

Ransomware Diaries Volume 4:

Ransomed and Exposed — The Story of RansomedVC

Written by Jon DiMaggio

481523

30 JAN, 2024

RANSOMED.VC

POLICE DEPT

WARNING:

PLEASE DO NOT TRY THIS AT HOME. ENGAGING WITH RANSOMWARE CRIMINALS SHOULD ONLY BE CARRIED OUT BY TRAINED PROFESSIONALS.

WHILE IT SEEMS "COOL" TO INTERACT WITH BAD GUYS, DOING SO PUTS YOU AND YOUR EMPLOYER AT GREAT RISK.

PLEASE DO NOT ATTEMPT TO EMULATE WHAT YOU SEE IN THIS REPORT UNLESS YOU HAVE THE KNOWLEDGE, EXPERIENCE, AND SKILL SET TO PERFORM SUCH ACTIONS.

THANK YOU!

Contents

Intro	4
Significant Findings	5
PART I: Impotent and Exposed	7
The Rebrand	7
The Backstory	8
Origin Story <i>Exposed</i>	10
RansomedSupport is Impotent!	14
Exposed	16
Impotent Leaks	18
Part II: The Rise and Fall of RansomedVC	26
Ransomed vs Exposed	27
Significant Attacks	32
The Sony Breach	39
Don't Make Putin Come to My House.....	42
See You Later Alligator	49
Resources and Leak Site Analysis	53
Engagement Analysis.....	55
What It's Like to Work with RansomedSupport	55
A Well-Kept Secret.....	59
Ragnar Locker?	60
The Man Behind the Mask	64
The End Is Near: Of the Paper, Not the World	65
Appendix	68

Intro

RansomedVC stands out as one of the most unconventional ransomware operations I've investigated. Its leadership strategically employs propaganda, influence campaigns, and misinformation tactics to gain fame and notoriety within the criminal community. While I may have my assessment of RansomedVC, I cannot deny the effectiveness of its tactics. It also rubbed many people the wrong way, including other criminals.

While there is no question that RansomedVC runs cybercrime operations, I have questions about the claims it made regarding the authenticity of the data it stole and the methods it used to extort victims. Before beginning my research, I discussed RansomedVC with other analysts and found that confusion and differing opinions were the only common factors across all my conversations.

Due to this, I questioned if RansomedVC was a true ransomware operation or, instead, a fraudulent attempt to repurpose leaked data from previous breaches used in conjunction with a criminal narrative intended to deceive and pressure victims into paying their extortion demands. To assess RansomedVC, I explored its entire operational lifecycle, including the previous criminal activity conducted by the humans behind the gang over the past year. I communicated with the leader of the gang directly for several months, asking him many questions. I also talked to some of the hackers who worked with RansomedVC to learn about their experiences and stories. Then, I used human behavior profiling techniques across current and previous criminal activities to analyze their operations further. As I pieced together this complex puzzle, a larger and more sinister picture began to emerge, comprised by theft, lies, deception, betrayal, and a great deal of drama. All these revelations will be disclosed in volume four of the Ransomware Diaries!

Objective: Many elements of this story do not add up, and I want to find the truth behind RansomedVC's motivations beyond what I was being told by the criminals themselves. There is a lot to unravel to truly understand RansomedVC, which I will analyze and detail through the research in this report. While many details have been previously disclosed, I want to look at everything known about the group's activity and provide new research to fill in the information gaps and create the "big picture view" detailing every aspect of the operation. My end goal is to assess if RansomedVC is actually a ransomware operation or something else entirely that the group's leadership has cleverly hidden from the world to benefit its agenda.

Significant Findings

- **Finding #1:** RansomedSupport was previously associated with the now-defunct Ragnar Locker ransomware gang. A known hacker who worked with RansomedVC claims RansomedSupport may have been involved in sharing information that led to the arrest of Ragnar Lockers' developer, and the detainment of five other suspects out of spite after falling out with the gang. RansomedSupport denies the accusations and claims he is not affiliated with Ragnar Locker nor had anything to do with the arrests.
- **Finding #2:** RansomedVC lied about stealing PII data from State Farm Insurance, resulting in a class-action lawsuit against the company by customers who read the media reports and believed the criminal's claims were true. RansomedVC "willed" the lawsuit into existence with their lies, which they legitimized with the media coverage surrounding the event.
- **Finding #3:** RansomedSupport admits that some of their attacks are completely fabricated and that they even created fictitious data to deceive one of their victims in September 2023. In other situations, RansomedSupport bought stolen data, or stole it from other criminals.
- **Finding #4:** According to RansomedSupport, affiliates are paid a salary between \$2.5k and \$5k a month. However, I found that several of the RansomedVC-associated hackers I spoke with were only partially paid or not paid at all.
- **Finding #5:** RansomedSupport intentionally manipulates the media to report RansomedVC attacks and then uses the "hype" from public reporting as validation the attack is real to pressure victims into paying extortion demands.

PART I: **IMPOTENT AND EXPOSED**



PART I: Impotent and Exposed

In November 2023, when I started writing this report, RansomedVC announced the shutdown of its operation. I reached out to the group through its public Telegram account, “RansomedSupport,” and communicated with an individual claiming to be the **“owner and creator of RansomedVC”**. Throughout my communications with RansomedSupport, it became evident to me that the actor I was chatting with was male. For this reason, I will refer to him by his seemingly preferred pronoun.

The first question I asked was why he was shutting down the ransomware operation. According to RansomedSupport, law enforcement may have arrested several men he is affiliated with and obtained their real names and home addresses. Though, at the time, I could not find evidence or arrests to support this claim. Additionally, RansomedSupport said he monitors logs associated with RansomedVC’s infrastructure and noticed login attempts from unauthorized IP addresses.

RansomedSupport claimed that several hours after learning about the arrests, he received two **“emergency alerts from our main operators”**. He explained the emergency message is derived from **“a small API based program that allows them (his operators) to send me a message from anywhere”**. At the time of our initial conversation, RansomedSupport was preparing to wipe RansomedVC systems but would delay for 24 hours so that I could reach him and conduct what would be our first of many engagements.

Shortly after our initial conversation, RansomedSupport carried out his claim and shut down RansomedVC, including its infrastructure, and deleted the content in its Telegram channel called “ransomed_channel” that was used for recruiting, leaking victim data, and sharing attack-related information. Before the shutdown, RansomedSupport provided an alternate account to stay in touch. From that point until the publication of this report, I had many interactions with the group’s leader. In this report’s “Engagement Analysis” section, I will provide further details and share the insights gained from these interactions.

The Rebrand

As we have observed in the past, cybercrime gangs typically persist unless arrests are made. Instead, they frequently rebrand themselves with a different name and continue their operations. This situation unfolded a few weeks later, on December 5, 2023, when a new message appeared on the website Ransomed[.]vc, declaring that the gang would now operate under the name “Raznatovic.”

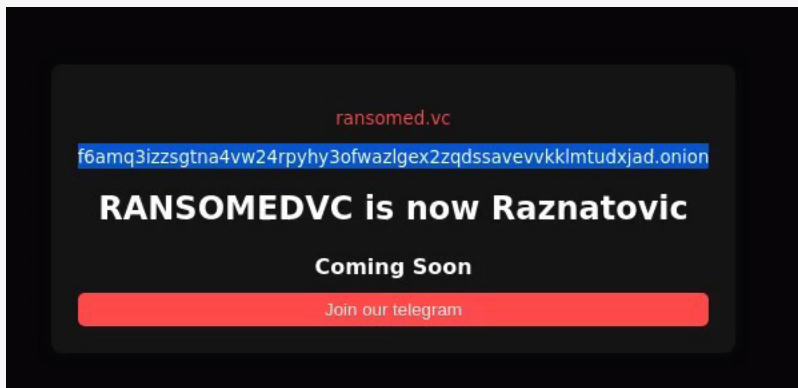


Figure 1: Message posted to Ransomed[.]VC announcing its new name/operation.

Interestingly, the name Raznatovic is not new but instead is associated with a [“Serbian mobster”](#) also known as Arkan, which is the name used in RansomedVC’s new telegram group titled **“Tigers of Arkan”**. Raznatovic (RansomedVC) then created a new chat channel titled **“Raznatovic Channel”** and updated the RansomedSupport alias to **“RaznatovicAdmin”**. This is not the first time the group has used Serbian names and references in its operation. For example, it previously used the alias **“Hriste Boze”**, which is the name of a patriotic Serbian song about leaving the homeland (Serbia) for battle. I asked the group’s leader if he was Serbian, and he told me no, he was Bulgarian, but had a love for Serbia, inspiring the new name and theme. These names are just a few of many used by the real-world person behind the activity.

Next, I looked at the new Telegram posts associated with the group’s personas. Within the first day of the new operation, RansomedVC began recruiting other hackers to help in its new Raznatovic operation. Upon seeing this, I had several questions. First, if RansomedVC was the operation it claimed to be, why did it need to recruit new criminals to help in this effort? What happened to the rest of the gang that allegedly implemented almost 50 attacks since August 2023? I asked the group’s leader, and he told me he let everyone go because he did not want to be responsible for affiliate arrests due to their mistakes during criminal engagements on its behalf. Yet, hiring new hackers would not change this scenario, so there may be more to it than that.

The Backstory

Before I begin my analysis of RansomedVC I want to share the backstory of what led me to write about the operation. On August 15, 2023, Analyst1 published the Ransomware Diaries Volume 3, titled [“LockBit’s Secrets.”](#) Part of my post-publication process is to evaluate how the security community received the report. Additionally, I enjoy seeing what the hacker community thinks of my work. To accomplish this, I monitor and review

discussions about the Ransomware Diaries on social media and underground hacking forums. So, on August 20, 2023, I logged into XSS, my favorite hacking forum frequently used by Russian speaking Blackhats and cybercriminals.

One of the first posts I reviewed was from a forum member who translated part of the Ransomware Diaries from English to Russian, making it easy for the Russian-speaking community to read and discuss. A thread of comments followed, but one response from my long-running adversary, LockBit, especially stood out.

The screenshot shows two forum posts. The first post, dated August 20, 2023, is from user 'LockBitSupp' (Premium, joined Mar 8, 2021, 664 messages, 1,382 reaction score). The user's profile includes a 'BANNED' stamp and the name 'MociBosi floppy disk' with a 'Banned' status. The comment text reads: 'Brandon said: [quote] These are just the latest guesses from one of the thousands of information security journalists who can only guess and create useless clickbait content, everyone knows that the LockBit group is based in the Russian Federation, and they don't give a damn what these journalists write [end quote] Regarding the guesses, you are right, everything is just a fantasy, there really is a problem with data storage and it is being solved, the data flow is so huge, that we do not have time to constantly expand the infrastructure and quickly process this data, as Johnny would like, but this does not in any way prevent advertisers from duplicating stolen information on their servers and calmly publishing on a blog while having a backup backup on their personal servers, which is a huge plus. You are wrong about the Russian Federation, here you become like Johnny by making your guesses public. No matter what Johnny says, I still love him, he is my most devoted fan and follows every sneeze, turning any sneeze into a huge sensation, a real journalist.'

The second post, dated August 31, 2023, is from user 'LockBitSupp' (joined Aug 30, 2023, 8 messages, -1 reaction score). The user's profile includes a 'BANNED' stamp and the name 'MociBosi floppy disk' with a 'Banned' status. The comment text reads: 'LockBitSupp said: [quote] Regarding the guesses, you are right, everything is just a fantasy, there really is a problem with data storage and it is being solved, the data flow is so huge, that we do not have time to constantly expand the infrastructure and quickly process this data, as Johnny would like, but this does not in any way prevent advertisers from duplicating stolen information on their servers and calmly publishing on a blog while having a backup backup on their personal servers, which is a huge plus. You are wrong about the Russian Federation, here you become like Johnny by making your guesses public. No matter what Johnny says, I still love him, he is my most devoted fan and follows every sneeze, turning any sneeze into a huge sensation, a real journalist. [end quote] Have you thought about simple cold storage? There are several 12TB hard drives that will serve the mission of storing old leaks.'

Below the second comment, a red box highlights the text: 'Owner And Founder of ransomed.vc'.

Figure 2: Comments from LockBit and MociBosi on the XSS. hacking forum about the [Ransomware Diaries Volume 3](#).

LockBit would never admit that I hit too close to home with my previous research, but If you read my last report, you know things got messy when I jokingly threatened to expose LockBit if they did not meet my \$10 million extortion demand. Some criminals affiliated with the LockBit operation don't have a sense of humor and didn't realize it was a joke. So based on the forum post, I was glad to see there were no hard feelings a few weeks after the report went public.

The first response to LockBit's comment came from an account with the username "MociBosi", which caught my attention for two reasons. The account had been created the day before, and the message included a signature claiming to be the "Owner And Founder of Ransomed[.]vc". This person was the same individual I currently communicate with using the RansomedSupport and RaznatovicAdmin monikers. Although my knowledge about RansomedVC is now extensive, their operation had only begun then, and my understanding was limited. However, it turned out that I knew more than I initially thought. While I am not the first to make this attribution, I believe RansomedVC had previously operated under another name, "Exposed", which had a very interesting history.

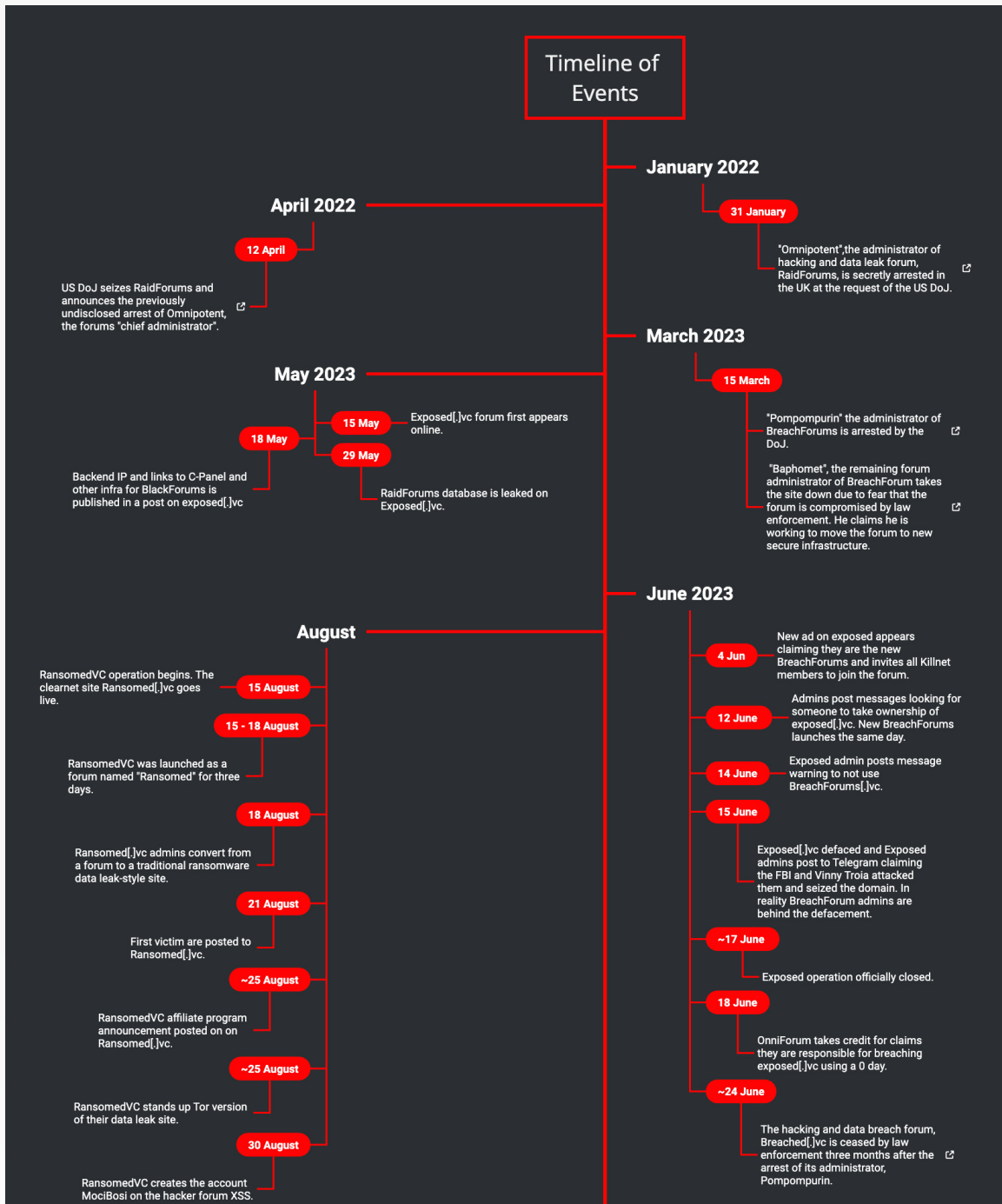
Origin Story Exposed

RansomedVC officially operated from August through November 2023. The Individuals behind the operation conducted cybercrime operations previously under different names and monikers. After spending time researching RansomedVC, analyzing the group and its activities, and talking to criminal insiders, I assess that before RansomedVC, the threat actor also conducted operations running the illicit forum ExposedForum, which was previously hosted on the domain "exposed[.]vc". I validated this claim from information shared by a well-known hacker who worked directly with RansomedVC and led some of their most damaging breaches, known as USDoD (AKA Equation Corp, NetSec, and several others). USDoD worked closely with RansomedSupport in the RansomedVC operation for several months. In a conversation I had with USDoD on Telegram, he told me that RansomedSupport previously ran Exposed under a different moniker which I will discuss shortly.

Note: When referencing to the criminal operation I will refer to it as "Exposed" and will refer to the forum as "ExposedForum" and will refer to the domain itself as Exposed[.]vc.

Next, I will provide an overview of the events and history of Exposed. To understand the story behind RansomedVC as you know it today, you need to better understand the events and motivations of key individuals, which may initially seem disconnected. While

RansomedVC has become a ransom-themed criminal operation, its true essence goes beyond just ransomware. You see, RansomedVC emerged as a byproduct of the “Forum Wars” that occurred between 2022 and 2023. Although RansomedSupport had prior involvement in hacking forums and cybercrime operations, their role in the forum wars sparked the idea to create RansomedVC. Below is a timeline of events you can use as a reference point as I walk through the events that took place in the Forum Wars, as well as the rest of this report.



[continued on the next page]

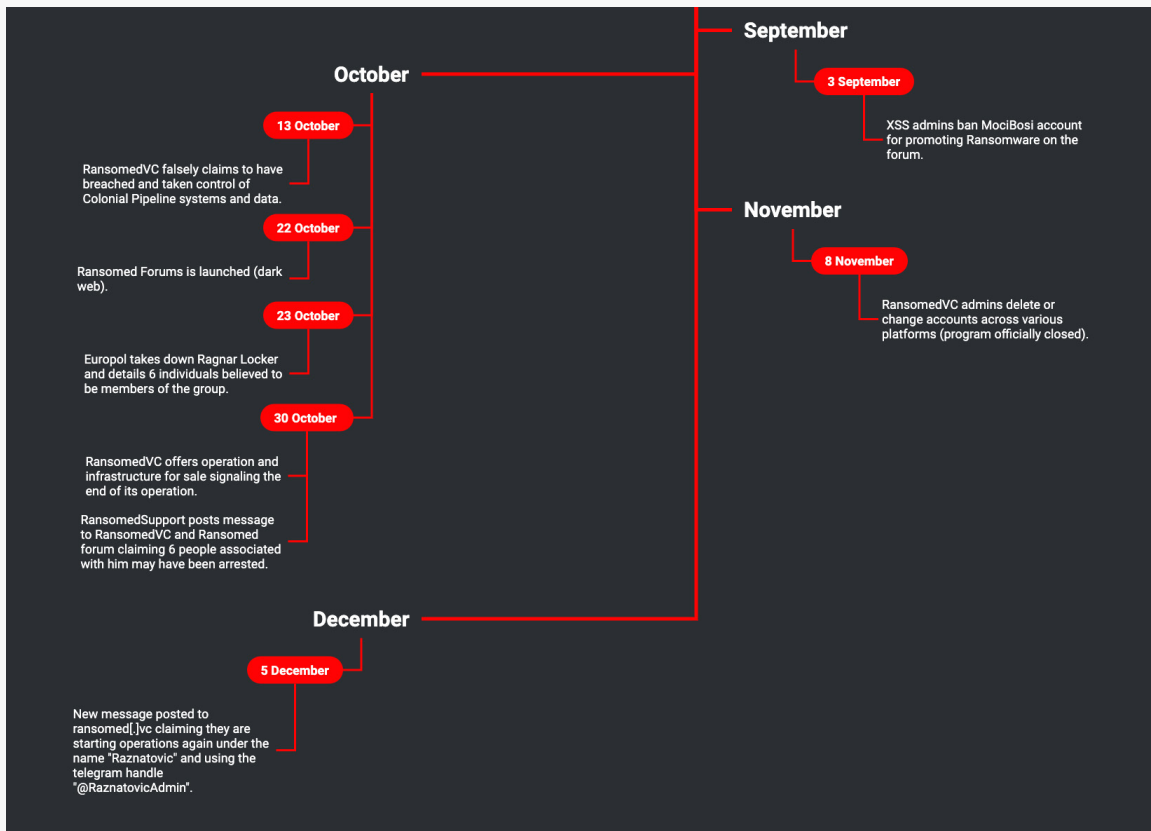


Figure 3: Timeline of significant events.

