ANALYST1™

NATION STATE RANSOMWARE

Jon DiMaggio

August 11, 2021

@UseAnalyst1 analyst1.com

ANALYST1™

Contents

Introduction

In June 2016, criminals in Russia made about $7,500 a month conducting ransomware operations.[1] Today, attackers make millions of dollars from a single attack. Unfortunately, ransomware is getting worse, not better. Earlier this year, the Washington DC Police Department fell to a ransomware attacker who threatened to post sensitive data about informants and undercover officers — unless they agreed to pay a hefty ransom. Then in May, Russian-based hackers attacked Colonial Pipeline, which resulted in a fuel shortage across the United States' East Coast. Shortly thereafter, other Russian-based attackers crippled JBS: North America's largest meat processing company. As a direct result of the attack, JBS temporarily shut down nine meat processing plants across the United States. Both the financial and operational impact of these attacks have placed ransomware as one of the biggest threats to the United States national security.

Goals

Several criminals who run or participate in organized cybercrime have been named and charged for their offenses in US federal indictments. Despite the criminal charges, the Russian government protects the individuals behind the attacks and does not consider their ransomware attacks a crime as long as they do not target Russian organizations. We know the Russian government is allowing the attacks which raises the question, is Russia behind or someway supporting ransomware attacks? To learn more, we conducted research in an effort to:

1. Identify human relationships between ransomware criminals and the Russian government.
    a. This includes relatives, friends, employers, and criminal-related affiliations.
2. Identify technical associations between ransomware variants and malware attributed to the Russian government.
3. Identify any evidence linking organized cybercriminals who conduct ransomware attacks to espionage related activities and operations.

Key Findings

Based on the research detailed in the rest of this report, Analyst1 identified the following key findings:

- For the first reported time, we uncovered connections between two Russian intelligence directorates, the SVR and FSB — in collaboration with a Ransomware gang, working together to compromise US government affiliated organizations between October and December 2020.
- Multiple individuals who conduct ransomware attacks and are affiliated with Russian-based criminal organizations do in fact have alliances with the Russian government. The Russian Federal Security Service employed individuals responsible for running multiple criminal organizations. One group conducted ransomware attacks, while the other specialized in banking malware operations.
    - Additionally, these men have affiliations with other Russian criminal gangs behind recent ransomware attacks.
- Custom espionage malware, known as Sidoh, shares source code with Ryuk ransomware, which Russian cybercriminals have frequently used.
    - Sidoh uses keywords to find and steal government/military documents from the United States.
- Despite the code overlap with Ryuk ransomware, Analyst1 does not believe Wizard Spider developed or uses Sidoh malware. However, we do believe someone with access to Ryuk source code developed Sidoh to use for espionage purposes. It may also be a false flag, but the new code added on top of Ryuk was not developed by the same author behind other malware used by Wizard Spider.
    - Sidoh's creators also purposed it to target financial institutions searching for SWIFT and IBAN-related data. This could indicate a desire to target financial institutions. However, the malware is poorly developed, noisy, and false positive prone. Thankfully, all of these factors make it easier to detect and mitigate at this stage of its development.
- A number of ties already exist between the ransomware attacker EvilCorp and an espionage adversary known as SilverFish. These ties include targeting, infrastructure, tactics, and other relevant tools.

- Previously observed Russian-based espionage malware from 2011, we are calling Infostealer.GOZ, shared source code and was essentially a modified version of GameOver Zeus (GOZ). It has similar functionality (not shared code) to the newly discovered Sidoh malware.

ANALYST1

Ransomware Gangs and the Russian Government

Ransomware Gangs and the Russian Government

Typically, when researching cybercrimes, we focus mainly on the technical aspect of attacks. However, to investigate if and how the Russian government is associated with ransomware criminals, we spent a lot of time studying the human element behind the attacks. On their own, several of the events we discuss previously appeared in court documents, media articles, cybersecurity blogs, and information released by various governments. By putting all of the smaller events together and identifying the individuals, timeframes, and criminal events collectively, we formed a more detailed picture of how the Russian government and cybercriminals work together. Then, we went back and reviewed the cyberattacks, operations, and technical details surrounding the groups and individuals identified earlier in order to make our own assessment, which we will present later in this report.

Once our initial analysis was complete, we recognized that several secondary associations exist, involving other known ransomware groups. Since these associations are "one removed" from criminals who do associate or work for the Russian government, we documented each for context in the hope additional information becomes available in the future, shedding more light on the topic. To begin, we will discuss the associations between ransomware gangs, the individuals behind them, and the government entities they support, if known.

In 2007, Evgeniy Bogachev developed Zeus, a banking trojan, he first used in cyberattacks beginning later in that year. It would be many years before his identity was disclosed, but Bogachev was one of the most nefarious cybercriminals to date and at the time of this writing is still at large. Bogachev developed banking malware and relied on mass "spray and pray" phishing (spam) campaigns to deliver the banking trojan and infect victims. If a potential victim clicked on an attachment or link in the email, Zeus would embed itself into the victim's operating system. Once present, Zeus lays dormant, waiting for the victim to use their browser to access their online banking.

When the malware detects the victim's browser attempting to resolve a bank website, it "injects" a fraudulent web page displayed in the victim's browser. Since the victim intentionally browses to the banking website, they believe they are on the authentic bank login page. However, Zeus has a keylogger capability, which captures the victim's banking credentials as they authenticate their account. Once captured, Zeus sends the credentials to adversary-controlled infrastructure, at which point the attacker uses them to log in and drain the victim's funds.

In early 2009, Bogachev added new functionality to Zeus, allowing it to defeat dual authentication techniques intended to prevent attackers from gaining access to a victim's account if their password is compromised. To achieve this, Bogachev incorporated Jabber: an instant messaging technology that Zeus uses to transmit the victim's credentials. This includes the one-time password, which is captured and transmitted via Jabber as the user types it into their bank website. Since Jabber operates in near real-time, the attacker can use the one-time password before it expires and gain access to the victim's bank account. This is how Bogachev made his initial wealth.

Additionally, Bogachev added botnet functionality to Zeus, allowing members of the service to use it to introduce other malware into victim environments. With many lucrative and appealing features available at an affordable cost, Zeus became popular in the criminal underworld. However, after its initial success, Bogachev realized he needed additional support to handle managing Zeus operations. Initially, Bogachev worked with other successful cyber criminals, like the RockPhish and Avalanche gangs. He eventually formed his own crime ring though, which he named "The Business Club". Figure 1 shows the Business Club (2007 – 2014).

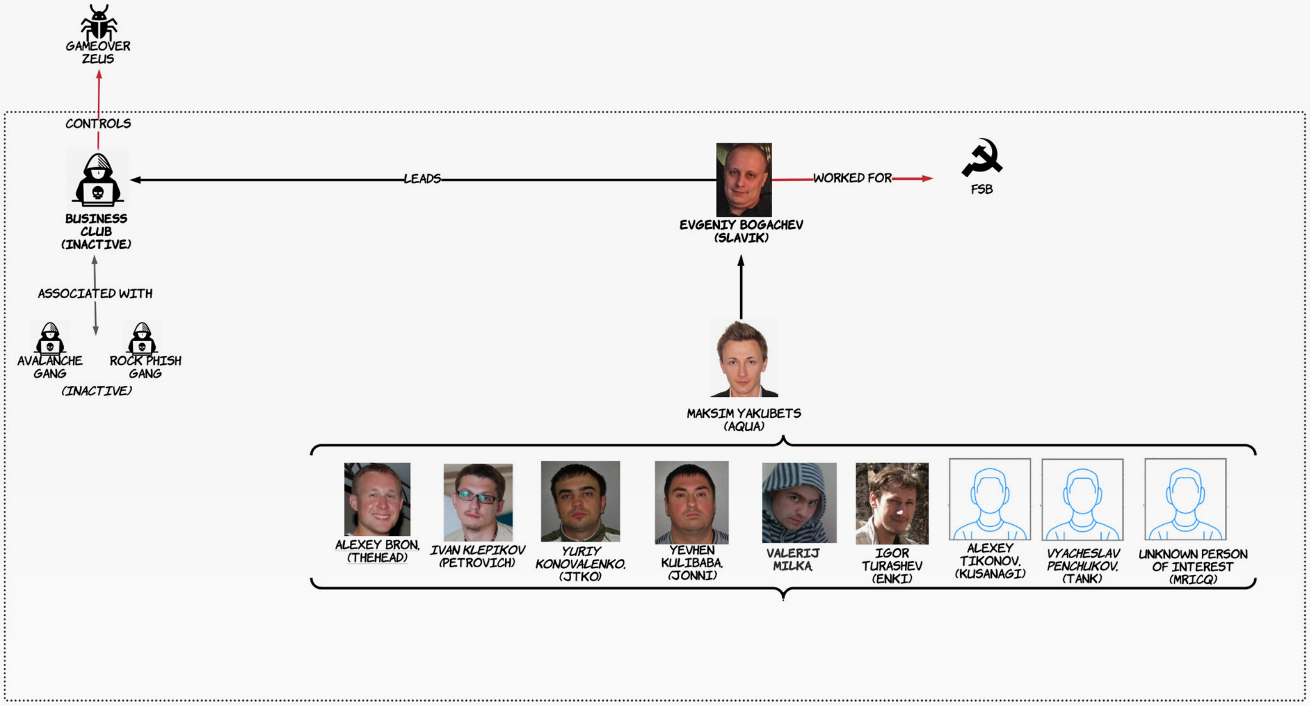


Figure 1: The Business Club and its members

The criminals affiliated with the Business Club reside in eastern Europe, primarily in Russia, the Ukraine, and Moldova. As stated earlier, Bogachev developed Zeus and played a major role in leading the group; however, until 2014, Bogachev was only known by his online monikers, “Slavik”, “Lucky 12345”, “Monstr” and others.[2]

Ironically, Bogachev’s online persona became publicly known through a criminal complaint filed in 2009 by a United States District Court in Nebraska, across the world from Anapa, Russia, where Bogachev allegedly lives. In the complaint, the FBI only knew Bogachev as “John Doe #1, also known as “lucky 12345”.[3] However, investigators identified a number of his Business Club affiliates by their actual names, giving way to the beginning of what would ultimately, years later, unravel Bogachev and his criminal empire.

Despite the indictment, Russia had no interest in working with the US to bring the criminals behind the attacks to justice.

Both United States and Ukrainian Law enforcement officials apprehended several of the named criminals in the indictment, but those based in Russia were untouchable. Despite the indictment, Russia had no interest in working with the US to bring the criminals behind the attacks to justice. Since no crimes took place against Russian organizations or its citizens, Russian law enforcement did not view their operation as a criminal act.

