On the Horizon: Ransomed.vc Ransomware Group Spotted in the Wild

Published: 2023-08-21 · Archived: 2026-04-05 15:45:13 UTC

[Update] November 9, 2023: "End of an Era, the Sinking of Ransomed.VC"

[Update] October 5, 2023: See the subheading: "RansomedVC De-anonymized Itself After Moving to WordPress."

[Update] October 2, 2023: See the subheadings: "RansomedVC Partners with STORMOUS Hackers," and "The Outcome of the Sony Leak."

[Update] September 15, 2023: See the subheading: "Ransomed.vc Interview."

[Update] September 4, 2023: The Ransomed team is collaborating with Everest Ransomware, read more under: "Old Ties, New Threats: Everest Echoes."

[Update] August 24, 2023: Added subheadings: "Ransomed.vc Lists Three New Victims and Receives Payment for a Previous Attack," "An Extortion Approach That Utilizes GDPR Fines."

We have been monitoring Telegram for a long time as many of the threat actors and dark web activities are also actively running on Telegram. A Telegram group that we previously monitored as **RansomForums** had recently announced that they would be doing a project called **Ransomed.vc**.

The group's owner has renamed his private chat room to Ransomed.vc Chat:

Figure. 1. First Message of Ransomed.vc Chat room

Figure 2. Welcome post of Ransomed.vc (Source: FalconFeedsio)

However, the site suffered a DDoS attack shortly after its launch and was dubbed BreachForums2 by the attackers:

Figure 3. Ransomed.vc's screenshot after being attacked (Source: Karol Paciorek)

Another Twitter user also discovered that RansomForums' favicon icon looks the same as BreachForums' favicon.

Figure 4. Favicons of RansomForums and BreachForums (Source: Crocodyli)

According to the group owner's chat messages, the admin will not use the forum for a while until Breachforums is closed and he has the source code of RaidForums:

Figure 5. Telegram group owner's statement

After this process, Ransomed.vc was transformed into a site sharing ransom victims:

Figure 6. Main page of Ransomed.vc

When we search the directories of the page domain, we see that they do not have any other **subpages** other than the ones they have shared at the moment:

Figure 7. Dirbuster output of Ransomed.vc domain

When we check the domain in VirusTotal, it appears clean, but in the relation graph, it is linked to an IP address tagged as malicious:

Figure 8. VirusTotal output and Relation graph of Ransomed.vc domain (Source:VirusTotal)

In addition, the group shares victim posts on its Telegram channel, which they actively use:

Figure 9. Telegram channel information

First Victims of Ransomed.vc

Figure 10. A1 Data Provider has been compromised by Ransomed.vc

Figure 11. A1 Data Provider's screenshots of Ransomed.vc

I&G Broker House:

Figure 12. I&G Broker House

Figure 13. I&G Broker House's screenshots of Ransomed.vc

We also see that they are looking for new operators on their Telegram channels, which suggests that there may be **more victim announcements** in the near future.

Figure 14. Ransomed.vc Telegram posts about they are looking for new operators

Ransomed.vc Lists Three New Victims and Receives Payment for a Previous Attack

Based on the latest information, the Ransomed.vc group has targeted three new victims. One of these victims is **Optimity**, a provider of managed IT services. The threat actors assert that they have exported Optimity's entire **Azure Cloud**, which granted them access to over a thousand companies.

Figure 15. Optimity

Another exported database belongs to **Transunion**. The ransom threat actors claimed that they successfully infiltrated the entire cloud, gaining possession of all materials used and downloaded by Transunion employees. One such dataset has also been obtained for a company named **Jhooker.**

Figure 16. Transunion

Figure 17. Jhooker

Furthermore, the ransomware operation has apparently received a payment following their attack on A1 Data Provider. However, only one out of four payments has been fulfilled. It appears that the ransom group accepts **payments in installments**, a departure from the norm among ransomware groups we have encountered so far.

Figure 18. ¼ partial payments have been paid by A1 Data Provider.

An Extortion Approach That Utilizes GDPR Fines

An additional revelation about the group has been shared in a tweet by vx-underground. The Ransomed.vc group seems to use an extortion strategy that leverages **GDPR** (Europe's General Data Protection Laws). Essentially, the group coerces victims into either paying the ransom or facing GDPR fines upon the exposure of their data. This GDPR-based extortion scheme diverges from the typical extortion approaches, as these threat actors **exploit protective laws** to intimidate victims for financial gain.

Old Ties, New Threats: Everest Echoes

In a recent post by the Ransomed team, we noticed that they are collaborating with Everest Ransomware, as evident in the details of **SKF.com**'s victim announcement. Upon reviewing Everest's claim post, we observed Everest also made the same post. Everest is a threat actor that has been active since 2020. Everest has been involved in ransomware attacks, initial access brokering, and data extortion activities. Additionally, they have been active on platforms such as XSS Forum and Breached.

Fig. 19. Everest and Ransomed's claim posts about SKF.com

Considering that Ransomed was one of the founders of BlackForums after Breached and Everest was active in Breached, we can infer that their fellowship is not for a single operation but a history.

