemble the data presented by Searchlight Cyber in the spring of 2023[4]. However, it is important to keep in mind that the methodology employed by this company for their analysis remains undisclosed. Therefore, I encourage readers to view these numbers as indicative rather than precise measurements.

Table 2. *Methodology: a user is considered as active in 2023 if he has published at least one message.

The observations of Tables 2 and 3 provide some insights about the sizes of each community, nevertheless this approach does not tell us anything about who “inhabits” these RLCF. This stresses the necessity of adopting a more comprehensive evaluation strategy that encompasses both quantitative and somewhat qualitative factors to gain a deeper understanding of RLCF’s roles within the cybercriminal landscape.

IV) Focus on commercial threads – a combination of qualitative and quantitative analysis.

An approach, which offers a more detailed and somewhat qualitative perspective, involves the analysis of new commercial threads published in 2023. Counting the threads where threat actors engage in selling or buying something is an effective way of gaining insight into the specialization of each community, facilitating comparisons between them.

However, it is essential to note that this approach doesn't consider older, yet active commercial threads created before 2023. Assessing these threads would require individually verifying whether the thread creators still engage in trading the offered goods or services, a task beyond the scope of this analysis. Additionally, this approach doesn't provide insights into the quality and complexity of the items or services being sold.

After gathering the commercial threads, they were organized into eight distinct trade categories for analysis. The figures presented bellow, while informative, should be regarded as indicators and not as a perfect representation of commercial activities within the forums. Please note that content related to drugs, arms, or violence was deliberately excluded from this study, even though these crafts represent the core activity of RLCF like “RuTor”.

- **Hacking**: threads related to the sale of malware, information-stealers distribution, databases, accesses to corporate networks, pentest, DDoS, hash cracking, sales of stollen accounts;
- **Banking fraud**: commercial threads that involves an activity focused on banking fraud with stolen credit cards and the proceeds of this malicious craft;
- **Fraud services**: commercial threads related to the sale of fake documents, lookup services, SIM cards trafficking, phone calls, spam services;
- **Financial services**: threads where threat actors sell money and cryptocurrency laundering services, cash in and cash out services, fake identities for tax fraud;
- **Hosting services**: threads where threat actors sell virtual private servers, proxies, and other hosting related services including bulletproof servers and domains;
- **Other services**: commercial threads with content related to Social Media Marketing (SMM – sale of fake audience, likes and comments on platforms such as YouTube), web development, etc.

Additionally, two other categories were established to account for uncategorized commercial content, including material that forum members were unsure where to post, as well as job posting and job searches. These categories help encompass content that doesn't neatly fit into the predefined trade categories.

Table 4. *For the RLCF RuTor, drugs, violence, and human trafficking related content were not counted.

Table 5. *For the RLCF RuTor, drugs, violence, and human trafficking related content were not counted.

Based on the statistics presented in Tables 2, 3, 4 and 5, one can make several observations. Even the most active RLCF, with communities focusing on Hacking, gather only several thousand active users. Conversely, RLCF popular among drug consumers and younger individuals tend to amass large audiences primarily focused on low-level content and fraud schemes. Even though not all members of advanced threat groups are directly present on RLCF, it is intriguing to consider that the significant damage inflicted by Russian speaking ransomware groups, malware developers and distributors or carders, could be predominantly caused by a relatively small number of individuals.

Moreover, the analysis of Tables 4 and 5 reveals several findings. Remarkably, there has been an evolution in the drugs forum "RuTor" since 2022, as it has expanded by introducing carding and fraud sections. However, overall, it becomes clear that commercial threads (excluding drug sales) are not abundant, even on forums with massive communities such as "LolzTeam" or "RuTor" (see Tables 2 and 3). This observation reinforces the argument made in Chapter I, that RLCF categorized under Other/Cybercrime and Drugs are only marginally involved in the same illicit activities as forums categorized under Carding, Cybercrime, or Fraud and are not necessary to attract the same type of threat actors.

A closer examination of threads in the jobs category supports this assessment. The employment opportunities offered on RLCF like “RuTor”, and to a lesser extent “Probiv” or “DarkMoney”, are primarily low-level technical roles focused on tasks like malware distribution and fraud schemes. In contrast, job advertisements on "Exploit" or "XSS", involve more technically sophisticated roles, with threat actors capable of creating advanced malware or executing complex network penetration tasks.

However, there are also similarities and connections among all the studied RLCF. A review of Tables 5 and 6 highlights the consistent presence of Financial and Hosting services across all RLCF. In fact, a detailed examination of hosting and cryptocurrency laundering services reveals that the same actors engaged in providing these services actively participate on all major RLCF.

Table 6. *Threat actors that are openly claiming to sell bulletproof hosting services and that were active at least once from December 2022 to March 2023.

