



THE **DARK SIDE** OF RUSSIA

How New Internet Laws & Nationalism
Fuel Russian Cybercrime

Table of Contents

3 Intro

4 Chapter 1: The Russian Cyber-Political Landscape

6 Sovereign Internet Law

8 Russian Cyber Warfare

10 Chapter 2: The Russian Cybercriminal Underground

11 The Process for Gaining Entry to Russian Hacking Forums

12 Russian Hacking Hubs

13 Tools, Tactics, Procedures

16 Carding and Hacking Forums

17 Insider Trading Forums

18 Conclusion

The Russian cybercriminal underground is a complex, sophisticated, and bustling hive of activity, continuing to thrive alongside the government's new restrictive internet policies that censor information and limit the content citizens can access. This report breaks down Russia's attempts to crack down on free internet use and illustrates the implications for businesses, consumers, and cybercriminals alike. It also provides a comprehensive breakdown of cyber threats originating on the Russian dark web and delves into the serious implications of Russia's state-sponsored cyber warfare tactics, designed to cause political unrest in numerous Western-world democracies.

Russian threat actors are known for developing advanced malware programs and innovative attack methods. They have launched large-scale cyberattack campaigns against global organizations and governments alike, resulting in massive data breaches, espionage, election meddling, and many other types of malicious activity. The geopolitical implications of the Russian cybercriminal underground are massive, and companies around the world need to keep a close eye on the underground Russian threat actor community.

But now, the Russian government is closing off internet access to the outside world, seeking to shield itself from foreign offensives and lock down sensitive internal information. Russia's new internet censorship mandate—modeled after China's "Great Firewall"—will change the landscape of the internet in Russia forever, including that of the cybercriminal underground.

Russia is a proud nation with a strong sense of nationalism, and the government has increasingly used cybercrime to wage cyber warfare and retaliate against organizations—both government and commercial—that oppose national interests.

Key Findings and Takeaways

- **Sovereign Internet Law:** Russia's new internet censorship law is set to restrict access to content and information the government deems to be oppositional, causing a ripple effect for businesses and users alike.
- **Political Influence and Cyber Warfare:** The Russian government disrupts and influences the political landscape in adversary states by hacking anti-Russian political candidates and releasing private or confidential information to foster instability.
- **Robust Cybercrime Underground:** The cybercriminal community in Russia is both vast and incredibly advanced. Russian hackers have developed cutting-edge malware and have been the first to discover new vulnerabilities since the community's development in the early 2000s.
- **Insider Trading Forums:** Russian threat actors can provide unprecedented levels of detail, including passport information, photos, marriage history, registered instances of border crossings, times associated with the use of domestic transportation services, video surveillance in certain cities, criminal investigations, and real estate information.
- **Early Bluekeep Access:** The latest Microsoft RDP vulnerability, CVE-2019-0708, dubbed Bluekeep, appears to have made the rounds on the Russian dark web long before Microsoft announced it to the world.
- **Black Markets and Forums:** The dark web is home to many Russian black markets that deal in malicious applications, stolen data and personal information, and other illegal goods and services. Russian cybercriminals have become more welcoming to new users over the years, realizing they can better monetize their assets by increasing their buyer bases.



Asia has many prominent cybercriminal outposts. Read our report on the vibrant dark web underground in the region.

[DOWNLOAD YOUR COPY](#)

THE RUSSIAN CYBER-POLITICAL LANDSCAPE

The Russian state has always been known for the control it has over its security forces. Be it the Soviet background, the vastness of the state itself, or the nature and culture of its people, Russia's government has always exerted strong control over its citizens. In recent years, the Russian government has identified the cyber landscape as a potential weakness and has tightened its grip on citizen internet freedoms. Increasingly restrictive censorship and anti-privacy legislation has been passed repeatedly and rapidly under the pretenses of state and individual security, emphasizing anti-terrorism. Russia's government attempts to regulate any entity that opposes the state or the status quo as part of its attempt to control the cyber landscape.

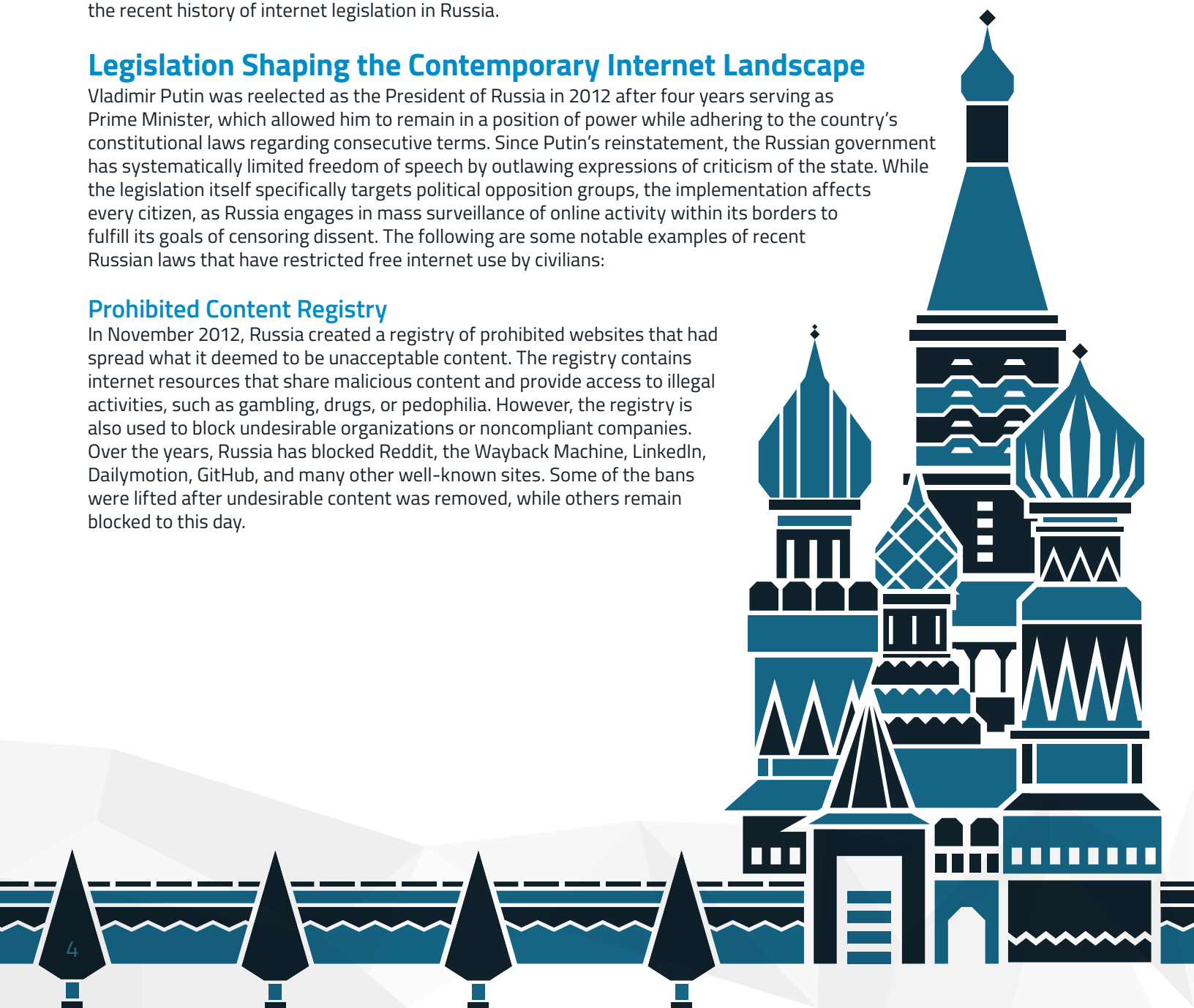
With specialized hardware and software installed in every Russian internet service provider, governmental and law enforcement agencies now have on-demand access to the private data of Russian citizens without the need to provide a court order. With the implementation of the new Russian Sovereign Internet Law, Russia could disconnect its citizens from the world wide web, further restricting internet freedom for users and bolstering the government's already-tight grip on how the internet is used within its borders. To understand why this bill passed, it's important to take a look back at the recent history of internet legislation in Russia.

