CYBER
THREAT
ANALYSIS
RUSSIA

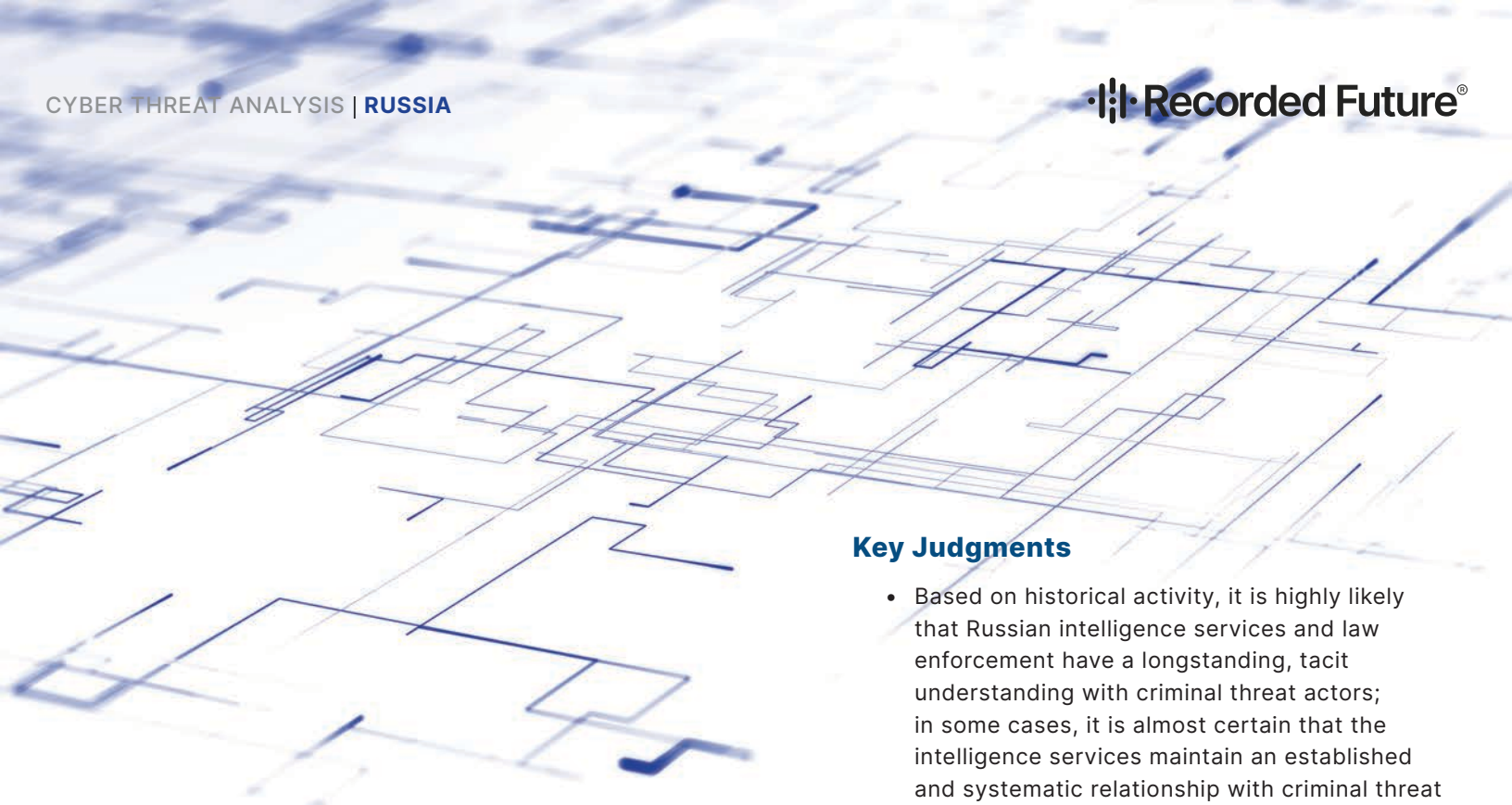
Recorded Future®

By Insikt Group®

September 9, 2021

Dark Covenant: Connections Between the Russian State and Criminal Actors

Recorded Future®



This report examines the unspoken connections between the Russian Federation (in the form of Russian intelligence services or the Kremlin) and cybercriminals in Russia and Eastern Europe. Sources include the Recorded Future® Platform as well as other dark web and open sources. The report will be of interest to threat researchers, as well as law enforcement, government, and defense organizations.

Executive Summary

The intersection of individuals in the Russian cybercriminal world and officials in the Russian government, typically from the domestic law enforcement or intelligence services, is well established yet highly diffuse. The relationships in this ecosystem are based on spoken and unspoken agreements and comprise fluid associations.

Recorded Future identified 3 types of links between the Russian intelligence services and the Russian criminal underground based on historical activity and associations, as well as recent ransomware attacks: direct links, indirect affiliations, and tacit agreement.

Even in cases with discernible, direct links between cybercriminal threat actors and the Russian state, indirect affiliations suggest collaboration, and a lack of meaningful punitive actions shows either a tolerance for, or tacit approval of, these efforts. This assessment takes into account that the Russian government possesses a robust surveillance apparatus and interfaces with cybercriminal elements and therefore has visibility into, if not control over, many of the resources used by these threat actors and can shut them down if they so desire.

Key Judgments

- Based on historical activity, it is highly likely that Russian intelligence services and law enforcement have a longstanding, tacit understanding with criminal threat actors; in some cases, it is almost certain that the intelligence services maintain an established and systematic relationship with criminal threat actors, either through association or recruitment.
- Precedent suggests that such activities and associations will almost certainly continue for the foreseeable future; however, these associations will likely adapt to provide greater plausible deniability and fewer overt, direct links between both groups.
- The open assertion made by US President Joe Biden that Russian cybercriminals are protected by the Russian government has placed Russian President Vladimir Putin on the defensive, forcing Russian domestic law enforcement to demonstrate that they are cracking down on ransomware operators.
- Following the disappearance of ransomware operators like REvil, we see other groups emerging in their stead and publicly committing to reforming their operations, including the refusal to attack critical infrastructure targets, which may be seen as a preliminary sign that the Biden administration's ultimatum to Russia has been successful, but it is still too early to gauge how great its long-term effect will be.
- If the Biden administration can persuade the Kremlin that bringing cybercriminal activity under some form of control is in their best interest — by granting sanctions relief, increased collaboration, or economic agreements — these immediate reforms may be substantive and long-lasting.

Table of Contents

Background

The Russian intelligence services' recruitment of highly skilled computer programmers, network specialists, and other technologically savvy personnel dates back to at least the 1990s and has even been reported in open-source publications like the Russian-language magazine "Hacker".[1] In one example from this publication in February 2002, an individual identified as "UFO" (ufobject@mail[.]ru) claimed that following his arrest for writing malware called "Dragon", which would enable any user to harvest passwords, he was approached by an individual with links to the Russian special services called "Sidorov". Sidorov claimed to have seen an expert examination of his case and was impressed with UFO's work. At a meeting in a Moscow restaurant, Sidorov told UFO that he needed an employee like UFO to search for vulnerabilities — work for which he would be well-compensated — and UFO accepted the position.

Such recruitment efforts continued through the 2010s. In his 2019 book "Intrusion: A Brief History of Russian Hackers", Daniil Turovsky quoted an unnamed Russian hacker who provided an account of the associations between the criminal underground and the Russian intelligence services. According[2] to the hacker, the Center for Information Security at the Russian Federal Security Service (CIB FSB) had limited technical staff, so it often brought in outside specialists, reportedly going so far as to hide some hackers in safe houses. On December 12, 2019, a Meduza report appeared to corroborate this account, suggesting that the FSB had been engaging in hacker recruitment efforts since at least the 1990s. The article also quoted an FSB officer as suggesting that as soon as hackers achieve a certain level of success they are targeted for recruitment. According to Meduza, "In [the FSB officer's] words, as soon as "the first technical college student from a humble background brought a Ferrari out onto the streets of Moscow", FSB agents started recruiting — both getting the cybercrime business under control and making it their own". In the early 2010s, in a conversation with a Recorded Future source, Sergei Mikhailov, who served as deputy head of the CIB FSB, confirmed that the FSB had visibility into some Russian-language criminal forums, though he claimed that they did not have their own operatives directly on the forums, instead relying on confidential informants. Mikhailov also stated that at the time, the FSB did not have enough technical experts and frequently worked with the Ministry of Internal Affairs' (MVD) Department K.

Andrei Soldatov, a Russian investigative journalist and co-author of "The Red Web", a book about the Kremlin's online activities, said that while the Russian government's tactic of outsourcing cyber operations to various groups helps distance themselves (and ultimately provides deniability), it also left them vulnerable to hackers running amok. In response to this, the Russian government engaged in limited cooperative agreements with foreign governments, like the US, to keep cybercrime under control. Russian and American federal law enforcement agencies maintained cooperative engagements in online crime during the 2000s via bilateral meetings and shared investigations. However, by the mid-2010s, such collaborative efforts were curtailed due to a lack of confidence from American law enforcement in Russian agents' abilities to execute their missions. According to former chief technology officer of the US Federal Bureau of Investigation's (FBI) cyber division Milan Patel, "We would tip them off about a person we were looking for, and they would mysteriously disappear, only to appear later on working for the Russian government. We basically helped the FSB identify talent and recruit by telling them who we were after". In another conversation with the Recorded Future source, Mikhailov opined that there were still quite a few "cold warriors" in the Kremlin who did not approve of the FSB's collaboration with US law enforcement and he was not at all certain that it would continue for much longer. His words appear to have been prescient.