An in-depth analysis of hosting and cryptocurrency laundering services is planned for the current year. What can already be mentioned is for example the presence of the "AudiA6" crypto exchange service across a minimum of 44 RLCF. This account offers an anonymous money and cryptocurrency exchange service and has been active for over ten years (see Figure 6). In the realm of bulletproof hosting services, it is worth noting the case of a service promoted under the pseudonym "Quahost," which is documented across a minimum of 31 RLCF and has maintained its operations for over fifteen years (refer to Figure 7).

Figure 6. AudiA6 mentions on XSS all the RLCF where he deposited money as a warranty. Auto translated from Russian.

Figure 7. An advertisement of Quahost’s bulletproof servers on LolzTeam from 2018.

To conclude we can already state that each of these communities plays a distinct role and has its own place within the broader cybercriminal ecosystem. Though RLCF are qualitatively and quantitatively different, each of them is nonetheless important in its own manner for the whole ecosystem. For instance, "LolzTeam", which mainly focuses on low-level cybercriminal content, serves as a starting point for many young Russian speaking individuals who begin their cybercriminal activities on this forum, notably by joining traffers[5] teams.

V) Qualitative analysis of major RLCF.

In the upcoming sections, I will present a qualitative analysis of significant RLCF. We will briefly delve into various prominent communities, assessing their reputation, the technical knowhow of their members, and the nature of the trade occurring within these forums.

A) “XSS” and “Exploit”: The backbone of the high-level Russian speaking cybercriminal ecosystem.

Established in 2004 and 2005, "XSS" and "Exploit" stand as among the oldest and most esteemed RLCF. These forums draw in a larger number of technically proficient cybercriminals compared to other RLCF and serve as significant hubs for illicit services and employment opportunities related to hacking and malware.

Table 7. *Methodology: a user is considered as active in 2023 if he has published at least one message.

1) XSS – The “place to be” for high-level threat actors.

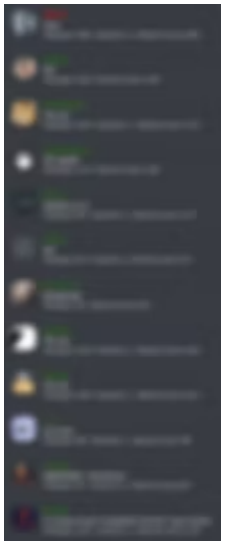

Figure 8. XSS staff in January 2024.

a) The origins of a veteran RLCF – from DaMaGeLaB to XSS.

"XSS" is among the oldest Russian language cybercriminal forums and has a rich history. According to "toha", the current administrator of "XSS", the forum was launched towards the conclusion of 2004 under the domain "winux.net.ru". It was then a personal project of the first administrator of the forum, the threat actor "Winux". Latter on he was joined by the threat actors "Great" and "Одинокий Волк" ("Lonely Wolf"), who became joint administrators[6].

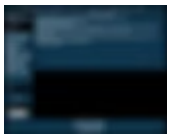

Figure 9. Archived version of the forum that will later become XSS.

Between 2006 and 2018 the forums was known under the name "DaMaGeLaB" and was accessible via the domains "damagelab.org" and "damagelab.in". At that time, one of the administrators of “DaMaGeLaB” was the Belarussian threat actor Mr. Sergei Yarets, operating under the alias "Ar3s"[7]. Mr. Yarets was arrested for his engagement in technical support for the loader Andromeda, which was considered as one of the largest botnets on the Internet at that time. He was rapidly released in 2018, which sparked rumors about a possible cooperation between Mr. Yarets and law enforcement agencies after he supposedly shared significant information about other members of the Andromeda team[8].

Figure 10. Screenshot of DaMaGeLaB from 2006.

After the arrest of "Ar3s" in November 2017, the forum was shortly under the control of the threat actor "Chococream" until its closure. The downfall was not definitive and a new iteration of the community appeared in 2018.

Figure 11. On the 21st of November 2018, the new administrator of XSS announces the reboot of the DaMaGeLab forum under the new name XSS. Auto translated from Russian.

The revival of the forum was made possible through a backup of “DaMaGeLaB”, which was generated back in 2015. This backup was reportedly handed over or sold by Mr. Yarets to his longtime acquaintance, a threat actor known as "toha”, which allowed him to relaunch the forum under the new name "XSS" in November 2018[9]. “toha” is also known in the cybercriminal community as the former owner of another renowned RLCF called "Exploit". It is believed that the collaboration between "toha" and Mr. Yarets began on "Exploit", where "toha" appointed Mr. Yarets as a moderator.

Interestingly, it appears that "toha" drew inspiration for the name "XSS" from the domain xxs.ru, which was associated with an older Russian forum called Web-Hack.ru, dedicated to hackers and information security experts. This forum was managed by an individual known as "Terabyte" from 2001 to 2010[10], and "toha" served as a moderator there as well.