RansomedVC Partners with STORMOUS Hackers

RansomedVC recently announced on Telegram that they have forged an alliance with Stormous ransomware.

The threat group's most recent message on its channel stated that while they had partnered in the past, they are now officially confirming it:

Fig. 20. RansomedVC's announcement about partnering with Stormous.

The fact that Stormous referred to the RansomedVC group as a partner in its own Telegram channel with one of their recent posts fully confirms their partnership.

Fig. 21. Stormous' message on Telegram.

In the message, the ransomware group also commented on the Sony breach, suggesting that they might intervene and **potentially release more data** for free.

The two ransomware groups appear to be trying to exert pressure on Sony, possibly with the aim of **further extorting** their victim or **damaging their brand reputation**. With the official partnership now established, we may expect to receive more updates regarding the Sony situation.

The Outcome of the Sony Leak

In a subsequent update, the RansomedVC threat actors have leaked the data they claimed to possess from the Sony breach on their Telegram channel. They mentioned that they extracted **only the important data** from Sony. See the message below:

Fig. 22. RansomedVC leaks the data from the Sony breach.

To learn more about the Sony breach, visit our other blog post: What You Need to Know About the Alleged Sony Breach

RansomedVC De-anonymized Itself After Moving to WordPress

RansomedVC has recently transitioned its website to WordPress, following the setup of a new virtual private server (VPS), hosted by a bulletproof hosting provider known as PONYNET.

Unfortunately for the RansomedVC threat actors, this migration has inadvertently exposed their **origin IP address** and a variety of associated **DNS entries**.

Exposed host information. (Source: X)

Additionally, their actions have led to oversights, as the site seems to be affected by vulnerability known as CVE-2017-5487 (Unauthorized Information Disclosure vulnerability in WordPress 4.7 before 4.7.1). The vulnerability further reveals RansomedVC's origin IP. The sensitive information is available within the profile of the administrator user:

Ransomed.vc's origin IP has been revealed. (Source: X)

The intention behind this disclosure by @htmalgae is to highlight how the threat actors hastily **de-anonymized** their hidden service before its full restoration was completed.

Ransomed.vc Interview

Daily Dark Web published an interview with Ransomed.vc on September 14th. The interview shows how a ransomware operator thinks and sheds light on many claims and points about Ransomed[.]vc. Some highlights from the interview are as follows:

Can you introduce your group and explain why you engage in ransomware attacks?

– Of course I can, we are a big team I have to say of 77 affiliates and a few more groups in partnership. We are financially motivated so this answers the second part of the question

- *More on the topic of their working scheme:*

What are the primary motivations behind your attacks? Is it for financial gain, ideological reasons, or something else?

– Financial gain and sometimes political reason.

How do you choose your targets? Are you targeting large corporations, small businesses, or individual users?

– I require at least 5M in revenue so it is even worth to work on.

- *Their answers to some of the claims we included in this article were as follows:*

In a recent post by the Ransomed team, they are collaborating with Everest Ransomware. Could you specify the nature of your connection with the Everest Group?

– Old friends dont forget their friends.

Alleged ties between Exposed Forum and Ransomed: Could you specify the nature of your connection with the Exposed Forum?

– I have seen the news yeah, idk what I can say about it, never been in their forum neither will I ever be.

Don’t forget to check out Daily Dark Web’s post for the full interview.

End of an Era, the Sinking of Ransomed.VC

> *Ransomed.vc’s last post on Telegram about the end of the operation*

Ransomed.vc shared a Telegram post announcing the shutdown of their operations due to the **arrest of six individuals** associated with their group. The announcement acknowledged that the financial gains did not outweigh the harm caused to their affiliates’ lives. It highlighted the mistake of hiring young and inexperienced people, which led to security lapses and likely contributed to their arrests. However, the post contained no apology for the ransomware attacks they were involved in. Concluding the post, Ransomed.vc distanced themselves from the actions of their former associates and the ongoing illegal activities, signing off with a casual farewell.

There are some questions in mind:

- What will happen to the Ransomed forum?
- What will happen to the victims?

We’ll see in the future…

Bonus:

Twitter is buzzing with claims that the Ransomed admins are impotent and self-report their affiliates to the feds. We don’t know if these rumors are true, but we discuss such rumors in another blog series, not here.

Follow Dark Peep if you want to know about rumors and interesting incidents happening on the dark web!

Discovering the Dark Web Landscape: SOCRadar XTI Monitoring and Threat Insights

Utilizing advanced monitoring techniques and AI-driven intelligence, SOCRadar XTI consistently surveils the entire web landscape, including the clear, dark, and deep web, alongside other hacker channels on platforms like Telegram. With its robust monitoring capabilities, SOCRadar provides an invaluable service by **alerting** organizations before compromise.

For a deeper understanding of the hidden facets of the internet and insights into threat actors operating from the depths of the dark web, and their malicious toolsets, **explore our platform.**

> SOCRadar Dark Web Monitoring

Furthermore, you can request **a free dark web report** here to learn the scope of your exposure to such threats and bolster your overall security posture.