Methodology

Based on an understanding of this historical context and considering the current cybercriminal and Russian government landscape, Recorded Future has classified the activity observed in this ecosystem into 3 major categories:

- Direct associations are identified by precise links between state institutions and criminal underground operators; an example of this is Dmitry Dokuchaev, a major in the Russian Federal Security Service who was recruited after working as a cybercriminal.
- Indirect affiliations occur in cases where a direct link cannot be established but there are clear indications that the Russian government is leveraging resources or personnel for their benefit; an example of this is the Russian government's likely use of the GameOver Zeus botnet for espionage or DDoS attacks by "patriotic hackers" during military conflicts.
- Tacit agreement is defined as the overlaps in cybercriminal activity, including targeting and timing, that benefit Russian state interests or strategic goals; such activity is conducted without direct or indirect links to the state but is allowed by the Kremlin, which looks the other way when such activity is conducted.

[1] The following contains a PDF: http[:]//web.archive[.]org/web/20210720233033/https[:]//xakep[.]ru/pdf/xa/038/

[2] http[:]//web.archive[.]org/web/20210720234233/https[:]//www.rulit[.]me/books/vtorzhenie-kratkaya-istoriya-russkih-hakerov-read-586355-49.html

Figure 1: Header for Dmitry Dokuchaev's personal website (Source: Internet Archive)

Threat Analysis

Direct Links

The worlds of cybercrime and the Russian special services intersect directly, either through coercive or willing recruitment. Willing recruitment occurs when individuals interested in supporting Russian government interests voluntarily seek to engage in efforts that support the state. Coercive recruitment occurs when the Russian government observes a skilled and successful malware coder on underground forums, arrests them for their activities, and presents them with 2 alternatives: prosecution and jail time or cooperation and a paycheck.

Another example of direct association occurs in cases in which the Russian intelligence services establish underground forums by which they can recruit participation from criminal threat actors ad hoc, which enables the Kremlin to surge effort for specific purposes. Some forums may take the form of overt criminal forums, which also allows intelligence services to spot talent for recruitment. Recorded Future sensitive source reporting indicates that around the time of Russia's conflict with Georgia in the late 2000s, Russian intelligence agencies attempted to create a new Russian-language hacking forum for "patriotic" hackers who would then target Georgia with DDoS and other cyberattacks. While the forum itself was not very active, Russian intelligence agencies attempted to lure Russian-speaking cybercriminals into the forum to destabilize the Georgian government with cyberattacks during the conflict.

The individuals outlined in this section have been reported as engaging in cybercriminal or financially motivated activity for personal gain and also have what we believe to be direct links to the Russian state, either through politicians, the Kremlin, or Russian intelligence services. More details on their histories and cases can be found in Appendix A.

Dmitry Dokuchaev

One of the most direct links between the cybercriminal community and the Russian intelligence community is former FSB employee Major Dmitry Dokuchaev. In the early 2000s, Dokuchaev was also known in underground communities by the nicknames "forbik" and "FORB", reportedly shorthand for "Forbidden". Dokuchaev claimed in a 2004 open-source interview that his interest in hacking initially manifested in intrusions against small local networks to freely access information. Dokuchaev also discussed making money by hacking and stated that "carding" (the practice of stealing and trafficking stolen payment card information) was the most financially profitable type of cybercrime.

Dokuchaev (like Evgeniy Bogachev, who is discussed in the Indirect Affiliations section) is described as a former member of high-profile carding platforms and likely engaged in spamming activities that would have drawn the attention of Russian law enforcement or intelligence services like the FSB. Sensitive sources appear to confirm that the FSB became aware of Dokuchaev due to his criminal activity, namely in carding. Dokuchaev reportedly was recruited by the FSB under threat of criminal prosecution; separate reporting indicates this approach is a common practice and suggests several employees of the CIS FSB have links to, or were members of, financially motivated targeted intrusion forums at some point in their careers. Despite the criminal activity or more likely because of it, Dokuchaev was hired by the CIS FSB, also known as Center 18. According to information from the FBI, he is believed to have been operating on behalf of this organization from at least January 2014 through December 2016, though open sources suggest that he began his work there as early as 2010. During his time at Center 18, Dokuchaev engaged in financially motivated cyber activity and also facilitated state-sponsored targeted intrusion activities. Dokuchaev and other personnel from Center 18 were reported to have "created and used the international hacker forum Mazafaka, aimed at hacking foreign financial institutions".

Figure 2: Dokuchaev (Source: FBI)

A February 2017 US Department of Justice (DoJ) indictment named Dokuchaev, as well as co-conspirators, for conducting intrusions and an expansive data theft operation targeting Yahoo in 2014, which sought to obtain information for use in espionage operations to benefit the Russian government. According to an FBI press release, "from at least January of 2014, continuing through December of 2016, Dmitry Aleksandrovich Dokuchaev is alleged to have conspired with, among others, known and unknown FSB officers, including Igor Sushchin, to protect, direct, facilitate, and pay criminal hackers, including Alexsey Belan". Dokuchaev and his conspirators allegedly gained unauthorized access to the computer networks and user accounts hosted at major companies providing worldwide webmail and internet-related services in the Northern District of California and elsewhere.

Konstantin Kozlovsky

Another significant cybercriminal with purported connections to the Russian intelligence community is Konstantin Kozlovsky, known as the leader of the Lurk cybercriminal group and creator of the Lurk malware. Kozlovsky, who was arrested in 2016, has since made several claims about working for the FSB under the guidance of Dokuchaev, and possibly others. Unlike most major cybercrime groups, Lurk primarily targeted victims inside Russia, causing speculation about why they felt safe doing so. According to Novaya Gazeta, a Russian independent news outlet, Kozlovsky claimed that Dokuchaev had ordered Lurk to target entities within Russia, such as entities owned by Evgeny Prigozhin, a close associate of Vladimir Putin and reported founder of Russian troll farms and the private military company Wagner. Kozlovsky suggested that such activity would benefit the FSB and enable them to conduct arrests and gain greater authority; however, such claims have not been confirmed.

In 2017, while incarcerated in Russia, Kozlovsky himself claimed that while he worked for FSB, specifically under Dmitry Dokuchaev, he was responsible for the 2016 hack and leak operation that targeted the Democratic National Committee (DNC) in the US. Furthermore, Kozlovsky stated that hackers supervised by the FSB used a new method of spreading ransomware, which consisted of "infecting one computer on the corporate network, raising privileges, gaining administrator access to the domain and stopping the activities of a company of any size with one button."

Maksim Yakubets and Evil Corp

On December 5, 2019, the US Department of Treasury (DoT) levied sanctions against a cybercriminal team operating out of Russia called Evil Corp, as well as Maksim Yakubets and Igor Turashev, the group's leaders. A DoT press release detailing the sanctions indicated that in addition to "managing and supervising the group's malicious cyber activities" from at least 2015, Yakubets was also "directly associated with Evgeniy Bogachev …[and was] responsible for recruiting and managing a network of individuals responsible for facilitating the movement of money illicitly gained through the efforts spearheaded by Evgeniy Bogachev".

At approximately the same time the sanctions were announced, the Russian-language investigative media outlet Meduza reported that Yakubets and Evil Corp maintained close associations with the FSB, stating that "Evil Corp's hackers belong to the families of high-ranking Russian state bureaucrats and security officials". Meduza, citing the Washington Post, suggested that Yakubets had been active in conducting intrusions since at least 2009 when the crew he was working with had reportedly stolen "$415,000 from the treasury of Bullitt County in far western Kentucky". The report indicated that by at least 2019, Yakubets was managing the group. In addition to conducting intrusions for personal gain, the DoT also indicated that Yakubets worked directly in support of FSB interests, stating,

> *Yakubets has also provided direct assistance to the Russian government. As of 2017, Yakubets was working for the Russian FSB, one of Russia's leading intelligence organizations. … As of April 2018, Yakubets was in the process of obtaining a license to work with Russian classified information from the FSB … Additionally, as of 2017, Yakubets was tasked to work on projects for the Russian state, including acquiring confidential documents through cyber-enabled means and conducting cyber-enabled operations on its behalf.*

Evil Corp is operated by Maksim Yakubets and Igor Turashev and is known to use the following malware variants: WastedLocker ransomware, BitPaymer ransomware, and the Dridex banking trojan. The preferred attack vectors used by Evil Corp are phishing and malicious code injection. According to Recorded Future data, Evil Corp has been in operation since at least 2011 and has targeted over 150 public and private sector entities in at least 25 countries, including organizations in the banking, automotive, government, information technology, law enforcement, retail, ICS/SCADA, manufacturing, and software development industries.