The Forum Wars

On April 12, 2022, the Department of Justice (DoJ) shut down the popular hacking forum RaidForums. The forum seizure triggered a *butterfly effect*, leading to a monthslong battle between rival hacking forums which became known as the “Forum Wars”. Before its closure, RaidForums was a popular Clearnet hacking forum that rose to fame beginning in [2015](#). While not a one-for-one, it created the model we see today in similar hacking data breach forums. However, on April 12th, forum members were greeted by a notice from law enforcement agencies, stating, “THIS DOMAIN HAS BEEN SEIZED”, as seen in Figure 4. That same day, the DoJ released a press statement detailing the seizure and announced the arrest of the forum’s infamous administrator, known by the handle “**Omnipotent**”.

The significant aspect of the operation was that Omnipotent had been quietly arrested by the Department of Justice (DoJ) two and a half months earlier. This implied that the authorities likely accessed Omnipotent’s computers, accounts, and even RaidForums servers and data before the seizure occurred. Although the arrest was not initially publicized, signs of its downfall emerged seven months prior, in October 2021, when the domain was [suspended](#) due to a law enforcement request made to the domain’s registrar.



Figure 4: RaidForums seizure message.

Nevertheless, the seizure caught many of its members by surprise and created a void in the data leak and hacking forum landscape. Consequently, several forums emerged over the following year attempting to fill the void left after RaidForum's closure. The administrators of the new forums all wanted to attract RaidForum's large user base and establish themselves as the predominant hacking forum. Among these new forums, one in particular, known today as BreachForums, emerged, claiming to be the true successor to RaidForums. One component of BreachForums success was due to its creator, "Pompompurin" AKA Pom. Pom not only created BreachForums, but was also one of the previous RaidForum administrators. BreachForums looked nearly identical to RaidForum, drawing even more attention to itself.

Pom should have realized that creating an almost identical site to RaidForums would have been a bad idea since it received so much attention from law enforcement and the media, but that was not the case. The launch of BreachForums was far from quiet as Pom and several other BreachForums administrators used social media and other resources to advertise its opening and invite the hacking community to participate in its new venture.

In March 2023, after only a year of operating BreachForums, history repeated itself when the DoJ arrested Pom for his criminal activities. The criminal [complaint revealed](#) his real name as Conor Brian Fitzpatrick from Peekskill, NY. Another administrator, Baphomet, considered moving the forum to new infrastructure but eventually decided against it due to law enforcement concerns. You can see an image of Pom's mugshot below.

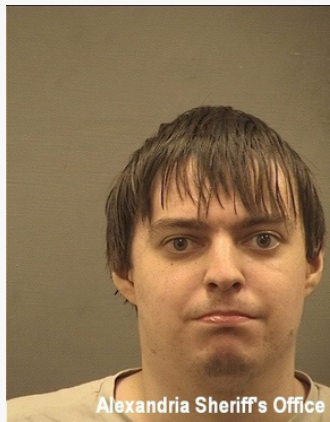


Figure 5: [Mugshot](#) of Conor Brian Fitzpatrick (Pom) the former BreachForums administrator.

After experiencing two forum seizures and two arrests, it would seem crazy to attempt the same action for a third time. Yet, someone did exactly that. Just two months later, on May 10, 2023, a new forum called ExposedForum emerged, strikingly resembling the previously mentioned forums. Unlike BreachForums, the creator of ExposedForum had no official affiliation with RaidForums. Below, you can see the similarities between RaidForums, BreachForums, and ExposedForum.

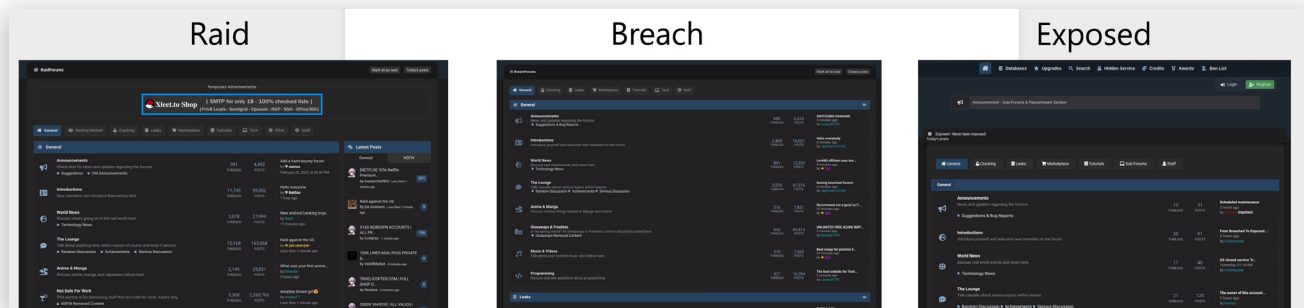


Figure 6: Raid, Breach, and Exposed Forums.

RansomedSupport is Impotent!

ExposedForum was created and administrated by an individual with the moniker "Impotent", AKA "The Impotent Admin". You read that right, he calls himself Impotent. The real-world person behind the Impotent facade, who I believe later created RansomedVC and Raznotovic, intended to mimic, or troll, Omnipotent, the now-arrested administrator of RaidForums, which he explains in a post on another unrelated Russian hacking forum.

Thanks to my chats with **USDoD**, the popular hacker who previously worked with RansomedVC I knew that Impotent was RansomedSupport. I asked him how he knew Impotent is RansomedSupport from RansomedVC, and he told me, "***I discovered Impotent and RansomedSupport were often online at the same time, so I asked him if they were***

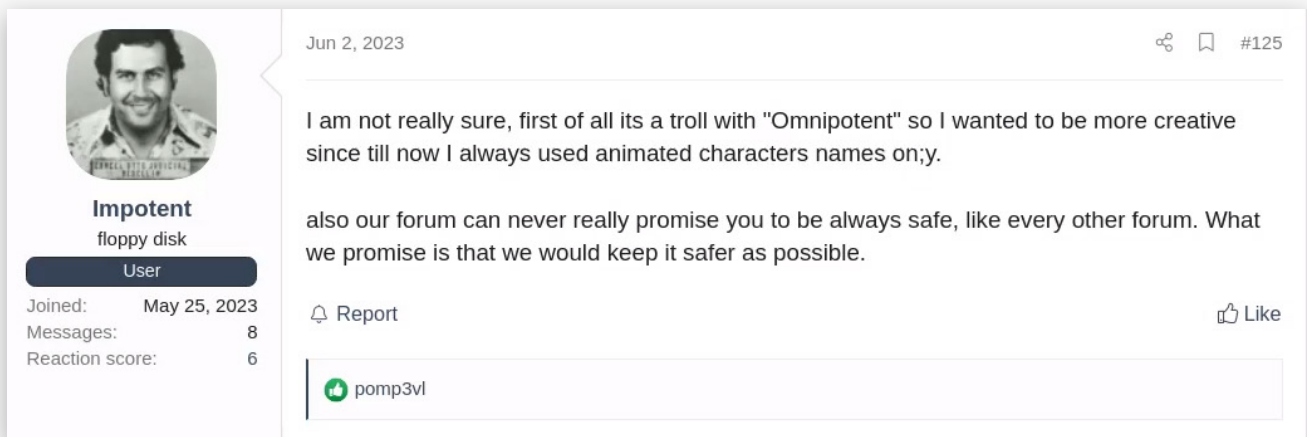


Figure 7: ExposedForum owner and administrator Impotent explains the origin of his name.

the same person and he admitted it and said yes". After talking to USDoD, I wondered if there could be additional criminal operations and forums Impotent operated in the past.

Based on conversations across several dark web forums amongst various hackers, it seems there are varying opinions. However, in an interview with the researcher and journalist, Dissent from DataBreaches.net, Impotent stated that he had previously owned several dark web markets, including Kilos, Elude, NightmareMarket, and WorldMarket, before starting ExposedForum. Beyond, Raznovic, RansomedVC, and Exposed, I could not validate these claims but included them for transparency. Throughout this research, I have found many names that are believed to be associated with the real-world person behind the Impotent facade. Below is a diagram linking Impotent to the dark web operations he is allegedly associated with and some of the handles I believe he has used.

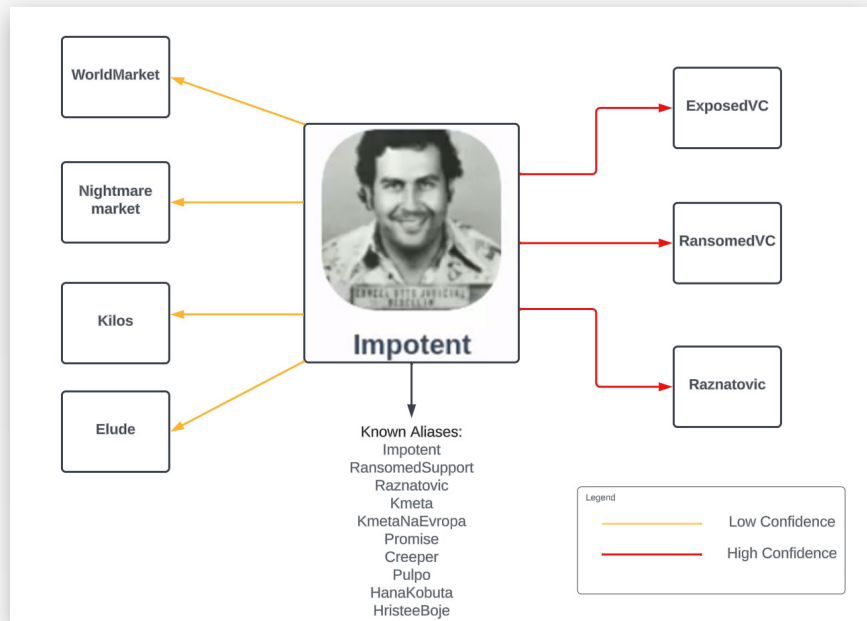


Figure 8: Impotent related operations and probable aliases.

Note: If you want to learn more about the link to Impotent, check out [Suspectfile's](#) interview with RansomedSupport.

Exposed

There are several reasons why ExposedForum stood out compared to most other criminal forums, and these characteristics can later be seen mimicked in the RansomedVC operation. For instance, ExposedForum created a dedicated sub-forum for Ransomware, which also appeared later RansomedVC's forum. The Ransomware sub-forum served as a space for sharing stolen data and recruiting individuals for ransomware activities. However, following the 2021 Colonial Pipeline incident, many hacker forums started prohibiting discussions related to ransomware. These forums no longer allow the topic to be discussed or provide a platform for posting victim data related to ransomware. The administrators of these hacker forums aim to avoid attracting attention from law enforcement and government agencies, so they enforce the ban on ransomware discussions, though it's selectively enforced. However, the "Impotent Admin" did not seem to share these concerns. Below is the initial post announcing the "Ransomware" sub-forum on ExposedForum.

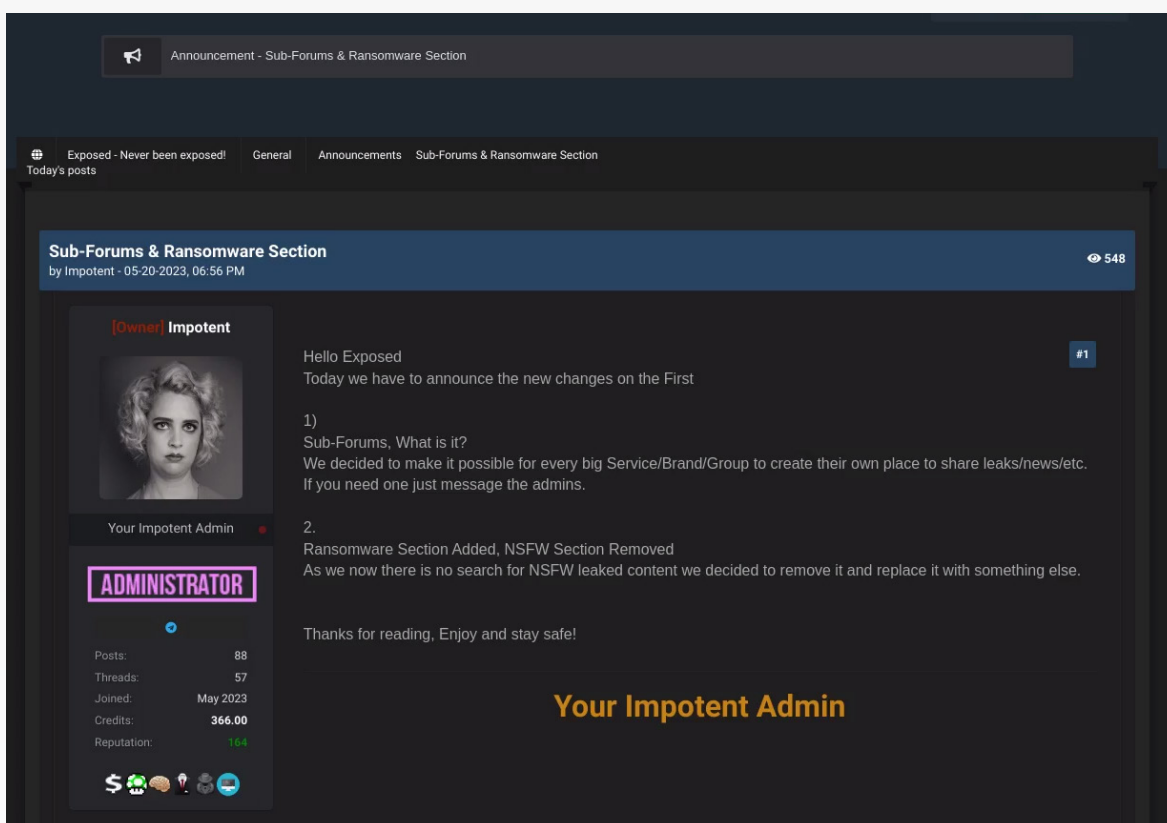


Figure 9: Impotent announces the new ransomware sub-forum on ExposedForum.

Impotent also created a list of other ransomware group data leak sites and established a bug bounty sub-forum. Initially, I believed this program would reward individuals for discovering a bug in the exposed forum that a third party could exploit. However, it turned out to be different. The bug bounty program allowed users to submit websites they wanted hackers to exploit, either by identifying a vulnerability or implementing an exploit. Once validated, the bounty would be paid. This program was advantageous because Impotent acted as an intermediary, facilitating the posting of target sites and handling payments to requestors in exchange for a fee. This setup ensured anonymity for all parties involved except for Impotent.

Over the next month, members of the ExposedForum posted several datasets associated with high-profile leaks. The leaks included data allegedly stolen from Japan's Ministry of Defense and data from government systems stolen from the City of Augusta (US). The [BlackByte](#) ransomware group and other known hackers used the forum to leak stolen data. The forum was gaining momentum in the criminal community, but that wasn't enough for Impotent. You see, Impotent enjoyed being in the spotlight and sought out confrontation. Winning wasn't sufficient; he wanted to make an example out of his competitors. For instance, Impotent deliberately provoked rival forum administrators to demonstrate that he could target anyone, regardless of their status.

On **May 18, 2023**, Impotent took on another hacking forum, BlackForums[.]net. He published the IP address and URL of BlackForums' hosting panel, which administrators use to manage the site. This action caused problems for the BlackForums administrators, as they host similar content to ExposedForum and BreachForums, providing a platform for sharing stolen data and discussing malware, exploits, and other aspects of cybercrime. By making the hosting panel address public, both law enforcement and criminals would have the opportunity to attempt access to the forum's management space. You can see Impotent's post below.

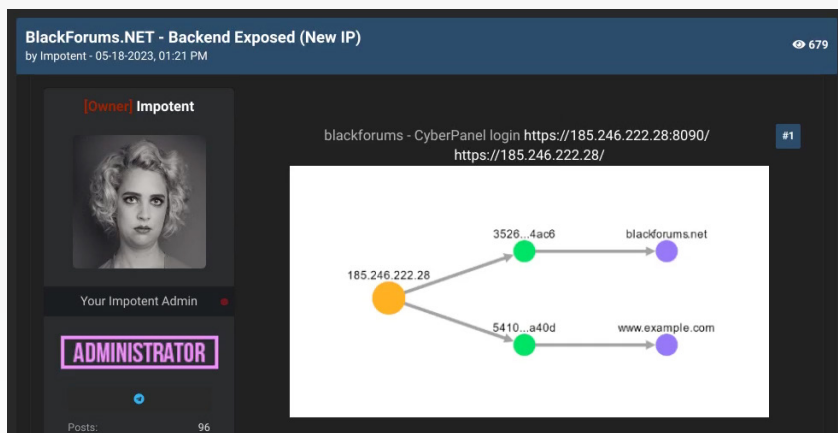


Figure 10: Impotent post on ExposedForum exposing the IP and URL for the BlackForums hosting panel.

Making light of the situation, after exposing BlackForums, Impotent created a [poll](#) on the Exposed Telegram channel. He asked users to vote on which competing forum they should target next. This time, it would not be an active forum that Impotent exposed.

Impotent Leaks

On **May 29, 2023**, Impotent created a post leaking data stolen from RaidForums. The leak included information about RaidForums users, such as usernames, email addresses, and other account-related details for over **478,000** of the forum's previous members. Impotent either did not realize or did not care that many of the users found in the leak were likely the same users he was working so hard to attract. Below is an image of the RaidForums leak post.

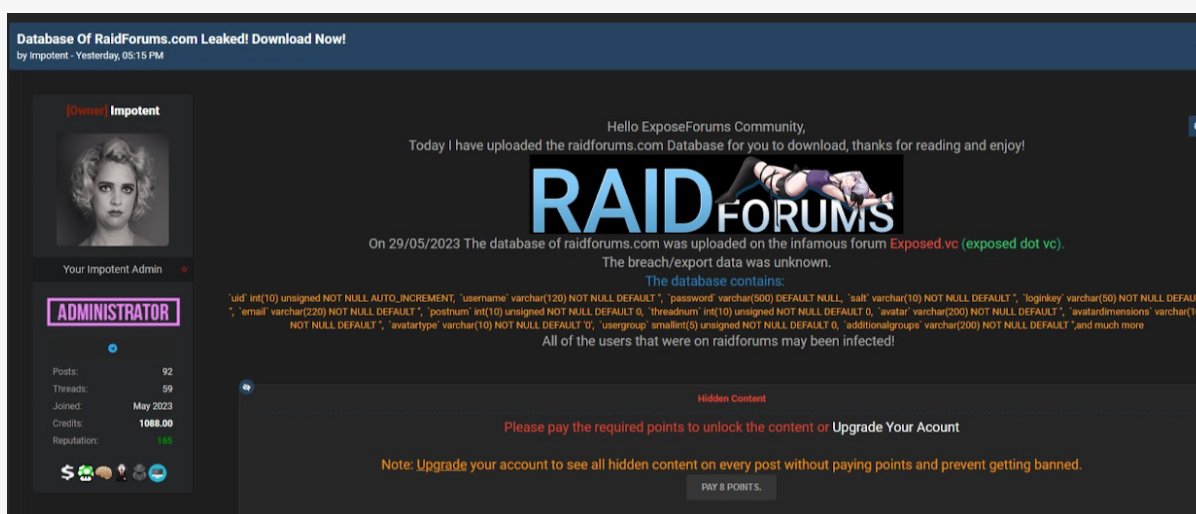


Figure 11: RaidForums Leak posted by Impotent on ExposedForum.

As it turns out, the leaked database was not complete. Between the time it was stolen and leaked, someone removed specific user accounts and associated data before publicly posting the information. According to Impotent's statement to [Bleeping Computer](#), some data was removed but **"still contains 99% of the original lines, with some removed to 'cause no drama.'"**

However, I find it difficult to believe Impotent's claim. Given his love for drama and previous actions, it is more likely that including high-profile hackers' account information would encourage him, not deter him. It is possible that Impotent had a working relationship with other criminals whom he did not want to expose in the leak. Furthermore, several "God" level users were members of the forum but were not included in the leak. I have an alternate theory: Some of the removed accounts may have belonged to the hackers responsible for the theft, including their names, handles, and associated information.

In the interviews with [Dissent](#), Impotent admitted to purchasing the RaidForums Database from a third party who conducted the breach. It is possible that it was not Impotent who removed the names but rather the individuals who initially stole the data. Whoever conducted the compromise likely had a presence on the forum before, which means that the email, password, and username they used to register for initial access would also be present in the stolen data. Of course, they would likely use a burner account to register on the forum but would still not want to leave any evidence behind.

If someone were to compromise a website to steal and sell its data, it would make sense for them to remove any data associated with themselves or hackers they had relationships with before selling it. This explanation would account for the motivation behind removing content from the leak and would make more sense than Impotent simply not wanting to cause “drama”. Unfortunately, I cannot prove my theory, and we may never know the truth.

