Orange
Cyberdefense

Epidemiology Labs | Threat Intelligence Report

Financial cybercrime in Russia

Date: June 4 (update)

Version: 2.0

Authors: OSINT Unit –
Part of the Orange Cyberdefense
Epidemiology Lab

Abstract

Russia's position towards cybercrime is ambiguous and complex. While the Russian government seems to engage against cybercrime and shows a strong will to regulate cryptocurrencies (that are also used by cybercriminals to get rid of existing banking regulations), it may also have links with hacker groups in order to pursue its own objectives in the cyberspace.

In Russia, financial cybercrime has expanded over the recent years. However, it is hard to know the exact number of groups operating in Russia because they dissociate and re-from easily. In order to lead malicious operations**, online platforms are used by the cybercriminal community in Russia to communicate, promote or even sell "services" and "products**".

Cybercriminal groups in Russia are based on "volunteering". Depending on the type and extent of the criminal group, heads of groups either hire "staff" to pay them a fixed salary, or punctually work with them on a freelance basis for some specific tasks. "**Money mules"** are indispensable in these groups: they are hired to transfer stolen money to the hacker accounts. Criminal groups can be classified in 3 categories, among which large groups are the most dangerous and destructive. **Cybercriminal groups mostly use cryptocurrencies to lead their illegal activities**.

Russia's relation towards cryptocurrency is complex and contradictory. If the Russian society shows a good knowledge and interest in cryptocurrencies, the Russian regulator is more skeptical. Russian central bankers particularly stand against cryptocurrencies. In the end of March 2020, a bill has been adopted after years of uncertainty, providing a definition of cryptocurrencies and prohibiting their use as a means of payment. More recently, in the end of May 2020, the government posted an updated version of their **new draft law on "Digital Financial Assets" for public comment, that would prohibit the circulation of all cryptocurrencies as well as their mining and advertising.**

However, **the bill has been delayed multiples times since 2018, and the COVID-19 crisis has not accelerated its adoption**. The economic impacts in Russia, due to the drop in oil demand and prices and the "war" with OPEC+, have led to the slow-down of all legislatives processes. That is why the legislative process will have to be closely monitored in the following weeks and months.

Moreover, **Russia's largest bank has issued a call for tenders to install nearly 5,000 Blockchain ATMs.** It seems that they could be used to mine cryptographic assets, which could herald a change in communication from Russian institutions and the use of the bank's vast network to distribute the "Cryptoruble".

Some elements could explain why cybercriminals are thriving in Russia. Even if statements that threaten cryptocurrencies were made recently, the **potential rewards are now still bigger than the risk of prosecution.** Russia may have links with cybercriminals for its own strategy. In exchange, these cybercriminals could carry out their illegal activities on the Internet (including extorsion) without being disturbed, as long as they do not affect Russian interests.

Finally, **the lack of established procedures for international cooperation between law enforcement agencies and expert organisations in different countries** is an additional reason for the tranquility enjoyed by criminals in the Russian cyberspace, even though Russia takes part to international initiatives to fight cybercrime.

Before reading

Based on NATO's codification of information scoring (see the appendice in section 6), the OSINT Unit of Orange Cyberdefense aims to be as exhaustive as possible and seeks to develop hypothesis that are considered to be the most likely.

The sources of this report mainly come from Open Source Intelligence and are considered from reliable to fairly reliable by the OSINT Unit.

Information have always been cross-checked, unless specifically mentioned in the text.

Summary

1 Introduction

A lot of current ransomware targeting companies over the last years are likely from Russian origin. Most ransomware use cryptocurrencies for the purpose of committing mischief.

As underlined by a report from Kaspersky[1], the "Russian-language cybercrime market is known all over the world". It is famous because online platforms used by the cybercriminal community to communicate, promote "services" and "products" or even sell them are accessible more or less easily. It also gets strong media coverage.

These products and services have now become focused on financial attacks – the most common ones being the stealing of payment card data to sell these data on the darknet. According to SecureList[2], "with the emergence of online stores and other services involving e-payment transactions, DDoS-attacks[3] and financial cybercrime have become especially popular with the fraudsters whose main targets are users' payment data or the theft of money directly from user accounts or companies". A popular mode of cyberattack targeting banks or other companies has become the use of ransomware.

Contrary to popular belief, ransomware have not only required payments in cryptocurrency. In 2013, CryptoLocker was probably the first to demand a Bitcoin ransom against a key to decrypt the victims' files[4]. Cryptocurrency is now mainly used by cybercriminals to get rid of existing banking regulations. Traditional paper money poses a lot of problems since some banking regulations, such as "KYC" (Know Your Customer[5]) and "AML" (Anti Money Laundering")[6], can induce banks to block or freeze funds in case of suspicious transactions (thanks to the knowledge of the account owner).

That is why we want to understand the relationships between the Russian financial cybercrime and Russian authorities, which also include their vision on cryptocurrencies and their exchanges into "fiat currency", allowing the money coming from cybercrime to be used "in real life" by hackers.

[1] https://securelist.com/russian-financial-cybercrime-how-it-works/72782/

[2] Ibid.

[3] A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.