Pavel Vrublevsky

According to a 2014 Russian-language article[3] in Forbes, Vrublevsky engaged in cybercriminal affairs and also "maneuvered between the Ministry of Internal Affairs and the FSB for many years, making acquaintances with high-ranking officials from the special services and in power, but the risky game ultimately led him to jail". Vrublevsky was similarly involved[4] in a 2007 investigation[5] as a witness to criminal activity. During the case, the investigator said the following:

> *Maltsev, who was involved in the criminal case, resigned from the Ministry of Internal Affairs and got a job in the security service at Chronopay. And when Vrublevsky ended up at Lefortovo [a high-security prison in Moscow], it was Maltsev, who by that time had received the status of a lawyer, [who] became one of the official defenders of the Chronopay CEO.*

When interviewed[6] by Russian-language media outlet Novaya Gazeta about whether Vrublevsky had been recruited by the FSB, Russian State Duma Deputy Ilya Ponomarev stated,

> *I have no such information. But Vrublevsky is a very large player in the payment system market. And this market cannot exist without the strong support of senior officials in the intelligence services. If you do not have cover either from the Ministry of Internal Affairs or from the FSB, you will not be able to work in this market. But protection is one thing, and the agents are another, they are different things.*

Vrublevsky also featured prominently in a recent treason trial in Russia. During Vrublevsky's 2013 trial, the former chief of the cybercrime department at Russia's FSB security service, Colonel Sergei Mikhailov, testified against Vrublevsky. After Vrublevsky's release, according to a report by Radio Free Europe/Radio Liberty, "Russian prosecutors accused Mikhailov and Stoyanov [a former researcher at the Russia-based cybersecurity firm Kaspersky Labs] of passing classified information about Vrublevsky to the FBI. Russian press reports, citing unnamed officials, alleged that Mikhailov was paid $10 million for the information". After a closed trial in 2019, Mikhailov was sentenced to 22 years in prison, and Stoyanov to 14 years.

Roman Seleznev

Roman Seleznev was born in 1984 in Vladivostok, Russia. The son of Valery Seleznev, a member of the Russian State Duma, Seleznev started his hacker career at the age of 18 in 2002. In his early career, Seleznev operated under the usernames "nCux" (a transliteration of пСих, meaning "psycho"), "Track2", and "Bulba", becoming one of the largest carders in the Russian hacker scene. Initially, nCux would break into databases to steal personally identifiable information (PII) and later moved on to stealing payment card information and selling it in underground carding forums. He primarily targeted databases of small businesses in the US, mainly due to low-security protocols used by many small businesses.

Seleznev attracted the attention of the US Secret Service (USSS) in 2005, and in 2009, USSS and FBI agents traveled to Moscow as part of a joint investigation with the FSB. The US agencies provided the FSB with information on Seleznev's underground identity and his activities. But a month after the meeting, Seleznev announced his retirement and deleted his profiles from underground carding forums. US indictment documents against Seleznev note that he was likely tipped off about the US investigation by the FSB. This theory is supported by a conversation Seleznev had with one of his associates, Vladislav Horohorin, in which Seleznev noted that he enjoys FSB protection and has ties to agents working for CIB. However, instead of retiring after deleting his online profiles, Seleznev quickly created several new usernames and expanded his carding operations. Operating under the usernames "Track2" and "Bulba", Seleznev created an online marketplace for carders, simplifying the purchase of stolen information.

[3] https://www.forbes[.]ru/forbes/issue/2014-11/270967-sex-drugs-and-rock-n-roll
[4] https://novayagazeta[.]ru/articles/2012/11/30/52573-kiberprestupnik-8470-1-pavel-vrublevskiy-superagent-ili-zhertva-fsb
[5] https://krebsonsecurity.com/wp-content/uploads/2010/05/ivptrans.pdf
[6] https://novayagazeta[.]ru/articles/2012/11/30/52573-kiberprestupnik-8470-1-pavel-vrublevskiy-superagent-ili-zhertva-fsb

Seleznev was arrested by the USSS while vacationing in the Maldives in 2014. In April 2017, he was sentenced to 27 years in prison for "computer hacking" that caused more than $169 million in damages. In September 2017, Seleznev was sentenced to 14 years (concurrent) in jail under similar charges. In the aftermath of his arrest, Russia publicly and vociferously objected to his arrest; a social media post from the Russian Embassy in the US stated that the "[a]rrest of [Russian] citizen Roman Seleznev who de facto was kidnapped in a 3rd country [sic] is unlawful". More details on Seleznev's history and case can be found in Appendix A: Additional Information on Direct and Indirect Links, Roman Seleznev.

Alexey Stroganov

Alexey Stroganov, also known as "flint24", a moderator of the "Carder" (carder[.]org) underground forum and the head of the criminal online shop "Real Plastic" (realplastic[.]org), is considered by many to be the most senior carder in all of Russia. His criminal record dates back to 2003, when he was arrested by Russian law enforcement due to his association with carding operations. According to Russian news sources, however, by the time of his arrest, Stroganov had already been wanted by the police for 9 years for unspecified fraudulent activity.

In addition to his criminal activities, Stroganov also operated multiple legal businesses in the Russian Federation and supported multiple charity causes as well as a non-profit "cybercrime-fighting" organization dubbed Kibalchish. Its official website, kibalchish[.]org, now defunct, claimed that the organization helped educate about and combat cybercrime such as carding and phishing. Additionally, it appears that Kibalchish was involved in combating the illegal sale of tickets during the 2018 World Cup in Russia.

Through these non-profits, Stroganov built ties with political figures. Ultimately Stroganov built a close friendship with Vadim Dengin, a Russian politician serving as the deputy of the State Duma of the Russian Federation, and a member of the Liberal Democratic Party of Russia. Importantly, Dengin is the First Deputy Chairman of the Committee on Informational Policy, Information Technology, and Communications, which oversees passing laws concerning RUNet (a general term for the Russian internet) and cybercrime. Beyond his ties with Dengen were indications that his attorneys used awards provided by both Vladimir Putin and FSB director Alexander Bortnikov to protect him from prosecution.

As Gemini Advisory points out, "In Russia, it is widely known that acquiring political ties comes with a level of immunity. One of the key elements in making those connections is finding politicians willing to accept bribes, which requires either knowing someone in political circles or knowing the politician directly."

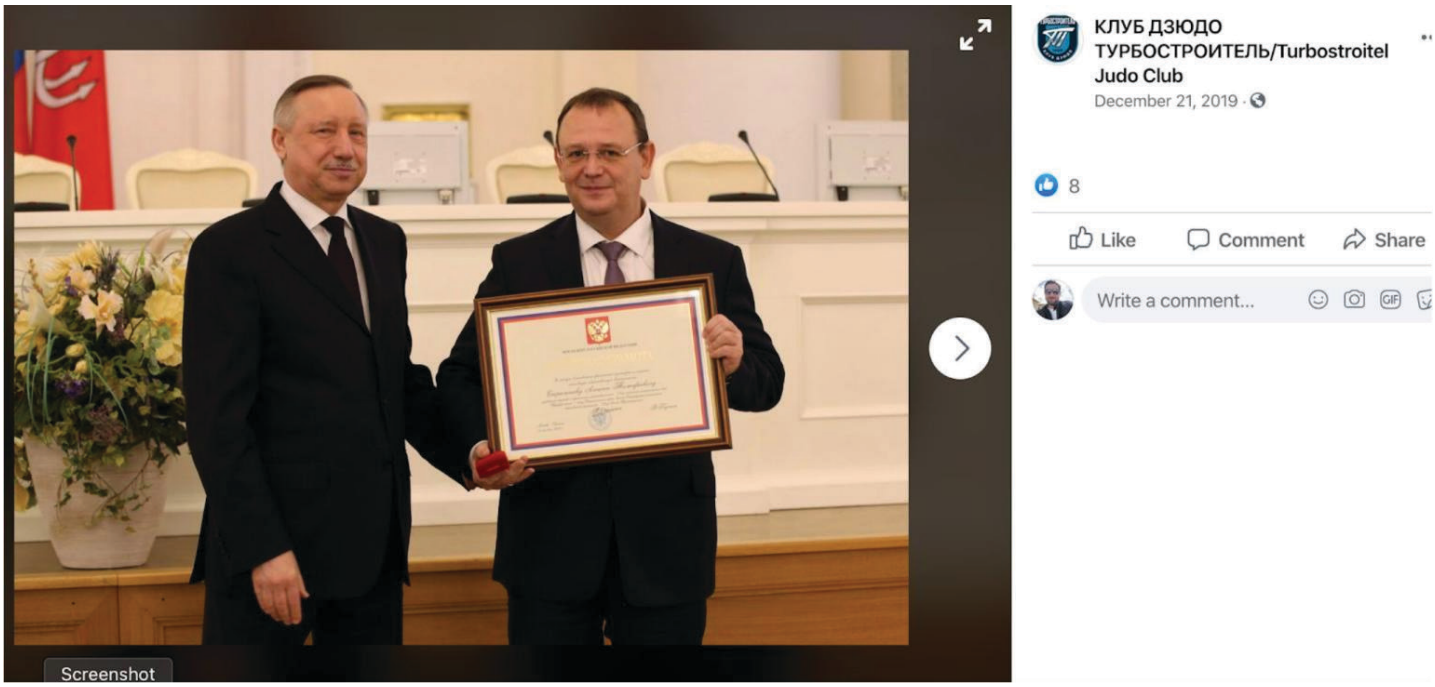


Figure 3: Image of Stroganov (right) receiving a Russian government award from the Governor of St. Petersburg, Alexander Beglov (Source: Facebook)