My next question is, why would Impotent leak the data for free when he could have sold it and made a profit as he does with most of the data he gets his hands on? [Dissent](#) asked Impotent this question, and he stated, *“It was leaked mostly for the forum to pop up. I wanted to use it as free advertisement.”*

This, I do believe, since it certainly would promote and raise awareness of his forum, which it did. Researchers and criminals alike discussed the leak, and media outlets covered the story, generating significant attention for ExposedForum. It is also important to note that, unlike most data leaks, the content from RaidForums primarily included sensitive information about other criminals and security researchers who were members of the forum. This made the information it contained highly significant.

High Profile Criminal Endorsements

Another twist came in **June 2023** when a message appeared on the pro-Russian hacktivist group Killnet’s Telegram channel. The message invited supporters to join ExposedForum, where they could participate in criminal activities, including ransomware. Killnet is a widely known pro-Russia hacktivist group with its activities aligned in support of the state’s political agenda, especially related to the invasion of Ukraine. The fact that Killnet, not Impotent posted the message, was significant. It was a direct copy of the same message Impotent had previously posted to ExposedForum’s channel. This suggests some form of collaboration between Killnet and Exposed. I contacted Impotent and asked him if he had a relationship with Killnet and he told me *“Yes, I help the owner with networking regarding a private stresser they own”*.

Note: The word “stresser” is associated with “stress-testing” and in this context, it refers to a service used to conduct DDoS attacks.

Later, RansomedSupport, AKA Impotent, claimed to have “*Russian investors*” who he believed were “*probably government-sponsored*”. While I am skeptical of his claim, the Killnet collaboration may support his assertion. Below you can see the message Killnet posted to its Telegram channel:

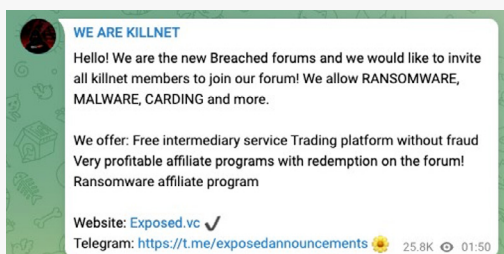


Figure 12: ExposedForum ad posted on a Killnet telegram channel.

Beyond Killnet, another big-name criminal posted a message directly to ExposedForum. The post caught my attention because it was allegedly created by LockBitSupp, [my BFF from the LockBit Ransomware](#) operation. The post included a recruitment ad, which was a word-for-word copy and paste of the same ad present on LockBit’s leak website. You can see the post below.

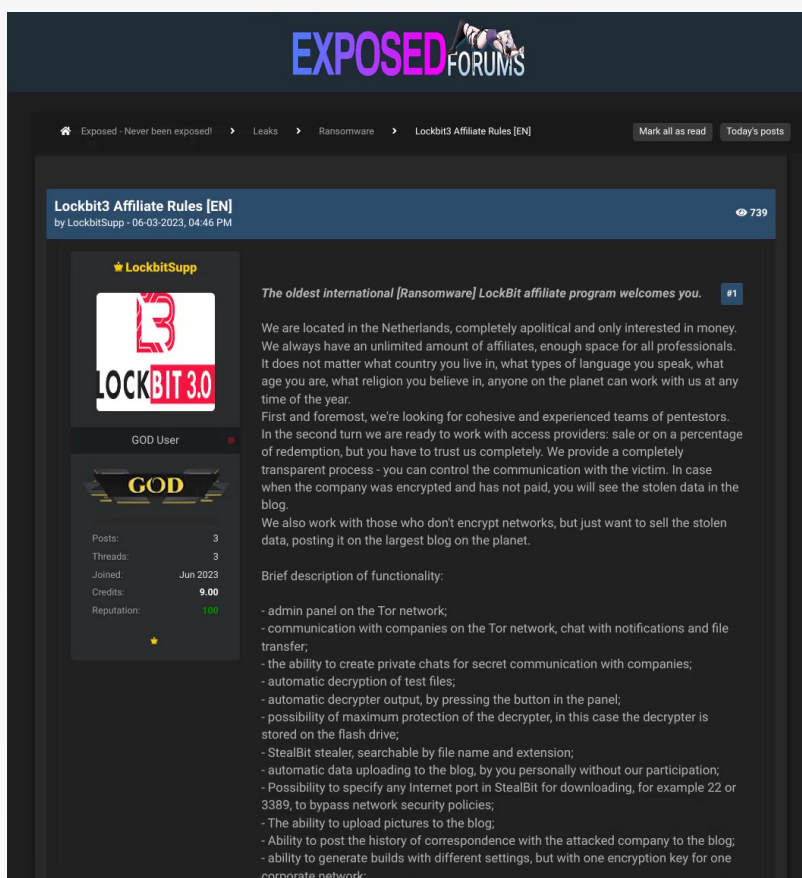


Figure 13: LockBit recruitment post on ExposedForum.

Since I have a history with LockBit, I reached out and asked the gang's leader if he made this post. **He immediately told me that he did not make the post, nor did he have an account on ExposedForum, and that it was a "scammer" pretending to be him to gain clout.** This is a good example of the influence tactics used by Exposed that are like those I later observed in the RansomedVC operation. Since the LockBit post was created by someone with "God" status on the ExposedForum, I can only conclude that Impotent or someone from his crew was behind it.

For Sale by Owner

For reasons I do not understand, despite the months of drama, threats, and relative success, Impotent took down ExposedForum on June 13, 2023. Impotent replaced the forum landing page with a message announcing that ExposedForum was for sale since Impotent no longer had the time to maintain the forum. At the same time, Impotent posted a similar message on the Exposed Telegram channel. Both can be seen below.

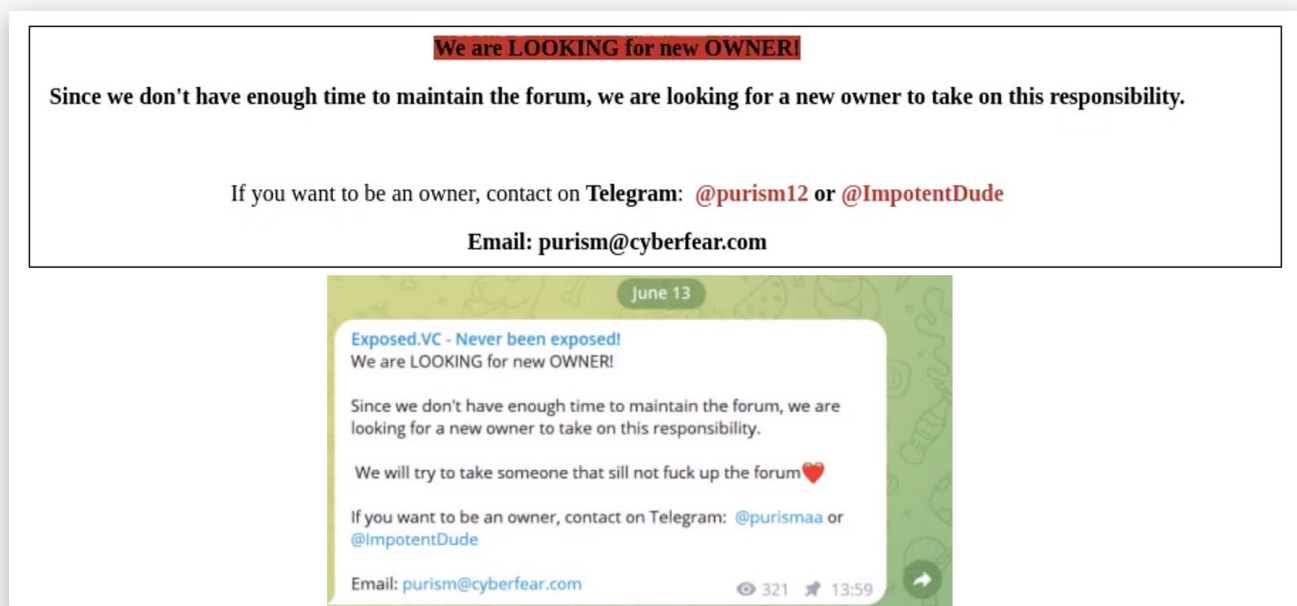


Figure 14: Messages on ExposedForum and Telegram announcing the forum was for sale.

Impotent was winning the forum wars battle and had established ExposedForum, which was becoming widely known, increasing in popularity, and had a stable growing userbase. Impotent always presented himself as confident and never backed down from a fight, so posting the forum for sale made little sense. Essentially, Impotent built the Exposed brand, which was quickly rising in popularity, when he abandoned the operation.

At the time of the sale, a potential buyer posted on Telegram to warn users that the sale was a scam. The buyer claimed he paid \$300, the first of an ongoing monthly fee, to become an administrator of ExposedForum. After the first payment, the buyer claimed

Impotent took their money and stopped responding. That was only \$300, however, and I can't imagine that if the whole thing was truly a scam, Impotent would have spent months building the brand to steal this minimal amount of money. There is more to the story. I asked Impotent if he took the potential buyer's money and he told me *"No comment, if anyone thinks I scammed them, they should contact me"*. However, the buyer did contact Impotent and posted to Telegram once Impotent stopped responding.

ShinyHunters

On June 15, BreachForums returned for a third time using new infrastructure and ownership. [ShinyHunters](#), a known hacking group affiliated with Baphomet and Pom, owned and managed the forum this time. All of them knew one another from their time on RaidForums. However, as you have read, Impotent did not play well with others and had a very adversarial relationship with Baphomet, Pom, and now ShinyHunters. Impotent warned ShinyHunters that if BreachForums returned, he would attack the forum.

I did not understand why both forums could not coexist. I asked Impotent why he had an issue with ShinyHunters, since his beef was with Pom and Baphomet. He responded, *"I dont know a way to communicate clearly with mentally ill people"*. He did not want to provide further context, but ShinyHunters were not new to the hacking community and had previously built a name for themselves. The group had a history of high-profile hacks and previously used RaidForums to sell and leak data obtained in their hacking campaigns. Due to this, when Impotent leaked the RaidForums Database, he also leaked ShinyHunters' account information, which did not sit well with them.



Orbitex	[REDACTED]
ShinyHunters	[REDACTED]@protonmail.com
Crenk	[REDACTED].com

Figure 15: Entry for ShinyHunters found in the RaidForums database.

As he promised, shortly after BreachForums was launched, Impotent attacked the forum. Impotent coordinated a [DDoS](#) attack against BreachForums, making it inaccessible. Impotent also continued his propaganda campaign while the site was down, putting out a narrative that it was a honeypot controlled by law enforcement. To back up his claims and make BreachForums users feel unsafe, Impotent posted BreachForums' backend IP address used to host and manage the website. Publishing the backend IP address does very little on its own, however, Impotent is good at using authentic data and misinformation to paint a narrative that benefits himself. The combination of the site's

unavailability, exposed IP, and the law enforcement rumors psychologically impacted the hacker community, who initially wondered if Impotent's claims were true. Others called out Impotent for his drama and tactics, speculating that cybercriminals would abandon ExposedForum for BreachForums, in response to the mess he created.

Exposed is Breached

In response to the DDoS attack, BreachForums administrators retaliated and launched a defacement attack on ExposedForum. As a result, when ExposedForum members visited the site, they were confronted with a website seizure message that imitated the banners used by government and law enforcement agencies during actual takedown operations. However, the message on the banner was highly personalized, stating that not only had law enforcement seized ExposedForum's servers, but also castrated its administrators! You can read the message yourself in the screenshot below.



Figure 16: Fake government seizure message seen on Exposed[.]vc implemented by competing rival forum, BreachForum.

Adding to the party, on June 18, 2023, OnniForum, another hacking forum that Impotent previously threatened, also targeted ExposedForum. OnniForum [posted](#) on their forum,

claiming to have revealed Impotent's real IP and email address. They alleged that they hacked and breached ExposedForum. shortly after Impotent terminated the sale of ExposedForum and closed the website. If you believe OnniForum, it was his post that led to the closure. However, others had attempted to dox Impotent previously, and that seemed to have little effect on his actions. The IP and email alone leaked by OnniFourm wouldn't be enough of a reason for Impotent to close the forum. Something else must have happened.

What Really Happened

If you believe Impotent, it's a coincidence he began looking for new ownership for ExposedForum at the same time BreachForums came back online. I believe that Impotent did not want to lose a very public battle with BreachForums and bowed out prematurely. The "Impotent Admin" told me himself that he **"needed money for our first phishing compaign [sic] :O) but still Exposed was great. I closed because BreachForums ofc [of course], but its no shame to give up when u jump higher than them. I wanted to keep it and sadly this happened. I made exposed [a] star"**.

Yet, with the previous arrests and spotty track record of BreachForums going on and offline in addition to actual law enforcement seizures and passing ownership from one entity to another, ExposedForum would've had a shot at maintaining its membership base if only it had maintained a stable presence. However, we will never know how that story would have ended. Building brands and prematurely tearing them down will happen again as we continue with Impotent's next endeavor, RansomedVC. In my opinion, Impotent underestimated himself as ExposedForum had gained momentum and left his mark on the hacking forum community.

The final nail in the coffin that officially ended the Forum Wars came from an unexpected player, the US Department of Justice. On June 23 2023, history repeated itself, and similar to the previous iteration of BreachForums, the DoJ seized the forum. **Maybe Impotent got out just in time.**

Note: The number of players, events, and forums involved in the "Forum Wars" has made this a challenging section to write. If you want to learn more about this topic, I encourage you to check out the excellent reporting from databreaches.net, which engaged with many of the threat actors mentioned when the events first occurred.

PART II:
THE RISE AND FALL OF
RansomedVC



Part II: The Rise and Fall of RansomedVC

It did not take long for Impotent to begin a new operation. He changed his name several times but settled on RansomedSupport, which he used to manage his new operation, RansomedVC. RansomedSupport set up the operation exactly the same as they did under the Impotent moniker, with Exposed. On **August 15, 2023**, the domain Ransomed[.]vc emerged with supporting Telegram-related channels and groups. In the first several days of the new operation, from 15 – 18 August 2023, the Ransomed[.]vc domain was a forum and not a ransomware data leak site as it was for most of its existence. You can see the early forum present on Ransomed[.]vc below as it looked on its initial launch. The Forum was initially named “Ransomed” Forum.

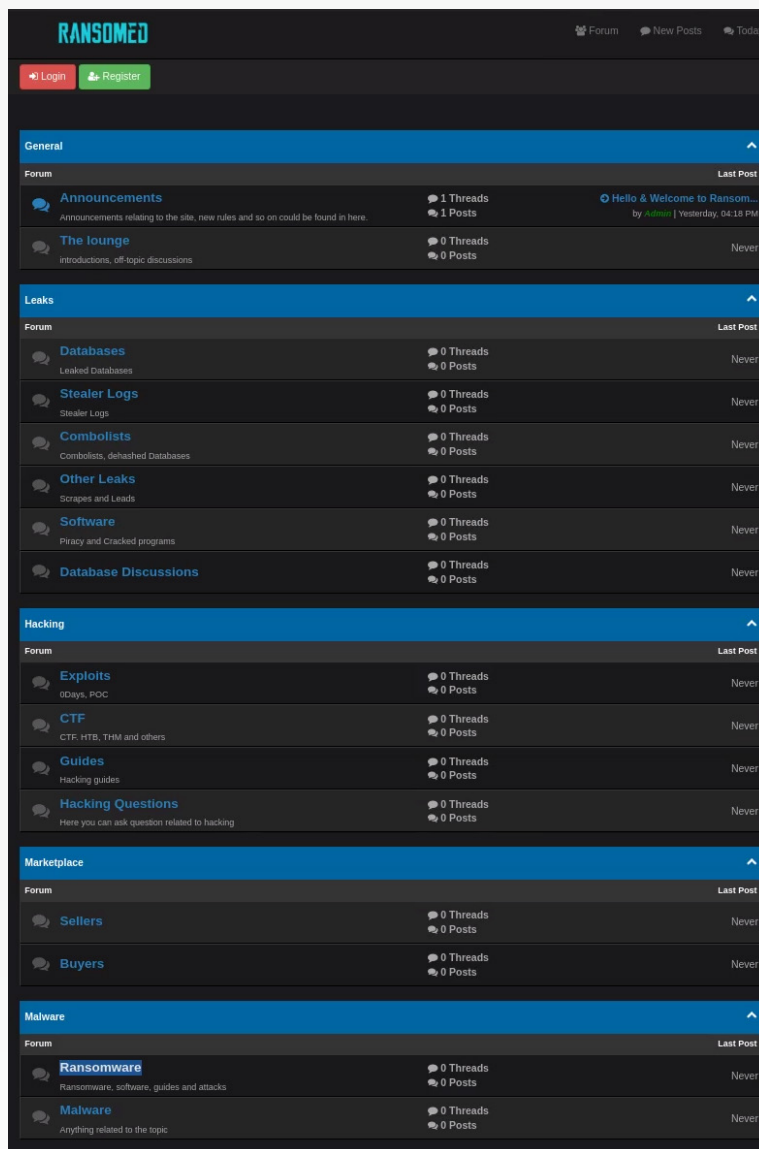


Figure 17: Ransomed forum from August 15th – August 18th.

Ransomed vs Exposed

The Ransomed forum present on Ransomed[.]vc may not have existed long, however, the first time I saw the forum, I immediately noted its similarities with ExposedForum. Beyond visual aesthetics, such as color and design, the new Ransomed forum shared many of the same forum categories found in ExposedForum, as compared below.

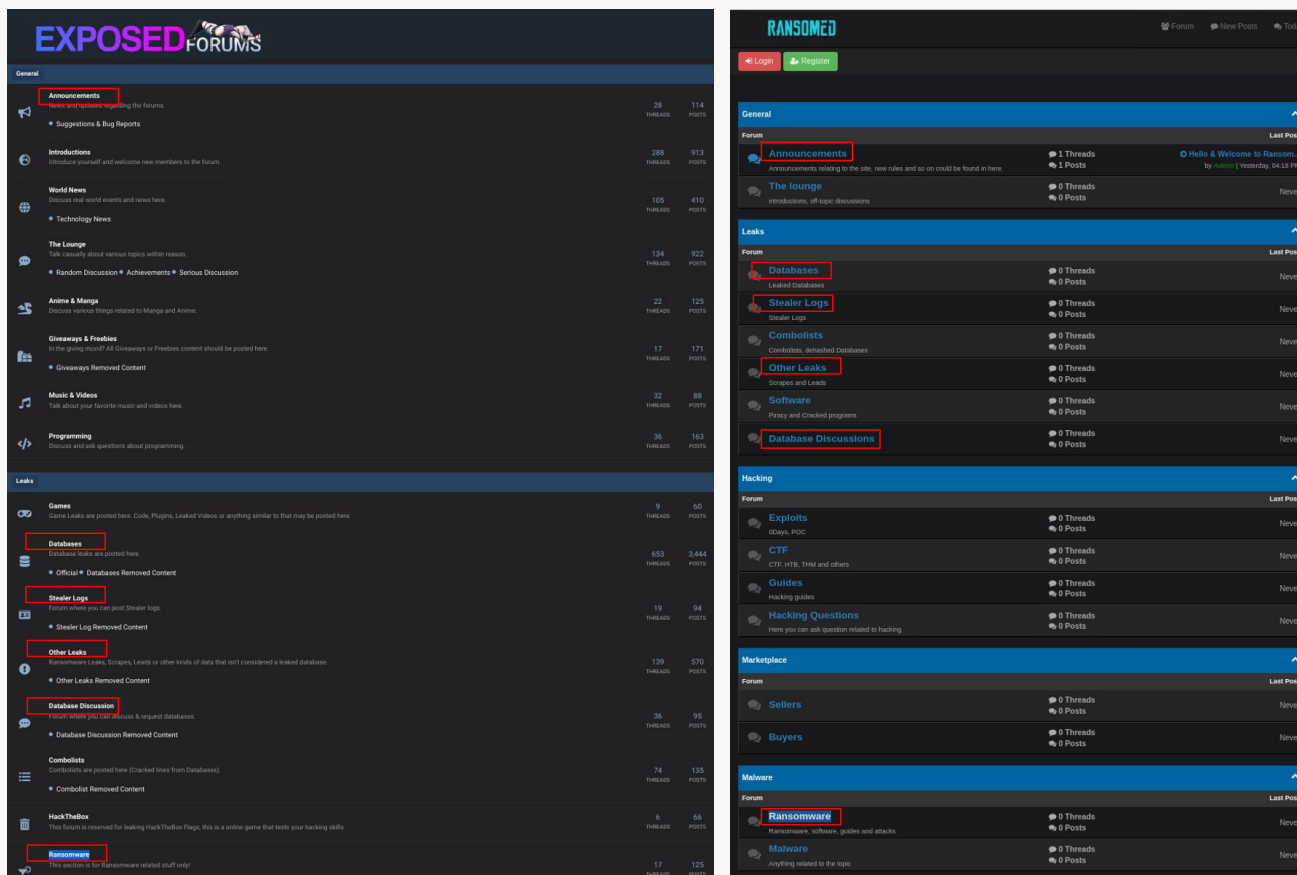


Figure 18: ExposedForum (left) compared to the initial forum style seen on the first several days of the RansomedVC forum (right).

