



| Flash |

Ransomed[.]vc Sunsets Operations, Auctions Off Infrastructure

F-2023-11-10b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Deep & Dark Web

November 10, 2023

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 09:00 AM (EST) on November 10, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Ransomed[.]vc Sunsets Operations, Auctions Off Infrastructure

› Key Findings

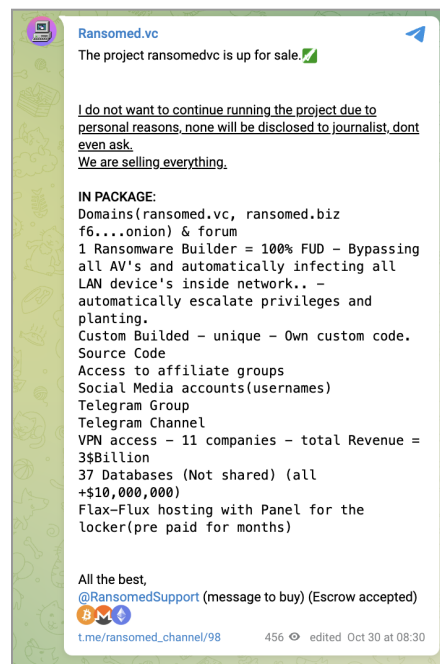
- The ransomware and data extortion (R&DE) collective known as Ransomed[.]vc announced in its Telegram channel that it no longer wanted to continue running the project and was selling all aspects of its infrastructure.
- At the time of writing, one Ransomed[.]vc leak site has been closed down, and the other hosts a closing note on its home page. However, its ransomware forum (on which Ransomed[.]vc coordinates its ransomware-as-a-service projects) remains active, likely to assist in the sale of its infrastructure and assets.
- Since August 2023, ZeroFox has identified more than 40 R&DE victims of Ransomed[.]vc, almost 60 percent of which are organizations based in Europe.¹
- These posts very likely represent a legitimate cessation of Ransomed[.]vc's activity and a fire sale of the operation's infrastructure. Threat actors will likely be motivated to purchase the infrastructure to target victims, create spin-off extortion operations, or leverage for further malicious activity. However, Ransomed[.]vc's closure is very unlikely to have any considerable impact on the broader R&DE threat.

¹ ZeroFox Intelligence Internal Collections

Details

R&DE collective Ransomed[.]vc announced in its Telegram channel on October 30, 2023, that it will discontinue the project and sell off its infrastructure. The collective's closure is unlikely to have any considerable impact on the broader R&DE threat landscape, as affiliates are likely to pivot to other extortion operations at pace and continue their respective targeting with little cessation or downtime. The post states that the sale package includes:

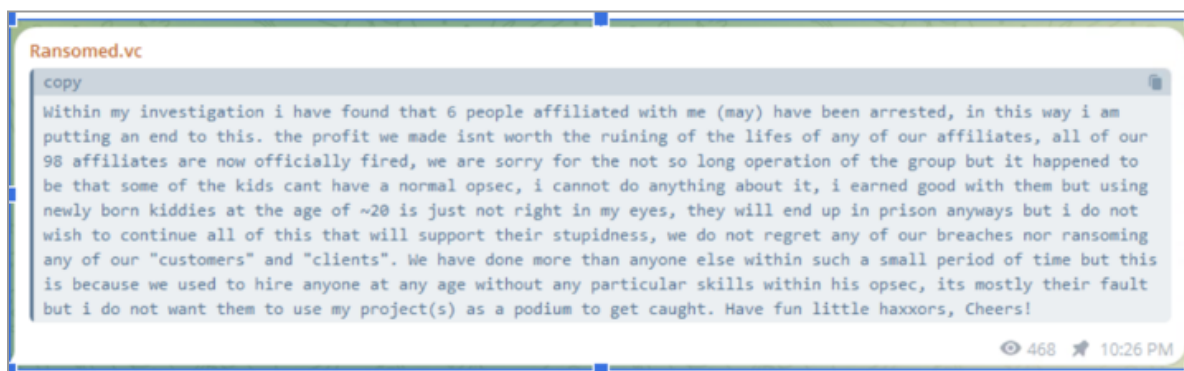
- Domains (Ransomed[.]vc, Ransomed[.]biz, and its dark web forum);
- A ransomware builder claimed to be fully undetectable;
- Source code;
- Access to affiliate groups;
- Social media accounts;
- Telegram channel and group;
- VPN access for 11 companies with revenue totaling USD 3 billion;
- Thirty-seven (37) databases; and
- A control panel for the locker.