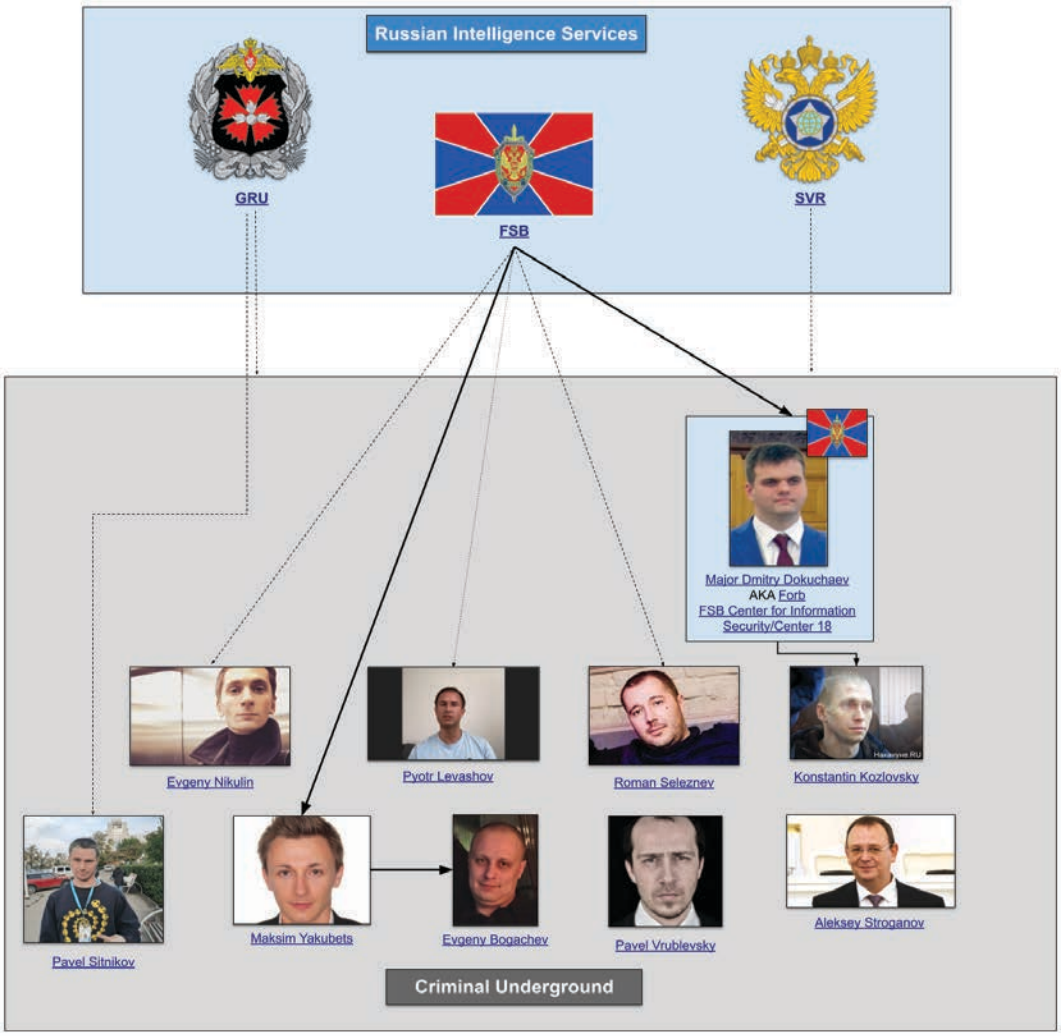


Figure 4: Graphical representation of the direct and indirect links between Russian Intelligence Services and individuals in the Russian criminal underground (Source: Recorded Future)

While the cybercriminals outlined in the figure above have been linked in various ways with Russian politicians, law enforcement, and intelligence agencies, they are by no means the only individuals whose activities appear to have benefitted members of Russian circles of power.

Indirect Affiliations

In other cases, the state may not directly employ individuals from the criminal hacking ecosystem but may use their infrastructure to further Russian government interests. Additionally, "patriotic hackers" may conduct actions that benefit the state but are not directly linked to any Russian government or intelligence service entity. In these cases, the associations between cybercriminals and the state are much more diffuse, but the effects still support Russian government goals.

A similar effort, falling under the indirect category of activity, occurred between April and May 2007 when DDoS attacks targeted Estonia's government, news, banking, and telecommunications online resources. The activity was described by the independent research organization CNA as "the first large-scale coordinated use of cyber by Russia to affect a strategic outcome in a neighboring state" but also tactically unsuccessful, given that it did not affect the root cause of the conflict, the relocation of a Soviet-era monument. An unidentified Estonian government official told the BBC that the attack "was orchestrated by the Kremlin, and malicious gangs then seized the opportunity to join in and do their own bit to attack Estonia".


На 9-е МАЯ планируется повтор данной акции!
Не дай унизить своих соотечественников, отомсти за издевательства !!!
@ адреса eSStонских депутатов

Программа для рассылки писем
(пароль на RAR: nnm)

Нажми (пуск -> выполнить -> cmd)
введи ping -n 5000 -l 10000 эSStонский_сайт -t . и жми ENTER ВСЕ !!! Твои пламенные приветы полетели...
пример: ping -n 5000 -l 1000 www.riik.ee -t
Это 3 элементарных действия, после которых многие эстонские сайты просто перестанут работать!!!
Или вот .BAT файл, который в автоматическом режиме последовательно пингует эстонские DNS и MAIL сервера. Цикл бесконечен :)
Скопировать (красным) нижеприведённый текст, вставить в блокнот и сохранить как priveteSStonia.BAT (название можно любое) файл
(ты можешь сам добавлять адреса)

Figure 5: Post describing how to conduct DDoS attacks found on Russian-language sites (Source: CCDCOE)

Some of the ways that these criminal efforts have benefited Kremlin interests include targeting Kremlin opponents with malicious activities against Estonia, Georgia, Ukraine, and Western countries as well as providing tools, infrastructure, and access to the Russian government and intelligence agencies both wittingly and unwittingly. Russian intelligence agencies have used criminal commodity malware to obfuscate their activities and make attribution more difficult. They have used criminal money laundering networks and bulletproof hosting to obfuscate the movement of funds and sponsorship of disruptive activities. They have also used networks compromised for criminal purposes to search for sensitive data and credentials to advance espionage activities and targeting against both domestic opposition and Western entities and governments. The following sections outline some of the individuals involved in activities and operations that we believe were either sanctioned or co-opted in some way by the Russian state.

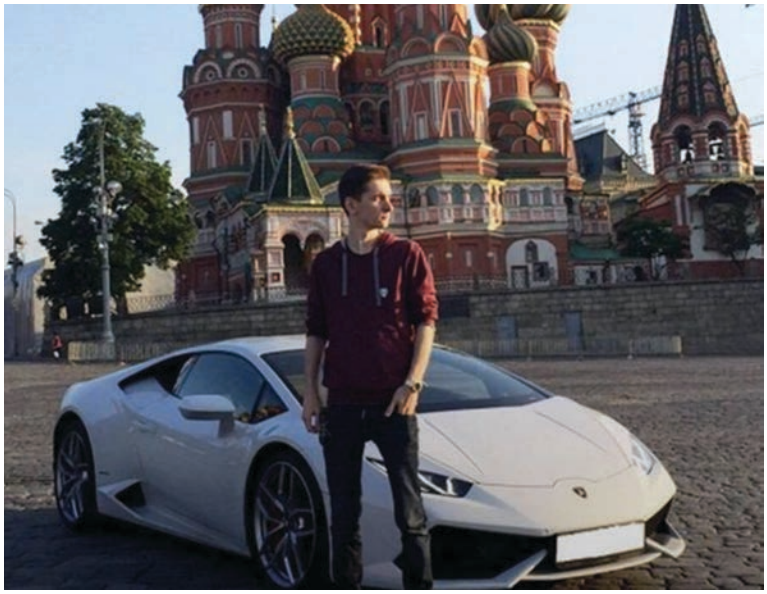


Figure 8: Evgeny Nikulin posing for a photo in front of St. Basil's Cathedral in Moscow's Red Square (Source: Gazeta)

Evgeny Nikulin

Evgeny Nikulin has been active since at least 2012 when, according to a charging document from the US District Court of the Northern District of California, he "engaged in a sustained campaign to steal user account credentials from major US companies" including LinkedIn, DropBox, and Formspring. Nikulin obtained LinkedIn user credentials by gaining access to a personal computer used by a LinkedIn employee who subsequently used the same computer to log in to LinkedIn company network resources via a virtual private network (VPN). Although the initial intrusion vector was not specified in the charging document, the court documentation indicated that a DropBox employee was targeted similarly via a spearphishing attack from the email addresses chinabig01[@]gmail[.]com and R00talka[@]gmail[.]com, which an FBI investigation linked to Nikulin as well as to the LinkedIn and Formspring activity. After gaining access to the user data from the targeted companies, Nikulin monetized the access by either posting the encrypted material to forums or negotiating the sale of the material to other Russian hackers. Beyond the value the information holds for sale to other Russian hackers on the black market, we assess that the value of this information to Russian intelligence services is also high; however, it is not publicly known whether Nikulin attempted to broker such a sale of these datasets to government agents.