According to revelations from the researcher "3xp0rt", the real identity of "toha" could be Mr. Anton Avdeev, and it is alleged that this threat actor resides in Russia[11]. (*Editor's note, 2025: The true identity of "Toha" was disclosed after his arrest in Ukraine on July 22, 2025. He was identified as Anton Gannadievich Medvedovskiy, 38, a resident of Kyiv. Anton Avdeev was a moniker).*

Figure 12. The researcher 3xp0rt is exposing Russian threat actors since the beginning of the Russian invasion of Ukraine.

b) Access to XSS and particularities of this RLCF.

In the present day, accessing the content of "XSS" necessitates registering an account, a process generally straightforward unless registrations are temporarily closed. A restricted section exists, accessible exclusively to designated members. Currently, the forum stands as one of the most active cybercriminal communities, offering automated escrow services to its users. Notably, it distinguishes itself by possessing an XMPP server that serves its community under the domain "@thesecure.biz".

For its own safety, the administration of "XSS" prohibits on engaging in any activities or selling data that could negatively impact the former Soviet countries, except the Baltic States.

c) XSS: a forum attracting high-profile threat actors.

While "XSS" stands as one of the most significant RLCF, its community size and message volume are relatively modest when compared to other Russian language cybercriminal forums. The forum's prominence lies in several key aspects, including the presence of high-profile threat actors, its robust knowledge base, and the perceived integrity of its administration. This last factor holds paramount importance in the cybercriminal realm because administrators of such communities must inspire trust by impartially investigating disputes and ensuring a minimum level of protection and anonymity for their members.

Renowned threat actors, including public representatives of ransomware gangs and administrators from other RLCF, maintain a presence on "XSS." Some of the most notable figures include affiliates of the LockBit, ALPHV or other ransomware groups, as well as the current owner of the "RAMP" forum, the threat actor "Stallman". Their participation on "XSS" serves both their operational needs and enhances their reputation within the cybercriminal ecosystem. "XSS" plays a substantial role for these threat actors because it serves as a platform for promoting affiliate programs, sell illicit services and malware, and of course, for communication with fellow cybercriminals. Additionally, it serves as a vital space for dispute resolution and the initiation of disinformation campaigns against rival actors.

Figure 13. Examples of arbitration threads opened on XSS. Auto translated from Russian.

One of these disinformation campaigns occurred in January 2022[12] and targeted the threat actor “KAJIT”, who was then the administrator of the RLCF “RAMP”. This dispute can be considered without exaggerations as anthological. It involved the representatives of the Ransomware as a Service (RaaS) LockBit, who accused “KAJIT” to be an infiltrated police agent. “LockBitSupp” got the upper hand as “KAJIT” got banned and the “XSS”’s administrator advised “KAJIT” to sell his forum “RAMP” to the threat actor “Stallman”, because no one trusted him anymore.

Figure 14. Stallman, the present administrator of RAMP, refutes the accusations of LockBitSupp against KAJIT and reaffirms that RAMP is not under the control of police. Auto translated from Russian.

d) XSS: an important illicit services and job market.

As displayed in the Table 8, the commercial threads advertised on “XSS” in 2023 illustrate that it is an all-round cybercriminal community, gathering carding specialists, initial access brokers, MaaS developers and other cybercriminal specialists. These categories encompass a large panel of cybercriminal activities that can be complementary.

For example, on “XSS” a cybercriminal can purchase a clean Cobalt Strike license, buy 0-day vulnerabilities, customized malware or subscribe to a MaaS and acquire an obfuscation service to evade antiviruses. To hosts their Command-and-Control servers (C2) cybercriminals can choose from a large inventory of bulletproof hosters. Eventually, once their activity has been monetized, threat actors can clean their cryptocurrencies or dirty money by contacting laundering services present on the forum.

Figure 15. The threat actor johndoe7 is selling Cobalt Strike licenses. Auto translated from Russian.

Figure 16. The threat actor backdoorseller is ready to sell a RCE exploit for 25,000 dollars.

Figure 17. The threat actor hackerGPT is ready to buy a 0-day exploit for up to 500,000 dollars.

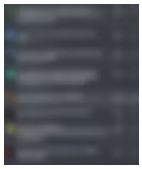

Figure 18. Example of MaaS and other services sold on XSS.

“XSS” and “Exploit”, although separate forums, closely cooperate in enforcing their rules. If a member is found to be involved in scams or rule violations on one forum, the other is likely to ban him as well, especially if a connection between his accounts is evident, such as having the same username or identical contacts. This cooperation is partly explained by the forums' shared history and the presence of moderators who serve on both platforms, like "Quake3" and "weaver". In January 2024, there was a highly publicized instance of this cooperation when "Exploit" also banned LockBit's representative account from the forum after he had been initially banned on "XSS”[13].