Ransomed[.]vc announces closure of operations

Source: [hXXps://t.me/ransomed_channel/98](https://t.me/ransomed_channel/98)

A follow-up post published in the Ransomed[.]vc Telegram channel on November 8, 2023, stated that six individuals associated with the operation may have been arrested, blaming their lack of effective operational security and inexperience. The post also stated that all 98 Ransomed[.]vc affiliates had been fired with immediate effect; ZeroFox has not independently confirmed the veracity of these claims.



Ransomed[.]vc announces possible arrest of operatives and firing of 98 affiliates

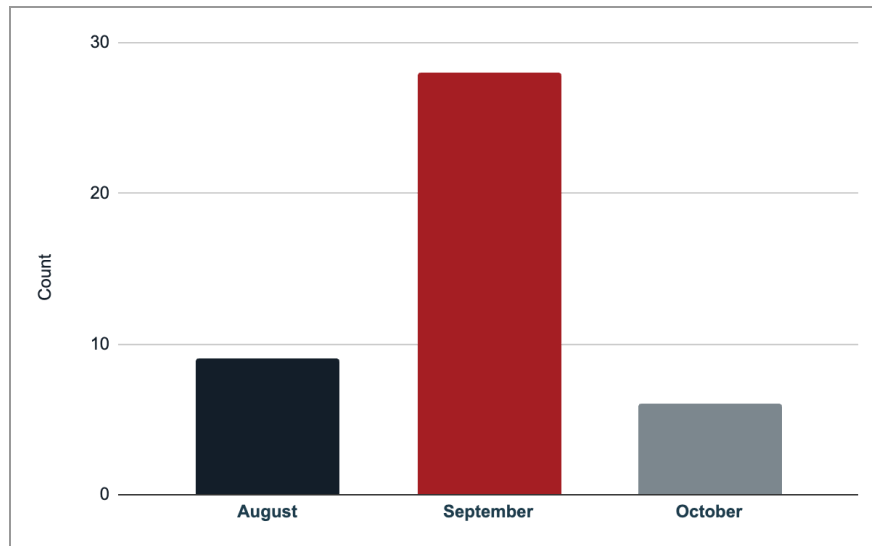
Source: [hXXps://t\[.\]me/ransomed_channel/147](https://t.me/ransomed_channel/147)

At the time of writing, one Ransomed[.]vc leak site has been closed down, and the other hosts a closing note on the home page. However, its ransomware forum (on which Ransomed[.]vc coordinates its ransomware-as-a-service projects) remains active, likely to assist in the sale of its infrastructure and assets.

Identified as early as August 2023, Ransomed[.]vc originated as an underground forum discussing cybercriminal activity, including data brokerage, network access, and exploitation of vulnerabilities. The group specialized primarily in Europe-based targets, and the operation was engaging in extortion activities by the end of August 2023. Since August, at least 40 victims of Ransomed[.]vc extortion were Europe-based, representing 60 percent of the collective's overall activity.

Flash | Ransomed[.]vc Sunsets Operations, Auctions Off Infrastructure

F-2023-11-10b
TLP:CLEAR



Ransomed[.]vc extortion incidents by month

Source: ZeroFox Intelligence

These posts very likely represent a legitimate cessation of Ransomed[.]vc's activity and a fire sale of the operation's infrastructure. Threat actors (not limited to extortion collectives) will likely be motivated to purchase the infrastructure to target victims, create spin-off extortion operations, or leverage for further malicious activity.

- Ransomware collectives are known to obtain and incorporate source code from other ransomware strains into their payloads.
- Threat actors deploying Ransomed[.]vc are very likely to continue their operations by pivoting to other ransomware-as-a-service offerings.

| Recommendations

- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Implement secure password policies with phishing-resistant MFA, complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform detection of R&DE threats and their associated tactics, techniques, and procedures (TTPs) and Indicators of Compromise (IOCs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system and ensure all business IT assets are updated with the latest software as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%