# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Goals</td>
<td>3</td>
</tr>
<tr>
<td>Executive Overview</td>
<td>4</td>
</tr>
<tr>
<td>The Prequel: REvil's Origin Story</td>
<td>7</td>
</tr>
<tr>
<td>Affiliate Recruitment</td>
<td>10</td>
</tr>
<tr>
<td>Part I: REvil Awakens</td>
<td>13</td>
</tr>
<tr>
<td>REvil Operations 2019</td>
<td>15</td>
</tr>
<tr>
<td>REvil Operations 2020</td>
<td>19</td>
</tr>
<tr>
<td>Part II: REvil Advances</td>
<td>23</td>
</tr>
<tr>
<td>Part III: Give Yourself to the DarkSide</td>
<td>28</td>
</tr>
<tr>
<td>DarkSide's Blunder</td>
<td>28</td>
</tr>
<tr>
<td>The Double-Cross</td>
<td>31</td>
</tr>
<tr>
<td>Part IV: Good vs. REvil</td>
<td>34</td>
</tr>
<tr>
<td>Part V: Deliver Us from REvil</td>
<td>38</td>
</tr>
<tr>
<td>Faces of REvil</td>
<td>43</td>
</tr>
<tr>
<td>Assessment: Beyond Good and REvil</td>
<td>48</td>
</tr>
<tr>
<td>Impact</td>
<td>48</td>
</tr>
<tr>
<td>Conclusion</td>
<td>54</td>
</tr>
<tr>
<td>Endnotes</td>
<td>62</td>
</tr>
</tbody>
</table>
Introduction

In our previous research we investigated a ransom cartel, and then we conducted a study on ransomware gangs and their links to Russian intelligence organizations. Now, we are conducting a use case into one of the world’s most notorious ransomware gangs, REvil. This particular case is fascinating because the gang has existed for several years, conducted many high-profile attacks, inspired several spin-off gangs, and in the end, caused major turmoil among partnering hackers who supported them. While many researchers and media organizations have produced reports on REvil, most of the accounts detail specific attacks, telling only part of REvil’s story. The purpose of this white paper is to provide a “big picture” assessment of the REvil crime organization by presenting a “cradle to grave” evaluation of actors behind it and their operations over time. Additionally, there are lessons we can learn from a criminal organization that, for the most part, had success where others failed. Overall, we think REvil presents an opportunity for analysts and defenders to learn from.

Goals

Analyst1 conducted research to address the following goals:

1. Show an inside view of REvil, their affiliates, and the “human” side of their operation through their own words and actions within the underground criminal community.

2. Profile REvil, their significant events, and the impact each event caused.

3. Identify REvil affiliates and detail how they integrate and operate within ransomware operations.

4. Identify areas of success and failure which eventually led to REvil’s demise and how it impacted the ransomware community.
Executive Overview

The REvil gang is an organized criminal enterprise based primarily out of Russia that runs a Ransomware as a Service (RaaS) operation. The core members of the gang reside and operate out of Russia. REvil leverages hackers for hire, known as affiliates, to conduct the breach, steal victim data, delete backups, and infect victim systems with ransomware for a share of the profits. Affiliates primarily stem across eastern Europe, though a small percentage operate outside that region. In return, the core gang maintains and provides the ransomware payload, hosts the victim data leak/auction site, facilitates victim communication and payment services, and distributes the decryption key. In simpler terms, the core gang are the service provider and persona behind the operation, while the affiliates are the hired muscle facilitating attacks.

REvil is known for its high-profile attacks. The attacks range from Grubman Shire Meiselas & Sacks, an entertainment law firm associated with many celebrities and political figures, from then-President Donald Trump to Kaseya, a Managed Service Provider which REvil leveraged to compromise nearly 1,500 companies, among many others. These are only two of many high-profile victims attacked by REvil over the lifetime of their activity. Like many ransomware attackers, in addition to encrypting their target’s data, REvil often stole and copied victim data to further extort the target. If the victim refused to pay, REvil leaked or sold their data to other criminals.

Nevertheless, while it is clear REvil savored the spotlight, their greed led to their downfall. In July of 2021, as a direct result of the Kaseya attack, the United States government began taking action against REvil. REvil’s actions eventually led to discussions between two of the most powerful leaders in the world, resulting in US federal indictments and arrests of REvil members by Russian authorities. Yet the most significant cause leading to REvil’s downfall resulted from their own actions when they betrayed the criminal community which supported them.

In the rest of this white paper, we detail REvil’s origin story, significant events, and the dramatic twists and turns from one of the most interesting criminal stories we have seen to date. Then, we provide a detailed assessment showing the impact to the ransomware community after both the US and Russian governments acted against REvil.

Based on the analysis and research presented in this white paper, we have two significant findings which affect the ransomware community:
1. The United States will likely never prosecute REvil or other Russian-based ransomware criminals in their own court of law. However, US actions have psychologically impacted the Russian ransomware community and directly affected their criminal operations.

2. Ransomware groups are changing their day-to-day operating procedures and have new significant concerns about their operational security due to recent interference of government and law enforcement agencies. Analyst1 identified evidence demonstrating recent actions against the REvil crime ring that caused distrust and paranoia, directly affecting key players in the ransomware community.
The Prequel: REvil’s Origin Story
The Prequel: REvil’s Origin Story

One aspect of REvil we found interesting is the group’s availability to both media and security researchers. The gang built its brand on its name and used it as a persona to conduct interviews and release statements publicly. For example, Tomas Meskauskas, a security researcher from PCrisk, first communicated with the attacker through their own chat portal on May 1, 2019, when the gang first started. Meskauskas captured their conversation in his blog, describing his interactions with the attacker. In the conversation, Meskauskas asked their name and told the adversary they were being called Sodinokibi by security researchers. Interestingly, REvil was unaware and asked him to point out where this information came from, which Meskauskas did. REvil was at a loss as they did not have a name at the time but did not like Sodinokibi and told him to give them a few days and they would come up with a name. This event initiated the attacker to brand themselves “REvil.” Below is the screenshot provided by PCrisk and Tomas Meskauskas displaying his conversation with REvil:

Figure 1: Chat between REvil operator and Tomas Meskauskas as posted on the PCrisk blog
Later, in October 2020, we learned more about the meaning of the name REvil when one of the group’s operators took part in an interview in which they discussed their origin and aspects of their attacks. In the interview, the REvil operator stated the gang’s name is a combination of the terms “Ransom” and “Evil” (REvil) and was inspired by “Resident Evil,” a popular video game.

However, the story behind the gang’s name is interesting because before its operations started in April 2019, the individuals behind REvil began their criminal careers under another ransomware operation. It was this early activity where the gang gained experience in conducting ransomware attacks. The men who ran the operation named both their gang and their ransomware payload “GandCrab.” Initially, GandCrab conducted their own attacks. However, the gang evolved, and similar to REvil, GandCrab began relying on affiliates to assist in their attacks.

GandCrab ransomware operations took place from January 2018 until June 2019 when they allegedly retired and shut down the RaaS program. Figure 2 below shows GandCrab’s retirement message posted to an underground forum.

![Figure 2: GandCrab retirement statement (translated from Russian) posted on 31 May 2019](image)

At the time, we had no real insight into the actual people behind GandCrab. When the gang retired in 2019, REvil emerged. Due to this and other associations, we initially believed the individuals behind the GandCrab gang simply rebranded as REvil. We believed this for several reasons.
First, the REvil payload shares similar development techniques and functionality with GandCrab ransomware. For example, both ransomware variants share the same string decoding functionality. The cybersecurity firm Secureworks noted the similarity and used the code to “fingerprint” the REvil payload. Using this “fingerprint,” they created a signature and explored malware repositories to identify other samples in the wild. Due to the similarities between both variants, their search returned both GandCrab and Sodinokibi ransomware payloads.

Second, the Sodinokibi payload used a similar method/function as GandCrab to facilitate the affiliate ID and sub-ID, which map the individual payload to the affiliate and its corresponding campaign. Third, in the first version of REvil ransomware, a debug path, “D:\gc6\core\src\common\debug.c”, exists. Note that the path includes the characters “gc6.” GandCrab produced several updates/versions to their ransomware over its lifespan. The last iteration was GandCrab version 5 (GC5), leading researchers to speculate Sodinokibi is the next generation of GandCrab ransomware, version 6.

Further, most GandCrab affiliates transitioned to the REvil operation, dispersing the REvil payload on victim systems once GandCrab exited, further supporting the link between the two gangs. For these reasons, we believed the entity behind REvil were the same individuals behind GandCrab. Instead, based on information provided in both REvil interviews and supporting evidence found in a US indictment, it appears we got this partially wrong.