Legislation Shaping the Contemporary Internet Landscape

Vladimir Putin was reelected as the President of Russia in 2012 after four years serving as Prime Minister, which allowed him to remain in a position of power while adhering to the country's constitutional laws regarding consecutive terms. Since Putin's reinstatement, the Russian government has systematically limited freedom of speech by outlawing expressions of criticism of the state. While the legislation itself specifically targets political opposition groups, the implementation affects every citizen, as Russia engages in mass surveillance of online activity within its borders to fulfill its goals of censoring dissent. The following are some notable examples of recent Russian laws that have restricted free internet use by civilians:

Prohibited Content Registry

In November 2012, Russia created a registry of prohibited websites that had spread what it deemed to be unacceptable content. The registry contains internet resources that share malicious content and provide access to illegal activities, such as gambling, drugs, or pedophilia. However, the registry is also used to block undesirable organizations or noncompliant companies. Over the years, Russia has blocked Reddit, the Wayback Machine, LinkedIn, Dailymotion, GitHub, and many other well-known sites. Some of the bans were lifted after undesirable content was removed, while others remain blocked to this day.



System for Operative Investigative Activities

In April 2014, the Russian government upgraded its mass surveillance system, SORM (which translates to “System for Operative Investigative Activities”). SORM is provided by the Federal Security Bureau (FSB), which has deep packet inspection capabilities. Installation is compulsory for all Russian telecommunications operators. SORM provides a direct interface to the data, allowing the FSB immediate access and negating the need to provide a court order to begin surveillance. The upgrade to the SORM 3 system increases the government’s surveillance abilities, as it gathers, stores, and filters data by the following criteria:

- IP addresses
- Web mail and instant messaging logins
- Email address
- IMSI (international mobile subscriber identity)
- IMEI
- MAC address

Data Localization Law

This law requires every company that processes the personal information of Russian citizens to store the data within Russian borders. The law, implemented in September 2015, was a direct response to Edward Snowden’s disclosure of the breaches of privacy that occurred under the United States NSA surveillance program. Companies that did not invest in physical infrastructure in Russia were blocked entirely. LinkedIn is a notable example of a site that is still not accessible in Russia as a result of this law.

Yarovaya Anti-Terrorism Law

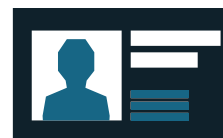
This law increased the authority of law enforcement agencies, allowing them to access data from Russian telecommunication providers without a court order. One of the amendments to the law requires telecom companies to store actual data of calls, text messages, and images for six months, as well as the metadata—time, location, sender, and recipients—for three years. The law also includes mandatory deciphering of encrypted channels. The Russian government banned Telegram, as it refused to provide decryption keys to its users’ correspondence.

VPNs and Anonymizers Law

This law requires every company that provides the means to use the internet anonymously to link and comply with the registry of blocked websites, and block access to restricted content within those anonymous networks. Taking effect in November 2017, the law forces Russian telecom providers to surveil VPN and proxy servers to detect the exact locations of their servers. Many VPN providers refused to comply, withdrew their physical presences from Russia, and now provide their services remotely to people within the country’s borders.

Messenger Identification Law

This law requires instant messaging service providers to verify any registered user’s real identity with mobile operators using their phone number. If a mobile operator does not have an ID on the number that tries to use instant messaging, the instant messaging provider must deny that user registration. The legislation was signed in July 2018 and just recently took effect in May 2019.



Sovereign Internet Law

Each of the above laws was merely a precursor to the massive Sovereign Internet Bill signed into law by President Putin on May 1, 2019. This law allows the Russian government to secure the world wide web within its borders, disconnecting from global internet infrastructure and facilitating mass surveillance and domestic internet control. The Russian Sovereign Internet Law is similar in nature to the Chinese Great Firewall, which similarly uses government authority to control its cyber space. The official Russia position is that the law is designed to protect its network from foreign intervention that might intend to disconnect Russia from the world wide web.

However, it can be interpreted to establish a means for closure of Russian access to the internet while still maintaining a functional internet inside the nation's borders. Under the law, while Russia states that it is preparing for a case in which foreign powers disconnect Russia from the internet, Russia could willfully disconnect from global root name servers, ensuring autonomous operation of Runet, the Russian internet sector. The law was adopted as a response to the aggressive nature of the United States National Cyber Strategy released in September 2018, accusing Russia, Iran, and North Korea of conducting "reckless cyber attacks that harmed American and international businesses, our allies and partners without paying costs likely to deter future cyber aggression."

Here are the main points of Russia's new Sovereign Internet Law:

- Development of new rules for network traffic routing
- Establishment of cross-border and internal traffic exchange points
- Installation of government monitoring hardware on traffic exchange points
- Creation of national domain name system

The Sovereign Internet Law is very vague and does not clearly define the threats, hardware, and software to be implemented. To date, there is no clear plan or division of authority, but the implications are clear: It will change how businesses and consumers alike use the internet in Russia.

There are a lot of similarities between the Chinese Great Firewall and the new Russian Sovereign Internet Law. Both Russia and China limit expression of free speech and prohibit criticism of the state. Both governments use any methods or technologies at their disposal to secure the current political status quo and distribution of power.

But despite all the similarities, it will take years for Russia to reach the advanced level of surveillance and content blocking seen in China—if it ever does. Runet was initially built to adhere to open Western standards, while the Chinese version was built as a controlled network from the ground up.

Beyond the inherently political nature of internet censorship, both China and Russia have clear financial motives: Blocking internet giants like Google, Facebook, Twitter, and others to replace them with internal counterparts like Weibo, WeChat, Yandex, VK, QQ, and Baidu provides an enormous economic boost to China's and Russia's domestic markets. Although Russia has similar domestic companies and products, it lacks China's population of more than 1.3 billion people who help fuel Chinese internet companies' success. In addition, Russia is officially a democracy and is still somewhat limited in the extent to which it can control its citizens before breaking the facade.

Over the years, the Russian government has implemented a series of cyber laws that have extended its control over media and telecommunication channels and their content. Russia has also implemented hard censorship and surveillance by providing an intrusive level of access to personal and private data. With the latest Sovereign Internet Law, Russia is centralizing its surveillance and censorship apparatus.



Implications for Businesses and Consumers

Implementation of the new hardware is subsidized by the government, but Russian telecommunication companies will have to accommodate installation and changes to network infrastructure. Companies will need to invest in the developed technologies and increase their storage space for data to adjust to the new laws. The operational costs will also increase for Russian telecom companies, and, as a result, for any company conducting business with them, and for consumers.

Decreased Stability in Communications

Although the law is presented as a measure to stabilize Runet against possible threats, the centralization of the internet infrastructure within Russian cyberspace will increase the chances of unexpected downtime and network outages, and the new supervision infrastructure will create traffic bottleneck points. This will make it easier to execute denial-of-service and traffic flood attacks. For example, Yandex—the Russian equivalent of Google—experienced a cyberattack while it was testing DPI hardware it was implementing to comply with this new law, reporting that most of its services were shut down due to the new hardware.

