Russian Language Cybercriminal Forums - An Excursion Into The Core Of The Underground Ecosystem.

cybercrimediaries.com/post/russian-language-cybercriminal-forums-an-excursion-into-the-core-of-the-underground-ecosystem

January 1, 2024

- Oleg
-
-
  - Jan 1
  -
  - 18 min read

ROKЯ

Chapter I. The origins of the Russian language cybercriminal ecosystem and the current cybercriminal forums landscape.

In this series of OSINT investigations, I would like to invite you on a journey to the Russian language cybercriminal ecosystem. We will start in the following first Chapter with an exploration of the origins of this ecosystem and an analysis of the Russian language cybercrime forums (RLCF), uncovering how they appeared, evolved and the current state they are in.

In Chapter II we will assess to which extent RLCF are hard to access for an outsider and understand how their administrators monetize them. As we will see the most successful forums are able to generate hundreds of thousands of dollars every year.

In Chapter III we will identify the most prominent RLCF and try to understand their pivotal role within the wider cybercriminal ecosystem and examine their interactions with Telegram communities.

Finally, in Chapter IV, we'll delve into the geopolitical influences shaping these communities. Here, we will analyze how recent global events and political dynamics have impacted the Russian language cybercriminal forums, providing a comprehensive understanding of their current state and potential future.

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

Insights of the first Chapter:

- RLCF can be classified into 6 categories containing both generalist forums, where a great variety of different illicit activities can be found, and communities that specialize in a particular segment of cybercrime.
- Out of 207 identified RLCF only 94 are active at varying levels. As it was the case 10 years ago[1], the number of highly active RLCF is stable at around 22 forums, although the nature and types of illegal activities have somewhat evolved.
- The Russian language cybercriminal ecosystem is rather well structured and stable with some old prominent forums occupying a key place in their own category. Overall, the technically advanced forums represent a minority and gather small but active communities.

- An exception is the drug-selling cybercriminal ecosystem who still did not stabilize after the closure of the “Hydra” marketplace. Rivalry and competition are predominant among the RLCF specialized in the trade of drugs. It is currently the most unstable category as new forums are often appearing and threatening to dethrone the current leaders.

I) The origins of the Russian language cybercriminal ecosystem and forums.

Our story about cybercrime in the Russian-speaking part of the world begins in 1983 in the USSR. This year the title of the first known hacker and cybercriminal of the Soviet Union was awarded to Mr. Murat Utrembaev, a young worker of the car manufacturing giant AvtoVAZ[2]. This Soviet citizen was a talented ethnic Kazakh from modest origins who managed to study mathematics in Moscow at the prestigious Moscow State University. Unfortunately for him, instead of pursuing a brilliant scientific career he was promised, Mr. Utrembaev was forced by the Soviet student repartition system to work as a second-class technical support employee at AvtoVAZ in the city of Tolyatti on the Volga.

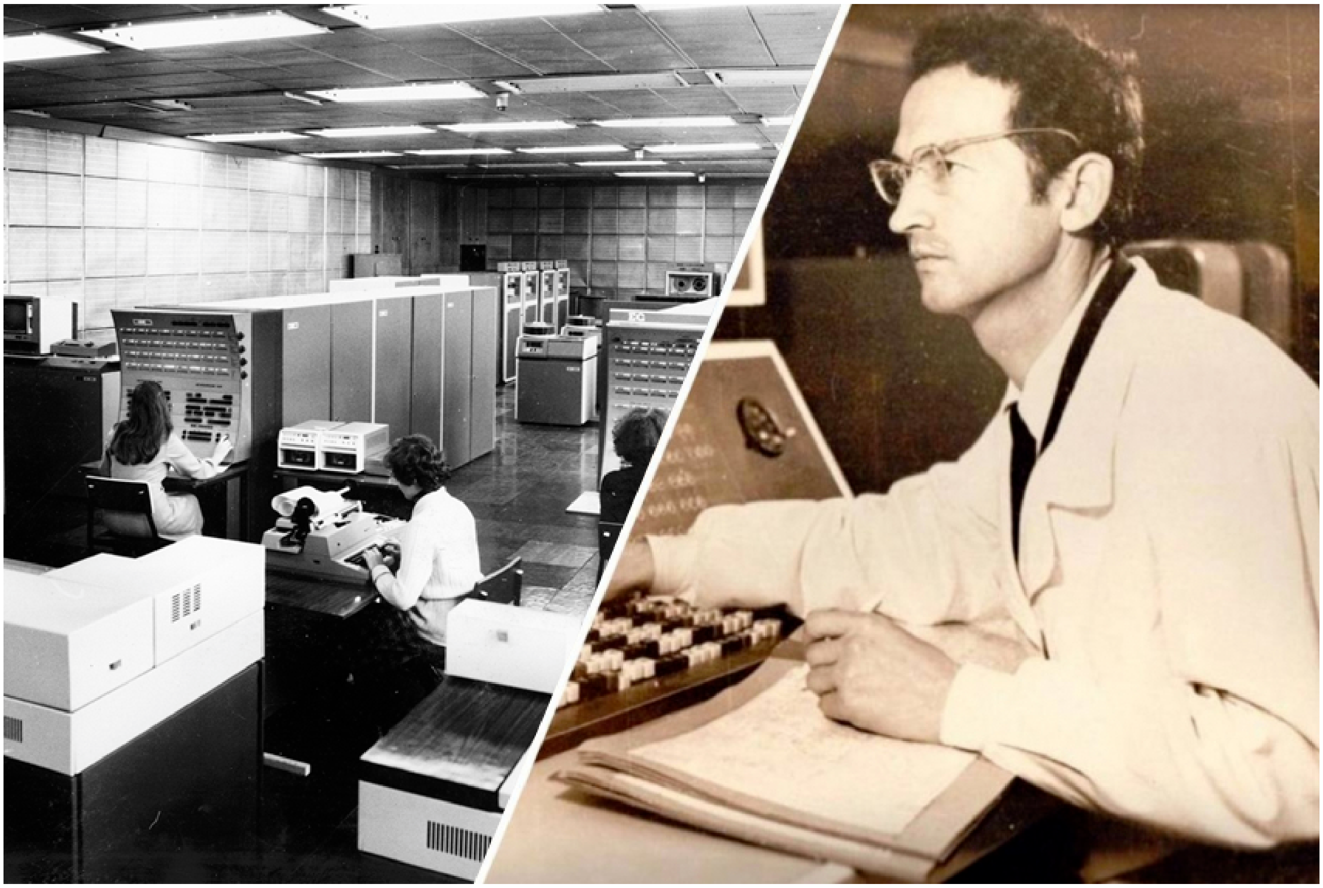


Figure 1. On the left side: the computing Center of the Volga Automobile Plant in Togliatti, Soviet Union.

On the right side: allegedly Mr. Murat Utrembaev. Source: AvtoVAZ archive.

Mr. Utrembaev perceived his situation as particularly unfair, as unlike his wealthier and well-connected Muscovite peers, he was unable to bribe his way into a desirable job. Instead, he found himself performing tasks for which he was overqualified. Despite working diligently and seeking recognition, he was left disappointed when the honorific diploma promised by his superiors never materialized. Frustrated by what he saw as a blatant disregard for his efforts, Mr. Utrembaev decided to retaliate by targeting the factory's computer system that controlled the entire car assembly line.

The young man executed his revenge by introducing a diskette with a specially programmed “update” for the factory’s assembly line control software. This act of cyber sabotage effectively halted the production of cars for three days, resulting in significant financial losses for AvtoVAZ, measured in millions of rubles. It took the factory's other programmers a substantial effort and time to identify and rectify the issue caused by Mr. Utrembaev's intervention.

Out of guilt and due to the pressure from law enforcement agents and the factory’s management, Mr. Utrembaev decided to denounce himself and was only sentenced to partially compensate the damage he caused and to conditional imprisonment under the article “For Hooliganism”. Anecdotally, this hack also helped AvtoVAZ’s directors to uncover other malicious activity that was conducted by the factory’s programmers. Some of them created and then solved problems they injected into the code to obtain the payment of bonuses.

22

87
1052

Figure 2. The software for feeding parts and assemblies to the main conveyor of the VAZ needed to work without interruptions. Source: AvtoVAZ archive.

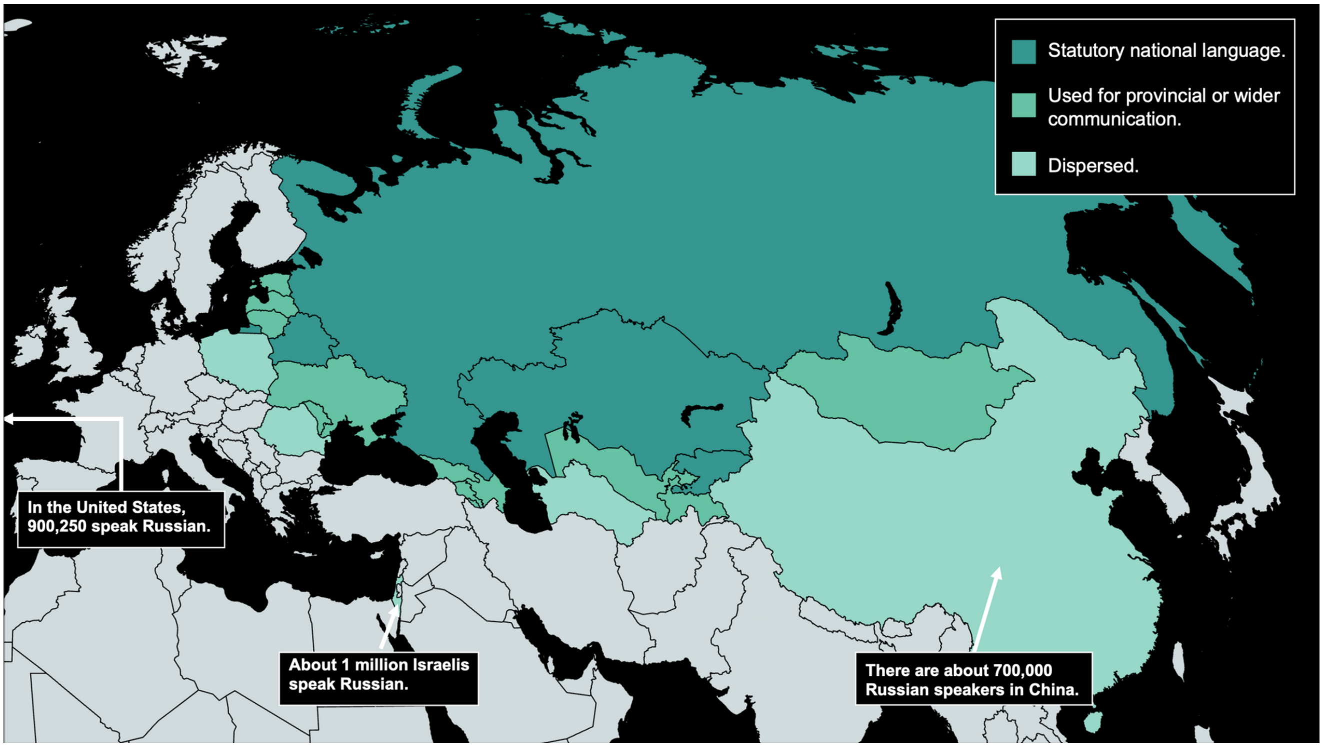
Interestingly, the outcome of this story brings to light several significant points that are important for readers to consider. These points give indeed a hint at the preconditions that allowed to the Russian language ecosystem to appear and develop.

