ANALYST 1

A History of rEVIL

By Jon DiMaggio

January 27, 2022

ANALYST1™

Table of Contents

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.[1] 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.

ANALYST1™

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.[2] 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.[3] 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:

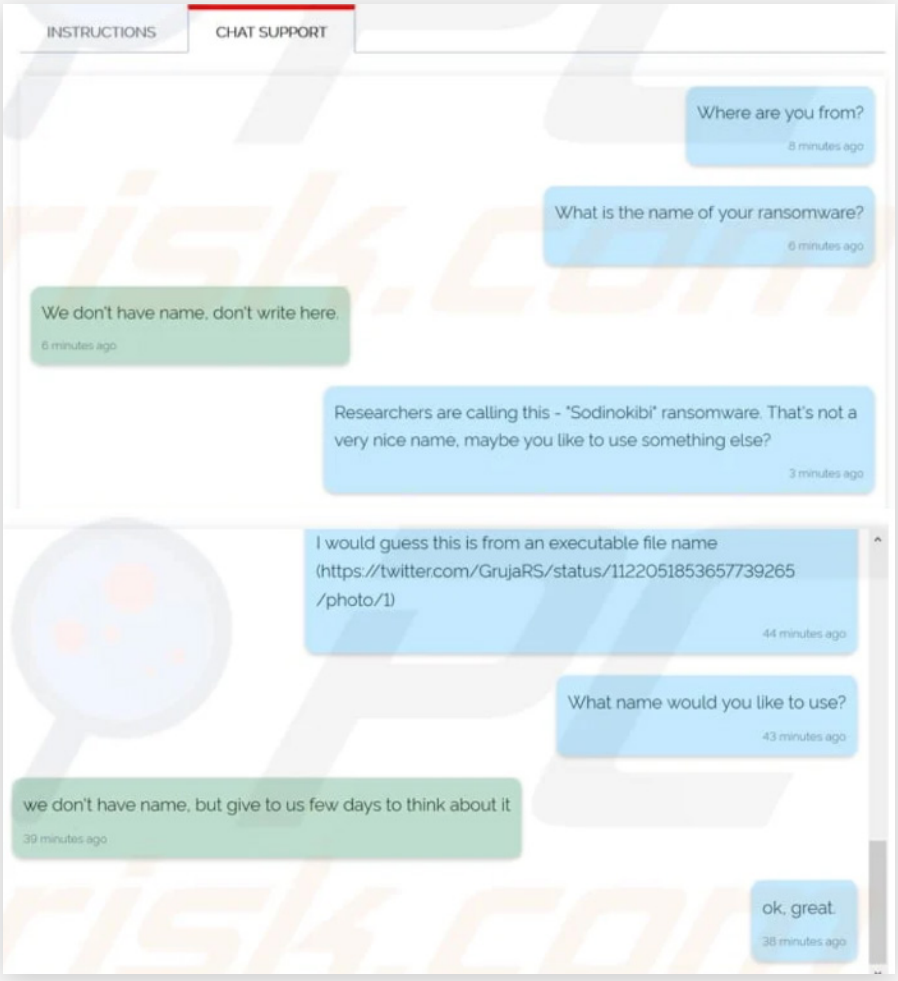


Figure 1: Chat between REvil operator and Tomas Meskauskas as posted on the PCrisk blog[4]

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.[5] In the interview,[6] 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.[7]

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[8] when they allegedly retired and shut down the RaaS program. Figure 2 below shows Gand Crab's retirement message posted to an underground forum.

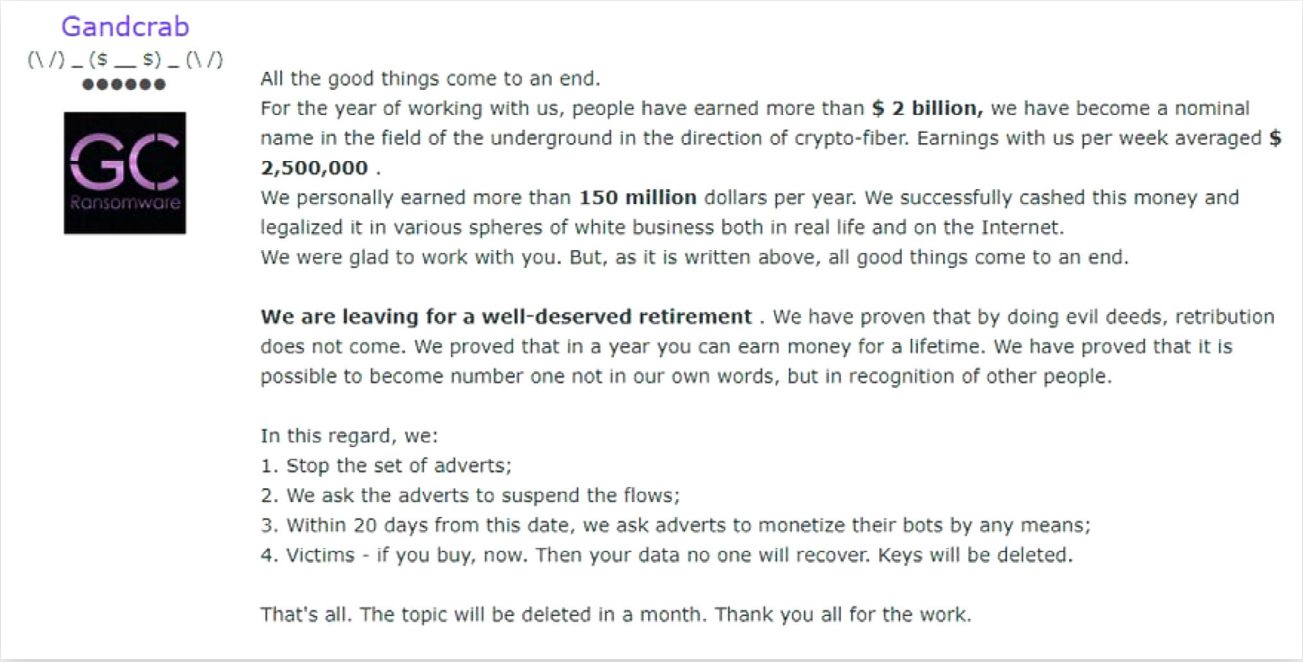


Figure 2: GandCrab retirement statement (translated from Russian) posted on 31 May 2019[9]

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.[10] 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.

> At the time, we had no real insight into the actual people behind GandCrab.

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.[11] 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.[12, 13]

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.[14] 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.

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.

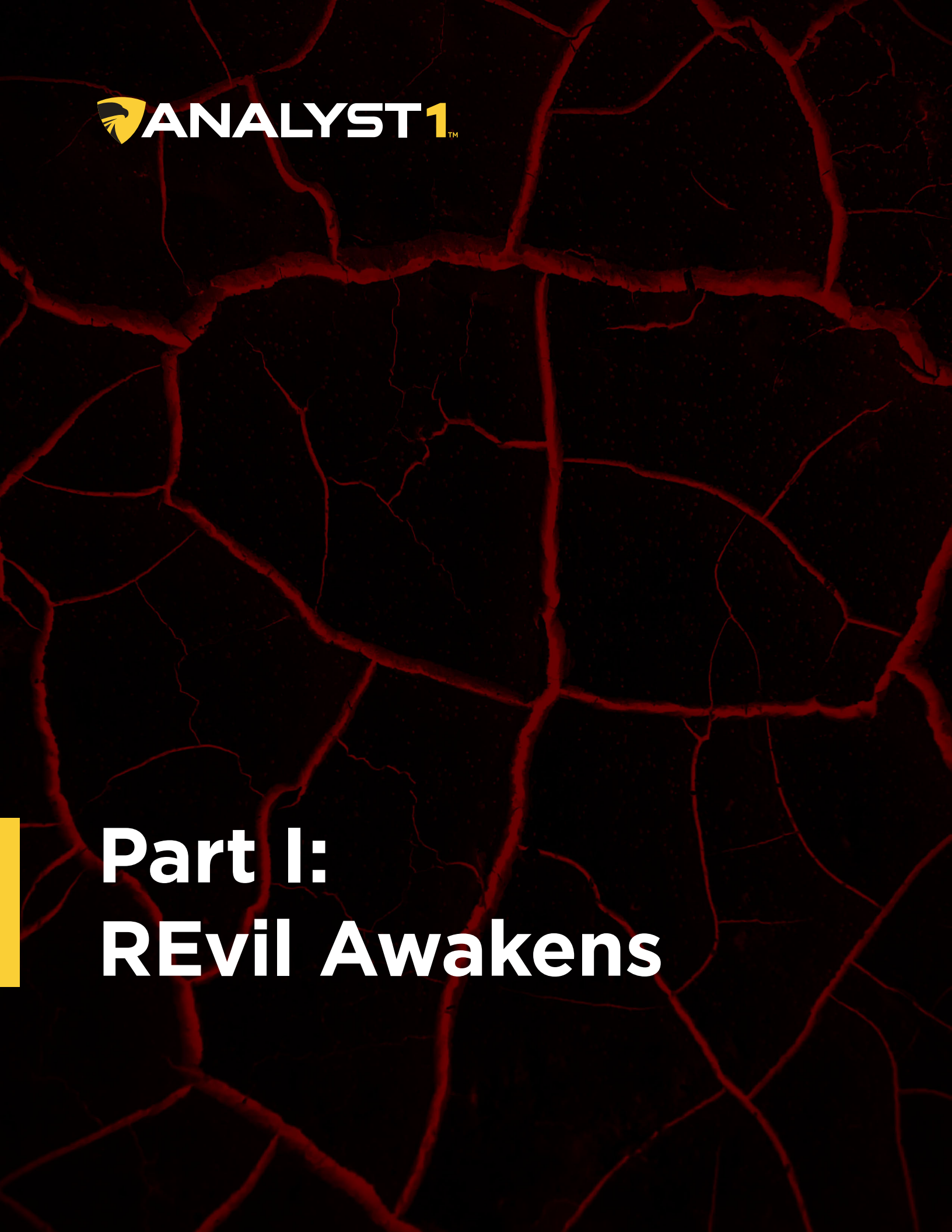
REvil needed experienced affiliates and wanted to ensure the affiliates who supported GandCrab moved to their program. To demonstrate they were a serious RaaS provider and show affiliates there was money to be made, REvil first deposited $130,000 worth of bitcoin across two underground forums where they 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.[18] To facilitate candidate interviews, REvil used qTox, an encrypted peer-to-peer chat, voice, and video communications client that functions over the Tor network.[19] 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. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has
extension 6kom116y.
By the way, everything is possible to recover (restore), but you need to follow our instructions.
Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do
not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for
free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and
data, cause just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
   a) Download and install TOR browser from this site: https://torproject.org/
   b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/
   D47985DD4C1063D2

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
   a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
   b) Open our secondary website: http://decoder.re/D47985DD4C1063D2

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:[REDACTED]