Based on the earlier interview with a REvil operator, the individuals behind it were actually affiliates of the GandCrab gang and not the core gang itself. According to a REvil operator, when GandCrab retired, the affiliate, which evolved into REvil, approached the GandCrab gang and purchased its ransomware source code. It is not clear if REvil purchased GandCrab v5 source code and used it to develop Sodinokibi or if GandCrab created it and sold it to the REvil gang.

Either way, someone repurposed, modified, and developed it, or parts of it, into the Sodinokibi Ransomware payload. It’s important to note that Sodinokibi and GandCrab ransomware are not the same source code. Still, they appear to share the same developer and use some of the same code logic to achieve similar functionality, as we discussed in the earlier example. REvil used this new (at the time) payload, Sodinokibi, throughout their operation.

At the time, we had no real insight into the actual people behind GandCrab.
We questioned REvil's claims surrounding their origin. It's possible REvil rebranded themselves from GandCrab and lied about their history. However, the REvil operator admits to conducting illegal ransomware and hacking activities supporting the GandCrab gang. To us, it seems illogical for REvil to lie about their affiliation to GandCrab yet admit to conducting the crimes behind its operation. For these reasons, we believe REvil’s affiliation claim is likely accurate. If REvil operators are GandCrab affiliates and not its core members as initially thought, the obvious question is who was behind GandCrab. While this question is outside the scope of this white paper, it has never been answered.

On April 25, 2019, over a month before GandCrab’s retirement, REvil conducted its first of many attacks. In the early attack, REvil took advantage of a zero-day, exploiting a vulnerability in Oracle WebLogic Server.15 16 After initial access, REvil enumerated the environment, identified domain controllers, and staged their payload in an attempt to infect the victim and encrypt their data. However, interestingly, in this first attack, REvil used both their new Sodinokibi payload and GandCrab ransomware on systems throughout the target environment. We don’t know why the attacker used both payloads, but the time frame and access to both ransomware variants further support the relationship between the two gangs.

Affiliate Recruitment

For a RaaS program to succeed, there must be a solid provider to support operations and even stronger affiliates to compromise targets efficiently. If either is weak or inefficient, so will the rest of the operation. For example, if you have a strong affiliate program that is exceptional at compromising victims, but the provider cannot negotiate with victims or launder the proceeds, the program will fail. Since REvil themselves began as an affiliate, they knew they needed to recruit the most qualified hacker teams to breach targets. To do so, REvil began posting recruitment ads to the same underground forums in which GandCrab previously participated.

REvil needed experienced affiliates and wanted to ensure the affiliates who supported GandCrab moved to their program. To demonstrate they were a serious RaaS provider and show affiliates there was money to be made, REvil first deposited $130,000 worth of bitcoin across two underground forums where they conducted recruiting.17 Money deposited to the forum can be used to purchase malware and services. REvil claimed to pay up to 70% of the profit earned from victim ransom payments in their recruiting posts. Initially, REvil only sought to partner with five affiliates:
“Five affiliates more can join the program, and then we’ll go under the radar. Each affiliate is guaranteed USD 10,000. Your cut is 60 percent at the beginning, and 70 percent after the first three payments are made. Five affiliates are guaranteed $50,000 in total. We have been working for several years, specifically five years in this field. We are interested in professionals.” — REvil

REvil also refused to work with mediocre hackers still learning their trade and considered only sophisticated and proven affiliates. Additionally, candidates for the affiliate program had to be native Russian speakers.

Note: Similar to other Russian-based ransomware attackers, REvil prohibits its affiliates from attacking countries within the Commonwealth of Independent States (CIS), which formerly made up the Soviet Union. REvil also configured the Sodinokibi ransomware to check systems for languages used in CIS-based countries. If the ransomware detects a CIS language used on the target system, the payload will not execute.

Further, to filter out law enforcement and researchers posing as candidates, REvil would ask questions based on local traditions or myths they believed could be known only to Russian and Ukrainian nationals. To facilitate candidate interviews, REvil used qTox, an encrypted peer-to-peer chat, voice, and video communications client that functions over the Tor network. Interviews involve the candidate and multiple REvil operators who communicate in the chat session. Candidates are interviewed and, if accepted, placed on an affiliate team comprised of four to five team members. The affiliate percentage of the profit, allegedly 70%, must be divided and shared among the members of the affiliate team.
Part I: REvil Awakens
Part I: REvil Awakens

By June 2019, GandCrab closed down its RaaS program, released a decryptor key, and went dark. REvil and their affiliates quickly filled the gap left by GandCrab’s departure. However, REvil added a new component to their attack playbook. In addition to encrypting victim data, REvil began stealing it as a second method to extort its target further. Now, if the victim chooses not to pay, REvil threatens to release or sell the victim’s data to other criminals. REvil was the first gang to use this tactic in attacks. REvil used the data as a double extortion tactic to demand higher ransom amounts from the victim. Today, most ransomware attackers have adopted this technique.

Once REvil affiliates complete the attack phase, the victim’s data is encrypted, and a ransom note, such as the one shown in Figure 3, is presented to the victim.

![Welcome Again](image.png)

**Figure 3: REvil ransom note dropped by the Sodinokibi payload**

The victim then uses the key included in the ransom note, which is specific to their organization, to log in to REvil’s chat/support portal and data leak site, displayed in Figures 4 and 5:
Additionally, each entry provided has its own countdown timer. REvil gives the victim a limited time frame to pay the ransom. During this time, REvil begins posting a small percentage of the data onto their leak/auction site with a brief description of each data archive that anyone can download and access.

Figure 4: REvil Chat Support used to communicate and negotiate with victims

Figure 5: REvil’s “Happy Blog” data leak website

Figure 6: Countdown timer indicating how long a victim has to pay the ransom
The longer it takes a victim to pay, the more of their data is exposed. If the victim refuses to pay and time runs out, REvil auctions their data to the highest criminal bidder. While the purpose of the leak site is to entice the victim to pay, essentially, it is an online auction, and if the victim does not pay for their data, someone else, a criminal, usually will.

**REvil Operations 2019**

With REvil, it’s all about the money, and they will use various methods to generate income from a target or its data. For example, a unique tactic seen in REvil’s early operations involved Point of Sale (PoS) systems. In addition to their normal ransom activities, REvil attempts to compromise PoS terminals and steal sensitive data, such as credit card information. This tactic is primarily used when the victim is in the retail industry.

In REvil’s first few months of operations, a managed service provider (MSP) became one of REvil’s initial victims between June and July 2019. Interestingly, GandCrab conducted a similar attack on another MSP only four months prior, in February 2019. Perhaps, as a former GandCrab affiliate, REvil knew an MSP would be a lucrative target. MSPs support and can access their customer’s environments, which is likely why REvil chose them as a target. REvil leveraged this access, compromised the MSP’s downstream customers, and used TrickBot malware to spread and infect them with Sodinokibi ransomware. In total, REvil compromised 23 local government organizations in Texas, a data backup company, and a large number of dental facilities within their first few months of operation. In the initial attacks, REvil exploited a Microsoft Windows vulnerability (CVE-2018-8453) in which a Windows component “fails to handle objects in memory,” allowing the attacker to “run arbitrary code in kernel mode.” The result allowed REvil affiliates to gain administrative privileges early in the attack while going unnoticed by defenders.

Note: While researching the attacks, we realized REvil and GandCrab compromised three major US MSPs and their customers between February 2019 and July 2021. We will discuss the 2021 MSP breach further in this report. Yet, MSPs continued to be targeted by ransomware attackers, as did their customers. To be fair, some of the compromised downstream MSP customers could have protected themselves if they had patched their software with updates offered by the MSP provider. Based on this historical reoccurring pattern of attacks on MSPs, we believe they will likely continue to be targeted by ransomware gangs looking for an easy target with deep pockets to pay out their ransom.
In late August 2019, REvil affiliates conducted reconnaissance on one of the largest banks in Chile, BancoEstado, identifying public and private email addresses used by employees for day-to-day business purposes. REvil crafted phishing emails using the target list that instructed the bank’s employee to open a weaponized office document. However, the document silently installs a backdoor on the bank system once opened. Fortunately for the bank, the initial breach provided REvil with access to only the bank’s corporate network used to facilitate day-to-day business, not the operational network used to facilitate financial transactions.

Once in the environment, REvil enumerated the bank’s network and identified high-value systems such as domain controllers and file servers. Next, REvil used publicly available hacktools, such as Mimikatz, to steal passwords from privileged users. With administrative privileges, REvil invoked Vssadmin to delete shadow copies necessary to restore data and executed scripts that disabled various security products that might identify their ransomware payload.

We believe it is likely that REvil stole bank data.