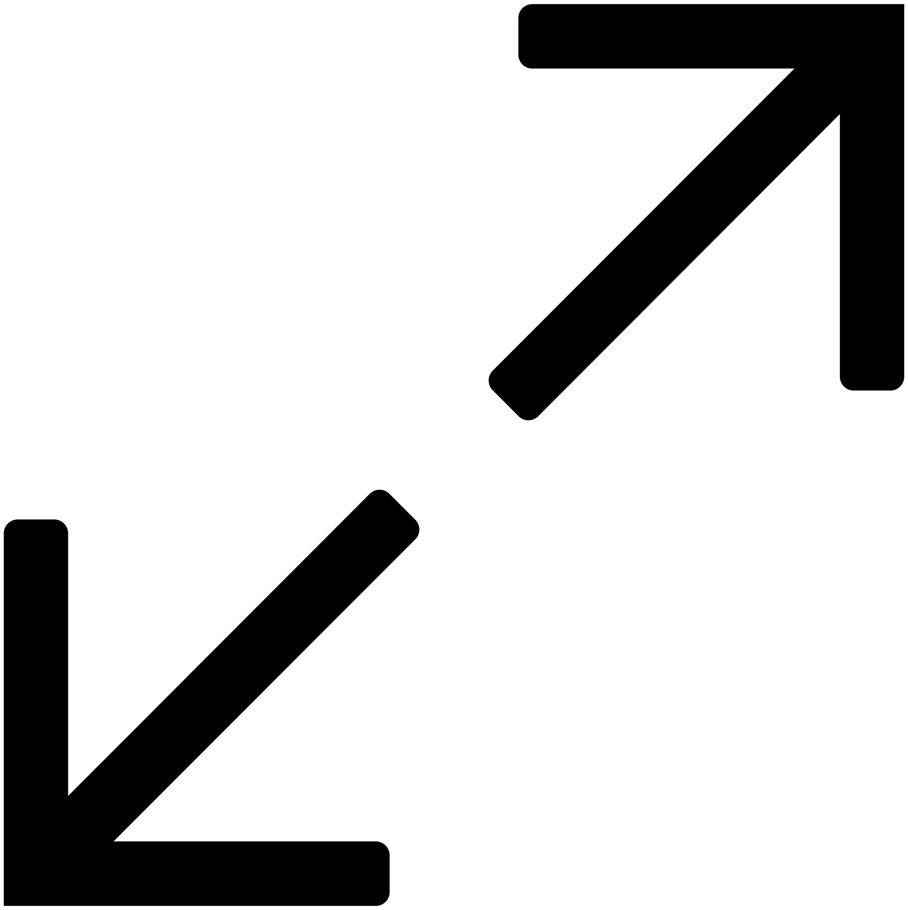
Firstly, it is useful to underscore the unpreparedness of the Soviet legal system to tackle cybercrime, a challenge that was not unique to the USSR and its successor states. This phenomenon reflects a broader truth: in all societies and areas of human activity, legal frameworks tend to be reactive rather than proactive. Lawmakers are constantly challenged to update regulations in response to emerging trends and the misuse of new technologies. Recent examples of this include the advent of cryptocurrencies, the scrapping of social networks and the last developments in generative artificial intelligence.

Furthermore, Mr. Utrembaev's case highlights the linguistic, political and ethnic particularities that are specific to the former Soviet area: a Russian speaker is not necessarily Russian. Indeed, the Russian language is widespread in the former Soviet republics because of the Russification policy that was enforced by the Russian Empire and later by the Soviet leadership. This may seem quite obvious but the confusion between spoken language, political identity, citizenship and ethnicity is so widespread when media talk about "Russian hackers", that I felt it is useful to underscore this point. To conclude this aside, the only thing that can be deduced from the use of Russian language by a threat actor is that he is probably, but not necessarily, from the former Soviet Union. The downfall of the USSR provoked a massive exodus of Russian speakers to countries like Israel or the United States, which somewhat complexifies the identification of Russian-speaking cybercriminals. In June 2023, the arrest in the United States of Mr. Ruslan Astamirov, a Russian citizen from Chechenia, for his involvement in deploying the LockBit ransomware, is a fresh example of some of the most confusing cases involving Russian-speaking cybercriminals[3].

Lastly, the motives of cybercrime can be diverse, ranging from an act of revenge, as it was for Mr. Utrembaev, to the lure of profits like it was the case for some of the AvtoVAZ's programmers who hacked their own company to get bonuses for solving the problems they created. The lack of professionally rewarding and well-paid opportunities was also a precondition that enticed Mr. Utrembaev to act the way he did. The downfall of the USSR confronted a significant quantity of technically qualified individuals with complex economic and personal situations, which sometimes corrupted them.

Table 1. Russian language in the world.


Statutory national language.
Used for provincial or wider communication.
Dispersed.
In the United States, 900,250 speak Russian.
About 1 million Israelis speak Russian.
There are about 700,000 Russian speakers in China.



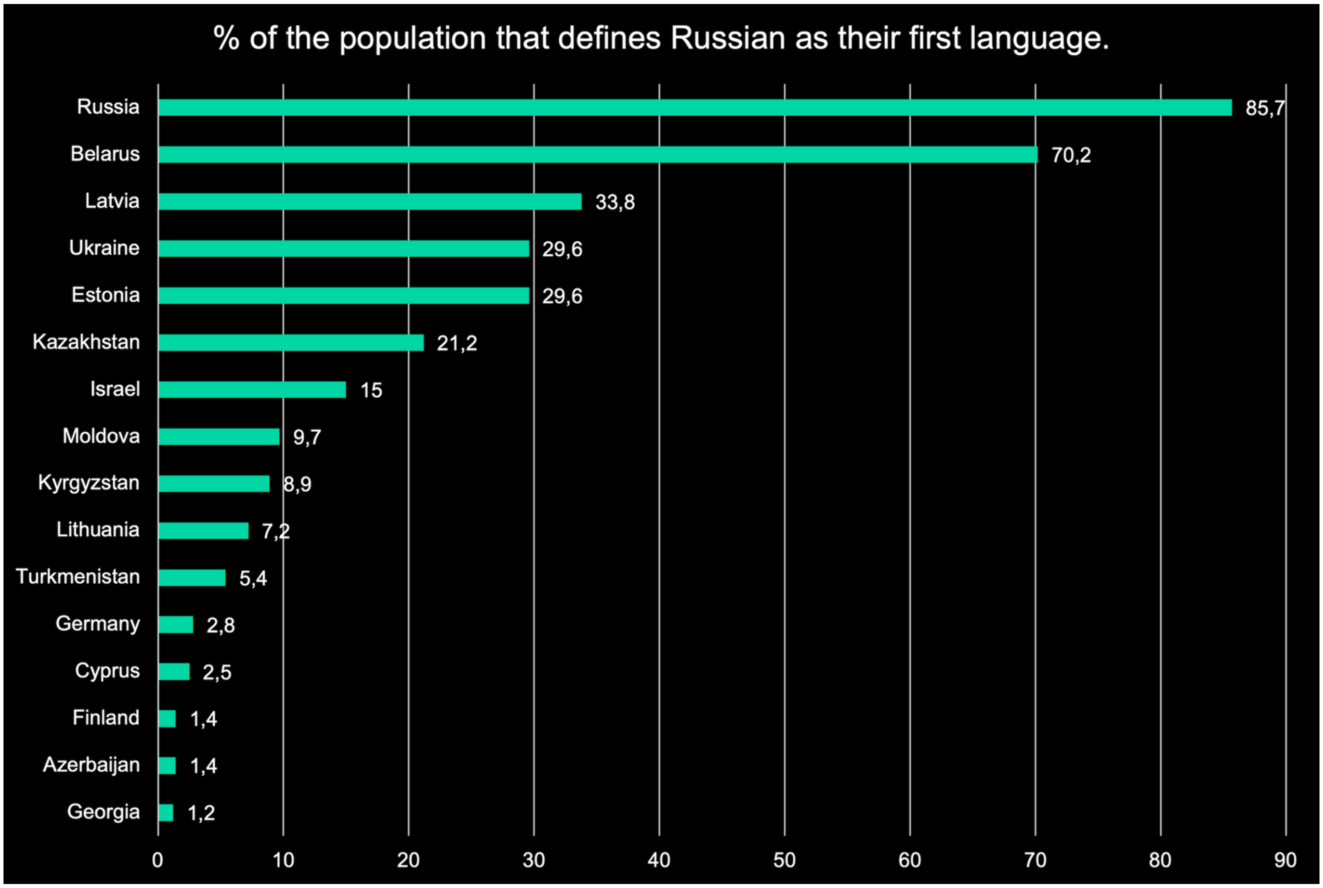

% of the population that defines Russian as their first language.
Russia 85,7
Belarus 70,2
Latvia 33,8
Ukraine 29,6
Estonia 29,6
Kazakhstan 21,2
Israel 15
Moldova 9,7
Kyrgyzstan 8,9
Lithuania 7,2
Turkmenistan 5,4
Germany 2,8
Cyprus 2,5
Finland 1,4
Azerbaijan 1,4
Georgia 1,2
0
10
20
30
40
50
60
70
80
90

Table 1. Source: RadioFreeEurope – data obtained between 2001 and 2017. C. Coelho. Ethnologue, media reports[4].

The collapse of the USSR in December 1991 fostered a deep economic and sociopolitical reconfiguration in the former Soviet satellites and particularly in the 15 newborn republics. For the citizens of these States, the 90s were characterized by high levels of poverty, unemployment, corruption, legal loopholes but also by freedom and, for a minority, by previously unseen enrichment opportunities[5]. Technological innovations, such as the swift deployment of the Internet, allowed for instance the development of online banking and new ways of social interactions like online forums. Hacking in the former Soviet Union became a popular thematic among the technically educated population and children eager to learn by reading one of the most famous Russian hacking magazines called “Haker” (see xaker.ru). These new opportunities were rapidly hijacked by immoral but technically literate individuals like Mr. Vladimir Levin, a microbiologist from St. Petersburg, who was able to steal 10 million dollars from the American Citibank in 1994[6]. Though Mr. Levin was arrested and imprisoned for three years, 400,000 dollars were never found.

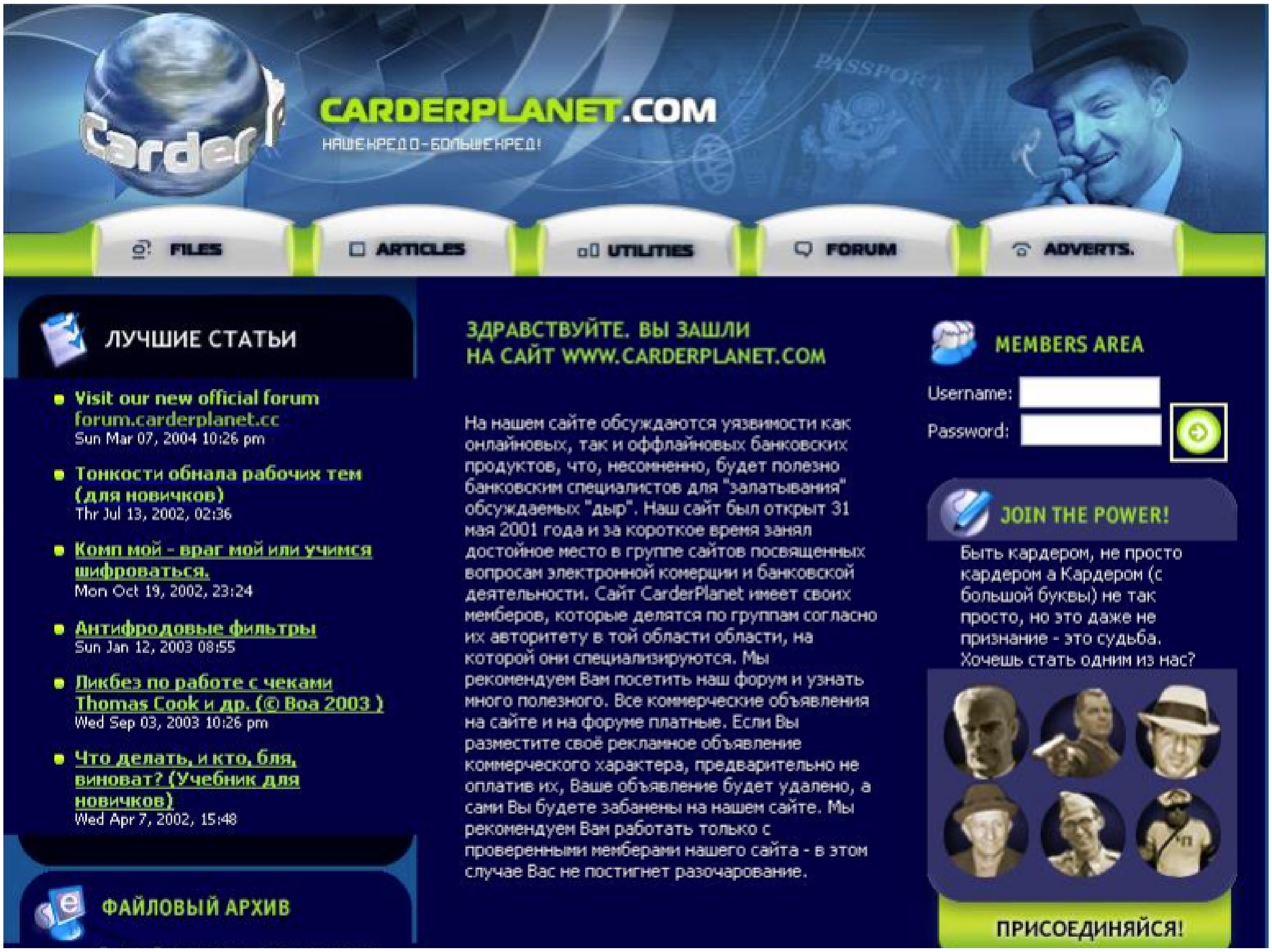
Figure 3. Photos of Mr. Vladimir Levin, a microbiologist from St. Petersburg, Russia.