--------------------------------------------------------------------------------

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or
antivirus solutions - its may entail damge of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make
everything for restoring, but please should not interfere.
!!! !!! !!!
```

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:

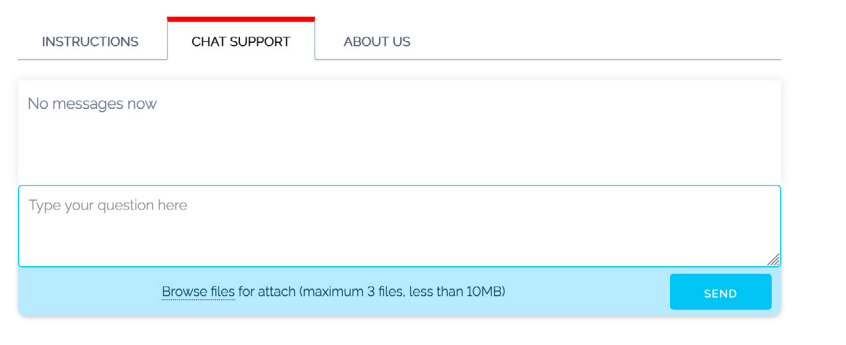


Figure 4: REvil Chat Support used to communicate and negotiate with victims

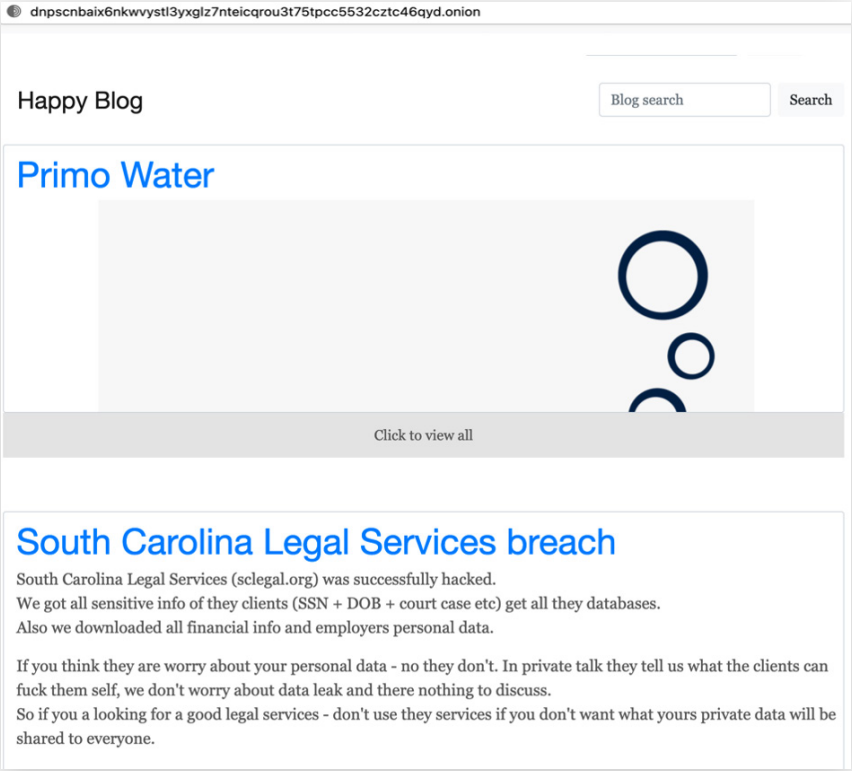


Figure 5: REvil's "Happy Blog" data leak website

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.

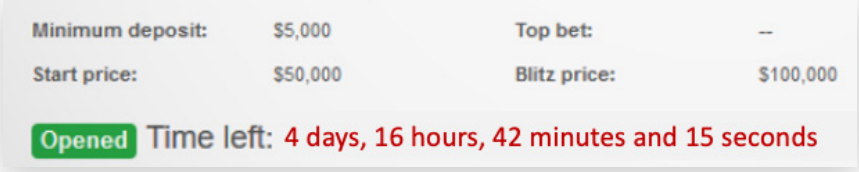


Figure 6: Countdown timer indicating how long a victim has to pay the ransom

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.[20] 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.[21] 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.[22] 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."[23] The result allowed REvil affiliates to gain administrative privileges early in the attack while going unnoticed by defenders.[24]

We believe MSPs will likely continue to be targeted by ransomware gangs.

> **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. Analsyt1 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.[26] In the campaign, targeted organizations spanned several Asian countries, including Malaysia, Vietnam, and Korea.[27] 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,[28] a data center and infrastructure-as-a-service (IaaS) provider.[29] Specifically, the organization "serves thousands of customers across 48 different data centers located around the world."[30] 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.[31]

CyrusOne claims they would not and did not pay the ransom.

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.[32] 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.

Travelex responded to the attack **very** poorly.

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.[33, 34] 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.[38] 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.[39] 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.[42] 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:

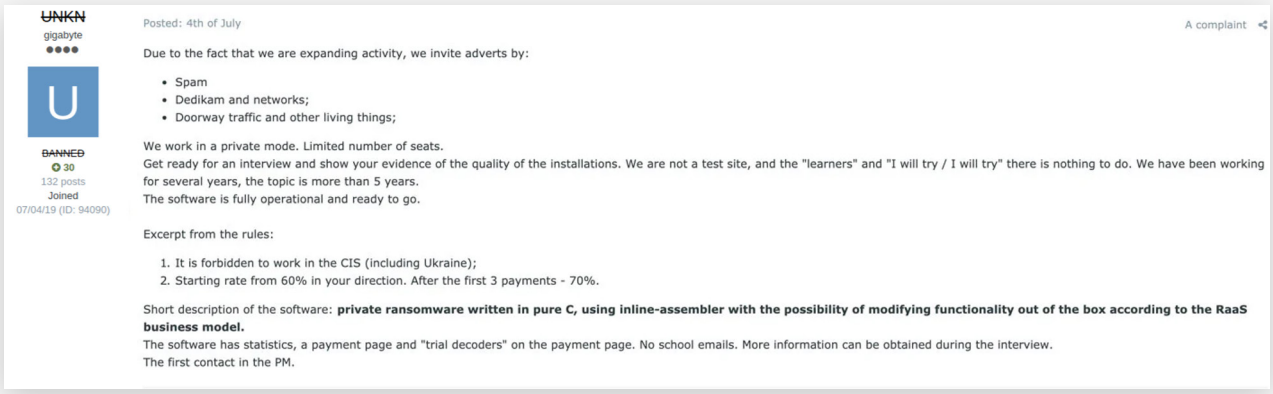
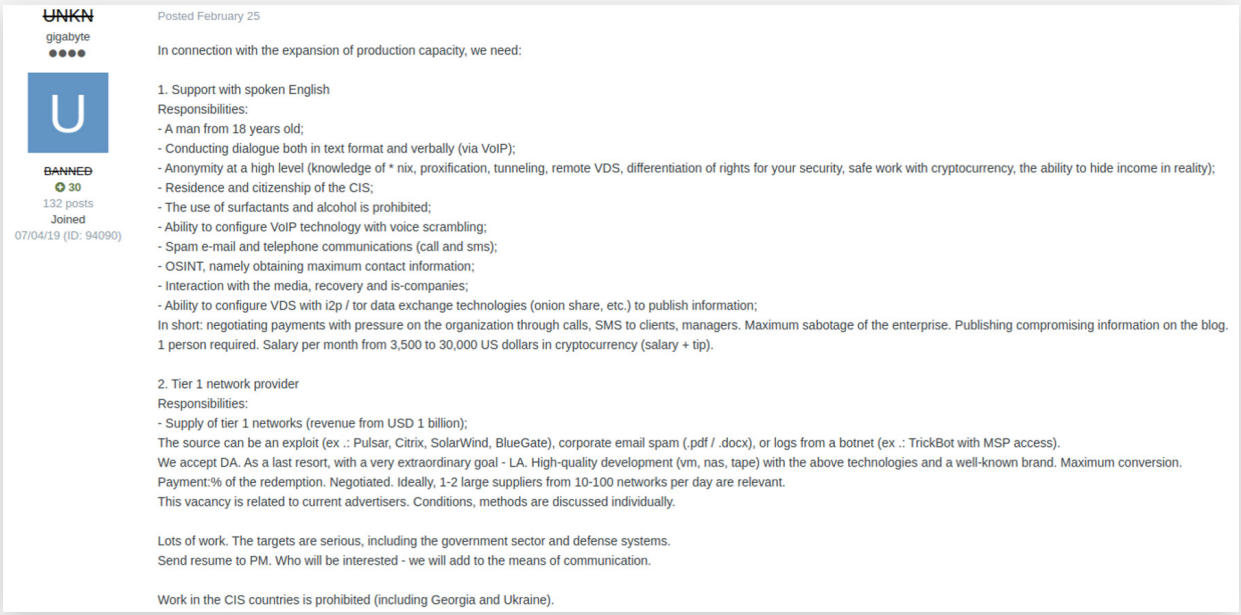


Figure 8: Ransom-based recruitment ad (translated from Russian)

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:



~~UNKN~~
gigabyte
●●●●

U

~~BANNED~~
✪ 30
132 posts
Joined
07/04/19 (ID: 94090)

Posted February 25

In connection with the expansion of production capacity, we need:

1. Support with spoken English
Responsibilities:
- A man from 18 years old;
- Conducting dialogue both in text format and verbally (via VoIP);
- Anonymity at a high level (knowledge of * nix, proxification, tunneling, remote VDS, differentiation of rights for your security, safe work with cryptocurrency, the ability to hide income in reality);
- Residence and citizenship of the CIS;
- The use of surfactants and alcohol is prohibited;
- Ability to configure VoIP technology with voice scrambling;
- Spam e-mail and telephone communications (call and sms);
- OSINT, namely obtaining maximum contact information;
- Interaction with the media, recovery and is-companies;
- Ability to configure VDS with i2p / tor data exchange technologies (onion share, etc.) to publish information;
In short: negotiating payments with pressure on the organization through calls, SMS to clients, managers. Maximum sabotage of the enterprise. Publishing compromising information on the blog.
1 person required. Salary per month from 3,500 to 30,000 US dollars in cryptocurrency (salary + tip).

2. Tier 1 network provider
Responsibilities:
- Supply of tier 1 networks (revenue from USD 1 billion);
The source can be an exploit (ex .: Pulsar, Citrix, SolarWind, BlueGate), corporate email spam (.pdf / .docx), or logs from a botnet (ex .: TrickBot with MSP access).