2) Exploit – A selective but successful high-level RLCF.

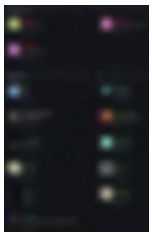

Figure 19. Staff members of Exploit.

a) Origins of one of the oldest and famous RLCF.

Launched around April 2005 under the name “Hack-All”, “Exploit” is another veteran RLCF. The forum changed its name after the control over the domain hack-all.net was purportedly stolen in 2006 [14], then the forum moved to the new domain exploit.in[15] and officially rebranded in February 2006. The forum also belonged to the threat actor “toha” until he allegedly sold it to “well known and trusted partners” in May 2018.

Figure 20. The first version of Exploit forum (then named Hack-All) in May 2005[16]. Auto translated from Russian.

b) Rumors running around Exploit – Under the control of law enforcement?

The transfer of “Exploit” to new management in 2018 stirred a significant amount of criticism and skepticism, primarily due to the undisclosed identities of the new owners. Speculations and rumors about a potential takeover by Russian or Ukrainian security services began to spread and have periodically resurfaced.

Figure 21. Exploit in 2024.

The rumors about the control of “Exploit” by law enforcement started to spread after the forum’s XMPP servers (@exploit.im) encountered unexpected and unexplained technical problems during the summers of 2018 and 2019.

According to the Russian hacker Mr. Andrei Sporov, aka “Sp0raw”, “Exploit” was infiltrated by the Security Service of Ukraine at least from 2015[17]. Indeed, the hacker claimed back in 2019 that “Exploit”’s moderator and then hoster “Whost”, was collaborating with the Ukrainian police after his arrest[18]. These allegations are unverifiable, but a substantial part of the cybercriminal community trusts them[19].

Figure 22. The threat actor Whost tried to plead, to no avail, that he has nothing to do with the FBI. Exploit members believed that although Whost was arrested in Ukraine, the FBI was behind the operation. Auto translated from Russian.

The most recent wave of rumors regarding “Exploit”'s control by law enforcement agencies emerged amid the Russian invasion of Ukraine in October 2022. Pavel Sitnikov, a pro-Russian individual and the administrator of the Telegram channel "Freedom Fox", specializing in cybercrime-related topics, asserted that “toha” had sold “Exploit” to the Security Service of Ukraine[20]. Following a public denial by “toha”, Mr. Sitnikov subsequently retracted his accusations. It is essential to acknowledge that these assertions may be a part of a disinformation campaign, and there are also unsubstantiated claims suggesting Russian Federal Security Service involvement in controlling "Exploit".

c) Access methods to Exploit and particularities of this RLCF.

Since 2018 and the arrival of the new owners, several changes have been made. The new administrators have implemented a registration fee of $100 to all new users to deter potential scammers and inexperienced threat actors from joining ($200 in 2024). However, newcomers can get a free membership if they hold administrative or moderator roles on other "friendly" forums or can demonstrate that they have knowledge in a field related to malware, software development, or hacking.

Additionally, "Exploit" has two closed sections: the "1st Access Level" and "2nd Access Level". The "1st Access Level" is password-protected, and a user can obtain the password after posting 50 messages. The "2nd Access Level" is accessible only to trusted and verified members who have been endorsed by forum members with access to this restricted level and by administrators.

Similarly to “XSS”, the targeting of countries with Russian speaking populations is heavily restricted[21].

Figure 23. First level password requirement.

d) Exploit – a key place for high-level cybercrime.

Figure 24. Lockbit's representative account on Exploit before it was banned on the 31st of January 2024. The threat actor used as a profile picture the photo of the cybersecurity expert Mr. Jon Dimaggio.

Very much like "XSS", "Exploit" is an important hub for advanced threat actors such as ransomware gangs, malware developers and initial access brokers. The same actors as on "XSS" can be found under identical or different handles on "Exploit". The relative selectivity of this RLCF facilitates the development of advanced content and gives its members access to a knowledge base.

Figure 25. Exploit features sections dedicated to providing knowledge on various valuable topics for hackers. Auto translated from Russian.

For instance, a substantial quantity of malware source code is freely available for members. Threat actors can then adapt the code to their own needs and develop new malware. The builder of the LockBit Black 3.0 or Babuk ransomwares, the source code of stealers, botnets and RATs are shared and discussed on "Exploit". Detailed tutorials about the exploitation of vulnerabilities in web applications or different types of software can also be easily found.

Figure 26. A threat actor published a reverse analysis of the Amadey loader. Auto translated from Russian.

e) Exploit: a key illicit services and jobs market.

As shown in the Table 9, with a total of over 12 thousand topics created during 2022, "Exploit" is a key public platform for cybercriminals. Auctions, job advertisements, spam distribution, and stolen logs are the most widespread topics on the marketplace. Some themes related to banking fraud are nevertheless restricted on "Exploit" which explains why no category reserved to carding exists on the marketplace.