Implications for Dark Web Users

The first rule of Russian dark web communities is to never target victims in CIS countries, especially Russia. Hackers that engage in malicious activity in post-Soviet countries are arrested on a regular basis. The sovereign internet will make it much easier for Russian law enforcement to crack down on hackers that target Russian entities, but the government will still likely turn a blind eye to threat actors that target foreign entities—particularly those operating in enemy states, like the United States. For example, in March 2019, Russian authorities apprehended Maza-In, the creator of the Anubis Android banking bot that is currently wreaking havoc around the world. In addition to worldwide banks, Anubis targets some Russian financial entities. While there is no official statement from law enforcement, there are rumours in the underground that Maza-In is being recruited by Russian intelligence due to his technical abilities.

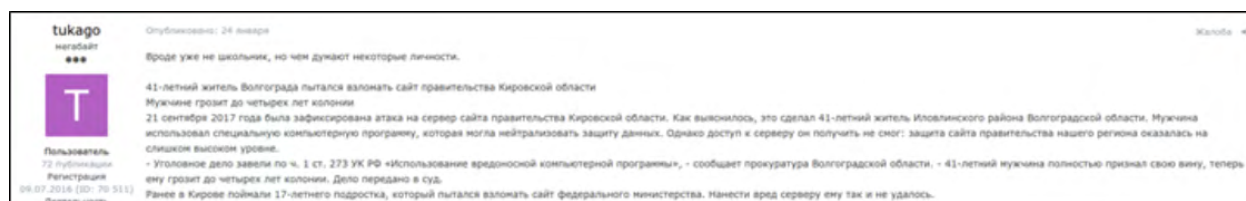


Figure 1: A post describing the arrest of a Russian hacker who tried to hack a local government site

In general, those engaged in activities on the dark web will have to invest more time and thought into building proxies and anonymizing their infrastructures. They will also need to conduct more thorough research of the VPN companies regarding their compliance—or lack thereof—with Russian laws and passing information to government agencies. There are discussions online about possible ways to bypass the new Russian government inspection equipment or alternative means of networking, but little has developed yet on that front.

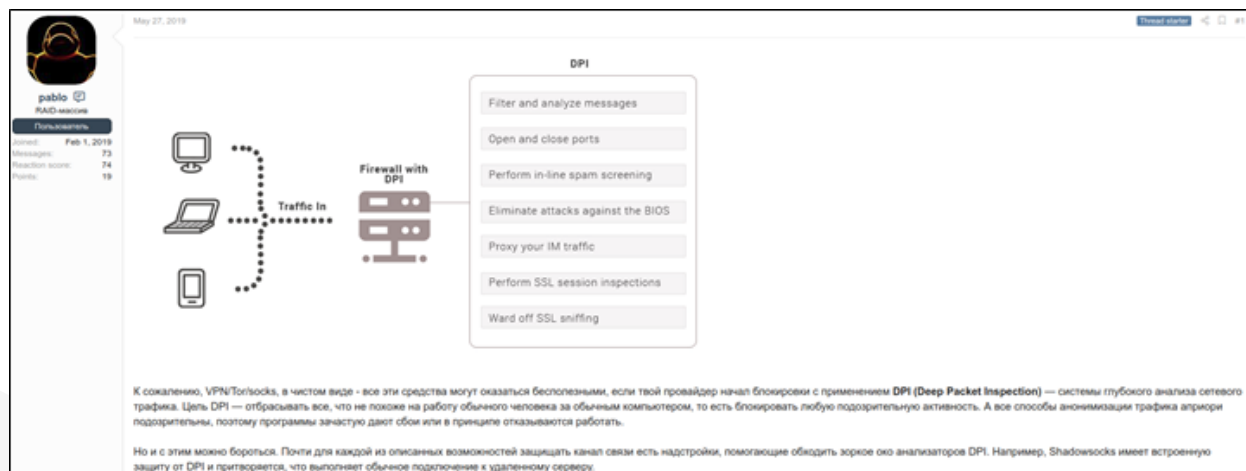


Figure 2: Discussion of possible methods to bypass DPI hardware

Russian Cyber Warfare

The recent internet laws have dramatically changed the internet landscape in Russia and will continue to do so for years to come. At the same time, Russia has a substantial history of conducting cyber warfare, which has also shaped its internet landscape. The Russian government has consistently pushed its political agenda with covert cyber operations in recent years. There are four major characterizations of the Russian cyber offensive.

Cyber Espionage

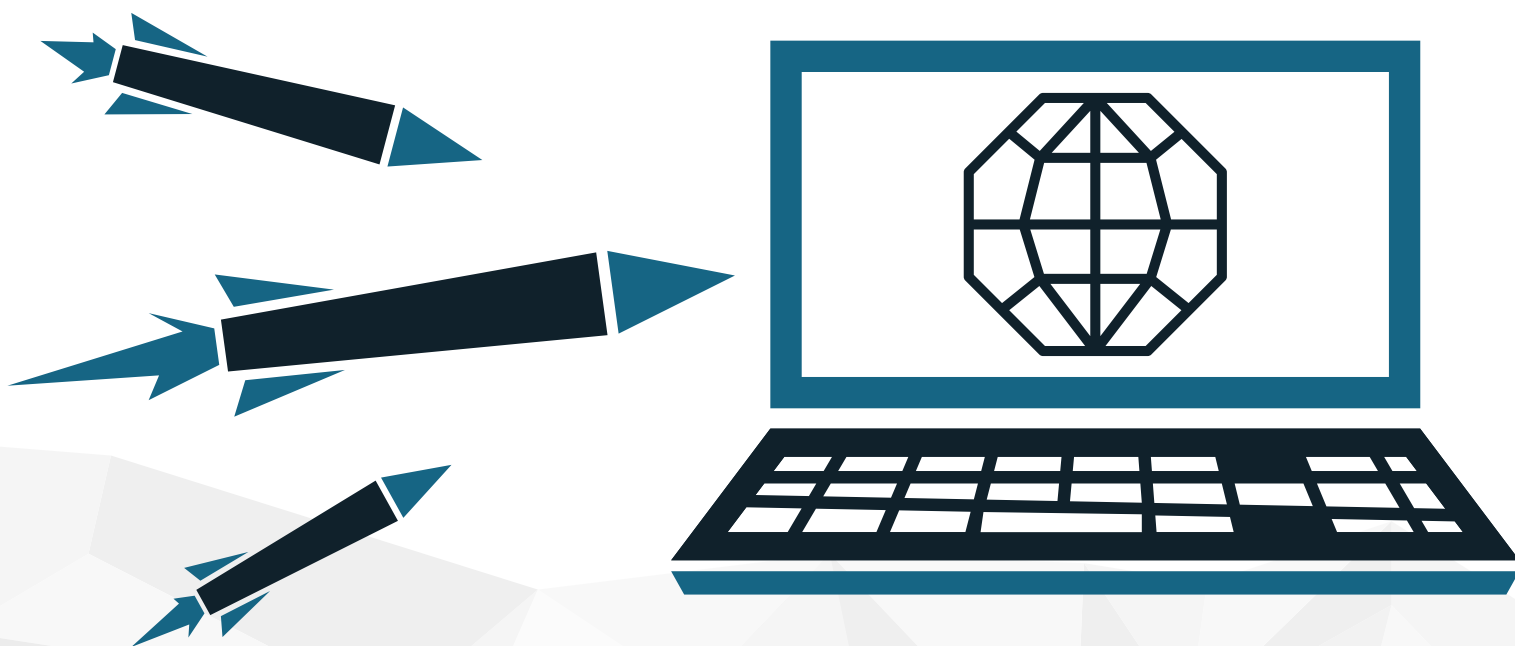
The Russian cyber espionage machine primarily targets critical infrastructure in adversarial states. It focuses on the energy sector, nuclear industries, the commercial sector, aviation, manufacturing, and other critical infrastructure. The Russian attacks are well planned, often last for years, are highly targeted, and employ various methods, including social engineering and specially developed zero-day exploits. The majority of reported attacks on critical infrastructure and industrial control systems use spear phishing through supply chains as a means of initial compromise. Hackers tend to pick less secure third-party vendors that have trusted relationships with the targeted entities and use compromised third parties as a foothold to infiltrate the actual target.