In the early hours of Saturday, September 6, 2019, with the environment primed for the attack, REvil used PsExec, a Windows administrative tool, to distribute and execute Sodinokibi ransomware throughout the environment, rendering the bank’s corporate data useless. When employees came into work a few hours later, they found their files encrypted and a ransom note displaying instructions to contact REvil and arrange payment in exchange for the decryption key. The bank had no choice but to close operations while dealing with the breach. Analyst1 could not confirm if REvil stole bank data in addition to encrypting it; however, based on previous attacks, we believe it is likely. It is also worth noting that, based on attack data analyzed, a pattern exists in which REvil often conducts the ransom execution phase of their attacks on weekend evenings when most organizations are closed, similar to the BancoEstado incident.

While not the only method, up to this point, the attacker primarily relied on phishing emails to infect targets. However, shortly after the BancoEstado breach, REvil altered its tactics for the initial breach and increased its use of “for sale” malware known as the RIG exploit kit. RIG’s attack chain primarily relies on “drive-by” infections, delivered through a malvertizing campaign in which a victim’s browser gets redirected to a website implanted with the Exploit kit’s malicious code.25

While drive-by infections are the most popular with exploit kits, it is not the only method effective at compromising targets. REvil used both drive-by attacks and phishing emails
in their attacks involving the exploit kit. REvil likely chose RIG due to its ability to provide various exploits, effective against many software vulnerabilities, increasing the likelihood of a successful infection. When a potential victim browses to a REvil-hosted malicious website, RIG provides an à-la-carte variety of exploit options, which the attacker relies on to identify and compromise a vulnerability in the target’s system, such as unpatched software. If successful, RIG then installs a backdoor or other malware used to further the attack and provide REvil access to the target’s system and environment.

REvil used the RIG exploit kit as early as June but still relied more on spam campaigns and other infection vectors. That, in addition to REvil’s targeting, changed in November 2019. At that time, REvil began to use RIG to target Asia-based organizations heavily. In the campaign, targeted organizations spanned several Asian countries, including Malaysia, Vietnam, and Korea. REvil’s most prevalent use of RIG was to exploit the victim and run code that downloads a malicious VBScript, giving the attacker the ability to install backdoors as well as their Sodinokibi payload.

On December 4, 2019, REvil compromised CyrusOne, a data center and infrastructure-as-a-service (IaaS) provider. Specifically, the organization “serves thousands of customers across 48 different data centers located around the world.” REvil leveraged the attack further to infect six of CyrusOne’s managed service customers, including financial and brokerage firms. At the time, CyrusOne stated they did not intend to pay the ransom. CyrusOne knew they could be a target for ransomware attacks as a data center provider. The company listed ransomware as one of its biggest risks in an annual report to the Securities and Exchange Commission about a year before the attack.

Admirably, CyrusOne claims they would not and did not pay the ransom. Fortunately, it appears the organization still had backups of their data, allowing them to restore their environment and assist customers affected by the attack. However, that only addresses the data REvil encrypted, not what they stole. It is unclear if REvil auctioned off the stolen data as they typically do when a victim does not pay. Additionally, CyrusOne stated they worked with law enforcement and cooperated with the investigation.

Like the June 2019 attack against an MSP, in this attack, REvil continued to show its targeting choices involve supply chain organizations. From an attacker’s perspective, this makes sense. They breach one organization and gain access to its downstream customers, who trust the initial target, further maximizing their opportunity to generate ransom-based revenue.
New Year is one of Russia's most celebrated holidays. Russians officially celebrate for ten days between December 30 and January 8. However, while the rest of the world celebrated New Year's Eve on December 31, 2019, REvil was hard at work to compromise Travelex, a foreign currency exchange, which at the time was REvil’s most significant target. While REvil conducted the ransomware execution phase of their attack on December 31, the earlier stages of the attack began much earlier.

BBC, a news and media organization reporting on the story, reached out to REvil on the gang’s chat support page. Surprisingly, REvil responded to their questions. According to REvil, the attack began six months prior, in June 2019. Most enterprise ransomware attacks range from three to twenty-one days. It’s doubtful an attacker would risk getting caught by sitting in a target environment for six months. Regardless of the time frame, REvil not only encrypted Travelex data, but it also claimed to have stolen a database containing Personal Identifiable Information (PII) on Travelex customers, such as names, dates of birth, and credit card numbers.

Unfortunately, Travelex responded to the attack very poorly, doing just about everything a company should not do when in such a situation. Travelex did not report the breach or the stolen data required by the General Data Protection Regulation (GDPR). Making matters worse, Travelex outright lied to both their customers and business partners who relied on their services, claiming the outage was due to “planned maintenance.” Travelex likely did not count on REvil posting messages and data related to the attack on its data leak site, let alone speaking to reporters. Further, due to the global outage of services, Travelex asked customers to go into branches in person where “pen and paper” transactions took place. Obviously, this response could not scale Travelex’s global operations, making it clear REvil’s claims were true.

Ironically, Travelex could and should have easily avoided the entire incident. According to Travelex revenue reporting, the company reported nearly a billion dollars in revenue in 2018, a year before the ransomware incident. Despite its deep pockets, Travelex cut corners and did not secure its infrastructure, making the initial breach extremely easy. REvil gained initial access and administrative privileges into Travelex systems by taking advantage of a vulnerability (CVE-2019-11510) in the company’s VPN software. Ironically, Pulse Secure, the VPN software provider, patched the vulnerability in April 2019, eight months prior to the breach. If Travelex simply applied the patch to its Pulse Secure VPN servers, REvil could not have exploited it. This vulnerability received a lot of media attention since it required little technical expertise to render the exploit and the extremely high level of risk associated with the vulnerability. Unfortunately, much like
their response to the breach, Travelex handled their security and vulnerability patching very poorly.

At the time, Travelex was not only REvil’s most prominent target, but it was also their most lucrative endeavor. REvil demanded a ransom of $6 million worth of bitcoin in exchange for the decryption key and a promise to delete and not sell their customers’ data (fingers crossed). In the end, Travelex made a $2.3 million ransom payout to REvil. Unfortunately, Travelex never truly recovered from this attack. Due to the breach, Travelex shut down business operations to include its websites, used by their customers, in over 30 countries globally. By August 2021, the firm ceased operations in the United States and was forced into Bankruptcy.35

REvil Operations 2020

Since the beginning, REvil has continuously made headlines with its attacks. However, REvil became known far outside the cybersecurity community when they took down Travelex. A little over a month after the Travelex attack, in February 2020, REvil compromised and extorted the clothing manufacturer and designer, Kenneth Cole Productions.36 Then, in May 2020, REvil compromised Grubman Shire Meiselas & Sacks, a New York-based entertainment law firm. A law firm may not seem as notable as Travelex or Kenneth Cole. However, this particular firm had well-known political and celebrity clients. REvil stole 756GB of sensitive data pertaining to various legal contracts and negotiations involving celebrity clients which the firm represented.37

Making the situation worse, the firm’s high-profile clients were at risk of blackmail, in addition to the $21 million ransom demand between REvil and Grubman Shire Meiselas & Sacks directly. In an attempt to apply pressure, REvil began to leak the firm’s data on their data leak (auction) site.

Figure 7: REvil’s auction of Grubman Shire Meiselas & Sacks on their data leak/auction site
The initial data leak included confidential legal information and contracts for celebrity clients such as Lady Gaga, Madonna, and Christina Aguilera. When the firm still refused to pay, REvil doubled the ransom, now demanding a $42 million ransom payment. Additionally, according to a post from a known REvil persona on a Russian-speaking underground forum, if not paid, REvil would release data on then-President Donald Trump:

“There’s an election race going on, and we found a ton of dirty laundry. Mr. Trump, if you want to stay president, poke a sharp stick at the guys; otherwise, you may forget this ambition forever, and to you voters, we can let you know that after such a publication, you certainly don’t want to see him as president. Well, let’s leave out the details. The deadline is one week.” — REvil

Now, you have to remember, while REvil had sensitive data between the law firm and their clients, that does not mean the information was actually as damaging as they claimed. For example, while sensitive, the celebrity data leaked was far from damaging or embarrassing, as the gang suggested. Instead, they were simply contracts with various entertainment and concert venues. More importantly, President Trump’s representatives stated the President was not a client of the law firm. Taking a page from their home countries’ government tactics, REvil may have taken valid stolen data and put a spin on it to make it appear far more damaging than it was. While REvil can hack some of the world’s most prestigious organizations, it failed to post 1GB of data containing a trove of documents related to the firm’s celebrity clients. REvil tried to post the data to a publicly available file upload service to make it more accessible to the average Joe. However, the provider immediately terminated their account and disabled the download, making REvil look foolish.

To try and save face, REvil posted 169 emails associated with or involving businesses surrounding President Trump. However, the emails were meaningless and did not provide “dirt” on President Trump. Instead, the effort showed REvil for what they are, lying criminals that steal and extort legitimate individuals and businesses.