In addition to Bogachev, a second hacker named in the indictment as John DOE #2, who used the online handle “aqua”, would also be identified years later as a man named Maksim Yakubets, who also resides in Russia. We will discuss Yakubets in detail shortly, but as seen in the 2009 indictment, Yakubets played a strong role in organized cybercrime, even in the mid to late 2000s.

While the indictments affected the gang, its most significant impact was the disruption to the money mule network used by the gang to launder millions of dollars. Interestingly, it was not savvy criminals who made up the mule network but instead university students who likely did not realize the severity of what and who they were supporting. The Business Club used social media to identify and recruit students, primarily from Eastern Europe and eligible for J1 visas in the US. Once recruited, the Business Club issued fraudulent passports and other documentation necessary to obtain US bank accounts.[4]

While the arrests temporarily slowed down the gang, operations ultimately continued. Still, less than a year later, Bogachev made a statement online under his Slavik moniker announcing his retirement. As a going-away present, Bogachev developed what was initially known as Zeus 2.1. One notable addition to the new variant was an encryption key associated with each payload. Bogachev implemented the key so he could step away from organizing and executing attacks. Instead, using Zeus 2.1, he created a Malware as a Service (MaaS) model. He maintained the malware and infrastructure necessary for Zeus operations selling access to criminals in a pay-to-play business model, mapping the encryption key in each payload to customers of the service. By selling to criminals of his choice, known as affiliates, Bogachev minimized his exposure, in turn reducing the risk of arrest.

Bogachev and the FSB

In 2011, Bogachev made another bold move on his own. This time, not even his Business Club associates knew his plan. For reasons unknown at the time, Bogachev created a secret Zeus variant and supporting network. However, Bogachev made this version to accomplish a very different goal. Up to this point, Bogachev was a career criminal who used his abilities and resources for cybercrime geared towards financial gain. In his new initiative, however, Bogachev used Zeus for espionage purposes. Specifically, Bogachev designed the new version of Zeus malware to infect government and military targets, including intelligence agencies affiliated with Ukraine, Turkey, and Georgia.[5]

In addition to the change in targeting, Bogachev also added new functionality to Zeus. This new version used a predefined list of keywords, all of which are pertinent to government and military operations. Zeus would infect the victim system and search every directory for documents and communications containing any of the keywords. If found, Zeus exfiltrates the document out to attacker Command and Control (C&C) servers. Bogachev used the espionage version of Zeus in operations for several years. The obvious question is, why?

Our theory is Bogachev, the Business Club, and their banking malware operations drew too much attention to themselves. Once multinational law enforcement operations began investigating and making very public arrests, it likely attracted the Russian government's attention. As mentioned earlier, Russia has a history of leveraging organized crime to support its interests. Russia also has a vast technical network embedded across telecommunication systems throughout the country to monitor and spy on its citizens. If the US government could identify Bogachev, so could his own government. Once identified, Russia may have extorted Boagachev to support government cyber espionage operations. Bogachev might have faced imprisonment unless he agreed to cooperate. If this scenario is true, it explains why he created the espionage variant and why he would hide it from the rest of the world.

In May of 2014, the United States officially indicted Evgeniy Boagachev. For the first time, Bogachev was publicly named for his criminal activities with the Business Club. At the time of this writing, seven years after his indictment, Boachev is still living free, presumably in Russia. Despite pressure from the US, Russia refuses to cooperate in apprehending or extraditing Bogachev.

The Ukrainian Interior of Ministry, who assisted the FBI during the initial investigation into Bogachev, provided additional answers about Bogachev's relationship with the Russian government. According to the Ukrainian government, Bogachev was "working under the supervision of a special unit of the FSB".[6,7]

While Bogachev evaded prosecution, the Business Club and its banking malware operations ceased. However, though Bogachev's story ends here, his partners and associates in the Business Club began new operations. Under new leadership, the remaining criminal element called their criminal enterprise "EvilCorp".

EvilCorp

EvilCorp

Maksim Yakubets, Igor Turashev, and several other Russian and Ukrainian men began using Bugat (built from Zeus source code) banking malware in 2009 when they were still working in the Business Club. Bugat evolved, and its developers used its code to develop several other malware variants over time, Cridex and eventually Dridex. As the malware evolved, the men behind it transitioned from the Business Club to EvilCorp. EvilCorp's banking operations increasingly drew attention due to the large sums of money stolen with Dridex malware.

EvilCorp used mass spam campaigns to distribute Dridex, making it highly prevalent. With its widespread distribution, many banking consumers became victims, resulting in significant financial loss. This drew the attention of both law enforcement and security vendors who monitored the activity. The heightened awareness began to make it increasingly difficult for the operation to continue with the same success. As a result, EvilCorp shifted its efforts away from banking malware operations. Instead, they began using Dridex to gain initial access and deliver ransomware in enterprise attacks. The gang used various ransomware payloads early on. However, in Aug 2017, EvilCorp designed their own ransomware — Bitpaymer — which shared code with Dridex malware.[8] Since then, EvilCorp released several other variants: Wasted Locker, and most recently, Hades ransomware.

In December 2019, the United States Department of Justice released an indictment against Yakubets and another member of EvilCorp, Igor Turashev. The United States charged the men for their cyber-crimes and financial theft.[9]

Additionally, the US Treasury issued sanctions to freeze assets and restrict individuals and companies from conducting financial transactions with EvilCorp making it harder for the gang to collect ransom payments or purchase resources necessary for their operations. Furthermore, the US officially identified Yakubets as the Leader of EvilCorp:

> *"Today's action clarifies that, in addition to his involvement in financially motivated cybercrime, the group's leader, Maksim Yakubets, also provides direct assistance to the Russian government's malicious cyber efforts, highlighting the Russian government's enlistment of cybercriminals for its own malicious purposes."*
> *— US Treasury Department's Office of Foreign Assets Control (OFAC)*[10]

More importantly, OFAC identified Yakubets as an agent of the FSB. Interestingly, Yakubets father-in-law Eduard Bendersky is also a career FSB officer who oversees an

FSB veterans' association and manages "private security agencies that provide services to state-owned companies."[11,12,13] Additionally, in 2019, Mr. Bendersky allegedly assisted in the assassination of a "former Chechen rebel field commander, who had fought Russia in the Second Chechen War". Unfortunately, similar to the Bogachev situation, Russia protects EvilCorp and its members and does not recognize them as criminals, preventing them from being brought to justice.

In May 2020, EvilCorp attempted to circumvent the sanctions, preventing companies from paying their ransom, by rebranding their operation with new ransomware: Wasted Locker. They also adjusted their targeting, primarily infecting US companies. In June 2020, US endpoint protection company Symantec identified 30 companies that EvilCorp breached and was in the process of staging their ransomware payload. Clearly, they intended to cripple the organizations and collect a hefty ransom.[14] All but one of the companies were US-based organizations. This targeting change was likely retaliation against the US indictment along with the sanctions against Yakubets and EvilCorp.

Fortunately, due to code and design similarities, investigators quickly attributed Wasted Locker (and later Hades) back to EvilCorp. Another significant change EvilCorp made was in the ransom demand. Before the indictment, EvilCorp ransom payments were less than $500,000. After the indictment though, the gang began instructing victims to pay millions of dollars to regain access to their data. For example, EvilCorp demanded Garmin, a fitness technology company, pay $10 million to obtain the decryption key necessary to unlock their data.[15] The trend stuck, and other Ransomware gangs such as Twisted Spider, Viking Spider, and Revil began asking for similar amounts.

Until late fall of 2020, EvilCorp was one of the most sophisticated and active criminal elements in the ransomware game. However, things quickly changed. After the initial Wasted Locker campaign, something shifted within the gang, directly affecting their operations. In the summer of 2020, ransomware groups began to evolve and started using new, more advanced tactics. For example, most advanced ransomware gangs began to use data leak sites (DLS) to expose victims, leak data, and apply pressure. Additionally, gangs introduced tactics of copying and exfiltrating victim data, using it for a second ransom, and demanding payment in return for not selling or exposing the data publicly. EvilCorp, however, has not used either tactic, with one exception.

As we mentioned earlier, even if a victim wants to pay EvilCorp's ransom, US sanctions prevent them from making payment. Additionally, the US Office of Foreign Assets Control makes it illegal to send payment to any financial account associated with EvilCorp or its members.[16]

When EvilCorp failed to conceal themselves as the criminal element behind Wasted Locker, fewer victims could pay the ransom, even when they desired. Both ransom negotiators and cyber insurance firms began to refuse work involving EvilCorp attacks. Then, in the summer of 2021, EvilCorp attempted to hide behind the name and brand of another attacker: Babuk. Recently, the Babuk ransomware gang rebranded and registered a new data leak site — payload[.]bin — after receiving more attention than they preferred following a ransomware attack on the Washington DC Police Department.

To deceive victims into paying their ransom, EvilCorp rebranded their ransomware to deliver a ransom note onto infected computers named "PAYLOADBIN-README.txt" and appended the file extension "PAYLOADBIN" to the end of encrypted files on the victim system. EvilCorp used the PAYLOADBIN name to mimic Babuk's new payload[.]bin data leak website. However, unlike the real ransomware associated with the payloadbin data leak site, the faux EvilCorp version directed victims to make ransom payment arrangements by contacting one of two email addresses — "rickhood@armormail[.]net" or "meredithpatrick@protonmail[.]com" — but not through the payload[.]bin site. EvilCorp attempted to take advantage of the fact that most victims are not familiar with ransomware gangs' infrastructure or their ever-changing brand names. They expected victims would assume the attack was by another criminal gang, not EvilCorp, thus making it easier to pay the ransom and bypass the sanctions in place. Unfortunately for them, we (security researchers) stalk ransomware groups and their activities. Given that, even despite their fake branding attempt, we quickly noted that the ransomware was actually Wasted Locker/Hades at the binary level, which is unique to EvilCorp.[17,18]

While more than sanctions are necessary to prevent ransomware attacks, they have still forced EvilCorp to devote additional time and resources to their efforts. Arguably, the sanctions have slowed and decreased the number of successful attacks in which the gang is able to collect a ransom payment. Making things even stranger, while EvilCorp once dominated headlines with attacks for several years, they have significantly decreased their operations. They still conduct attacks, yet they are nowhere near as significant in the cybercrime space as they were previously. At this point, the obvious question is, where did they go?

The obvious question is, where did they go?