Retaliation

In some cases, the Russian government executes cyberattacks without any particular strategic gain besides a show of power. As a result of diplomatic tension between Russia and Estonia in 2007, when the latter wanted to move the Bronze Soldier monument to the fallen Soviet soldiers of WW2, the public outcry in Russia was enormous. The massive DDoS attack that ensued rendered Estonia's online banking, governmental email services, and media outlets unavailable.

Other examples of Russian retaliation were the attacks against the World Anti-Doping Agency in 2016 and International Association of Athletics Federations (IAAF) in 2017. Russian hackers orchestrated these attacks as payback for the ban on the Russian Athletics Federation in international competitions, including the Olympics. The hackers obtained and published sensitive and private documents of international athletes.

Olympic Destroyer, as the cyberattack against the IAAF is known, was not attributed directly to Russia, as it contains fingerprints of different state-sponsored APTs. However, it is likely that it may also be a product of Russian retaliation as most of its athletic team was banned from participating. The admitted athletes had to participate under the Olympic Flag and Olympic Anthem as any Russian attributes were barred.



Political Influence

The Russian government constantly attempts to disrupt and influence the political landscape in adversary states. This is usually carried out by hacking anti-Russian candidates and releasing private or confidential information, while promoting its allies, to destabilize the political stage. Another tactic used is an army of social media bots that spread fake news and misinformation.

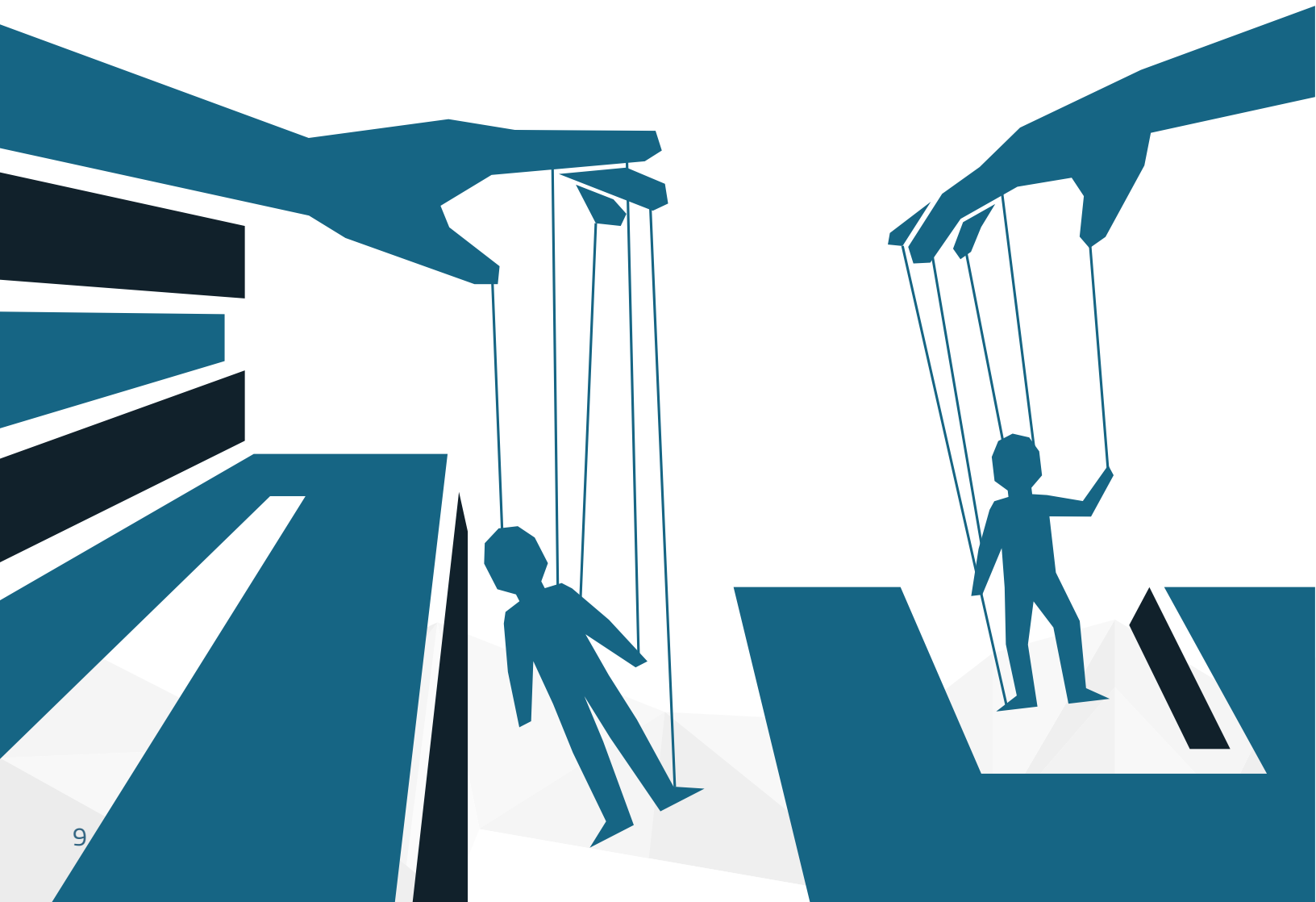
The government also attempts to breach anti-Russian parties and candidates. One of the most well-known examples is the hacking of the Democratic National Committee (DNC) during the United States general election in 2016. Russian threat actors successfully breached the DNC and released sensitive information about prominent candidates and party members.

Another known case occurred in 2017, when hackers accessed systems of French Prime Minister Emmanuel Macron's election campaign, releasing more than 20,000 emails that were posted across Twitter and Facebook.

Military Operations

Russia supports its military aggression with covert cyber operations to disrupt enemy communications and spread misinformation. During the Russo-Georgian War of 2008, Russia executed a massive denial-of-service attack on Georgian servers, targeting government and media infrastructure to prevent communication and crucial information distribution.

During the annexation of Crimea and war in Donbass in 2014, Russian hackers successfully infiltrated the Ukrainian government network via the Turla rootkit, disrupting communication and exfiltrating crucial intelligence. Russia successfully infiltrated the Ukrainian Army's Rocket Forces and Artillery with an infected mobile application. The original app was developed by the Ukrainian military to process targeting data and increase the artillery fire rate. The infected version of the application allowed the hackers to retrieve communication between Ukrainian forces and the location of their artillery batteries.



THE RUSSIAN CYBERCRIMINAL UNDERGROUND

Now that we've outlined some of the key factors influencing the Russian internet landscape, let's take a look at the underground Russian cybercriminal community. Before the development and popularization of the world wide web, the Russian hacking underground was relatively small and gathered in private bulletin board systems over FidoNet. As the internet started to take shape, Russian hackers began to congregate on the emerging cyber fraud forums that were available and easily accessible to anyone.

One of the first publicly available hacking forums that provided a place to share and discuss malicious activity was HackZone.ru, which was created in 1997. The forum had public and closed sections where users shared and discussed various security articles. HackZone.ru still exists today, but it was abandoned in 2012 and has had almost no activity since then.



Figure 3: The archived main page of HackZone.ru from 1998

The period between 2000 and 2007 shaped the Russian cybercriminal underground and hacking culture as they exist today. Central hubs for communication were created and evolved into communities, while various hacking resources rose and fell with great frequency.