You could argue these categories might be popular on any hacking forum, but with as many matching categories found, it caught my attention, and I wanted to present all the similarities between the two forums. Both Ransomed and ExposedForum shared Announcements, Databases, Stealer Logs, Other Leaks, Database Discussions, and Ransomware subsections. I also noticed that the corresponding Telegram channels/groups for both Exposed and RansomedVC shared many of the same members and followers.

Since RansomedSupport denied ownership of ExposedForum when I asked about the association, this time I believe he realized he should distance his new forum from the previous operation. This would explain why, on **August 19, 2023**, Ransomed[.]vc changed from

a forum to a ransomware data leak site. If I noticed the similarities between the two sites, others would also. You can see how Ransomed[.]vc looked after the initial update below:

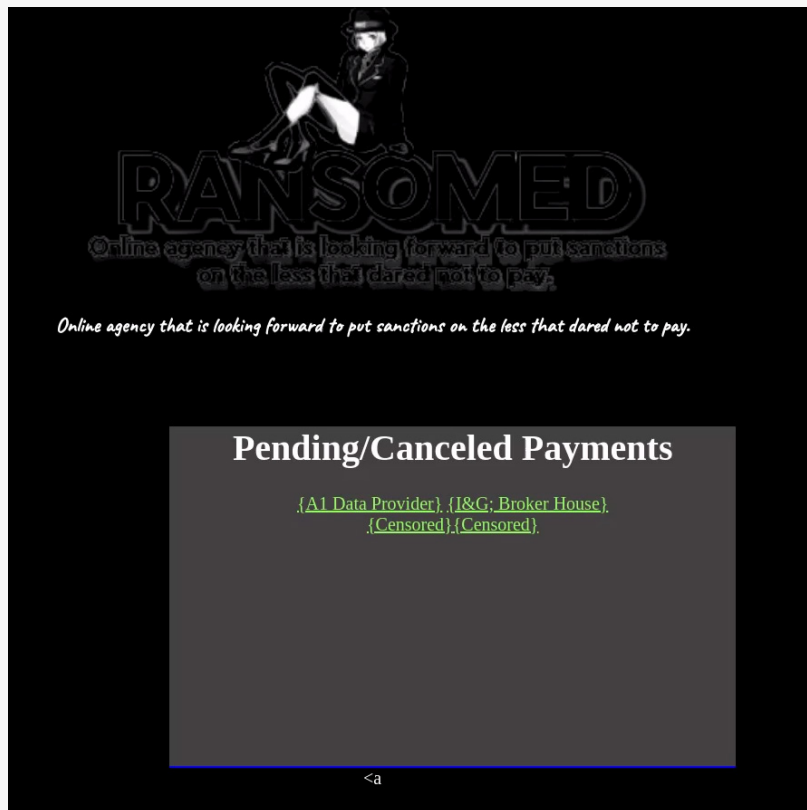


Figure 19: RansomedVC data leak site on August 19, 2023.

I also noticed a similarity with the RansomedVC logo used in early August. The logo was similar to BlackForums'. Remember, Impotent published the backend IP address hosting BlackForums in a post on ExposedForum. The similar branding was likely a continuation of the trolling effort. Perhaps RansomedSupport realized it might be obvious the new forum was established by the same leadership behind ExposedForum if they continued to troll BlackForums and decided to remove the logo before anyone noticed. You can see the similarities between the logo found on both sites in Figure 19, above and Figure 20, below.

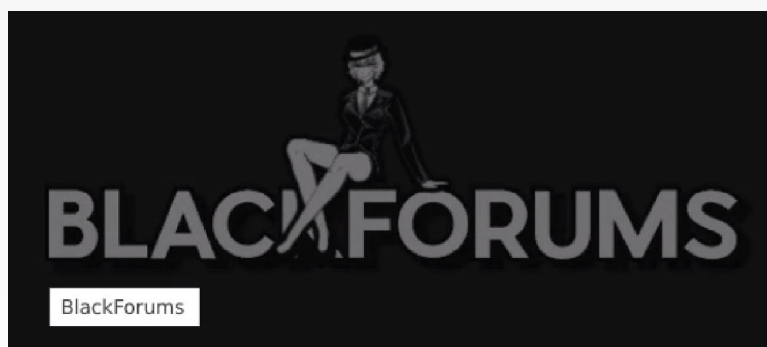


Figure 20: BlackForums logo.

[REsecurity](#), a cyber security company, reported another reference to BlackForums, which was initially identified by the Computer Security Incident Response Team of the Polish financial sector (CSIRT KNF). There was a reference to the Telegram account “@EOMLOL” in the source code of the Ransomed[.]vc landing page in August 2023 and later removed. The Information listed on @EOMLOL’s Telegram account includes a reference to the BlackForums user account “EOM”. That account primarily posts to the data leaks section of BlackForums. I asked RansomedSupport about the reference to the Telegram account in their source code, and this is what he told me:

Jon:

The account “[T.ME/EOMLOL](#)” was listed in the HTML source code of Ransomed[.]vc. EOMLOL has a presence on BlackForums. You also made your website resemble their landing page for a short time. What is your relationship/opinion of EOMLOL?

RansomedSupport:

This guy is a regular clown from the community who proposed to make our design. It was a temp design, (and) he wanted to have the credit, so I left it there.

There is one problem with the explanation. EOMLOL, was promoted to [Administrator](#) of BlackForums in May 2023. After the back-and-forth hacking efforts between BlackForums and ExposedForum, it seems odd that EOMLOL would help RansomSupport establish a new forum. Even if EOMLOL did not know RansomedSupport was previously behind ExposedForum which directly competed with BlackForums, I can’t see why an administrator of one forum would help another competing forum, which Ransomed[.]vc was intended to be before the site update. It also does not make sense that RansomedSupport trusted the admin of a forum he had a previous altercation with to design their website. It is also possible RansomedSupport placed the handle on the website source code to cause drama and distrust with EOMLOL and other administrators on BlackForums.

Regardless, that iteration of RansomedVC’s website was not present for long. Perhaps RansomedSupport realized it might be obvious the same entity behind ExposedForum established the new forum if they continued to troll BlackForums and decided to remove the logo before anyone noticed, or maybe EOMLOL realized RansomedSupport was really Impotent and asked for the tag and logo to be removed. This is another part of the story I cannot explain because it simply does not make sense. Could it be possible there is a working relationship between these competing forums, and the public events are conducted as a larger coordinated effort to increase their credibility and make headlines? For the most part, none of the breaches and defacements have revealed useful or damaging information about the forum or its administrators.

All the groups mentioned have various connections, background relationships, and small hidden clues to suggest larger ties. However, to make that assessment, I would need to dedicate time and effort to a stand-alone research report, which I cannot do within this report. So, for now, we will leave it as an unknown.

Note: For more information on the link between BlackForums, RansomedVC, and several other hacking groups, read [this report](#) published by the KNF CSIRT.

A few days later, RansomedSupport updated Ransomed[.]vc to include affiliate rules detailing the requirements necessary to join the new RansomedVC operation.

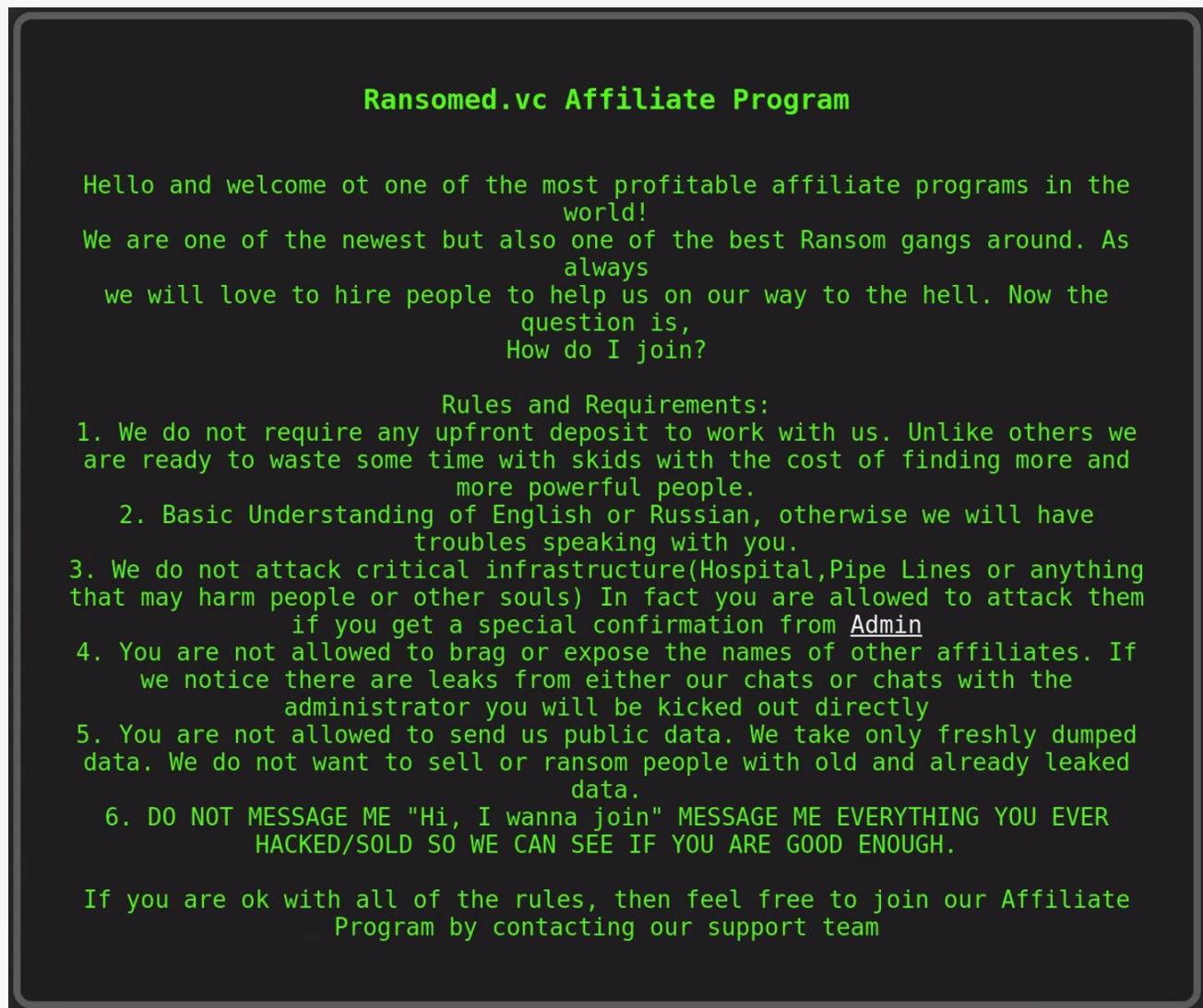


Figure 21: RansomedVC affiliate rules.

Now, RansomedSupport presented RansomedVC as a full-scale Ransomware-as-a-Service (RaaS) program.

I asked RansomedSupport why he switched the operation from a forum to a ransomware service, and he told me he “needed it as a proxy project for a ransomware gang that failed to have a good reputation, and I needed some more finances”. In response, I asked him what failed ransomware operation he referred to, but he did not wish to disclose the affiliation publicly. In addition to their site, RansomedVC recruited for their program on other forums and social media platforms. While they did not use it much, RansomedSupport even created TikTok accounts, which is something I have not seen a ransomware threat actor do before. Marketing RansomedVC on social media is an attempt to reach new audiences, which was important to RansomedVC. The group even claimed to hire an employee to conduct their PR, though I think this was likely RansomedSupport himself based on similar marketing and branding tactics. Below are images from a few of their accounts.

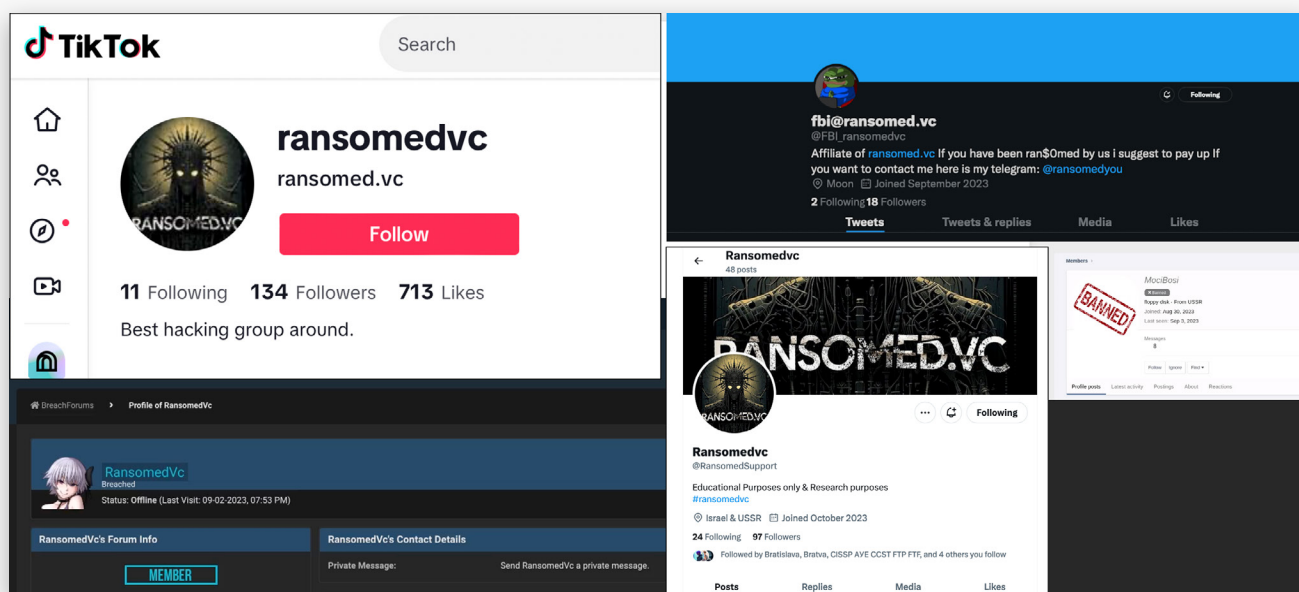


Figure 22: Example of RansomedVC social media and forum accounts created for use in influence and recruiting campaigns.

Note: A complete list of RansomedVC accounts and aliases can be found in the appendix of this report.

RansomedVC launched a strong ransomware recruiting campaign but did not target high-profile affiliates as you would expect. Instead, it was recruiting less-experienced hackers to support their program, who were much cheaper to employ. Plus, RansomedSupport felt he did not need to invest in paying established and experienced ransomware adversaries when he could get by with younger hackers who wanted to gain experience in a ransomware program. At the time, RansomedSupport already had a working relationship with two very experienced hackers, USDoD and Intel Broker. In response to a comment

LockBit posted on XSS in August 2023, RansomedVC stated that its affiliate program was for hackers who were “not [good] enough to join LockBit3”.

This is important to note as we discuss the legitimacy of compromises and data leaks RansomedVC claims responsibility for between late August and November 2023.

Significant Attacks

In early August, when the group first transitioned to a ransomware operation, they had victims listed on day one of the operation, which you can see in Figure 19. Since they were a new RaaS, I thought it was interesting that they already had victims and associated leak data present on the site. This could be associated with RansomedSupport’s claim he previously worked with another ransomware program, or it could be data acquired from his previous operation. You can see the posts below from the first victims, which appeared on Ransomed[.]vc in late August.

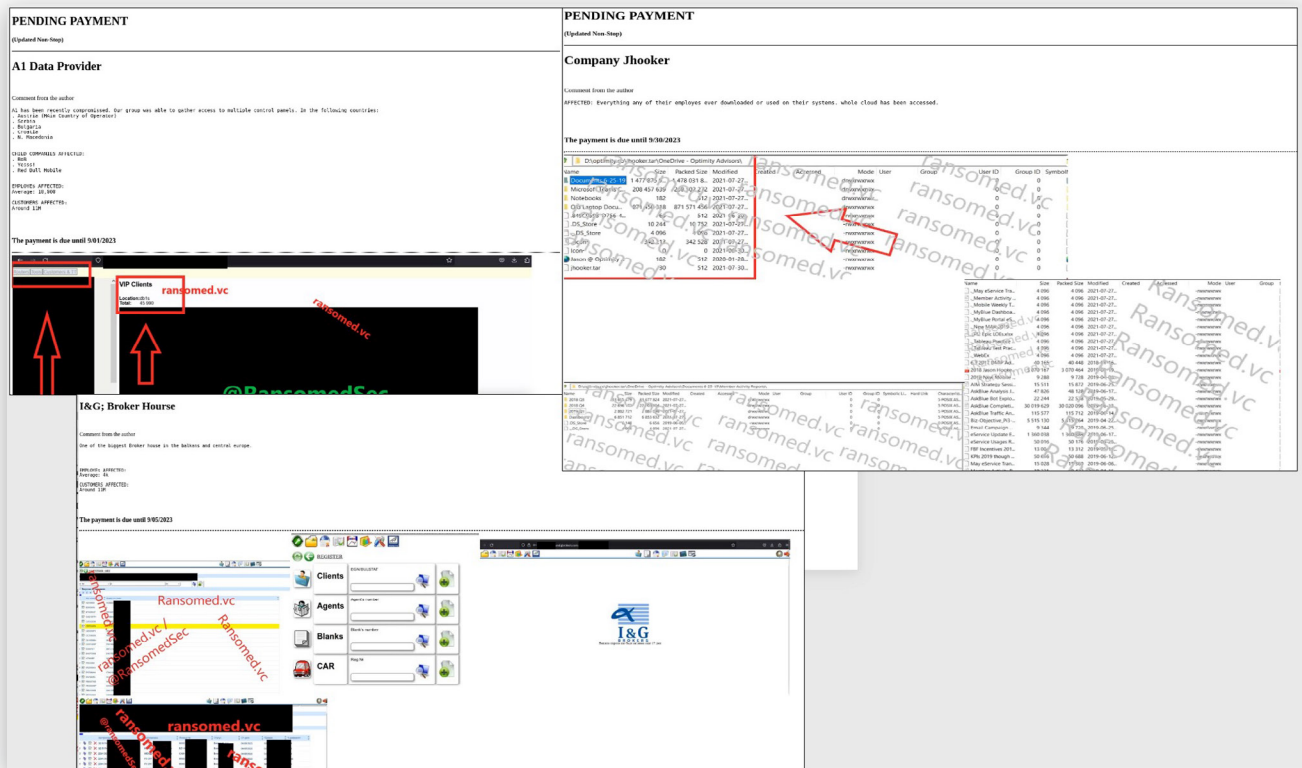


Figure 23: RansomedVC's first victims as seen on their data leak site in August 2023.

The screenshots show images from various directories from victim systems and images associated with their organization's data. The problem with screenshots alone is that the victim cannot validate data to confirm its authenticity. RansomedVC also posted the file tree associated with each victim's environment as further support that the attack

was real. The File Tree shows the internal directory structure associated with the stolen data. It's also possible to fabricate directory trees as they are merely text files, making them more for show than evidence of a breach, though many groups use this tactic since posting data requires additional infrastructure and resources (just ask LockBit!).

Still, according to RansomedVC's leak site, one victim, A1, partially paid the ransom. RansomedVC appears to allow installment payments. This is a new tactic that I have not seen used by other criminal ransomware groups and seems like a strange concept since most companies either pay or don't. However, in late August, the threat actor updated A1's victim post claiming A1 made one of four payments and had until **August 25th** to pay the next installment.

Another victim shown in Figure 23, I&G Broker House, had until **September 5, 2023** to pay RansomedVC's demand. The payment period passed, and I&G did not pay. Normally, victim data is leaked or placed for sale once the payment deadline ends, but that did not happen. Instead, thirteen days later, on **September 18, 2023**, a RansomedVC affiliate who goes by the alias "BankManagers" created a post about the I&G victim on XSS, the Russian-speaking forum I mentioned earlier. The affiliate was not selling I&G data as I would expect after a victim missed a payment deadline. Instead, the post mimicked the original leak notification, which is typically used to publicize an attack in hopes that public awareness will pressure the victim to pay. This was strange since the tactic is only effective during the payment window, not weeks later. There is no value in making a victim notification post like this on a forum like XSS unless to sell the data. Based on this, I believe the XSS post was another attempt to gain attention and promote RansomedVC to other ransomware criminals and had little to do with the victim or the alleged stolen data itself. The post made by the RansomedVC affiliate can be seen on the next page.

The payment period passed, and I&G did not pay.

Based on defaulting on their threat, it looked like RansomedVC did not have the data to sell, and I believe this was an empty threat. Then, on October 8, 2023, over a month after the payment deadline terminated, RansomedVC put I&G data for sale on their site. Later, USDoD provided information, that led me to validate that the compromise and victim data was authentic. **All the noise around the I&G breach represents the confusion, misinformation, and circus surrounding most of RansomedVC's ransomware campaigns.**

You never know when victims are true victims or if the data theft is legitimate. Sometimes it is, and other times it's a fairy tale. You might think this makes RansomedVC less dangerous, but it makes them worse than traditional ransomware threat actors since you cannot easily evaluate the threat or the validity of their claims.