The "Auctions" section of "Exploit" is mainly filled with corporate access for sale. These accesses are belonging to a variety of companies, from very small ones to huge multibillion transnational firms. Less frequently threat actors put up for auction stolen databases or banking information.

Figure 27. Auctions on Exploit are mainly composed of topics linked to the sale of access to companies' infrastructure, databases, credit cards dumps and fake documents. Auto translated from Russian.

The “Job” section contains hundreds of topics created by cybercriminals looking for malicious code developers and of threat actors searching for an employer and advertising their capabilities. The “Other” section includes around a thousand threads with different tools such as parsing scripts, log checkers, antidetection browsers, and lookup services. The “Access” section is small because on “Exploit” most transactions related to corporate accesses are rather occurring in the “Auctions” section.

Figure 28. A threat actor with a 1 BTC deposit advertises his coding capabilities. Auto translated from Russian.

Although not as famous as “XSS” or “Exploit”, who almost acquired a worldwide mediatization thanks to the presence of major ransomware threat actors, other RLCF play a central role in the cybercriminal ecosystem and need to be briefly mentioned.

B) LolzTeam aka “social engineering” forum – the realm of traffers and young cybercriminals.

As previously mentioned, RLCF within the **Other/Cybercrime** category were not originally created exclusively for cybercriminal activities. In fact, most of these forums began as discussion platforms for gamers and teenagers. However, their administrators recognized that permitting cybercriminal activities to flourish on their forums could draw a larger audience and generate additional revenue. The undeniable leader among these forums is "LolzTeam", not only because of its vast community but also due to the pivotal role it plays in the broader Russian language cybercriminal ecosystem.

The success of "LolzTeam" has motivated other threat actors to establish their own versions of this community in an attempt to attract a similar audience. An example is the "Lozerix" forum, launched in 2021. "Lozerix" even endeavors to replicate the structure and appearance of "LolzTeam" but is currently far from achieving the same level of success. Another case is the RLCF “Mipped” that is very lowly active comparatively to “LolzTeam” and very active comparatively to “XSS” or “Exploit”. A qualitative analysis of this forum, primarily centered around video game hacking and cheating, suggests that "Mipped" is uninteresting for further discussion in this paper.

1) LolzTeam – a giant community that marginally focuses on cybercrime.

Established in 2013 by Mr. Grisha Sutchkov, "LolzTeam" also known as "Zelenka", is currently one of the most popular Russian language forums. Boasting a community of approximately 250,000 daily visitors, the forum has essentially evolved into a kind of social network for teenagers. While the vast majority of members of this forum are uninvolved in any illicit activity, a minority of cybercriminals specializing in various forms of low-level fraud, traffic generation (traffers) and accounts theft is active on this board.

Figure 29. LolzTeam in 2024.

According to official statistics, 65% of “LolzTeam”’s members originate from Russia, 20% from Ukraine, and the remainder from other former Soviet republics such as Belarus[22]. The majority of visitors fall within the 16 to 25 age range, which aligns with the forum's primary thematic focus. “LolzTeam” primarily delves into topics related to competitive video games, cheating tools, and in-game items (character attire, weapons, and other items commonly referred to as "loot" in English).

Lately the reputation of this RLCF among cybercriminals has suffered from the aggressive monetization policy of its administration that targets MaaS sellers.

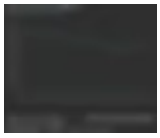

Figure 30. Official activity statistics of LolzTeam – May 2023.

Blue line - number of daily visitors. Green line - number of daily views.

2) The inception of a “social engineers” (fraudsters) community inside LolzTeam.

Since its inception, in addition to the development and sale of goods and services related to video games, the community gradually began selling stolen Steam and social network accounts. This shift towards hosting a cybercriminal community began around 2016 when the forum's administration started publishing tutorials on how to steal social network accounts and conduct small-scale fraud schemes. Contrary to “XSS” or “Exploit” targeting Russian speakers is an accepted and widely popular activity for threat actors active on “LolzTeam”.

Various fraudulent methods, such as the notorious "Antikino" technique, are frequently discussed and popularized on this board[23]. This method involves extorting money from a victim by convincing them that they are purchasing a cinema ticket for a first romantic date. Typically, the victim has met an attractive individual on a dating app and, at their proposal, agreed to a first date at the cinema. After asking his victim to purchase tickets on a fake cinema website, the charming individual ceases all communication. The manipulation of victims through various forms of social engineering constitutes a substantial part of illicit activity within “LolzTeam”.

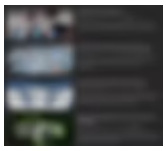

Figure 31. Blog posts published by the administration of LolzTeam in 2016. Auto translated from Russian.