[4] https://www.zdnet.fr/actualites/ransomware-et-cryptomonnaies-jamais-l-un-sans-l-autre-39893607.htm

[5] Know Your Customer: The know your customer or know your client (KYC) guidelines in financial services requires that professionals make an effort to verify the identity, suitability, and risks involved with maintaining a business relationship.

[6] Anti Money Laundering: Anti-money laundering refers to a set of laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income.

Contact:cyber.defense@orange.fr

2 The organisation of the Russian cybercriminal market

The set of "services" and "products" mentioned in the introduction are used for a wide range of illegal actions in the cyberspace.

The "products" can include trojans, exploits, databases of stolen credit card or other valuable information, or internet traffic. The "services" can notably include spam distribution, organisation of DDoS attacks, testing malware, packing of malware, VPN, rent of botnets or dedicated servers or withdrawal of money and cashing.

All of them are generally bought via an e-payment system such as WebMoney, Perfect Money, Bitcoin … and can be used in different combinations to enable different types of crimes, which can overlap as well. In 2015, Kaspersky Lab divided them in different categories:

- DDoS attacks (ordered or carried out for the purpose of extortion);
- Theft of personal information and data to access e-money (for the purpose of resale or money theft);
- Theft of money from the accounts of banks or other organisations;
- Domestic or corporate espionage;
- Blocking and encrypting access to data on infected computers for the purpose of extorsion (basically ransomware, which offers to give the data back if the ransom is paid).

2.1. The workforce of financial cybercrime

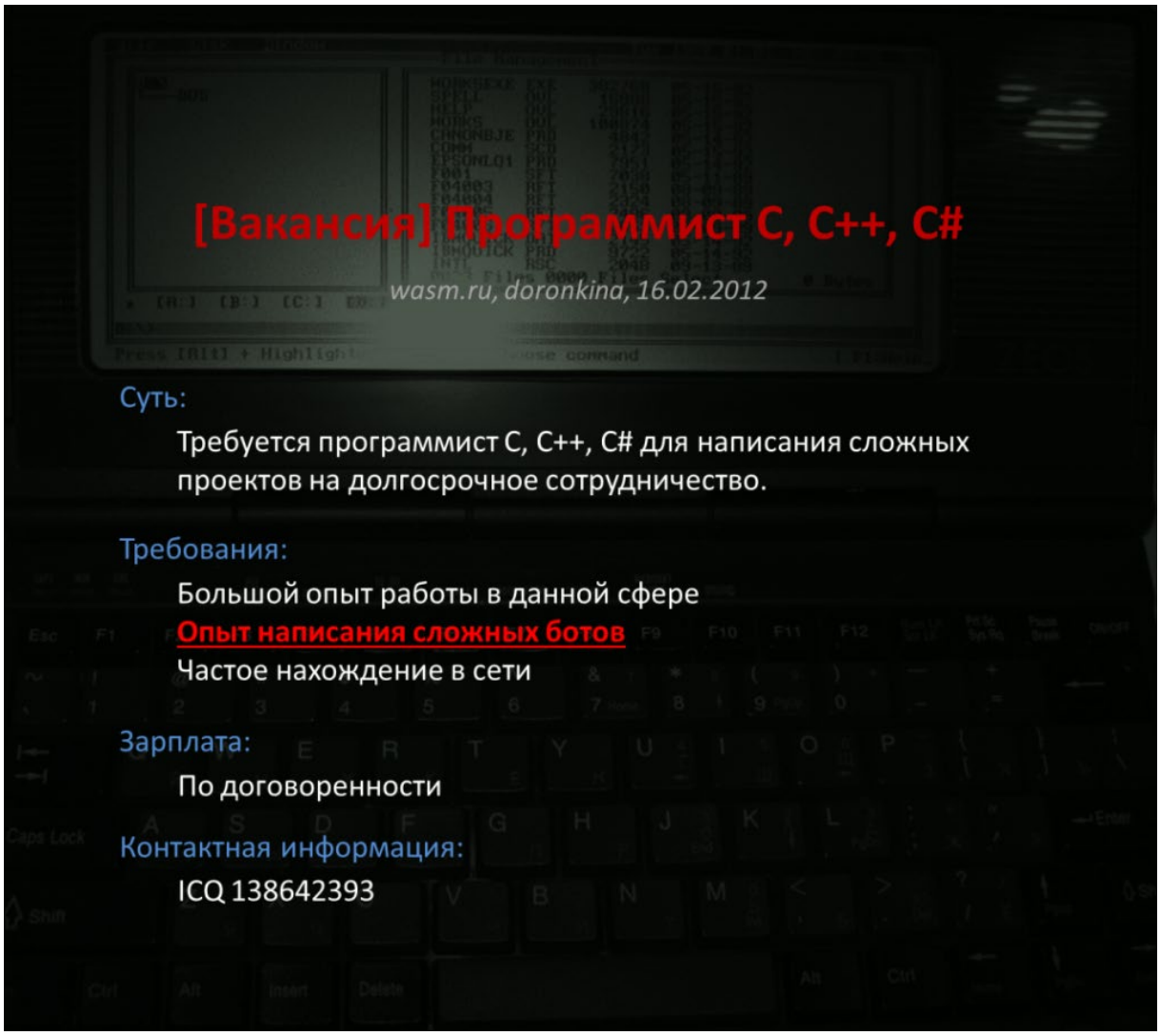
A complex network

It is important to underline the complex network behind Russian criminal groups creating and distributing malware. They are usually composed of "heads", "money flow managers" (in charge of the withdrawing of money from compromised accounts) and "heads of money mules". These ones supervise the process of cashing the stolen money, usually got in cryptocurrency.