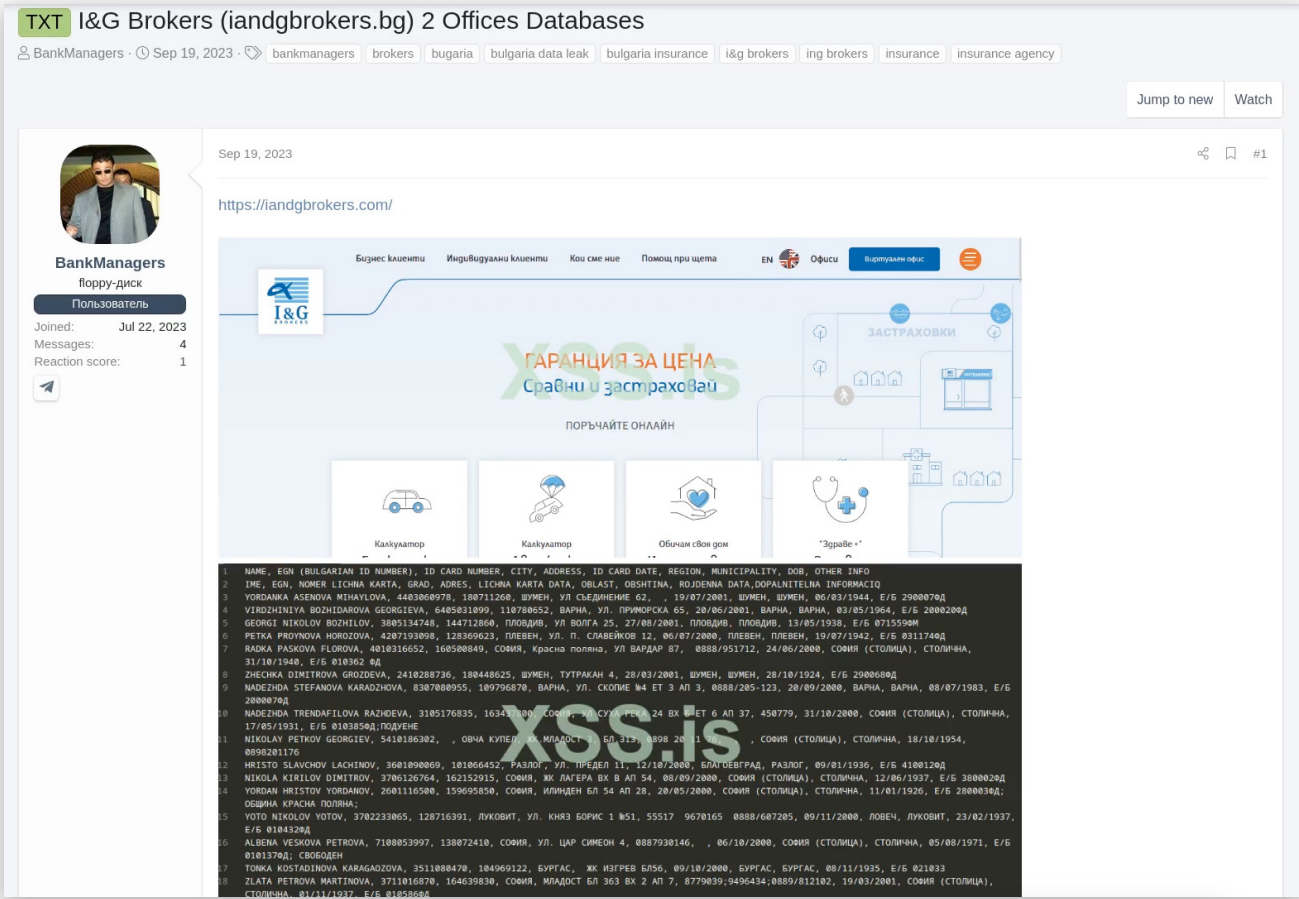


Figure 24: RansomedVC affiliate post made in September 2023 on the XSS forum.

The Transunion Debacle

On August 26, 2023, RansomedVC announced they breached the consumer credit reporting agency [Transunion](#). Several events transpired after the announcement which contradicted RansomedVCs account of the attack. This incident demonstrates how RansomedVC leverages stolen data to maximize media attention, increase brand awareness, and sometimes make money.

What RansomedVC told us:



Figure 25: RansomedVC leak post for Transunion.

RansomedVC stated that they had stolen “*everything any of their [Transunion] employees ever downloaded or used on their systems*” and that Transunion’s cloud “*database has also been exported*”.

If these claims were true, the data stolen by RansomedVC could impact millions of citizens for whom Transunion collects and stores data. Since the data held by Transunion is used for credit reporting services, it’s exactly the type of data criminals can use to steal your identity and open fraudulent financial accounts in your name. All of which leave a mark on your credit that can take months or years to reconcile – if it can be accomplished at all. It can affect your ability to obtain a loan, get insurance coverage, and any benefit or service requiring good standing credit. Given the sensitive nature of the data allegedly stolen by RansomedVC, media outlets worldwide reported the attack which was also discussed heavily on social media.

In response to the RansomedVC’s claim and associated media attention, Transunion released the following [message](#):

“Through our investigation, we have found that multiple aspects of the messages – including the data, formatting, and fields – do not match the data content or formats at TransUnion, indicating that any such data came from a third party.” – Transunion

Based on my research, it appears RansomedVC did have data related to Transunion, so their blanket denial was a bit misleading. I say “related” because the data RansomedVC acquired and threatened to leak was taken from a third party connected to Transunion, which they clarified in their public statement. The fact that the stolen data did not come directly from Transunion’s systems is irrelevant since it is associated with their use of consumer credit services and originated from a third party which the organization conducts business. In my opinion, Transunion’s statement brushed this off since it came from a third party which I have an issue with since it is data associated with their organization. Stronger action and accountability should be the bare minimum in their response. Transunion did not provide any context to explain what information was lost or how it could impact its customer base. The third party did not either. The only entity that did explain was the RansomedVC, who we can’t trust because they are criminals. This was a lose-lose situation for the victims whose data was not protected.

What Really Happened:

So, the question is, did RansomedVC steal the Transunion-related data themselves or obtain it from a third party? The answer is both. In March 2022, more than a year before RansomedVC made their claim, a criminal breached and stole a 3GB database that

contained sensitive credit-related information associated with over [58,000 individuals](#). The information included names, dates of birth, passport numbers, loan account information, employment details, and other Personally Identifiable Information (PII) used by Transunion.

The data also included internal Transunion identifiers, which is one reason I have such an issue with Transunion's dismissal of the incident. It turns out that RansomedVC got Transunion's data from the hacker I mentioned, USDoD, who brought it with him to RansomedVC when he began working with the group. He also shared details about the incident with me, which allowed me to validate the data. I assess with strong confidence that the leaked data did contain PII and Transunion-related information.

RansomedVC's high-profile criminal operation and leak site provided an opportunity to pressure Transunion in the hopes it could extort the company for payment to delete the data, and if not, they could reach many potential buyers. Yet, in the end, USDoD did not benefit from his work. According to USDoD, RansomedSupport only paid him \$1k, which was a small fraction of what he was owed, for the Transunion-associated data. Several hackers who claim to have worked for RansomedVC have told me similar stories of either not being paid at all or only receiving a minimal amount of what was promised to them.

In the end, how RansomedVC obtained the data is irrelevant. The important aspect is that they obtained authentic data related to Transunion, which garnered attention from the media and the security community, including myself. This attention increased the value of the data on the criminal market, enabling RansomedVC to profit by selling it to other criminals. Judging by Transunion's response, it didn't seem to care much either. The only ones who suffered in this incident were the innocent people whose data was stolen.

The only ones who suffered in this incident were the innocent people whose data was stolen.

RansomedVC's Makes a Friend!

In September, RansomedVC continued its effort to extort new victims. The first notable event was the collaboration with the **Everest Ransomware group**. Both RansomedVC and Everest created victim leak posts for SKF, PSM, and State Farm Insurance. To confirm the [collaboration](#), the two ransomware groups announced they worked together to breach these companies on their data leak sites.

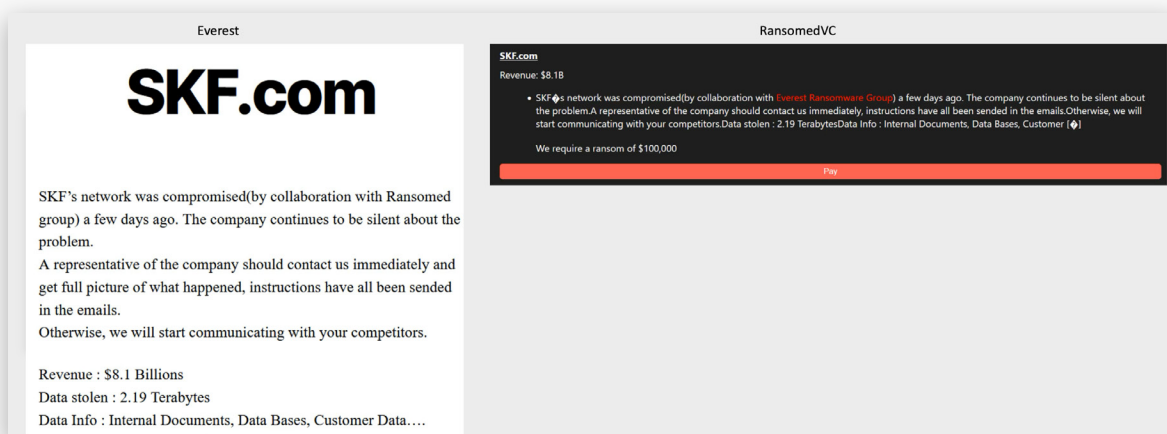


Figure 26: Collaboration messages from Everest and RansomedVC ransomware groups.

These breaches are the only joint attacks conducted by the two groups. Once again, no data was posted to the data leak sites. The ransom demand from SKF exceeded other extortion demands seen with RansomedVC targets. This higher demand can be attributed to the fact that RansomedVC and Everest would share the proceeds. Based on the entries on RansomedVC’s and Everest’s sites, it appears that SKF did not pay. In a previous incident in 2021, the BlackMatter ransomware gang compromised and exfiltrated 40GB of data from SKF. SKF also did not pay Blackmatter’s ransom demand in that case, which raises the question of why RansomedVC and Everest would expect a different outcome this time. It is possible that the stolen data from the recent attack was repurposed from the BlackMatter leak, which could explain why the data was not leaked.

You Have the Right to Remain Ransomed

In late August, RansomedVC claimed to have breached and stolen data from State Farm Insurance. Several days later, on **September 2, 2023**, Everest, who supported the attack, posted about the incident on their website. The post followed the same pattern as previous attacks, showing screenshots of a database without providing any sample data for validation. Both threat actors asserted that the compromised database contained “400,000,000 customer insurance records.” However, no evidence supports their claim that they obtained State Farm’s data, and I remain skeptical about its authenticity.

This incident is reminiscent of the SKF breach, where previously [leaked data](#) may have been repurposed in a current attack. If RansomedVC/Everest indeed possesses State Farm data, I strongly advise State Farm to compare it with the data obtained from the earlier breach. Considering the lack of substantial evidence, I believe this incident may have been fabricated or the data is less sensitive than what RansomedVC claims. Therefore, I was surprised to learn that a [class action lawsuit](#) was filed against State Farm several months later, in November 2023.

According to ClassAction[.]org, a site dedicated to class action suits, a suit was filed against State Farm due to a breach in August 2023 that resulted in the loss of 400 million records. The timeline and associated loss of data align with the RansomedVCs allegation. The initial court filing claims that State Farm did not disclose the breach or notify affected parties whose data was now “in the hands of cybercriminals” and “[State Farm](#) could have prevented the data breach by properly vetting and monitoring its systems”.

The insurance company [responded](#), “State Farm denies the allegations in the complaint, which are factually and legally baseless”.

I assess that RansomedVC fabricated the breach, which is why they cannot provide State Farm, the public, or myself with sample data to validate its authenticity. It was RansomedVC who first alerted the media that they attacked State Farm. Once the media began reporting the event, a snowball effect emerged, and State Farm customers believed the ransomware group had stolen their data and sold it to other criminals. **RansomedVC leveraged the media to build credibility that the attack was legitimate.** The media coverage caused State Farms customers to panic, leading them to file suit. This brings a new concern about how ransomware attacks affect companies and their clients. Imagine the amount of money State Farm will spend to fight a legal battle built on a false narrative willed into existence by criminals. **This is truly diabolical.**

I understand why State Farm’s customers filed the lawsuit, as RansomedVC generates a lot of noise and surrounds its attacks with propaganda, making it extremely difficult to distinguish what is real and what is not. I also understand why journalists report on such attacks. Most of the high-profile attacks you read about are genuine, and it is less common for a ransomware group to fabricate an incident.

In my experience, most ransomware groups care about their reputation and avoid jeopardizing their credibility by making unsupported, fictitious claims. Fabricating an attack and using the media to such an extent is something I have not witnessed before. After this incident, researchers, including myself, and the media should take a step back, analyze the evidence, and publicly report a threat actor’s claim only when it can be verified. Further, I would suggest not reporting a RansomedVC incident unless the victim validates the breach took place. The situation State Farm is going through should never happen again.

A Juice Box a Day Keeps Ransomware Away

Other notable attacks claimed by RansomedVC in September include Hawaii Health System. RansomedVC posted an entry for Hawaii Health on **September 2, 2023**, and

added a link to a snapshot from archive[.]org of what it claimed was a defacement of the site. The problem is when you go to the archive from RansomedVC’s post, it does not lead you to Hawaii Health’s website, which is “hpsc[.]org”. Instead, RansomedVC defaced “https://healthybydefault.hawaii[.]gov”, a website that provides compliance and policy information related to healthy beverage options for children and is used as guidance for restaurants in [Hawaii](#). You can see the defacement and its URL below.

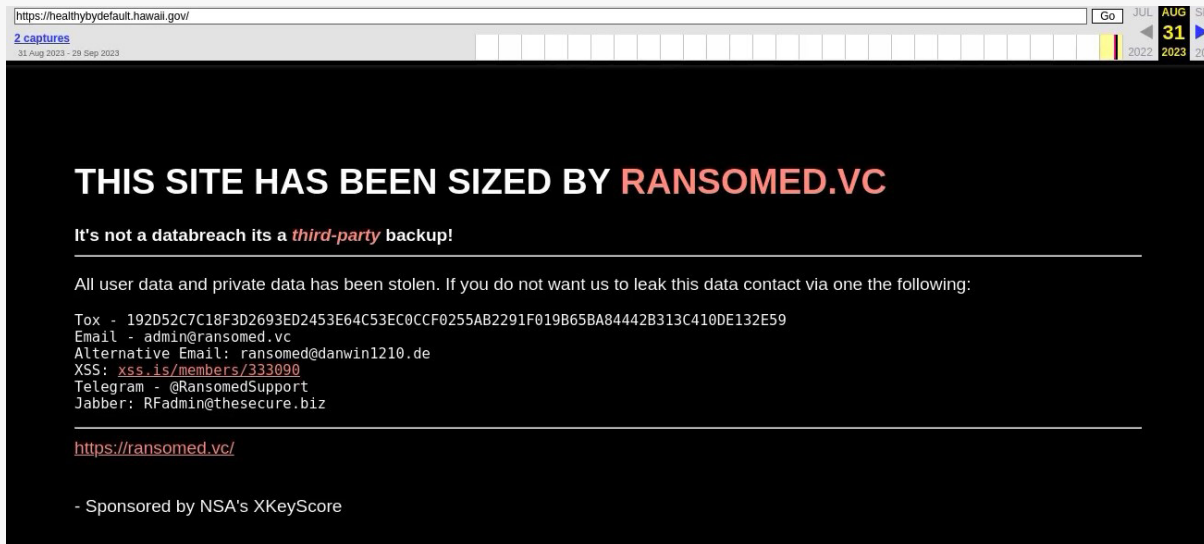


Figure 27: Site defacement seen on healthbydefault[.]hawaii.gov.

The attack would have been more significant if RansomedVC had breached and stolen data from Hawaii Health Systems. However, despite being a “.gov” hosted site, HealthybyDefault has little value for extortion or defacement purposes. An official from Hawaii’s Department of Health, told [Jonathan Grieg](#), a journalist for Recorded Future News, that the HealthybyDefault website is externally hosted, meaning it is not connected to other government sites or systems and was in its pre-launch phase at the time of the attack, populated only with test data. As you can imagine, no one will pay a ransom to prevent publicly available policy information related to children’s beverage nutrition from being leaked. This is another example in which you can see how RansomedVC manipulated the situation to try and fabricate a victim and leverage the narrative to obtain an extortion payment.

The Sony Breach

On **September 26, 2023**, RansomedVC claimed it hacked Sony, stealing 260GB of data. Unlike many of the breach claims I have discussed, RansomedVC posted sample data this time. In the I&G Brokers breach, I discussed how RansomedVC waited over a month before posting the victim’s data for sale after the extortion deadline had passed. In the

Sony incident, the exact opposite took place. Two days after creating the Sony victim post, RansomedVC updated their site, declaring, **“We have successfully compromised all of Sony systems . We won’t ransom them! We will sell the data due to Sony not wanting to pay. DATA IS FOR SALE”**.

When a threat actor changes their tactics and behaviors, I always look for the cause that led to the effect resulting in the change. In this situation, I wondered why RansomedVC would rush such a large corporation with deep pockets who could easily pay the ransom amount demanded by the gang. As I mentioned earlier, RansomedVC demands far less than most ransomware groups seen today. Based on their leak site information, most of their extortion attempts are for less than \$100k, with a few exceptions. Sony, like other victims I have discussed, had data stolen and leaked previously. The ClOp ransomware group compromised and stole data from Sony and hundreds of other companies in the [MOVEit](#) related attack, which took place in May 2023. While unlikely, I needed to rule out the possibility that this was the same data from the ClOp incident. The data from the RansomedVC breach looks to have originated from a single Sony system, likely located in Japan based on its language settings seen in the sample data, as opposed to the ClOp breach, which affected much of Sony’s US infrastructure.

RansomedVC demands far less than most ransomware groups seen today

Further, the data acquired by RansomedVC was stolen on August 10, 2023 based on screenshots and dates within the stolen data set, not May. Since the data is unrelated to ClOp and appears authentic, you might conclude that RansomedVC did breach Sony and steal its data. However, like most RansomedVC breaches, there was more to the story.

On September 26, 2023, the same date RansomedVC put Sony’s data up for sale, a hacker using the moniker “MajorNelson” created a post on the latest iteration of BreachForums. MajorNelson accused RansomedVC of lying and scamming “gullible” journalists to gain influence. He implied that he, not RansomedVC, had stolen the data, but there is little evidence to determine who stole it first. If MajorNelson did steal the data, how did it end up in the hands of RansomedVC, or vice versa?

Below, you can see both RansomedVC and MajorNelson’s posts about Sony’s data.

After examining the data leaked by Major Nelson and comparing it to the sample data acquired by RansomedVC, I discovered that the screenshots and files obtained by RansomedVC were also present in Major Nelson’s data. The Sony accounts, passwords, and computer names were consistent between both data sets. This is why RansomedVC quickly posted the data for sale instead of extorting Sony.

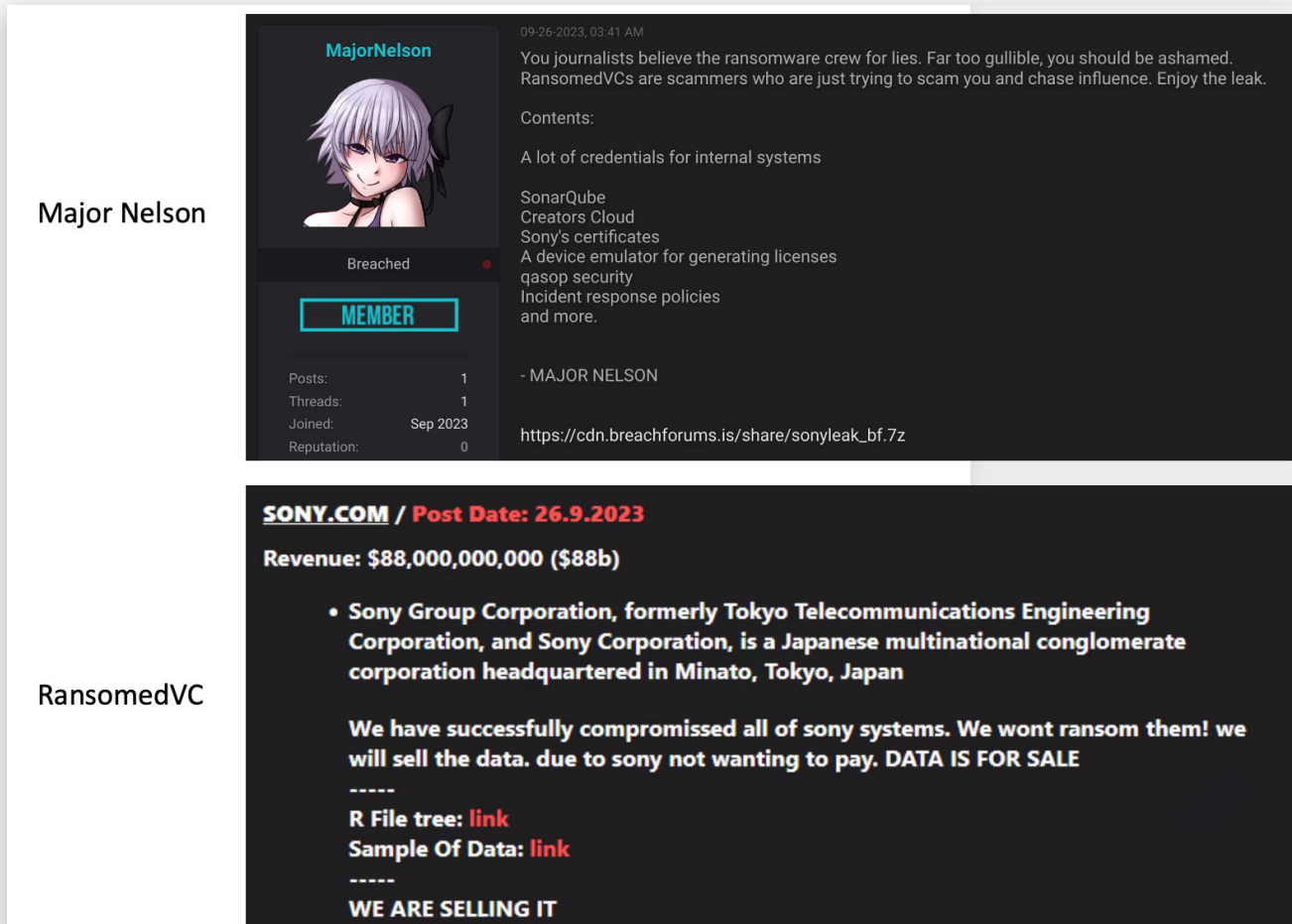


Figure 28: Major Nelson & RansomedVC's posts associated with stolen Sony data.