In the end, REvil continued to release data until their auction countdown ran out. Taking advantage of the media attention this attack drew, REvil made a spectacle of selling the data to the first criminal willing to pay the $1.5 million price tag. However, to their embarrassment, no one bought the data when the auction ended, once again leaving REvil to look silly. This embarrassment is important to note, as REvil began to significantly target larger, more noteworthy targets after this attack in a likely effort to reclaim their credibility after such a public failure.
Following the failed extortion attempt against the US law firm, REvil conducted attacks against a major ISP in Sri Lanka, Sri Lanka Telecom (SLT), and the largest telecom in Argentina, Telecom Argentina, between May and June 2020. The attack in Sri Lanka failed, leaving only a small subsection of the company’s infrastructure exposed to REvil, who tried to deploy Sodinokibi throughout their environment. Fortunately, the Sri Lanka telecom identified actors in their network and mitigated the threat before REvil could complete the attack, and neither operating services nor customer data were affected.40

Telecom Argentina, however, was not as lucky. REvil attackers gained administrative privileges early in the attack and quickly stole and encrypted data on almost 18,000 systems within the provider’s infrastructure.41 Still, REvil failed to affect customer services such as internet connectivity in this attack. Instead, systems and data relating to the ISP’s call center took the most damage. REvil demanded Telecom Argentina pay $7.5 million to restore systems and prevent stolen data from being sold at their criminal auction. Showing their greed, REvil threatened to double the price to $15 million if not paid within three days. The telecom claims they did not pay the ransom. Since no customer-facing operational services were affected, and business continued as usual, it seems likely they did not. Additionally, REvil did not remove the telecom from their auction site, indicating the ransom was never paid. Despite their initial success, this was another example of a string of failures in which REvil put in the time and effort to reach a target but failed to generate income for their actions.

Note: We are calling out a string of failed ransom attempts by REvil. However, there are other breaches during this time that did result in a ransom payment. Nevertheless, the string of very public failed attempts involving high-profile targets likely embarrassed REvil and demonstrated a trend that we believe led REvil to invest in themselves and further develop their operation.
Part II: REvil Advances
Part II: REvil Advances

Several months after the public embarrassment of REvil’s failed attempt to extort celebrities, the US president, and several global telecom/ISPs, REvil made a significant move to improve their operation. On September 27, 2020, REvil reinitiated its efforts to recruit the best ransomware affiliates. In an effort to draw affiliates away from other RaaS providers, REvil deposited 99 bitcoins, valuing $1 million at the time, to an underground hacker forum, demonstrating there was money to be made with their partnership. The public embarrassment and failure to monetize the data stolen from Grubman Shire Meiselas & Sacks likely contributed to REvil’s increased effort to grow their operational efficiency. As a result, REvil hired more skilled hacker affiliates and initiated new campaigns against even bigger targets. Figure 8 shows REvil’s recruitment ad posted to an underground Russian-speaking forum:

Figure 8: Ransom-based recruitment ad (translated from Russian)

A second recruitment ad showed REvil was looking for a negotiator and a “tier 1 network provider.” From the post, you can see some of the differences in skill sets desired compared to earlier efforts discussed. For example, the negotiator must speak English, which is likely due to the high number of US targets and the ability/experience in communicating with media, recovery, and insurance companies — all of which could play a role in negotiating ransom payments. We found it interesting that REvil sought individuals who could use “VoIP technology with voice scrambling” to conduct negotiations “both in text and verbally.” This is interesting since we are unaware of an incident in which REvil conducted negotiations over the phone and have only observed negotiations through the gang’s chat portal hosted on their infrastructure or by email.

Furthermore, note that REvil calls out targets in the government sector and defense systems. Again, in the tier 1 network provider role, REvil seeks candidates who have experience exploiting technologies such as Citrix, SolarWinds, and BlueGate, which are
all critical technologies seen compromised in ransomware attacks. The recruitment post can be seen below in Figure 9:

As mentioned earlier, REvil enjoys the spotlight and has conducted interviews over the lifespan of its operations. Before October 2020, REvil’s communications took place on their chat portal, email between themselves and select reporters, and posts to underground forums. In October, that changed when YouTube channel Russian OSINT conducted a lengthy interview with one of REvil’s core operators. The interview is in Russian, but researcher @Sapphirex00 translated and posted an English version here. The interview provided insight into REvil’s mindset and details about their origin. The interview revealed interesting information. For example, REvil claimed it makes $100 million annually and relies on ten developers internally to maintain and upgrade the Sodinokibi payload. As discussed earlier, REvil disclosed their background prior to becoming REvil and the significance of their name, among other interesting details.

A few weeks later, on November 16, 2020, REvil attacked Managed.com, a website-hosting provider. The attack resulted in both service downtime and likely a loss in customers who could not risk having their websites offline. After the attack, the website-hosting provider took down their entire hosting infrastructure globally to prevent further damage. In the end, REvil demanded a 500K ransom that would double if not paid before the auction timer on REvil’s data leak site expired. Again, note REvil’s trend in attacking organizations with relationships and access to many other organizations through their services and infrastructure.
While not a ransomware attack, another significant event took place in November when REvil purchased the source code for KPOT 2.0, an information-stealing malware variant. KPOT is used to steal usernames and passwords from “web browsers, instant messengers, email clients, VPNs, RDP services, FTP apps, cryptocurrency wallets, and gaming software.” REvil purchased KPOT for $6,500 from its author who was moving on to other projects. Its developer decided to sell KPOT on an auction on a dark web forum. REvil purchased the malware to add to its toolbox to leverage in attacks against its targets. It’s unclear how long it took REvil to further develop and integrate KPOT into its attacks. However, shortly after its purchase, in December 2020, the gang compromised another significant target — “The Hospital Group,” a large plastic surgery chain known for its celebrity clients. REvil did not learn its lesson after failing to extort public figures when they previously compromised the entertainment law firm. Similar to other incidents, REvil conducted their typical attack chain of stealing and then encrypting the plastic surgeon’s data. REvil threatened to release intimate patient photos such as their “before and after” pictures if the organization did not pay the ransom.

It was over the next few months when REvil’s endeavor to advance their effort and recruit more experienced and advanced affiliates finally paid off. First, on January 14, 2021, Pan-Asian Group “Dairy Farm,” a retailer with over ten thousand locations throughout Asia, became one of the year’s first victims. Unfortunately, the Dairy Farm Group did not understand the full magnitude of the breach. According to early reports, Dairy Farm believed the attacker impacted only a small portion of their network. Additionally, Dairy Farm did not believe REvil stole their data or had access to their network. The Dairy Farm Group either did not want to disclose the full impact of the attack or was truly unaware of how bad things were about to get. They did not know that REvil had already begun to exfiltrate and stage Dairy Farm data to their leak site, in preparation to auction off the retailer’s data if the ransom went unpaid. Worse, REvil embedded itself throughout the retailer’s network and threatened to use its infrastructure for future phishing campaigns. While we cannot confirm if this ever came to fruition, it is an interesting play by the attacker, who could leverage the access acquired in the initial Dairy Farms attack to infect their customers and partners via Dairy Farms’ own infrastructure. Making things more alarming, REvil demanded Dairy Farm pay $30 million, the highest ransom demanded by any ransomware gang, at the time. However, the record ransom lasted for only a short time.
On March 14, 2021, REvil attacked the Taiwanese computer manufacturer Acer and demanded $50 million, which would increase to $100 million if not paid at the termination of the data auction. Acer unsuccessfully tried to negotiate a $10 million payment, which the attacker rejected. While Acer did not pay the $50 million ransom, on April 18, 2021, REvil continued their pursuit with another high-profile target, Quanta Computers, asking for the same amount. Similar to other attacks, in addition to exposing Quanta, REvil also threatened to expose data associated with their customers. Except this time, REvil had far more leverage since Quanta manufactured laptops for the computer and phone giant Apple. Now, REvil threatened to release sensitive blueprints associated with Apple’s new laptop and smartwatch. Quanta denied the severity of the breach publicly, but the leaked data made it clear REvil was not bluffing. When Quanta chose not to pay, REvil threatened Apple directly:

“Drawings of all Apple devices and all personal data of employees and customers will be published with subsequent sale.” — REvil

Then, on April 20, while Apple announced new products at a live online sales event, REvil leaked additional data to include schematics of Apple’s new MacBook Pro laptop. REvil also threatened to release additional data every day until the action ran out or Apple paid the ransom. However, REvil terminated their auction early, removed Apple data from their leak site, and made no further threats or ransom demands to Apple. Usually, this only happens if a victim pays. It would appear REvil’s attempt to hire highly skilled hackers as affiliates after several failed attempts finally paid off for a big payout.
Part III: Give Your Self to the DarkSide
Part III: Give Yourself to the DarkSide

Have you ever seen a fictional movie where the villain has an overzealous sidekick or protégé that screws everything up? If this were one of those stories, that protege would be DarkSide. DarkSide was another RaaS provider that conducted attacks from August 2020 through May 2021. DarkSide was a well-versed and sophisticated attacker, but they were too ambitious for their own good. Like REvil, DarkSide started as an affiliate supporting another RaaS provider. You likely guessed that provider was REvil.56

Several ties exist between the two gangs to support this theory. DarkSide’s ransomware shared similar code found only in REvil’s Sodinokibi payload. REvil controls Sodinokibi and its source code, which is not publicly available. It is unlikely the REvil gang would share it unless a trusted relationship existed between both parties. We believe the individuals behind DarkSide likely knew or, at a minimum, associated closely with REvil operators.

