RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

RUSSIA'S CHANGED ATTACK TACTICS AND VECTORS IN CYBERSPACE

GIORGI TIELIDZE

171

EXPERT OPINION

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

EXPERT OPINION

GIORGI TIELIDZE

RUSSIA'S CHANGED ATTACK TACTICS AND VECTORS IN CYBERSPACE

171

2021

The publication is made possible with the support of the US Embassy in Georgia. The views expressed in the publication are the sole responsibility of the author and do not in any way represent the views of the Embassy.

Technical Editor: Artem Melik-Nubarov

ISSN 1512-4835
ISBN

Introduction

The attack tactics of Russian special services in cyberspace have undergone a significant alteration in the recent period. This is mainly manifested in the fact that Russian security structures drastically increased attacks against their main targets in the West by using groups of cyber criminals active in Russia and not through their state cyber espionage units directly. It must also be pointed out that the Russian Federation also used to engage cyber criminals in the past and with some regularity; however, the Kremlin has more recently used these groups as a vanguard of its attacks against the critical information systems of Western states.

It is widely known that multiple organized crime groups are operating in Russia with impunity (for example: DarkSide, Evil Corps, Revil and others). They have recently become especially active against the member states of the North Atlantic Treaty Organization, performing attacks targeting their critical infrastructure. The most relevant examples in this regard are against the Colonial Pipeline in the US and the JBS corporation where system management files in the information and communication systems of these organizations were encrypted. For the key to decipher these files (the so-called decryptor), the attackers demanded USD several million in Bitcoin. Apart from direct financial damages which were connected to paying the ransom for decrypting the files, the US financial and economic sector sustained significant losses given due to the collapse of the functioning of these two companies. Colonial Pipeline is the main oil product distributor throughout the territory of the United States and JBS supplies meat products to American consumers. The situation was also identical regarding the attack against the network infrastructure management software of the Kaseya company which resulted in the stoppage of the functioning of multiple companies in Europe.

It must be pointed out that the activation of Russian organized cyber-crime groups is dangerous for critical public infrastructure and private information systems in Georgia as well. The practice shows that malware used by Russian organized criminal groups with a view to financial gain also contained modules that aimed to gather various types of sensitive information from the computers which were originally infected. In addition, Georgia's information resources and the private sector were also being

attacked by an organized crime group, RBN (Russian Business Network), and Russian security services during the August 2008 war.

Overview of Major Russian Cyber-Crime Groups

Before directly addressing the specifics of the Kremlin's usage of organized crime groups which has particularly intensified after the Russian Foreign Intelligence Service's attack on the SolarWinds Corporation, an overview of the organized cyber-crime groups directly connected to the Russian intelligence and law enforcement apparatus will be made as well as defining their criminal association.

DarkSide is an organized cyber-crime group based in the Russian Federation that is mainly focused on ransomware attacks. Recently, the group has placed its malware samples in various Darknet forums which could be used by third parties based on respective "remuneration to perform ransomware attacks."[1] Therefore, the sphere of DarkSide's criminal activity has increased with the addition of knowledge-based and offensive tools for sale on the Darknet. These knowledge-based and offensive tools are referred to as Ransomware as a Service (RaaS). DarkSide is also actively communicating with the public by actively posting on various Darknet forums as well as running its own blog. Moreover, it regularly clarifies that its attacks are not politically motivated which means its activities are only for economic gain.

DarkSide has performed numerous attacks in recent years. The most notable of these was the May 7 ransomware attack against Colonial Pipeline, the largest oil product distribution company in the United States, in the form of the aforementioned encrypting of the company's key information and communication system management panels which forced the stoppage of 45% of the oil product supply designated for the Eastern United States for about a week.[2] Moreover, the US economy sustained losses of tens of millions of dollars at the federal level with hitherto fully uncalculated amounts of additional lost income. Ultimately, Colonial Pipeline was forced to pay the attacker USD 5 million for the tailor-made decryptor. However, the Federal Bureau of Investigation of the United States managed to return most of this ransom money to the victim; namely, USD 4.4 million, several weeks after the ransom had been paid.[3]