If they had made an extortion demand and waited for a response from Sony, they would have looked foolish if a third party leaked or sold the same data. Instead, they hoped to sell it to another criminal and make a profit before MajorNelson could have a chance to do the same. Once, MajorNelson realized RansomedVC was selling the same data he possessed, he decided to leak it to prevent RansomedVC from benefiting from the sale.

I asked RansomedSupport if he obtained the data from Major Nelson, and he said no. He also told me that he did initially attempt to extort Sony:

Jon:

So, you did not extort Sony because the Nelson dude was going to leak it and you had to try and sell it before he could?

RansomedSupport:

No, I was extorting Sony actually.

I got nearly paid, until they investigated, lol.

Jon:

Did you steal the Sony data from Major Nelson or was it the other way around because I looked and the data you leaked is also what he leaked.

RansomedSupport:

no

RansomedSupport:

Its intel broker who trusted him to give the data and was to [sic] ashamed to say he was working for me

:DDDD

Now you have RansomedSupport's account of what happened with the Sony data. The claims and allegations have varied since September, when it was first posted to the leak site, making it difficult to know who is telling the truth. Still, there is a pattern where RansomedVC obtains data from others and uses it to extort victims. RansomedVC is known for stealing data from other criminals, but I have not witnessed other criminals successfully stealing from them. Therefore, I believe it is more likely that Major Nelson had the data first. This is why many criminals do not trust RansomedVC. They target not only corporations and businesses but also other criminals. Still, it was Sony who suffered the greatest loss. Although the stolen data itself was not very damaging, the public embarrassment resulting from the attack was significant.

Note: If you want to know more about Intel Broker, HackRead does a good job detailing his breaches which you can read about [here](#).

Don't Make Putin Come to My House

There is one rule that is sacred to almost all ransomware gangs operating today: do not target Russia or other countries within the Commonwealth of Independent States (CIS). The rule is followed by ransomware syndicates with one exception, RansomedVC. On October 4, 2023 RansomedVC posted a victim notification for a Russian medical center (medcentertambov[.]ru). Of course, I had to ask RansomedSupport about this one.

Jon: You are the only group I have ever seen target a Russian-based organization, AND it was a hospital.

RansomedSupport: Don't make Putin come to my house, please!

RansomedSupport: Wasn't it a plastic surgery company?

Jon: It's listed on ransomware watch-list sites as a "Medical Center"?

RansomedSupport: I was probably high at the time of posting and don't remember, lol.

RansomedSupport: I posted it, yeah.

RansomedSupport: Well, I wanted it to be a detrace mostly.

RansomedSupport: The center was provided free decryption even though I used 3rd party RA.

I do not believe RansomedSupport encrypted systems because no other victims have reported encryption being used in an attack by RansomedVC. However, it is possible that RansomedSupport regretted targeting the organization since they have yet to attempt to sell the medical center's data. Yet, if RansomedSupport truly felt remorseful, they could have removed the post entirely from their leak site. As we have established, RansomedVC is not always truthful, but I cannot think of any sane reason to fabricate the extortion of a Russian medical center. However, given this group's behavior, I would not put anything past them.

RansomedSupport was incorrect in his claim the victim was a plastic surgery center and not a medical center. You can see from the organization's website below that they cater to many types of medical treatments, as you would expect at a hospital or medical center.

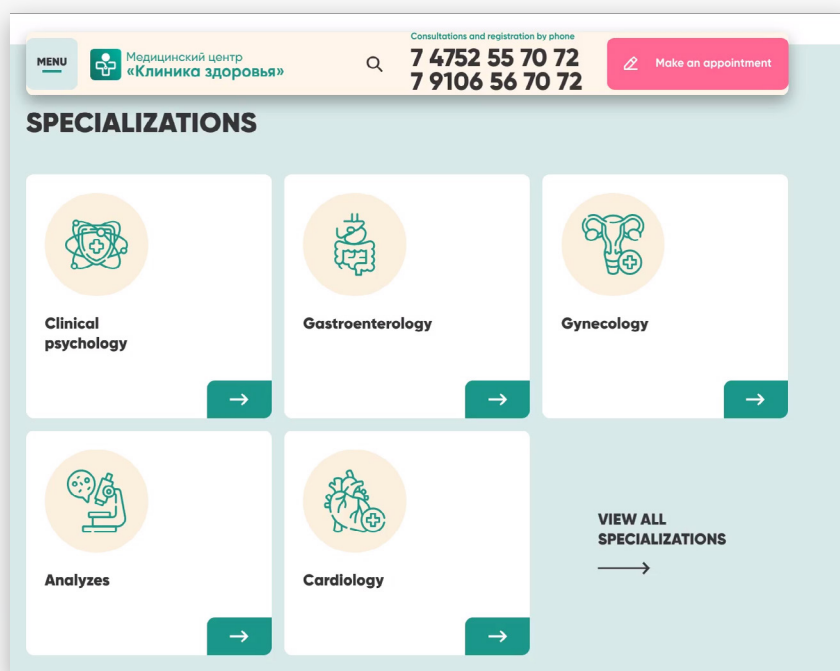


Figure 29: Screenshot of services offered at medcenter-tambov[.]ru.

If RansomedVC did not actually attack the medical center but instead made the whole thing up, it shows RansomedVC will do anything to gain attention, regardless of the consequences.

Rob, The Notorious Threat Actor!

If you lived on the East Coast of the United States in May of 2021, you remember driving from gas station to station looking for fuel after the pipeline shutdown due to an attack conducted by the Darkside ransomware gang. So when RansomedVC announced the breach on Friday, **October 13th, 2023**, it was concerning. In a post on their leak site, the gang [announced](#), **“We have successfully taken control of the data of Colonial Pipeline”**. Adding to the legitimacy of this announcement, RansomedVC leaked 5GB of data on their Telegram channel to prove they accessed Colonial Pipeline’s internal infrastructure. The data included industrial control systems (ICS) and supervisory control and data acquisition systems (SCADA) related documents and diagrams, which initially appeared genuine. The same evening, in response to questions from Dissent at databreaches.net, Colonial put out a [statement](#) responding to the allegations:

“Colonial Pipeline is aware of unsubstantiated claims posted to an online forum that its system has been compromised by an unknown party. After working with our security and technology teams, as well as our partners at CISA, we can confirm that there has been no disruption to pipeline operations and our system is secure at this time.”

The data looked real, but Colonial claimed they were secure and had not been compromised. My first thought was that the data could be from the previous breach in 2021, but according to [Colonial](#), that was not the case:

“Files that were posted online initially appear to be part of a third-party data breach unrelated to Colonial Pipeline.”

If the documents were not from the previous breach and unrelated to the pipeline, why were their names and logos all over the data? Now, I was confused. I did not think Colonial would lie if they were breached after what happened the first time, so I presumed they believed what they said in their statement. However, once again, things were not making sense, and the information from each party contradicted one another.

Luckily, I did not have to wait long for a sensible answer to explain what happened. RansomedVC cleared up the situation, stating that the whole thing was the fault of a notorious threat actor, Rob Lee of Dragos! Statements like this make my job fun. Rob Lee is the CEO of the cyber security company “Dragos”. He is not a threat actor, which is why I found the statement so amusing.

To support the claim, RansomedVC released images on its leak site showing what it claimed were email communications between the ransomware group and Rob. Since

RansomedVC has a long history of lying and fabricating data, I have decided not to repost images of the email exchange as they are likely fabricated. However, I want to discuss the statement RansomedVC included in its post, as it provides clues as to why the gang is so motivated to slander Rob and Dragos.

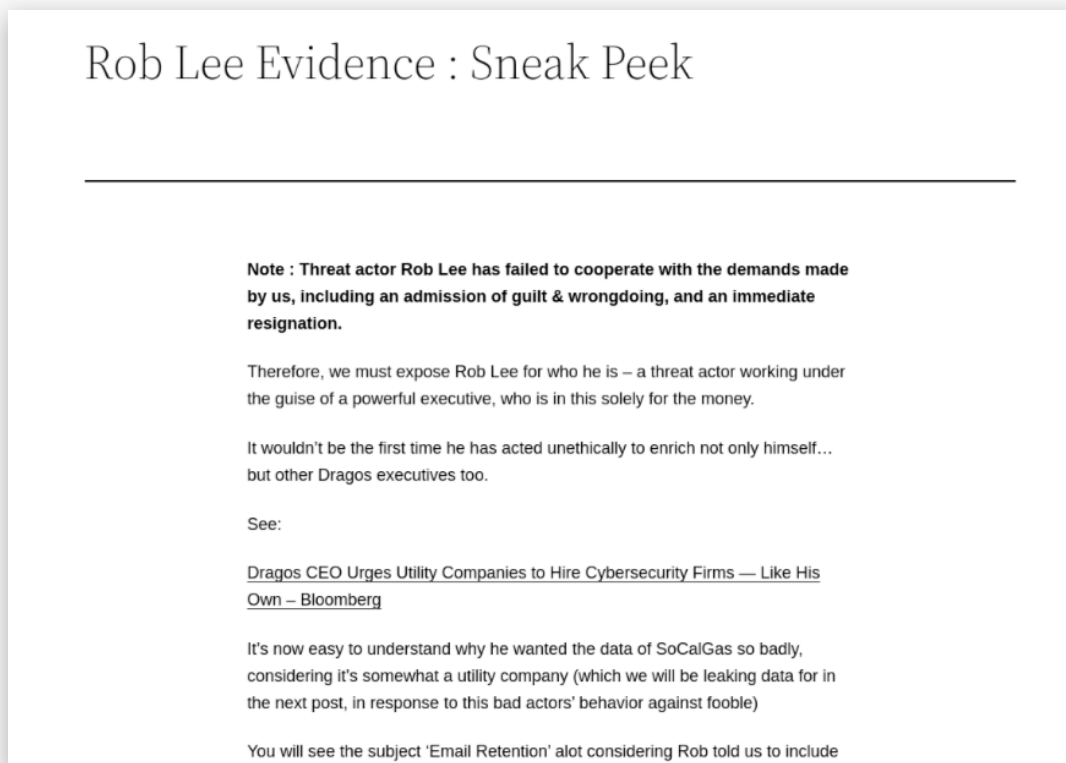


Figure 30: Post and email images surrounding Rob Lee and RansomedVC communications as seen on RansomedVC's leak website.

Apparently, RansomedVC wanted revenge against Rob for the way he and Dragos treated someone named “Fooble” in regard to data associated with SoCal Gas. Rob’s company, [Dragos](#), is a cybersecurity company that specializes in securing and protecting operational technology (OT), ICS, and SCADA infrastructure and [SoCal](#) Gas is a natural gas distribution utility company so it seems logical that SoCal Gas would be the type of business that would utilize and benefit from the services and specialization that Dragos offers. If you believe RansomedSupport this is why Rob wanted data from Fooble associated with SoCal.

Who the hell is Fooble, you ask? Since RansomedSupport is defending Fooble and seems upset about how Rob treated them, Fooble is likely a threat actor or a player in the criminal community. I began searching Telegram and hacking forums for accounts with this name and found the account existed on the well-known Russian-speaking underground forum “Exploit”.

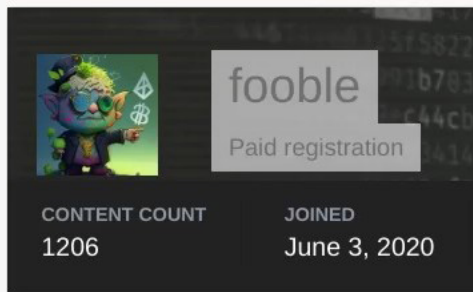


Figure 31: Fooble account on the Exploit forum.

The person behind that account has posted on Exploit over 1,200 times since June 2020 and has a good reputation on the forum. Fooble has bought and sold access to breached entities and often discusses malware, botnets, crypto, and has an interest in financial-related cybercrime. I also found a [blog](#) detailing Fooble's activity from 2021, when it was seen selling "700 Citrix, VPN, and RDWeb compromised network accesses".

To summarize, Fooble is a well-versed hacker who uses their skillset to compromise vulnerable targets and then sells access on dark web forums to other criminals. Based on this context, I believe RansomedVC is insinuating that Dragos had some engagement with Fooble that went poorly. Perhaps Rob and Dragos mitigated a threat executed by Fooble to protect their customers, but there is no way to know for sure. Regardless, **I don't believe RansomedVC's claim against Dragos or Rob, the Notorious Threat Actor!** While this may explain RansomedVC's motivations, it does not answer my questions about the Colonial Pipeline incident.

So, I asked RansomedSupport about the leaked data, and he answered: "**it was from the same colonial pipeline hack (in) 2021**". Regarding Rob being a threat actor, RansomedSupport responded that "**it's mostly for the troll**". This part about Rob was one of the few times the threat actor told the truth. Still, based on information provided in Dissent's blog, and my own research, the majority of the data was not taken from the 2021 breach. So where did it come from? Well, at the time of the incident, Dissent asked RansomedVC, and the gang provided a different answer than what it told me. [RansomedVC told Dissent](#) that "**Accenture (was hacked), but Rob (Lee) bought the files as leverage to poach Colonial Pipeline from Accenture.**" RansomedVC also told Dissent that Fooble targeted an employee with a phishing email to gain access to the data seen in the leak.

While I am always hesitant to believe anything RansomedVC says, the explanation it gave to Dissent is plausible. Yet, neither Dissent nor I could conclusively validate that the data came from Accenture, though there were a few folders that appeared to be related to the Accenture found in the Colonial Pipeline leak. Based on Colonial's account of the breach,

the Accenture claim fits well with the known details surrounding the attack. Colonial Says the data came from a third party, and since the data does not appear to be from the 2021 breach, Accenture may be where it came from. Still, with so many lies from RansomedVC, there is likely more to this story than what we know.

Ransomed Forum Returns

On **October 22, 2023**, RansomedVC announced on social media and their website that they were launching a new dark web forum. You can see the announcements below.

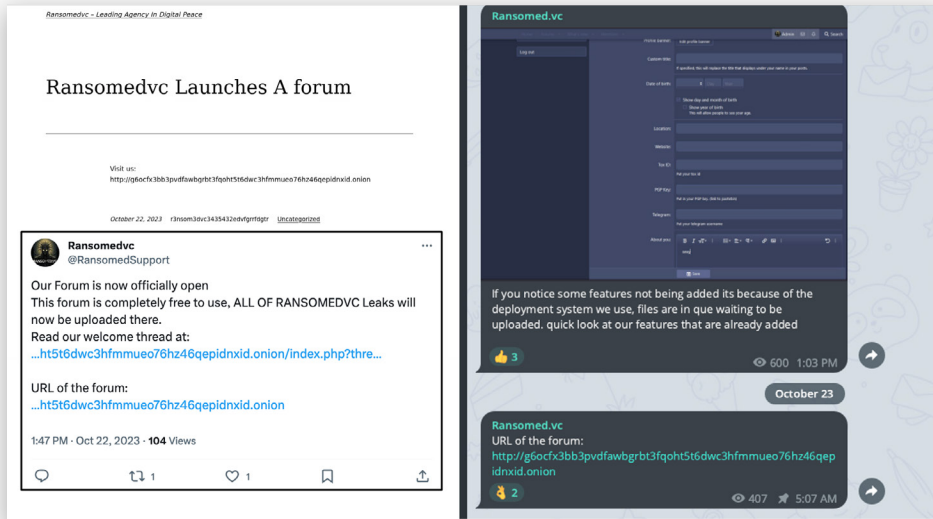


Figure 32: Posts from RansomedSupport about their new forum.

RansomedSupport posted the first message to the forum explaining the features and services provided on the forum and a Q&A detailing the forum structure, the logging policy, and paid ranks, which its members could purchase to elevate their status.

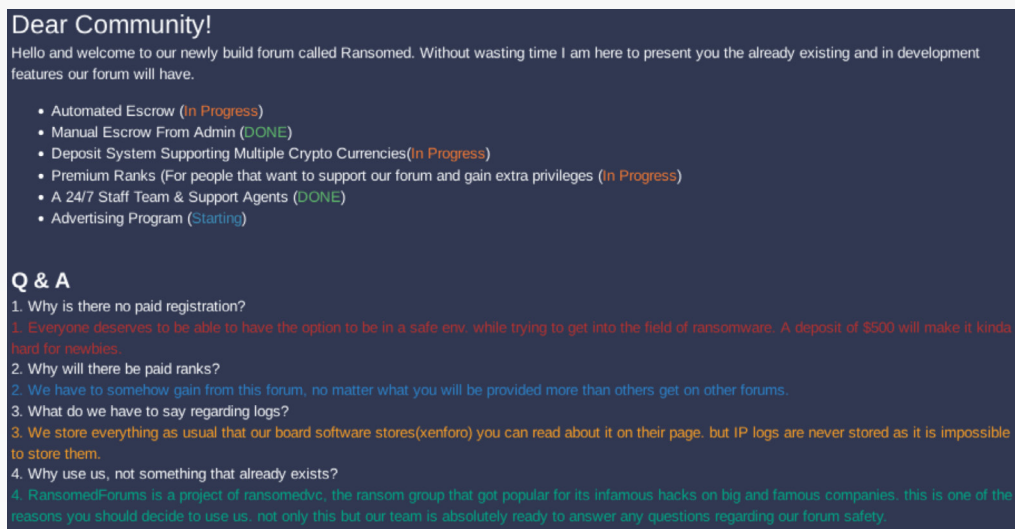


Figure 33: Ransomed forums welcome message from RansomedSupport.

If you recall from earlier, the data leak site Ransomed[.]vc was a forum, named “Ransomed” for the first three days it was online. The new forum shared the same name, and while it was visually different from the earlier forum, many of the subforums carried over, including ransomware. The new forum however was only available on the dark web. The forum appeared to be well received initially, and criminals quickly leveraged the site to sell malware, ransomware, and stolen data. Below is a post of a Ransomed forum member selling what they claim is a newly developed ransomware variant.