These groups are based on "volunteering" and do not function as a "normal company". This is more an (illegal) "partnership". Depending on the type and extent of the criminal group, heads of groups either hire "employees" to pay them a fixed salary, or punctually work with them on a freelance basis for some specific projects.

"Staff" of ransomware operations can have different roles: programmers/encoders/virus writers, web designers (creation of phishing emails…), system administrators (for the construction and support of the IT infrastructure), testers (to test the malware before launching it for real) but also "cryptors" (responsible for the packing of malicious code to bypass antivirus detection for instance)[7].

[7] https://securelist.com/russian-financial-cybercrime-how-it-works/72782/



Source: Secure List. https://securelist.com/russian-financial-cybercrime-how-it-works/72782/

"An offer of employment posted on a semi-closed forum inviting a programmer to join a cybercriminal group. The job requirements include experience in writing complex bots".

The importance of "money mules"

In the "labor market" of "executors", there are three types of ways to hire people:

- "Staff" is hired through traditional cybercriminal activity websites;
- "Staff" is hired through resources for people interested in non-classic ways of making money online;
- "Staff" is hired through work-at-home job solicitations sent out by email and mainstream job search sites. This particularly targets IT specialists from remote regions of Russia or neighboring countries where salaries are low and job offers quite rare.

On this market, there are also two "types" of people recruited:

- Those who know that the project or work offered is illegal;
- Those who know nothing about it (at least in the beginning, but the tasks requested after some time usually become enough suspicious to warn the person that this is not a "normal" job).

The hired "staff" for these tasks are called "**money mules**". They receive small commissions for each successful transfer. However, they often end up "getting stiffed out of a promised payday, and/or receiving a visit or threatening letter from law enforcement agencies that track such crimes"[8].

Actually, "criminals also often give preference to candidates who have not previously been involved in cybercrime activity"[9]. Job offers are presented as a "legitimate work" and the work then becomes clearer once the task is received.

Highlight on the Evil Corp recruitment process

For instance, the method of the hacker group called "Evil Corp", accused by the U.S. Department of Justice of stealing roughly $100 million from businesses and consumers[10] (including through the famous ransomware "JabberZeus" and "Dridex"), has been analyzed by Krebsonsecurity.

The pattern in the naming convention and appearance of several money mule recruitment websites being operated by Aqua, a.k.a the leader of "Evil Corp" Maksim V. Yakubets, is the following : people responding to recruitment messages "were invited to create an account at one of these sites, enter personal and bank account data (mules were told they would be processing payments for their employer's "programmers" based in Eastern Europe) and then log in each day to check for new messages"[11].

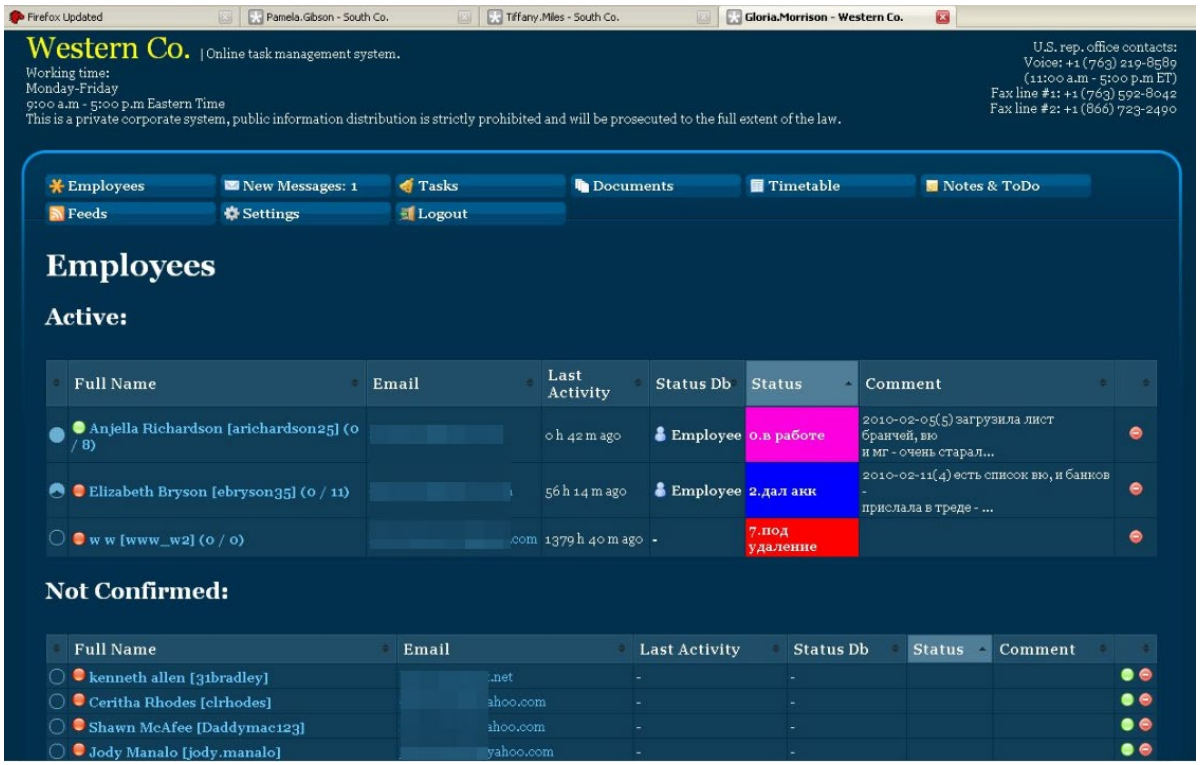
In the beginning, money mules were asked busy work or secondary tasks. Only after would they be asked to handle money transfers. This could be considered as a "trial period": the victim's bank usually tries to reverse any transfers that had not been withdrawn by the mules, so the money mule has to be effective and quick. If they are too late to carry out simple tasks, then they cannot be considered as reliable by hackers.