The lack of dissuasive legal sanctions strengthened the perception of impunity and omnipotence felt by Russian-speaking cybercriminals because they were able to strike anywhere in the world, where a computer system was connected to the Internet. I would like to note that the particularity of life in the Soviet Union, and afterwards in new republics during the complicated 90s, produced a subculture of permanent survival for a part of the population who often faced rationing and poverty. This encouraged a minority of these individuals to distrust anything linked to the administration and disregard laws. Mixed to the remnants of Marxist ideology, and perverted patriotism, it became acceptable for some to steal from the “rich” or from the “bourgeois” (name given to westerners). The main rule of the most capable

Russian-speaking cybercriminals was, and still is, to avoid attacking the countries that compose the Community of Independent States (CIS). This code of conduct is sometimes motivated by “patriotic” concepts but also by a rational calculus: avoid attracting the attention of the local law enforcement.

II) The genesis of the first Russian language cybercriminal forums - A permanently moving and adapting ecosystem.

The subsequent low risk – high reward situation led to the apparition of the first Russian language cybercrime organizations, and forums specialized in carding. This malicious craft is a form of credit card fraud in which a stolen credit card is used to charge prepaid cards or purchase goods. Websites like the “Boa Factory” or the forum “CarderPlanet”, created among others by the Ukrainian hackers Roman Vega and Dmitry Golubov[7], were popular places for buying and selling virtually all assets produced by financially motivated online criminal activity in the beginning of the 2000s. The apotheosis of impunity was undoubtedly met when around 40 cybercriminals from the “CarderPlanet” forum organized in 2002, the first "World Carders" conference in the city of Odessa in Ukraine[8].



ЛУЧШИЕ СТАТЬИ

- Visit our new official forum forum.carderplanet.cc
  Sun Mar 07, 2004 10:26 pm
- Тонкости обнала рабочих тем (для новичков)
  Thr Jul 13, 2002, 02:36
- Комп мой - враг мой или учимся шифроваться.
  Mon Oct 19, 2002, 23:24
- Антифродовые фильтры
  Sun Jan 12, 2003 08:55
- Ликбез по работе с чеками Thomas Cook и др. (© Boa 2003)
  Wed Sep 03, 2003 10:26 pm
- Что делать, и кто, бля, виноват? (Учебник для новичков)
  Wed Apr 7, 2002, 15:48

ФАЙЛОВЫЙ АРХИВ

ЗДРАВСТВУЙТЕ. ВЫ ЗАШЛИ НА САЙТ WWW.CARDERPLANET.COM

На нашем сайте обсуждаются уязвимости как онлайновых, так и оффлайновых банковских продуктов, что, несомненно, будет полезно банковским специалистов для "залатывания" обсуждаемых "дыр". Наш сайт был открыт 31 мая 2001 года и за короткое время занял достойное место в группе сайтов посвященных вопросам электронной комерции и банковской деятельности. Сайт CarderPlanet имеет своих мемберов, которые делятся по группам согласно их авторитету в той области области, на которой они специализируются. Мы рекомендуем Вам посетить наш форум и узнать много полезного. Все коммерческие объявления на сайте и на форуме платные. Если Вы разместите своё рекламное объявление коммерческого характера, предварительно не оплатив их, Ваше объявление будет удалено, а сами Вы будете забанены на нашем сайте. Мы рекомендуем Вам работать только с проверенными мемберами нашего сайта - в этом случае Вас не постигнет разочарование.

MEMBERS AREA

Username:

Password:

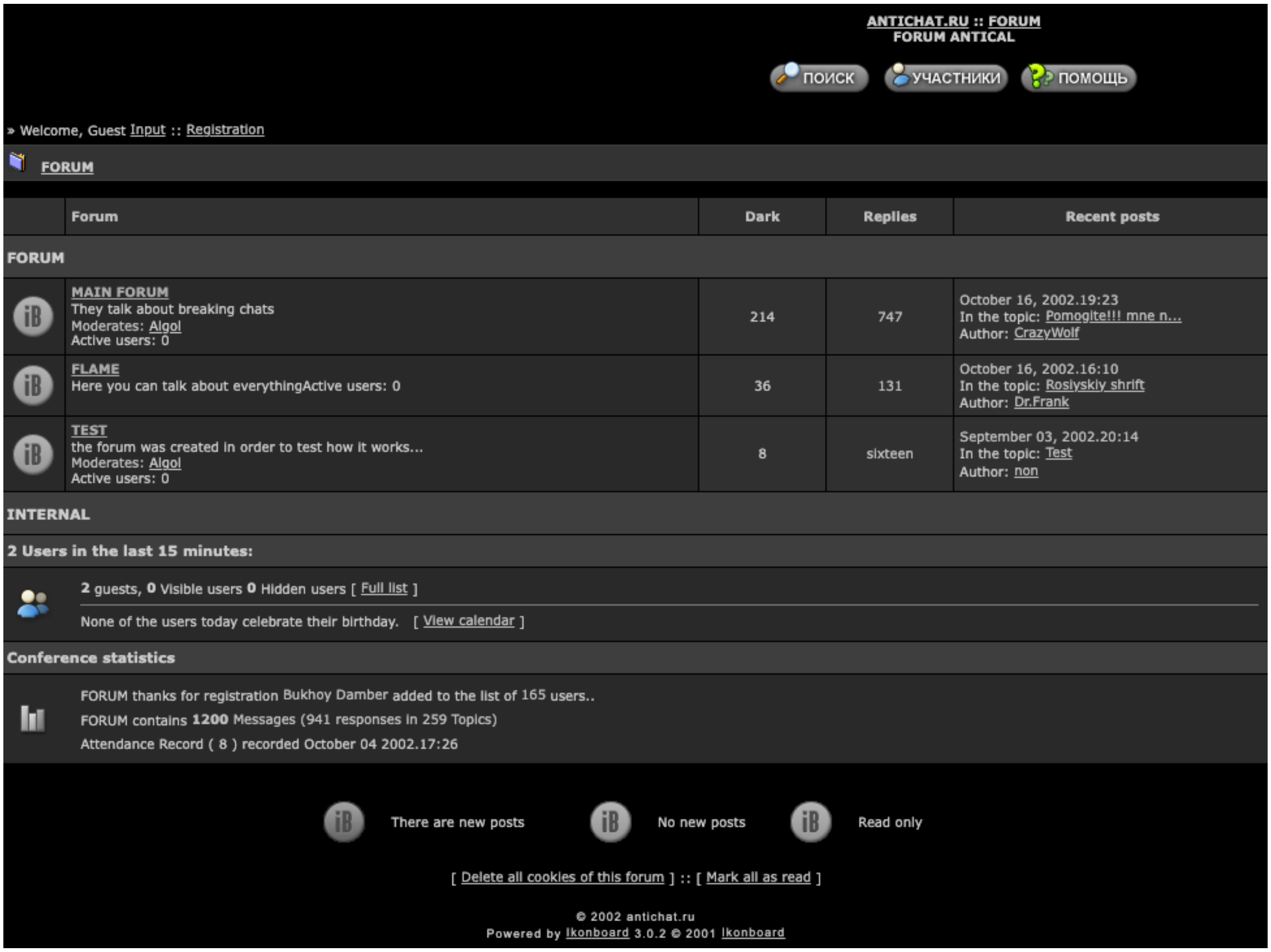
JOIN THE POWER!

Быть кардером, не просто кардером а Кардером (с большой буквы) не так просто, но это даже не признание - это судьба. Хочешь стать одним из нас?

Figure 4. A screenshot of the CarderPlanet forum from 2004.

During the first years of the new century Russian-speaking cybercriminals began congregating on various forums such as Antichat (2002), DaMaGeLaB (2004), WASM (2004) or Arbitraj Foum (2004). These platforms serve to this day as hubs for hackers to conduct business, recruit new members, improve skills and learn, all while allowing their member to maintain a degree of anonymity. The later became gradually a crucial aspect of RLCF operations, as over time cybercrime risks escalated even in the post-Soviet States. To enhance privacy, the most sophisticated RLCF began creating Onion mirrors, making them accessible through the Tor network, and claimed that they stopped logging members' IP addresses.

From its inception, this digital ecosystem has continuously evolved and adapted to new lucrative activities like carding, probiv[9], malware as a service, and the trading of illegal products such as drugs. The Russian-speaking cybercriminal community has been a pioneer in the cybercriminal field and its adaptivity allows it to remain a robust ecosystem to this day. The advancement of technology and various geopolitical developments have nevertheless significantly influenced this ecosystem, leading to its transformation. Like any social group, RLCF have undergone changes over time, with some forums disappearing or losing popularity.