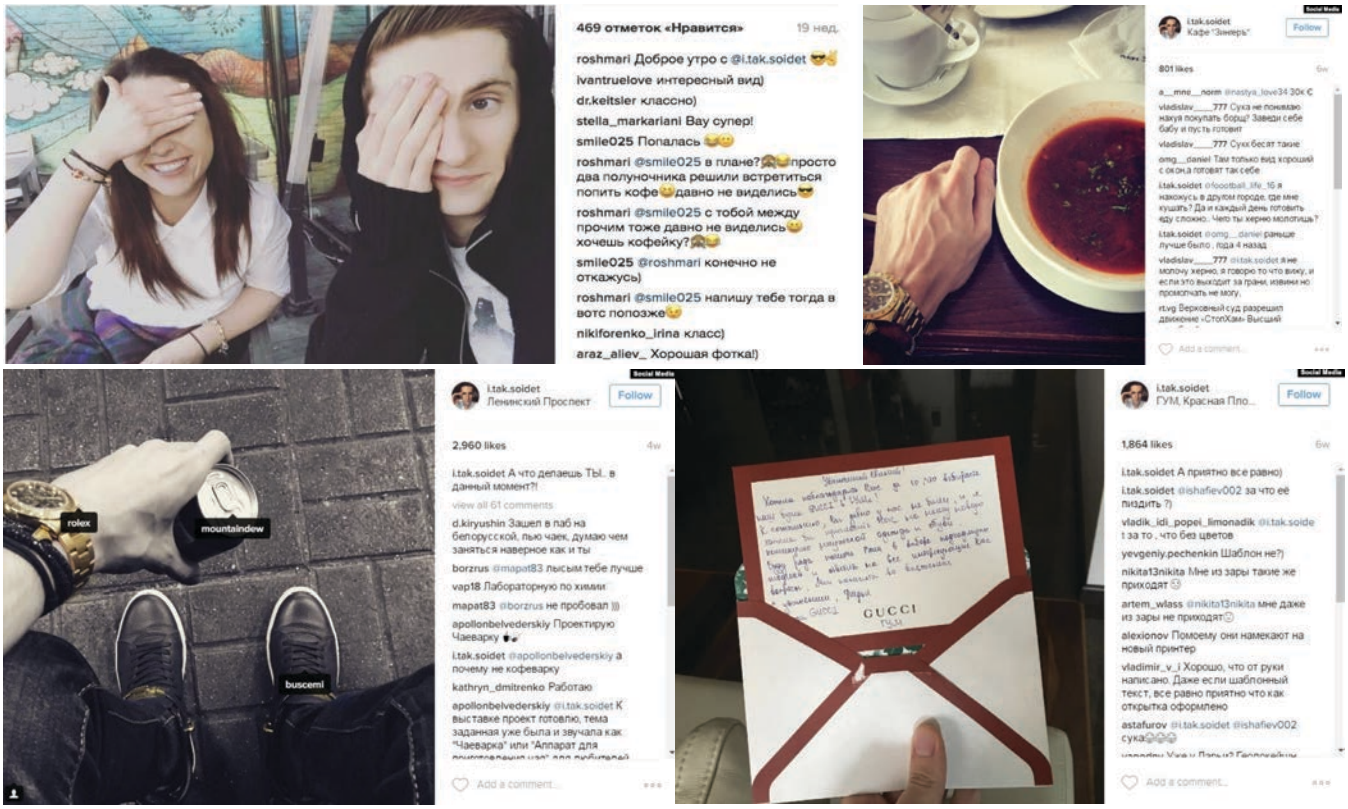


Figure 7: Images in which Nikulin demonstrates his associations with United Russia-affiliated personnel as well as his interest in luxury goods (Sources: Gazeta and Currenttime TV)

Nikulin was detained in the Czech Republic on October 5, 2016, and, following a court battle between the US and Russian governments about which state would obtain Nikulin, he was eventually extradited to the US in 2018, where he was charged for his role in the LinkedIn, DropBox, and Formspring intrusions. In the wake of his arrest and extradition, open-source media reports identified Nikulin's social media accounts, which revealed his associations to individuals like Maria Roshchina, affiliated with the pro-Kremlin United Russia party, as well as his lavish lifestyle in which he flaunted his interest in luxury goods. The case has also drawn some attention in Russia, where reporters have unearthed photos of the self-described "used car salesman" driving lavish cars and taking photos with the Russian elite. Nikulin's social media pages had included snaps with both the daughter of Defense Minister Sergei Shoigu and Kremlin press secretary President Dmitry Peskov; however, it appears that these photos have been scrubbed from his social media at the time of writing.

Pyotr Levashov

Another particularly colorful figure on the Russian dark web is Pyotr Levashov. Also known by the alias "Severa", he is responsible primarily for distributing spam via the Storm Worm, Waledac, and Kelihos botnets; given how prolific he was, some identify Levashov as the "king of spam". A July 13, 2021 sentencing document indicated that "Levashov used the knowledge that he obtained working with Storm Worm to develop, and to pay others to develop the Waledac botnet". Waledac exceeded Storm in its distribution of spam, sending more than 1.5 billion spam messages a day. The Waledac botnet was taken down by Microsoft in March 2010. Levashov then built the Kelihos botnet, which again exceeded the spam volume of its predecessor, sending more than 4 billion spam messages a day. In addition to his involvement in developing these botnets, Levshov is charged with engaging in credential harvesting and denial-of-service attacks. The Kelihos botnet was taken down in April 2017.

Figure 10: Photos of Bogachev engaging in his hobbies of exotic cat ownership and boating (Source: New York Times)

After the Microsoft takedown of Waledac, on April 1, 2012, Levashov created a lengthy post on Russian-language forums stating that he was officially quitting cybercrime and moving to Microsoft to head up their new cybercrime fighting team. While the April Fools joke elicited some confusion, it was the post that Levashov crafted on April 1, 2013, on several Russian-language dark web forums that drew substantial attention. This time the post suggested that he was entering into an affiliation with the Russian intelligence services; specifically, he appeared to attempt to recruit individuals on the forum to work for a new organization that he claimed to lead in the FSB, identified as the Separate Special Information Security Battalion. Although the post was likely a joke, it did elicit some lively conversation on the forums, including some interest in the forum from individuals who appeared to be taking the post seriously and indicated an interest in working for the new organization. This April Fools joke could have easily helped the Russian intelligence services to identify potential recruits among the threat actors who took the post seriously. After Levashov's arrest and extradition to the US, Levashov's wife claimed that he was being questioned about potential links to Russian nation-state activity.

Evgeniy Bogachev

Perhaps the most effective cybercriminal of all time and one who has held the top spot on the FBI's list of most-wanted cybercriminals is "slavik". According to a US DoJ indictment filed in May 2014, Evgeniy Mikhailovich Bogachev, also known by his online pseudonyms "lucky12345", "slavik", and "Pollingsoon", created and employed a vast network of computers consisting of "an estimated 500,000 to 1 million compromised systems globally", known as the GameOver Zeus Botnet, to obtain personal and financial information from infected hosts. The indictment indicated that "Zeus is malware specifically designed to automate the theft of confidential personal and financial information, such as online banking credentials, from infected computers through the use of keystroke logging and web injects". This feature of the malware, in conjunction with the number of infected hosts, was likely of interest to the Russian government, as open-source reporting suggests that the Russian intelligence services sought to use GameOver Zeus in "attempts to gain access to sensitive military and intelligence information on infected computers in the United States, often consisting of searches for documents containing the words 'top secret' or 'Department of Defense'".

Figure 11: Sample of the type of espionage-related content observed with GameOverZeus Botnet activity (Source: GameOver Zeus – Bad Guys and Backends)

Open-source reporting, which cites information from the Ukrainian Interior Ministry, suggests that Bogachev had been "working under the supervision of a special unit of the FSB". A former assistant special agent in charge of cyber investigations for the FBI, Austin Berglas, supported this assessment, suggesting that Bogachev was "doing the bidding of Russian intelligence services, whether economic espionage or straight-up espionage".

The same reporting, which cites FBI data, states that Bogachev "used to sell malicious software on a site called Carding World, where thieves buy and sell stolen credit card numbers and hacking kits". His activity on this website likely drew the attention of Russian intelligence security professionals present on these forums and may have resulted in his recruitment by the Russian government. Indeed, Zeus and the slavik moniker were made known to the FSB by US law enforcement representatives as part of the joint counter-cybercrime collaboration efforts and according to sensitive sources Russia may have initially been involved in Operation Tovar, a multinational effort to take down the GameOver Zeus network in 2014, before pulling out at the last minute. It is not currently possible to validate that connection between Bogachev and the Russian government definitively.

Nevertheless, there are indications that Bogachev has, at a minimum, enjoyed protection from Russian law enforcement as he lives a luxurious life freely on the Black Sea city of Anapa, Russia. Additionally, unnamed officials suggest that Bogachev owned a luxury yacht and "had three Russian passports with different aliases allowing him to travel undercover". A Recorded Future source also claimed that Bogachev was involved in acting as a go-between for Vladislav Surkov, Putin's close advisor, and paying for Russian disinformation campaigns run by independent disinformation as a service actor targeting the West.

BLACKENERGY

Disruptive attacks aimed at the Ukrainian energy grid in December 2015 relied, in part, on a backdoor called BlackEnergy3 to facilitate access to the targeted systems. BlackEnergy3 is a specialized variant of an older, similarly named cybercriminal tool called BlackEnergy. BlackEnergy, and a later variant called BlackEnergy2, trace their origins to a developer named Dmytro Oleksiuk (also known online as "Cr4sh"), who initially designed the malware to conduct DDoS attacks, distribute spam email, and steal personal or financial information from targeted hosts. A separate open-source report corroborates the link between Cr4sh and BlackEnergy, noting the author's name in a "screenshot of the software's point-and-click panel".