We accept DA. As a last resort, with a very extraordinary goal - LA. High-quality development (vm, nas, tape) with the above technologies and a well-known brand. Maximum conversion.
Payment:% of the redemption. Negotiated. Ideally, 1-2 large suppliers from 10-100 networks per day are relevant.
This vacancy is related to current advertisers. Conditions, methods are discussed individually.

Lots of work. The targets are serious, including the government sector and defense systems.
Send resume to PM. Who will be interested - we will add to the means of communication.

Work in the CIS countries is prohibited (including Georgia and Ukraine).

Figure 9: REvil recruitment ad (translated from Russian)

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.[43] 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.[44] 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.[45]

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.[46, 47] 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.[48] 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.[49, 50] 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.

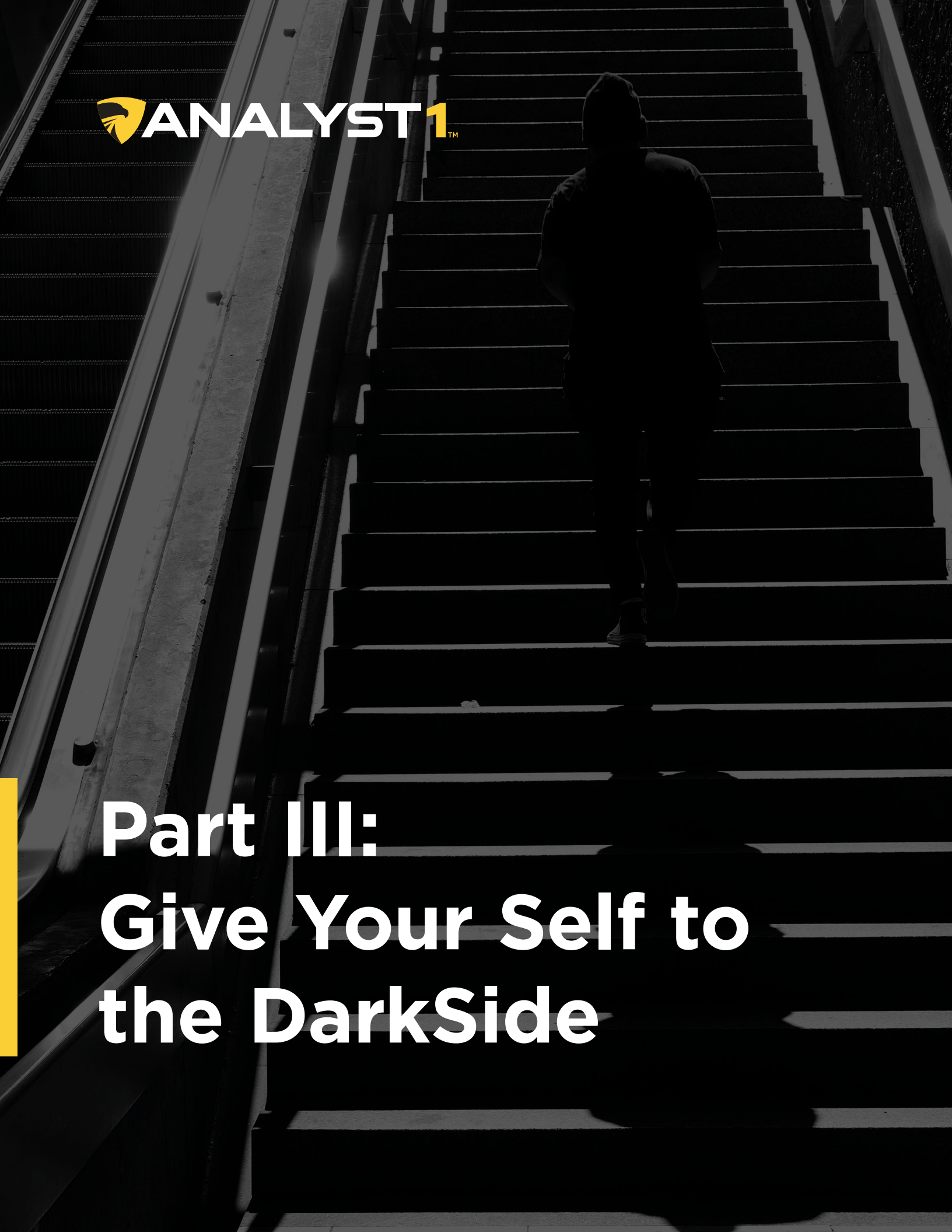
The Dairy Farm Group either did not want to disclose the full impact of the attack or was truly unaware of how bad things were about to get. They did not know that REvil had already begun to exfiltrate and stage Dairy Farm data to their leak site, in preparation to auction off the retailer's data if 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.[51] 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.

Over the next few months, their effort paid off.

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.[52] 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.[53] Quanta denied the severity of the breach publicly, but the leaked data made it clear REvil was not bluffing.[54, 55] 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.[57]

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.

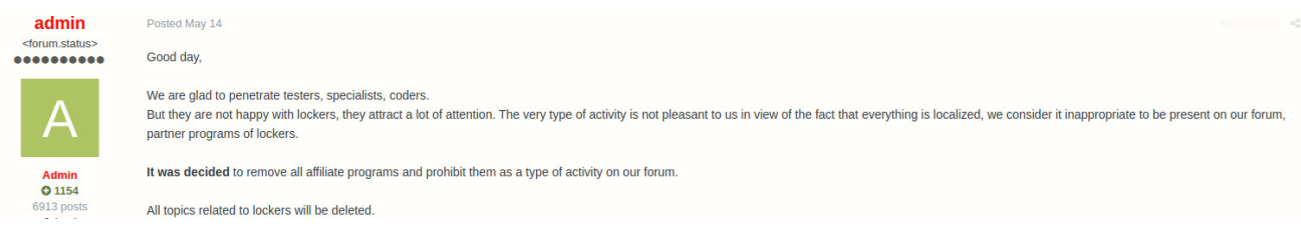


Figure 10: Ransomware ban posted by administrators on a dark web forum (translated from Russian)

Further, administrators banned DarkSide and took their bitcoin deposit for themselves.[58]

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.[59] 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:

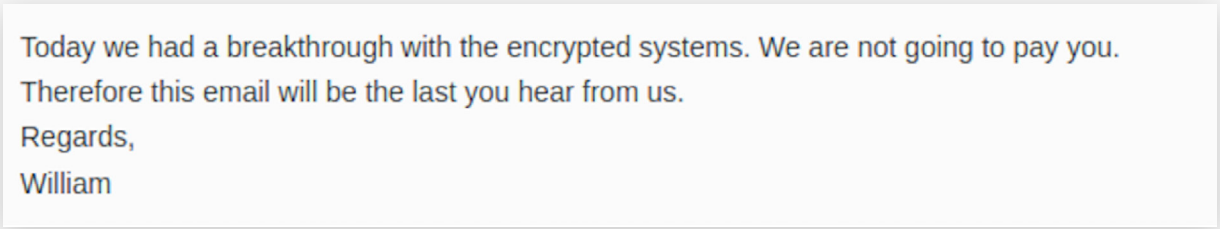

Today we had a breakthrough with the encrypted systems. We are not going to pay you.
Therefore this email will be the last you hear from us.
Regards,
William

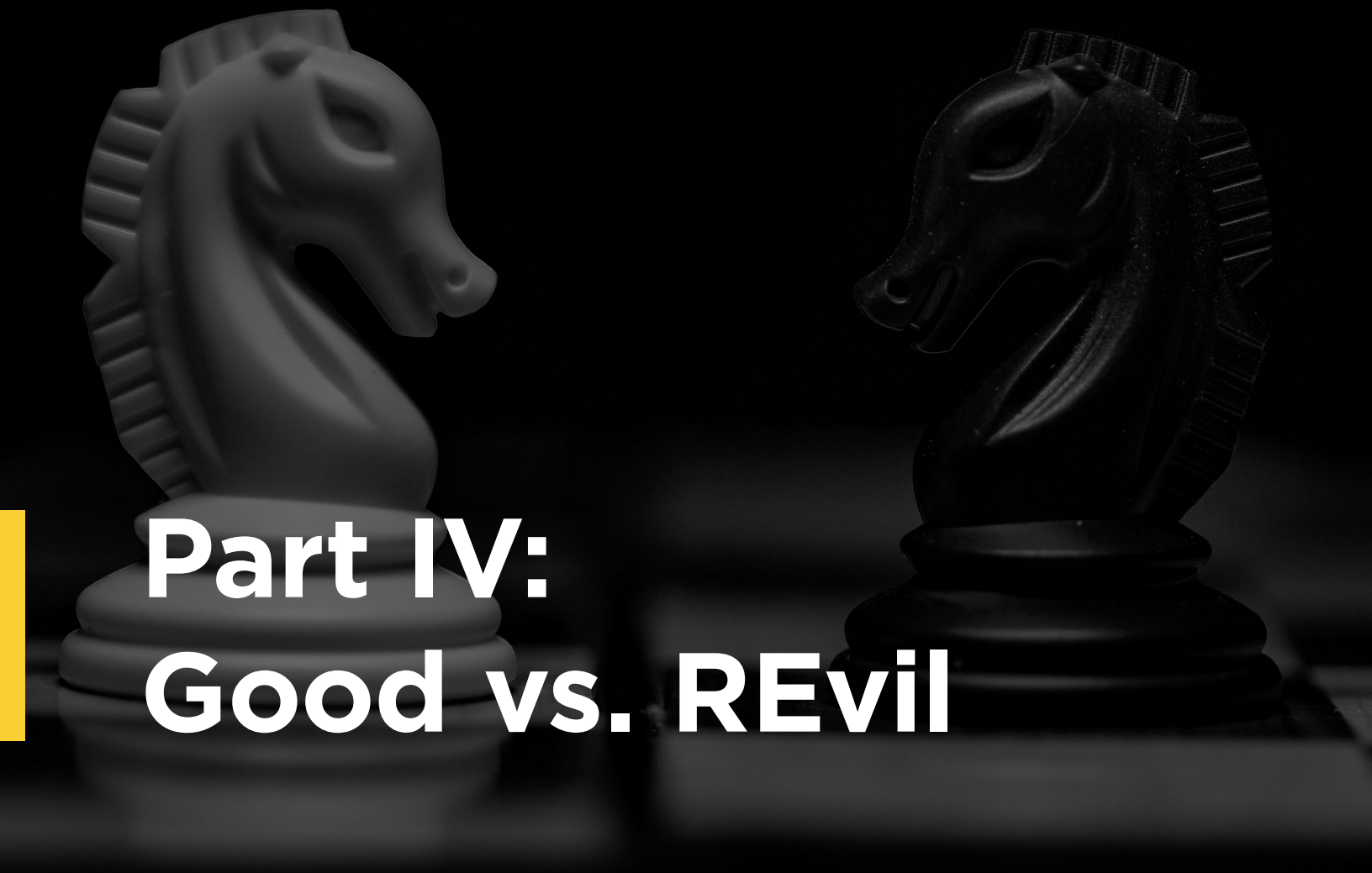
Figure 11: Victim message (email) to REvil affiliate as posted as evidence in their arbitration case

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, deploy 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

ANALYST1™



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."[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.[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.

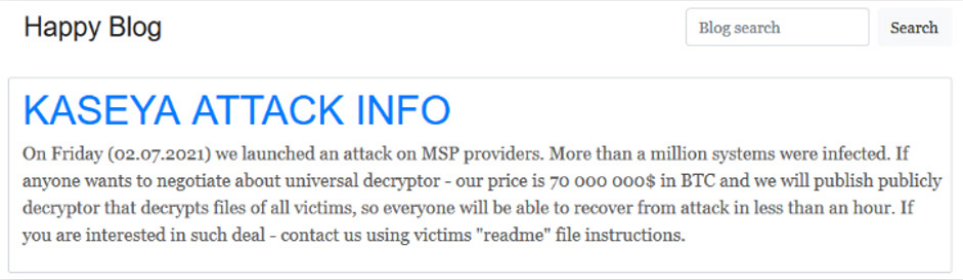


Figure 13: REvil Happy Blog post for Kaseya

Eleven days after attacking Kaseya, in the early hours of the morning on **July 13, 2021**, REvil's infrastructure used to leak and auction victim data, as well as their payment portal, mysteriously went offline.[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.[71] 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.[72] 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.[73, 74]

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

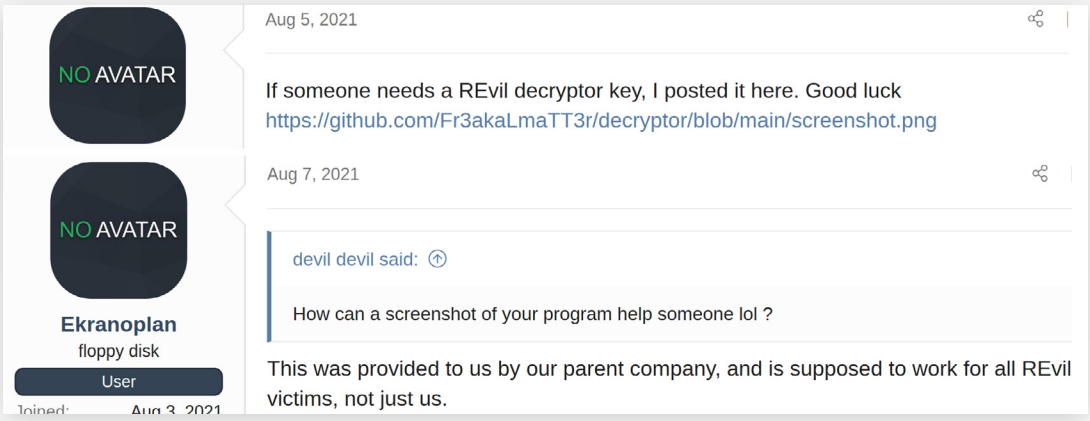
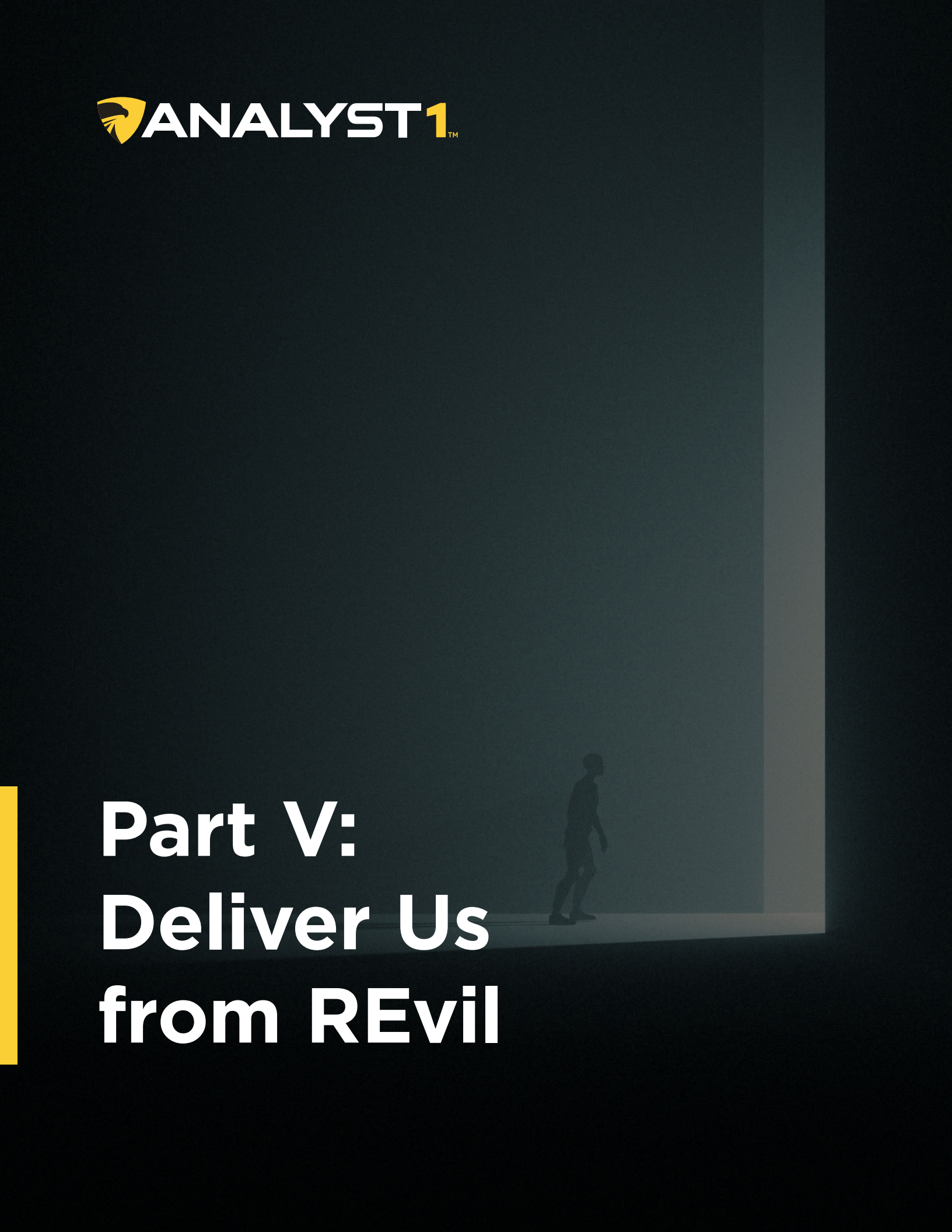


Figure 14: Forum post about REvil decryption key

ANALYST1™



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, 202**1, 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.[75] 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.[76] 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.[77] 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:

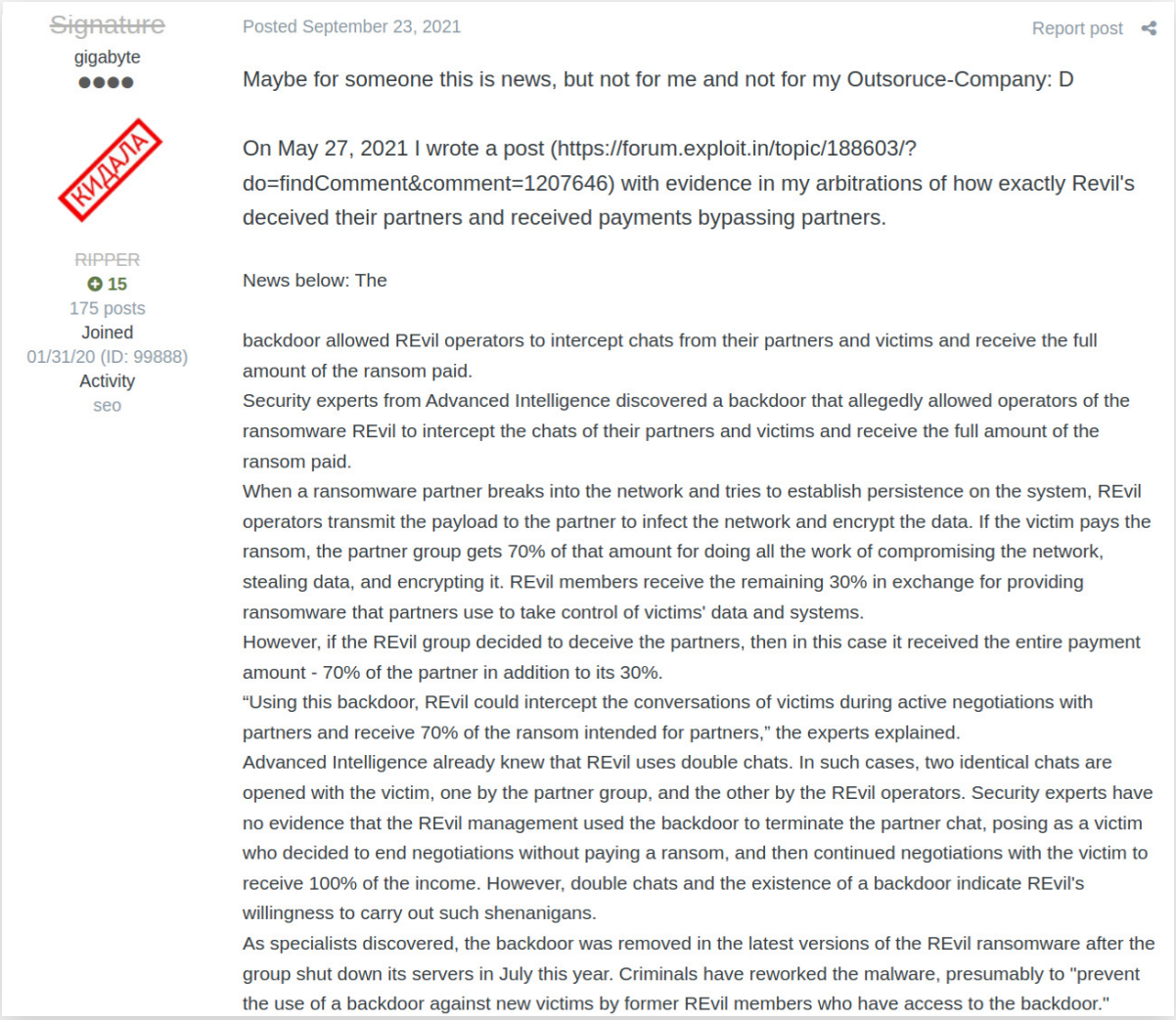


Figure 15: Signature's post following news of REvil's double-cross

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:

```
v0 = registry_read(0x80000002, &subkey, &name_masterpubkey, &type_2, &size);// 1
v15 = v0;
if ( !v0 )
{
  v15 = registry_read(0x80000001, &subkey, &name_masterpubkey, &type_2, &size);
  v0 = v15;
}
v1 = registry_read(0x80000002, &subkey, &name_pc_publickey, &type_1, &size_1);// 2
if ( !v1 )
  v1 = registry_read(0x80000001, &subkey, &name_pc_publickey, &type_1, &size_1);
v2 = registry_read(0x80000002, &subkey, &name_unkwn_key, &type, &size_2);// 3
if ( !v2 )
  v2 = registry_read(0x80000001, &subkey, &name_unkwn_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.

```
generate_pc_pub_and_priv_keys(&pc_private_key, &pc_public_key);// (a)
size = 32;
v22 = 32;
v1 = encrypt_key_by_aes_curve(&master_pk, &pc_private_key, 32, &size_1);// (b)
encrypted_backdoor_key = encrypt_key_by_aes_curve(&backdoor_key, &pc_private_key, 32, &size_2);// (c)
wipe_data(&pc_private_key, 32);
if ( !v1 || !encrypted_backdoor_key )
  return 0;
memcpy(&global_enctypted_master_key, v1, size_1);
memcpy(&global_enctypted_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)***

Hide contents

this is a cryptobackdoor, since knowing the private key from the backdoor (sewn into the stub) you can decrypt the private key of the computer. The public key of the computer encrypts the private key for encrypting files, and having the private key of the computer, the files can be decrypted.
Here is the public key of the crypto-backdoor from the sample
FF5EEDCAEDEE6250D488F0F04EFA4C957B557BDBDC0BBCA2BA1BB7A64D043A3D

Figure 16: Forum post analyzing the Sodinokibi payload and pointing out the backdoor found in its code (translated from Russian)

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."

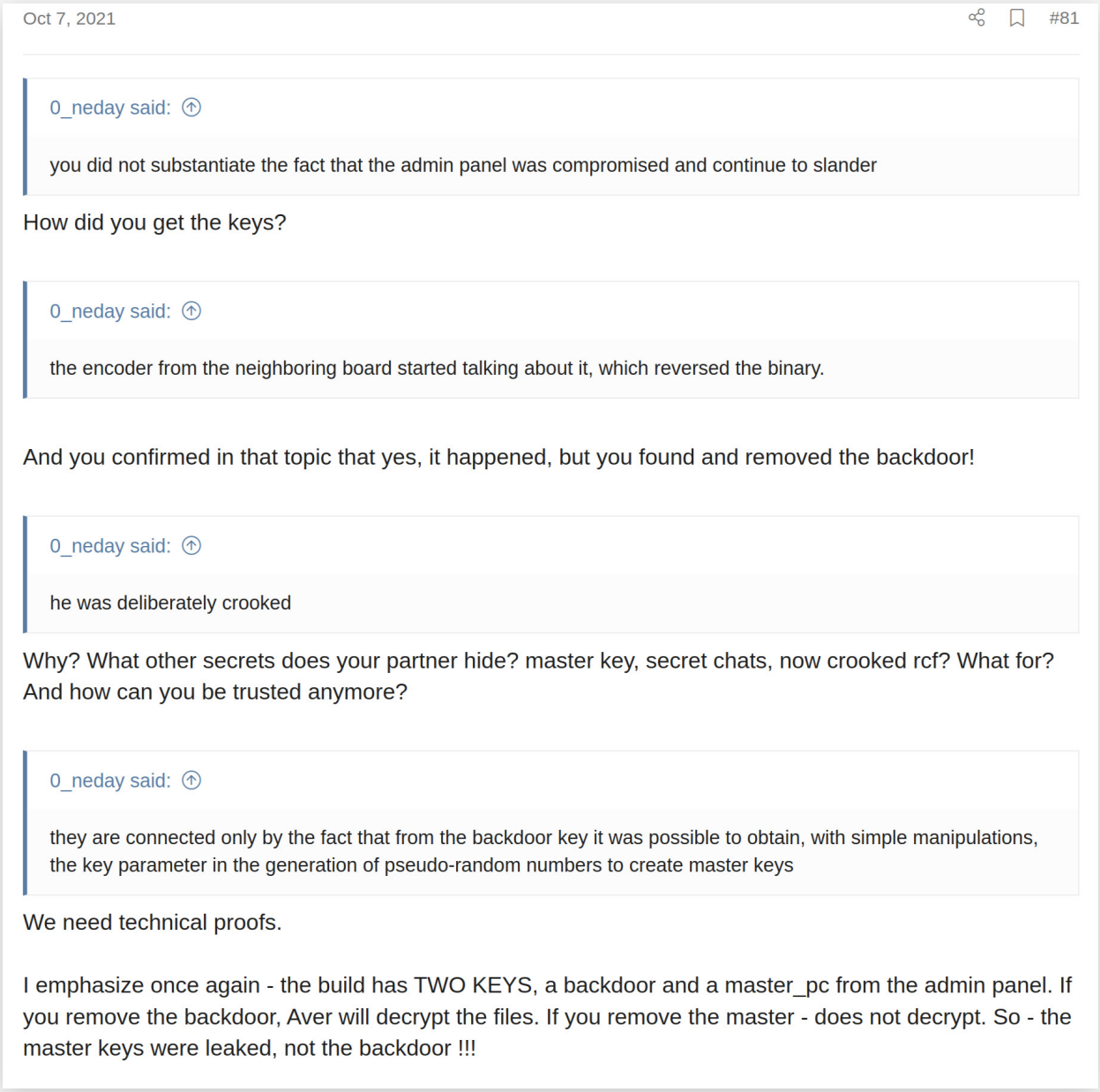


Figure 17: Forum post challenging REvil's trustworthiness in relation to their hidden backdoor used to double-cross affiliates (translated from Russian)

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.

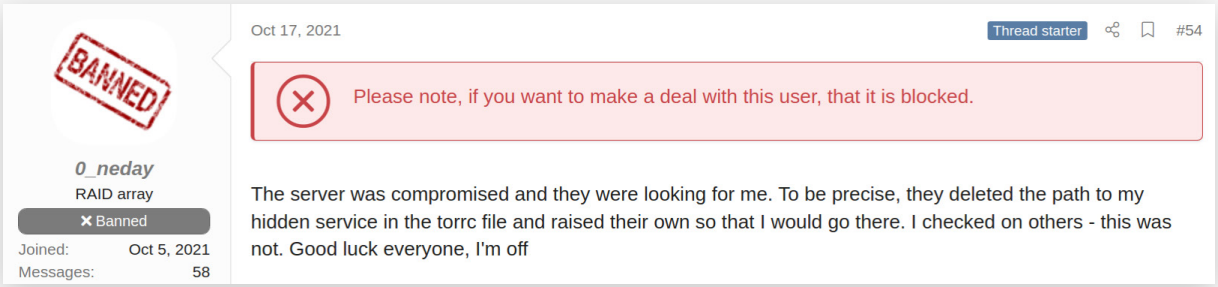


Figure 18: REvil post claiming their infrastructure was compromised (translated from Russian)

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.[78] The first indictment was against Yaroslav Vasinskyi, 22, a Ukrainian national, and Yevgyeniy 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, Yevgyeniy 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.

Figure 19: FBI wanted poster for Yevgyeniy Polyanin

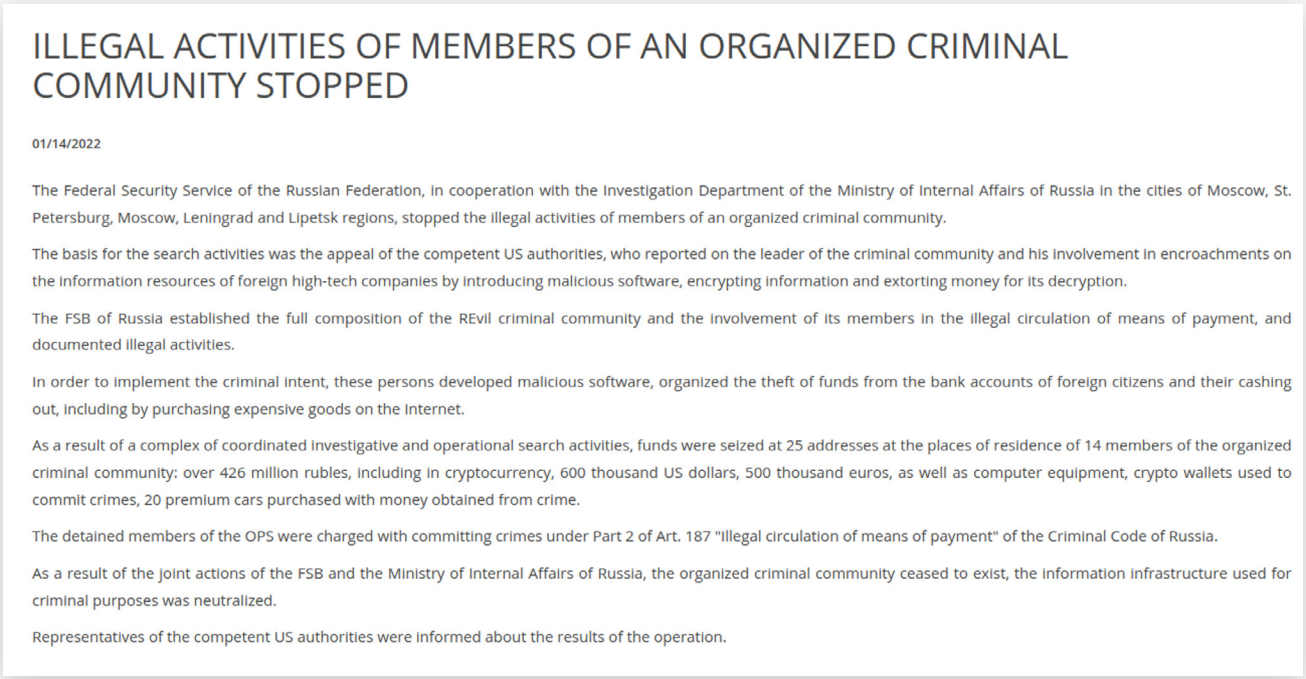
Figure 20: Twitter post from security researcher @3xp0rtblog showing Yaroslav Vasinskyi[79]

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*[80]

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.



ILLEGAL ACTIVITIES OF MEMBERS OF AN ORGANIZED CRIMINAL COMMUNITY STOPPED

01/14/2022

The Federal Security Service of the Russian Federation, in cooperation with the Investigation Department of the Ministry of Internal Affairs of Russia in the cities of Moscow, St. Petersburg, Moscow, Leningrad and Lipetsk regions, stopped the illegal activities of members of an organized criminal community.

The basis for the search activities was the appeal of the competent US authorities, who reported on the leader of the criminal community and his involvement in encroachments on the information resources of foreign high-tech companies by introducing malicious software, encrypting information and extorting money for its decryption.

The FSB of Russia established the full composition of the REvil criminal community and the involvement of its members in the illegal circulation of means of payment, and documented illegal activities.

In order to implement the criminal intent, these persons developed malicious software, organized the theft of funds from the bank accounts of foreign citizens and their cashing out, including by purchasing expensive goods on the Internet.

As a result of a complex of coordinated investigative and operational search activities, funds were seized at 25 addresses at the places of residence of 14 members of the organized criminal community: over 426 million rubles, including in cryptocurrency, 600 thousand US dollars, 500 thousand euros, as well as computer equipment, crypto wallets used to commit crimes, 20 premium cars purchased with money obtained from crime.

The detained members of the OPS were charged with committing crimes under Part 2 of Art. 187 "Illegal circulation of means of payment" of the Criminal Code of Russia.

As a result of the joint actions of the FSB and the Ministry of Internal Affairs of Russia, the organized criminal community ceased to exist, the information infrastructure used for criminal purposes was neutralized.

Representatives of the competent US authorities were informed about the results of the operation.

Figure 21: FSB Press release about raids on members of REvil[81, 82]

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.[83]

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.[84]

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[85]

ANALYST1™

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.[86] 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").[87] 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.

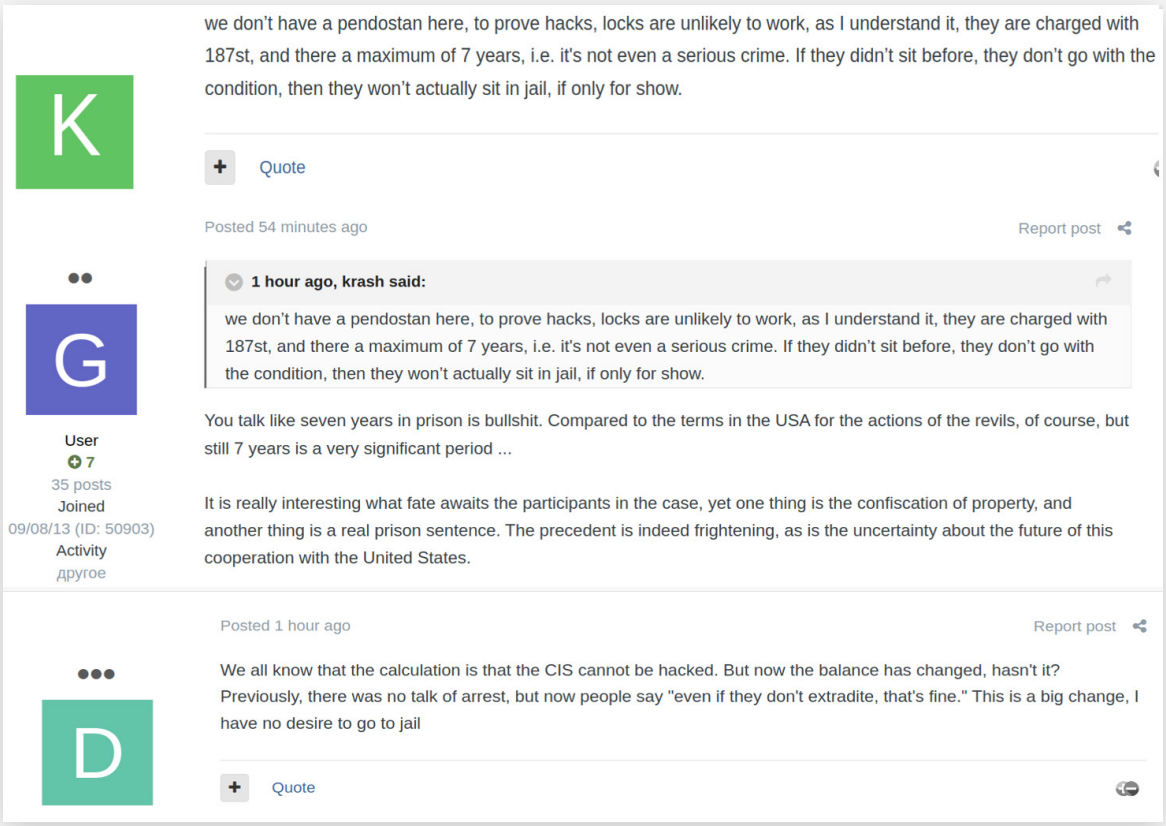


Figure 23: Messages on Russian underground forum used by REvil that discuss the fallout of the January 2022 REvil arrests (translated from Russian)

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.

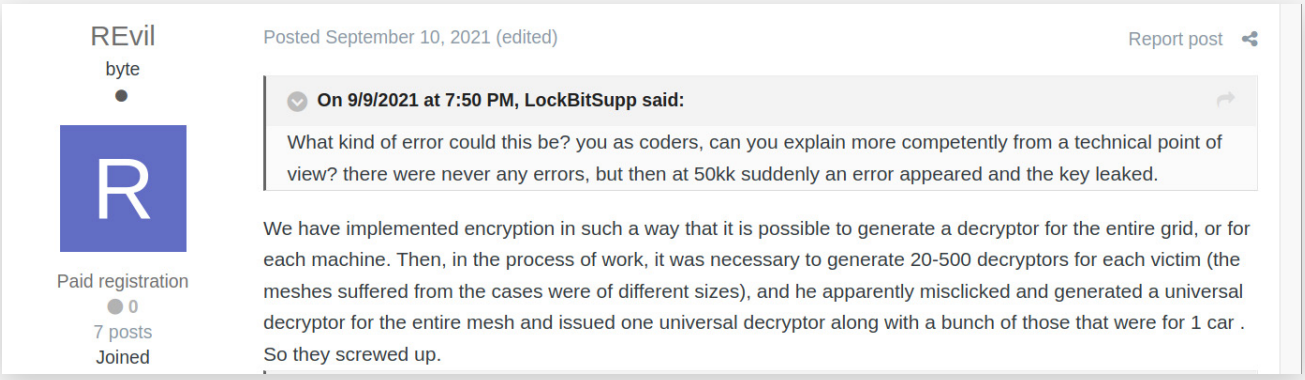


Figure 24: REvil forum post responding to LockBit (translated from Russian)

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.

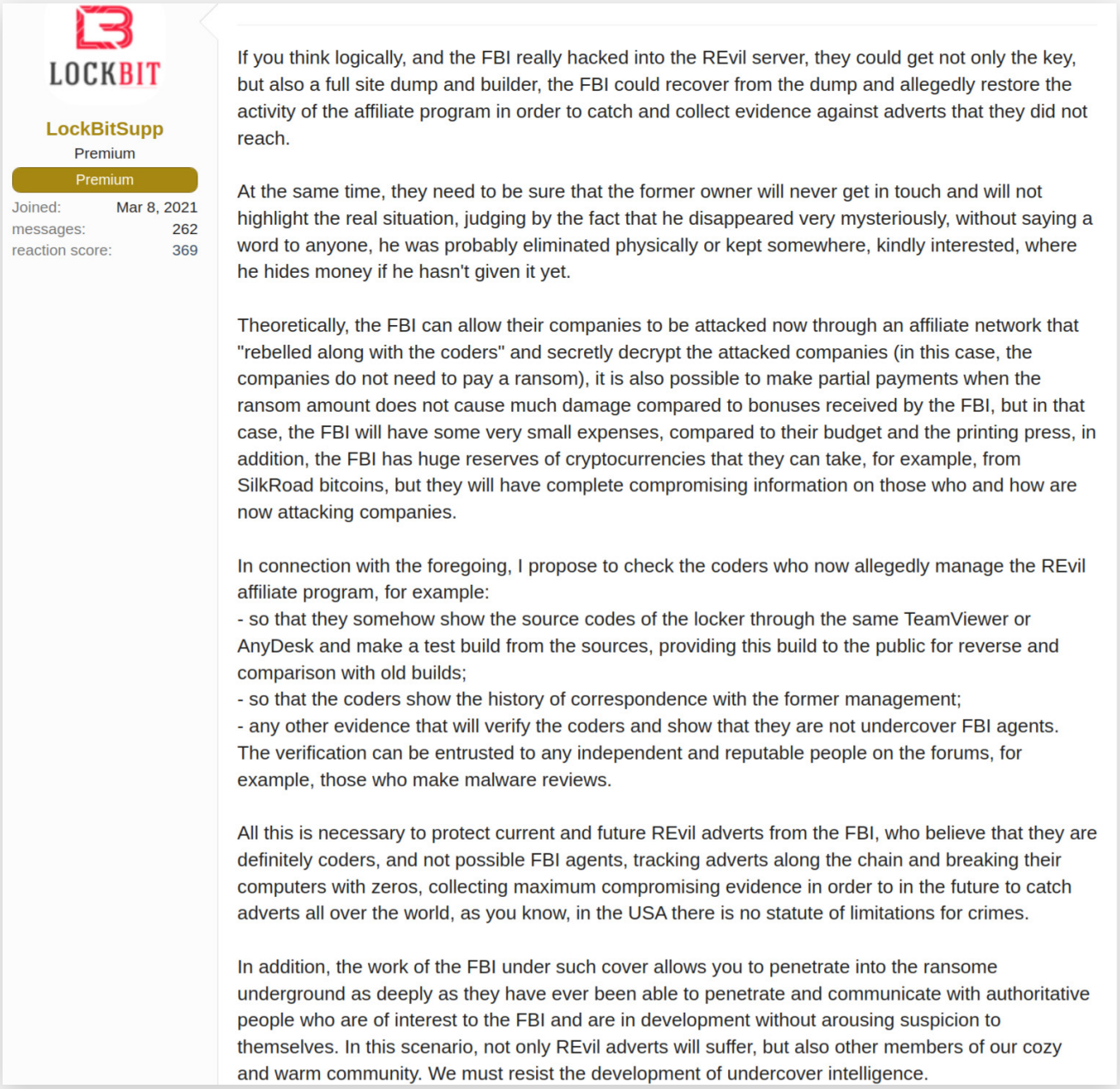


Figure 25: LockBit post calling for better operational security and vetting of both ransomware code and the developers who create it

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 0neday."

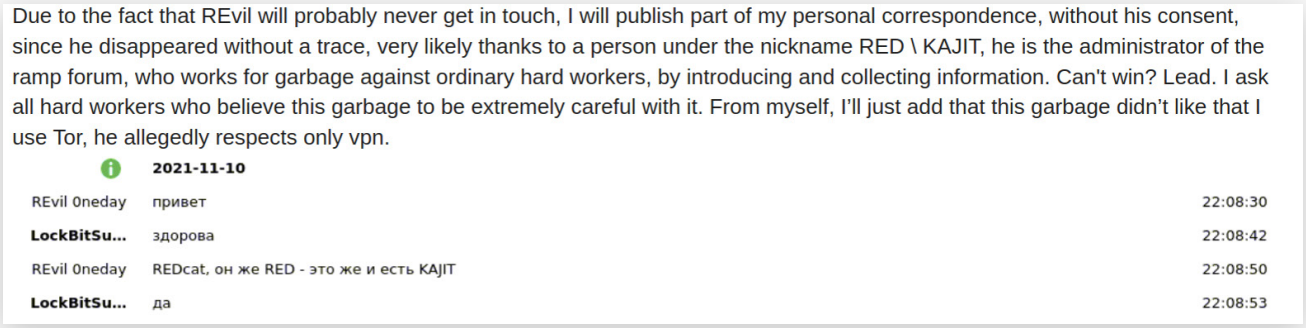


Figure 26: Post of private conversation between REvil and LockBit operators

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