The SilverFish Espionage Campaign

In December 2020, reports began to surface detailing a major cyberespionage campaign geared to steal data such as documents and communications from government, military, defense contractors, and associated private sector companies. The espionage campaign began when the attacker compromised SolarWinds — a tech firm that provides software and network solutions designed to manage IT networks. In this case, adversaries targeted SolarWinds due to their large number of US government clients.

To gain access to SolarWinds customers, the attacker installed a backdoor into the SolarWinds software, which was in turn distributed to their customers. By conducting a supply chain attack, the downstream customers blindly installed the backdoor, providing remote access to the adversary. At this point, the attacker installed other hacktools and malware to obtain legitimate credentials, which they then used to identify and steal sensitive government information. In total, attackers compromised thousands of organizations through the SolarWinds breach.

There are several adversaries involved who took advantage of the vulnerabilities used in the attacks. However, shortly after discovering the breach, the US government attributed the attack to the Russian government. It also revealed that despite its identification in December 2020, the campaign originally began and has been ongoing since March 2020.[19,20]

In addition to our research at the time, in early 2021, several security vendors published their analyses and findings surrounding the attacks. We found two reports that provided insight relevant to our topic: ransomware and the Russian government. The first report, published by Prodaft, a cyber intelligence company, detailed how the attacker obtained access, what they did once present in victim environments, and how they utilized C&C to manage the operation.[21] More importantly, however, Prodaft noted several indicators used in the SilverFish espionage campaign, which EvilCorp previously used in ransomware attacks.

After the initial Prodaft report, Truesec, another cybersecurity company, shed more light on the correlation between the two groups.[22] First, TrueSec identified a target of an EvilCorp ransomware attack in October 2020 who fell victim to the SolarWinds (SilverFish) espionage campaign two months later, in December. Remember, when the US indicted Maksim Yakubets in 2019, the US Treasury placed sanctions against him and EvilCorp, and they also named him as an agent of the FSB. The previous US attribution, combined with both EvilCorp and SilverFish's attacks, makes a compelling story that fits together well.

To formulate our own assessment, we took details from the Prodaft and Truesec reports. Since both publications focus on specific areas of the operation, we had several information gaps in the attack chain events specific to enumerating the network, gaining administrative credentials, and staging the ransomware. To make the most accurate assessment possible and fill in the gaps, we used data from previously observed EvilCorp "on-network" operations. Doing so allowed us to form what we believe is an accurate account of the adversary's behavior and actions. While this method allowed us to formulate our analytical assessment of EvilCorp and SilverFish activities, please note that a margin of error could still exist. However, Analyst1 believes this method provides the most accurate picture possible, outside of having direct access to victim data from the specific incidents that the Truesec and Prodaft reports discuss. Using Figure 2, let's explore the ties across both operations.

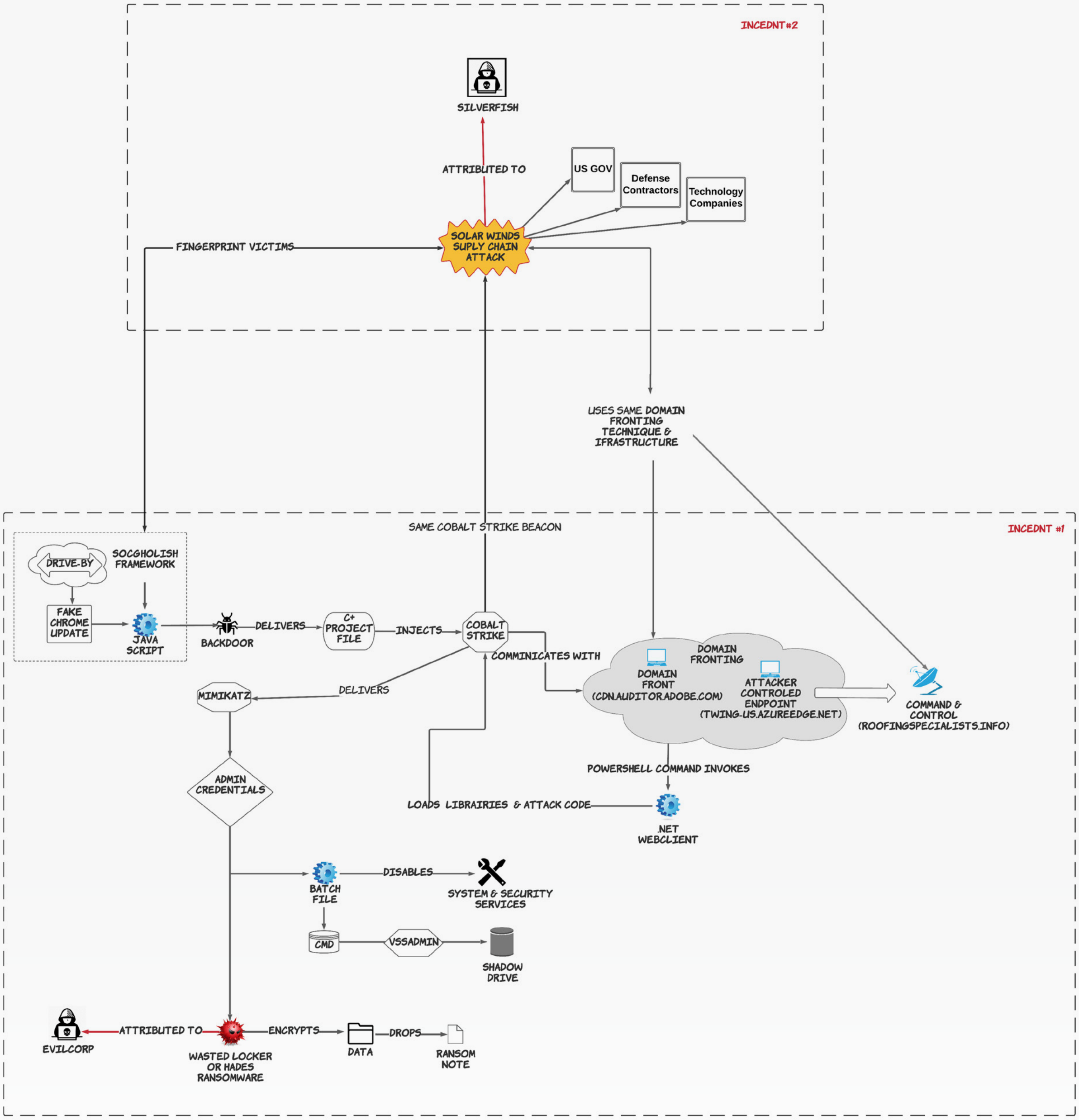


Figure 2: EvilCorp Attack chain detailing the overlap with the Silverish espionage group

Attach Chain Overlap

In the diagram above and in the associated details below, we detail EvilCorp's attack chain. We labeled it as Incident #1 in Figure 2. Furthermore, we call out the phases from Incident #1 (which overlap with Incident #2, the SilverFish espionage campaign) below:

1. Attacker breaches victim security initially via a "drive-by" attack derived from the SocGholish framework.
   a. Here, attackers use SocGhoulish to fingerprint systems in the SilverFish espionage attack on the same victim. Note the connection to Incident 2
2. As a result of the drive-by attack, a java script file installs a backdoor.
3. The backdoor then runs a script that injects code on the victim system.
4. The code executes in memory on the victim system to compile CobaltStrike, which facilitates the rest of the attack.
5. CobaltStrike beacons to Command & Control, masking its activity by using a domain fronting technique, acting as a proxy leveraging legitimate content delivery network (CDN) domains to deceive defenders and downloads attacker code and additional libraries.
   a. SilverFish uses the exact same CobaltStrike Beacon two months after EvilCorp used it in an attack on the same victim. – Incident 2
   b. SilverFish uses the same domain-fronting technique and exact infrastructure previously used by EvilCorp on the same victim –Incident 2
   c. The domain "roofingspecialists.info" used as EvilCorp Command & Control infrastructure in Incident #1, also delivers SilverFish malware to the same victim-Incident #2.– Incident 2
6. From here, the attacker installs Mimikatz and uses it to obtain admin credentials.
7. Once the attacker has administrative privileges, they use their access to distribute a Batch file (using PSExec and PowerShell) to systems throughout the environment. The Batch file then disables system and security services present on systems within the victim environment.
8. Next, EvilCorp issues a vssadmin command to delete shadow copies on the victim systems, thereby preventing them from using recovery features to restore data.
9. Finally, the ransom payload disperses throughout the environment, encrypting victim data and delivering the ransom note.

As you can see, several ties exist between EvilCorp and SilverFish activity such as infrastructure, tools, and the tactics they use. Yet, it is important to note that indicator and tool overlap are not strong enough to attribute EvilCorp to SilverFish definitively. Nevertheless, it is also too compelling to ignore. SilverFish could have intentionally reused EvilCorp's infrastructure and tools to throw off investigators. However, the

Russian Intelligence association made by the US concerning both the SolarWinds attacker (Silverfish) and Evilcorp (Yakubets) makes this a far more solid theory when combined with the evidence.

Russian Intelligence Ties

According to the United States Cybersecurity & Infrastructure Security Agency (CISA) and the White House, the Russian Foreign Intelligence Service (SVR) is behind the SolarWinds initiated espionage campaign.[23,24] Unlike its government and military counterparts, the SVR does not disrupt or sabotage its targets; but instead, it focuses on remaining hidden and present on the victim infrastructure. By gaining and maintaining a presence within their adversaries' infrastructure, the SVR attempts to create a long-term collection capability. Here, they continue to steadily monitor the victims and gather intelligence that they disseminate to other Russian directorates and units such as the FSB and the Main Directorate of the General Staff (GRU).

This SVR attribution presents an issue with the theory that Yakubets (and in turn EvilCorp) is or supports the SilverFish espionage group. If you recall, the United States maintains their contention that Yakubets is an agent of the FSB. Therefore, if SilverFish is a unit of the SVR, then Yakubets/EvilCorp are unlikely to be behind the attack. However, we believe two intelligence directorates worked together to compromise the United States government — not just one. Next, we discuss our theory that explains EvilCorp's engagement in the SVR's operations.