ANTICHAT.RU :: FORUM
FORUM ANTICAL

» Welcome, Guest Input :: Registration

FORUM

Forum	Dark	Replies	Recent posts
FORUM			
MAIN FORUM They talk about breaking chats Moderates: Algol Active users: 0	214	747	October 16, 2002.19:23 In the topic: Pomogite!!! mne n... Author: CrazyWolf
FLAME Here you can talk about everythingActive users: 0	36	131	October 16, 2002.16:10 In the topic: Roslyskiy shrift Author: Dr.Frank
TEST the forum was created in order to test how it works... Moderates: Algol Active users: 0	8	sixteen	September 03, 2002.20:14 In the topic: Test Author: non

INTERNAL

2 Users in the last 15 minutes:

2 guests, **0** Visible users **0** Hidden users [Full list]

None of the users today celebrate their birthday. [View calendar]

Conference statistics

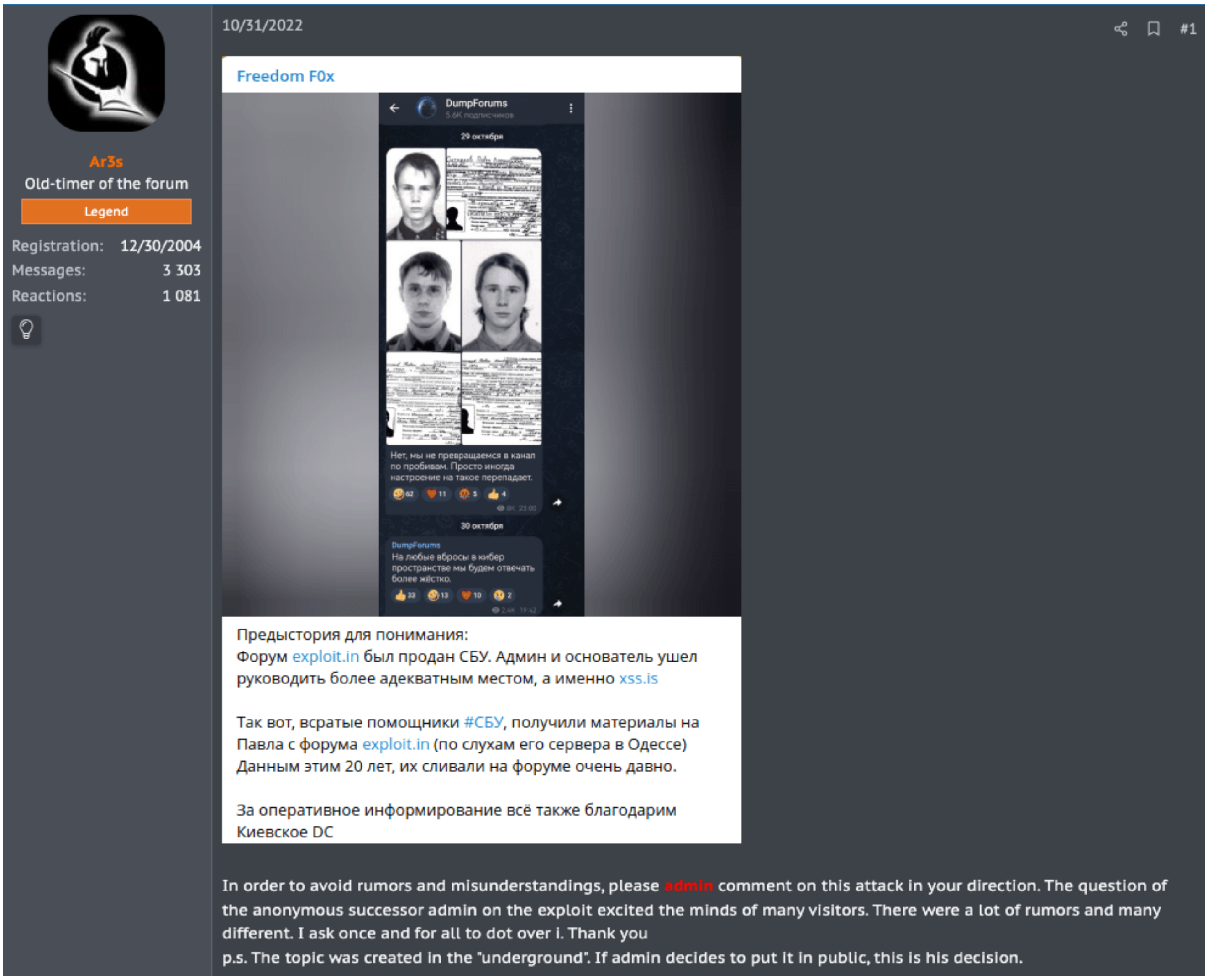
FORUM thanks for registration Bukhoy Damber added to the list of 165 users..
FORUM contains **1200** Messages (941 responses in 259 Topics)
Attendance Record (8) recorded October 04 2002.17:26

[Delete all cookies of this forum] :: [Mark all as read]

© 2002 antichat.ru
Powered by Ikonboard 3.0.2 © 2001 Ikonboard

Figure 5. Screenshot of Antichat from 2002, one of the oldest RLCF that is still active today.

In recent years, Russian language and other global cybercrime forums have faced various challenges affecting their growth. Between 2018 and 2020, a series of confirmed and suspected security breaches impacted several well-known Russian RLCF including "Exploit" [10] and "BHF"[11]. These incidents adversely influenced the users' trust in the forums' safety and anonymity. Following these events, persistent rumors circulated about the possible control of major RLCF by Russian or Ukrainian intelligence agencies. These speculations frequently resurface, causing unrest among the members of forums like "XSS", "Exploit" and "RAMP".



Ar3s
Old-timer of the forum
Legend

Registration:	12/30/2004
Messages:	3 303
Reactions:	1 081

10/31/2022

Freedom F0x

Нет, мы не превращаемся в канал по пробивам. Просто иногда настроение на такое перепадает.

На любые вбросы в кибер пространстве мы будем отвечать более жёстко.

Предыстория для понимания:
Форум exploit.in был продан СБУ. Админ и основатель ушел руководить более адекватным местом, а именно xss.is

Так вот, всратые помощники #СБУ, получили материалы на Павла с форума exploit.in (по слухам его сервера в Одессе) Данным этим 20 лет, их сливали на форуме очень давно.

За оперативное информирование всё также благодарим Киевское DC

In order to avoid rumors and misunderstandings, please admin comment on this attack in your direction. The question of the anonymous successor admin on the exploit excited the minds of many visitors. There were a lot of rumors and many different. I ask once and for all to dot over i. Thank you
p.s. The topic was created in the "underground". If admin decides to put it in public, this is his decision.

Figure 6. Auto translation from Russian. Ar3s, the previous owner of XSS, reached out to the forum's current administrator to address speculation about purported connections with the Security Service of Ukraine (SBU).

Source: XSS [12].

At the same time, the expansion of Telegram's user base, which soared to 700 million monthly active users in 2023[13], along with its open API system and flexibility, motivated many cybercriminals to adopt this instant messaging platform. The near-total impunity experienced within Telegram's environment made it an attractive alternative or a supplementary tool to traditional forums for these cybercriminals.

In parallel, global geopolitical shifts have also left their mark on RLCF. The thaw in relations between Belarus and the West from 2015 to 2020, for instance, paved the way for cooperation between Belarusian law enforcement and the U.S. Federal Bureau of Investigation (FBI). Such collaborations have borne fruit, as seen in the arrest of "Ar3s," a key figure in the Andromeda Trojan group and an administrator of the RLCF "XSS," previously known as "DaMaGeLaB"[14]. The onset of the Russian-Ukrainian conflict in February 2022 has introduced fresh geopolitical tensions, had already an intriguing impact on the RLCF landscape.

Reflecting on the inception of this research just a year ago, the sheer pace and scale of change within RLCF and their communities have been staggering. In the past year alone, 17 RLCF have been shuttered or abandoned. At least 15 have had to relocate their domains following seizures by law enforcement. An entertaining instance is the rise and fall of the hacktivist forum "Infinity," created by leaders of the pro-Russian hacktivist group Killnet. This forum's lifecycle - launching at the end of 2022, closing in the spring of 2023, reopening in September 2023, and then being deserted once again - exemplifies the fluidity that is intrinsic to the nature of RLCF and emblematic of the cybercriminal ecosystem as a whole.

III) Methodological notes and foreword.

This first Chapter will mainly talk about RLCF and try to present an exhaustive analysis of the current landscape, nevertheless, forums allowing the topics related to the sale of weapons and illicit pornographic content are not covered. Furthermore, private internal chats, such as the one that existed in the Conti ransomware gang, or private TOX and Jabber communications, are also out of the scope of this research. The same limit applies to Russian language marketplaces as they are not truly places where threat actors communicate, but rather purchase different goods or services.

Our focus on RLCF does not imply that Russian is the sole language that is spoken on these forums. During this investigation I considered that a forum can be labeled a RLCF if Russian is the main spoken language on it, or if the administrators are Russian-speaking threat actors. Presently, the popularity of the Russian language cybercriminal ecosystem magnetizes threat actors from all around the world. This materializes either by the creation of specific English language sections or by the acceptance of the publication of messages in English everywhere. Rare cases of RLCF allowing as well as other languages like Chinese were also observed.

IV) 2024 landscape of the RLCF ecosystem.

In 2024 the Russian language cybercriminal ecosystem is composed of at least 113 inactive and 94 forums active to a different level.

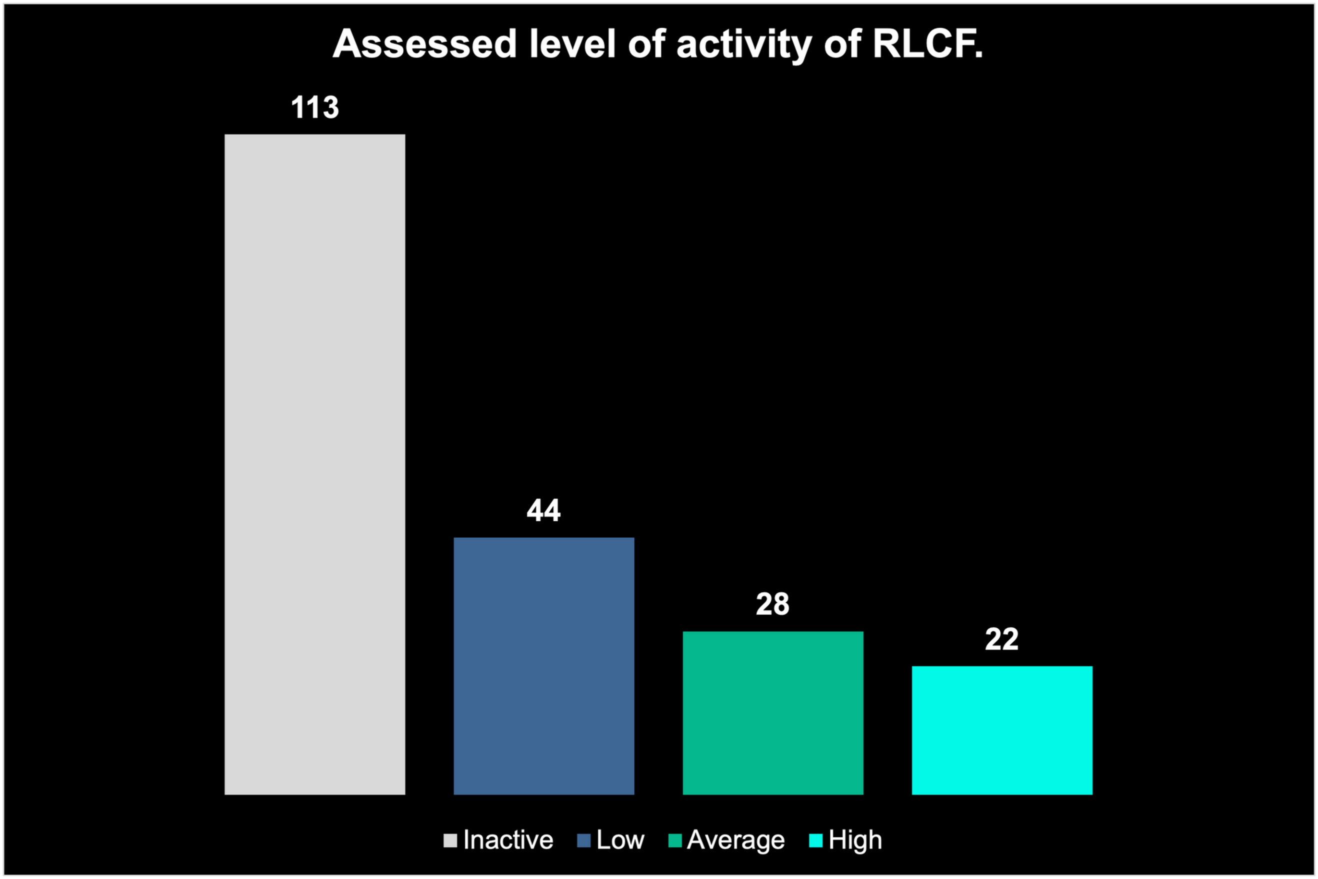


Table 2. Source: Cybercrime Diaries – January 2024.

V) A glance at the current situation: RLCF typology, creation date and level of activity.

Mapping these RLCF implies the need to properly categorize them to facilitate our analysis. To accomplish this task, I have established six categories that represent the primary focus of the forums within the ecosystem. These categories are not ideal and are not meant to encapsulate every activity occurring on each forum; rather, they provide a general sense of the forum's main area of specialization. For example, while many RLCF feature sections on carding, this does not necessarily mean that their central activity is focused on the theft and misuse of banking details. Therefore, these categories should be viewed as archetypes that assist in understanding and evaluating the ecosystem.