33BC14D231A4AFAA18F06513766D5F69D8B88F1E697CD127D24FB4B72AD44C7A
2896B38EC3F5F196A9D127DBDA3F44C7C29C844F53AE5F209229D56FD6F2A59C
64076294E761CEE0CE7D7CD28DAE05F483A711EAFE47F94FE881AC3980ABFD8F
45B6349EE9D53278F350B59D4A2A28890BBE9F9DE6565453DB4C085BB5875865
59A2A5FAE1C51AFBBF1BF8C6EB0A65CB2B8575794E3890F499F8935035E633FC
56DE41FA0A94FA7FFF68F02712A698BA2F0A71AFCECB217F6519BD5751BAF3ED
538078AB6D80D7CF889AF3E08F62C4E83358596F31AC8AE8FBC6326839A6BFE5
B1B00F7B065E8C013E0C23C0F34707819E0D537DBE2E83D0D023A11A0CA6B388
E35C31BA3E10F59AE7EA9154E2C0F6F832FCFF22B959F65B607D6BA0879AB641
4B25F708C506E0CC747344EE79ECDA48D51F6C25C9CB45CEB420575458F56720
11AF3609884AD674A1C86F42EC27719094E935D357D73E574B75C787A0E8C0F1
8D44894C09A2E30B40927F8951E01708D0A600813387C3C0872BCD6CB10A3E8C
8DD620D9AEB35960BB766458C8890EDE987C33D239CF730F93FE49D90AE759DD
1FE9B489C25BB23B04D9996E8107671EDEE69BD6F6DEF2FE7ECE38A0FB35F98E
8E846ED965BBC0270A6F58C5818E039EF2FB78DEF4D2BF82348CA786EA0CEA4F
81D0C71F8B282076CD93FB6BB5BFD3932422D033109E2C92572FC49E4ABC2471
0496CA57E387B10DFDAC809DE8A4E039F68E8D66535D5D19EC76D39F7D0A4402
66490C59CB9630B53FA3FA7125B5C9511AFDE38EDAB4459065938C1974229CA8
AAE6E388E774180BC3EB96DAD5D5BFEFD63D0EB7124D68B6991701936801F1C7
CC0CDC6A3D843E22C98170713ABF1D6AE06E8B5E34ED06AC3159ADAFE85E3BD6
D5CE6F36A06B0DC8CE8E7E2C9A53E66094C2ADFC93CFAC61DD09EFE9AC45A75F
D55F983C994CAA160EC63A59F6B4250FE67FB3E8C43A388AEC60A4A6978E9F1E
D8353CFC5E696D3AE402C7C70565C1E7F31E49BCF74A6E12E5AB044F306B4B20
DC6B0E8C1E9C113F0364E1C8370060DEE3FCBE25B667DDECA7623A95CD21411F
DF2D6EF0450660AAAE62C429610B964949812DF2DA1C57646FC29AA51C3F031E
E2A24AB94F865CAEACDF2C3AD015F31F23008AC6DB8312C2CBFB32E4A5466EA2
36A71C6AC77DB619E18F701BE47D79306459FF1550B0C92DA47B8C46E2EC0752
45AEBD60E3C4ED8D3285907F5BF6C71B3B60A9BCB7C34E246C20410CF678FC0C
FF61085FF157EF0A98AB65A5343E65637EE24E12CAC3B418E45532FC2747F3E5
FDDDBBC09972A8DA879209F8B45796B4343FFD8C74AE8E56BFE78AEBC710777B
FAC5D96467B6B9725B412D3B78EB52E3FA71BE748579896774DF3F86BE1FBA4E
F92933369385D3E441642B60857A102B91738351630A10BB4194CB1ED65793B7
F1BC14943C240F59B8D3AD4D6E3AD5568F896F80E79697E690612C5602FA653D
F195FB77843E110FF91656C09D277563EE32C2D36388E556F25328BF0AAC80BE

F0C60F62EF9FFC044D0B4AEB8CC26B971236F24A2611CB1BE09FF4845C3841BC
EB486E276B6FB580C58508D71D303B0535970AC243021EEEDE55BCD253F114CF
E7DDB20095CD733EFC10FBA3FF1A8B3E83767CC900B5A976D4029456226612B0
E713E3F1E74DF404568466E88DBFA1BE33C917472830CDB54CE803DFA8EC3FF0
E630185053EE119AC973AA341C74FB1A9006B7F1A58E9F4C47EFB1DA9DD7BC0C
E5A9E0E9EAA33CE2AC37AF1894986B5378267BD98148F2FDB762EF627DDED3F5
E281347D6FAF8FA17E9BCD79D0F815187506C89E8BCA9FFAE78170E31FF07438
DE0B6C17C7C921FC515BBDB7ED2FDC1F1069860CFE2B611C105201A916D0E87D
D4E89180E559721E6BCD9C03549D540282C3774BDD6AE61A61D57A23C10FC299
D011469083D12AD3D94925DBCF113136039A5B53D70E0F99FF04267A4BF80B6D
C73116292F7373E4271D58B48FBC64FA031C8C2C5DA8745A64E86D4625FF54AC
C6D72DBC8C2CA62471A786A4A00E771D8683A7C7429D2C67F059315CD6AD443D
C407C0DB2F79F607DFDC5EB2F4F222491F96EA3540D8689C8ED6FBA89A240757
BD4BCC8CB3E33C018A4D9037BF5CF9BD6F7CE0A5C4B862E94C098366004563D4
BBCA6188AAC86332E90673E663F91F3097A63153835B4F9D058E90BAF075012A
B6E27E49D83F82F0FEAA1B41D7B8906B9237E08968BB2CD5AE6F4F97B4C9F5C8
B6A2162E86DBF9D501555377A6262BA63F5D1FF87D47A284BA3E8A9D7EF26CC9
B4436606C93AE464876A0E229342503CF754D9951D61D9E2E3FCBDF680FDFFC4
B202927E24727AC2677F9635DC7BCFAB8E812B3F74F85D40F198642D182D671C
ADD230A2E7AABF2EA909F641894D9FEBC6673CF23623A00CE3F47BC73EC9B310
AC3E29E3C35138E857BFFBC8CF5F8414B71C5694E7E13ABE59620D2BDE408887
A8D1D6CF7E591719401DF17979782244D70DBF59823C889F5329E1F2BCFCA1E1
A8928D557ECCDE515B1ACD7E326D073684690D4BD7538B6842F0F4C48120D984
A88E2857A2F3922B44247316642F08BA8665185297E3CD958BBD22A83F380FEB
A6E3D32365196D053A488D68D00ADAB68F4953956FDB1FE0CC5915A0C4848E14
A6C1DBA2085634D0A104551CBDB41F6652DC8A7ABA9A40BE094E971E310F38A1
A389E24BF0AF9BC81B8133A600A2B6C875D32AA0885964D0B9F3AC6DB5FEE762
A2FBF151010D614AC772D2232E94FAF278F2AD9F650197987A0E2A4DF2CC892E
A2715F4FE971766681C17CCD0E045F87F7B09D4D57ADB99601078EA5C8BBF68A
A1B4C2B6F0311B510119B8B7D5394CB63EE5A983588462C1E798EB9F3471687B
9FED4AEC732E2B564F0E63F37893B3C00DEAB31580580EB3045541A05CAE8766
9FA3A004576F357B5174DD1C29EF7D13005D996D5F9FB4B86D6D978D1A4A84AE
9E31D426701CF1E9CA72F71E88A3F50978AB2D67088E96F1C3B954DF1E673BDF
9A995D6A6A6764632E7DE12E48462B352C04D81D1CBF30920FFC55F9B0AD8794
984E8A13D4AD8E1DCA468337ECBA4F221688EF6B96E9D1238E5C1BC92E4DC3B7
97612C95AA764CB2A4DA61DD6C25192EB2DBC8D8D75D9D0FE57FA0101157E28F
963E31FEF7C8DB9E002C56EE30FD3CD4B240DB466BC23687979E2F161BA5606E
95F29F45C33D66B22E71B0FC0C1C03F7415F08B30DFC9BEA0902C19D29A0B137

9539C6B525E9EA6F0D84979A7285CDBA416BBC134C0D6985FDF5D86607B30383
938248B6428D12E57D4BCAD2C36B369599B5EB7687F16C0998CA967D9C8E228C
917F1FEEA1242D962205BA1827D036F55482E83AC4008A84C518479A3364D4E5
90C9B6460C240177644D028458874167FEDF7CA459381DDE17D44446BB9BA501
8C8481C65F40FB55FCD8AA077F3D20702F366C365E276AB7C3FA03A98310A277
8AB99AC368B338310CB1E130D9971AEDCDD3B79E5C7143E8B4B0A8CE894F9C78
89D80016FF4C6600E8DD8CFAD1FA6912AF4D21C5457B4E9866D1796939B48DC4
87883AC1EF972338D4E632F4BCA5AD222F21D95F77DFECACE09F30FEBA37D173
8704B9BAEFE5060C0622B14A3930B8901A0CC5CE53F9395B1F2CC3EFD7D5BD69
861BC212241BCAC9F8095C8DE1B180B398057CBB2D37C9220086FFAF24BA9E08
85D76BE0E7A1F112D8B7E221F5F95CF6A665338F96CEAEA1FE495C7903AB4A61
84F909F2A044110A830148D98D47351342A2F1C9D5F75E6B8801FF34C9E9FA98
834CEB76DDFE5549B0DD8E10891949E9FC4DC23B68517FCE991D7EFDC7AB8EB2
80BBE933CC68FD5837B0BA84F17B9F796918125C52321D3D504468E837239765
7EA8DD20165E86544214BD59B7AFC09872AAC6DACD41C5C1683C3CB86D88B9F4
7E959A5F638FA02C0C29D21E3076C987A5A9E1AAA6024C3A47167F1398387F44
7D0A7B508D1CCC7CE49B234A25BFF26C487A85EC7E81DDF6325E8E301516CEAE
7BAFD5DE1B6724962AB920F71031978A101055F061AE3CC21DB8BB9FA64C5829
7A512C1DCA5DA7CB27D59E002A3AAA42073BFEC1AF23AD8CF73F967617A2A9DC
794DA0CA9DD97421AFD80B3F9AAF6E25DCB969ADC296825A439FEAC58A77025A
754C6C376B1E322E03FECAEAC592971CC2A07F614D71529939A46046D1D87695