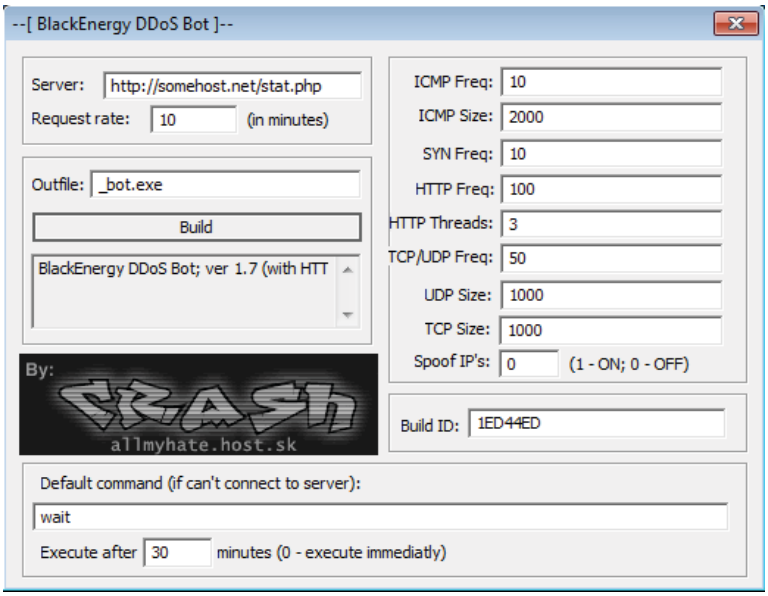


Figure 12: Initial BlackEnergy panel showing the name "Crash" as the author (Source: BlackBerry ThreatVector Blog)

According to open-source reporting, "Around 2007, Oleksiuk had sold BlackEnergy on Russian-language hacker forums, priced at around $40". Separate, public reporting indicated that "though Dmytro has always denied involvement in developing later versions of the tool ... The Sandworm team [a Russian APT associated with Unit 74455 of the Main Intelligence Directorate] appears to be using the malware to collect intelligence. The researchers say their use of BlackEnergy indicates a link between the attackers and the criminal underground, although their campaign is more sophisticated".

Alexander Vinnik

In July 2017, the DoJ issued an indictment against Alexander Vinnik, claiming that BTC-e, a cryptocurrency exchange that he established in 2011 and maintained access to, facilitated "numerous ransomware and other cybercriminal activity". Reporting indicates that BTC-e was run out of several locations, including Bulgaria, Cyprus, and Seychelles and was "heavily reliant on the criminal underworld and people and entities interested in anonymity or hard-to-trace transactions". Vinnik was arrested by authorities in Greece in conjunction with the indictment in the US. Additionally, the DoJ indicated that they had seized BTC-e infrastructure citing its links to cybercriminal activity as well as the allegation that Vinnik received funds from the 2014 intrusion of the cryptocurrency exchange Mt. Gox.

Vinnik and BTC-e are of relevance to the Russian intelligence services given that bitcoin analysis firm Elliptic traced the use of bitcoin by GRU-linked advanced persistent threat (APT) group APT28 "to a number of sources including BTC-e". APT28 employed cryptocurrency to purchase infrastructure, such as domains, lease servers, and VPN accounts that were then used in targeted intrusion operations, such as the one which impacted the Democratic National Committee (DNC) in 2016, according to a 2018 DoJ indictment. Bolstering the likelihood of this connection, the Russian government put up an extensive legal effort to fight the US request for extradition, going as far as quickly opening a case against Vinnik in Russia and requesting his extradition there to stand trial.

Tacit Agreement

Ultimately, whether or not there are connections between Russian authorities and cybercriminals becomes a moot point. Cybercriminals are widely known both inside Russia and abroad, and aside from pursuing the few individuals who have targeted entities inside Russia or who have crossed some sort of political line, Russian authorities have done little to try to disrupt the Russian-language criminal ecosystem. The Kremlin's muted response to cybercriminal activities originating from within Russia has nurtured an environment where cybercriminal organizations are well-organized enterprises. Until the Russian government decides to investigate and prosecute cybercriminals operating in Russia, it will continue to be a safe haven.

Tacit agreements occur when the Russian criminal hacking ecosystem conducts activity independent of any directive by the state. This type of activity, and its timing, are consistent with Russian government strategic goals; although, there are no direct or indirect links within these efforts. The Russian government forms a tacit agreement between the individuals conducting the attacks by not prosecuting them so long as they target "the right" entities and do not harm Kremlin interests.

Malware That Looks Like Ransomware

Tacit links also occur when state-sponsored activity employs malware that looks like ransomware to provide plausible deniability, or complicate attribution, for cyber operations that benefit the state. These are not direct links as it is not clear whether the individuals employing this malware are members of the cybercriminal ecosystem, but the malware itself certainly takes its appearance or code framework from cybercriminal sources. It is not indirect as it is not the sharing of a criminal resource for state benefit. Rather, this tactic is emblematic of the state's tacit approval of the cybercriminal ecosystem.

The use of commodity malware by Russian intelligence services almost certainly allows the Russian government to maintain plausible deniability[7] in targeted intrusions, especially when nuances between the details of specific variants of malware are used. In addition to modifying and using commodity malware like BlackEnergy, Sandworm has also been linked to other intrusions which employed modified versions of ransomware in order to conduct disruptive and destructive intrusions. The most widely known examples of this type of activity include a series of attacks against systems in Ukraine in 2017 designed to look like ransomware; these attacks employed XData, FakeCry, PSCrypt, and NotPetya malware. The discovery of these tools as part of a likely state-sponsored operation, as opposed to a financially motivated one, was realized when researchers discovered that payments for advertised decryption tools associated with these attacks were either impossible to complete or had no effect.

[7] In a June 14, 2021 interview with NBC News, Russian president Vladimir Putin contradicted the claim that Russia engaged in cyber attacks against US targets, stating "We have been accused of all kinds of things … Election interference, cyberattacks and so on and so forth. And not once, not once, not one time, did they bother to produce any kind of evidence or proof. Just unfounded accusations".

Outlook

Based on the longstanding relationship between the Russian intelligence services and the Russian cybercriminal ecosystem, it is almost certain that these connections will persist for the foreseeable future, and very likely continue to facilitate Russian intelligence service operations. As long as cybercriminals remain protected from domestic prosecution, are allowed to profit from their operations, and the Russian government maintains plausible deniability in their operations, there is no indication that such activity will stop, and malware procurement and infrastructure use via these relationships will continue. However, if the Russian government determines that the cost of protecting or ignoring cybercrime is higher than the benefit, we believe they can significantly reduce Russian cybercriminal activity.

The high-profile ransomware attacks against Colonial Pipeline, JBS, and Kaseya, have increased pressure on the Russian government to take action against the cybercriminal groups behind this activity. It is widely known that the groups behind these attacks are located in Russia; the lack of action by the Russian government only highlights the apparent complicity of the Kremlin in these efforts. This pressure already appears to have yielded statements that indicate a potential change in relation to ransomware operations, such as the recent BlackMatter ransomware gang's pronouncements that it will not target critical infrastructure.

But irrespective of the costs and incentives, the current Russian government is not likely to crack down on cybercrime in the near future beyond potentially taking some limited steps to appease international demands. In addition to these actions, the threat actors themselves will likely improve or increase their operations security (OPSEC). Furthermore, the Russian cybercriminal and intelligence services will likely obfuscate their affiliations and collaboration or compartmentalize duties in order to reduce the likelihood of discovery or detection.

We have seen a shift in calculus following recent high-profile ransomware attacks and subsequent intergovernmental consultations between the US and Russia. In terms of ransomware operations, the administrators of 2 major Russian-language forums, Exploit and XSS, quickly banned ransomware topics on their criminal underground platforms. Moreover, DarkSide, REvil, and Avaddon ransomware families halted extortionist activities right before or days after the first meeting between Presidents Biden and Putin.

Presidents Biden and Putin met for the first time on June 16, 2021, in Geneva, Switzerland. One of the major topics of the meeting was reported to have been a request for the Russian government to address domestic ransomware and cybercrime. The prioritization of this issue reveals an awareness of the connections between the ransomware decision-makers and the Russian state. Although President Putin has publicly denied any Russian government involvement in these incidents, there has been a shift in the policies of ransomware operators in the days following the summit.

In an exclusive interview conducted by Recorded Future analysts with BlackMatter ransomware operators, the group said some industries were off-limits: It would not extort healthcare, critical infrastructure, oil and gas, defense, non-profit, and government organizations. The White House deputy national security adviser for cyber and emerging technology, Anne Neuberger, issued a statement at the Aspen Security Forum on August 4, 2021, which suggested that the interview is a positive sign of compliance by the Russian government of requests made by the Biden Administration to bring Russian domestic cybercrime under control. In her statements, reported by Recorded Future's Record Media, Neuberger stated the following:

> *We think we're seeing a commitment, and we will look to see the actions that follow on that commitment... As we looked at that interview, we took it as evidence, or perhaps as a sign, that the message regarding the disruptive ransomware activity against critical infrastructure is unacceptable ... We're looking to see the changes and addressing disruptive cyber activity over time.*

Appendix A: Additional Information on Direct and Indirect Links

Dmitry Dokuchaev

Dokuchaev was born in Kamensk-Uralskiy, Russia in 1984 and developed his interest and skills in computer programming and network systems administration until eventually specializing in computer and network intrusions. In early 2006, Dokuchaev served as an editor at the Russian technology magazine "Hacker" under the supervision of Nikita Kislitsin.[8] Dokuchaev, who is reported to have engaged in carding, admitted that such activity was not without its risks, claiming that authorities in Russia were cracking down mercilessly on those engaging in this type of criminal activity domestically. Although Dokuchaev did not say when he conducted those initial intrusions against small local networks, what is known is that Dokuchaev later graduated to state-sponsored attacks to deliver malware to targeted hosts abroad, including in the US and other Western countries.

