



THREAT PROFILE:

# Alphv Ransomware



# Table of Contents

Executive Summary	2
Description	3
Previous Targets: Alphv <ul style="list-style-type: none"><li>• Previous Industry Targets</li><li>• Previous Victim HQ Regions</li></ul>	5
Data Leak Site: Alphv	7
Known Exploited Vulnerabilities	8
Associations: Alphv	10
Known Tools: Alphv	12
Observed Alphv Behaviors <ul style="list-style-type: none"><li>• Windows</li><li>• Linux</li></ul>	15
MITRE ATT&CK® Mappings: Alphv	17
References	23

# Executive Summary

## First Identified:

2021

## Operation style:

Ransomware-as-a-Service (RaaS), affiliates earn 80% of payments up to \$1.5 million, 85% of payments up to \$3 million, and 90% of payments over \$3 million.

## Extortion method:

Double extortion – combining the traditional ransomware extortion method (encryption) with exfiltration of victim’s sensitive data; the group threatens to leak the data via a data leak site if the ransom demand is not paid.

## Most frequently targeted industry:

- Industrials (Manufacturing)
- Professional & Commercial Services

## Most frequently targeted victim HQ region:

- United States, North America

## Known Associations:

- FIN8
- FIN12
- DEV-0237
- DEV-0504
- Scattered Spider
- ShadowSyndicate
- UNC4466
- BlackMatter Ransomware

### INITIAL ACCESS

Valid accounts, exploiting external remote services, vulnerability exploitation, social engineering (MITRE ATT&CK: T1078, T1133, T1190, T1566)

### PERSISTENCE

Valid Accounts, abuse of system processes, Registry Keys, Startup Folder, server software component (MITRE ATT&CK: T1078, T1505, T1543, T1547)

### LATERAL MOVEMENT

Abuse of remote systems, lateral tool transfer (MITRE ATT&CK: T1021, T1570)

# Description

Alphv (AKA BlackCat, Noberus) is a ransomware variant that has been active since at least November 2021 and operates using the double extortion method – where victim data is stolen and leaked if a ransom is not paid. Alphv operates as a RaaS (Ransomware as a Service), where affiliates gain access to victim environments, deploy the Alphv encryptor and then split the ransom payment with the developers. Affiliates can earn 80% of payments up to \$1.5 million, 85% of payments up to \$3 million, and 90% of payments over \$3 million. Due to the use of an affiliate program, Alphv operators gain initial access in a variety of methods, including social engineering, exploiting vulnerabilities, initial access brokers (IABs), and more.

Alphv's operators were one of the first to successfully use the Rust programming language to compromise victims. Alphv's use of Rust enables the operators to increase their defense evasion capabilities and avoid code similarities with other ransomware variants. Due to the flexibility of Rust, it likely allows Alphv's operators to tailor attacks to each specific victim. Alphv is able to target Windows, ESXi, Debian, Ubuntu, and ReadyNAS/Synology environments.

Alphv is consistently updating and refining their operations to ensure they remain as effective and successful as possible. One update included an ARM build to encrypt non-standard architectures and a feature that adds new encryption functionality to its Windows build by rebooting into Safe Mode and Safe Mode with networking. A new restart logic was added, along with a simplification of the Linux encryption process.

Affiliates can earn 80% of payments up to \$1.5 million, 85% of payments up to \$3 million, and 90% of payments over \$3 million.

In August 2022, the group was observed deploying a custom Exmatter data exfiltration tool, which had been previously used with the BlackMatter ransomware. A new variant of Alphv, dubbed Sphynx, was observed that contained new command line arguments and methods for evading detection.

In December 2023, the FBI announced the seizure of the Alphv ransomware data leak site and were able to provide decryption keys for 500 victims of the ransomware group, saving nearly \$68 million in ransom demands. Additionally, the FBI seized the domain for Alphv's data leak site, which displayed a banner stating it was seized. However, within the same day, the group "unseized" the site and posted a new site link. Additionally, the site hosted a message that due to the takedown, the group was removing all rules for their affiliates as far as vertical targeting. The only rule that affiliates reportedly have to follow is to avoid targeting organizations in CIS countries.

# Description

In March 2024, the threat actors behind the Alphv ransomware operation shut down their data leak site and rumors began that the group conducted an exit scam. The group posted the same images of the seizure notices on their site; however, security research Fabian Wosar, reported that the “seizure” was fake and that the group was pulling an exit scam. In addition to law enforcement denying any involvement, the source code of the new takedown notice indicated that it was a saved version rather than an original takedown notice.