7047DF7A1EFE3C1CECC26445B59AC74FD912C9E77EE01F74D653DD20D5EDBD0D
6F286E8322E4799F8AFE0F431DEC82E955F193E68E81D1EC0A94F7597840317C
6EFD9AAE5E112418BD43AB48EC4A1FCE191C7503FCD11FDB95E89AD0217ADB7A
6EDEF9C0343C53EF394251A1BF0A890BFC0C51AEB283D0A4A4B15C5294EF484D
6EB8E811BA663FFEE249A3DEBC32646070D3662C34CC99A5F580C750C46C71ED
6D642157D0C3FBB0BF52C8920D5F06B40B907558645D53F8C18C48746D17BDD4
6CD6C3AB26DBC9E0725D4DB991895F4B48AE3C6B3D3C67D98DADCAC81C7CDC5C
6727EDBB5D6ABEE908851A8C5FD7B4ACA6D664634FDCDFC15E04502B960ABBC5
61EA9401C86F28DB49A766B180B1B43335DA1AADB9E8CFF5441670D05EE8A0B6
5FE8E804CC0E7D211019BF37DBB18E4A00AF24BE11CC9407FAC6D648C01716FB
5CC16295598BDC30829A906F3187A60D3C52E7A939ECD2B4DBB4E810EBC281F5
5C959580ADF1FBDFEA872ECE4D29EE6A8319A88273A9923988EF8BE4197833BD
5928DB8B7B1714EAD51392AD809242CD5A158DEFEFE5309F3AE0238C20A500AB
58CFFA69E8B4F26209DA073A6B8CBB6EDE9B2A3F7646D08C91B11DF729A6B9AA
564D9DD23E81BB35EF2C6D8FF8976C9CD88A45291430B3758ED475E5D238C5C7
51F7BCC2DA2C7A0704F1F537C42279B0FA3D3A72808BC8938880DE88B21945B9
51923EC74555541E3567F87BDC189934003B9D32403840CBC1FF5F8B2DD4DF05

509C851E9914E818E1B925C9B60126B40B66B0B57FC3C7A3ECC46D28DCFF5527
507F7B533834CD9445983A89766CB35C6F71857658D7F7B028D4FFBC941CFACC
4E1317C219C4BF78403E8E8D78C694598996236F629B96C904AE02FA05764A10
4D3FB0E2D5BA3F2EECBB2AC62A0A73581C57A2BE39246D861657F21FE2D2C6E6
4748E9729F2E0B1BB151950CDAA75D51AD74612A1C12FF124A492A9A67C2F49B
41050EA37693DB3F76887D9FBCC6B2EEFD4357AB7F49E3CCCF682B5AF49A68BC
3D96D4D5E89B643897CAD61778F54F8741338A3F3F9ACCEAB965C417B35A74BD
39C70F85E6FE3000CD7383E324B705B6A709171E07DAADA3E2D56B2004D33B53
36FA3F72AFC2DD6F206A295FC618038FEF5E241BC48BD5451AC9BAB9128734DD
34F01B17B678FC4BABCEF41731D708CB16BC33A284D87B8675605D0BAFDEB20C
34BA7E6DD88471C7AEC1612270ABD57D445030906375722A78A9E73CE6097FDD
32A72F3BC54B65651EC263C11E86738299D172043A9CDD146001780501C75078
30D11E193A44C2A9807B073854DE1370977AE7C3E99B0243F83D34B261EB2B9E
30980F00BC1BCBA4E2EA3E32EBD7FEB759C87FA2593A6164BCCDDFCB26846933
2EA781140F7E86C63B636249B5FDBA9828661BDD846FD95C195C5B986B84A507
2A995CA24AF128EDBD324BD501C205E8F788E78A0FEBD23B4F9249E6ECA1825C
2A55B2836DDB2EB3AFE78E360D3E59DE661877939F62A47FC9E72186FC9B69C9
245F43B7D93D48E12DB0082955712B7A229127FDD37E5B162007DB85C463CCA6
2181579E0125E8087A3269EE8A90A973307F67ECEB7122FDC7463DB6BC5050B5
207B3353FA8BCB64966BA9F126E62753A00D22AC3702F2BDD34EC658D6D6144C
200D374121201B711C98B5BB778AB8CA46D334E06F2FC820A2EA7E70C251095E
1F7B15F6CF07C5943CE8AB5BFD0700E4919808FCA4260FFD2A509100D45FADAF
1E1653773E590EA0CFDA3B5E772B1F03C9A08A3CD595061100E2F2C50A3053A5
1937098609FBBDA1B470811A7FFE5FA044058655722D84BD029050D54F2B1496
17FFD90D20CBD49C4E0D65A484EEAE65A107D5BAD9582AFC51C4EAD8BBC147E1
17D153A225EA04A229862875795EEEC0ADB8C3E2769BA0E05073BAAF86850467
151271BF05310F94CD33CBA3EB90BE264EDC4828C04E4E82F492B8E2576EE7A6
1501F261A66EEFCE47DC47CB8A426107C4B694A41B5B9FD000D0AD2EA76D8E34
139F7532810E92346FF3B103064A26E460DEB05005104CC30F9F4E2B3EAB595E
139A7D6656FEEBE539B2CB94B0729602F6218F54FB5B7531B58CFE040F180548
12096093901347150AC72D6C9C1CBACF4DE7D6A51EF1AB4CDDC06F85311DD8AB
0E375AB01A08CD6827CE399F43CBF35B3495EB4AE45FDBAD18B812513B68AF94
0AEBC3C9DD12779C489012BF45A19310576EC0E767AC67D1C455839302465AFA
0AE199C13E033F6E63A388151E33C00EC374E1716A40E4BC1769B9CA559852CA
08542EA965F7AC97C90635444860C5D35A8E8E81C7EDF3DDBF6C1736A8C61B63
0832B9544B38AEB0E7731CFC3A676365224472A62D3628A0DFB838D3E5202E1C
069D993C71E2C78FD73FDEF9CE4CED7FE0CE1B49F458A3EC3FAE53208D382F3C
064B5A8A6527E9B7B857C78417C9701CCAB7F6FD0CFCC367AA73A98A91E1F6A2

046A416F4A41DA0874C49C2F279ECC5D27F196E8A9086F9F250830C570113905
00D015EDBFB34E16B5B4086D25174AE435CA86D8CD267E0ED9B32DB7D1D8AE2F
25AC4873AE4F955032F8F0E8ED4EC78DF2E2CE814454B7B5ABD9489FEB4E30C3
367D49308535C2C368604B4B7ABE8353ABE68E42F9C662A5D06AADC6F17DF61D
79CD20FCE73EE1B81A433812C156281A04C92255E0D708BB9F0B1F1CB9130635
53D8250B7A17BB9E53268B03C324B50344CF3DA7A0A8EE1A788D2C6EE6B6FA32
BB7B6898501F7D84591F42687771D676762C65895449977058EEF92FD982D4F1
8B15999CFF808E9477D25BF0F839AC7C93FA4E62710FB6AE29D33787F1A05F12
A1F8ED12EA8B480128DAE07B18E08AF722260CF879145D699FF691B444DBE21F
12D8BFA1AEB557C146B98F069F3456CC8392863A2F4AD938722CD7CA1A773B39
9AE7AB0AFCCF76719A56FBF5C016995AA52043B2D4649B4F9F8822D31F5E5296
2659C3BDBC7EBA9E3A10275353FFBED470235B27627ED1D7FFA5C6891E21C4FB
6A9CBD41CBEDEB6E5883F55075E37404B35ECD7F7A01C02361740FF01866583E
4D139974F02981F05AB792965CD80B7CF999C19ABA4DFA3F1F9A675D88E67C5C
7CD8F10164A6C3209574751D16C4E9297334F11A08ADE649055450D41E0D31E9
93CE973DAA9687F185966B3133F7003006655EC9D5BF3EDB881EFAF0E4FBAFC7
BA530FDEE3102E32519DFDDC4A31A0A45B10F103F672E12E87ACF77AA5F2E151
9F256973EE6DDCD3D781761480C00220A140FAD833DC9A6A085F45C419D1714E
60F1FC7E684C71E0203D7E6EA7FCB691B5CD723A7DA6EF4E4E462AE7F262E857
7211A9816D88228A88E64919BC822E2EA84260592FEFC616A5691F4A6E347678
7D7F255E2090DE48AB0112A63AF0D195AA7956B3DC3AE94FAB5FE65609212CAF
62A27299A63F16F14AB36532E5AFC203F817DF9EEF94630A4873D35D8F685FBD
939F58C10211A768F664A8F54310DCC42EB672887BE61D5D377B5A88BE107B9D
8C283ACE779977A0642254AC184617C69943FECB7EF66BCA1B8AB4136AA8AE9F
312CA11397995095130A472628944FA9F604F01B456B58F9C067A772B44484DE
ECE4C1E4C72A361DB47C69DF061A2AECCDDB5DBA17D8FB1EFF6CAD0A67975B2B
06B323E0B626DC4F051596A39F52C46B35F88EA6F85A56DE0FD76EC73C7F3851
C731575D62FB7B5AAD53810832534E56C8A58DD49DF8F38732A2F6CF2FC53648
AD6B1C258C45D7661EF929A5250A69F1A1C7898E90D782772671F3398CB875FB
9958E259BAD37BF1F02C9AE1A171D37ABE94E50B3D846F845CB362584769F97D
63C8A4195BBC2E20050DDBEE4F133432E126580881E17B681253A482ADA51675
16BB2FD2A291F8C5A0CA60B834106D037BDBC3C3C47FADFD19E208A4A2A5B4D6
BFAA65989845F239DB78488783FA72BA55037DA1AF409376C4E1926D545506CC
1BA80558A948A2E2AFFE8CC0AC487BE65C67EAA1F12ACB87071FF34A95FC2F8A
DA025CE7C0F6977DA21A1B14DE081D828B51BA0488783E042CA747FA96C040B6
F1CFF858F5006EBDB0971652D0F2F36E7ED085FE13ECDAEA1CE8384EABA702D7
16E1978623CE9C48FD18BC77FF78AF626B170C5ECFAF8BF3A2C511277040C826
71947B1BB929D72B0451F3810BCC0517C1D1816E927C62675821470CE7A51B0A