"ВЧК-ОГПУ", a Russian-speaking Telegram channel with 162,000 subscribers and website rucriminal[.]info, explained to their readers details of Dokuchaev's case:

> *To understand the story of how Dmitry Dokuchaev, an employee of the Information Security Center of the FSB of the Russian Federation, was immediately accused of treason in Russia and at the same time of cybercrime in the United States, one must carefully study the indictments. But only not the one in the United States, although there are interesting moments there, but to carefully study the indictments of hackers whom the FBI arrested after the arrest of Dokuchaev in Moscow. And also to study the documents of the trial of the hacker Kozlovsky in Yekaterinburg and the confrontation around the stolen money of the WEX crypto exchange and the programmer Vinnik. All these cases are connected with each other by one person - Dokuchaev.*
>
> *From the documents of the United States it becomes clear that Dokuchaev had a small army of hackers, and with many he became close friends even before he got into the FSB. This army made obscene money (hundreds of millions of dollars) from cybercrime both outside Russia and in Russia. Members of this army and hackers Nikulin, Kislitsyn, and, for example, two Ukrainian hackers, who were put on the wanted list by the United States a week ago. This army rallied back in Yekaterinburg, its members from there moved together to Moscow. From the American documents on Kislitsyn and Nikulin, it is clear that another member of their inner circle was Oleg Tolstykh. This person subsequently pelted the Web with documents of strange content and then went into the shadows. Konstantin Kozlovsky and his Lurk gang were from the same army. He just did not go to Moscow, stayed to work, and specialized in hacking non-Western and Russian banks. There were at least six bands like Lurk. And they all cleaned out the banks. And at the head of the army was Dokuchaev.*
>
> *Kozlovsky, unlike other army men, was initially more independent, although he was also Dokuchaev's connection. Kozlovsky has an interesting point in the case - the real hacker (MEG), who broke Sberbank and other banks, turned out to be an agent of the TsIB (CIB) of the FSB of the Russian Federation. The activities of Lurk became a reason for Sberbank to invest a billion dollars under the leadership of the head of the Central Information Security Service of the FSB Sergei Mikhailov in the creation of BiZone (protection against cyber threats and testing of the bank's security systems).*
>
> *This entire army is members of a number of famous online cyber crime forums - exploit.in, MAZA.la and Zloy. These forums grew on the foundation of the Carder Planet forum of Ukrainian Dmitry Golubev (Script, leader of the Internet party of Ukraine) after the closure of his project. Therefore, the army was originally Russian-Ukrainian. Controlling the forums means controlling all cybercrime to some degree. And these forums were under the control of the CIB, Dokuchaev answered specifically. The forums were in the shadows - because it was beneficial for the CIB to keep them in the shadows.*

[8] Kislitsin was indicted by the Department of Justice in 2014 for trafficking hacked data.

Ruslan Stoyanov, a former MVD and "Kaspersky Lab" employee, who was convicted for treason charges together with Dokuchaev and Mikhailov, made a public statement after his conviction:

> *There is a huge temptation for "decision makers" to use ready-made solutions to Russian cybercrime in order to influence geopolitics.*
>
> *The worst scenario is to give cybercriminals immunity from retaliation for stealing money in other countries in exchange for intelligence. If this happens, a whole layer of "patriotic thieves" will appear, violating the principles of the rule of law and the inevitability of punishment.*
>
> *The appearance of such people will immediately give rise to a new subculture. Through underground forums, the phenomenon will be romanticized and generate a wave of followers almost uncontrolled by the state and by nature inclined towards anonymity.*
>
> *It is difficult to steal from international financial organizations, and our talents, having failed there, will turn their attention to where everything is in Russian, throwing away all the patriotic fervor. We will get a new wave of crimes in Russia. That is, everything that we have fought for over the past 5 years will pass to dust.*

In late 2016, Major Dmitry Dokuchaev, by this point a senior officer of the FSB's Second Operational Management Department of Center for Information Security, was arrested by Russian law enforcement and subsequently convicted of high treason. The treason charges stemmed from claims that Dokuchaev, along with other suspects, transferred data about an individual engaging in financially motivated threat activity to US intelligence officials. In April 2018, Dokuchaev signed a pre-trial agreement accepting a conditional guilty plea in relation to charges relating to the transfer of data about financially motivated intrusion actors and was sentenced to 6 years in prison on high treason. On May 13, 2021, the Lefortovo Court of Moscow released Dokuchaev on parole.

Konstantin Kozlovsky

A first-person account, by Kozolvsky, of activity he conducted on behalf of the FSB via the Russian-language publication The Insider:

> *"Being engaged in computer technology, I communicated on numerous Internet forums. In 2008, I entered into a dialogue about vulnerabilities in email services. During the discussion, I started a dispute for $ 500. as a result of which I demonstrated the vulnerability using the example of one email, having posted the password for public viewing in the forum. Then I demanded money from the disputant, offering to meet. In the established place, 2 people approached me. Having determined that I am the person who hacked the mail, they showed me an FSB officer's ID and persistently asked me to get into the car.*
>
> *I was brought, as I later found out, to the courtyard of the FSB headquarters in the Sverdlovsk region (Yekaterinburg). I spent two days in a room 3 by 3 meters. No food was given. Only 2 times water in an aluminum bowl. A bucket was brought in to cope. FSB officers gave a choice: work with them or send them to prisons for hacking mail. I agreed by signing the paper.*
>
> *Over the years of cooperation, I have completed many assignments. Ilya is my curator (later at the trial he will indicate that he meant FSB officer Dmitry Dokuchaev. - editor's note) gave tasks and supervised me, supplied me with hardware and software. patronized in matters with law enforcement.*
>
> *In recent years, the focus has been on the servers in America and the EU. The instructions for hacking the National Committee of the Democratic Party of the United States, Hillary Clinton's correspondence, I successfully complete*d, transferring the data on the hard drive to the FSB officer Ilya (850 GB compressed with videos of the hacking)."

According to Kozlovsky, he worked for Dokuchaev and the FSB since 2008, when he was apprehended by the FSB for gaining unauthorized access to an email account, and that since 2008, he had performed numerous tasks for the agency. Kozlovsky also claims that the creation of the Lurk and WannaCry viruses were supervised by employees of FSB and that Dokuchaev and others with access to the viruses "could independently work with infected targets". Such a statement appears to undermine Kozlovsky's credibility or understanding of Russian state-sponsored operations, given that WannaCry is publicly attributed to North Korean nation-state threat actors.

In October 2020, Kozlovsky was released from the Matrosskaya Tishina prison in Moscow, though some of his activities, such as using internet and phone services, were restricted. Following his release, Kozlovsky traveled to Moscow, but on March 18, 2021, the Kirov District Court of Ekaterinburg repealed the decision and sent Kozlovsky back to the pre-trial detention center claiming that Kozlovsky is a flight risk. On March 29, 2021, during a court hearing Kozlovsky gave his wife a note which said that he is under "immense psychological pressure" and that he does not wish to commit suicide. A similar note was given to Kozlovsky's mother which noted he wants to live but might be killed. After Kozlovsky shared the notes with his family, he was transferred to the medical building of the pre-trial detention center for an evaluation. The results of the medical examination were not made public.

Pavel Vrublevsky

Pavel Vrublevsky (who also operated under the sobriquet "RedEye"), rose to prominence in the early 2000s as the co-creator of the online payment service ChronoPay. According to Vrublevsky in an interview with Recorded Future's The Record, ChronoPay was initially created to act as a payment gateway for several of his unspecified "entertainment projects", and later grew to include such partners[9] as "state-owned Rostelecom, Mosenergo, the Russian telecom operator MTS, and the Russian airline Transaero". Both Forbes and Russian-language media outlet TAdvisor[10] state that Vrublevsky worked closely with Leonid Terekhov, an alleged former member of the Russian military intelligence apparatus, the GRU (Main Intelligence Directorate).

In 2013, Vrublevsky was sentenced to 2 and a half years in prison for soliciting operators of a botnet to conduct a DDoS attack against a major ChronoPay competitor, Assist. The attack resulted in serious service disruption, preventing the Russian state-run airline, Aeroflot, from selling tickets "for several days, costing the company millions of dollars". Vrublevsky is also accused of having run a large spam botnet, Rx-Promotion, based on leaked ChronoPay emails "showing ChronoPay executives passing credentials to Rx-Promotion's administrative back end database".

Pavel Vrublevsky openly criticized Dokuchaev and his supervisor, Sergei Mikhailov, for harboring cybercriminals: "the whole crowd of hackers, including their curators, all together were essentially forum guys from the same forums: Exploit, Maza, and Zloy, which in turn seem to be stupidly owned by Dokuchaev." Pavel Vrublevsky continues: "Historically, not the smartest guys in uniform who earned money from these "themes" originate in the same forums and in the same communities that were supervised by Major Dokuchaev from the FSB CIB: Maza, Verified, Exploit."

Roman Seleznev

Seleznev operated carding forums, such as bulba[.]cc and Track2[.]name, until 2011, when he was a victim of a terrorist attack in Marrakesh, Morocco. The attack left Seleznev in a coma from which he recovered towards the end of 2012. The marketplace stopped operating a few months after Seleznev fell into a coma, citing a lack of new stolen material.