Further, both REvil and DarkSide operators participate in the same underground Russian-speaking forums and post within the same threads. Making the tie stronger, REvil has posted messages publicly on behalf of the DarkSide gang. Next, we discuss DarkSide’s final operation in detail. This is important to our story because it starts a series of events that lead to REvil’s demise.

DarkSide’s Blunder

On May 7, 2021, the DarkSide gang attacked Colonial Pipeline, the organization responsible for distributing fuel across the entire east coast of the United States. The impact of the attack forced Colonial to shut down pipeline operations. As a result, a fuel shortage ensued. Many Americans across the east coast could not obtain fuel for their vehicles. More importantly, concern grew that emergency services could be affected by the fuel shortage.

The attack caused unease among the population. US citizens wanted answers about how cybercriminals could disrupt a significant element of US critical infrastructure. The US government saw this as an aggression against national security, questioning if a criminal organization could have conducted the attack on its own or had help from a foreign government. Further, the Biden administration received criticism as fear grew that the fuel shortage would impact emergency services and critical infrastructure.

Due to the impact and criticism, President Biden addressed the situation, stating the United States would go after whoever was behind the attack. He also planned to address
the issue with Russian President Vladimir Putin when the two met the following month. Shortly after the statement, DarkSide posted the following message to the “press” section of their data leak site:

“We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for other our motives,” the group wrote in a recent statement on its dark web site. “Our goal is to make money and not creating problems for society. From today, we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.” – DarkSide

Based on their statement, DarkSide realized they went too far and gained the attention they had not expected from the US government. The following day, DarkSide’s payment portal, leak site, and content delivery network (CDN) went offline.

With the US government in pursuit and the loss of operating resources, DarkSide made one final post on an underground forum declaring they were shutting down their operation. Intel471, a cyber intelligence company, translated the post, which they detail in their blog here. Also, DarkSide stated they intended to pay their affiliates money owed and provide decryption keys necessary to decrypt data should existing victims decide to pay.

On May 14, 2021, seven days after the pipeline attack, the administrators on the affiliate recruitment forums banned future discussions about ransomware, aka “lockers.” It was wise to restrict the topic to stay in business and keep US intelligence and law enforcement agencies from interfering with their operations. Administrators likely knew the same attention would fall on their forums should it continue to support ransomware operations.

Further, administrators banned DarkSide and took their bitcoin deposit for themselves.

A few weeks later, in early June, the Department of State announced they “seized 63.7 bitcoins currently valued at approximately $2.3 million” from the DarkSide attacker. Strangely, while taking responsibility for the seizure of funds, the United States claimed
they were not behind the infrastructure takedown. Nonetheless, it’s widely speculated the takedown effort was, in fact, the work of the United States Cyber Command.60

This would not be the first time the US government conducted a “takedown” operation to remove assets used by cyber adversaries. However, it is the first time we have seen such a large amount of cryptocurrency taken from a crypto wallet unbeknownst to its legitimate owner.

Still, DarkSide obtained far more in ransom payments over the lifetime of their operation than they lost in the seizure of funds. Yet, despite promising to pay their affiliate partners, DarkSide left many of their peer criminals unpaid after the takedown. As a result, they trashed their reputation in the Russian criminal community, and several affiliates filed arbitration claims against them for millions of dollars' worth of owed money.

Note: Russian-based criminals who support ransomware operations rely on the criminal court system, known as arbitration, to recover unpaid funds for work conducted on another criminal's behalf. For additional information, see our blog “Dark Web – Justice League,” which details the underground arbitration process.

Now, DarkSide was hiding from the US government and the criminals they owed money to. Due to their absence, REvil acted as a spokesman on DarkSide's behalf. In a public statement posted to a Russian OSINT telegram channel, REvil provided details confirming the takedown of DarkSide's infrastructure and loss of funding.61

After disappearing, many researchers wondered if DarkSide would stop their criminal activity or rebrand and return with a new online persona. While outside the scope of this report, researchers Fabian Wosar and Brett Callow of Emsisoft found evidence to support DarkSide may have returned later that summer as the BlackMatter ransomware gang.62 You can find additional information in their blog covering their findings.

Shortly after speaking for DarkSide, while the United States' response took place in May, REvil conducted another high-profile attack. This time, the victim was JBS USA Holdings, Inc., a Brazilian-based meat processing and distribution company. JBS processed and distributed one-fifth of the meat distributed throughout the United States. Due to the attack, JBS shut down parts of its operation, resulting in meat shortages across the United States. To address the situation, JBS decided to pay the $11 million ransom to bring services back online quickly. While the impact was not as bad as it could have been, fear and concern among the US population rose. In the same month, ransomware attackers impacted both fuel and food resources across the country. DarkSide may have run, but REvil stood its ground, taunting the United States.
The Double-Cross

In May, while the Colonial Pipeline and JBS attacks were occurring, an affiliate opened an arbitration case. This complaint, however, was against REvil, not DarkSide. The affiliate claimed REvil owed them over $14 million for work they did to breach and extort a large “holding company.” The affiliate said they negotiated the ransom with an employee named William. Apparently, the affiliate and negotiator agreed on a ransom amount the victim would pay in exchange for the decryption key. However, they needed a few days to allocate the funds and transfer them to bitcoin. Time passed, and the affiliate had not received payment from William. Finally, several days later, William responded with one final message:

![Figure 11: Victim message (email) to REvil affiliate as posted as evidence in their arbitration case](image)

In the complaint, the affiliate continued to prove his case to the arbitrator. He stated that only the provider, REvil, had the decryption key, which he believed William obtained. The affiliate believed REvil double-crossed them and made the deal to provide the key to William themselves. The affiliate provided logs and emails of their negotiation with William to support their claim. The logs supported that the affiliate did indeed conduct the breach, deploye the ransomware, and negotiate with William. Still, they could not prove that REvil made contact or received a payment from the victim. The affiliate believed that REvil interfered with the negotiation and made a deal without them, taking all the proceeds. Further, only four days later, REvil deposited $1 million in bitcoin to the same forum in which arbitration took place and began recruiting other affiliates. Based on the deposit made to the forum, REvil may have influenced the arbitrator’s decision. While the deposit funds are not intended to benefit the forum administrator, they have direct access to the money itself and can (and have) confiscated funds from users who have been banned. The arbitrator refused to award compensation to the complainant without proof of payment. Some individuals on the forum were also displeased the complainant provided so much information and evidence at the public level. They were concerned researchers, like us, who would write about it. Others, like LockBit, a competing ransomware gang, claimed they had heard similar claims about REvil from other affiliates. For now, it was the
affiliate's word against REvil's and, unfortunately, had little impact on REvil's ransomware business or their ability to recruit affiliates at that time.

Figure 12: LockBit comment regarding REvil double-crossing affiliates
Part IV: Good vs. REvil
Part IV: Good vs. REvil

On June 16, 2021, both Russian and US presidents met in Geneva as planned. Both administrations had a full schedule of issues and topics prepared for the meeting. However, ransomware dominated the discussion. President Biden requested help from the Russian government to deter criminals and warned if the attacks continued, the United States would “respond in kind.”63 If the attack against US critical infrastructure by the Russian-based DarkSide attacker did not occur, it’s unlikely the two world leaders would even have discussed ransomware. Now, it was the focus of their first meeting.

You would expect an adversary like REvil, who tries so hard to portray themselves as an elite attacker, would have the sense to lay low until the storm passed. Instead, again in June, REvil posted another message to the Russian OSINT Telegram channel they previously used to discuss DarkSide after the pipeline attack. This time, they directed their declaration directly to the United States government. REvil stated they were “not afraid of being labeled a cyber-terrorist group” and “in light of US actions and posturing to retaliate for the JBS Foods attack, the group will now lift the restriction on attacking US targets.”64 Just a few weeks later, REvil made good on their threat and conducted their most significant attack yet.