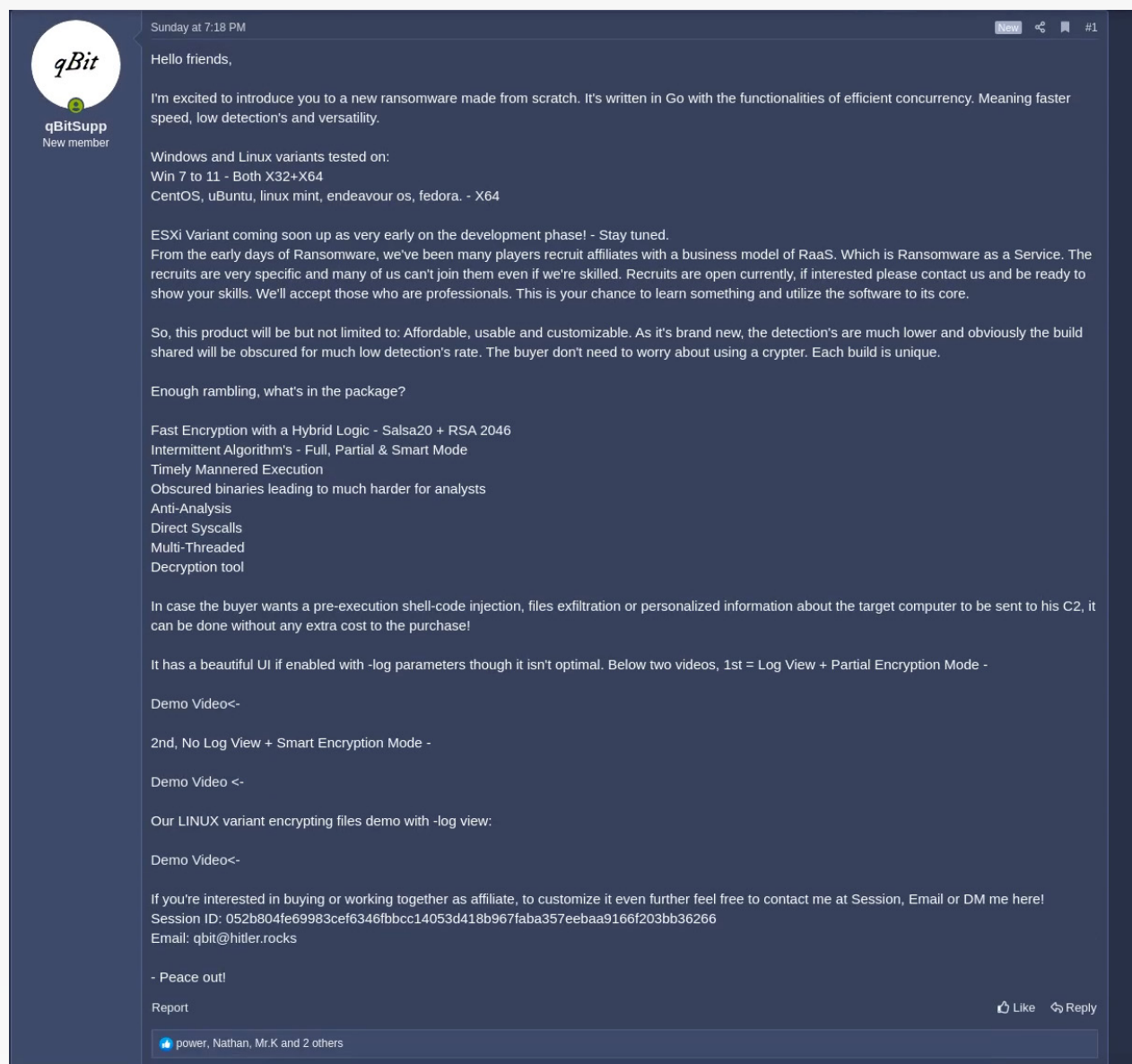


Figure 34: Ransomed forum member selling newly developed ransomware variant.

In addition to the leak site, RansomedSupport and his affiliates also used the forum to sell data they allegedly stole. You can see various accounts below selling or leaking data from companies previously listed on Ransomed[.]vc:











Databases				Filters ▾
	Colonial Pipeline Database Admin · Yesterday at 9:11 PM	Replies: 1 Views: 57	Today at 2:57 PM dyn1s7rA	
	webpag.com.br and novoingresso.com.br Database Leaked Admin · Yesterday at 9:18 PM	Replies: 2 Views: 43	Today at 2:56 PM dyn1s7rA	
	Sony Leak megalodon · Yesterday at 11:14 PM	Replies: 1 Views: 70	Yesterday at 12:03 AM hurricane	
	Zacks.com Database Leak megalodon · Yesterday at 11:21 PM	Replies: 0 Views: 25	Yesterday at 11:21 PM megalodon	
	Hhs.gov Usa Doctors 6.5M xekasama · Yesterday at 9:14 PM	Replies: 0 Views: 33	Yesterday at 9:14 PM xekasama	

Figure 35: Stolen data listed for sale on Ransomed Forum.

The notable data for sale is the Hawaiian Health Care breach, which we discussed did not include Hawaiian Health Care data but was instead publicly available data from <https://healthybydefault.hawaii.gov>. According to RansomedSupport himself, the Colonial Pipeline data is also previously available data leaked from the 2021 breach by DarkSide. Earlier we saw RansomedSupport try and trick both Colonial Pipeline and Hawaiian Health Care into buying the fictitious data and when the attempt failed, RansomedSupport decided to scam the criminals who support his forum.

Despite this, the forum was off to a good start and had a flood of new members. Several well-known hackers from the criminal community joined the forum and participated in conversations, which certainly helped increase its popularity. However, as you know by now, the man behind the RansomedSupport mask never keeps his shiny new toys for long. Based on his history of building up new forums and operations, it was only a matter of time before he would get bored and move on to something else. I just did not think it would happen so quickly.

See You Later Alligator

Despite the initial interest and criminal popularity of RansomedVC and Ransomed forums, RansomedSupport put RansomedVC up for sale on **October 30, 2023**. Below is a message RansomedSupport posted announcing its sale. He posted a similar message to Ransomed[.]vc and the forum.

Based on the post, RansomedSupport was selling the clearnet and dark web infrastructure used to support the operation. He was also selling a ransomware builder, the RansomedVC social media accounts, the affiliate program, access to victimized companies and databases, and the admin panel used to host the ransomware builder. Now, if you

have followed along closely, many things in this post should stand out. If you recall, no victims have reported an incident in which RansomedVC used actual ransomware to encrypt victim systems. Further, remember RansomedSupport told me earlier that law enforcement had gained access to the builder's source code and could decrypt encrypted data without an attacker-provided decryption key. If he was telling the truth, he certainly did not mind selling it to unsuspecting criminals who would find this out the hard way.



Figure 36: RansomedVC for sale, post seen on Telegram.

Additionally, Ransomed support told me that he fabricated “100,000,000 lines of da-ta” in an attempt to deceive and extort NTT Docomom, a Japanese communications company. So, regardless of whether you are a legitimate company being victimized by RansomedVC, or another criminal trying to buy stolen data, you can't trust RansomedSupport.

It seems Bratva, a well-known entity within the cybercrime and ransomware community, caught on to the lies and realized the operation RansomedSupport was trying to sell was bogus. In a post to the Ransomed forum, Bratva mocks RansomedVC and the sale of its operation.

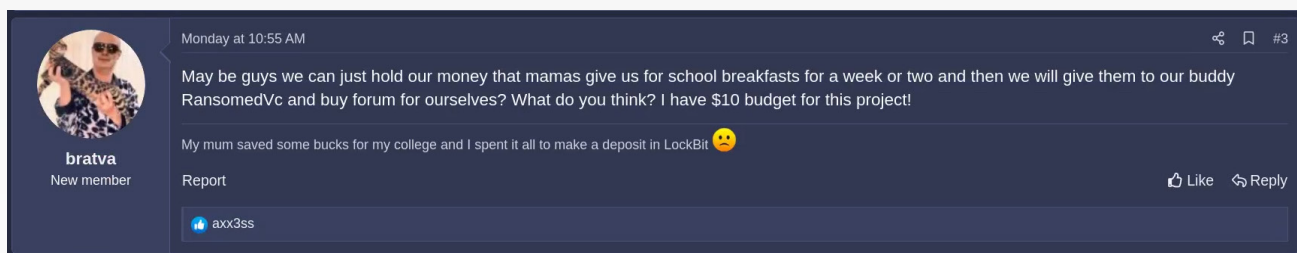


Figure 37: Bratva mocking RansomedVC and the sale of its operation.

When it was all said and done, like ExposedForum, no one bought RansomedVC and the website and forum closed. In November, RansomedSupport posted a final goodbye with the following explanation detailing why they were moving on.

“Within my investigation i have found that 6 people affiliated with me (may) have been arrested, in this way i am putting an end to this. the profit we made isnt worth the ruining of the lifes of any of our affiliates, all of our 98 affiliates are now officially fired, we are sorry for the not so long operation of the group but it happened to be that some of the kids cant have a normal opsec, i cannot do anything about it, i earned good with them but using newly born kiddies at the age of ~20 is just not right in my eyes, they will end up in prison anyways but i do not wish to continue all of this that will support their stupidity, we do not regret any of our breaches nor ransoming any of our “customers” and “clients”. We have done more than anyone else within such a small period of time but this is because we used to hire anyone at any age without any particular skills within his opsec, its mostly their fault but i do not want them to use my project(s) as a podium to get caught. Have fun little haxxors, Cheers!” RansomedSupport

Up to this point, I was unable to find supporting evidence to indicate a law enforcement arrest took place. It does not mean it did not happen, but with so many stories and lies told, I need hard evidence to believe anything he says. Yet, I did have a clue that might shed some light on why RansomedSupport wanted to close the program.

What Really Happened

At the end of November, Ransomed support shared an email message on Telegram that he received from Apple.

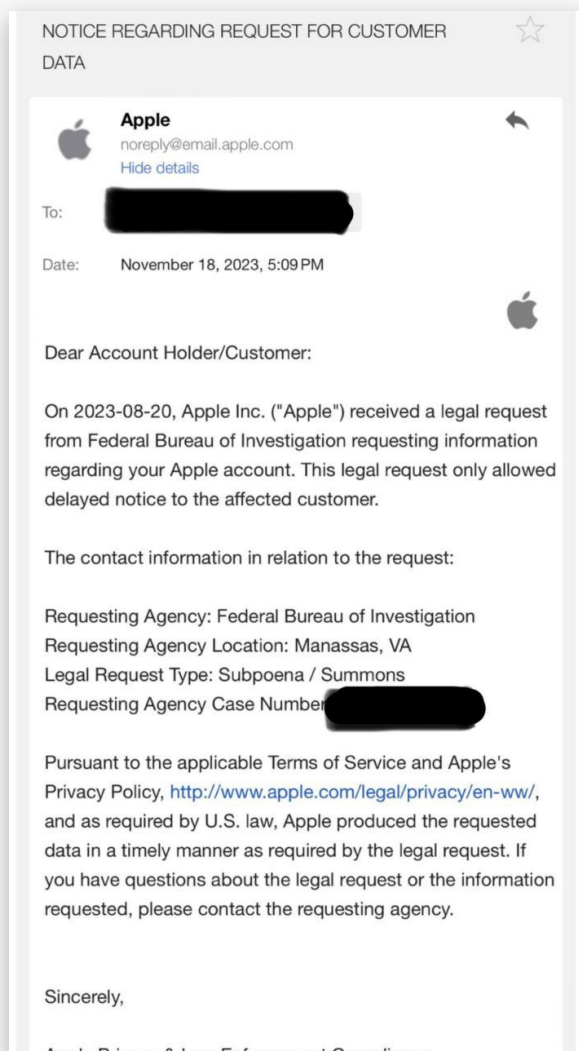


Figure 38: Apple email to an account associated with the person behind the RansomedSupport account.

The FBI is getting closer to finding out who RansomedSupport is. The message shows that the FBI issued a subpoena to obtain the data and information associated with an Apple account used by the real-world person behind it. While RansomedSupport closed RansomedVC in November, before receiving this email, I think he likely knew the FBI was getting closer to finding him. He stated as much earlier on the Ransomed forum claiming the US government was watching him which led to his decision to close the forum. Then a few weeks later he received the subpoena notification from Apple. I don't know how close the FBI is to finding him, but RansomedSupport is still free and conducting crimes and has not been arrested or charged at the time of this writing.

Resources and Leak Site Analysis

Since no victim has publicly reported a RansomedVC attack involving traditional ransomware data encryption, but the group claims it took place, I wanted to see what I could find. I searched malware repositories and could not find a payload that included a ransom note referencing RansomedVC or their known infrastructure or accounts.

I did speak with [someone](#) who claimed to be associated with a malware developer named “Kanna” whom RansomedSupport hired to create a payload for use in attacks. He said RansomedSupport never paid Kanna as promised, and they stopped working and exited the program. RansomedSupport denied this and claimed he had a payload from another ransomware gang they intended to use but had concerns that law enforcement may have access to the source code and decided not to use it. RansomedSupport also says he has no idea who Kanna is. Since there is no technical evidence to support the claims, I don’t know what is true, but the unpaid malware developer’s story certainly matched similar accounts I was told by RansomedVC affiliates. Regardless, my conclusion is RansomedVC has not used a ransom payload in its attacks.

The primary website RansomedVC used, Ransomed[.]vc, also has some unique features not usually seen with ransomware data leak sites. For example, the site includes a **Social Security Number (SSN)** lookup feature. Clicking the link takes you to a Telegram bot, which can search through stolen and publicly available data for a person’s SSN. I don’t know if RansomedVC owned or created the bot or how they benefitted from its use. You can see the SSN lookup feature present on the data leak site below.

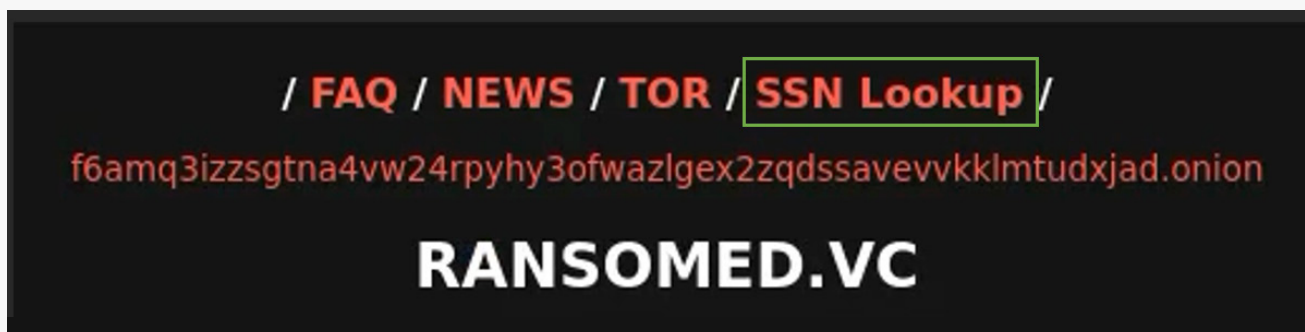


Figure 39: SSN lookup feature on RansomedVC.

RansomedVC also offers a **DDoS service** executed with its own “*stresser*” tool called “**RansomedStresser**”. For a fee, criminals can pay to have RansomedVC target a website of their choice and decide how long the attack should continue. You can see the service offering below.

RANSOMEDVC

Ransomedvc is expanding its infrastructure currently, this is the reason why we are on way on opening more and more projects **RansomedStresser** is one of them, we are here to provide the service many failed to provide in the last few year.

How To Buy?

Message our **admin** they will forward your request to our network specialists.

What can we offer you?

Our team of network specialists can offer you one of the best and most stable **ddos-for-hire services** currently on the market. Our power is not shared, and when we say we will complete the job, we complete it. Our power is completely raw and never based on someones api like this we have 98% power available most of the time, our network is close up to one of the biggest botnets ever made. Our layer 7 power is mostly based on big servers and millions of proxies worldwide. We offer free test attacks with duration up to 50 minutes for serious buyers.

Figure 40: RansomedVC DDoS service offering.

RansomedVC also used a lot of infrastructure for its operation. In addition to Ransomed[.]vc and the Ransomed forum, it also used multiple onion sites, accessible on the dark web which mirrored Ransomed[.]vc. The onion sites were not used concurrently but instead, one was used in the early operation while the others replaced it later. The table below shows the URLs and description of the infrastructure used to support the RansomedVC throughout its operation.

Description	URL
Former RansomedVC and currently Raznovic dark web DLS	http://f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvklmtudxjad[.]onion
Original Dark Web mirror/DLS	http://vq5vmkcfnslr2c2syhe5sw46bzsfrjdy42zlxxluf2fgzn56sfljid[.]onion
Ransom Forum	http://g6ocfx3bb3pvdawbgrbt3fqoht5t6dwc3hfmmueo76hz46qepidnqid[.]onion
Dark Web mirror/DLS	http://k63fo4qmdnl4cbt54sso3g6s5ycw7gf7i6nvxl3wcf3u6la2mlawt5qd[.]onion
Cleartnet DLS	Ransomed[.]vc

Engagement Analysis

I wanted to share details about the engagements I had with actors involved with RansomedVC. After many years of doing traditional CTI and intelligence analysis, I have learned to enjoy talking to people, especially criminals, and getting a feel for who they are and why they do the things they do. It's not always pretty, but it's real and provides a view into the people behind the crimes I read about every day. To begin, I want to share details I learned from the criminals who worked in the RansomedVC operation. I started my research with the idea of finding out what it is like to work in RansomedVC, which I will share next. However, the more I talked to criminals involved with the operation, the more I learned. Eventually I had found so much information that I decided to write a full report about RansomedVC. The biggest surprise, however, is yet to come.

What It's Like to Work with RansomedSupport

Let's start with what it's like for criminals to work at RansomedVC or any of their associated operations. I directly spoke with several former members of RansomedVC. Some I named, within this report while others I left anonymous based on their wishes. Ultimately, we don't know who they are, and obtaining their experiences, which I used to gain intelligence and fill in information gaps, was more valuable than documenting their aliases in my research. However, their stories all ended the same. They were criminals who were conned, lied to, and taken advantage of by another criminal, RansomedSupport. This is not new information within the criminal world. RansomedSupport simply does not play well with others. I have mentioned USDoD throughout this report. He is also a criminal, but he is well-liked in the criminal hacking world in comparison to RansomedSupport. To tell his account of RansomedSupport, I will share parts of the conversation about his feelings and experience.

Jon:

I have been talking to RansomedSupport. He says you still work for him?

USDoD:

Lying. I dont work for anyone.

USDoD:

Not even talked with him since I quit the group.

USDoD:

I blocked him on tg.

USDoD:

I am not related to any of his activities.

Jon:

Shocking... he lied, lol. Do you like RansomedSupport, or what are your feelings about him personally after working with him and interacting with him?

USDoD:

I dislike him a lot, using my data and my work to grow his reputation.

Jon:

Honestly, I agree. You are liked within the blackhat/hacking community, and I do believe you working with them and the breaches you supported brought credit to them. Because you have a better name in the hacking world than they do.

Jon:

How do you know RansomedSupport is Impotent? did he tell you?

Jon:

That sounded funny, lol.

USDoD:

Yes, I discovered impotent and ransomed support online at the same time.

USDoD:

So I asked him.

Jon:

As of now, you worked there but only got paid if they got paid? He did not pay you much for what you did with Transunion. Were there other authentic attacks?

USDoD:

Yes, there is a few others not as much relevant as Transunion

Jon:

Can you share if there were any victims that you know the attack was real?

USDoD:

Yes, Opptimity the uk company is one of real one.

USDoD:

Optimus

Jon:

what about State Farm?

USDoD:

It was real but there is no PII information

Jon:

Yeah, so there is a class action lawsuit against them. They are paying millions in lawyers to defend themselves in court for not notifying victims. But I already figured out there was no customer PII. So even though its not real they are paying all this money because Ransomed lied and the media reported it making it real even though it was not. That is fucking crazy.

USDoD:

Crazy indeed

Jon:

What data was obtained?

USDoD:

I still have the backup here.

Jon:

Can we talk about Sony? That is another strange one. Ransomed did not try to extort them and tried to sell it instead. He did that because he knew someone else had it, too. He told me he got the data from Intel Broker but won't tell me how MajorNelson got it or if he stole it from them. But I compared the data from Nelson, and the data RansomedSupport has. It is the same data from the exact same Sony system. Do you have any info to clear that up? Do you know anything about MajorNelson?

USDoD:

No, I don't and I'm not related to MajorNelson or Ransomed

Jon:

Understood.

Take Away: RansomedSupport screws everybody. I have always known you can't trust a criminal, but I struggled to find many examples where RansomedSupport told the truth or kept his word with victims or criminals he worked with. We saw examples of this earlier when RansomedSupport lied about elements of his attacks, seen in the Sony, State Farm, and the Hawaiian Health Care incidents. It honestly surprised me how RansomedSupport lied and cheated the people who helped him make money.

I also talked to RansomedSupport about his program, how he shares profit with affiliates, and the layout of his program. Once again, RansomedSupport surprised me with his response.

Jon:

Do you pay a salary or percentage of ransom to your affiliates?

RansomedSupport:

Salary, its a lot cheaper. When I did the math it's just 30% of the ransom.

RansomedSupport:

But paying 98 salaries may be harsh if no luck.

RansomedSupport:

In some teams the salaries are 5k a month, but the minimum is 2.5k

RansomedSupport:

3k for a 15/16 year old is ok probably. They (can) buy weed. So, I can get sued for child labor

HAHAHAHAHAH

RansomedSupport:

People should remember

RansomedSupport:

They cant be next to me.

RansomedSupport:

They can be under me.

RansomedSupport:

Or at the bottom.

RansomedSupport:

I usually forget who is who. I number them like dogs

RansomedSupport:

Affiliate 1 to affiliate 124

RansomedSupport:

bcs removed ones

RansomedSupport:

They know they are dogs for me

Take Away: Keep your kids off the internet! Initially, I did not believe that Ransomed-Support only paid small salaries since so many other criminal ransomware operations pay far more. Yet, based on what I have seen from the people who follow and interact with him online, many of them do appear to be younger. If that is true, he likely does pay his employees in this manner. Based on how he talks about them, calling them dogs and how they are under him or at the bottom, shows how RansomedSupport feels about the hackers he pays and how he treats people.

A Well-Kept Secret

Later, I followed up with USDoD to discuss his experience further, and I was not expecting what I was about to learn.

Jon:

OK anything I missed or that I should know about RansomedVC or Impotent?

USDoD:

You should know that impotent/ransomed is not trustable.