To bolster the development of the sale of legitimately owned or stolen accounts, an entirely separate marketplace was created by “LolzTeam”’s administration[24]. In February 2024, reportedly 282,999 social networks and gaming platform accounts are for sale on the marketplace belonging to “LozlTeam”. The most popular ones are Steam, Vkontakte, Telegram and TikTok accounts.

Figure 32. Allegedly, 282,999 stollen and legitimate accounts are for sale on the dedicated marketplace belonging to LozlTeam in February 2024. Auto translated from Russian.

3) LolzTeam - Traffer's realm.

Beyond these minor frauds, more dangerous activities involving the sale of infostealers and advertising of traffers teams have appeared on "LolzTeam". "Traffers" are cybercriminals seeking to distribute malicious software, often by exploiting well-established YouTube, Instagram or TikTok accounts with an important user base. Typically, they will post attractive content, such as an advertisement for a "free Photoshop license" with URLs in the comment redirecting to a malicious website or a file infected with infostealer malware. For instance, a stolen YouTube account with 172,000 subscribers was put up for sale for approximately 550 dollars on "LolzTeam" and could have been used precisely for this purpose.

Figure 33. A threat actor was selling in March 2023 a compromised YouTube account with 172,000 subscribers for 550$.

Our observations lead us to conclude that "LolzTeam" plays an interesting role in the Russian speaking cybercriminal ecosystem for recruiting traffers and assembling dedicated teams. This lead generation activity is subsequently leveraged by other cybercriminals who, for example, purchase logs or develop infostealers. Presently, an entire section is dedicated to this type of activity, with numerous teams recruiting new traffers and offering to educate beginners.

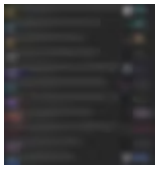

Figure 34. Traffers teams recruiting new members on LolzTeam. Auto translated from Russian.

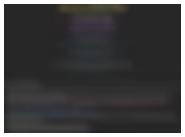

Figure 35. A traffer's team recruiting new members on LolzTeam. Auto translated from Russian.

The barrier to entry in this cybercriminal activity is in fact very low as detailed manuals, explaining what a traffer's job is and how to do it are freely available on the forum[25].

Figure 36. A detailed tutorial explaining how to become a successful traffer that was shared on LolzTeam. Auto translated from Russian.

4) LolzTeam – an important hub for beginner fraudsters and wannabe cybercriminals.

The commercial threads published on “LolzTeam” in 2023, as shown in Table 11, highlight the presence of cybercriminal activities related to traffers, infostealers, and associated services like log parsing and crypto wallet verification. In contrast, sections dedicated to jobs and services focused on programming, phishing, and scripting are less popular and less technically advanced than on other prominent RLCF.

5) Mr. Grisha Sutchkov at a crossroad?

When he created “LolzTeam” in 2013 at the age of 15, Mr. Grisha Sutchkov did not expect his project to become as popular and successful so swiftly, nor that his forum will later become a hub for cybercriminals. These facts and the young age of Mr. Sutchkov probably explain why, contrary to other RLCF administrators, he openly shared a significant amount of personal information, eventually becoming a sort of celebrity within the community he has created. Members of "LolzTeam" actively follow Mr. Sutchkov on social networks and have even created numerous memes featuring his photos.

In his interview in April 2023[26], Mr. Sutchkov seems to acknowledge that the income generated by his forum could be seen at best as "gray" which puts him in a complicate position with his country’s authorities. The administrator of “LolzTeam” may need to decide in the coming years between continuing to promote cybercriminal activities or exploring alternative monetization methods.

Since 2022, there has been a noticeable decrease in content related to infostealers and traffers on "LolzTeam". This may suggest that the administration has chosen to limit the amount of illicit content on the forum. Another possible explanation is the reported aggressive monetization approach targeting MaaS sellers on "LolzTeam". According to threads on other RLCF[27], infostealers developers have voiced concerns since May 2023 about being repeatedly scammed by "LolzTeam" moderators, who frequently close their commercial threads under various pretexts and request payments to allow them to pursue their activities on the forum. This situation has evidently had a detrimental impact on the reputation of "LolzTeam" among cybercriminals.

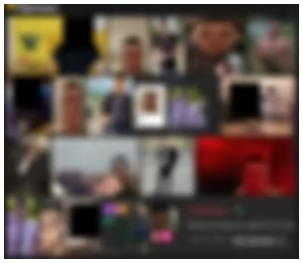

Figure 37. Examples of photos and memes that can be found online with the search “lanskoy” on Yandex (one of Mr. Sutchkov's handles).

C) Banking fraud and carding RLCF.