[8] https://krebsonsecurity.com/tag/money-mules/

[9] https://securelist.com/russian-financial-cybercrime-how-it-works/72782/

[10] https://krebsonsecurity.com/tag/money-mules/

[11] Ibid.



Source: Krebsonsecurity.

One of several sites set up by Aqua and others to recruit and manage money mules.

When it was the right time to transfer stolen funds, the recruiters would send a message to their mules, asking them to withdraw the funds in cash and wire the money to the fraudsters.

Fraudsters hacking corporate bank accounts typically launder stolen funds by making deposits from the hacked company into accounts owned by money mules.

It seems that the mules are increasingly instructed to remit the stolen money via Bitcoin ATMs. Actually, sending funds requires the user to scan a QR code shared by the recruiter, and then insert cash into the Bitcoin ATM[12]. This is a very interesting method for hackers, as Bitcoin is a non-refundable form of payment: once the money is sent, the transaction cannot be reversed.

[12] Ibid.

2.2. Different types of criminal groups

The number of participants to criminal groups responsible for money or financial information theft differs, as well as the scope of activities. They can be classified in 3 groups[13]:

"Affiliate programs"

The organisers provide to their affiliates almost all the tools needed to commit their activities. Then, it is a "win-win" system: the more the affiliates succeed in spreading the malware, the more they receive money. The organisers share the income received as the result of successful infections. Infection of users' mobile devices with malicious programs were commonly used, but the Russian regulator introduced in 2014 new requirements for the organisation of such services and it allowed the reduction of malicious mobile partner programs. Distribution of encrypting ransomware is now more popular.

"Single dealers, small and middle-sized groups (up to ten members)"

Criminals organise their own fraudulent schemes. Most of the components needed for the attack are bought on the black market and criminals are often not experts. Moreover, buying widely-available malware also means rapid detection by security solutions. This makes criminals invest more money in the "re-packing" to bypass detection and this lowers the final profit for the attacker. These groups are also more likely to be arrested.

"Large organised groups (ten or more participants)".

Such groups can comprise up to several dozen people (apart from money mules). Their targets are not limited to individuals but they attack small to medium-sized companies, "while the largest and most sophisticated of them (…) focus mostly on banks and e-payment systems[14]". Large groups are more likely to have a "regular" staff perceiving "regular" income. Third contractors are sometimes requested to carry out some of the tasks.

The large groups are the most dangerous and destructive.

[13] https://securelist.com/russian-financial-cybercrime-how-it-works/72782/

[14] Ibid.

2.3. The orchestration of a large-scale cyberattack by large criminal groups

As illustrated by the most important and famous cyberattacks over the last years, major financial cybercrime can result in multi-million dollar losses for attacked organisations. Not only does malware have to be developed and customized, but it also has to be transformed to bypass anti-virus detection. Above all, a thorough and meticulous study of the target company must be carried out if it is specifically targeted.

2.1.1 Stages of the attack

There are “typical” schemes of the stages of an attack.

1. Exploration

If the attack is specifically planned on a company, contractors have to collect information about the company – it can help to develop social engineering[15] plans. If the attack targets individuals, they are usually part of a “group” (for example, users of an online banking service). This is indeed easier to create fake websites or emails to attract them.

2. Infection

Spear-phishing, phishing mass-mailing containing an attachment with a malicious document or web-link is sent to the corporate network. When the attachment is open, this leads to malware infection – the user usually does not even realise something is happening.

Compromised popular sites “on which a tool is placed that invisibly redirects users to a third-party site containing a set of exploits” can also be used to infect a network.

3. Exploration & Implementation

Programs to commit mischief are downloaded onto compromised computers and can be used by cybercriminals to gain system administrators’ credentials.

4. Money theft

Cybercriminals finally “access the financial systems of the targeted organisation and transfer money from its accounts to the accounts of the mule project or withdraw money directly at ATMs”[16].

[15] Social engineering: in the context of information security, is the psychological manipulation of people into performing actions or divulging confidential information.

[16] https://securelist.com/russian-financial-cybercrime-how-it-works/72782/

3 What are the links between the Russian State and Russian hacker groups?

3.1. Russia's Cyberwarfare

Russia's Cyberwarfare[17] would include "distributed denial of service attacks (DDOS), hacker attacks, dissemination of disinformation and propaganda, participation of state-sponsored teams in political blogs, internet surveillance using SORM[18] technology, persecution of cyber-dissidents and other active measures"[19]. According to the investigative journalist Andrei Soldatov[20], some of these activities were coordinated by the Russian Signal Intelligence, which was part of the FSB[21].