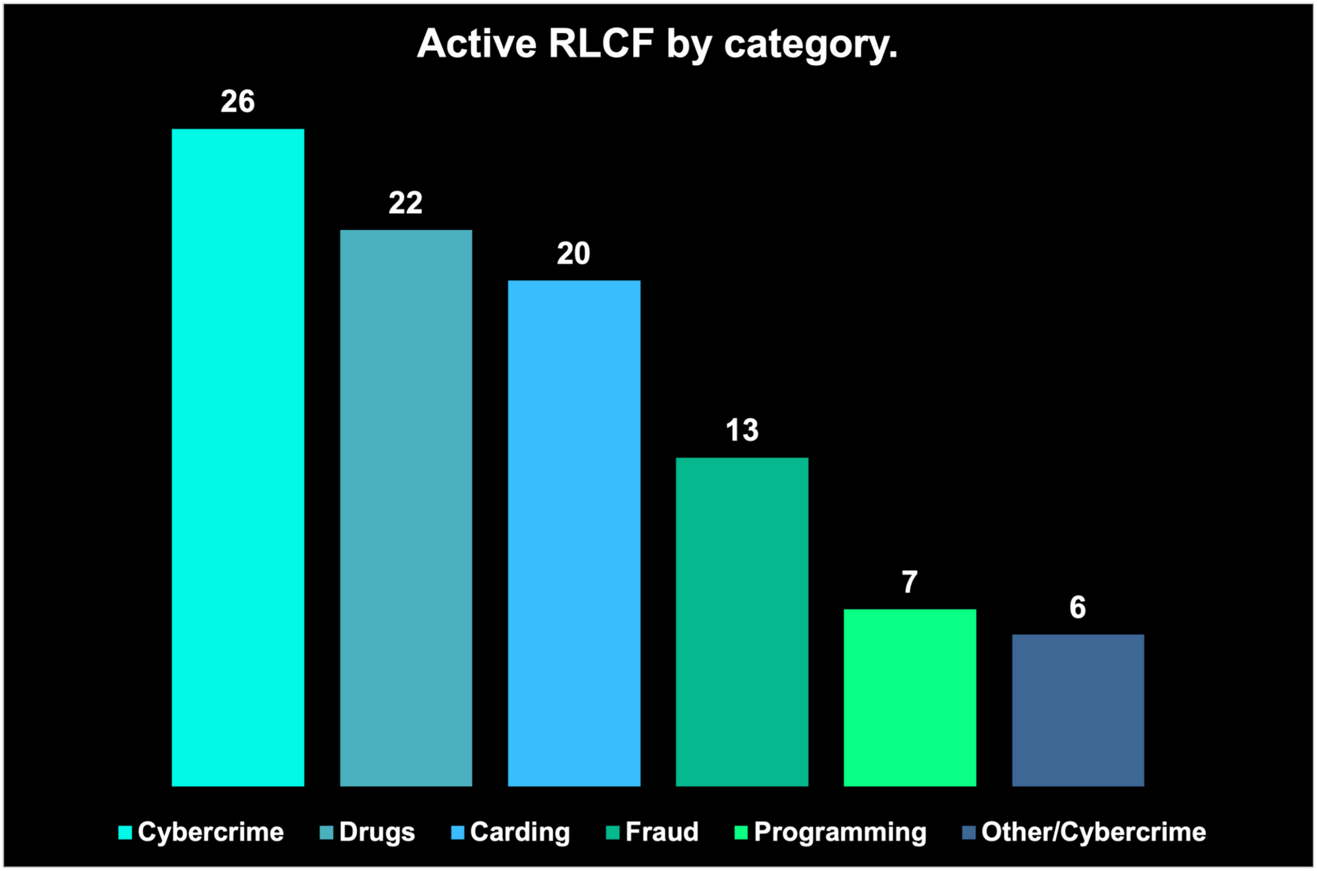


Table 3. Source: Cybercrime Diaries – January 2024.

A) Classification of the identified RLCF.

- Cybercrime: this category encompasses generalist forums that provide a large range of services and knowledge related to cybersecurity and computer literacy. Typical cybercrime forums are for instance “Exploit” or “XSS”. A threat actor can find there, among other things, topics covering network security, malware and buy access to corporate networks. These communities avoid selling any illicit substances such as drugs or weapons.

- Several subcategories can be established:
    - Data Leak: RLCF specialize in the sale and dissemination of stolen data belonging to companies or to individuals. "Nohide" is one of the most active forums from this group.
    - Ransomware: this subcategory is based on only one forum, but its uniqueness deserves attention. The RLCF “RAMP” was created in 2021 at a moment when other cybercriminal Russian language forums decided to ban any topics related to ransomware after the Colonial Pipeline attack[15]. Though ransomware gangs are de facto tolerated again on RLCF, “RAMP” is a gathering place for threat actors involved in this activity.
- Carding: as the name explicitly suggests, these forums are mostly specialized on credit card fraud where stolen credit cards and banking data are used to purchase prepaid cards or goods that are easy to resell. Other financial fraud technic and tools can be found there. A good example of a RLCF from this category is “WWH-Club”.
- Programming: the predominant Russian language forums centered on programming languages and computer literacy are typically harmless. However, for this study, our selection was limited to forums that permit members to actively develop and discuss malicious code. "WASM" stands out as one of the most renowned programming-focused RLCF, but like many forums in this category, it currently exhibits minimal activity.
- Fraud: The RLCF classified in this category concentrate on a variety of fraud schemes implying the use of a computer or phone. Techniques like counterfeit document production, money laundering, social engineering, and to a lesser extent, malware distribution, are actively discussed on forums such as “Center Club,” “Darkmoney,” and “Dublikat.”
    - Lookups (Probiv): These Fraud forums are likely among the most unique types of cybercriminal communities specific to the CIS. They predominantly deal in the sale of databases filled with personally identifiable information about individuals, mainly from the former Soviet Union region. A notable service offered on an RLCF named “Probiv” involves compiling comprehensive data about a person or a company. This often entails acquiring private databases or engaging insiders within state administration or telecommunications companies.
    - Fake documents: communities like “Dublikat” are specifically focused on the creation of fake documents.
    - Financial services: “Darkmoney” offers a concentration of services related to money laundering and financial fraud.

- Drugs: this type of RLCF is focused on the promotion and trade of drugs. Customers can find information about sellers and means to exchange their money for cryptocurrencies. “RuTor”, “WayAway” and “Pasaremos” are some examples of such forums.
- In the Other/Cybercrime category, forums often specialize in topics like video games, teenage life, or information technology, but they also tolerate discussions related to cybercrime and fraud. While cybercrime is not the principal focus of forums like “LolzTeam,” such platforms have become significant hubs for threat actors, particularly those specializing in the distribution of infostealers[16].

B) Levels of activity and creation dates of RLCF.

To measure the activity levels of each forum, I assessed the average number of messages posted per day as a benchmark. Forums where the daily message count averages between 1 and 20 were classified in the "Low" activity group. Those with a daily message average ranging from 20 to 100 were considered to have "Average" activity. Finally, forums with a daily message count exceeding 100 were labeled as having "High" activity.

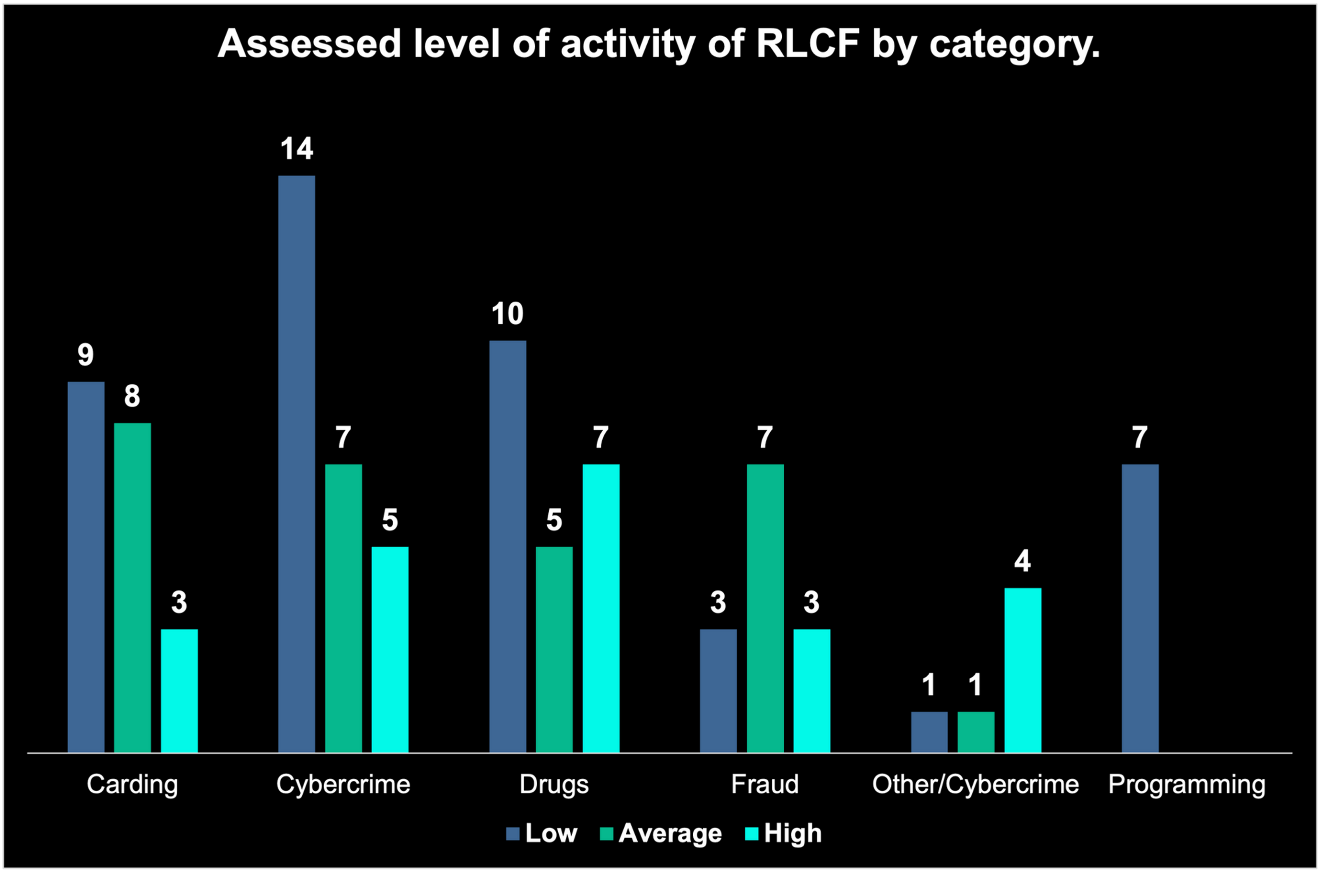
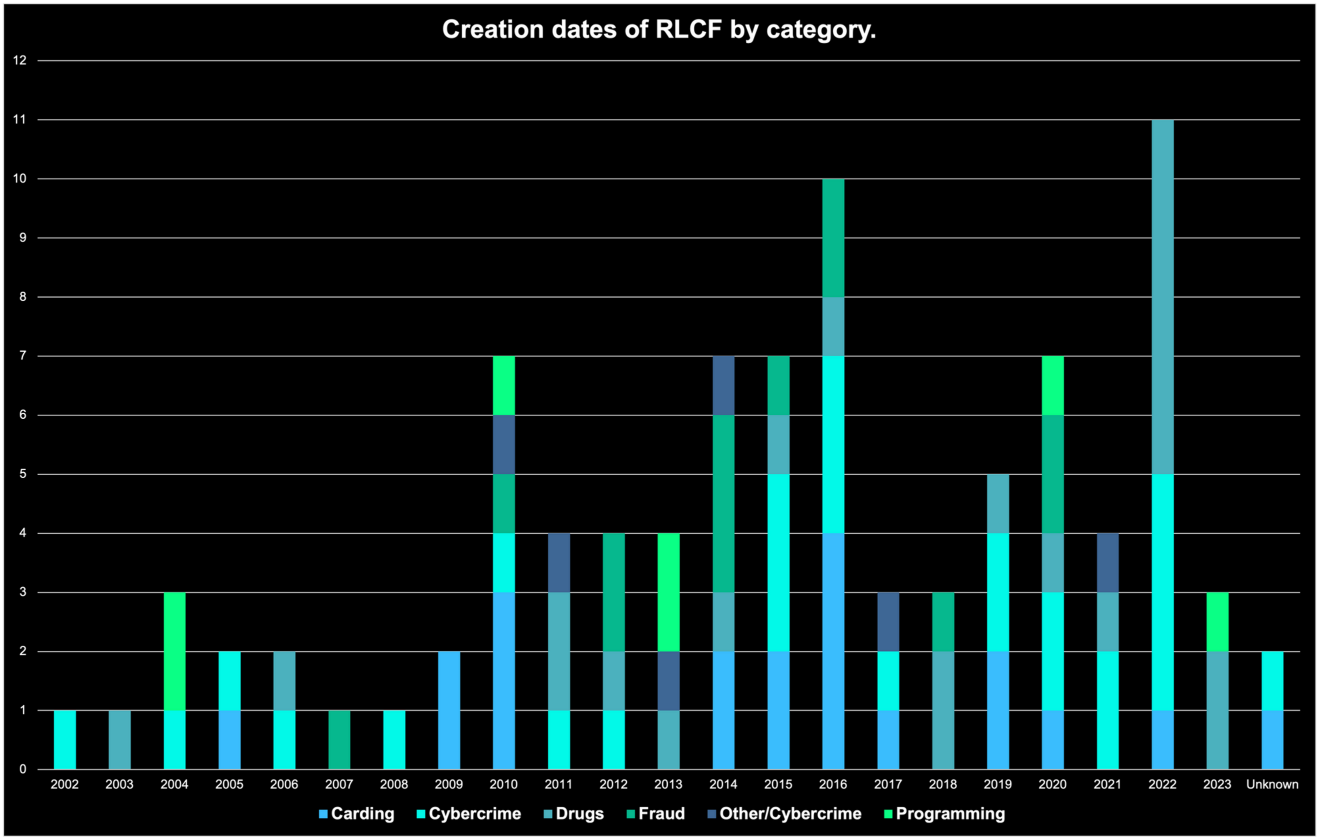