In 2000, Carder.org was created as the world's first publicly available forum solely dedicated to obtaining credit card and banking information, as well as hacking methods. The forum was largely professional and highly targeted, prohibiting any discussions besides fraud-related topics and playing host to many major players in online cybercrime.



Figure 4: Example of carding tools for sale on carder.org

In 2001, carder.ru was created and shortly after was rebranded as CarderPlanet.com, which operated until 2004. CarderPlanet was initially a tight community with strong relationships and communication. Eventually, scammers and con artists overran the community, contributing to the decline and closure of the forum. Not long after, the creators of CarderPlanet were apprehended by law enforcement and sentenced to prison.

In 2005, the infamous exploit.in was created, rapidly gaining a reputation for its large user base, amount of posts, and threads, each of which doubled from year to year. In 2006, it had 1,910 users and 14,448 messages. In 2019, the forum reached almost 45,000 users and 976,115 messages—the highest in its history to date.

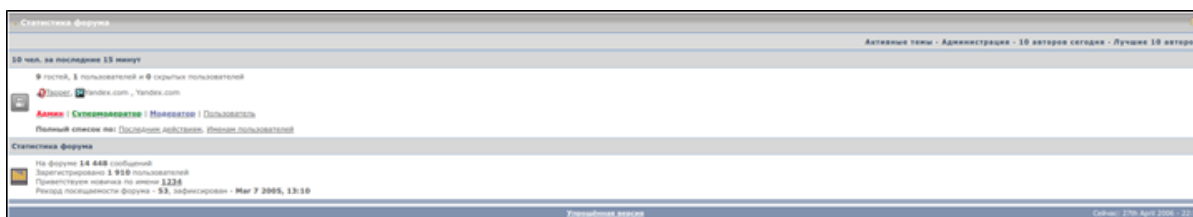


Figure 5: A look at 2006 usership of exploit.in, back in its formative days

The Process for Gaining Entry to Russian Hacking Forums

Initial entry into the Russian hacking underground is relatively simple. Most forums are accessible on the clear web, can be Googled, have open registration, and sometimes even have a “beginners” section with various educational articles and guides. Some forums with better reputations are more exclusive and allow entry only to users who have either paid, are established in other forums, have proven experience and knowledge in hacking disciplines, or have been vouched for by respectable forum members. This is done to prevent an influx of possible scammers and script kiddies, and to maintain the reputation of these more prestigious communities.

Some forums have closed sections that can be accessed only after a thorough verification process, which is often initiated by reputable users who already have access to the closed section. The candidacy is discussed by members. If the candidate is approved, rigorous interviews follow. At the end of the process, members of the closed section publicly vote on whether or not to provide access based on the interviews.

Another example of an exclusive closed community is the Cult of Russian Underground. The forum centers solely around the technical aspects of hacking and exploitation. Currently, it has very few users, and each of them underwent an interview process with highly technical questions and public voting. Any commercial activity is strictly prohibited, as this forum is intended for advanced technical discussion and education only.

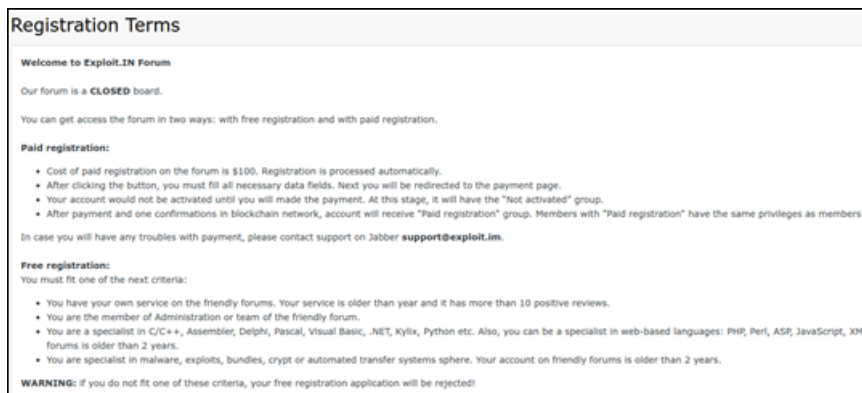


Figure 6: Exploit.in registration terms



Figure 7: Restricted sections of exploit.in

Russian Hacking Hubs

Threat actors in the Russian underground typically congregate on hacking forums. Many of them have chat rooms where hackers engage in general chatter. Initial contact is mostly done through private messages on the underground forums, then typically proceeds to more secure apps like Telegram or Jabber, two popular private instant messaging applications. In addition, many Russian hackers still use the ICQ instant messaging platform. The actual business is conducted mainly in Telegram and Jabber for maximum security. Some of the forums even offer their own Jabber servers. Russian hackers have a variety of Telegram channels where they discuss and share news and information, and learning channels are provided to teach courses for newcomers.

Communication Styles in Russian Hacking Hubs

The Russian hacking underground is an open community in that it does not use any specialized code or cipher to conceal communications. Technologies like Pretty Good Privacy (PGP) and end-to-end encryption have eliminated that need. The reason that translating Russian forums is difficult is because computer technologies and technical documentation are historically written in the English language, and the majority of the Russian hacking community does not speak English fluently. Community members usually know many of the standard technical terms, but they use “Russified” versions that have been derived from and substituted with similar-sounding Russian words.

Here is a list of new terms that entered the Russian hacking lexicon with the continued development of technology:

Term	Pronunciation	Description
Сплойт	Sployt	Derivative of exploit, literal meaning
Трафф	Traff	Derivative of traffic, literal meaning
Связка	Svyazka	Translated as bundle. Refers to exploit packs.
Отстук	Otstook	Translated as knock back. Refers to percentage of bots that “knock back” after being infected as a result of executing an exploit pack
Обход	Obhod	Translated as bypass. Refers to bypassing of defensive measures as UAC or Anti-Viruses.
Лодырь	Lodyir	Derivative of loader. Refers to the module of initial persistence that downloads main payload.
Админка	Adminka	Derivative of admin panel. Refers to the command and control interface of a botnet.
Дамп/Сдампить	Damp/Sdampit	Russian transliteration of dump. As a noun, it refers to a part of memory or to the magnetic strip of a credit card. As a verb, it refers to the process of saving part of the memory to the hard drive.
Крипт	Kript	Derivative of encrypt. Refers to the process of encrypting malicious code to obfuscate it from AV engines.
Шелл	Shell	Russian transliteration, mainly refers to web-shells.
Сигнатура	Signatura	Derivative of signature. Refers to signatures of the files in terms of obfuscation and signature-based detection mechanisms of antivirus engines.
Троянец, троян,трой	Trojanets, troyan,troy	Derivative of Trojan, literal meaning
Стилер	Stiler	Russian transliteration of stealer. Refers to password-stealing malware.
Носок/Сокс	Nosok/Soks	Literal translation of sock. Refers to socks5 proxy.
Килогер	Kiloger	Derivative of Keylogger, literal meaning
Картон/картофель	Karton/kartofel	Literal translation of Cardboard/Potato. Derivation of credit card.
Руткит	Rootkit	Russian transliteration of Rootkit, literal meaning
Жаба	Zhaba	Derivative of Jabber. Refers to the XMPP messaging app or to the Java programming language.
Брут	Broot	Derivative of Brute-force, literal meaning

The winds of change have been blowing throughout the Russian underground over the last few years. Russian forums are becoming more friendly, more patient, and more accepting toward newcomers. This cultural shift is due to the commercialization of malicious services and the migration to subscription-based models in dark web offerings. Nowadays, you do not need to be technically sophisticated to create a malicious campaign. You can hire the services of professionals who will support your operation, answer any questions, and give you a refund if their service is unsatisfactory. Scammers are getting banned swiftly by admins of respectable forums and escrow services, thus raising the credibility and quality of dark web services.