According to an ARTE reportage[22] on Russian hackers, the "Russian state would use cybercriminals for its own strategy": it would mainly use them as contractors to carry out some types of attacks against agencies, institutions and company assets.

Michael Hayden, a former NSA director, says that he would not be surprised if Russian criminal gangs worked behind the scenes of the Russian state[23]. Gangs would be free in their activities, on the sole condition that they only attack foreigners. However, they should respond positively if the Russian state asked for their help to carry out specific tasks.

Different western countries have claimed being attacked by Russian hackers, and they officially pointed out Russian intelligence services. For instance, the United States have accused Russia of interference into the 2016 U.S. Presidential campaign. The former special counsel for the Department of Justice and former director of the FBI, Robert Mueller, indicted twelve Russian intelligence officers for hacking into the computers of the Democratic National Committee and the Clinton campaign. The indictment maintained that the Russian government had executed a sprawling and sustained cyberattack on at least three hundred people connected to the Democratic Party and the Clinton campaign, infiltrating their computers and implanting malware that, in some instances, enabled spies to covertly monitor their keystrokes[24].

However, it would have not only spied – what is, according to Michael Hayden, what every state does - but also tried to influence the outcome of the presidential election. He claims that Russia stole information but also weaponized it by transferring it to Wikileaks and other leaking platforms, which sent this information back to the U.S. society "in order to disrupt public dialogue".

[17] Cyberwarfare is the use of technology to attack a nation, causing comparable harm to actual warfare.

[18] SORM (In English: 'System for Operative Investigative Activities') is the technical specification for lawful interception interfaces of telecommunications and telephone networks operating in Russia.

[19] https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia

[20] https://echo.msk.ru/programs/albac/41311/

[21] FSB : Federal Security Service of the Russian Federation is the principal security agency of Russia and the main successor agency to the USSR's KGB ('Committee for State Security'). Its main responsibilities are within the country and include counter-intelligence, internal and border security, counter-terrorism, and surveillance as well as investigating some other types of grave crimes and federal law violations.

[22] https://www.arte.tv/fr/videos/080159-000-A/les-nouveaux-mercenaires-russes/. ARTE (Association relative à la télévision européenne) is a Franco-German free-to-air television network that promotes cultural programming

[23] Ibid.

[24] https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump

3.2. The special case of APT 28

One group in particular could be "state-sponsored" by Russia: "APT 28" or "Fancy Bear". Kevin Mandia, CEO of FireEye, has linked this group to more than 550 malware, and said his team has found more than 500 hosts or IP addresses were used in one sole attack. This means the existence of a very big infrastructure of compromised machines.

Though it could find no direct link to the Russian government, a FireEye report[25] said the intelligence sought by the hackers was consistent with Russian interests. It stated that "APT28 is most likely supported by a group of developers creating tools intended for long-term use and versatility, who make an effort to obfuscate their activity. This suggests that APT28 receives direct ongoing financial and other resources from a well-established organisation, most likely a nation-state government". This hacker group has attacked governments in Georgia, the Caucasus and eastern Europe, but also NATO and defense contractors across the west of Europe. Members of APT 28 could then have links with the GRU[26], the foreign military-intelligence agency of the General Staff of the Armed Forces of the Russian Federation.

The GRU has become known after the revelations about the 2016 U.S. election, but it just put light on them. This might only be one of their interventions: they could also be responsible for the blackout in Ukraine in December 2015[27] and NotPetya ransomware cyberattacks (2017).

A report from Booz Allen Hamilton also links the GRU to Fancy Bear and a group called Sandworm. The Sandworm Group would be the elite division of the GRU[28].

That is why some hackers could have links with Russian intelligence services, even if it is unclear if they are working with them, helping them "occasionally" or sharing profits with them. In exchange, hackers could lead their own malicious activities in the cyberspace, as long as they do not target Russian interests. They could also have wide access to resources, such as receiving government IDs and counterfeit passports[29].

If it exists, this type of "win-win" exchange could explain why Russian cybercriminals thrive in Russia, in spite of an apparent unfavorable regulation towards cryptocurrency (see Section 4) – the means most used by cybercriminals to make money from fraudulent operations in cyberspace.

[25] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

[26] https://www.arte.tv/fr/videos/080159-000-A/les-nouveaux-mercenaires-russes/

[27] Power was turned off to a quarter million Ukrainians after massive cyberattacks against critical infrastructures.

[28] https://siecledigital.fr/2020/03/31/publication-dun-rapport-sur-15-annees-de-cyber-operations-menees-par-des-pirates-militaires-russes/?amp&__twitter_impression=true

[29] https://geminiadvisory.io/fsb-takes-down-top-tier-marketplace-arrests-admins/

3.3. Has the “rule” been broken?

A recent event seems particularly interesting. Russian media reported that the Russian Federal Security Service (FSB) arrested 30 members of a hacker ring on March 20, 2020. The hackers purportedly specialized in selling compromised debit and credit cards stolen. They were located across 11 regions of Russia and included citizens of Ukraine and Lithuania. Russian media reported that this hacker ring operated more than 90 dark web markets, but it did not indicate that any of these marketplaces were taken offline. However, Gemini Advisory noted that a popular dark web marketplace known as BuyBest, as well as what it calls its “mirrors”, went offline. Alexey Stroganov (a.k.a. “Flint24”) was arrested during this operation. He was associated with GoldenShop, a “mirror” market of BuyBest: they sold compromised credit card information from the same sources and are oftentimes operated by the same groups of criminals. According to Gemini Advisory[30], this shows that the arrested members operated BuyBest and its mirrors, which have been taken offline by Russian law enforcement.