Revil is another organized cyber-crime group which conducts large-scale and financially motivated criminal offenses in the United States and Western European states according to its presence in various Darknet forums. This group is behind the attack on the JBS meat processing company which was established in Brazil and owns the main meat product distribution network in the United States. As a result of the attack and much like the Colonial Pipeline case, the systemic management files of JBS were encrypted, forcing the victim to pay the equivalent of USD 11 million in Bitcoin.[4]

Furthermore, much like DarkSide, Revil also intensively uses the RaaS model and mediates between the victims and the attackers who employ their cyber offensive tools. Revil gets a pre-negotiated "fee" for rendering this service.[5]

When further analyzing Revil's attacks, it must also be noted that the group is responsible for the supply chain attack against the Kaseya software provider company. However, Kaseya managed to obtain a free-of-charge universal decryptor for its beneficiary companies shortly after this attack and once the highest US leadership intervened and conducted negotiations with the Kremlin. Subsequently, Revil and its infrastructure completely vanished from the Darknet for a certain period of time.[6]

When talking about Russian organized criminal groups, we must also refer to the extremely dangerous criminal syndicate known as the Evils Corps that managed to illegally acquire approximately USD 100 million belonging to US citizens by using various malware samples. This group actively used former Soviet citizens in the United States to get the illegally acquired money and transfer it to Russia and Ukraine where the leader of Evil Corps, Maksim Yakubets, and his associates lived.[7] Unlike the two previous groups, the battle of US law enforcement structures against Evil Corps turned out to be much more effective, taking into account that the identity of the group's leader was established. Maksim Yakubets is now wanted internationally while the US also managed to reveal his connections with Russian intelligence services.[8]

Finally, the following important factor must be pointed out: despite the fact that these groups (DarkSide and Revil) vanished for a certain period of time and their infrastructure became unavailable, they returned with their own name, in the case of Revil, and with an altered name, in the

case of DarkSide, after a short pause when tensions between the United States and the Russian Federation vis-à-vis SolarWinds Orion normalized.[9] [10] The situation with Evil Corps is also identical as it returned with various different names (WastedLocker Ransomware Group) despite the removal of its infrastructure and the arrest of some of its managing individuals.[11]

Connections between Russian Organized Cyber-Crime Groups and the Intelligence Apparatus

There is a great deal of evidence about the connections of the abovementioned groups and Russian security services. Some of this is found in documents from US official institutions as well as in the technical investigation documents from various well-known cyber security organizations. Therefore, I will rely only on the information publicized by these two types of sources in order to avoid any conspiracy theories while discussing this topic.

The US Trade Department officially connected the head of Evil Corps, Maksim Yakubets, to the Russian Federal Security Bureau (FSB) and alleged that he acted in line with direct orders from the FSB and periodically conducted attacks on targets with a high intelligence value.[12]

Furthermore, the track-record of the activities of the famous criminal, Evgeniy Bogachev, as well as the reverse engineering of the Zeus malware which he developed (with modules having a clear espionage functionality) also point to direct ties with Russian security services. More precisely, Zeus was initially used to gain real-time access to banking information contained in infected computers when the victims used their authorization data to access specific online banking platforms.[13] In 2015, Bogachev issued an updated and a modified version of Zeus with the name GameOverZeus. The reverse engineering process of the aforementioned malware demonstrated that it contained malicious code modules built-in with certain keywords through which it was possible to find and exfiltrate files containing these words from infected computers in Georgia, Turkey and Ukraine. More specifically, the malware vis-à-vis Georgia was configured in such a way that it could find any files which included keywords such as *secret, Russia, Krasnodar* and *external intelligence* in victim computers, either in the title or body text of any file, particularly in text editors and

.pdf type documents. The topical search modules were also similar in the case of the infected machines in Turkey and Ukraine. The image bellow enumerates the search word catalogue in decrypted malware modules in the Georgian, Turkish and Ukrainian languages.[14]

Source: M. Sandee, T. Werner and E. Peterson

Another important factor providing robust evidence regarding connections between Russian security services and organized cyber-crime groups operating on the territory of Russia is the fact that the configuration of the malicious codes developed by DarkSide and Revil precludes the running of this malware on computers that have Russian or any other language used in the post-Soviet republics installed on them.[15] This restriction does not apply to the target systems if any of the languages of the Baltic States is installed. Revil's motivation in applying such an approach is mainly due to the fact that the post-Soviet states have rather small numbers of financially powerful organizations that would be willing and able to pay millions of dollars like Colonial Pipeline and JBS did in order to regain access to their data

Moreover, given that Russian law enforcement bodies have close connections with their colleagues in other post-Soviet states with the exception of Georgia and Ukraine, it is to be expected that these countries will address the Russian Federation for legal assistance and that the latter

will likely react positively to such requests since the Kremlin has strategically important relations with the majority of these states. Therefore, it can be assumed that Russia will avoid damaging its ties with them.