Assessed level of activity of RLCF by category.
9
8
3
14
7
5
10
5
7
3
7
3
1
1
4
7
Carding
Cybercrime
Drugs
Fraud
Other/Cybercrime
Programming
Low
Average
High

Table 4. Methodology: Low activity – 1-20 messages/day, Average – 20-100 messages/day, High – over 100 messages/day. Source: Cybercrime Diaries – January 2024.



Creation dates of RLCF by category.

Table 5. Source: Cybercrime Diaries – January 2024.

C) Global observations and trends.

The inauguration dates and activity metrics of RLCF highlight noteworthy patterns within the cybercriminal landscape. Among the RLCF that are still active nowadays, only 20 were launched during the first ten years of the century, which highlights the high attrition rate among RLCF but also the durability of some key communities. A second cohort of presently active RLCF was established between 2010 and 2020, with a notable surge of new forums from 2014 to 2016. This period accounts for the creation of 54 RLCF that maintain activity today.

Carding – as one of the oldest cybercriminal craft – is a good illustration of how evolution in popularity and profitability of a particular cybercriminal craft can affect the whole ecosystem itself. A significant proportion, 15 out of 20 RLCF dedicated to carding, commenced operations between 2010 and 2020, reflecting sustained interest in this illicit activity. Nonetheless, the proliferation of carding sections within Cybercrime, Fraud, and even Drugs forums have intensified competition for an active user base. In recent times, numerous carding focused RLCF have shuttered or fallen into disuse, with 9 currently exhibiting low activity. The enduring presence of carding forums, despite the migration of their participants to Telegram, can be partly attributed to the lower barrier to entry in this illicit trade, which does not always necessitate sophisticated technical skills.

The rise of Ransomware as a dominant threat to enterprises, particularly post-COVID pandemic, has concurrently become a profitable venture for cybercriminals. RLCF such as "XSS" and "Exploit" are recognized as hubs for ransomware operators and initial access brokers. Following the Colonial Pipeline cyberattack in 2021[17], leading RLCF temporarily prohibited discussions related to ransomware – a strategic deception. This environment encouraged the notorious ransomware operator, Mikhail Matveev, known as "wazawaka," to establish "RAMP" (Ransomware Anonymous Market Place – not to confound with the famous Drugs forum named Russian Anonymous Marketplace, which was closed in 2017), a forum dedicated to ransomware activities and aiming at facilitating them. Despite initial traction, RAMP's growth has been hampered by the erratic conduct of its founder. Its activity level gradually increased since the transfer of ownership to the threat actor Stallman in 2022, but it is still trailing behind forums like "XSS" or "Exploit". This suggests that ransomware, though it is one of the biggest cybersecurity threats, cannot gather a huge community only by itself and remains a specialized subset within the wider cybercriminal milieu.

Although apparently not directly linked to hacking, Drugs RLCF are gigantic cash generating machines who have their own money laundering system that is used by other cybercriminals, including the ransomware business. One of these platforms was the Russian language marketplace “Hydra” closed by German authorities in April 2022[18]. Since then, 8 new Drugs RLCF were launched, which illustrates the dynamism of the ongoing competition between drug dealers targeting the CIS market. After the closure of the marketplace “Hydra”, RLCF like RuTor, Legalizer, and WayAway saw a surge in registrations, accruing between

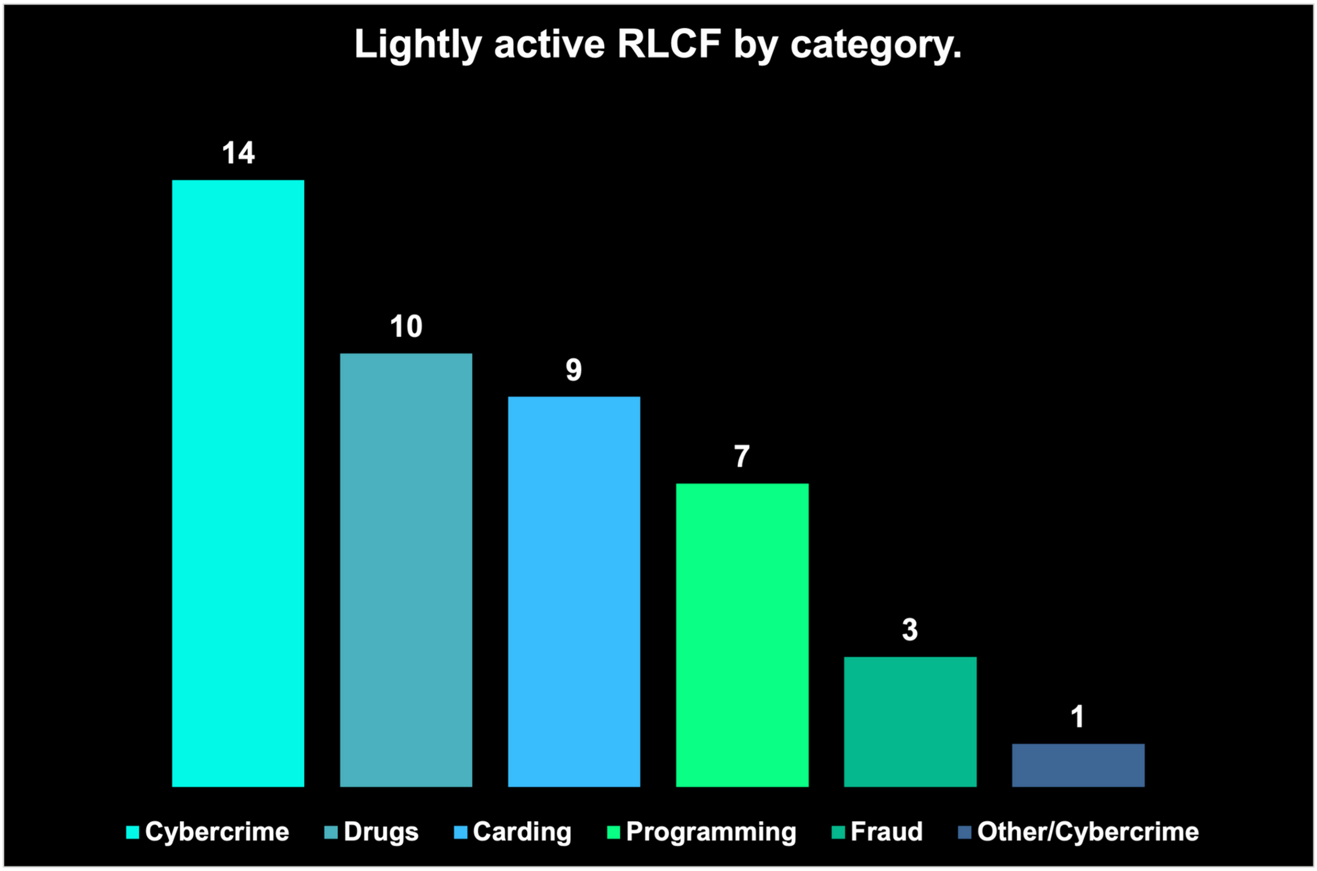
160,000 to 300,000 new accounts each[19]. On the other hand, the Russian invasion of Ukraine had a negative impact in the Drugs RLCF targeting the Ukrainian market. The Drugs forum Legalizer who is focusing on the Ukrainian market has seen the number of its users drop in 2023.

D) Lightly active RLCF – forums on the decline and new communities.

The majority of lightly active RLCF are rather old Cybercrime, Drugs, and Carding communities. Generalist forums such as “Prologic” or “Xaker” that were launched respectively in 2006 and 2007 are almost abandoned. A similar fate of relative decline can be witnessed on several old Carding forums. RLCF from this category like the forums “Carding forum” or “Monza” which were created in 2009 and 2012, went offline during 2023.

In the Drugs category 10 RLCF are lightly active. This is either explained by the fact that they appeared recently, like for example the forum Solaris, who is linked to a drugs marketplace of the same name, or because they are old but dying projects such as the RLCF “SKP”, thereby their future is hard to predict. As an example, the drugs RLCF “DeepRC” was launched in 2022 but did not survive. Further observation is needed to assess the viability of those forums.

In the case of Programing RLCF the assessment is easier to make as all the 7 forums that are dedicated to malware development are nowadays almost inactive. Their communities were absorbed by generalist Cybercrime forums where topics connected to malware development and programming are commonplace. Forums such as “WASM”, were particularly interesting to follow at a period of higher activity because several moderators of "XSS" and "Exploit" have started their cybercriminal activities there. Interestingly, the “R0” forum migrated to its own Telegram channel, but the latter is also not very active lately. The creation of the forum “RootZone” is nevertheless an interesting development that can be considered as a risky investment considering the fate of other communities in this category.



Lightly active RLCF by category.

Table 6. Source: Cybercrime Diaries – January 2024.

