Ransomware Profile: ALPHV

blog.emsisoft.com/en/40931/ransomware-profile-alphv/

February 23, 2022

- Malware Lab
- Ransomware

- Senan Conrad
- February 23, 2022
- 8 min read

ALPHV is a ransomware variant that encrypts data on infected systems and threatens to leak stolen data if the ransom payment is not made. It is highly customizable, which enables threat actors to easily tailor an attack to the target environment. ALPHV was first observed in November 20201 and is believed to be the first active ransomware coded in the Rust programming language.

What is ALPHV?

ALPHV is a strain of ransomware that encrypts files using AES encryption (although the process can be overridden to use ChaCha20) and demands a large ransom for their decryption. It is the only active ransomware developed using Rust, a programming language renowned for its performance and safety. ALPHV has used Rust's cross-platform capabilities to develop both Linux and Windows variants of the ransomware.

ALPHV is categorized as ransomware-as-a-service (RaaS), a business model whereby the developers of the ransomware lease it to affiliates, who earn a portion of ransom payments in exchange for executing a successful attack. ALPHV offers affiliates a larger revenue share than many other RaaS operations, with affiliates earning 80% of payments up to $1.5 million, 85% of payments up to $3 million and 90% of payments over $3 million. The developers of ALPHV typically recruit affiliates on Russian-speaking hacking forums.

To amplify the impact of an attack, ALPHV uses data exfiltration to put further pressure on victims and increase their chances of a payout. During an attack, threat actors extract large amounts of data from the compromised system and threaten to publish it on the ALPHV leak site unless the victim pays the ransom.

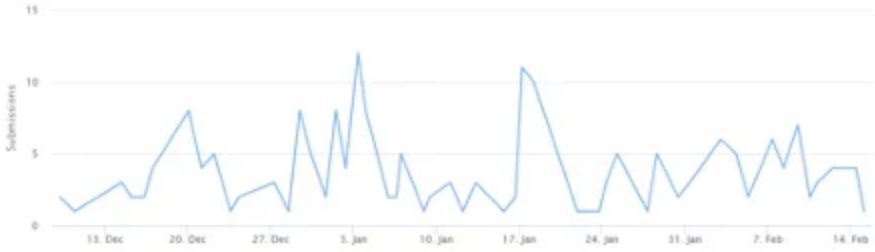
ALPHV is one of a handful of ransomware groups that also threatens to DDoS victims that fail to pay the ransom. ALPHV allegedly uses its own botnet to manually perform the DDoS attacks. The group frames DDoS as an exclusive feature of sorts, available only to affiliates who have generated more than $1.5 million in ransom payments.

The history of ALPHV

ALPHV was first detected in November 2021 and quickly claimed dozens of victims in the first few months of operation.

It is likely that ALPHV is a rebrand of a ransomware group known as BlackMatter, which was itself a rebrand of a group known as Darkside. It's believed that these rebranding efforts may be an attempt by threat actors to distance themselves from a costly development blunder that allowed Emsisoft to create a free Blackmatter decryption tool.

Cybersecurity researchers originally named the ransomware 'BlackCat' after the image of an inky feline that was depicted on every victim's Tor payment site. However, in February 2021, a representative of the group confirmed that its only official name is ALPHV.



Since ALPHV was first discovered, there have been 194 submissions to ID Ransomware, an online tool that helps the victims of ransomware identify which ransomware has encrypted their files. We estimate that only 25 percent of victims make a submission to ID Ransomware, which means there may have been a total of 776 ALPHV incidents since the ransomware's inception. During this time, the group also published on its leak site the stolen data of at least 40 organizations.

ALPHV ransom note

After the ransomware has been deployed and the encryption process is complete, ALPHV drops a ransom note on the infected system. The ransom note is named after the apparently random file extension that ALPHV appends to all encrypted files, and uses the following naming format: 'RECOVER-[RANDOM EXTENSION]-FILES.txt'.

The ransom note informs the target that their files have been encrypted and includes a link to a .onion site where the victim can make payment. The note also includes examples of the type of data that was stolen during the attack, along with threats that the data will be

published if the victim refuses to cooperate.

Below is a sample ALPHV ransom note:

> >> Introduction
>
> Important files on your system was ENCRYPTED and now they have “[REDACTED]” extension.
>
> In order to recover your files you need to follow instructions below.
>
> >> Sensitive Data
>
> Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate.
>
> Data includes:
>
> [REDACTED]
>
> – And more…
>
> Private preview is published here: [REDACTED]
>
> >> CAUTION
>
> DO NOT MODIFY FILES YOURSELF.
>
> DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
>
> YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
>
> YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.
>
> >> Recovery procedure
>
> Follow these simple steps to get in touch and recover your data:
>
> 1) Download and install Tor Browser from: https://torproject.org/
>
> 2) Navigate to: [REDACTED]

Who does ALPHV target?

ALPHV tends to target large organizations with the resources and motivation to pay large ransom demands. It is capable of infecting both Windows and Linux systems.

ALPHV prohibits attacks on nations belonging to the Commonwealth of Independent States (CIS), which includes Azerbaijan, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan and Ukraine.

The group also prohibits attacks on government, healthcare and educational institutions. If an entity belonging to one of these sectors is attacked, ALPHV claims that it will provide free decryption and ban the offending affiliate.

As always, any claims made by cybercrime groups should be taken with a grain of salt. ALPHV has already published stolen data from at least one victim in the healthcare sector (the group has stated that its rules around avoiding the healthcare sector do not apply to pharmaceutical companies and private clinics). Additionally, even if the group does provide free decryption to an impacted entity, the recovery process may still take days, weeks or months to complete. This level of disruption can have a significant impact on patient health.