On July 2, 2021, REvil executed an attack against Kaseya, the US-based MSP we discussed at the start of this white paper. REvil began with a SQL attack to exploit a zero-day vulnerability (CVE-2021-30116) in Kaseya’s Virtual System Administrator (VSA) servers. As an MSP, one of Kaseya’s business practices is to push software updates to its clients, ensuring downstream customers maintain and stay current with its software.65 REvil leveraged Kaseya’s patching process and client-trusting infrastructure to push a weaponized update, infecting 1,500 companies across 22 countries.66 On a good note, Kaseya was transparent about the attack and its impact, unlike many of REvil’s previous victims. They also reacted quickly, turning off vulnerable VSA servers, which prevented REvil from infecting additional customers.

The United States government took note of the aggression. Shortly after Kaseya reported the incident, President Biden addressed reporters at a press conference. He was “still gathering information to the full extent of that attack” and that he had just “received an update from (his) national security team” and would “have more to say about this in the next several days,” but he felt “good about our ability to be able to respond.”67

Additionally, the White House put out an official statement about the Kaseya attack: “Yesterday, President Biden directed the full resources of the government to investigate
this (Kaseya) incident.\textsuperscript{68} REvil was now the focus of interest for US national security resources, such as Cyber Command, CISA, DIA, and other US intelligence agencies with more significant resources than law enforcement alone.\textsuperscript{69}

Despite the United States’ response, REvil demanded $70 million, one of their highest ransom demands to date, in exchange for a universal decryption key that Kaseya victims could use to restore their data. Further taunting the United States, REvil added an entry to their website naming Kaseya as their latest victim.

Eleven days after attacking Kaseya, in the early hours of the morning on \textbf{July 13, 2021}, REvil’s infrastructure used to leak and auction victim data, as well as their payment portal, mysteriously went offline.\textsuperscript{70} This included both REvil infrastructure hosted on the dark web and sites accessed from the traditional internet. We do not know if REvil willingly took its infrastructure down or if it went offline as part of a covert government operation. However, several sources, including other Russian ransomware gangs such as the LockBit gang, claimed on underground forums that REvil took down their infrastructure due to pending government actions with their site-hosting providers.

Alternatively, the US government may have conducted a hostile takedown of REvil’s sites. In our opinion, the government would take credit and highlight the takedown as a victory in its new, very public war on ransomware. Remember, several embarrassing attacks occurred earlier that year in which the United States had no recourse before its response against DarkSide. We think they would want to make a public example if they were behind the takedown. Realizing this, we agree REvil decided to delete their virtual footprint and remove all their infrastructures to prevent the United States from using it against them in their pending operations.

REvil talked a big game. Yet only a month after taking a bold stance against the United States, the individuals hiding behind the REvil persona were quiet as a mouse. There were no more threats, no more grandstanding, and, most importantly, no more attacks. It would seem no one wanted anything to do with REvil, including the forums in which they
frequented. The administrators of the top two underground forums banned the account REvil used to recruit and communicate with the criminal underground.

REvil may have vanished, but Kaseya and its customers still faced the challenge of decrypting their data. Many of Kaseya’s customers affected by the attack were upset because they no longer had an option to pay the ransom and obtain the decryption key. However, on July 22, 2021, things took an unexpected twist. A “trusted third party” provided Kaseya and its customers with the decryption key necessary to unlock their data. Normally, only REvil could access and provide the key. Remember, REvil demanded $70 million for the key, so they would unlikely give it away for free.

The obvious questions: who was the third party and how did it obtain the decryption key. We know this was not a “back-alley deal” because the third party required victims to sign a non-disclosure agreement (NDA). An NDA would be useless if the third party were a criminal. However, it would be helpful if the third party were the US government and did not want to disclose how they obtained the key. The problem was, some customers paid the ransom weeks prior, and others already spent considerable time and money in rebuilding their infrastructure. If the US government had released the key, they should have kept the victims abreast of the effort before victims spent millions to recover. As news of the key began to circulate, media organizations began to report the key originated from the Russian government. According to Bleeping Computer, Russian intelligence may have obtained the key directly from REvil and provided it to the United States. This theory is plausible since the United States asked Russia to intervene during the Putin/Biden meeting.

Several weeks later, on August 5, 2021, a user named “Ekranoplan” posted a message on one of the underground forums with a link to a GitHub page that included a screenshot of the decryption key.

It is impossible to validate, but the individual behind the post claimed they obtained the key from their “parent company.”

![Figure 14: Forum post about REvil decryption key](image-url)
Part V: Deliver Us from REvil
Part V: Deliver Us from REvil

Almost two months passed in which the world had not heard from REvil. Then on **September 7, 2021**, REvil’s infrastructure came back online. Their data leak/auction site and payment portal were suddenly up and running. Previous victims who had not paid their ransom had new auction timers set. A few days later, REvil created new accounts on the same underground forums that previously banned their accounts.

Further, *Bleeping Computer* published screenshots of a recent conversation between REvil and a security researcher. In the discussion, REvil stated they had taken a break. Again, of the possible theories, we think it is likely REvil realized a takedown operation was underway and took their own infrastructure offline. We know we cannot trust REvil.

Eventually, the FBI acknowledged they were the “trusted third party” who provided victims with the encryption key. According to FBI Director Christopher Wray, other law enforcement agencies involved in the investigation were to blame for the delayed release of the key and lack of transparency. Unfortunately, he did not state how they acquired the key.

If you recall, an affiliate had a dispute with REvil earlier that year in May 2021. This incident was far more significant than anyone comprehended at the time. The affiliate had opened an arbitration case claiming that REvil deceptively took over the negotiation process and never paid them. You see, what we did not know then was that the accusations were not only accurate, but they were part of a much larger plot. Now, in September, researchers at AdvIntel found evidence proving REvil had built in a backdoor allowing them to cheat their criminal business partners.

Specifically, AdvIntel found evidence that REvil used the backdoor to establish a second chat session with victims, unbeknownst to the affiliate. Affiliates relied on an admin console to manage the attack and communicate with the victim. The “double chat” capability allowed REvil to monitor these conversations. If the conversation went well and REvil believed the victim would pay, they would make it appear to the affiliate the victim had a change of heart and terminate the discussion. Then, secretly, they (REvil) negotiate with the victim directly. To the affiliate, it would appear the victim simply decided not to pay and disappeared. In reality, REvil finished the negotiation independently and collected the ransom. Based on promises in their recruitment ads, REvil would have to share 70% of the profit. Now they kept all of it for themselves.

Affiliates and other criminals across the Russian forums quickly began to turn on REvil as the news spread. However, the loudest voice came from the affiliate, whose post...
we discussed earlier. The news validated his claims. Now there was no question, REvil were deceptive liars that even criminals could not trust. Figure 15 displays the affiliate complaint:

![Signature's post following news of REvil's double-cross](image)

Still, REvil tried to conduct damage control and defend their actions. Using their two new forum accounts, they responded to the allegations. REvil responded to other criminals on the forums, which discussed their actions. Nevertheless, no one believed them. One user took REvil’s Sodinokibi code and directly pointed out binary evidence in a detailed analysis directed at REvil. Still, REvil was adamant that they had not double-crossed their partners.
So, the software started. After initializing the config, the registry is checked for the presence of keys for encrypting the system (apparently this was done so that the software, launched a second time, would not generate keys again). And here it immediately catches the eye that 3 values are read from the registry:

```c
u0 = registry_read(0x80800002, &subkey, &name_masterpubkey, &type_2, &size); // 1
u15 = u0;
if ( !u0 )
{
    u15 = registry_read(0x80800001, &subkey, &name_masterpubkey, &type_2, &size);
u0 = u15;
}
u1 = registry_read(0x80800002, &subkey, &name_pc_publickey, &type_1, &size_1); // 2
if ( !u1 )
    u1 = registry_read(0x80800001, &subkey, &name_pc_publickey, &type_1, &size_1);
u2 = registry_read(0x80800002, &subkey, &name_unck_key, &type, &size_2); // 3
if ( !u2 )
    u2 = registry_read(0x80800001, &subkey, &name_unck_key, &type, &size_2);
```

1. Public master key - taken from the config in the stub itself and for some reason still stored in the registry
2. Public computer key - generated uniquely on each new system
3. Some incomprehensible key

If they are not in the registry and the software is launched for the first time, they are generated.

```c
\generate_pc_pub_and_pri_keys(&pc_private_key, &pc_public_key); // (a)
size = 32;
u22 = 32;
u1 = encrypt_key_byaes_curve(&master_pk, &pc_private_key, 32, &size_1); // (b)
encrypted_backdoor_key = encrypt_key_byaes_curve(&backdoor_key, &pc_private_key, 32, &size_2); // (c)
wipe_data(&pc_private_key, 32);
if ( !u1 || !encrypted_backdoor_key )
return 0;
memcpy(&global_encrypted_master_key, v1, size_1);
memcpy(&global_encrypted_backdoor_key, encrypted_backdoor_key, size_2); // (d)
```

Revil first creates a private and public key for the victim's computer. Further manipulations take place around this particular pair. (a)
Then the generated private key of the computer is encrypted with the master-public key (this is the key that is in the stub config) (b)
And last of all, the same private key of the computer is encrypted with an unknown public key, embedded in the stub (c)

Another forum member also challenged REvil directly and wanted to know how they could trust them. REvil obviously thought they could talk their way out of the situation because they continued to post and defend themselves rather than close their account and disappear. However, the damage was done. Figure 17 shows an affiliate challenging REvil's (0_newday) previous post in which they attempt to portray themselves as a “victim of slander.”
As you can see, REvil destroyed its own reputation, losing credibility with affiliates across the ransomware scene.