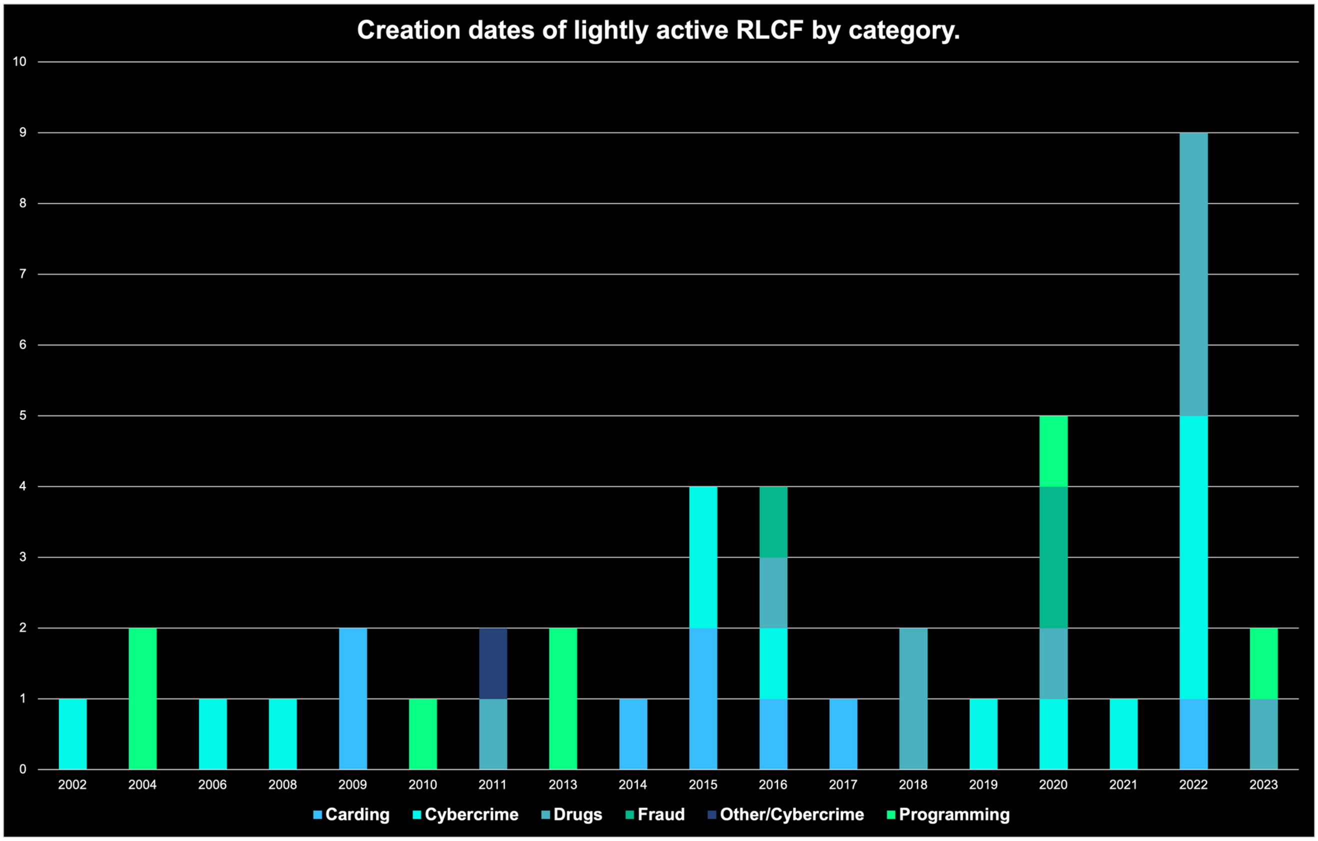

Creation dates of lightly active RLCF by category.
10
9
8
7
6
5
4
3
2
1
0
2002
2004
2006
2008
2009
2010
2011
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
Carding
Cybercrime
Drugs
Fraud
Other/Cybercrime
Programming

Table 7. Source: Cybercrime Diaries – January 2024.

E) Moderately active RLCF – at a crossroad.

The group of RLCF with a daily message count ranging on average between 20 and 100 messages are mainly composed of Cybercrime and Carding communities. Moderately active RLCF are nevertheless way more important for the cybercriminal ecosystem than the declining or new forums. This group includes forums that are often at a crossroad as they were in the past either popular forums or are new forums that are on the rise.

The famous generalist forum “Antichat”, launched in 2002, and the Carding forum “Verified”, created in 2005, were both at some point very trendy and attracted an extensive cybercriminal community, but lately their popularity is declining. It is hard to assess if they will grow again or fade into insignificance. Meanwhile, new communities such as “Antimigalki”, “DeepWeb” or “Lozerix” have managed to attract several thousands of users and could become important congregation places in the future if they maintain the current ascending trend.

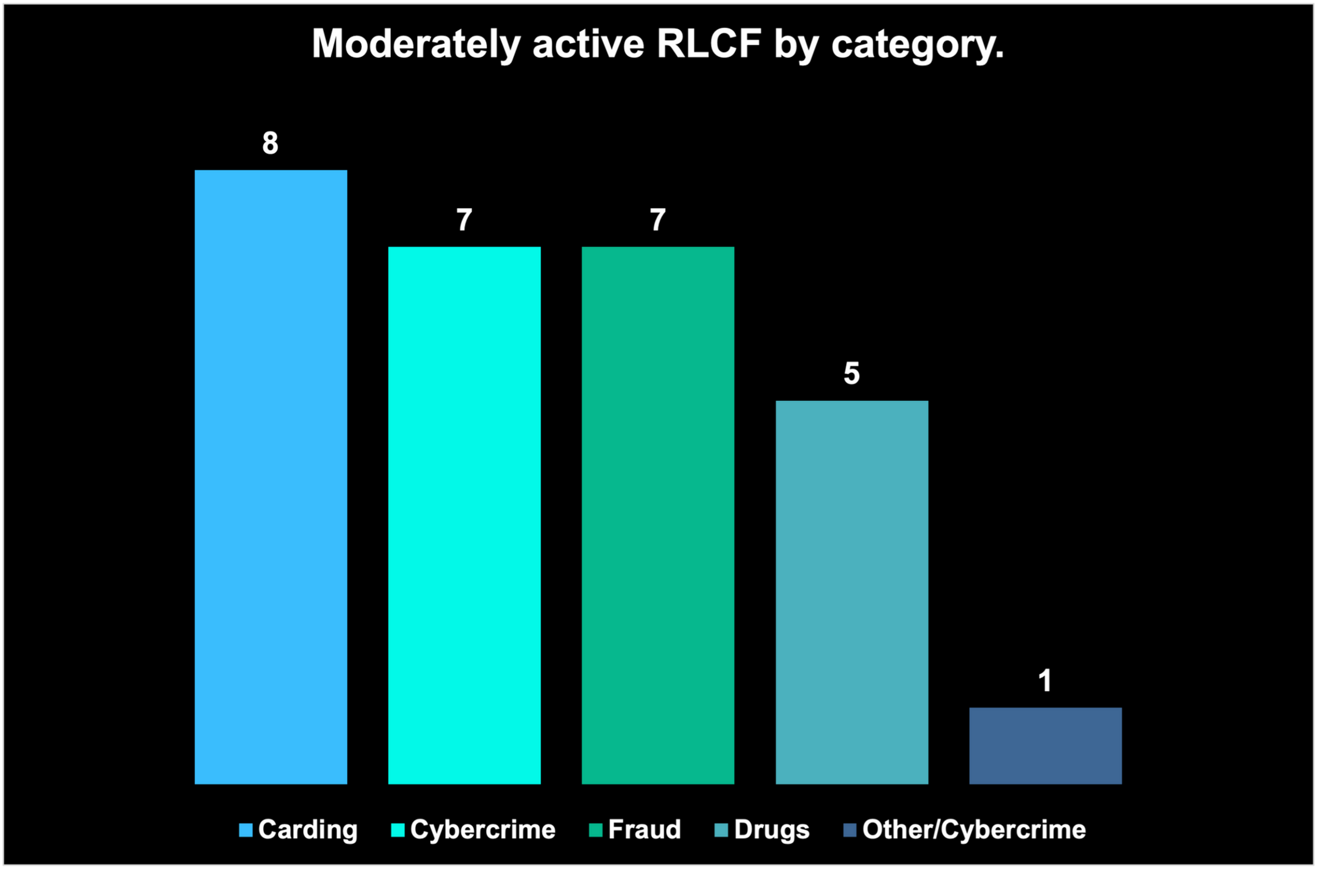


Table 8. Source: Cybercrime Diaries – January 2024.

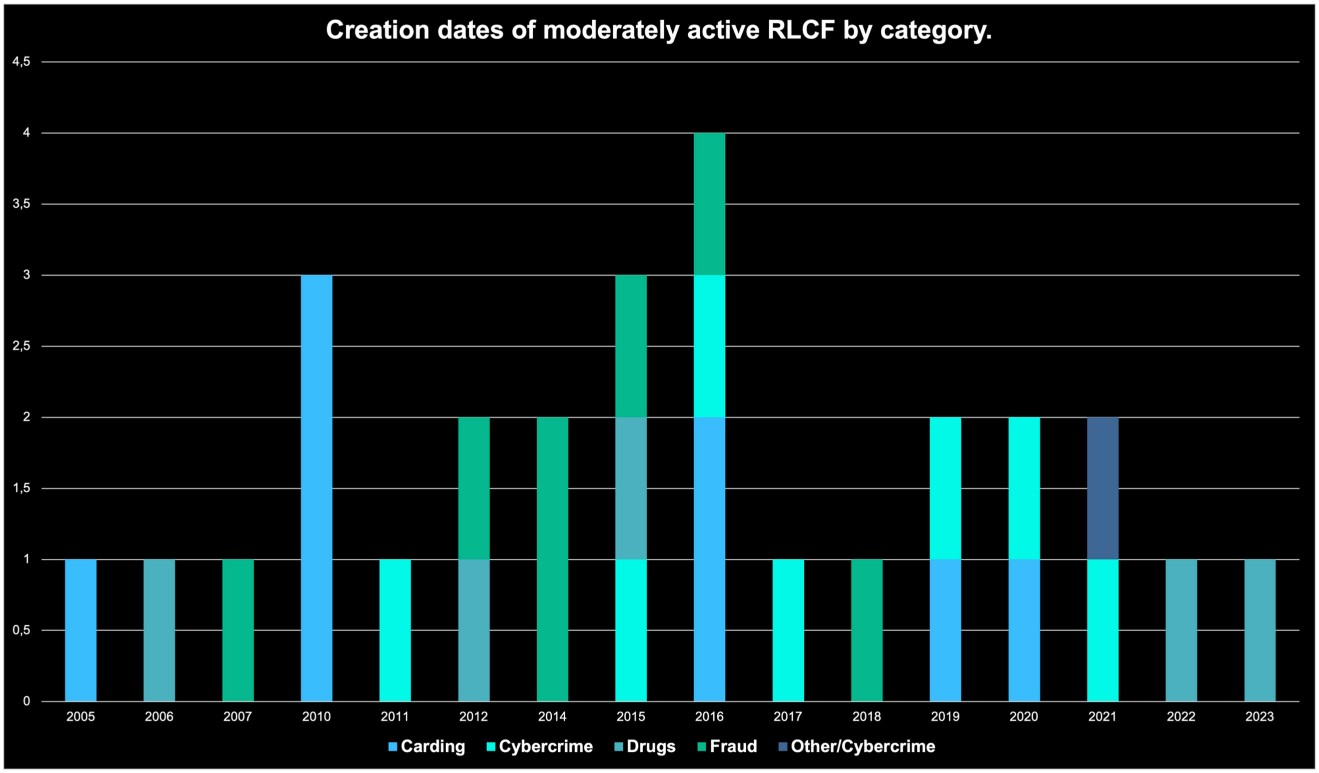

Creation dates of moderately active RLCF by category.
4,5
4
3,5
3
2,5
2
1,5
1
0,5
0
2005
2006
2007
2010
2011
2012
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
Carding
Cybercrime
Drugs
Fraud
Other/Cybercrime

Table 9. Source: Cybercrime Diaries – January 2024.

F) Highly active RLCF – the core of the Russian language cybercriminal world.

Finally, let us have a look at the highly active RLCF, it appears that they are mainly composed of communities focusing on Fraud, the sale of Drugs and gaming forums allowing cybercriminal activity. These groups encompass specialized forums offering illicit financial services, lookup services, creation of fake documents, and of course, various drugs. Successful forums from both categories were mainly launched in the last ten years.