8ECDB6D0E67DE0F44098AE8CB8697DEAA6E0CC8C45A9CF77F862DBB30E5D2DBA
B627EB2AA0953CF6CA40071CD54F8F1D5B036302012ADB69704C91A4320DEF1C
909B520C493BD868B94E361035C425A343786CF06B935D3A01621DFFD849E0FE
7B7975CC04C6F440B04A5C9CD41AA8C86A0E6DE72B8E8DDC75A6B0E142683A8D
AA48CBB39BA760613C102F08814685C742F92C7E34E357A9A81204170E28DDBC
14840130AB75587BC52C2F6CAB5725E7D23FEE87F2AE8B80921738632BD81182
49E921914B6AAEFF48E1EAEB31C4A38C5D369FA512A34D54665BF171C9B4A68F
EE6D924628818E6A2FCDCD5B47953D2F55DA0C5134516CBF97D1932B897D63AD
574DC0B771C37BACA84B715A97DC31F9C1C50EA1C100C0711B9569F7746C9680
EE0A18F121CCF96B1A346F5C6B4C69E735DEA57B3F45977A139135D177B266B8
2F5312AE2A1C8509265493A5082F6263E9BCD25FDABD97DA21C68F3AFB151D3C
2DFCAFE237C7B43332D888E8868C4A6C6D992453F9F66CAC604903809037DBE4
AA6280916B0E8991871E59CBA0933D41C20960B9D7763CD199E4E42398A094DF
33F75E31C16B0386D8C155EF3DDF08A97106238CA554A2966F1032AE1E736214
23A7F703F82E97AD99BA068099435185C7C3798BB468BADB47182C615E31FA56
A30E9D09D5962E56F958944ACDD7DE33E369ACFADE437743308202F9C975B52A
0A0B908283EC320211E20527EBBB20CAD17FC9A7058EDFB33D302EC04AB0AC3B
4B24E4B296677A0F4DE09F6AE3D676EFD620FDB040B69C94B8E98F471F5A6454
1DE6B3564E9F9C57561559DE76C7D07231FD0F564F9CF7E46613A722E22DE015
F060508128CEC81900681D00DCB87346D3F30C883B7A1CD657B93564963462FF
528E1DF23DC41F9FE783EDAB41B3B89F47E9A34C265EB8406261B7BD92158040
9E7DBF6B828E52DCBED4C6578A5269872EF1BEF953EFDAC803854EE89535C24D
6C8887BD717D98663F37F19EDB72C350BD622B7112C0ADE5FDABD9BA182C67F4
B7AE354E1227E211B73CBABD1989A86DA6018D6ABE756C2D16506AFF46B3CFA2
4265B4461D213A6E99447FC255A5D4DE9A18B92756CFB66A247472261AB01154
C6BBCBD392E5828B0FD1130E4C27CF352415295B0428C6B1CE6707528CFA8502
338B9B5EA11C502F5EAB38C606740319AE6606E17E29106348CBDDC312F0343C
17B89590D4A732821269F81D0E2A307554A516AAC41A25386A660EFC31F11579
DAD3431F42DD3BAC7FA36ED24B40BFB6E8D7CCCE71C325EE0C068E7B1A1DE1AD
7F2290DF275B8B87C0F8158AFEC08D1C5201F6112AB01E36CE7CD6FD01E1AF6B
250643C78220F6913F63F9AFFFC2F2178453B25551D0B0331F571B810E97D146
C81A1BB8E9DB03BF19883977AEC6487B0D432635DEF4C9CC349C4153521542F4
4BB9DEF5BFDDDCD575DD7B07800290B37304253979E0D2CC8EE38A52711FD327
61FDA8FCE4674AFD868CEEABD6172D2A6BC95D3B1DBAEFAACD8E340CF024726F
B2F393FC463CB2B9AAAEC34BA98BE049FB8D3E747FB61C30D3B7D21D58283D81
E6AF534B1DBEE86E294E4110DD70A1DD089FEEF0C7E4C9946ABAC7B988FE7763
D91FB28BBAF54E85E5A87E608C2BB630E7BE06815F17541D680823FAAB4A8FB5
F97175FDAD804A02E6F24273B371184D816044EB2409DADAAD683C07FD41E992

A3CDB3929B4AD03371335E2CB854E5CFB61816821CD4FCB9807E4FAC57F65EA4
09E20223D059891D4712C1FD14423AC5AEE9177BCB5E4C7E2D8778415F146499
D0FB6F4C608994C787F15EE3B5CC1297180687522ADE080C07A708E55CE23DE8
ED70847AEEE2BD0DF8F5787C4F580BF7B8E46D7F46B8F6E2BF082C4014C90261
0390701032E3B623A9B43927C6374ABCB2C040B343147D934CD0C91F638CF8B8
B831D550B25956A849594B8E00791EDCEC7D603ED28948259A8EC62F3EF1B21D
7C9967AF20CF6415B6D581D74EFAF9E8F9181DA92CBA43D7B4056F7FAB97C976
BBF341BA4E7AEC31155E16F82572F6022C413735E63F0550685846945EC95DAF
4CC16F4D2AE63DB6A45E397A134FC8FA23D8AB1EC60610A46142403D40EF6454
995F0EE67D4FDF4E5182FD09D7D1084F35F863E08AC3989C7CF5174E6FE0333C
443140EF94C80B615EEAC17CF63580E85CCEB57C6C417273A65872FFE0F712B2
DA74221E6E6EEE961014701CD7F8BE3805B324A602264B6801E766C4991906BE
9FB4ACA06E67C01E6AE8C11817428CFB8E9206D9BF2FE1126AF8BFEF3D16835F
D0BF90AB2E04BE11A67D7901047A4D0ADCCC31B436FEB4100A09F527A2FE751E
D41FD38A8478BF788F5DC0ACF0E070DD360DDC9BFFF0804E6B5254CC0116AA81
982F8E3329EF811BDE84FD0CD5009DBFDA6ED5E22E10EEA796AC128E787F4F50
462257012D62EAD365AF0198457C64CC07A0597461CE79496C0F22B91273DCDE
362FC55F5CD3D5338827DE0EAFDB7EB34C26885345706852184DB95AD9996A5C
2D22D812117FF4CA4D8BCBD45EC20C77F52E907BF7320D44F6A4FD6C7BEB066E
37AFE4A36A980DD0609F8E6CCFCFE037AA336D16E1BA811D926EED4050E595EC
C0FAF72BB6E93878EBA4B86CAC0E949336C971172071A89EB9AF3EF768804282
2D82BC93B52CAAD80213EEC95E897909C57D75D82A4AEC9D1C2FBC204B7104BA
DAA70A3C21659EAE084F570AAA66FE194D4CBCE337815B460C40AB744583C762
63700DA4A03A05B362337224C6245F09DD5E9D72312C600EA0B607107BC82CA0
31F5E6D1E938023BBB9FE4F760EB068819E6707E0304D3A16A414103BA1C3CD2
11AACCD9547FD5A71335F33CE8E48BA37381013E16D4E69D01AA4252CFB17A33
F1662BFEBF68D8DA9879FD50B41536078C0C06ED4616DC388EE78A30CE8CCD27
2253F5222EBAD25243CD8E3D7AC416939A7CF4F52E991EE3BD6E2F2847D28FAF
B80B9AA14AF3D1AF9246B14855D717EF5BD3AD0C26978C312B74323A2DA0DBE7
1363B70D46C3AF4D0794ECF650E3F50CEB3F81302E6059E42D94838E9ADA1111
CBF87C3FCE4C8608FCC1B1960CC4DC305ADDFDAE889EE3998629D18D8ED2EE1C
9B183AFCFCCC12AF90F82C5F5B8A077BD8C77CF815C62E946A0DFDB4BC78847F
9F79EA51439742E0888ABD4273B62BCD247D1C72EA4F729EE870669A13F192C5
BBCAEE51155609D365F6BB297D124EFEA685DF0243EC1D4EFB5043D9AFE5963D
C8466C386261FACF38CE62E75A8C6414AFFBFAED439E91FA00E515E079702FE0
B10D9A62EDB6081AA9F7FC865554064BB212555392B1181DC40040E12927F988

Endnotes

1 https://www.cnn.com/2021/07/06/tech/kaseya-ransomware-attack-businesses-affected/index.html

2 https://www.pcrisk.com/removal-guides/14942-sodinokibi-ransomware

3 https://twitter.com/GrujaRS/status/1122051624535568384

4 https://www.pcrisk.com/removal-guides/14942-sodinokibi-ransomware

5 https://pastebin.com/YBXgiGSS

6 https://sapphirex00.medium.com/revil-aka-sodinokibi-ransomware-operator-interview-english-version-a5cb3e52ff2

7 https://www.youtube.com/watch?v=ZyQCQ1VZp8s

8 https://www.fortinet.com/blog/threat-research/gandcrab-threat-actors-retire

9 https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-operator-arrested-in-belarus/

10 https://www.secureworks.com/blog/revil-the-gandcrab-connection

11 https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-the-all-stars/

12 https://twitter.com/noblebarstool/status/1146079158096687105

13 https://twitter.com/noblebarstool/status/1179481010561523714

14 https://sapphirex00.medium.com/revil-aka-sodinokibi-ransomware-operator-interview-english-version-a5cb3e52ff2

15 https://www.oracle.com/security-alerts/alert-cve-2019-2725.html

16 https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html