How does ALPHV spread?

ALPHV attacks begin by breaching the target network. Affiliates can use a variety of methods to infect the target system, including compromised RDP, phishing attacks, stolen credentials and exploiting known vulnerabilities.

Once the system has been compromised, attackers may use a variety of tools to prepare the environment for encryption and maximize the impact of the attack. Tools such as Mimikatz, LaZagne and WebBrowserPassView are used to access saved passwords, which enable threat actors to escalate privileges and spread laterally across the network. MEGAsync is often used to exfiltrate data, while anti-forensics tools like File Shredder are sometimes used to securely delete files and thwart analysis. PowerShell is often used to modify Windows Defender security settings and shadow volume copies are deleted prior to encryption to prevent organisations from restoring encrypted files.

ALPHV requires a specific access token for the ransomware to execute properly. The access token acts as a unique key, which is used to verify the identification of the victim and must be provided when accessing the ALPHV .onion payment site. The access token prevents third-parties (such as ransomware researchers) gatecrashing what is supposed to be a private negotiation between victim and attacker.

As ALPHV operates as a RaaS and can be distributed by many different affiliates, the exact anatomy of an attack can vary from incident to incident.

Major ALPHV attacks

- **Oiltanking:** In late November 2021, German petrol distributor Oiltanking GmbH was the victim of an ALPHV attack. The incident affected 13 fuel terminals, including the automated systems responsible for loading and unloading fuel tanks, and forced the company to resort to manual processes. More than 200 petrol stations, mostly located in northern Germany, were impacted during the attack.
- **Swissport:** In February 2022, Swissport, the world's leading provider of ground services and cargo handling for the aviation industry, was allegedly hit by ALPHV. The group posted on its data leak site a small sample of files that were apparently stolen during the attack, including passports, internal business notes and the personal information of job candidates. The group also offered to sell the entire 1.6 TB set of stolen data.

How to protect the network from ALPHV and other ransomware

The following practices may help organizations reduce the risk of an ALPHV incident.

- **Cybersecurity awareness training**: Because the majority of ransomware spreads through user-initiated actions, organizations should implement training initiatives that focus on teaching end users the fundamentals of cybersecurity. Ransomware and propagation methods are constantly evolving, so training must be an ongoing process to ensure end-users are across current threats.
- **Credential hygiene**: Practicing good credential hygiene can help prevent brute force attacks, mitigate the effects of credential theft and reduce the risk of unauthorized network access.
- **Multi-factor authentication**: MFA provides an extra layer of security that can help prevent unauthorized access to accounts, tools, systems and data repositories. Organizations should consider enabling MFA wherever possible.
- **Security patches**: Organizations of all sizes should have a robust patch management strategy that ensures security updates on all endpoints, servers, and appliances are applied as soon as possible to minimize the window of opportunity for an attack.
- **Backups**: Backups are one of the most effective ways of mitigating the effects of a ransomware incident. Many strains of ransomware can spread laterally across the network and encrypt locally stored backups, so organizations should use a mixture of media storage, and store backup copies both on- and off-site. See this guide for more information on creating ransomware-proof backups.
- **System hardening**: Hardening networks, servers, operating systems and applications is crucial for reducing attack surface and managing potential security vulnerabilities. Disabling unneeded and potentially exploitable services such as PowerShell, RDP, Windows Script Host, Microsoft Office macros, etc. reduces the risk of initial infection, while implementing the principle of least privilege can help prevent lateral movement.

- **Block macros**: Many ransomware families are delivered via macro-embedded Microsoft Office or PDF documents. Organizations should review their use of macros, consider blocking all macros from the Internet, and only allow vetted and approved macros to execute from trusted locations.
- **Email authentication**: Organizations can use a variety of email authentication techniques such as Sender Policy Framework, DomainKeys Identified Mail, and Domain-Based Message Authentication, Reporting and Conformance to detect email spoofing and identify suspicious messages.
- **Network segregation**: Effective network segregation helps contain incidents, prevents the spread of malware and reduces disruption to the wider business.
- **Network monitoring**: Organizations of all sizes must have systems in place to monitor possible data exfiltration channels and respond immediately to suspicious activity.
- **Penetration testing**: Penetration testing can be useful for revealing vulnerabilities in IT infrastructure and employees' susceptibility to ransomware. Results of the test can be used to allocate IT resources and inform future cybersecurity decisions.
- **Incident response plan**: Organizations should have a comprehensive incident response plan in place that details exactly what to do in the event of infection. A swift response can help prevent malware from spreading, minimize disruption and ensure the incident is remediated as efficiently as possible.

How to remove ALPHV and other ransomware

ALPHV uses encryption methods that currently make it impossible to decrypt data without paying for an attacker-supplied decryption tool.

Download now: Emsisoft Anti-Malware free trial.

Antivirus software from the world's leading ransomware experts. Get your free trial today. Try It Now

Victims of ALPHV should be prepared to restore their systems from backups, using processes that should be defined in the organization's incident response plan. The following actions are recommended:

- Take action to contain the threat.
- Determine the extent of the infection.
- Identify the source of the infection.
- Collect evidence.
- Restore the system from backups.
- Ensure all devices on the network are clean.
- Perform a comprehensive forensic analysis to determine the attack vector, the scope of the incident and the extent of data exfiltration.
- Identify and strengthen vulnerabilities to reduce the risk of a repeat incident.

Senan Conrad

As a cybersecurity enthusiast, Senan specializes in giving readers insight into the ever-changing world of malware, and the ransomware scene in particular. When he's not tapping away at his keyboard, you can catch Senan drinking a good coffee or tinkering in his workshop.