On the contrary, the most prominent forums of the Cybercrime category are old. “XSS” (initially named DaMaGeLaB) and “Exploit” were created respectively in 2004 and 2005, while the less famous but still popular RLCF “BHF” was created in 2012. Thereby, the high-level Russian-speaking hacking community involved in ransomware attacks, advanced malware development and vulnerability identification is to a certain extent concentrated around a small number of reputable forums.

Nevertheless, as we are going to see in the Chapter III, RLCF with less advanced communities, like “LolzTeam”, from the Other/Cybercrime category, are playing a crucial role in the Russian language cybercriminal ecosystem as they gather huge communities of youngling who get familiarized with hacking and illicit activities by, for instance, joining traffers teams.

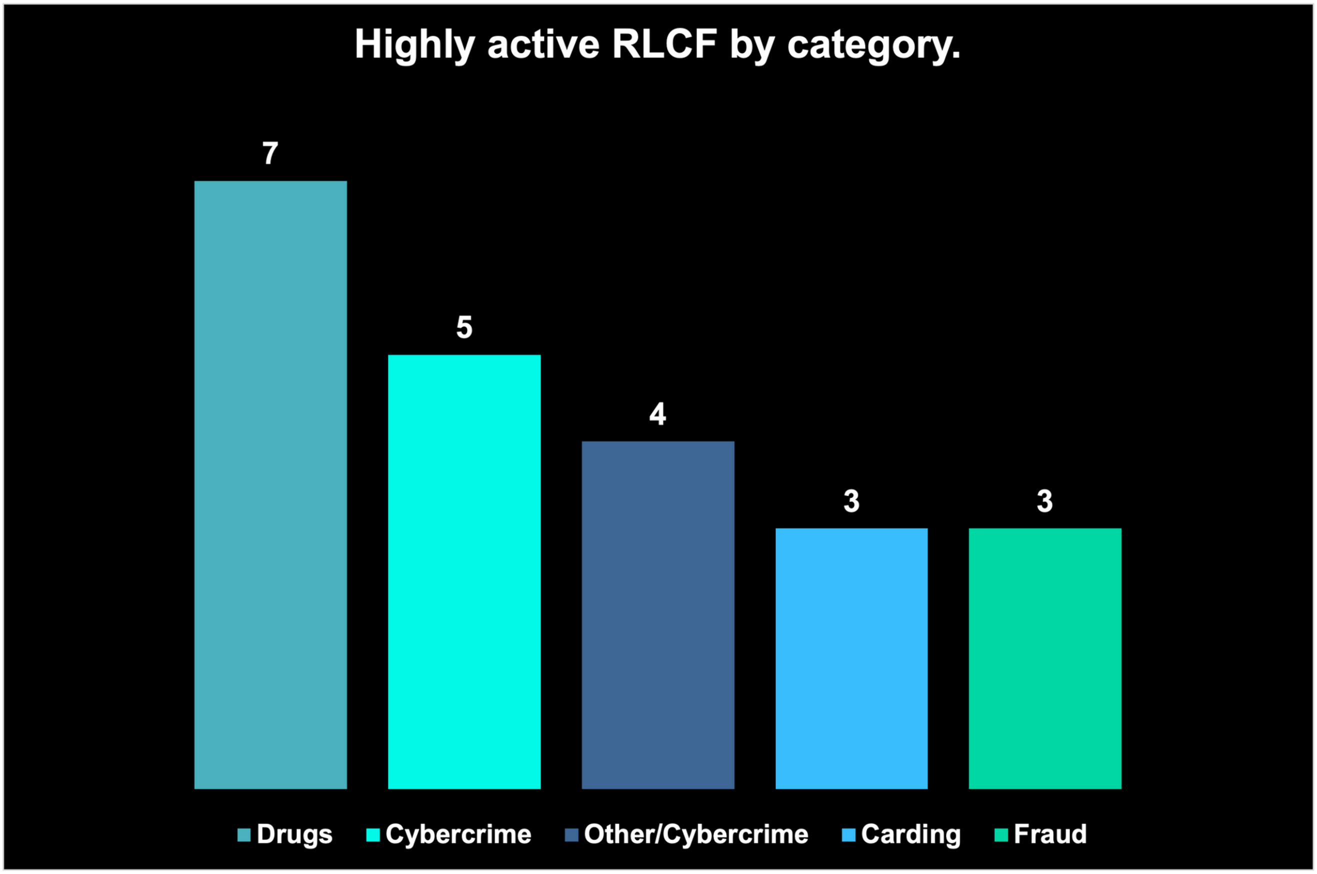


Table 10. Source: Cybercrime Diaries – January 2024.

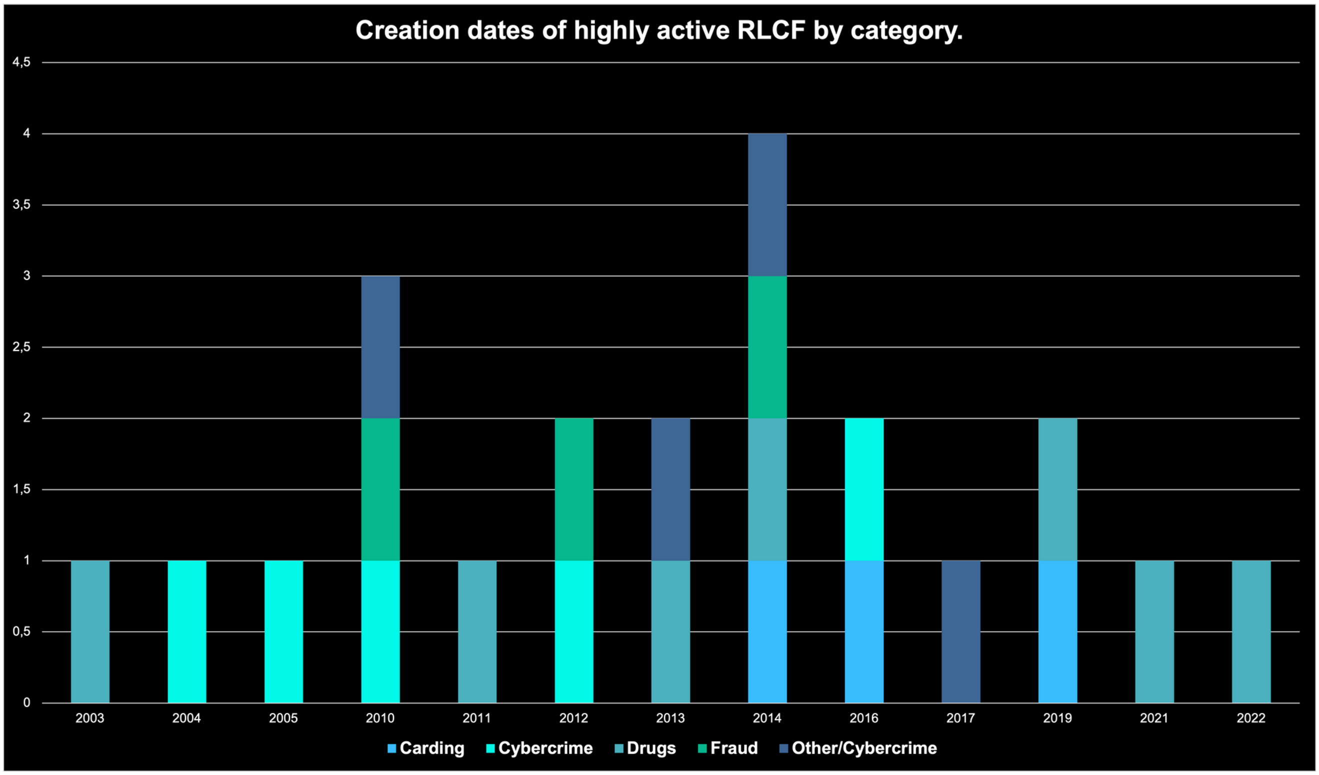

Creation dates of highly active RLCF by category.
4,5
4
3,5
3
2,5
2
1,5
1
0,5
0
2003
2004
2005
2010
2011
2012
2013
2014
2016
2017
2019
2021
2022
Carding
Cybercrime
Drugs
Fraud
Other/Cybercrime

Table 11. Source: Cybercrime Diaries – January 2024.

I hope you have enjoyed this first Chapter and are eager for more in the next one!

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

Sources:

[1] Max Goncharov, “Russian Underground 2.0,” n.d.

[2] “Отомстил за унижения: ветеран следствия рассказала, как ловили первого хакера СССР,” accessed December 28, 2023, https://bloknot-samara.ru/news/otomstil-za-unizheniya-veteran-sledstviya-rasskaza-1500195.

[3] “Office of Public Affairs | Russian National Arrested and Charged with Conspiring to Commit LockBit Ransomware Attacks Against U.S. and Foreign Businesses | United States Department of Justice,” June 15, 2023, https://www.justice.gov/opa/pr/russian-national-arrested-and-charged-conspiring-commit-lockbit-ransomware-attacks-against-us.

[4] “The World Of Russian,” RadioFreeEurope/RadioLiberty, June 6, 2019, https://www.rferl.org/a/the-world-of-russian/29984902.html.

[5] Lucie Kadlecová, ‘Russian language Cyber Crime: Reasons behind Its Success’, n.d.

[6] Amy Harmon, “Hacking Theft of $10 Million From Citibank Revealed,” Los Angeles Times, August 19, 1995, https://www.latimes.com/archives/la-xpm-1995-08-19-fi-36656-story.html.

[7] Diasp, “Вне закона: самые известные кардеры,” Diasp.pro - Арбитраж Трафика и Заработок в Интернете, December 6, 2021, https://diasp.pro/vne-zakona-samye-izvestnye-kardery/.

[8] Matt Richtel, “CREDIT CARD THEFT IS THRIVING ONLINE AS GLOBAL MARKET,” The New York Times, May 13, 2002, sec. Business, https://www.nytimes.com/2002/05/13/business/credit-card-theft-is-thriving-online-as-global-market.html.

[9] Probiv is a type of service provided by threat actors specialized in gathering personal data about their targets. Probiv service providers offer to try to find the information about their targets from open sources and from stolen private and governmental databases.

[10] “Интересно - Слив exploit,” UfoLabs - Лаборатория нло, July 19, 2019, https://ufolabs[.]net/threads/cliv-exploit.6198/.

[11] “BHF Взломали,” Информационный портал DARK2WEB, September 9, 2020, https://dark2web[.]org/threads/126993/.

[12] “Freedom Fox - Форум Exploit[.]in Был Продан СБУ,” XSS[.]is (ex DaMaGeLaB), accessed November 29, 2022, https://xss[.]is/threads/74967/.

[13] Ash Turner, “How Many Users Does Telegram Have? (Dec 2023),” April 1, 2023, https://www.bankmycell.com/blog/number-of-telegram-users/.

[14] ‘Mastermind Behind Andromeda Botnet Arrested in Belarus’, accessed 16 April 2023, https://www.recordedfuture.com/ar3s-behind-andromeda.

[15] “Cyberattaque de Colonial Pipeline,” in Wikipédia, January 15, 2022, https://fr.wikipedia.org/w/index.php?title=Cyberattaque_de_Colonial_Pipeline&oldid=189910790.

[16] “What Is an “info-Stealer"? (Part Ⅰ),” InfoStealers (blog), accessed December 30, 2023, https://www.infostealers.com/article/what-are-info-stealers/.

[17] “The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years | CISA,” May 7, 2023, https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

[18] “Sanctions on Darknet Market and Ransomware-Enabling Virtual Currency Exchange,” United States Department of State (blog), accessed December 30, 2023, https://www.state.gov/sanctions-on-darknet-market-and-ransomware-enabling-virtual-currency-exchange/.

[19] “Resecurity | Dark Web Markets Compete for the Drug Trafficking and Illegal Pharmacy Monopoly,” accessed February 20, 2023, https://www.resecurity.com/blog/article/dark-web-markets-compete-drug-trafficking-illegal-pharmacy-monopoly.