It seemed like things could not get much worse for REvil. However, on October 16, 2021, it did. Someone sabotaged REvil’s infrastructure and secretly took control of their Tor servers. The attacker could have taken REvil’s servers offline. Instead, they left it up and running, appearing exactly as it did under REvil’s control. Unfortunately, due to their paranoia, REvil identified the compromise immediately.
Realizing what happened, REvil made their final post to the underground Russian forum. In their post, REvil stated “the server was compromised” and that someone “deleted the path to my hidden service in the torrc file and raised their own so that I would go there.

Figure 18: REvil post claiming their infrastructure was compromised (translated from Russian)

While REvil identified the operation against them, it still resulted in a positive outcome. With affiliates turned against them and a third party infiltrating their internal servers, REvil decided to close its ransomware operation. After more than two years of wreaking havoc, REvil ran away embarrassed and defeated. Still, you have to wonder, who was behind the sabotage operation?

Affiliates and criminals closest to REvil discussed two theories on the underground forums. The first was that another REvil operator who had previously been the group’s voice had gone rouge and attempted to take over their servers. We don’t feel this theory is likely. There is little benefit in sabotaging a dying operation. The second theory, which we believe to be accurate, is that the US government was behind the operation to hijack and compromise REvil’s infrastructure. The US government had the motivation and ability to conduct the operation.

Remember, this was an offensive strike, but the attacker did not intend to result in a loss of services forcing REvil to stop their operation. Instead, the attacker intentionally tried to go unnoticed, hoping REvil would continue business as usual. Then, the entity behind the attack could quietly observe REvil’s actions, collect evidence, and gather intelligence on the gang itself and the affiliates who support them. We believe the operation was the work of US intelligence agencies who were fed up with REvil and building a case against them. While Russia historically has protected ransomware criminals, the genius of this operation is that, despite this, it resulted in the demise of REvil. Further, it most certainly had a psychological effect on both REvil and affiliates. They likely wondered if the United States could infiltrate REvil’s operation; what else did they know.
Faces of REvil

On November 8, 2021, the US government answered this question publicly. The United States issued indictments against two men whom they claimed supported REvil and took part in the attack against Kaseya. The first indictment was against Yaroslav Vasinskyi, 22, a Ukrainian national, and Yevgyeni Polyanin, a Russian citizen. Additionally, the US Department of Justice stated two other Sodinokibi/REvil affiliates in Romania were also under arrest. The United States seized over $6 million in bitcoin currency from a REvil-owned digital wallet.

Vasinskyi was arrested in Poland and is awaiting extradition to the United States. He shockingly had poor OSINT practices. While only his first name, we found it odd for a cybercriminal to use any part of their actual name in their online identities, but he did. He used the online monikers “Yarik45,” and “Yaroslav2468.” Yaroslav used the same handles across numerous forums and social media websites, creating a large online footprint. Yaroslav also registered email addresses on some of these sites, making it easy to pinpoint his identity once you knew he associated with REvil. The second individual indicted, Yevgyeni Polyanin, is also believed to be an affiliate who supported REvil operations. Specifically, the United States believes he took part in the attack against Kaseya.

Below you can see images of both men. Figure 19 displays the FBI wanted poster for Polyanin. The second image, Figure 20, displays Vasinskyi as seen on social media.
The real question is, did Vasinskyi's parents sign his field trip form the day this photo was taken? We may never know. Regardless, the indictment certainly sent a message that the United States could identify individuals behind REvil attacks. However, its impact was minimal, and the men named were only REvil affiliates and not core members of the gang itself. Still, the United States continues to pursue REvil, offering millions for information leading to the arrest of the gang's leadership. The US Department of State released the following statement regarding REvil members still at large:

“The Department of State is offering a reward of up to $10,000,000 for information leading to the identification or location of any individual holding a key leadership position in the Sodinokibi ransomware variant transnational organized crime group. In addition, the Department is offering a reward offer of up to $5,000,000 for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in a Sodinokibi variant ransomware incident.” — US Department of State

We thought this was the end of REvil's story. However, on January 14, 2022, Russian authorities conducted night raids, kicking in doors and taking 14 individuals into custody. Allegedly, the individuals include the gang’s ringleaders and not affiliates alone, like the previous arrests in Ukraine. According to a press release on the Russian FSB website, the raid was a joint operation between the Russian FSB and the Ministry of Internal Affairs
(MVD) conducted at the request of the United States. Russia also stated they kept US authorities informed of the outcome of the operation.

**Figure 21: FSB Press release about raids on members of REvil**[^1][^2]

The REvil members arrested were apprehended in Moscow, St. Petersburg, and in the regions of Leningrad and Lipetsk. As of this writing, the FSB has not released the identities of the men arrested. However, a Russian court identified two of the men as Roman Muromsky and Andrei Bessonov and placed them in custody for two months while they are tried for their crimes.[^3]

Additionally, while arresting REvil’s members, the FSB confiscated nearly $7 million (in total), 20 “premium cars,” and computer equipment. A camera crew present during the operation recorded footage as the FSB raided several of the accused men’s homes.[^4]

The arrests will make a significant impact on ransomware criminals. More importantly, this is where REvil’s story ends.

[^1]: ILLEGAL ACTIVITIES OF MEMBERS OF AN ORGANIZED CRIMINAL COMMUNITY STOPPED

[^2]: [Image of FSB Press release about raids on members of REvil]

[^3]: The arrests will make a significant impact on ransomware criminals. More importantly, this is where REvil’s story ends.

[^4]: The arrests will make a significant impact on ransomware criminals. More importantly, this is where REvil’s story ends.
Figure 22: Images from footage of REvil members arrested during FSB raids.
Assessment: Beyond Good and REvil
Assessment: Beyond Good and REvil

It is too early to tell if Russia will continue to hold ransomware criminals accountable despite the arrests. In recent months, Russia has been posturing troops along the border of Ukraine in what many believe is the early stages of a military invasion. The cooperation may only be an effort to build a stronger relationship with the United States, hoping it will not interfere should a military conflict ensue. Suppose the United States does interfere or attempt to enforce additional sanctions against Russia, which seems likely. In that case, the cooperation will likely cease, and ransomware criminals will once again be protected by the Russian government as long as they do not target organizations in the Commonwealth of Independent States (CIS). Another concern is history will repeat itself, and Russian Intelligence will recruit cybercriminals, such as REvil operators, to support their needs. In our previous report, Nation-State Ransomware, we describe several past instances where this exact scenario occurred. Regardless of the arrests, we do not believe REvil could continue to operate based on the distrust and loathing the ransomware community has for the gang.

Impact

Russia is not charging members of REvil with computer crimes, among other charges they would face in the United States. Russia is charging REvil only with committing crimes “under Part 2 of Art. 187 of the Criminal Code of the Russian Federation” (“Illegal circulation of means of payment”). In the past, sentencing guidelines in Russia show criminals found guilty of the same charge were imprisoned for no more than seven to ten years. While this is a long time, it certainly does not seem to fit the crimes REvil committed in their lifetime of attacks.

Prior to the arrests, Russian ransomware criminals within dark web communities had little to no fear of repercussions for their actions. Based on conversations over the past several years on these forums, ransomware criminals believed they were untouchable. The only concern commonly discussed by forum members were arrests should they leave Russia. Based on REvil’s story and events that have been detailed in this paper, we wanted to address how, if at all, the events have changed the mindset and/or operational lifecycle of ransomware attacks.

To answer these questions, we looked to the members of the underground criminal community that REvil used for affiliate recruitment themselves. Shortly after news broke
of Russia’s cooperation with the United States, leading to the REvil arrests, several of the community’s members began to discuss the topic, as displayed in Figure 23 below.