Both BuyBest and GoldenShop were large and top-tier marketplaces. It was known for selling phished data, which often included Social Security Numbers (SSNs), dates of birth (DOBs), victim IP addresses and User Agents.

BuyBest appears to have subscribed to the “implicit” rules by prohibiting the sale of Russian card data. That is why the spectacular arrest seems unclear: some rules of the “win-win” exchange could have been broken.

BuyBest marketplace did not allow the sale of compromised Russian-issued payment cards, but it remains unclear if arrested hackers targeted Russian businesses. If they did so, the data may have appeared on one of the 90 dark web markets and then have drawned the attention of law enforcement. There could also have been a conflict with another group of hackers. It already happened in the past[31].

Anyway, this shows that the Russian government can keep control over what happens in the Russian Cyberspace.

[30] Ibid.

[31] https://krebsonsecurity.com/2019/10/briansclub-hack-rescues-26m-stolen-cards/#more-49161

4 The complex and ambiguous relation of Russia towards cryptocurrencies

4.1. A high interest in the Russian society for cryptocurrencies

Russia is a highly centralised state and a strong bureaucracy, which may explain why Russian developers are attracted to blockchain. During the Cold War, USSR spent a lot of money in technological advancements to demonstrate the world its superiority while engaged in a race with Americans. This is no stranger to technical education for citizens and thus a place of highly skilled developers nowadays.

Figures confirm this trend. According to a Skalex report[32], as of 2017, a full twenty percent of the top fifty blockchain projects (as ranked by funds raised) were founded uniquely or in part by Russians. Moreover, more CEOs of blockchain projects came from Moscow than any other city across all ICO[33]s last year.

Russia is a difficult place to access start-up, and venture capital is limited. That also explains why blockchain and cryptocurrency attract Russian entrepreneurs. Russian blockchain can raise money from around the world.

The Russian society's relation towards cryptocurrency must be highlighted: almost 50% of Russians have heard of it and 13% even claim to understand it well, according to a research from Romir[34]. 56% of Russians would also have heard of Bitcoin in 2018, reaching 74% in Moscow[35].

4.2. The paradoxical attitude of the Russian government towards cryptocurrency

Divided and indecisive Russian authorities

According to Skalex, Russia would hope to control the early growth of blockchain, similarly to the way U.S. dominated the early growth of the internet[36].

Actually, Putin's view on cryptocurrency seems to vary over the years. By October 2017, Putin said Russia should support and welcome cryptocurrency. He supported the idea of the creation of a framework for cryptocurrency companies in Russia and pushed for a national infrastructure to support cryptocurrency. He even talked about a cryptocurrency version of the Russian ruble, the "CryptoRuble".

[32] https://www.skalex.io/crypto-russia/

[33] An initial coin offering (ICO) or initial currency offering is a type of funding using cryptocurrencies. It is often a form of crowdfunding, however a private ICOs which does not seek public investment is also possible.

[34] https://www.skalex.io/crypto-russia/

[35] Ibid.

[36] Ibid.

However, Russia is definitely divided and indecisive about the blockchain. Some actors are deeply opposed to it, others have conflicting opinions "on the role blockchain should play in Russian society", as illustrated by Vladimir Putin: "shortly before announcing a plan to nurture young technologies, [he] criticized crypto and called for a regulatory crackdown"[37]. According to Global Legal Insights, Russian authorities are recalcitrant to cryptocurrencies despite the generally welcoming attitude of the government towards blockchain as a technology. This would be due to the generally non-transparent nature of transaction with this type of currency and the associated compliance and similar risks[38].

The fear of a "Ponzi scheme"

Russian central bankers have called cryptocurrencies a "pyramid scheme"[39] (e.g. a business model that recruits members with the promise of being paid if they enroll others). They started a crackdown on cryptocurrencies with the Russian government in October 2017. Putin stated that cryptocurrencies were used by criminals to launder money and make illicit payments, and the central bank thought about blocking Russian websites that offer digital assets to consumers. Most Russian banks actually do not want to deal in cryptocurrencies due to the lack of well-defined regulations. History plays a role in it: regulators would be concerned that the cryptocurrency is a Ponzi scheme[40] that affected millions of Russians after the collapse of the USSR. The important number of fraudulent ICOs in the market in 2017 did not improve the image of cryptocurrencies.

A new law could prohibit the circulation of all cryptocurrencies

On January 16, 2020, Mikhail Mishustin, the new Russian Prime Minister, stated that "[he is] convinced that it is necessary to tax [all operations with cryptocurrency], and to correctly assess any economic consequences of using cryptocurrencies".[41] As a reminder, this was only 24 hours after Putin replaced Prime Minister Dmitri Medvedev, his long-time partner, in a reshuffle of the cabinet. This shows the concern of Mishustin, a former tax man and former director of the Russian version of the Internal Revenue Service[42], about cryptocurrency. Without proper regulation and oversight, crypto is considered as one of the best tools for tax evaders, fraudsters or money launders.