Additionally, adding Russian to the aforementioned list of languages is the main insurance that individuals or financial corporations residing in Russia will not be infected in the case of a large-scale ransomware attack since the Kremlin will definitely react given that the majority of such corporations are under the protection of Russian security services.[16]

Last but not least, it is also worth noting that Russian security services do not merely cooperate with criminal actors on the basis of maintaining confidentiality. In the situation when a person who is engaged in cyber-crime is especially valuable for Russian intelligence services, they even accept them within their own ranks in the capacity of a full employee and even promote them to middle and high-ranking positions in some cases. The best example is Dmitry Dokuchaev, quite a famous individual with many aliases on Russian Darknet forums for his phenomenal carding skills (stealing and forging of credit cards) in the early 2000s. Later, he started working for the FSB as an informant; however, his status changed when he became officer in the 18th division (Information Technologies Center) in 2014.[17]

Changes in Attack Vectors and Tactics of Russian Security Services in Cyberspace

Given that ties between particular cybercriminals and the Russian security system have been confirmed, let us review how the Russian Federation has altered attack tactics and vectors using the aforementioned criminal groups.

On April 15, 2021, the White House imposed sanctions on the Russian Foreign Intelligence Service and connected organizations who were providing offensive tools and services to the SVR.[18] The sanctions imposed by the White House are rather vast and will significantly impede the development of the offensive capabilities of the Russian Foreign Intelligence Service as well as the commercially profitable operations on international markets on behalf of the abovementioned organizations. In its statement announcing the sanctions, the White House also indicated

that the US would react strictly and adequately to any such incident occurring in future.[19]

It seems that the Russian side learned this "lesson" only in terms of offensive attack methods and tactics. However, as is characteristic for the high-level Russian political and security leadership, they decided to test the reliability of the commitments made in the April 15 statement of the US presidential administration, especially given the fact that the current administration assumed power only several months ago. The Russian leadership was obviously interested to see the extent to which the Americans would go in order to fulfill their promises vis-à-vis response measures.

As a result, on May 7, 2021, DarkSide performed the aforementioned attack on Colonial Pipeline. In so doing, the Russian Federation managed to achieve two tactical and yet very important objectives:

- The Kremlin checked the readiness of the US presidential administration to respond on the basis of the principle of reciprocity.
- The Kremlin managed to achieve this first goal in a way so as to avoid a full-scale confrontation in cyberspace. With the involvement of the DarkSide organized crime group, it gave the Russian side the possibility of plausible deniability taking into account that it is extremely difficult to connect this criminal syndicate to the Russian state under international law.[20]

This incident caused a prompt response from the president of the United States (May 7, 2021) who stated that even though he **did not believe** the attack to be organized by the Russian government, there was evidence indicating that the attack was conducted from the territory of Russia. Hence, President Biden called on the Russian side to suppress the criminal activities of the individuals involved in the planning and the implementing of this attack through criminal charges against them.[21]

As it later became clearer, this statement from the US presidential administration and the steps taken thereafter were insufficient in deterring the Russian Federation. Hence, the Kremlin again achieved its abovementioned tactical goals that cleared the path for similar activities in the future. More specifically, another attack took place on May 30 on behalf of a different organized cyber-crime group called Revil which

resulted in the stoppage of the activities of the largest meat distributing plant and network in the US – the JBS company, as has been referred to previously within this paper.