17 https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

18 https://cybernews.com/security/how-we-applied-to-work-with-ransomware-gang/

19 https://github.com/qTox/qTox

20 https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sodinokibi-ransomware-cobalt-strike-pos

21 https://ithome.com.tw/news/144900

22 https://www.zdnet.com/article/at-least-20-texas-local-governments-hit-in-coordinated-ransomware-attack/

23 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-8453

24 https://www.zdnet.com/article/gandcrab-ransomware-gang-infects-customers-of-remote-it-support-firms/

25 https://cybersecurity.att.com/blogs/security-essentials/exploit-kits-for-drive-by-download-attacks

26 https://twitter.com/tkanalyst/status/1193121699002114048

27 https://howtofix.guide/cybercriminals-spread-sodinokibi-ransomware-through-rig-exploit-pack/

28 https://threatpost.com/ransomware-data-center-cyrusone/150873

29 https://cyrusone.com/solutions

30 https://www.infosecurity-magazine.com/news/ransomware-attack-on-cyrusone/

31 https://investor.cyrusone.com/node/11856/html

32 https://www.bbc.com/news/business-51017852

33 https://threatpost.com/sodinokibi-ransomware-travelex-fiasco/151600/

34 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510

35 https://www.scmagazine.com/news/security-news/travelex-driven-into-financial-straits-by-ransomware-attack

36 https://https://www.cyber.nj.gov/alerts-advisories/kenneth-cole-fashion-house-suffers-breach-after-ransomware-attack

37 https://www.infosecurity-magazine.com/news/celebrity-data-stolen-in/

38 https://abovethelaw.com/2020/05/lady-gaga-documents-leaked-after-law-firm-was-hacked/?rf=1

39 https://www.forbes.com/sites/daveywinder/2020/05/18/hackers-claim-trump-dirty-laundry-data-has-been-sold-to-interested-party/?sh=370ef317bca4

40 http://www.colombopage.com/archive_20A/May25_1590431138CH.php

41 https://www.teiss.co.uk/telecom-argentina-ransomware-attack/

42 https://www.bleepingcomputer.com/news/security/revil-ransomware-deposits-1-million-in-hacker-recruitment-drive

43 https://www.youtube.com/watch?v=ZyQCQ1VZp8s&feature=youtu.be

44 https://intel471.com/blog/revil-ransomware-interview-russian-osint-100-million

45 http://securityaffairs.co/wordpress/70429/deep-web/deep-web-book.html

46 https://www.zdnet.com/article/revil-ransomware-gang-acquires-kpot-malware/#ftag=RSSbaffb68

47 https://www.proofpoint.com/us/threat-insight/post/new-kpot-v20-stealer-brings-zero-persistence-and-memory-features-silently-steal

48 https://hacked.com/ransomware-revil-hacks-celebrity/

49 https://www.manageengine.com/ems/cyber-town/dairy-farm-fell-victim-to-revil-ransomware-attack.html

50 https://www.bleepingcomputer.com/news/security/pan-asian-retail-giant-dairy-farm-suffers-revil-ransomware-attack/].

51 https://www.binarydefense.com/threat_watch/pan-asian-retail-group-dairy-farm-attacked-by-revil/

52 https://securityaffairs.co/wordpress/115777/cyber-crime/acer-revil-ransomware.html

53 https://www.forbes.com/sites/daveywinder/2021/04/23/ransomware-gang-demands-50-million-for-apple-watch-and-macbook-pro-blueprints/?sh=458f18f05839

54 https://www.crn.com/news/security/apple-menaced-after-revil-ransomware-attack-against-supplier

55 https://www.nbcnews.com/tech/apple/hackers-try-extort-apple-stealing-files-company-makes-products-rcna750

56 https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime

57 https://www.trtworld.com/business/servers-of-us-oil-pipeline-hackers-darkside-gets-shut-down-46726

58 https://www.flashpoint-intel.com/blog/revil-is-down-not-out/

59 https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

60 https://www.trtworld.com/business/servers-of-us-oil-pipeline-hackers-darkside-gets-shut-down-46726

61 https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/

62 https://www.techtarget.com/searchsecurity/news/252508633/Emsisoft-cracked-BlackMatter-ransomware-recovered-victims-data

63 https://news.yahoo.com/biden-meets-putin-first-time-114506623.html

64 https://threatpost.com/revil-spill-details-us-attacks/166669/

65 https://www.theverge.com/2021/7/22/22589643/ransomware-kaseya-vsa-decryptor-revil

66 https://threatpost.com/kaseya-universal-decryptor-revil-ransomware/168070/

67 https://www.dailymail.co.uk/news/article-9762037/If-Russia-doesnt-deal-cyber-criminals-Biden-spokesperson-issues-warning-Putin.html

68 https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/03/remarks-by-president-biden-after-visiting-king-orchards/

69 https://www.dailymail.co.uk/news/article-9762037/If-Russia-doesnt-deal-cyber-criminals-Biden-spokesperson-issues-warning-Putin.html

70 https://www.washingtonpost.com/technology/2021/07/13/revil-disappears-kaseya-hack

71 https://www.bleepingcomputer.com/news/security/kaseyas-universal-revil-decryption-key-leaked-on-a-hacking-forum/

72 https://www.cnn.com/2021/07/23/tech/kaseya-encryptor-ransomware-victims/index.html

73 https://twitter.com/pancak3lullz

74 https://github.com/Fr3akaLmaTT3r/decryptor

75 https://www.bleepingcomputer.com/news/security/revil-ransomware-is-back-in-full-attack-mode-and-leaking-data/

76 https://www.zdnet.com/article/fbi-decision-to-withhold-kaseya-ransomware-decryption-keys-stirs-debate

77 https://www.linkedin.com/feed/update/urn:li:activity:6845837344713519104/

78 https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

79 https://twitter.com/3xp0rtblog/status/1457845398077386760

80 https://www.state.gov/reward-offers-for-information-to-bring-sodinokibi-revil-ransomware-variant-co-conspirators-to-justice/

81 http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html

82 https://twitter.com/ddd1ms/status/1481977005180653574

83 https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/

84 https://tass.ru/proisshestviya/13431243

85 https://tass.ru/proisshestviya/13431243

86 https://analyst1.com/file-assets/Nationstate_ransomware_with_consecutive_endnotes.pdf

87 http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html

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**