Previously, the SVR worked in conjunction with other intelligence directorates, such as the GRU. In the attack against the United States Democratic National Committee (DNC), the SVR, which security vendors knew as "Cozy Bear", breached and gained initial access to the DNC. After securing and fortifying access to the target, GRU Unit 26165, known as "Fancy Bear", used custom backdoors and exploits to target high-profile DNC-related servers and individuals to steal data. They would later use this in an attempt to disrupt the 2016 United States Presidential election. A classified Russian report surfaced in 2021, providing further evidence that Russia intended to influence the US population in the 2016 election in a longer-term campaign. In the operation, Russia hoped to divide the United States and cause the population to distrust its government.[25]

According to the report, Putin met with leadership from Russian intelligence directorates such as the FSB, SVR and the GRU to discuss the operation. Putin himself approved the campaign, which arguably was successful based on the divide in the United States existing today. At the time, the media and general public discussed this topic, but no proof existed until years later. We feel this is similar to how Russia uses ransomware gangs in its mission to disrupt and influence the United States today.

While this is only one example, it still demonstrates the various responsibilities and working relationships between Russian intelligence agencies. Based on this information, Analyst1 believes the FSB worked in conjunction with the SVR on a joint mission to compromise the United States government. This explains both the attribution made by the United States regarding the SolarWinds attacks and its attribution of Yakubets' involvement with the FSB in relation to the attack's details. Additionally, this demonstrates not only how Russian intelligence organizations work together, but also how Russia uses ransomware gangs to advance their offensive cyber capabilities against foreign targets.

Sidoh Espionage Malware

Sidoh Espionage Malware

In our last whitepaper, Ransom Mafia — Analysis of the World's First Ransomware Cartel, we profiled Wizard Spider, a notorious ransomware gang behind attacks against JBS food processing services, HSE Healthcare, the City of Tulsa, and hundreds of other organizations since they began operations in 2018. Currently, the gang runs two operations leveraging Conti and Ryuk ransomware variants. Additionally, the gang has a large arsenal of supporting malware that Wizard Spider uses to breach and compromise victims.

Interestingly, Wizard Spider malware and ransomware have historical ties with Dyre and Hermes malware. Both have their own stories and interesting attribution theories behind them, which is out of scope for the purpose of this report. However, Wizard Spider used code from each to develop and evolve the resources it uses today. Figure 3 shows many of the malware resources Wizard Spider utilizes in their attacks.

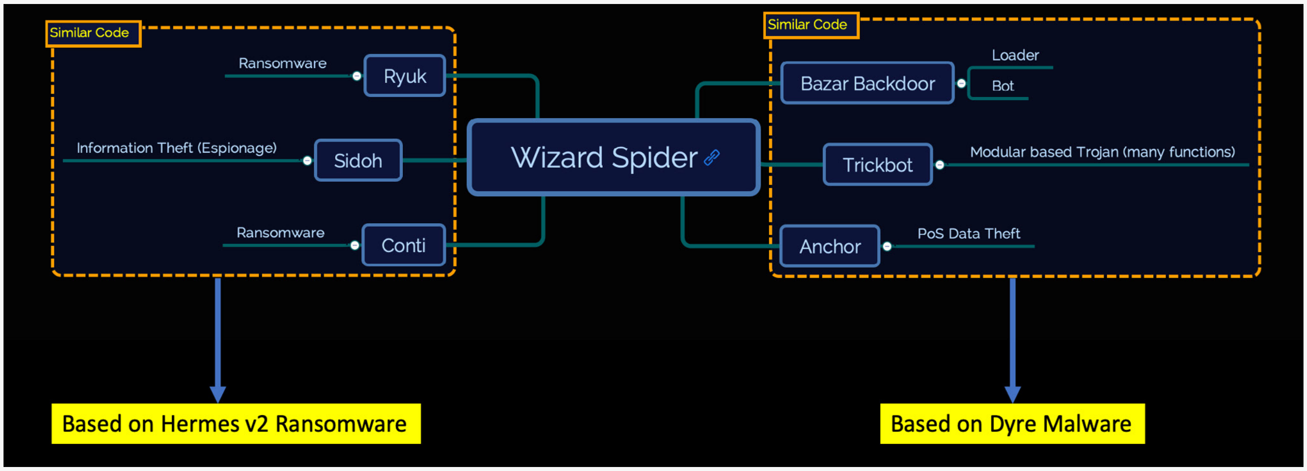


Figure 3: Wizard Spider malware

***Note:** Conti shares code similarities with Ryuk, so we included it in the Hermes section of Figure 7. However, to clarify, Ryuk is specifically based on Hermesv2 and the other families shown share similarities with Ryuk, in turn linking back to Hermesv2 through their Ryuk code association.*

While our previous research discussed each variant shown in Figure 3, at that time, we had little first-hand knowledge of the information-stealing malware known as Sidoh. This espionage malware especially stands out since it is allegedly built with Ryuk ransomware source code. Next, we will discuss our findings based on evidence discovered in our research to assess Wizard Spider's level of involvement, if any, with espionage operations. We researched and analyzed Sidoh to answer the following questions:

1. What does Sidoh do, and how?
2. What infrastructure does Sidoh communicate with?
3. How is Sidoh similar/different from Ryuk ransomware?
4. What is Wizard Spider's level of involvement, if any, with the Russian government?

We analyzed multiple ransomware samples and identified a suspicious file present in a malware repository. At this point, we then analyzed the sample and determined that it was a malicious binary designed to steal information, and that it shared code unique to Ryuk ransomware. The code overlap with Ryuk also explains why signatures mistakenly detect it as ransomware. To expand the dataset we used to derive our findings, we used the initial binary discovery to write Yara rules (found in Appendix B), which then identified five similar samples. Table 1 displays the SHA2 hashes and C&C of each sample.

Sha2	CompileTime	C&C
a8c4703fab7d2548701523b4c215d7cb57d337cc243046647bda18d4e6690853	2020-01-18 23:44:40	66.42.108.141
		45.76.1.57
c64269a64b64b20108df89c4f1a415936c9d9923f8761d0667aa8492aa057acb	2019-08-18 19:45:35	66.42.76.46
		185.254.121.15
cc4a0b4080844e20fb9535679f7b09a3e2449729ce1815d1e5a64272b0225465	2019-07-17 12:12:37	66.42.76.46
		185.254.121.157
6f06e5a8bdf983ec73177ef63ea053d391b46915a7dd1fbd0ddea5c70471f593	2019-07-11 22:26:03	185.254.121.157
		109.236.92.162
e6762cb7d09cd90d5469e3c3bfc3b47979cd67aa06c06e893015a87b0348c32c	2019-07-08 17:21:37	185.254.121.157
		109.236.92.162
a1ce52437252001b56c9ccd2d2da46240dc38db8074a5ed39a396e8c8e387fc2	2019-06-22 03:37:21	185.254.121.157
		109.236.92.162

Table 1: Sidoh sample details

Take note of the CompileTime for each sample. The developer compiled all but one during the summer of 2019. While each sample is slightly different, we found that the overall functionality remains the same: to identify files of interest based on preselected keywords and exfiltrate the data to adversary-controlled infrastructure. Next, we analyzed the Sidoh samples. In comparison to traditional Ryuk ransomware, Sidoh has three primary differences in its functionality:

1. Sidoh uses unique strings (keywords) to search victim systems for files to collect.
2. Sidoh uses File Transfer Protocol (FTP) to exfiltrate data from the victim machine.
3. Sidoh has no encryption routine and does not lock/encrypt files for ransom or drop a ransom note.

Sidoh uses a list of search variables (represented in ASCII and Unicode) to determine which files it collects for transmission. Table 2 is the list of keywords Sidoh uses to identify data of interest:

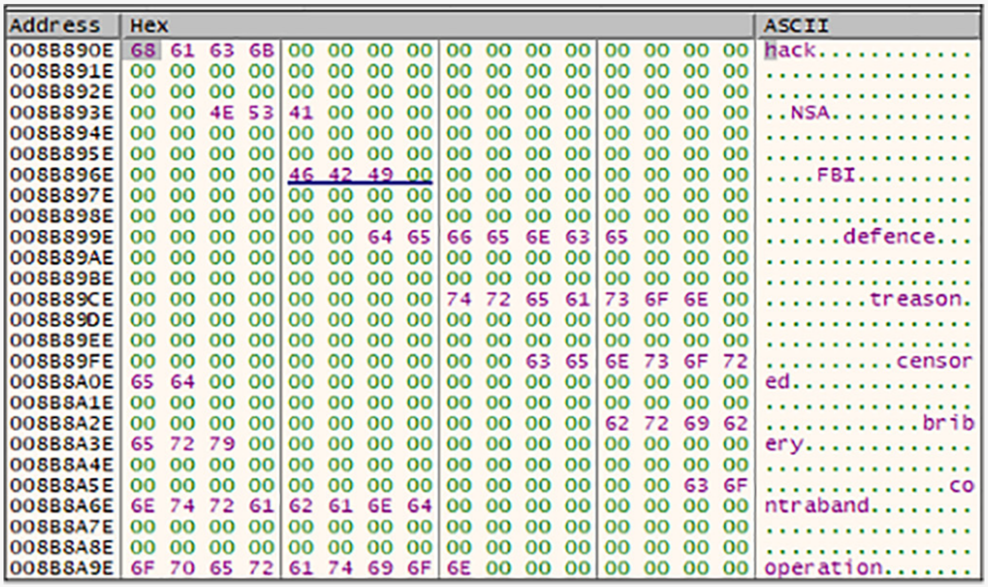
Sidoh Keywords		
personal	secret	backdoorundercover
securityN-CSR10-SBEDGAR spy radaragentnewswire	balance	investigation
marketwired	statement	passport
defence	checking	victim
treason	saving	Olivia
censored	routing	SECURITY
bribery	finance	newswire
contraband	agreement	convictMilitary
operation	license	Submarinesecret
attack	NSA	treasonrestricted
military	FBI	important
convict	Compilation	undercover
scheme	report	federal
tactical	confident	bureau
Engeneering	hidden	government
explosive	clandestine	unclassified
traitor	illegal	Clearance
suspect	compromate	letter
document	privacy	William

Sidoh Keywords		
embeddedspy	private	Isabella
submarine	contract	Sophia
restricted	concealed	hack

Table 2: Search strings Sidoh uses to identify data of interest

We use the keyword list to help determine the motive behind its use. Based on the keywords searched, the developer of Sidoh is interested in data associated with government, military, and diplomatic targets. Once executed, Sidoh loads the strings into memory and searches for their presence in filenames and content.