There are numerous RLCF primarily specialized in carding, with approximately 20 active communities identified. However, their levels of activity vary. Nowadays, only about three forums are highly popular, namely “WWH-Club”, "Club CRD" and “CrdPro”, with the latter being mainly frequented by English speakers. These communities offer access to a wealth of knowledge about credit and gift card theft and fraud. Among them, one forum stands out - “WWH-Club” serves as a platform where cybercriminals can acquire skills related to credit card data theft and learn how to profit from this illicit activity.

Table 12. *Methodology: a user is considered as active in 2023 if he has published at least one message.

1) WWH-Club – the king of carding.

Created in 2014, "WWH-Club" has evolved into one of the most active RLCF specializing in carding and banking fraud. Over the years, it has successfully built a substantial community and positioned itself as an educational hub for threat actors looking to enhance their carding expertise. The forum's administration capitalizes on their knowledge by offering training courses to members willing to invest $1200 for a premium membership.

The forum's aggressive monetization strategy implemented in recent years, coupled with numerous[28] complaints about their biased arbitration process accessible only to premium members[29], have adversely impacted its reputation and trustworthiness.

Figure 38. WWH-Club in 2024.

Account creation on the forum is without charge; however, to gain full membership privileges, including the ability to engage with the community by posting messages, new members are required to make a minimum payment of 100 dollars. In May 2023, the forum's administration reported a total membership of 353,000 users, with approximately 112,000 members active within the past 72 hours. These figures appear to be inflated, possibly with the aim of attracting advertisers. In March 2023, the same account stated that the forum had 540,000 members and also that 112,000 of them were active in the last 72 hours.

Figure 39. In March 2023, the administration of WWH-Club claims that the forum has 353,000 registered accounts and 112,000 active members during the last 72 hours. Auto translated from Russian.

In spring 2023, the staff of “WWH-Club” introduced a new satellite website, essentially functioning as a marketplace. While the services and products offered are closely aligned with those available on the main forum,

the marketplace format is designed to enhance the user experience and generate greater value from the forum's community. It appears that this idea did not work as intended because almost a year after its launch the marketplace is less popular than the forum itself[30].

Figure 40. In spring 2023, WWH-Club has launched its own marketplace.

When it comes to the services that a cybercriminal can find on “WWH-Club”, the Table below shows explicitly that these offers are heavily focused on the carding community. In total 8870 topics were posted in 2023, from which around 3799 in the section allocated to the carding activity itself. Quantitatively speaking, the second most important section titled “Everything else”, is dedicated to the sale of goods and services such as objects bought with stolen credit cards, spam services, and other advertisements that users did not know where to categorize.

Other sections like “Debit cards, ready-made wallets” are offering threat actors services to open banking accounts with fake identity in different countries. These services as well include technic to extract the stolen money through banking accounts – or as it is called in the jargon “to cash-out”.

Therefore, a variety of services necessary to conduct a carding business, such as fake identification documents, bulletproof infrastructure or databases, are present on the marketplace. Between 2022 and 2023, there was a decrease in the release of new commercial threads. Pinpointing the exact cause of this downturn is challenging, but it may be attributed to the cybercriminal community on this forum consolidating around a smaller number of established threat actors and illegal services. Another possible factor could be the consequence of "WWH-Club"'s shift towards less appealing and more aggressive monetization strategies, discouraging some threat actors from advertising their business their. Further analysis is necessary to understand the dynamics of this change.

D) Fraud RLCF – a variety of services ranging from fraudulent schemes to cash-out and money laundering services.

Among the 13 identified Fraud forums, 3 are presently highly active and popular. While these forums share some similarities, each strives to establish its unique identity. For instance, "DarkMoney" focuses on money laundering, "Probiv" specializes in lookups, and "DarkSave" is renowned, among other things, for selling counterfeit documents.

Our observations indicate that these communities primarily attract cybercriminals engaged in fraud schemes targeting CIS countries and that their reputation is fluctuant.

1) Laundering dirty cryptocurrencies.

Multiple laundering and cash-out services can be found on “DarkMoney”. The cybercriminals behind these services promise to clean the dirty cryptocurrencies and organize the cash-out either on a banking account, which can also be purchased or created from scratches with a fake identity, or through an intermediary called a “drop”.

An example of one of the many observed services on “DarkMoney” accepts for instance various cryptocurrencies and allows its clients to retrieve cleaned fiducial money in cash, in the currency of their choice, or to get the money on an account of a Russian or Ukrainian bank. Finally, multiple accounts explaining how to run a business with dirty money and evade taxes can also be found on the forum.

Figure 41. Cash-out service advertised on DarkMoney. Auto translated from Russian.

2) Probiv - Finding information about anyone.