Reacting to this attack, the Press Speaker of the US Presidential Administration, Jen Psaki, stated that the US is "considering all options," including a reciprocal response and the dismantling of the infrastructure used in the attack.[22] In response to the JBS and Colonial Pipelines attacks, the US president ultimately gave the president of the Russian Federation a list of 16 critical sectors that must not be subject to any sort of cyber-attack from the territory of Russia during the Geneva Summit on June 16.[23]

Obviously and again, the Russian side did not consider this call as a deterrent against acting malignly through criminal proxies. Hence, shortly after the abovementioned communication, the Russian-based Revil exploited the vulnerability inside Kaseya's software that was outsourced by several important European companies; however, US businesses were also partially harmed. This was once again followed by President Biden's appeal to Moscow in which he yet again called on the president of Russia to suppress the activities of cyber-crime actors on the territory of Russia.[24] In light of all of the abovementioned facts, it is clear that the Russian side has activated cyber-crime groups on its territory against the United States and members of the North Atlantic Treaty Organization, given that the Kremlin can easily explain any type of attacks from these groups with trivial criminal motives and goals. Therefore, the Kremlin has so far managed to successfully avoid direct responsibility with this approach, denying any participation in the aforementioned offensive campaigns. Moreover, the negative image of Russian law enforcement on the international arena in terms of the fight against crime also "contributes" to the Kremlin's explanation of its "inability" to dismantle such criminal syndicates. Namely, both the security and the state political leadership in the West is well aware that the Russian law enforcement system is corrupt and, therefore, it is largely incapable of controlling the work of organized crime syndicates. Contrary to this belief, however, the facts presented above clearly show that Russian security services fully control and utilize the work of individual cyber criminals or groups operating on their territory.

In addition, as the analysis and the timeline of the aforementioned attacks demonstrate, sanctions alone or, even worse, statements and calls do not

work properly vis-à-vis the Russian side and cannot serve as an effective deterrent mechanism. Moreover, Russia considers the limited response to its actions as a sign of weakness on behalf of the West which further encourages it to commit more malicious acts in cyberspace. This statement is especially relevant with regard to the current US administration which is substantially different from Team Trump in its attitude towards Russia. Therefore, the Kremlin will most likely and more frequently attempt to challenge the US with such actions and then not expect any proportionate response. In its turn, Russia will use its disinformation system to portray such cases as major victories for its domestic audience as well as on the international stage.

Hence, the approach of the Secretary of the US National Security Council must be fully shared, according to which it is also necessary to perform small-scale defensive operations against the hostile powers, mainly the Russian APT groups, apart from sanctions.[25] These measures could also contain components of attack in the case of Revil when the FBI finally managed to dismantle the group's offensive infrastructure and obtained a universal decryptor for free.[26] After such an approach, Revil was less active against US targets and has recently completely disappeared from the Darknet. Finally, let us underline that only a reciprocal approach that also includes an offensive component will have significant influence on reducing cyber threats stemming from Russia and rendering the actions of the Kremlin in cyberspace more-or-less predictable.

Conclusion

It must be pointed out that the recent change in attack methods and vectors on the part of the Russian Federation in cyberspace involving organized criminal syndicates has important motivations and objectives. Namely, through this approach the Kremlin tries to continue its destructive actions in cyberspace but in a way as to avoid any proportionate response from US and/or punitive measures against the Russian intelligence apparatus. Furthermore, this stance is further challenging as Russia is showing the US and the Western world at large that apart from the conventional cyber-forces (FSB, SVR, GRU cyber-divisions), the Kremlin also has non-conventional capacities which it will activate upon necessity. These supposedly guerilla activities will be no less damaging for the targeted

countries while the Kremlin will not have to pay a high price for their activities. At least, there will be no clear legal argumentation that will be based on digital evidence.

The United States and NATO need to formulate a clear response strategy which will be based on the principle of a proportional and/or asymmetric response so that such active defense measure will be adequately painful and damaging for the Kremlin. Georgia could also become part of this strategy if the Kremlin decides to activate its non-conventional attacking capacities against the country.