Our OSINT Unit believes that the taxation could be motivated by financial reasons. Russia's economic situation is not optimal: the economic recovery that began in 2017 remains limited. Public finances, which rely heavily on hydrocarbon revenues, are deteriorating. Russia could then be tempted to tax cryptocurrencies in order to replenish the state's coffers. Since cryptocurrency is popular in Russia and also used by many cybercriminals probably based in the country, this could be a good means to bring money back to the state.

[37] Ibid.

[38] https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/russia

[39] https://www.skalex.io/crypto-russia/

[40] As a reminder, a Ponzi scheme is a form of fraud that lures investors and pays profits to earlier investors with funds from more recent investors. The scheme leads victims to believe that profits are coming from product sales or other means, and they remain unaware that other investors are the source of funds. A Ponzi scheme can maintain the illusion of a sustainable business as long as new investors contribute new funds, and as long as most of the investors do not demand full repayment and still believe in the non-existent assets they are purported to own.

[41]https://www.forbes.com/sites/kenrapoza/2020/01/17/russias-new-prime-minister-wants-cryptocurrency-to-be-taxed/#4bd108ab79ba

[42] The Internal Revenue Service (IRS) is the revenue service of the United States federal government. It is responsible for collecting taxes and administering the Internal Revenue Code, the main body of federal statutory tax law of the United States.

The Chairman of the State Duma Committee on Financial Markets also said in January 2020 that the Russian parliament was "99% likely" to adopt a new law on crypto in Spring 2020.[43] In the end of March 2020, the Chairman has confirmed that the bill has been completed[44]. It provided the definition of cryptocurrencies and prohibited their use as a means of payment.

Finally, at the end of May 2020, the government posted an updated version of its new draft law "On Digital Financial Assets" for public comment, along with it additional documents that significantly change the way cryptocurrency is regulated in Russia[45]. Breaking the rules now means legal penalties. This law is finally in keeping with official positions on privately issued cryptocurrencies, but is even harsher as it prohibits the circulation of all cryptocurrencies, as well as their mining and advertising.

The new law does not mean Russians cannot own digital financial assets legally. The Russian Central Bank has not yet introduced the rules for inclusion in cryptos as a security.

According to a member of the Russian State Duma, the country's new crypto law won't go into effect until the summer[46]. He also added that people can buy and hold cryptocurrencies, but should declare it on their taxes so that they can be given legal protections (since the cryptocurrency will be considered as a property). There will be no legal penalties for owning cryptocurrencies, but digital currency platforms will be prohibited on the territory of Russia (meaning no exchanges).

However, it is worth noting that if cryptocurrencies are not allowed and financial assets based on blockchain technology are going to be subject to regulation, blockchain technology itself is still a go.

The adoption of the bill has been delayed multiple times since 2018, and the COVID-19 pandemic has not accelerated its adoption. Russia's economic situation is indeed deteriorating: the pandemic has led to a drop in oil demand, contributing to a plunge in crude oil process. After Russia's refusal on the renewal of a reduction in production with the Organisation of Petroleum Exporting Countries (Opep)[47] to support prices, Saudi Arabia sharply lowered its prices, flooding the market with low-cost barrels to gain additional market shares.

The situation has kept deteriorating and Putin, unwilling to tap Russia's financial reserves and facing a pandemic and ever-worsening oil prices, inclined to make a deal[48]. Saudi Arabia and Russia agreed in April 2020 to further output cuts after the latest OPEC+ deal to curb global oil supplies failed to stem crude's downward spiral[49].

[43] https://www.forbes.com/sites/kenrapoza/2020/01/17/russias-new-prime-minister-wants-cryptocurrency-to-be-taxed/#4bd108ab79ba

[44] https://news.bitcoin.com/russia-cryptocurrency/

[45] https://www.forbes.com/sites/kenrapoza/2020/06/01/russia-sort-of-dropped-the-hammer-on-bitcoin-crypto/#61c34a4e6a83

[46] Ibid.

[47] OPEC is an inter-governmental organisation of countries aimed at negotiating with oil companies on all matters relating to oil production, its price and future concession rights.

[48] https://news.bitcoin.com/russia-cryptocurrency/

[49] https://www.bloomberg.com/news/articles/2020-04-16/russia-s-oil-pain-deepens-as-opec-prepares-to-cut-output

Finally, Opep and Russia are nearing a compromise to extend oil production cuts over a period of one to two months as of June 1st, 2020[50]. Despite the gradual lifting of closures, which is leading to an upturn in economic activity, Saudi Arabia wishes to extend this production cutback until the end of the year and has initiated discussions to this end, but as not yet obtained the support of Russia, which believes that production cuts could be gradually eased. The oil-price crash has indeed been particularly painful for Russia. Because of the coronavirus crisis, all legislative processes have slowed down.

The main opponent to cryptocurrency in Russia: the Central Bank

Russia's upcoming regulation comes after years of uncertainty, and numerous delays in providing any regulatory clarity. In January 2018, Putin has ordered the adoption of the bill "On Digital Assets" twice, but the legislation is still on the road.