Below in Figure 4 you can see several of the keywords which Sidoh searched for in the victim's system upon execution:



```
Address   Hex                                              ASCII
008B890E  68 61 63 6B 00 00 00 00 00 00 00 00 00 00 00 00  hack............
008B891E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B892E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B893E  00 00 4E 53 41 00 00 00 00 00 00 00 00 00 00 00  ..NSA...........
008B894E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B895E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B896E  00 00 00 00 46 42 49 00 00 00 00 00 00 00 00 00  ....FBI.........
008B897E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B898E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B899E  00 00 00 00 00 00 64 65 66 65 6E 63 65 00 00 00  ......defence...
008B89AE  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B89BE  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B89CE  00 00 00 00 00 00 00 00 74 72 65 61 73 6F 6E 00  ........treason.
008B89DE  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B89EE  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B89FE  00 00 00 00 00 00 00 00 00 00 63 65 6E 73 6F 72  ..........censor
008B8A0E  65 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ed..............
008B8A1E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B8A2E  00 00 00 00 00 00 00 00 00 00 00 00 62 72 69 62  ............brib
008B8A3E  65 72 79 00 00 00 00 00 00 00 00 00 00 00 00 00  ery.............
008B8A4E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B8A5E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 63 6F  ..............co
008B8A6E  6E 74 72 61 62 61 6E 64 00 00 00 00 00 00 00 00  ntraband........
008B8A7E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B8A8E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008B8A9E  6F 70 65 72 61 74 69 6F 6E 00 00 00 00 00 00 00  operation.......
```

Figure 4: Hex view of Sidoh Strings used to search data on the victim system

However, several of the keywords left us puzzled as to their intended use. For example, the names "William", "Isabella", and "Sophia" seem out of place with the overall keyword theme. We also noted financial/banking related terms Sidoh searches for such as "balance", "statement", "checking", "saving", "routing", and "finance". It would make sense to see banking terms, since all known Wizard Spider operations to date have been for financial gain. However, they only make up a small percentage of the keywords, and the volume of government-related terms makes it clear that Sidoh is geared towards espionage — not financial gain.

Another strange design aspect to note is that Sidoh does not search directory paths for the keywords. If data is in the directory "C:\Users\(User_Name)\Documents\ Secret_NSA_Documents", Sidoh would not identify and collect it unless this data specifically had one of the terms present. To us, this seems like an oversight: it would be simple to include this function and make the malware more effective.

Our biggest surprise yet is an odd one regarding Sidoh's functionality: it searches for the terms "document" and "Microsoft"! We do not know what benefit the attacker gains by collecting data that includes these terms. Here, the attacker identifies and collects every victim file with the name "Microsoft" (which, of course, is present across the operating system) alongside data with the term "document". Additionally, attackers also collect all the Microsoft Event TraceLog Files (ETL) in C:/ProgramData and many configuration/ log files within each user's home directory. All of this makes the entire Sidoh operation extremely noisy, and this adds a massive amount of erroneous data that the attacker must sort through.

Finally, to facilitate the exfiltration, Sidoh uses the FTP protocol, which transmits in clear text and is noisy, increasing the risk of detection. Conducting exfiltration in this manner made us suspicious. If you are not familiar with Wizard Spider, realize they are an advanced adversary with many resources, and that they have an arsenal of custom-developed malware that, unlike Sidoh, is sophisticated and stealthy. Sidoh functions and tactic seems out of place given Wizard Spider's modus operandi.

Sidoh Evaluation

Analyst1 strongly believes that Wizard Spider *did not develop* Sidoh espionage malware. Instead, we feel it is more likely that a person or government entity obtained Ryuk source code and then did a terrible job of repurposing it as espionage malware. As the author of this research, I have primarily spent my career focusing on Nation-State attacks geared toward espionage, until transitioning to ransomware several years ago. I have rarely seen government-grade espionage malware designed this poorly.

Analyst1 strongly believes that Wizard Spider did not develop Sidoh espionage malware

Simply put, Sidoh is noisy, sloppy, and false-positive prone. Wizard Spider is an elite attacker, and none of the details we discussed fit their profile. Perhaps, the Russian government obtained Ryuk source code using the threat of imprisonment, or perhaps Russia used government resources to steal it. It is also plausible that Sidoh's developer created it to use as a false flag, intentionally populating it into public malware repositories to confuse and deceive researchers and investigators. We do not know exactly, but we strongly believe Wizard Spider *did not develop it*. Furthermore, if they did not create Sidoh, it explains why no one has seen Sidoh used in a Wizard Spider attack.

While we do not believe Wizard Spider created Sidoh, *someone* still did. For what it's worth, it shares similar keywords seen in the espionage version of GameOver Zeus. Still, we do not know who created it. It is also important to note that while it may be noisy and poorly developed, it works for its intended purpose: to find and steal documents from the United States Government.

Assessment

Assessment

To this point, we have provided the history of cybercriminals' roles and responsibilities along with the history of the Russian Government exploiting them. Each piece of the puzzle provides a unique view into their operation, but the picture becomes clearer when pieced together. Our assessment in Figure 5 shows several potential links connecting the Russian Government to prominent Russia based cybercriminal gangs."

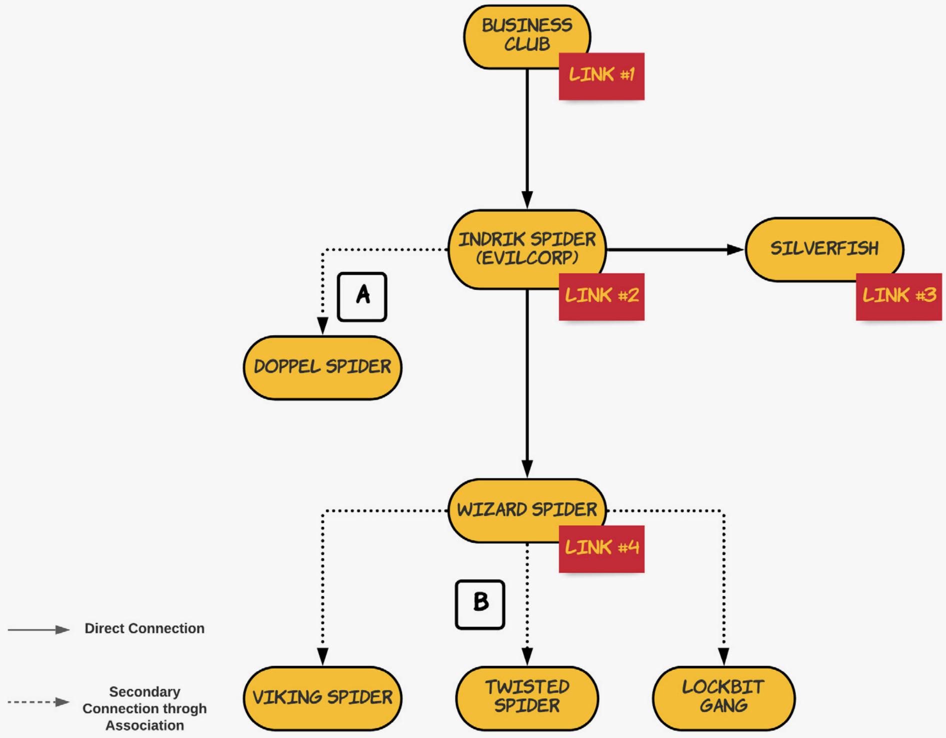


Figure 5: Ransomware links to the Russian governement diagram

**A detailed version of the above diagram is provided in the Appendix A of this white paper*

Link #1:

- Evgeniy Bogachev — the former leader of the now defunct criminal enterprise the Business Club — worked for the FSB since at least 2011. Bogachev supported Russian intelligence using his criminal network, custom malware, and cyber means.[26]
    - Bogachev created a modified version of GameOver Zeus malware to support espionage operations for the FSB targeting government, military and diplomatic

targets in Georgia, Ukraine, and other countries of Russian interest. Bogachev kept the work hidden from his Business Club criminal associates.[27,28]

- In addition to its re-purposed espionage use, Bogachev hosted a malware as a service network via the Business Club, banking malware, and ransomware operations.

Figure 6 is a visual representation of Link #1:

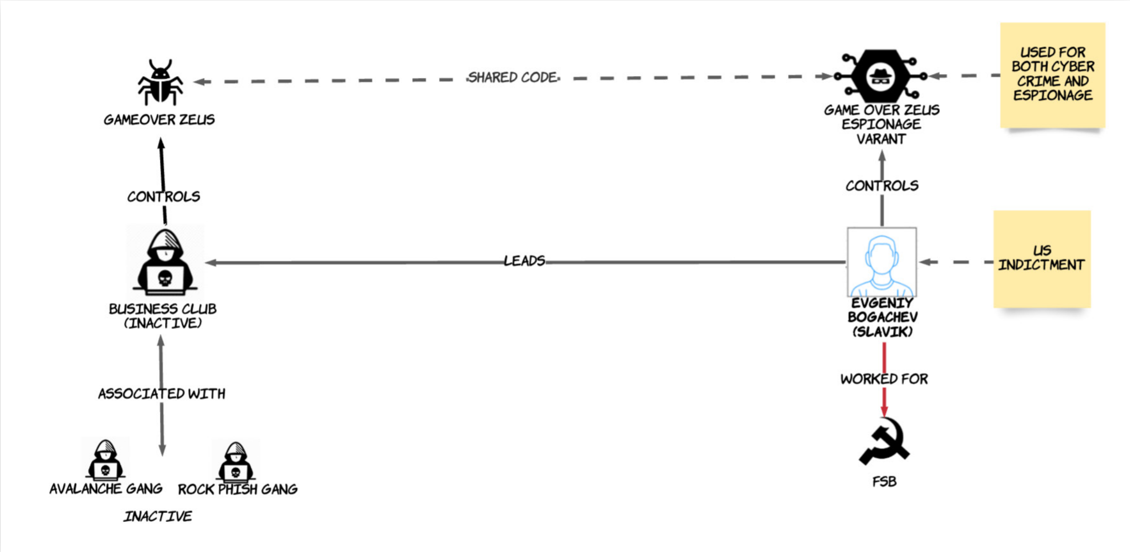


Figure 6: Business Club diagram associated with Link #1

Link #2:

- In June 2014, a multinational law-enforcement taskforce took down GameOver Zeus infrastructure, disrupting the Business Club's malware as a service operation.
  - Shortly after the takedown, a new criminal banking operation began—these attacks centered around malware known as Dridex. Dridex is banking malware based on GameOver Zeus, and it shares a similar structure, such as its P2P network design and features.[29] Like GameOver Zeus, Dridex began as banking malware, but criminals eventually began using it in enterprise ransomware attacks.
- The Business Club dissolved, and the United States indicted Evgeniy Bogachev for his cybercrime operations involving GameOver Zeus. Despite the indictment, he remains free today. However, Maksim Yakubets, another senior member of the Business Club and close associate of Evgeniy Bogachev, took leadership of the Business Clubs' former empire. In doing so, he established a new gang: EvilCorp.