We were surprised to see the tone in the conversation change. Of course, some criminals will stand by their original viewpoint on the topic. Yet this is the first time we have seen broad concern regarding ransomware attacks. **While the United States may never prosecute REvil or other Russian-based ransomware criminals in their own court of law, they have psychologically impacted the Russian ransomware community.** Honestly, we did not think the day would come where criminals would make statements like “the balance has changed” and be concerned they could “go to jail.” These are only a few examples of many similar concerns voiced in the ransomware community over the past 48 hours since the arrests. Initially, this may sound like a small win, but in our opinion, this is a huge accomplishment and the first significant step to thwart future ransomware attacks. Getting into the head of your adversary could undoubtedly impact its future actions.

Next, we want to access how this affects ransomware gangs from an operations perspective. This time, we wanted to look to other well-known ransomware service
providers to see if there was evidence of them making changes to how they conducted their day-to-day criminal activities. One of the prominent gangs known to voice their opinion within the ransomware community is the LockBit gang, whom we assessed in our previous reporting. At that time, LockBit was a bold and highly intuitive gang that often developed new methods and techniques to compromise targets. Unlike REvil, LockBit is straightforward in its communications on the underground forums, has a good reputation, and keeps its word with affiliates, making them a viable information source.

Historically speaking, LockBit has always been critical of REvil and suspected that they were untrustworthy, even before evidence had surfaced. However, at the time, we believed it was simply their bias since they directly compete with REvil for affiliates within the ransomware space. When affiliates began to complain, LockBit quickly criticized REvil, making comments REvil could not be trusted.

LockBit was also one of the first to accuse REvil of working with the United States, once the FBI released REvil’s decryption key to Kaseya victims. In a conversation on the forum, LockBit challenged REvil to explain how the key leaked. REvil told the LockBit operator that one of their developers “misclicked and generated a universal decryptor.” LockBit was not buying the story or letting REvil off the hook with their explanation. He pointed out how careful the group operated and how convenient the timing of the leaked key correlated with the US/Kaseya incident.

![Figure 24: REvil forum post responding to LockBit (translated from Russian)](image)

You could see things beginning to unravel. LockBit began posting messages about not trusting anyone and claimed “snitches are everywhere.” In another post, LockBit called for new vetting procedures in which trusted forum members could review code and ensure its developers do not install backdoors into their ransomware payloads.
Further, LockBit wanted the developers themselves to be “vetted” to ensure they were not secretly working with the FBI, as it believed REvil did. In short, LockBit believed REvil was compromised and working with the FBI, which it repeats in several other posts between September 2021 and January 2022.

In January, after news of the arrests in Russia, LockBit posted a private conversation, something rarely done, that it had with a REvil operator who used the alias “REvil Oneday.”
The issue was the REvil operator disappeared in November 2021, shortly after their conversation. LockBit believed another individual he referred to as “RED \ KAJIT” was to blame. LockBit stated KAJIT was an administrator on another underground forum and was working with the FBI. In November, administrators took the forum down for several days before the REvil operator’s disappearance. If LockBit is correct, KAJIT may have provided the FBI with information or possibly access to all its members and back-end data, which is how the FBI could get to REvil and potentially other ransomware affiliates.
Conclusion
Conclusion

REvil's narrative sounds more like fiction than reality. Their story includes:

- Multi-million-dollar ransom schemes
- Meetings between world leaders
- Secret government operations
- Hidden backdoors and betrayal
- Night raids and arrests

The only thing missing is a good car chase. While REvil's story is fascinating, it also provides us with a wealth of knowledge about the inner workings of organized criminal ransomware gangs. As defenders and researchers, we often focus on technical details and rarely get insights into the human aspect of attacks. Between research reports, government indictments, video footage, and several years of conversations and discussions on underground forums, we feel REvil's account provides the most in-depth use-case to date on a ransomware gang and their criminal operation. It is also the first time we have captured the entire life cycle, from the cradle to the grave, of a ransomware gang and their operation.

REvil's biggest mistake was their ego, which led to their downfall. Had they targeted smaller, non-essential organizations and not betrayed their own people, they would likely still operate their crime syndicate instead of facing prison. While REvil is unlikely ever to show its face again, ransomware will continue to be a problem. However, with governments increasingly taking this problem head-on, dedicating vast resources to mitigate the problem, we hope to see attacks decrease. We also believe Russia's involvement in this problem is critical to reducing or mitigating ransomware attacks. If the Russian government falls back to its long-standing practice of protecting cybercriminals, it's unlikely we will resolve the ransomware problem anytime soon.
Appendix

IOCs

33BC14D231A4AFAA18F06513766D5F69DB88F1E697CD127D24FB4B72AD44C7A
2896B38EC3F5F196A9D127DBDA3F44C7C29C844F53AE5F029229D56FD6F2A59C
64076294E761EE0CE7D7CD28DAE05F483A711EAEF47F94FE881AC3980ABFDD8F
45B6349EE9D53278F350B59D4A28890BEEF99DE6565453DB4C085BB5875865
59A2A5FAE1C51A5BBF1BF8C6EBA65CBB2B8575794E3890F499F9893053E633FC
56DE41FA094FA7FF6F68F02712A698BA2F0A71AFCECB217F6519BD571BAF3ED
538078AB68D0D7C889AF3E08F62C4E83358596F31AC8AE8FBC6326839A6BFE5
B1B00FB0B658EC013E0C3C0F34707B19ED0537DBE2E83D0D023A11A0CA6B388
E35C31BAE310F59AE8A9154E2C0F6F832FCFF22B959F65B607D6BA0879AB641
4B25F708C506ECC747344EE79EDCAA485D1F6C25C9CB45CEB420575458F56720
11AF3609884AD674A1C86F42ECC7719094E93D357D73E574B75C787A0E8C0F1
8D44894C09AE3004927F8951E01708D0A600813387C3C0872BC6CB10A3E8C
8DD62D9AE35960BB66458C890EDE987C33239CF730F93FE49D90AE759DD
1FE9B489C25BB2304D9968E1087671EDE69DB6D6DEFE7ECE38A0FB35F9E8
8E846ED965BBC0270A6F58C5818E039EF2FB78DE4D2BF82348CA786EA0CEA4F
81D0C71FB82B6D9B5BFD392422D033109E2C92572FC49E492C4271
0496CA57E387B10DFDAC809DE8A4E039F668E8D6535D5D19EC76D39F7DD402
66490C59CB963OB53FA3FA7125B5C951AFDE38EDAB4459065938C1974229CA8
AA6E638E774180BCE96DAD55B5EFD63DOEB7124D68B699170193680F1FC7
CC0CDC6A3843E22C98170713ABF1D6AE06B5E34ED0E6AC3159DADE85E3B6D
D5CE63F6A06B0DC8CE8E7E2CA953E66094C2ADFC9CFC61DD9EFE9AC45A75F
D55F983C994CA160E63A59F6B4250FE67FB3E8C3A388AEC6A0A4697B9E9F1E
D8353CFC5E696D3AE402C7C70565C1E7F3E49BCF74A6E12E5AB044F306B4B20
DC6B0E8C1E9C113F0364EC18370060DEE3FCBE25B667DDECA7623A95CD21411F
DF2D6E0450660AAA62C429610B964949812DF2DA15C75646FC29A51C3F031E
E2A244AB94F865CAEACDF2C3AD015F31F23008AC6DB8312C2CBBF32E4A5466EA2
36A71C6AC77DB619E18F071BE47D79306459FF1550B0C92DA47B8C46E2EC0752
45AEBD60E3C4ED83D2859075FB6C71B360A9B6B7C34E246C20410CF678FC0C
FF61085FF157FE0A98BA5343E65637EE24E12C3C4B18E4532FC2747F3E5
FFDDDBBC09972A8DA7892209FB45796B4343FDD8C74AE8E56BEF78AEB7C71077B7
FAC5D964676B9725B4123B78EB52E3FA71BE748579896774DF3F86BE1FBA4E
F9293336935D3E441642B60857A102B91738351630A10BB4194CB1ED65793B7
F1BC14943C240F59BBD3AD4D63AD5568F896F80E79697E690612C5602FA653D
F195FB77843E110FF91656C09D277563EE32C2D36388E556F25328BF0AAC80BE
Endnotes

3. https://twitter.com/GrujaRS/status/1122051624535568384
5. https://pastebin.com/YBXgiGSS
7. https://www.youtube.com/watch?v=ZyQCQ1VZp8s
12. https://twitter.com/noblebarstool/status/1146079158096687105
13. https://twitter.com/noblebarstool/status/1179481010561523714
19. https://github.com/qTox/qTox
26. https://twitter.com/tkanalyst/status/1193121699002114048
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

Any technical information that is made available by Analyst1 is the copyrighted work of Analyst1 and is owned by Analyst1. 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.