The exit came just after the group received a \$22 million payment to a cryptocurrency wallet, reportedly a ransom demand from Change Healthcare – although the company has not confirmed the payment at the time of writing. On the cybercriminal forum RAMP, a user “Notchy” reported that they were the Alphv affiliate responsible for the Change Healthcare attack and that Alphv operators emptied the wallet and did not pay Notchy their share of the payment.

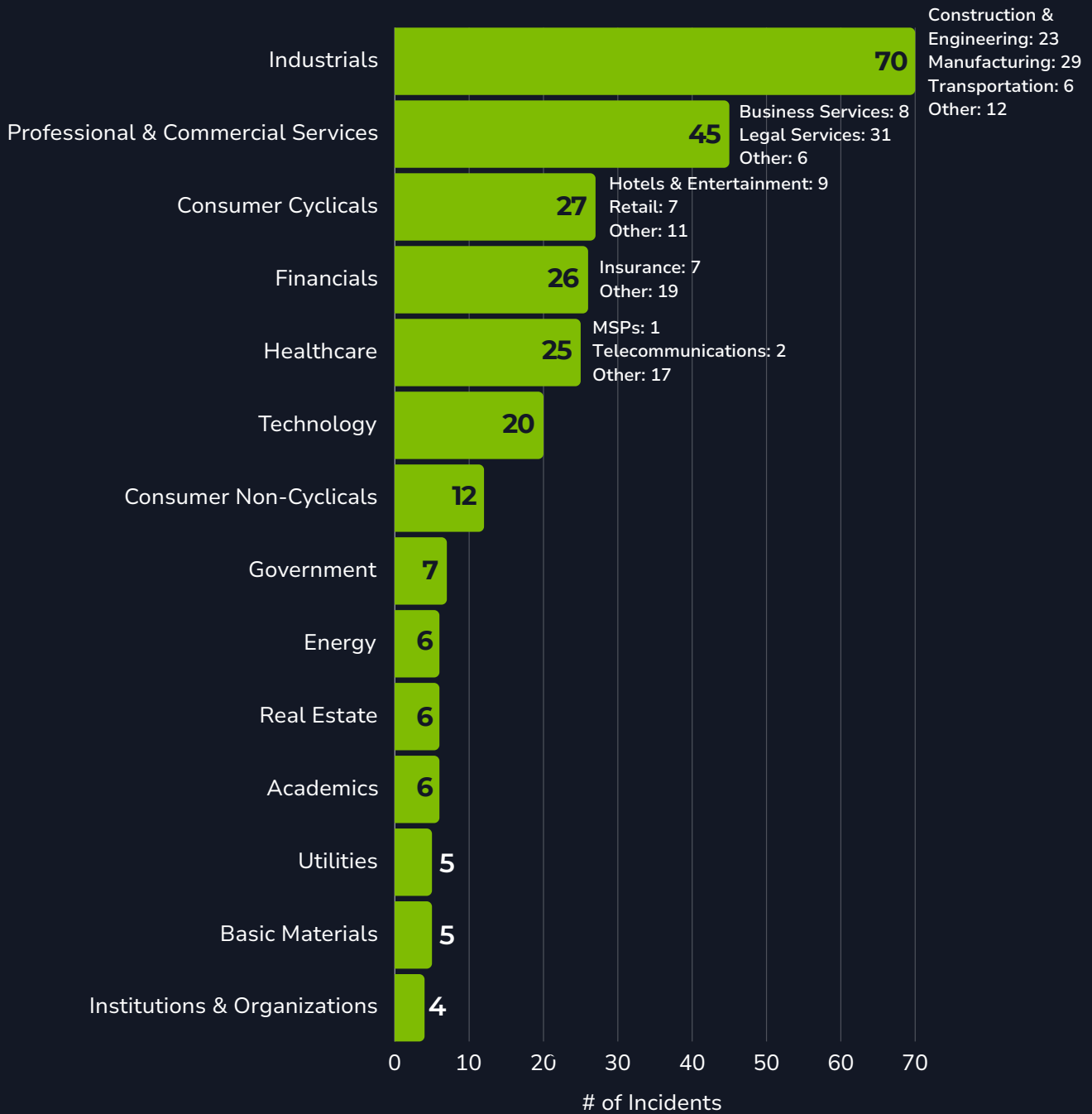
There is an even chance that the Alphv operators conducted these actions due to fear of another takedown; the exit came two months after the FBI disrupted the operation and shortly after the LockBit operation was disrupted. Additionally, LockBit operators released a statement warning that law enforcement likely had access to other operations, which likely attributed to Alphv’s decision to exit at this time.