Bibliography

1. FireEye, “Shining a Light on DARKSIDE Ransomware Operations”, available at: https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html; Accessed: 21/09/2021
2. NPR, “What We Know about the Ransomware Attack on a Critical US Pipeline”, available at: https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline; Accessed: 21/09/2021
3. BBC, “Colonial Pipeline: US Recovers Most of Ransom, Justice Department Says,” available at: https://www.bbc.com/news/business-57394041; Accessed: 21/09/2021
4. BBC, “Meat Giant JBS Pays $11m in Ransom to Resolve Cyber-Attack,” available at: https://www.bbc.com/news/business-57423008; Accessed: 21/09/2021
5. Palo Alto Networks, *Understanding REvil: The Ransomware Gang Behind the Kaseya VSA Attack*, available at: https://unit42.paloaltonetworks.com/revil-threat-actors/; Accessed: 21/09/2021
6. Zdnet, “Kaseya Says it Has Now Got the REvil Decryption Key and it Works,” Accessed: 21/09/2021; available at: https://www.zdnet.com/article/kaseya-says-it-has-now-got-the-revil-ransomware-decryption-key-and-it-works/
7. KrebsonSecurity, “Inside ‘Evil Corp,’ a $100M Cybercrime Menace”, available at: https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/; Accessed: 21/09/2021
8. US DoJ, Russian National Charged with Decade-Long Series of Hacking and Banking Fraud [..], available at: https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens; Accessed: 21/09/2021
9. The Quartz, “The Colonial Pipeline Ransomware Gang is Back Under a New Name”, available at: https://qz.com/2043312/the-colonial-pipeline-ransomware-gang-is-back-under-a-new-name/; Accessed: 21/09/2021
10. Zdnet, “REvil Ransomware Group Resurfaces after Brief Hiatus,” available at: https://www.zdnet.com/article/revil-ransomware-group-resurfaces-after-brief-hiatus/; Accessed: 21/09/2021
11. CybersecurityHelp, “Evil Corp Gang is Back with New WastedLocker Ransomware”, available at: https://www.cybersecurity-help.cz/blog/1338.html; Accessed: 21/09/2021
12. US Department of Treasury, “Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware”, available at: https://home.treasury.gov/news/press-releases/sm845; Accessed: 21/09/2021
13. Analyst1, *Nation State Ransomware*, pp, 7-8, available at: https://analyst1.com/file-assets/Nationstate_ransomware_with_consecutive_endnotes.pdf; Accessed: 21/09/2021

14. Michael Sandee, Tillmann Werner and Elliott Peterson: *Gameover Zeus – Bad Guys and Backends*, available at: https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends.pdf; Accessed: 22/09/2021

15. Trustwave, *Diving Deeper into the Kaseya VSA Attack: REvil Returns and Other Hackers are Riding Their Coattails*, available at: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/diving-deeper-into-the-kaseya-vsa-attack-revil-returns-and-other-hackers-are-riding-their-coattails/; Accessed: 22/09/2021

16. Recorded Future, *Dark Covenant: Connections Between the Russian State and Criminal Actors*, pp-14-15; available at: https://www.recordedfuture.com/russian-state-connections-criminal-actors/; Accessed: 22/09/2021

17. Ibid.

18. The White House, *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government,* available at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/; Accessed: 22/09/2021

19. Ibid.

20. Recorded Future, *Dark Covenant: Connections Between the Russian State and Criminal Actors*, p 15

21. The White House, "Remarks by President Biden on the Colonial Pipeline Incident", available at: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/; Accessed: 22/09/2021

22. ABC News, "White House Puts Blame on Russia for JBS Ransomware Attack, Weighs Responses," available at: https://abcnews.go.com/Business/white-house-contact-russia-meat-producer-jbs-hit/story?id=78021754; Accessed: 22/09/2021

23. Yahoo News, "Biden Gave Putin List of 16 Critical Infrastructure 'Entities' that Must be Off-Limits to Cyberattacks," available at: https://news.yahoo.com/biden-gave-putin-list-16-175500657.html; Accessed: 22/09/2021

24. CNN, "Biden Warns Putin During Call that 'We Expect Him to Act' on Russian Ransomware Attacks," available at: https://edition.cnn.com/2021/07/09/politics/biden-putin-call-syria-ransomware/index.html; Accessed: 22/09/2021

25. NY Times, "Preparing for Retaliation Against Russia, US Confronts Hacking by China;" available at: https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html; Accessed: 21/09/2021

26. Arstechnica, "FBI, Others Crush REvil Using Ransomware Gang's Favorite Tactic Against It"; available at: https://arstechnica.com/tech-policy/2021/10/fbi-others-crush-revil-using-ransomware-gangs-favorite-tactic-against-it/; Accessed: 22/10/2021