The Russian term "probiv," which translates to "breaking through" something, is commonly used on RLCF to advertise lookup services. One notable forum, aptly named "Probiv," is recognized for its significant presence of threat actors engaged in these activities. What sets these lookup services apart is that the cybercriminals advertising them often have access to databases of States and companies. Such access is typically acquired through stolen databases or by recruiting insiders employed in law enforcement agencies, governmental bodies, banks, or mobile phone operator companies.

Having an insider's assistance enables lookup service providers to obtain a wide range of information about individuals from countries in the former USSR. Furthermore, threat actors interested in recruiting insiders also target online payment services, social networks, and instant messenger companies.

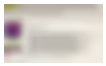

Figure 42. A threat actor looking for insiders in various companies and administrations. Auto translated from Russian.

Several cybercriminals do not hesitate to try to recruit insiders with access to international law enforcement agencies databases. Individuals with an access to Interpol and Europol databases are among the personnel that is looked for.

Figure 43. Example of a probiv service with access to Europol and Interpol insiders. Auto translated from Russian.

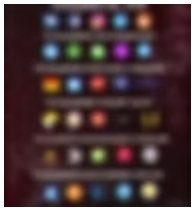

Figure 44. A threat actor searching for social networks employees.

As illustrated in Table 16, “Probiv” is also attracting threat actors specialized in the sale of fake ID, cash in and cash out services and automobile-related fraudsters. The job sections mainly advertise employment and job searches related to “drops”. Drops are real or fake people ready to give all their official documents to open bank accounts or to accomplish various tasks such as retrieving money or drugs for the real owner in exchange of a commission.

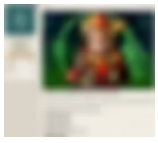

Figure 45. Example of “drop” service advertised on Probiv. Auto translated from Russian.

E) Diversification drugs RLCF.

RLCF focusing on the promotion and sale of Drugs are highly active and successful communities. Forums such as “WayAway” generate substantial revenues thanks to advertisements and partnerships with drug dealers. Due to the obvious nature of the trade ongoing on these forums we will not provide any details, nevertheless some interesting trends can be succinctly highlighted.

1) RuTor’s diversification strategy - development of carding and other malicious activities.

Since the start of 2023, we have observed that “RuTor” has initiated diversification in its activities, opening or enhancing sections dedicated to carding and various malicious schemes.

“RuTor”'s administration has not only launched a carding section but has also introduced sections for money laundering, hacking, and fake documents. This illustrates the intention of the owners of this RLCF to expand the forums' userbase and potentially increase the purchasing power of drug consumers.

“RuTor”'s administration has invested in the development of carding activities through the publication of tutorials and manuals. More than 91 threads have been published in the tutorial subsection, and forum members are offering to teach carding techniques for a fee. The mission of the threat actor and moderator "Princess" is to develop this section and create content, highlighting “RuTor”'s financial commitment, as moderators do not provide their services for free.

Furthermore, the presence of a section dedicated to hacking, database leaks, and traffic generation underscores the forum's diversification. Currently, the hacking and malware offerings advertised on this RLCF differ from those on top forums like "Exploit" or "XSS", by focusing on low-level content such as hacking social network accounts and DDoS services.

To assess the long-term consequences, it is essential to monitor the evolution of Russian-language drug forums in response to these developments.

Figure 46. A carding section on the Drugs RLCF RuTor.

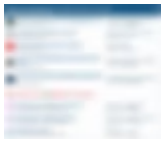

Figure 47. Hacking and DDoS sections are also present on RuTor.

Table 17. Drugs related topics were not counted, please note that they constitute the majority of commercial threads on RuTor. Source: CybercrimeDiaries.com

I hope that you found this Chapter informative and insightful. If you wish to engage in discussions regarding any of the subjects explored in this blog post, please feel free to reach out to me via Twitter/X or LinkedIn.

In the upcoming and final Chapter, we will delve into the analysis of how geopolitical events have influenced RLCF and their communities.

This blog post is also available on my company's blog (OWN).

Sources:

[7] "«Если прибыли ФБР, Интерпол и отдел „К“, что-то у них на меня есть». Тот самый хакер из Речицы впервые говорит о своём деле," dev.by, accessed January 21, 2024, https://devby.io/news/hacker-from-rechitsa.

[20] "Telegram: @freedomf0x - Свежий Слив, Свежей Справки По Форме 1. По Переданной Нам Информации Из Киевского DC (От Души Парни), Сливают в СБУ Инфу Из 18 Центра ФСБ РФ.," 2024, https://t.me/freedomf0x/18183.

[23] "Авторская статья - Антикино от А до Я (популярная мошенническая схема в 2019)," Форум социальной инженерии — Zelenka.guru (Lolzteam) https://zelenka[.]guru/threads/1057828/.

[27] “Арбитраж - Как Заработать На Audi A7 - Lolz Scam - Ланской,” XSS.is (ex DaMaGeLaB), May 14, 2023, https://xss[.]is/threads/87960/.