The Chairman of the State Duma Committee said several times in the past that the bill was ready. However, he later explained that due to irreconcilable disagreements in the government regarding this new type of asset, the bill was repeatedly amended and its adoption subsequently delayed. The Central Bank, for example, has opposed its legalisation[51].

We must also underline that the Bank of Russia issued a set of rules for suspicious transactions, that categorised any crypto-related transaction as a potential money laundering risk. Still the central bank is thinking about the emission of its own digital currency. In December 2019, the Central Bank's President Elvira Nabiullina said that the institution was exploring the possibility of issuing a digital ruble.

Russia's biggest bank is buying 5,000 Blockchain ATMs that could mine crypto

Sberbank has called for tenders to provide around 5000 ATMs with a built-in graphic card capable of supporting "blockchain operations"[52]. As a reminder, Sberbank is the oldest and largest bank of Russia and holds almost 44% of all personal deposits in the country. Its chairman and CEO is also Russia's former minister of Economics and Trade and known to be a be a big proponent of new technology, including blockchain.

However, this announcement raises questions: why does a bank ATM need a graphic card that is capable of handling some blockchain operations?

According to Cointelegraph[53], the most obvious case is cryptocurrency mining. This could then mean that Sberbank will issue its own cryptocurrency, or that the Russian government will use the network of the bank to distribute the "Cryptoruble". The other explanation would be a simple error in the tender's document description. In that case, the graphics card is only needed for image recognition (these ATMs could also have biometric authentication).

[50] https://investir.lesechos.fr/marches/actualites/l-opep-et-la-russie-discutent-d-une-prolongation-de-la-reduction-de-la-production-petroliere-1911572.php

[51] https://news.bitcoin.com/russia-cryptocurrency/

[52] https://cointelegraph.com/news/russias-biggest-bank-is-buying-5000-blockchain-atms-that-can-mine-crypto

[53] Ibid.

This project could herald a change in communication from Russian institutions. So far, they have not embarked in the race for the CBDC (Central Bank Digital Currency), contrary to other countries such as China or France.

This news comes up with the recent announcements about the risks following illegal crypto exchanges: the Russian government may want to "clean up" the market before taking an official position[54].

5 Conclusion

Financial cybercrime operating from Russia has become widespread over the recent years. Current "working" conditions for Russian cybercriminals have been favourable: despite recent statements on the taxation or prohibition of the circulation of cryptocurrencies, the risk of prosecution is still low while the potential rewards are high. This might yet change.

There would be an implicit agreement between the Russian state and criminals: some hackers could have links with Russian intelligence services, even if it is unclear if they are working with them, helping them "occasionally" or sharing profits with them. In exchange, they could carry out their own malicious operations in the cyberspace, as long as they do not target Russian interests.

This type of "win-win" exchange could explain why Russian cybercriminals thrive in Russia, despite of an apparent unfavorable regulation towards cryptocurrency.

A lack of established procedures for international cooperation between law enforcement agencies and expert organisations in different countries can also explain why cybercriminals can continue their activities while being "discovered".

However, Russia shows a desire to fight cybercrime by taking part to projects such as the "No More Ransom" website : it is an initiative of the National High Tech Crime Unit of the Dutch police, the European Cybercrime Centre based at Europol, Kaspersky and McAfee which aims to help victims of ransom software to retrieve their encrypted data without having to pay the criminals. Police agencies and computer security companies have joined forces to combat cybercriminal companies with ransom connections. The Russian police is one of the police agencies that joined the initiative, which shows their willingness to fight cybercrime, or at least their willingness to communicate about it on the international arena.

[54] https://cryptoast.fr/5-000-distributeurs-cryptos-banque-russe/

6 Appendices

6.1. Selected Repository for the Classification of Sources and Information

Source ratings[55]

Code	Source rating	Explanation
A	Reliable	No doubt of authenticity, trustworthiness or competency; has a history of complete reliability
B	Usually reliable	Minor doubt about authenticity, trustworthiness or competency; has a history of valid information most of the time
C	Fairly reliable	Doubt of authenticity, trustworthiness or competency, but has provided valid information in the past
D	Not usually reliable	Significant doubt about authenticity, trustworthiness or competency but has provided valid information in the past
E	Unreliable	Lacking in authenticity, trustworthiness and competency; history of invalid information
F	Cannot be judged	No basis exists

[55] US Department of the Army (September 2006). "FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations" (PDF). FM 2-22.3. Retrieved 2007-10-31.

Information content ratings[56]

Code	Rating	Explanation
1	Confirmed	Confirmed by other independent sources; logical in itself; consistent with other information on the subject
2	Probably true	Not confirmed; logical in itself; consistent with other information on the subject
3	Possibly true	Not confirmed; reasonably logical in itself; agrees with some other information on the subject
4	Doubtfully true	Not confirmed; possible but not logical; no other information on the subject
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject
6	Cannot be judged	No basis exists

6.2. Disclaimer

Orange Cyberdefense strives to ensure the accuracy of the information gathered in this document, but no warranty, express or implied, can be given.

Orange Cyberdefense disclaims any liability for errors or omissions resulting from/related to the use of the information and material in this document.

[56] Ibid.

Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries.

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.