Tools, Tactics, and Procedures

The Russian underground covers virtually any known type or method of malicious activity. If news outlets are talking about it, it is likely Russian cybercriminals have already had it for some time. For example, the latest Microsoft RDP vulnerability CVE-2019-0708, dubbed Bluekeep, appears to have made the rounds on the Russian dark web long before Microsoft announced it to the world. On May 15, 2019—one day after Microsoft issued its notice about this critical vulnerability—a group of Russian hackers discussed their prior use of this vulnerability. While there is no hard proof of this, the discussion among numerous users—seen in the screenshot below—indicates that Bluekeep may have been a known exploit for months before Microsoft’s acknowledgement.

The latest malware trend among Russian hackers includes the use of Trojans with hidden VNC (hVNC) and hidden RDP modules. The technology is not new, having existed in malware such as Gozi v2 and Trickbot, but it seems that the demand for that particular module increased in 2019. Each new piece of malware that is offered in the Russian underground sees requests from potential buyers for the hVNC module, and the sellers stress the fact that they have it implemented.

The hVNC module provides attackers with a direct hidden connection to the infected machine while in use. This technique lets the attacker obtain an authentic digital fingerprint of the victim—such as cookies, stored sessions, or IP addresses. All this is paired with the stolen credentials, allowing the attacker to commit fraud or steal personal data through the victim’s machine. Russian hackers have already commercialized the process of selling metadata and personal details identifying their victims in black markets.

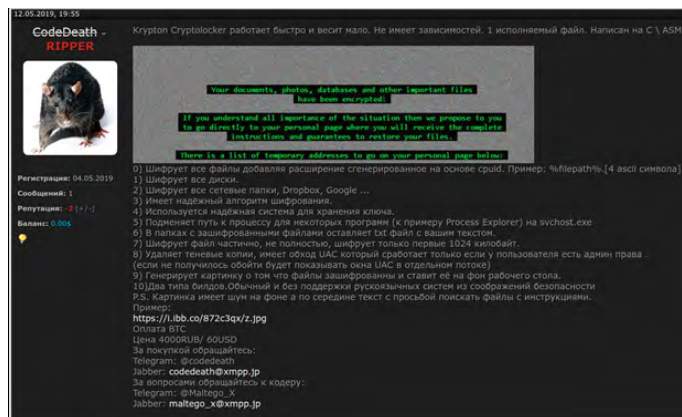


Figure 8: Seller offering Krypton ransomware-as-a-service that scammed his customers

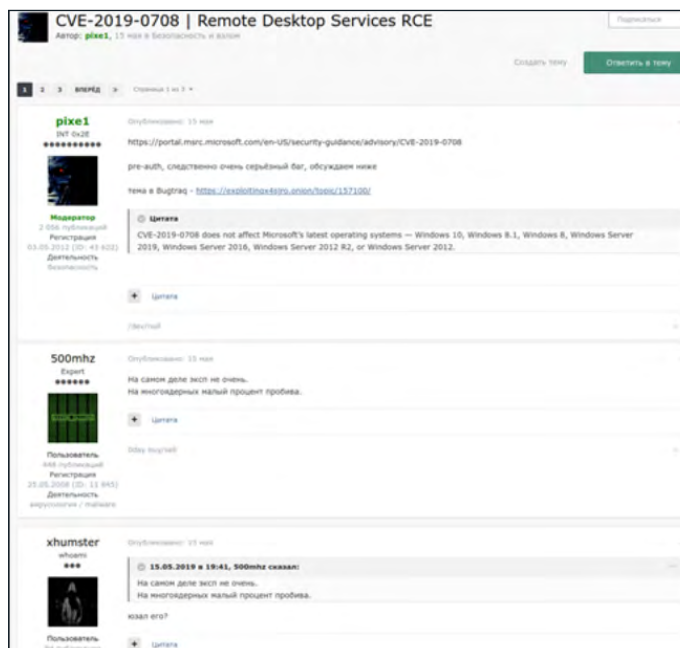


Figure 9: A thread regarding the Microsoft Bluekeep exploit with hackers stating they had used it prior to Microsoft’s acknowledgement of the vulnerability

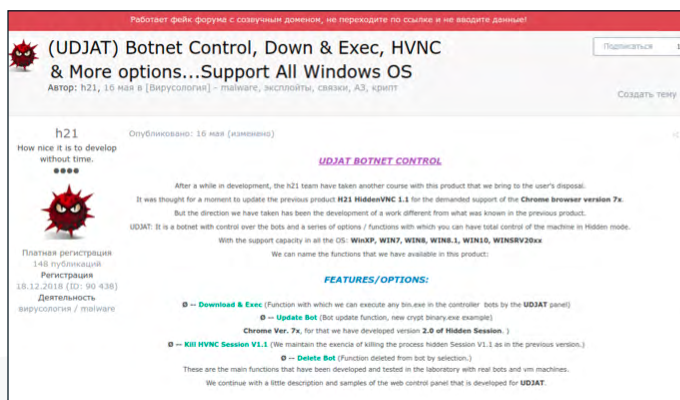


Figure 10: New Trojan UDJAT offered for sale, stressing hVNC capability

Clear and Dark Web Resources

The division of websites between the dark web and clear web in Russia is based on the attitude of the state toward the resource in question, and the potential damage it could inflict on the Russian government. In general, hacking-related services live and thrive on the Russian clear web, have common .ru top-level domains, and are accessible from within Russia. On these clear web forums, the Russian government looks the other way, as most members of these forums only target foreign nations—especially the United States and European countries. Targeting Americans is still considered “sticking it to the enemy” by Russian threat actors, as a remnant of the Cold War that has transitioned into cyberspace, and the Russian government is happy to turn a blind eye. Many of these clear web resources still have .onion mirrors, mainly to allow international users to take part.

Black Markets

Black markets that sell drugs, counterfeit currency, guns, or other prohibited goods are located mostly in .onion websites. Clear web mirrors are constantly monitored and closed by the Russian government. Those marketplaces began to grow in popularity in 2012 with the expansion of Bitcoin as a widely used anonymous currency. The most popular and successful marketplace in Russia was Russian Anonymous Marketplace (RAMP), which operated between 2012 and 2017. The market outlived other famous dark web markets like Silk Road and Agora, probably due to the strict policy of its creator, Darkside, who prohibited any political discussions, selling of child or even legal pornography, and illegal weapon sales. Anything that could bring the attention of authorities was banned and removed from the market. Providing services only to Russians allowed RAMP to survive Operation Onymous—carried out by joint international law enforcement—that closed Silk Road 2 and Hydra, as well as later joint operations that brought down Hansa and AlphaBay.

The closure of RAMP in 2017 was rumored to be an exit scam by the market’s new administrators, as Russian law enforcement notified the public about the closure three months after the market became unavailable and did not release any details regarding the operation.