After recovering, Seleznev returned to carding, operating under the username "2Pac". He created another carder marketplace, this time allowing for other hackers to sell information on his platforms. He has also created a website, called POS Dumps, with the intention of teaching carding to new hackers. The website offered a step-by-step guide on how to commit credit card fraud, providing links for necessary tools.

Alexey Stroganov

In the 2003 arrest of the criminal ring, Stroganov was one of 3 key players, along with the ringleader Artur Lyashenko "Bigbuyer" and manager Gerasim Selivanov "Gabrik". Although Stroganov was sentenced to 6 years in prison in 2006, flint24 continued his criminal activities from behind bars and upon release in 2008, Stroganov had established a criminal distribution network for compromised credit card data.

While Stroganov appears to have maintained ties with government figures like Dengin for years without backlash, his public affiliation with President Putin's judo gym likely crossed a line. The motives and decision-making process behind Stroganov's second arrest are not public, but the timing of his award as a Turbostroitel board member followed by the FSB's unusual, high-profile cybercrime arrests on Stroganov's birthday indicates that his political overreach triggered a severe backlash from those close to the Russian president, resulting in Stroganov's second arrest.

[9] https://www.forbes[.]ru/forbes/issue/2014-11/270967-sex-drugs-and-rock-n-roll
[10] https://tadviser[.]com/index.php/Person:Vrublevsky_Pavel_Olegovich

In March 2020, the FSB arrested 30 members of a hacker ring. These members were scattered across 11 regions of Russia and included citizens of Ukraine and Lithuania. According to the Russian media, the hackers specialized in selling compromised debit and credit cards stolen from both Russian and foreign citizens. During the arrest, authorities uncovered over $1 million USD, 3 million rubles, gold bars, computers, servers that were used to host dark web marketplaces, counterfeit ID cards (including Russian passports and government IDs), and weapons. Alexey Stroganov was among the arrested hackers and was associated with the GoldenShop and BuyBest credit card shops. Stroganov's arrest has been officially confirmed by the Moscow General Judicial Court.

"My opinion is that there are only two options as to why they could have been taken now. First, they worked on Russian targets. Perhaps, they could not resist something "tasty" or did not control their partners, and as a result, working on .ru became a fact unpleasant for them. The second option - they violated an agreement with the FSB or refused to perform some important tasks, or the task, in general, went too far. These are all guesses, but I see no other reason", an unidentified hacker is quoted as saying in a conversation with Meduza.

Evgeny Nikulin

Open-source, Russian-language reporting cited Yegor Krasnoborov, 1 of Nikulin's purported associates, as suggesting that Nikulin was always interested in technology and computers. Krasnoborov claimed that the Russian government would be able to somehow rescue Nikulin, suggesting that the charges against the hacker are geopolitically motivated and that despite Nikulin being a highly skilled hacker capable of committing the intrusions, he was "not a member of any hacker groups and acted alone".

Yevgeniy Nikulin was convicted in July 2020 for the intrusions against LinkedIn, Formspring, and Dropbox. Later, on September 29, 2020, Nikulin was sentenced to 88 months in prison for breaching several technology firms, capping a drawn-out legal battle that has involved competing extradition attempts, luxury sports cars, and delays due to the coronavirus outbreak. According to the US Attorney for the Northern District of California David Anderson, "Nikulin's conviction is a warning to would-be hackers, wherever they may be. Computer hacking is not just a crime, it is a direct threat to the security and privacy of Americans. American law enforcement will respond to that threat regardless of where it originates".

Pyotr Levashov

Despite the seeming tongue-in-cheek postings in underground forums, Levashov was also known to align himself with, or openly support, Kremlin interests. In his 2019 book "Intrusion: A Brief History of Russian Hackers", Danil Turovsky indicated that in 2012, Levashov engaged in a campaign of harassment surrounding Russian presidential candidate Mikhail Prokhorov and in 2014, as the Russian government supported the conflict in Ukraine, Levashov offered 30% discounts to send spam to "Ukraine, the USA, nations in the EU and 'others who imposed sanctions'" on Russia.

In early April 2017, Levashov was arrested in Barcelona, Spain and the Kelihos botnet was seized. Levashov was subsequently indicted by the US District of Connecticut District Court. According to the DoJ, in September 2018, "Levashov entered into a guilty plea, thus admitting in open court to his criminal conduct and avoiding the need for a trial". Later in December 2018, the DoJ charged Levashov with "one count of causing intentional damage to a protected computer, one count of conspiracy, one count of accessing protected computers in furtherance of fraud, one count of wire fraud, one count of threatening to damage a protected computer, two counts of fraud in connection with email and one count of aggravated identity theft". During his extradition process from Spain, Levashov's wife Maria made claims that US law enforcement was questioning Levashov about his involvement with Russian nation-state cyber efforts against the West.

On July 20, 2021, a US judge sentenced Peter Levashov to 33 months, time served, and 3 years of supervised release for creating and operating Kelihos, 1 of the largest spam botnets that ever existed. The judge also ordered that Levashov would have his computer monitored during the supervised release to prevent the former malware coder from engaging in new illegal activities.

Evgeniy Bogachev

The GameOver Zeus activity was not the only financially motivated activity conducted by Bogachev. According to a 2014 DoJ indictment, he also operated Cryptolocker ransomware, which "infected more than 234,000 computers, with approximately half of those in the United States. One estimate indicates that more than $27 million in ransom payments were made in just the first two months since Cryptolocker emerged". As of this writing, it is unclear if Bogachev remains active in conducting financially motivated intrusion activity or what type of relationship, if any, he may maintain with the Russian government. At least 1 sensitive source has claimed Bogachev has been involved in financing Kremlin-backed disinformation efforts against the West.

Appendix B: Additional Sources

- September 27, 2016: Open-source reporting from The New York Times (NYT) suggesting that the Russian intelligence services employ Russian domestic infrastructure for hire in order to conduct targeted intrusions for espionage
- September 29, 2020: Report in The Record about Evgeny Nikulin's sentencing
- October 5, 2020: Interview on The Record with Pavel Vrublevsky
- May 5, 2021: Open-source reporting from TruSec further discussing the overlap between the Russian intelligence services and the cyber criminal ecosystem
- May 19, 2021: Open-source reporting from Meduza revealing that OPSEC errors in activity reveal links between cybercriminal elements and the Russian government
- August 4, 2021: Report in The Record discussing White House response to a BlackMatter interview conducted by Recorded Future analysts

Recorded Future Threat Activity Group and Malware Taxonomy

Recorded Future's research group, Insikt, tracks threat actors and their activity, focusing on state actors from China, Iran, Russia, and North Korea, as well as cybercriminals — individuals and groups — from Russia, CIS states, China, Iran, and Brazil. We emphasize tracking activity groups and where possible, attributing them to nation state government, organizations, or affiliate institutions.

Our coverage includes:

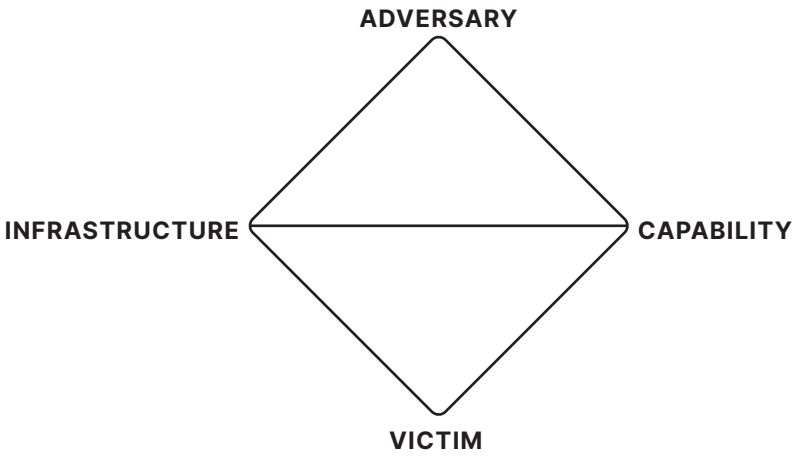
- Government organizations and intelligence agencies, their associated laboratories, partners, industry collaborators, proxy entities, and individual threat actors
- Recorded Future-identified, suspected nation-state activity groups, such as RedAlpha, RedBravo, Red Delta, and BlueAlpha and many other industry established groups
- Cybercriminal individuals and groups established and named by Recorded Future
- Newly emerging malware, as well as prolific, persistent commodity malware

Insikt Group publicly names a new threat activity group or campaign, such as RedFoxtrot, when analysts typically have data corresponding to at least three points on the Diamond Model of Intrusion Analysis with at least medium confidence. We will occasionally report on significant activity using a temporary activity clustering name such as TAG-21 where the activity is new and significant but doesn't map to existing groupings and hasn't yet graduated or merged into an established activity group. We tie this to a threat actor only when we can point to a handle, persona, person, or organization responsible. We will write about the activity as a campaign in the absence of this level of adversary data. We use the most widely used or recognized name for a particular group when the public body of empirical evidence is clear the activity corresponds to a known group.

Insikt Group uses a simple color and phonetic alphabet naming convention for new nation-state threat actor groups or campaigns. The color generally corresponds to that nation's flag colors, with more color/nation pairings to be added as we identify and attribute new threat actor groups associated with new nations.

For newly identified cybercriminal groups, Insikt Group uses a naming convention corresponding to the Greek alphabet. Where we have identified a criminal entity connected to a particular country, we will use the appropriate country color, and where that group may be tied to a specific government organization, tie it to that entity specifically.

Insikt Group uses mathematical terms when naming newly identified malware.



About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.