- It is unclear if Bogachev's direct association with the Russian government led to recruiting Yakubets, but in 2017 Russia's main intelligence directorate, the FSB, hired Maksim Yakubets. Here, they hired him to support Russian State intelligence through cyber-espionage operations. It is likely that Yakubets uses his criminal network and the access it provides to benefit the FSB.[30]

Figure 7 is a visual representation displaying the associations discussed in Link #2:

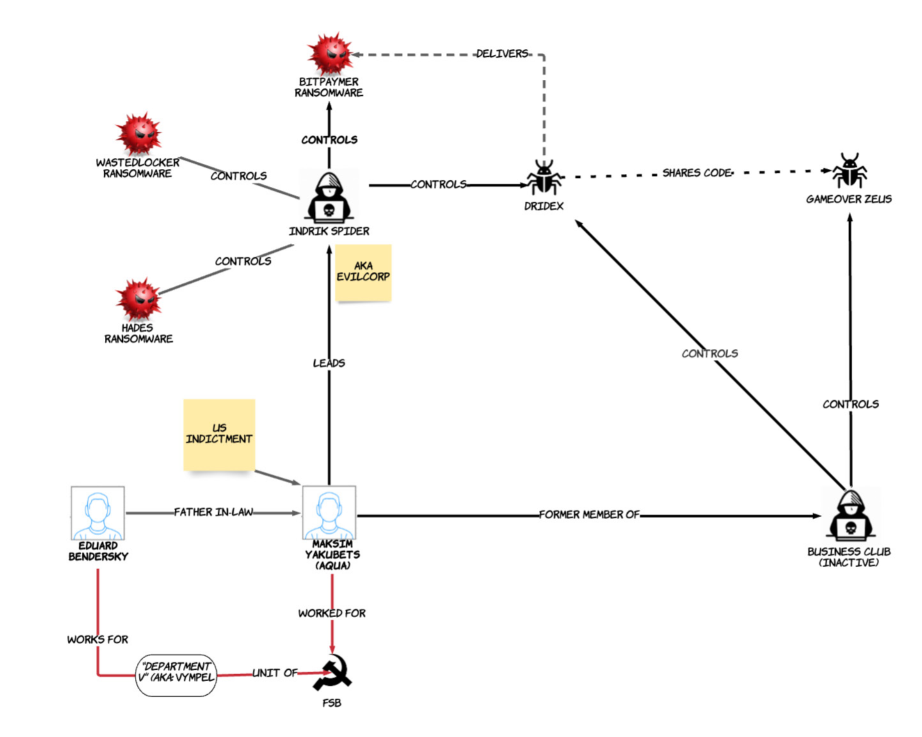


Figure 7: Detailed view of Link #2 centering around EvilCorp and Maksim Yakubets

Link #3:

- SilverFish, a Russian attributed espionage attacker, used C&C infrastructure previously seen in an EvilCorp ransomware attack against the same victim organization within a few months of one another.[31,32]
    - In the attack, both EvilCorp and later SilverFish use the same unique CobaltStrike Beacon.
    - The Beacon from both attackers used a domain fronting technique with the same legitimate Content Network Delivery (CND) domains and downloaded the identical PowerShell script in both attacks from the same C&C server.

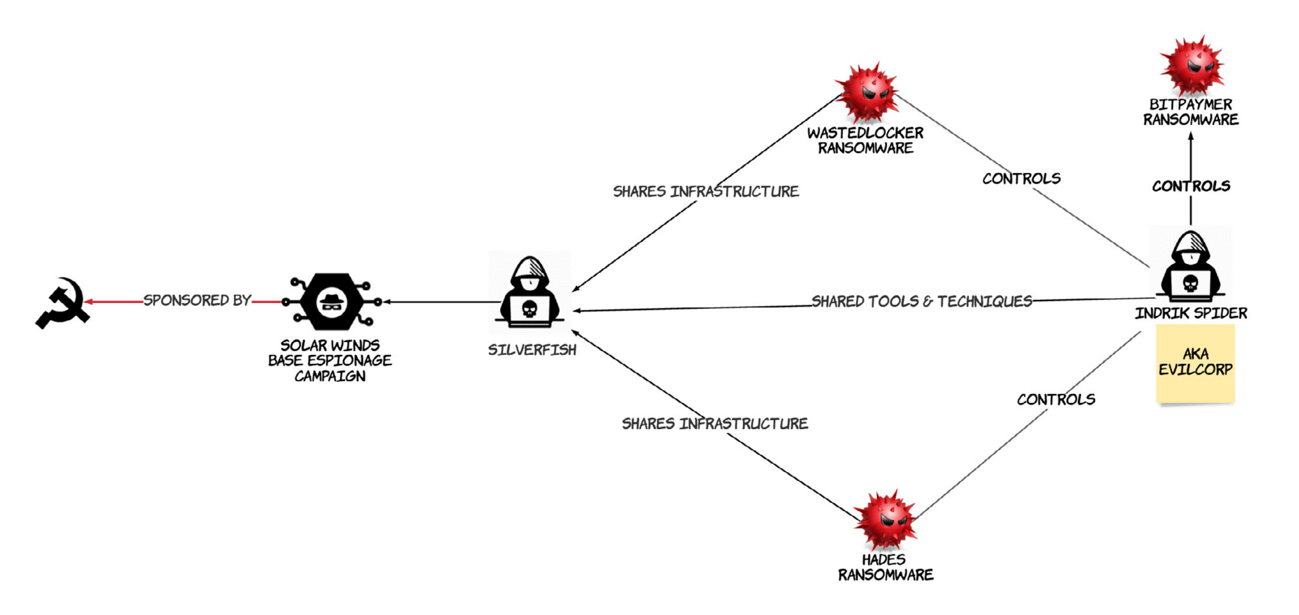


Figure 8: Detailed diagram of Link #3 involving EvilCorp and SilverFish attackers

Link #4:

- Another Russian-based cybercrime gang, Wizard Spider, may associate with EvilCorp. Wizard Spider is one of the longest-running and most experienced ransomware gangs operating today. Wizard Spider currently runs both Conti and Ryuk ransomware operations, and the gang controls or has exclusive access to the developer of Trickbot. While Trickbot is highly prevalent, it is controlled and managed by a central entity. Given this link, Analyst1 believes this controlling entity is likely Wizard Spider.

- EvilCorp and Wizard Spider previously used Trickbot malware to deliver their respective ransomware payloads — those being Bitpaymer/EvilCorp and Ryuk/Wizard Spider, respectively. The shared use of Trickbot indicates that a relationship may exist between EvilCorp and Wizard Spider.

- In 2019, someone began developing espionage malware based on the source code used in Ryuk ransomware. The malware, called "Sidoh", searches for keywords, such as classification markings and others related to government and military content. Sidoh's keywords and search functions are similar to infostealer.GOZ, which the Business Club developed. No other similarities or code use exist between the two.

- Analyst1 felt that too many inconsistencies exist between Sidoh and other Wizard Spider malware. Sidoh is noisy and false positive prone. As stated in our earlier review of the activity, Sidoh simply does not fit with the Wizard Spider's historical operations, malware, or behaviors.

- Sidoh is either developed by someone who acquired Ryuk source code, or it was created as a false flag to throw us off. It is not a product of Wizard Spider.

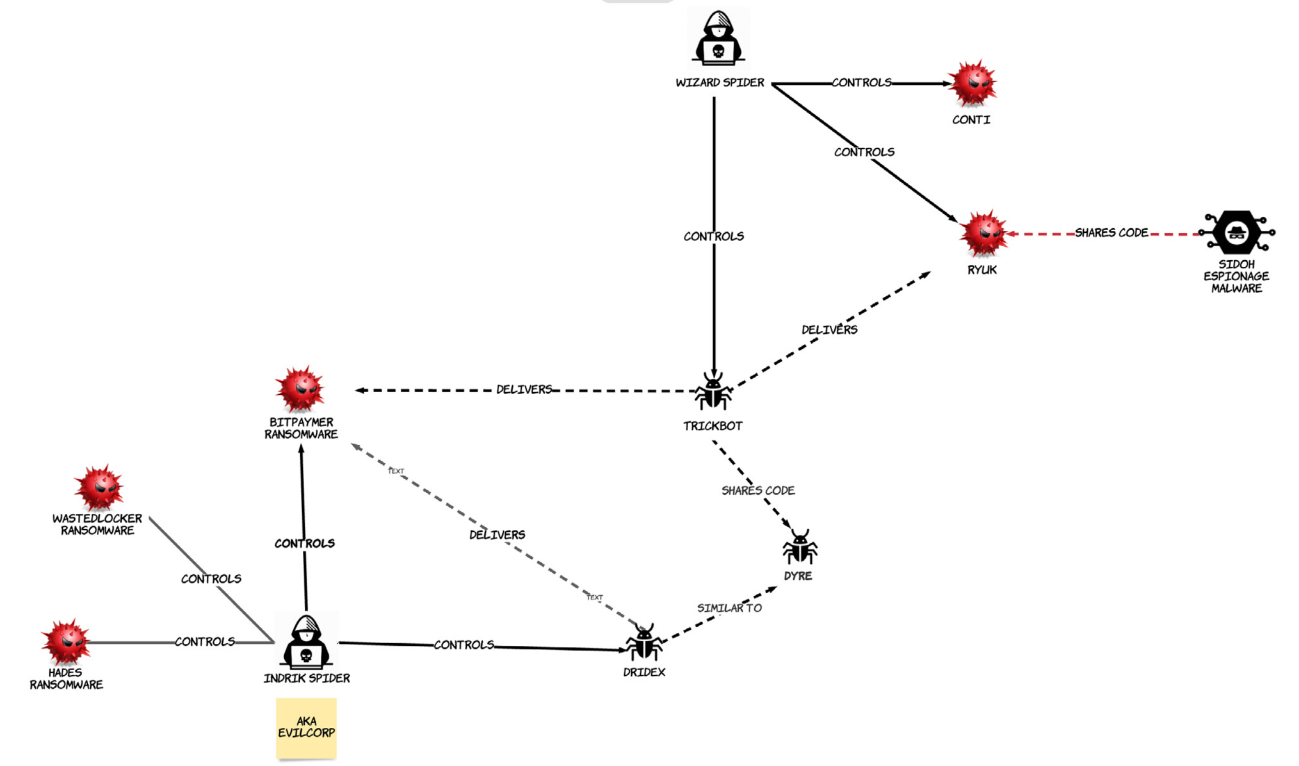


Figure 9: Detailed view of Link #4 involving Sidoh espionage malware

Secondary Links Through Association

The following links do not directly connect the gangs discussed with the Russian government. Instead, they provide context to other ransomware gangs affiliated with the groups and individuals that the Russian government has access to.