He wont stop until they get money.

No one should work with him plus he will turn everyone to the feds.

At least 3 member got arrested

The reason I left ransomed is their lack of transparency, and plus I was warned multiples time that they will scam or report to feds.

Jon:

Wait, he reports to the Feds? Do you know if the arrests he claims are real? I thought he made that up, but it sounds like you are saying it was real. How do you know it's not a lie, too?

USDoD:

A few people who got arrested worked in other instance or have other groups and they got removed to. They shared in some tg groups.

Jon:

Do you have anything from Telegram or other places you can point me to that would help validate that claim as it would go further to show some evidence to connect the dots.

USDoD:

[https://finance.yahoo.com/news/international-police-down-capcom-hackers-160000136.html? guccounter=1](https://finance.yahoo.com/news/international-police-down-capcom-hackers-160000136.html?guccounter=1)

So, I looked at the article, and this is what I saw:

International Police Take Down Capcom Hackers



Someone is holding a phone with the Capcom label against a purple background emblazoned on the screen.

A hacker gang that breached various high-profile companies like computer component manufacturer ADATA and video game publisher Capcom within the last several years has been arrested by an international police force, according to law enforcement agency Europol.

"Prevention and security are improving, however ransomware operators continue to innovate and find new victims," Edvardas Šileris, head of Europol's European cybercrime center, said in the report. "Europol will play its role in supporting EU Member States as they target these groups, and each case is helping us improve our modes of investigation and our understanding of these groups. I hope this round of arrests sends a strong message to ransomware operators who think they can continue their attacks without consequence."

According to Europol's findings, Ragnar Locker isn't just the name of the now-defunct group. It's also the name of the ransomware the gang developed for its cyberattacks, including more recent ones against the Portuguese national carrier and an Israeli hospital. It used this malware to attack devices running Microsoft Windows, exploiting services like Remote Desktop Protocol to gain access to devices and data. So, while speculative, breaking into Windows PCs may have been how Ragnar Locker slipped through Capcom's defense systems.

Kotaku reached out to Capcom and Europol for comment.

Figure 41: Article referenced by USDoD in relation to RansomedVC.

Jon:

Did RansomedSupport ever tell you he worked with Ragnar Locker?

USDoD:

No comment

Ragnar Locker?

Earlier in my research, I asked RansomedSupport about his involvement with other ransomware groups, but he did not want to tell me which group he worked with but admitted that he did. This may have been one occasion he was telling the truth!

Jon:

When and why did you start Ransomed VC?

RansomedSupport:

15 august

I Needed it as a proxy project for a ransomware gang that failed to have good reputation and I needed some more finances.

Jon:

Can you share the previous gang that you were part of?

RansomedSupport:

No

Interpol took down the **Ragnar Locker** organization on **October 23, 2023** and identified six men they believed participated in the criminal operation. Law enforcement [arrested](#) the developer who created Ragnar Locker ransomware and detained five other suspected gang members.

This was significant. Law enforcement suspected and detained six alleged Ragnar Locker gang members, and if you recall, seven days later, on October 30, 2023, RansomedSupport posted *“I have found that 6 people affiliated with me may have been arrested”*. I had missed this! I assumed RansomedSupport meant law enforcement may have arrested six people associated with RansomedVC. As an analyst, I should never have assumed.

It is not surprising if RansomedSupport partnered with Ragnar, but it is new information. If true, it provides context to explain why he wanted to start RansomedVC. In 2021, Ragnar Locker was one of the top ransomware gangs and had a good reputation within the ransomware criminal community. The group [worked closely with Maze](#) at the time and seemed to be growing. Then for whatever reason Ragnar Locker’s number of attacks reduced over time. In 2023 the group only had 21 alleged victims posted to their leak site for the entire year. You can see the decline in claimed attacks in Figure 42 below.

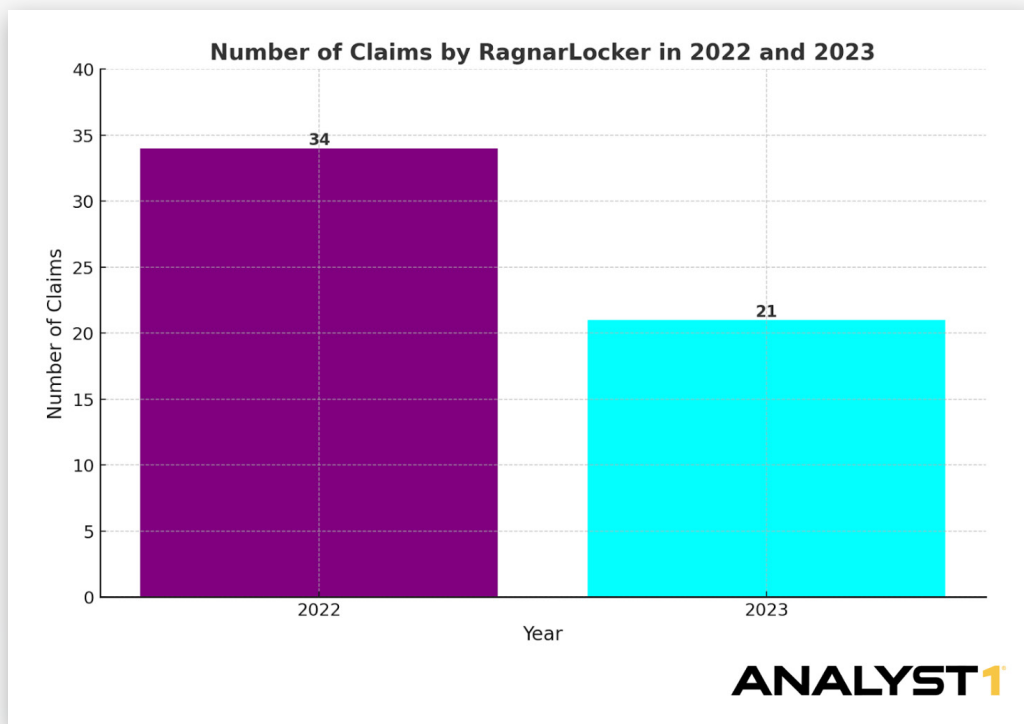


Figure 42: Ragnar Locker stats for 2022 - 2023.

Based on the following information, I assess that it is probable that RansomedSupport did conspire with Ragnar Locker:

Supporting information:

- A RansomedVC Insider (USDoD) claims RansomedSupport previously worked with Ragnar Locker.
- Previously RansomedSupport told me he started RansomedSupport because he **“Needed it as a proxy project for a ransomware gang that failed to have good reputation”**. Ragnar was certainly that.
- Six men were detained by Interpol associated with Ragnar Locker and RansomedVC claimed Six men affiliated with him may have been arrested.
- RansomedSupport started Ransomed forum on October 22, 2023, indicating he had no plans to terminate the operation, and based on opening the forum, he was actually expanding the operation. The very next day Europol takes down Ragnar Locker and seven days later RansomedSupport announces the operation is for sale and closes RansomedVC shortly after.

When I asked RansomedSupport if he used a ransomware payload to encrypt data or just stole data for extortion, he told me he stopped using the payload out of fear law enforcement obtained the decryption key, which would allow victims to decrypt their data without paying a ransom. He told me that after the Ragnar Locker takedown took place. If he was referring to that, it also fits this story.

■ **Note:** You can read my analysis of Ragnar Locker in 2021, [here](#).

If RansomedSupport did work with Ragnar, he may have been concerned the detained men would provide Europol with information that could jeopardize RansomedVC and himself, leading him to close the operation and rebrand a month later under the guise of a new threat actor name. However, a few things contradict this, which I can't explain. If he was concerned about law enforcement, I can't explain why he would reuse RansomedVC infrastructure under the new Raznatovic rebrand. Perhaps his concerns lessened as time passed. Between the allegation made by someone close to RansomedSupport and all the circumstantial evidence listed above, the claim fits this scenario well.

Now, let's address the claims RansomedSupport tipped off Europol. I want to be careful before accusing a criminal of ratting out other criminals because it's an easy actuation to make. I talk to criminals often and I am good at reading people. USDoD believes what he has said to me is true, whether it is or is not I don't think he is lying. As much as RansomedSupport lies, it's also possible he told USDoD a story to boast that included some truth and some lies. Yet, there are several comments RansomedSupport made to me in our engagements that now, stood out.

For example, RansomedSupport once told me “I have a lot of contact with feds”, which I thought was sarcasm, and it may be, but with the above allegations, he should not make jokes any longer. He also told me he reports ransomware affiliates that attack hospitals to the FBI, which is also likely a lie fabricated to lead me to depict him as compassionate in my research. The thing about that is I assess people based on their actions, not their words and RansomedSupport allegedly attacked a medical center in Russia, which is equivalent to a hospital in the US. More importantly, in a conversation I had in November 2023 with RansomedSupport about what he planned to do in his newest Raznatovic operation, this is what he told me:

RansomedSupport:

I just wait up until I get to fuck the people who betrayed me.

RansomedSupport:

They forgot they used to use my infra, and I like to keep logs, evidence :)

RansomedSupport:

The rats die first.

RansomedSupport:

In that count one USDoD

one intel broker

sheriff is also a autistic creature but he couldnt do much

we'll see for who I have resources ;d

There are two ways to read this. He is either saying he is not above providing law enforcement information on other criminals whom he feels betrayed him or he is threatening to kill them. I will let you make up your mind on this one.

Based on the statements made in November and the recent claim made by USDoD, I followed up with RansomedSupport a second time in January 2024, asking additional questions about the allegation that he provided information about criminals to the cops.

Jon:

Is the allegation true that you turn people into the feds?

RansomedSupport:

WTF

HAHAHAHAHAHA

idk why they say that

Jon:

Is there anything else you want to say about it?

RansomedSupport:

Just that I deny the claims

fuck them idk I am speechless

(I'm) getting on a new project anyways

Would RansomedSupport rat out other criminals out of spite? RansomedSupport rarely backs down from a fight with other threat actors as demonstrated in the Forum Wars I detailed earlier in this report. While it would be a sin, even amongst criminals, to tip off law enforcement, anything is possible with RansomedSupport. Without additional evidence, I will not speculate what I think happened, but now you have information and can make your own decision.

The Man Behind the Mask

Next, I will discuss what I learned about the person behind the many masks that RansomedSupport wears. This section is not about a dox, as mentioned, that is not what I do but instead, I will shed light on the characteristics, behaviors, and personality of the person I talked to the past few months. To begin, I want to provide my overall assessment of the criminal I have gotten to know.

Assessment: RansomedSupport is unhappy, unfulfilled, and is chasing money and fame which he thinks will make him happy, but never does. His constant need to reinvent himself limits him from reaching the criminal success he deeply desires. That is why he destroys things as quickly as he builds them, as seen with both Exposed and RansomedVC operations. He is a master at self-branding, marketing, deception, and misinformation. Unfortunately, between life circumstances, his poor mental health state, and questionable ethics, he is unlikely stop committing crimes until he is caught.

The Devil in the Details

I spent a lot of time communicating directly with criminals while conducting research for this report. RansomedSupport was certainly an interesting character. With such a wild and dramatic public persona, it was interesting to get to know the actual person behind it. Of course, RansomedSupport only told me things he wanted me to know or believe, but I was able to use the information, even when it was false, to further my research, which often led me to learn the truth about events detailed in this paper.

RansomedSupport enjoys being a criminal and loves the spotlight. He is drawn to conflict, as demonstrated in the Forum Wars and has a track record of alienating those around him. While I do not claim to know him well, after many hours of conversations, I now have a much clearer understanding of who he is as a human being.

RansomedSupport is a criminal “*bad guy*” but I saw a side of him not many others have — the human side. I was direct and truthful with my intentions to write this report and never tricked him or tried to use a fake persona to obtain information. At times, his answers were so astonishing that I had to ask him if he was sure that was the response he wanted to provide. I asked this because his response to some of my questions would significantly damage his already tarnished reputation and make him look like a monster. If that was how I would portray him, I wanted to ensure I was not leading him to these answers. On every occasion, he persisted. **I believe RansomedSupport is on a course for self-destruction.**

He was never hostile or adversarial towards me, though he will likely not like what I wrote about him. However, he has read the Ransomware Diaries and had to know this would be similar to my previous research. Still, he was friendly and professional and almost always answered my questions, and I had many of them. Despite some of the outrageous things he would say, including the lies he told me, RansomedSupport was a likable person in comparison to many criminals I have engaged with in the past. In an attempt to better understand who he is, our conversations often extended beyond ransomware. He shared personal details of his day-to-day life, which I will never discuss because I think some things should remain private, even if you are a criminal, and they provide no benefit to the purpose of my research.

I found RansomedSupport has a dark sense of humor and the ability to laugh at himself. He even admitted to some of the mistakes he has made in life. He has good days and bad, just like the rest of us, except his good days often involve committing crimes against others. He also has struggles and admitted that he was told he has psychopathy, which is apparent in his actions. Though I knew he would likely laugh at the idea, I suggested he talk to someone or seek help to stop the endless cycle of crazy that has overtaken his life. **Unfortunately, he considers it weak to seek help, and being a criminal is all he knows.**

The End Is Near: Of the Paper, Not the World

RansomedVC has made an art of lying, scheming, conning, and stealing from both victims and other criminals. When RansomedVC claims to breach and steal data from a company, you have no idea if they did what they claim. The group may lie about breaches but sometimes it does have victim data. It really does not matter if RansomedVC purchases the data, pays someone else to steal it, or steals the data themselves. The point is sometimes they do have the data they claim. The problem is that there have been many examples where they don't. The result leads us to not believe their claims, and sometimes, we dismiss them when we should not, and the victim suffers because of it.

On the other hand, the group not only lies about their crimes, but they repurpose previously stolen data and have even gone as far as to fabricate victim data. This makes it hard to determine when we should dismiss them as noise vs. respond to it as a legitimate attack. That confusion is often viewed as a weakness yet based on the amount of money and damage caused to a company's reputation due to RansomedVC's ability to influence the reporting of their attacks, I consider it their strength. It is a mistake to dismiss them without properly assessing the incident. The other problem is RansomedVC attacks are often reported by the media as soon as they are posted to the leak site or claimed on the group's social media channels. This attention makes the attack real, even when it's not, which in turn hurts the victim company and gives validity to the attack making it harder for the victim to properly respond. So don't write about this report!

RansomedVC was able to make State Farms customers believe their data was exposed when, in fact, it was not, resulting in a class action suit. This is a prime example of what RansomedVC is capable of. I am not suggesting the media or researchers, including myself, should not share information about attacks but it should be done to make the public aware that the group's claims are often nothing more than a con. At the same time, since RansomedVC does have the ability to obtain authentic data, we cannot simply dismiss them. So, what do you do? This is why the group is dangerous and why RansomedVC is a bigger problem than it appears at first sight.

RansomedVC is a bigger problem than it appears at first sight

Criminals should not trust RansomedVC either. Based on every account from the hackers I communicated with for this research there is one common theme. The only target RansomedVC abuses more than actual victims, is other criminals. Time after time, I was told stories of how RansomedVC stole money from a criminal or left them unpaid. I hope this research will also serve as a wake-up call for criminals to stop working with the group. Without help, RansomedVC goes from a dangerous threat group to a lone, crazy-ass criminal, RansomedSupport, who will find it much harder to commit crimes on his own without support.

RansomedSupport only knows the criminal life and has been hustling and committing crimes for most of his life. RansomedSupport says he lives in Bulgaria, and while I cannot confirm if that is true, I do not believe he is in Russia, and he won't receive the same level of protection other ransomware groups do from a government that looks the other way as long as you don't target victims within their borders. Based on what I have learned about RansomedSupport if he continues down this path, I don't think this story will end well for him when it's all said and done.

Conducting research for this report has been like riding a roller coaster with many twists and turns. I found myself constantly getting thrown through loops just to find everything was upside down, leaving me sick to my stomach and just hoping the ride was almost over. Thankfully, for me, now, it is.

Special Thanks: I want to thank Dissent from DataBreaches.net who helped review my findings and analysis found throughout this research. More importantly, thank you for helping me not go insane! As I said, this was one hell of a ride.

Appendix

RansomedVC Associated Accounts:

Type	URL	Type
RansomedVC[@]yahoo[.]com – Probable Email associated with RansomedVC seen in RobinHood Data Leak	RansomedVC[@]yahoo[.]com	Yahoo
MosiBosi (RansomedVC XSS account)	https://xss[.]is/members/333090/#recent-content	XSS forum account
BorisTulev – BreacheForum account claiming to be a RansomedVC affiliate	https://breachforums[.]is/User-BorisTulev	XSS aff account
Ransomed Twitter Account	[@]RansomedSupport	Twitter
Ransomed VC original Twitter Account	[@]ransomedVC	Twitter
Tox ID for RansomedVC and MociBosi (XSS)	192D52C7C18F3D2693ED2453E64C53EC0 CCF0255AB2291F019B65BA84442B313C4 10DE132E59	Tox
Ransomed VC TikTok account	[@]ransomedvc	TikTok
RansomedVC Telegram account (userID:6188325351)	[@]ransomedSupport	Telegram account
Early Telegram for RansomedVC	[@]ransomedSec	Telegram account
Early Telegram for RansomedVC	[@]HristeeBoje	Telegram account

Type	URL	Type
[@]HanaKobuta - Original username for ransomedVC telegram account	[@]HanaKobuta	Telegram account
Ransomed Telegram Channel	https://t.me/ransomed_channel	Telegram Channel
Jabber account for Exposed[.]vc account	impotent[@]thesesecure.biz	Jabber
RansomedVC[.]gmail[.]com – probable Email associated with RansomedVC seen in RobinHood Data Leak	RansomedVC[@]Gmail[.]com	Gmail
Ransomed[@]nigge.rs account listed on RansomedVC (temp email account)	Ransomed[@]nigge.rs	Disposable
Account used for communicating with hosting/service provider Danwin2010	Mariamagdalen1337[@]mailfence[.]com	Disposable
RansomedVC BreachForum Account	https://breachforums[.]is/Thread-Ransomed-vc-is-Looking-To-Hire-Buy-Access-RDP-VPN	Breach account
@ransomware_official	Alt telegram account	Telegram
Alternate admin email	ransomed[@]danwin1210[.]de	Backend account

RansomedVC attacks

It is difficult to determine when RansomedVC has authentic data or if the victim named is a victim. I spent time going through the previous leaks on their leak site, forum and Telegram channel. I created a table detailing if data (inclusive or a sampling of data) was leaked or if a website defacement took place:

Title	Date	Data Sold Or Leaked	Data Sample leaked	Site Defacement
A1 Data Provider	8/21/23	X		
InG Brokers	8/25/23	X	X	
Jhookers	8/25/23	X	X	
Optimity	8/25/23	X	X	
TransUnion	8/25/23	X	X	
State Farm	8/26/23			
Metropolitan Club DC	8/27/23	X	X	
PSM	8/29/23	X		
Hawaii Health System	9/3/23	X		X
I&G Brokers	9/3/23	X		
Optimity.co.uk	9/3/23	X		
paynesvilleareainsurance.com	9/3/23			
phms.com.au	9/3/23			
Powersports Marketing	9/3/23			
S&P	9/3/23			
SKF.com	9/3/23	X		
Balmit Bulgaria	9/4/23	X		
easydentalcare.us	9/4/23			X
laasr.eu	9/4/23			
makflix.eu	9/4/23			
medcenter-tambov.ru	9/4/23			
nucleus.live	9/4/23			X
quantinum.com	9/4/23			


Title	Date	Data Sold Or Leaked	Data Sample leaked	Site Defacement
Swipe.bg	9/4/23			
wantager.com	9/5/23			X
Linktera	9/8/23			
airelec.bg	9/9/23			
kasida.bg	9/9/23			
pilini.bg	9/9/23		X	
proxy-sale.com	9/9/23			
gov.ia	9/15/23			
andrews.bg	9/24/23			
ardes.bg	9/24/23			
arelion.com	9/24/23			
bnm.bg	9/24/23			
districtshoes.bg	9/24/23			
ebag.bg	9/24/23			
ecco.bg	9/24/23			
footshop.bg	9/24/23			
mango.bg	9/24/23			
myshoes.bg	9/24/23			
popolo.bg	9/24/23			
Punto.bg	9/24/23			
SONY.COM	9/26/23	X	X	
DC Voter data	10/4/23	X	X	
NTT Docomo	10/6/23			
DallBlog	10/8/23		X	
iLife.bg	10/8/23		X	
Kasida.bg	10/8/23	X		
novoingresso.com.br	10/8/23	X		
Optimity UK	10/8/23			

Title	Date	Data Sold Or Leaked	Data Sample leaked	Site Defacement
pilini.bg	10/8/23	X	X	
rodoviariaonline.com.br	10/8/23		X	
webpag.com.br	10/8/23	X	X	
Colonial Pipeline Company	10/14/23	X	X	

Since RansomedVC uses various sources to leak and sell data there may be additional leaks beyond what I have included in the table above. It is also important to remember that RansomedVC often uses fictitious or previously stolen data to repurpose in new attacks. Concerning RansomedVC, leaking or selling data does not indicate the data is authentic.

ABOUT US:

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

 @UseAnalyst1

 analyst1.com/blog

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

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