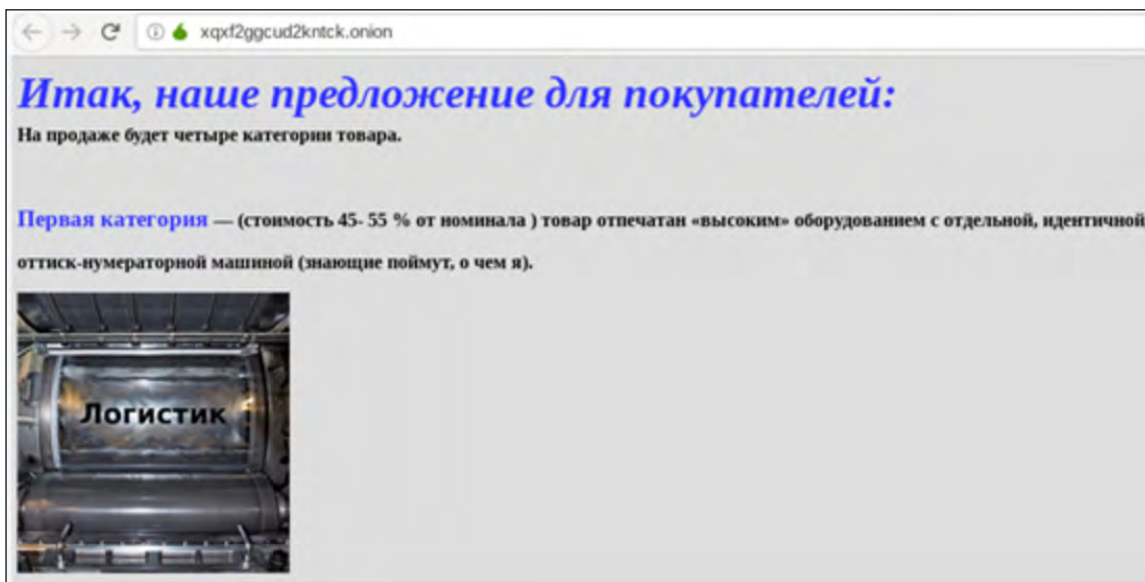


Figure 11: A .onion website offering counterfeit bills

RAMP’s niche was quickly filled by competitors, the biggest one being Hydra Market—a Russian market that opened with the same name as the now-defunct American version. Hydra was actively advertised and featured in YouTube ads for a short period of time as part of its promotion strategy. Hydra has more than 1,740 automated shops that mainly sell various drugs. The second-biggest offering is job openings within the cybercriminal drug underworld. There are more than 1,200 available jobs as couriers, warehouse managers, and those who are called “KladMan” (literal translation: treasure-man)—a person who delivers purchased drugs to secret drop sites. The market has its own legal and narcological services available around the clock. In addition to drugs, there are offerings of counterfeit money, fake documents, anonymizing services, and other digital goods.

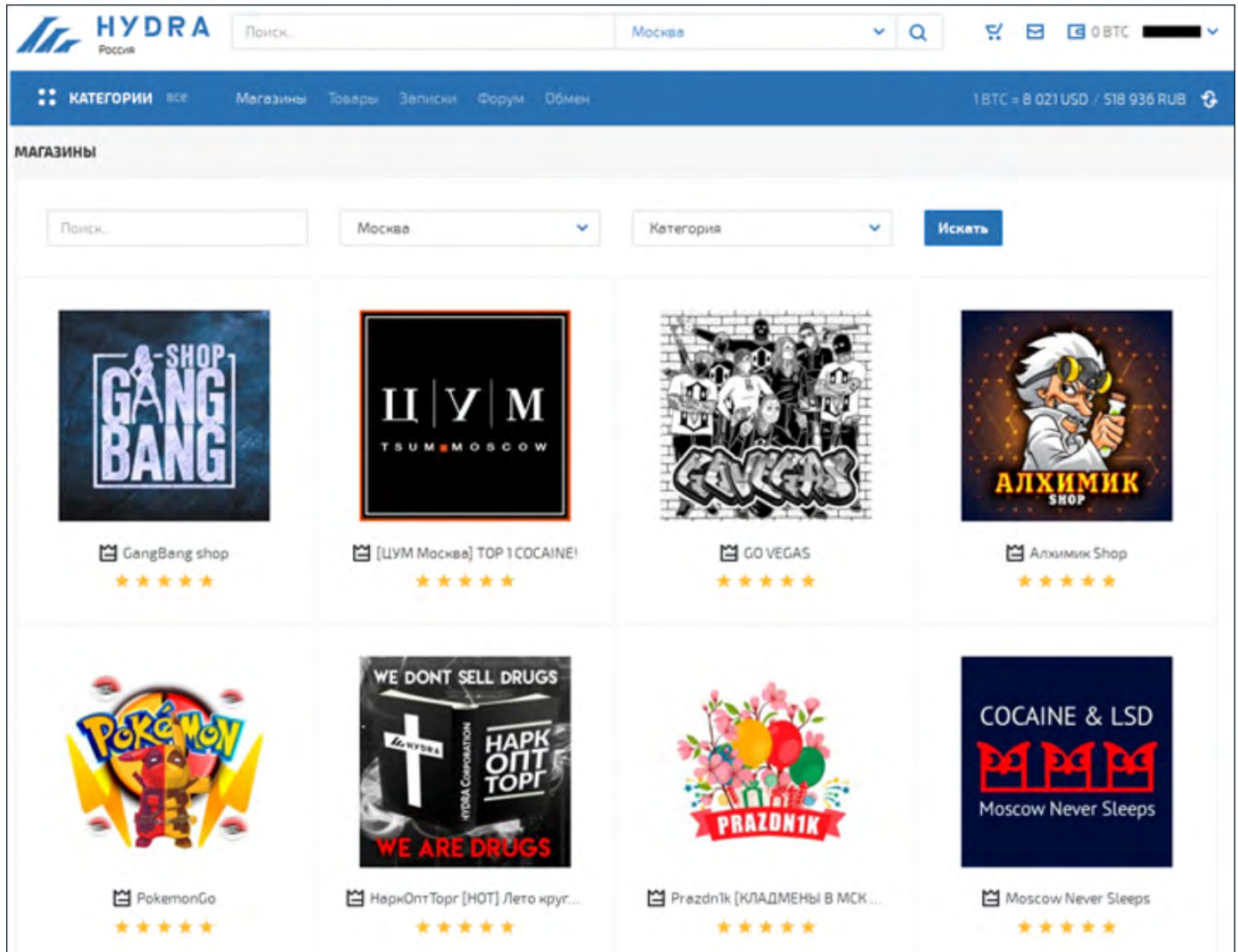


Figure 12: The Russian Hydra main page with some of its offerings

There is a high level of competition between Russian black markets. Rival markets actively execute DDoS and phishing attacks against their competitors to undermine their reputations and steal credentials. They also try to block sellers from using competitors—for example, Hydra does not allow double listing on rival markets.

Other big Russian markets include Russian Anonymous Shadowland (RASH), WayWay (an affiliate of Hydra), and Unity Market. All of them mainly sell drugs, with little deviation from market to market. However, others also provide insider trading and other services.

117 В целях повышения безопасности проекта, администрация HYDRA запрещает финансирующих и организующих DDoS атаки на наш сайт. Магазины должны сделать свой выбор и сообщить об этом администрации. В черном списке: darkcon, rutor, solaris, consortium.

Figure 13: Hydra's terms of service prohibiting double listing in other markets, such as darkcon, rutor, solaris and consortium

Forum Statistics	
Discussions:	1,125
Messages:	8,702
Members:	22,969
Latest Member:	lenengradbear

Figure 13: RASH market's forum statistics

Carding and Hacking Forums

The hacking forums in the Russian underground can mostly be divided into three themes: technical forums that revolve around coding aspects and nuances in malware; carding forums that specialize in credit card fraud, money-laundering, and other schemes; and insider trading forums offering information from within Russian companies and government agencies.

The division is based on the area of expertise and discussed topics. In general, these forums include segmented content for users of all levels of expertise and knowledge.

Technical Forums

The biggest and most well-known Russian hacking forum is exploit.in. Dating back to the early days of the Russian cybercriminal community, exploit.in gained a reputation as the place to conduct fraudulent business or ask for advice about particular technical problems. In an average week, the forum gains more than 100 new registered accounts, 200 newly opened threads, and over 1,300 comments.