- **Link A:** EvilCorp developed Dridex malware (Link #2), which they controlled and used in operations for several years. They used the Dridex source code to develop Bitpaymer ransomware. DoppelPaymer, another ransomware variant, also shares source code with Dridex, and in turn, Bitpaymer. Dridex source code is not publicly available and closely held by EvilCorp indicating a close relationship likely exists between the two groups.
- **Link B:** Wizard Spider (Link #4) is associated with several other Russian-based ransomware gangs, Twisted Spider, Viking Spider, and the Lockbit Gang. Together they began a fictitious propaganda campaign engineered to make the general public believe that the groups joined forces to create a criminal Cartel. Based on our previous research, Analyst1 believes the gangs shared resources and communicated with one another, however we do not believe an actual Cartel exists.[33]

Conclusion

Conclusion

If you lived on the East coast of the United States in May 2021, you remember visiting gas stations searching for fuel. Unfortunately, what we found instead were "out of gas" signs. News stories discussed the worst-case scenarios causing outages of police and emergency services. Fortunately, the panic was short-lived, and Colonial Pipeline, with the help of the US government, restored services before that scenario became a reality. Yet, the panic and disruption did not fit the typical pattern seen from criminal activity. However, it did fit the modus operandi of a Russian government attacker.

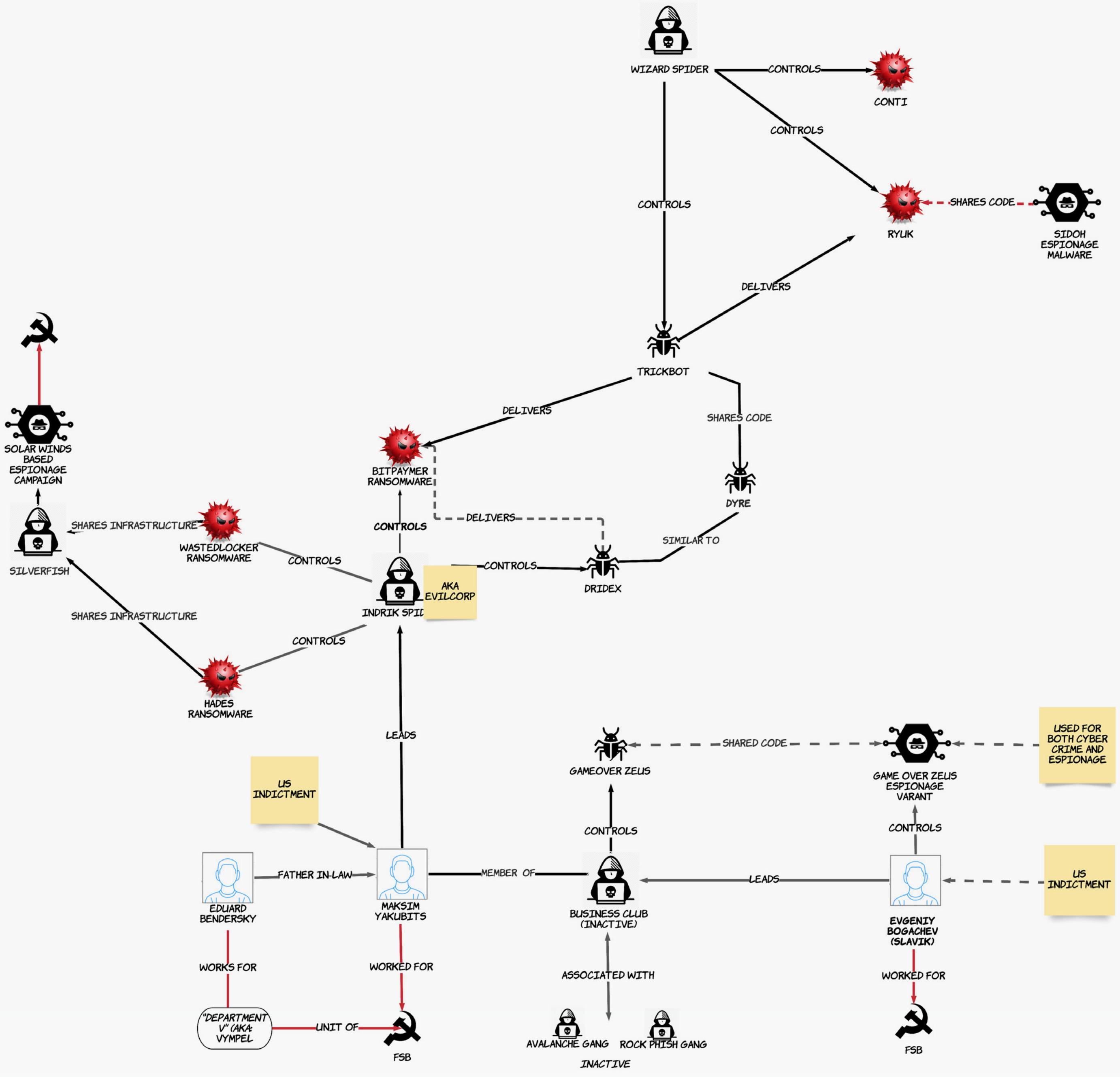
While the story fits, and it is easy for us to blame Russia, behavioral analysis and profiling are not enough to pin the activity on an individual, let alone an entire government. Based on this, Analyst1 wanted to review all information available to access activity from Russian-based ransomware attackers to see where the evidence led us.

It was important to fairly and accurately assess the situation. We began by reviewing all publicly available information on the topic, such as court documents, security blogs, and media reports. Then we identified, collected, and analyzed malware samples. Afterward, we reviewed "on network" activity involving Russian-based ransomware gangs. We looked for evidence and overlap with espionage activity and signs of any relationship with government organizations.

After conducting this assessment, Analyst1 strongly believes the Russian government uses its power to influence and benefit from the sophisticated criminals operating within their country. Russia uses cyber gangs and their technical skills as weapons against foreign targets. Using ransomware criminals to play a role in a much larger politically-driven operation allows Russia to strike its adversary while claiming no part in their actions.

Analyst1 will continue to monitor and research both ransomware activity and state-sponsored threats. As we identify and analyze new information, Analyst1 will provide updates on our research. We hope the information found in this paper will encourage researchers and security companies to continue searching for evidence to publicly expose the Russian government for its role in ransomware activities against foreign targets.

Appendix A:
Detailed Association Diagram



Appendix B: Sidoh Yara Rules

```
rule ransomware_sidoh_analyst1_core_001

{
meta:
  author = “Analyst1”
  date = “2021-07-04”
  version = “1”
  description = “Detection for Sidoh Malware based on 5 samples with RyukReadMe
   Strings”
strings:
  $s1 = “RyukReadMe” fullword wide
  $s2 = { 49 73 44 65 62 75 67 67 65 72 50 72 65 73 65 6e 74 }
  $s3 = { 47 65 74 49 70 4e 65 74 54 61 62 6c 65 }
  $s4 = { 46 69 6e 64 46 69 72 73 74 46 69 6c 65 }
  $s5 = { 46 69 6e 64 4e 65 78 74 46 69 6c 65 }
  $s6 = { 56 69 72 74 75 61 6c 41 6c 6c 6f 63 }
  $s7 = { 49 6e 74 65 72 6e 65 74 4f 70 65 6e }
  $s8 = { 46 74 70 50 75 74 46 69 6c 65 }

condition:
  all of them
  and (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550)
}

rule ransomware_sidoh_analyst1_core_002
{
meta:
  author = “Analyst1”
  date = “2021-07-11”
  version = “2”
  description = “Detection for Sidoh Malware based on 5 samples”
strings:
  $s1 = “RyukReadMe” fullword wide
  $s2 = “UNIQUE_ID_DO_NOT_REMOVE” fullword wide
  $s3 = { 49 73 44 65 62 75 67 67 65 72 50 72 65 73 65 6e 74 }
  $s4 = { 47 65 74 49 70 4e 65 74 54 61 62 6c 65 }
  $s5 = { 43 6f 6d 6d 61 6e 64 4c 69 6e 65 54 6f 41 72 67 76 }
  $s6 = { 46 69 6e 64 4e 65 78 74 46 69 6c 65 }
  $s7 = { 46 69 6e 64 46 69 72 73 74 46 69 6c 65 }
  $s8 = { 47 65 74 43 75 72 72 65 6e 74 54 68 72 65 61 64 49 64 }
  $s9 = { 46 74 70 50 75 74 46 69 6c 65 }
  $s10 = { 47 65 74 4c 6f 67 69 63 61 6c 44 72 69 76 65 73 }
  $s11 = { 47 65 74 50 72 6f 63 65 73 73 48 65 61 70 }
  $s12 = { 53 6c 65 65 70 }
  $s13 = { 57 72 69 74 65 46 69 6c 65 }
  $s14 = { 47 65 74 4c 61 73 74 45 72 72 6f 72 }
  $s15 = { 4d 75 6c 74 69 42 79 74 65 54 6f 57 69 64 65 43 68 61 72 }
  $s16 = { 45 6e 74 65 72 43 72 69 74 69 63 61 6c 53 65 63 74 69 6f 6e }
  $s17 = { 49 6e 74 65 72 6e 65 74 4f 70 65 6e }

condition:
  ($s1 or $s2) and (12 of ($s3,$s4,$s5,$s6,$s7,$s8,$s9,$s10,$s11,$s12,$s13,$s14,$s15,$s16
    ,$s17))
  and (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550)
}

rule ransomware_sidoh_analyst1_companion_001
{
meta:
  author = “Analyst1”
  date = “2021-07-11”
  version = “1”
  description = “Strict Detection for Sidoh Malware Unique Stings based on 6
    samples”

strings:
  $s1 = “RyukReadMe” fullword wide
  $s2 = “UNIQUE_ID_DO_NOT_REMOVE” fullword wide
  $s3 = “backdoorundercover” fullword ascii
  $s4 = “marketwired” fullword wide
  $s5 = “compromate” fullword ascii
  $s6 = “clandestine” fullword wide
  $s7 = “investigation” fullword wide
  $s8 = “concealed” fullword wide
  $s9 = “wallet.dat” fullword wide
  $s10 = “undercover” fullword wide
  $s11 = “spy” fullword ascii
  $s12 = “newswire” fullword wide
  $s13 = “anonymous” fullword wide

condition:
  ($s1 or $s2) and ( all of ($s2,$s3,$s4,$s5,$s6,$s7,$s8,$s9,$s10,$s11,$s12,$s13))
  and (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550)
}

rule ransomware_sidoh_analyst1_companion_002
{
meta:
  author = “Analyst1”
  date = “2021-07-11”
  version = “1”
  description = “Loose Detection for Sidoh Malware Unique Stings based on 6
    samples”

strings:
  $s1 = “RyukReadMe” fullword wide
  $s2 = “UNIQUE_ID_DO_NOT_REMOVE” fullword wide
  $s3 = “undercover” fullword wide
  $s4 = “PerfLogs” fullword wide
  $s5 = “spy” fullword ascii
  $s6 = “newswire” fullword wide
  $s7 = “investigation” fullword wide
  $s8 = “concealed” fullword wide
  $s9 = “backdoorundercover” fullword ascii
  $s10 = “marketwired” fullword wide
  $s11 = “compromate” fullword ascii
  $s12 = “clandestine” fullword wide
  $s13 = “SECURITYN-CSR10-SBEDGAR spy radaragentnewswire” fullword wide
  $s14 = “securityN-CSR10-SBEDGAR spy radaragentnewswire” fullword ascii
  $s15 = “wallet.dat” fullword wide
  $s16 = “anonymous” fullword wide
  $s17 = “explosive” fullword wide
  $s18 = “submarine” fullword wide

condition:
  ($s1 or $s2) and ( 7 of ($s2,$s3,$s4,$s5,$s6,$s7,$s8,$s9,$s10,$s11,$s12,$s13,$s14,$s15,
   $s16,$s17,$s18))
  and (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550)
}
```

Appendix C: IOCs

Sidoh SHA2:

a8c4703fab7d2548701523b4c215d7cb57d337cc243046647bda18d4e6690853

c64269a64b64b20108df89c4f1a415936c9d9923f8761d0667aa8492aa057acb

cc4a0b4080844e20fb9535679f7b09a3e2449729ce1815d1e5a64272b0225465

6f06e5a8bdf983ec73177ef63ea053d391b46915a7dd1fbd0ddea5c70471f593

e6762cb7d09cd90d5469e3c3bfc3b47979cd67aa06c06e893015a87b0348c32c

a1ce52437252001b56c9ccd2d2da46240dc38db8074a5ed39a396e8c8e387fc2

Infrastructure used by Sidoh espionage malware (FTP):

66.42.108.141

45.76.1.57

66.42.76.46

185.254.121.157

109.236.92.162

EvilCorp C&C:

Roofingspecialists[.]info

Endnotes

1. Szoldra, Paul. “Hackers Are Making $7500 per Month by Holding People’s Data Hostage.” Business Insider. Accessed July 28, 2021. https://www.businessinsider.com/flashpoint-report-ransomware-2016-6.

2. United States of America v. Evgeniy Bogachev (Clerk US District Court - West Dist. of Pennsylvania May 19, 2014).

3. United States of America v. Vyacheslav Penchukov, Ivan Viktorvich Klepikov, Alexey Dmitrievich Bron, Alexey Tikonov, Yehven Kulibaba, Yuriy Konovalenko, John Doe 1, John Doe 2, and John Doe 3. Accessed July 28, 2021.

4. Zetter, Kim. “U.S. Charges 37 Alleged Mules and Others in Online Bank Fraud Scheme.” Wired, September 30, 2010. https://www.wired.com/2010/09/zeus-botnet-ring/.

5. Sandee, Michael, Tillmann Werner, and Elliott Peterson. “Gameover Zeus – Bad Guys and Backends,” August 5, 2015, 53.

6. Atlantic Council. “Russia: It’s Not Just Putin,” September 13, 2017. https://www.atlanticcouncil.org/blogs/ukrainealert/how-to-understand-russia-today/.

7. “Inside the Hunt for Russia’s Most Notorious Hacker.” Wired. Accessed July 29, 2021. https://www.wired.com/2017/03/russian-hacker-spy-botnet/.

8. “The Malware Dridex: Origins and Uses.” Threat Report. TLP: White. Agence Nationale de la Securite des Systemes d’Information, July 17, 2020. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf.

9. “Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of ‘Bugat’ Malware,” December 5, 2019. https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens.

10. U.S. Department of the Treasury. “Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware.” Accessed July 29, 2021. https://home.treasury.gov/news/press-releases/sm845.

11. “Opinion | New Revelations Depict a Russian-Sponsored Assassination on German Soil.” Washington Post. Accessed July 29, 2021. https://www.washingtonpost.com/opinions/global-opinions/new-revelations-depict-a-russian-sponsored-assassination-on-german-soil/2020/02/23/af9ff1e6-5366-11ea-9e47-59804be1dcfb_story.html

12. The FSB’s Personal hackers how EVIL Corp, the world’s most Powerful Hacking COLLECTIVE, takes advantage of its deep family ties in the Russian intelligence community. Meduza. (2019, December 12). https://meduza.io/en/feature/2019/12/12/the-fsb-s-personal-hackers.

13. Dobrynin, S., & Krutov, M. (2019, December 11). In lavish wedding Photos, clues to an Alleged Russian CYBERTHIEF’S FSB family ties. RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/in-lavish-wedding-photos-clues-to-an-alleged-russian-cyberthief-fsb-family-ties/30320440.htm

14. “WastedLocker: Symantec Identifies Wave of Attacks Against U.S. Organizations.” Accessed July 29, 2021. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us.

15. “The Garmin Hack Was a Warning | WIRED.” Accessed July 29, 2021. https://www.wired.com/story/garmin-ransomware-hack-warning/.

16. U.S. Department of the Treasury. “Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal

Group Behind Dridex Malware." Accessed July 29, 2021. https://home.treasury.gov/news/press-releases/sm845.

17. "Behavioral Report." Accessed July 29, 2021. https://tria.ge/210606-s6arabmc1x/behavioral2#report.

18. Fabian Wosar. "Looks like EvilCorp Is Trying to Pass off as Babuk This Time. As Babuk Releases Their PayloadBin Leak Portal, EvilCorp Rebrands WastedLocker Once Again as PayloadBin in an Attempt to Trick Victims into Violating OFAC Regulations. Sample: Https://Virustotal.Com/Gui/File/69775389eb0207fec3a3f5649a0ad9315856c810f595c086ac49d68cdbc1d136/Details." Tweet. @fwosar (blog), June 5, 2021. https://twitter.com/fwosar/status/1401110845820747797.

19. Supply Chain Compromise. "Supply Chain Compromise | CISA." Accessed July 29, 2021. https://www.cisa.gov/supply-chain-compromise.

20. McMillan, Dustin Volz and Robert. "Suspected Russian Hack Said to Have Gone Undetected for Months." Wall Street Journal, December 15, 2020, sec. US. https://www.wsj.com/articles/suspected-russian-hack-said-to-have-gone-undetected-for-months-11607974376.

21. "SilverFish Group Threat Actor Report." Threat Report. TLP: White. USTA Prodaft, March 17, 2021. https://www.prodaft.com/m/reports/SilverFish_TLPWHITE_v2.pdf.

22. Wåhlén, Mattias. "Are The Notorious Cyber Criminals Evil Corp Actually Russian Spies?" TRUESEC Blog, May 5, 2021. https://blog.truesec.com/2021/05/05/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies/.

23. The White House. "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," April 15, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

24. "Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise." Fact Sheet. Cybersecurity & Infrastructure Security Agency, May 2021. https://us-cert.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR_Activities_Related_to_SolarWinds_Compromise_508C.pdf.

25. Harding, Luke, Julian Borger, and Dan Sabbagh. "Kremlin Papers Appear to Show Putin's Plot to Put Trump in White House." the Guardian, July 15, 2021. http://www.theguardian.com/world/2021/jul/15/kremlin-papers-appear-to-show-putins-plot-to-put-trump-in-white-house.

26. United States of America v. Evgeniy Bogachev (Clerk US District Court - West Dist. of Pennsylvania May 19, 2014).

27. Intelligence, Counter Threat Unit Threat. "Evolution of the GOLD EVERGREEN Threat Group," May 15, 2017. https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group.

28. Sandee, Michael, Tillmann Werner, and Elliott Peterson. "Gameover Zeus – Bad Guys and Backends," August 5, 2015, 53.

29. Stone-Gross, Brett. "The Lifecycle of Peer to Peer (Gameover) ZeuS." The Lifecycle of Peer to Peer (Gameover) ZeuS. Accessed July 29, 2021. https://www.secureworks.com/research/the-lifecycle-of-peer-to-peer-gameover-zeus.

30. U.S. Department of the Treasury. "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware." Accessed July 29, 2021. https://home.treasury.gov/news/press-releases/sm845.

31. Wåhlén, Mattias. "Are The Notorious Cyber Criminals Evil Corp Actually Russian Spies?" TRUESEC Blog, May 5, 2021. https://blog.truesec.com/2021/05/05/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies/.

32. "[SILVERFISH] Global Cyber Espionage Campaign Case Report - PRODAFT." Accessed July 29, 2021.

https://prodaft.com/resource/detail/silverfish-global-cyber-espionage-campaign-case-report.

33. DiMaggio, Jon. “RANSOM MAFIA. ANALYSIS OF THE WORLD’S FIRST RANSOMWARE CARTEL,” April 7, 2021, 58.

ABOUT AUTHOR:

Jon DiMaggio, Chief Security Strategist

Jon DiMaggio is a Senior Threat Intelligence Analyst and has over 14 years of experience. He possesses advanced expertise in identifying, tracking, and analyzing Advanced Persistent Threats (APTs). Additionally, Jon speaks at national level conferences such as RSA and BlackHat. He conducts interviews based on his research with media organizations such as Fox, CNN, Bloomberg, Reuters, Wired magazine, and several others.

ABOUT US:

Analyst1, engineered by cyber threat analysts, offers an enterprise-scale platform that operationalizes threat intelligence and enables security teams and analysts to focus on deeper analysis and response. With **Analyst1**, organizations gain visibility into advanced persistent threats attempting to infiltrate their networks.

@UseAnalyst1 **analyst1.com/blog**

NO WARRANTY . The technical information is being delivered to you as is and Analyst1 makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Analyst1 reserves the right to make changes without prior notice.