The content of the forum covers virtually any threat actor need, from creating anonymous infrastructure to exfiltrating money from hacked bank accounts with two-factor authentication interception. It features a discussion section, a commercial section for auctions, and general listings. The following is a breakdown of the different categories of content:

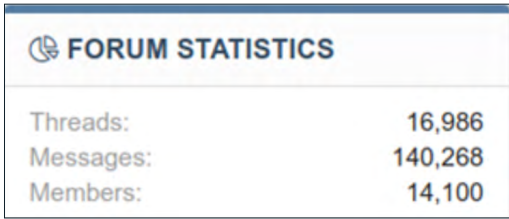
- **Virology:** Trojans, exploit-packs, crypting for files, loaders, and web-injects for all browsers and targets
- **Access:** Various resources, including web shells, RDP access, hijacked dedicated servers, admin credentials, and domain controllers of corporate networks
- **Servers:** Secure infrastructure like bulletproof hosting, quality proxy infrastructure, and VPNs
- **Social Networks:** Hacking and selling of email services, social networks, and other web services
- **Spam:** Email databases of various thematic and malspam services
- **Traffic:** Loading and installation services for malware
- **Mobile:** Services for SMS and spam calls, SMS and call interception, and various phone number databases
- **Payment Systems:** Various payment system accounts, e-wallets, exchange services, and cryptocurrency
- **Finances:** Banking accounts and related services
- **Jobs:** Jobs such as coders, pentesters, network administrators, and designers

Another rapidly developing technical forum is xss.is. The forum is a reincarnation of DaMaGeLab.org, which went offline at the end of 2015. Xss.is was created in September 2018 and swiftly developed a strong reputation among community members. Currently, there are more than 14,000 registered users.

Carding Forums

Carding forums are higher level and do not dive into the small coding details featured in technical forums. They tend to focus more on the final stage of fraud, which involves using or cleaning fraudulently obtained money. This might include methods for using stolen credit cards in legitimate markets, bypassing security measures, or buying goods and delivering them from abroad. Carding forums have sections discussing various scams or fraud schemes—both online and in person—and provide corresponding infrastructure, like forged documents and fake companies around the world, to complete fraudulent transactions.

One of the biggest carding forums in Russia is Club2Crd. As of June 2019, it had more than 36,000 threads, 234,000 messages, and 117,000 users. Like all malicious forums, Club2Crd has sections for the technical aspects of malicious campaigns, such as spamming, installation services, secure infrastructure, and more. The main vectors are credit cards, bank accounts, payment systems, and other similar services.



FORUM STATISTICS	
Threads:	16,986
Messages:	140,268
Members:	14,100

Figure 14: xss.is forum statistics



Figure 15: Threat actor selling debit cards together with the owners' passport scan, banking account, and sim card

Insider Trading Forums

One of the most distinguished features of the Russian underground is insider trading forums. The level of infiltration threat actors make into private and governmental entities is truly unprecedented and is not seen in any other country. Unlike other underground resources, insider trading forums work exclusively inside the Commonwealth of Independent States (CIS).

The biggest insider trading forum is probiv. As of June 2019, it had more than 50,000 threads, 585,000 messages, and 41,000 registered users. The core offerings are government entities, mobile operators, banks, credit history, and a separate section for uncategorized requests and offers.

The level of detail Russian threat actors can provide is frightening. They offer domestic and international passport information for individuals, including photos, marriage history, any registered instances of crossing borders, times using internal transportation services, video surveillance in certain cities, instances of all-points bulletins (APBs) that indicate a criminal being pursued by American or Canadian authorities or any other criminal investigation (including Interpol requests), and real estate information.

The infiltrated Russian government entities are:

- Ministry of Internal Affairs
- General Administration for Traffic Safety of the Ministry of Internal Affairs of Russia
- Federal Service of Court Bailiffs
- Federal Migration Service
- Federal Tax Service
- Pension Fund Agency

These threat actors have the capabilities of a full-scale intelligence agency and are constantly looking for employees of the targeted entities.

The dossiers produced are very thorough and highly detailed. They include passport details and histories, known addresses, family ties and relative information, lists of acquaintances or other affiliates, official and unofficial employment records, real estate or personal property, bank accounts, criminal and debt history, and movement within or through the border.

The mobile insider information provides registration details of the registered number, calling and messaging history, geolocation history, and the times of activity of mobile devices. There are a variety of forged and original documents offered for sale, such as passports, birth and death certificates, university diplomas, and others.

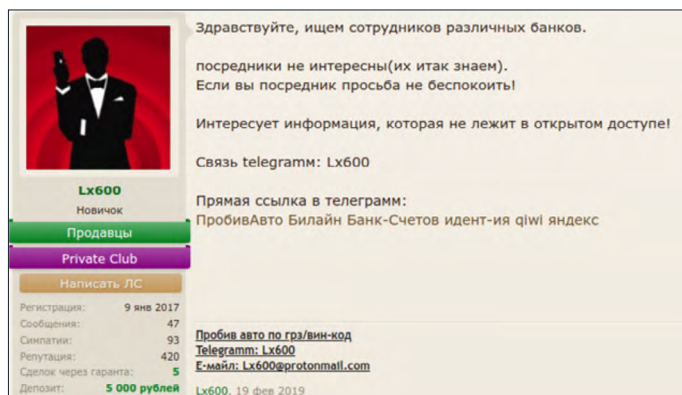


Figure 16: Threat actor looking for employees of Russian banks



Figure 17: An example of a dossier containing the subject's PII and mobile history

Conclusion

The underground Russian cybercriminal landscape is both incredibly advanced and widespread. There is no other hacking community that can boast such a breadth of knowledge, resources, and manpower. While the impact of Russia's new Sovereign Internet Law on clear web hacker resources is as of yet unknown, it is abundantly clear that the government, in many cases, turns a blind eye to cybercriminal activity that supports national interests—particularly if it targets geopolitical rivals, like the United States and Western European countries. Overt, state-sponsored cyber warfare is also likely to increase.

Cybersecurity teams face a daunting challenge when it comes to Russian cybercriminals, especially those working for organizations that may compete with Russian companies. Russian hackers are known for developing cutting-edge malware, exploit kits, and highly technical hacking methods.

New cyber laws, particularly The Sovereign Internet Law, will make it more difficult for companies operating in Russia to protect their customers' information/privacy. It will also likely make it easier for Russia to control content and protect its citizens online, which should fuel additional cybercrime activity that supports Russia's national interests. So security teams should expect to see an uptick in Russian cybercrime.

Despite the government's selective attempts to control internet users, Russia's cybercriminal underground has continued to grow in recent years. Experienced threat actors who make up the communities in hacking forums have grown increasingly "friendly" to non-technical cybercriminals—as long as they have the money to pay for the services. The bottom line is that Russia is a haven for cybercriminals so long as they do not attack CIS assets.

Cybersecurity teams must remain vigilant as Russian cybercrime continues to increase in both frequency and severity. The Russian hacking community's advanced technical capabilities paired with the government's apparent apathy toward – or even support for – attacks on foreign entities leave multinational companies as common targets. To protect your organization, it is imperative to keep up with Russia's expansive cybercrime underground and identify threats to your assets, employees, brands, and customers.



About the Author

Andrey Yakovlev is a Security Researcher at IntSights, focused on intelligence hunting from the Russian Dark Web. He is an experienced professional with nearly a decade of expertise in the cybersecurity field. Andrey specializes in threat discovery, computer forensics and behavioral analysis of Trojans.

About IntSights

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the open, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Singapore, Tokyo, New York, Dallas, and Tel Aviv.

learn more, visit: <https://www.intsights.com>