Whether the group pulled an exit scam or not, the Alphv operation appears to be ceased. However, it is likely that the affiliates of Alphv will move to other operations over the next 30 days; there is an even chance that Alphv operators will either sell their source code – which will likely result in many offshoots emerging – or rebrand their operation and begin conducting ransomware attacks again over the next 12 months.

Whether the group pulled an exit scam or not, the Alphv operation appears to be ceased.

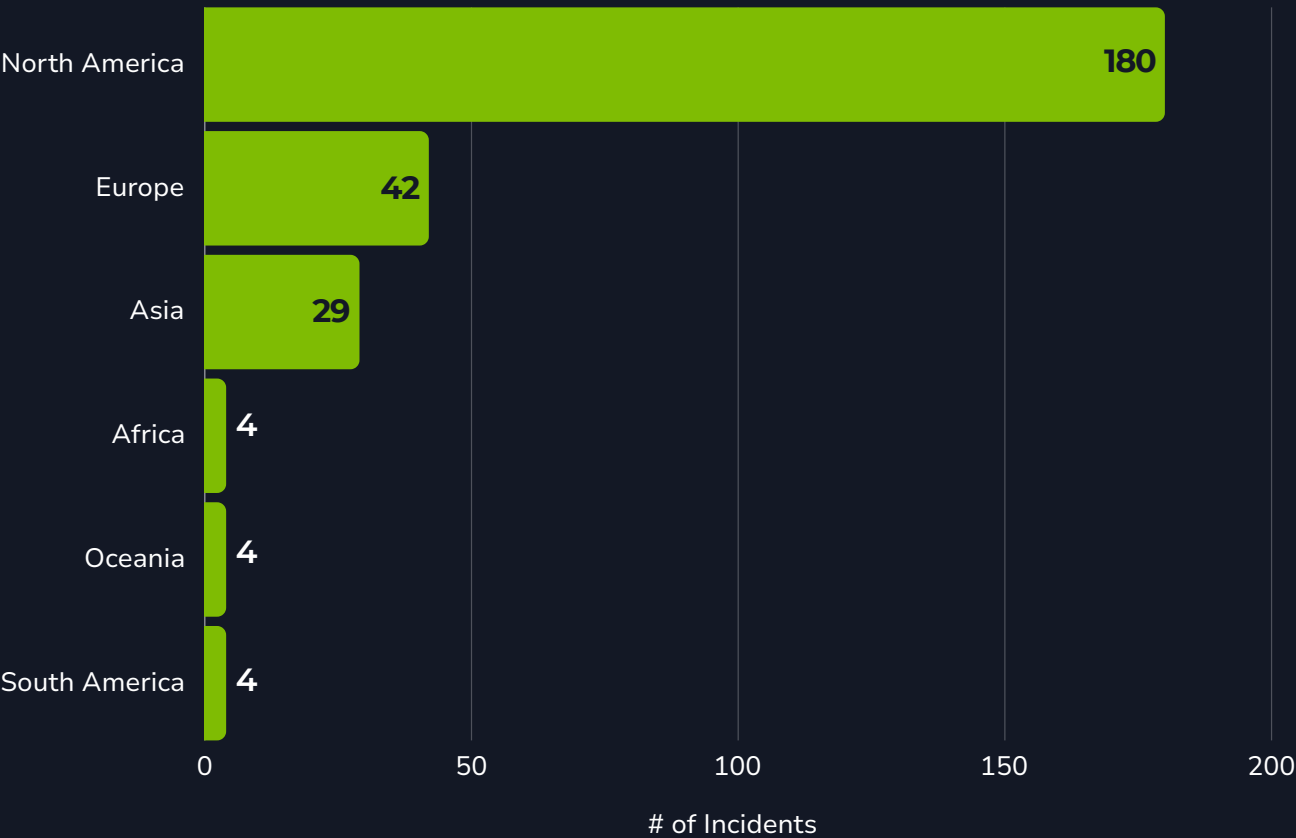
# Previous Targets: Alphv

Previous Industry Targets from 01 Jul 2023 to 30 Jun 2024

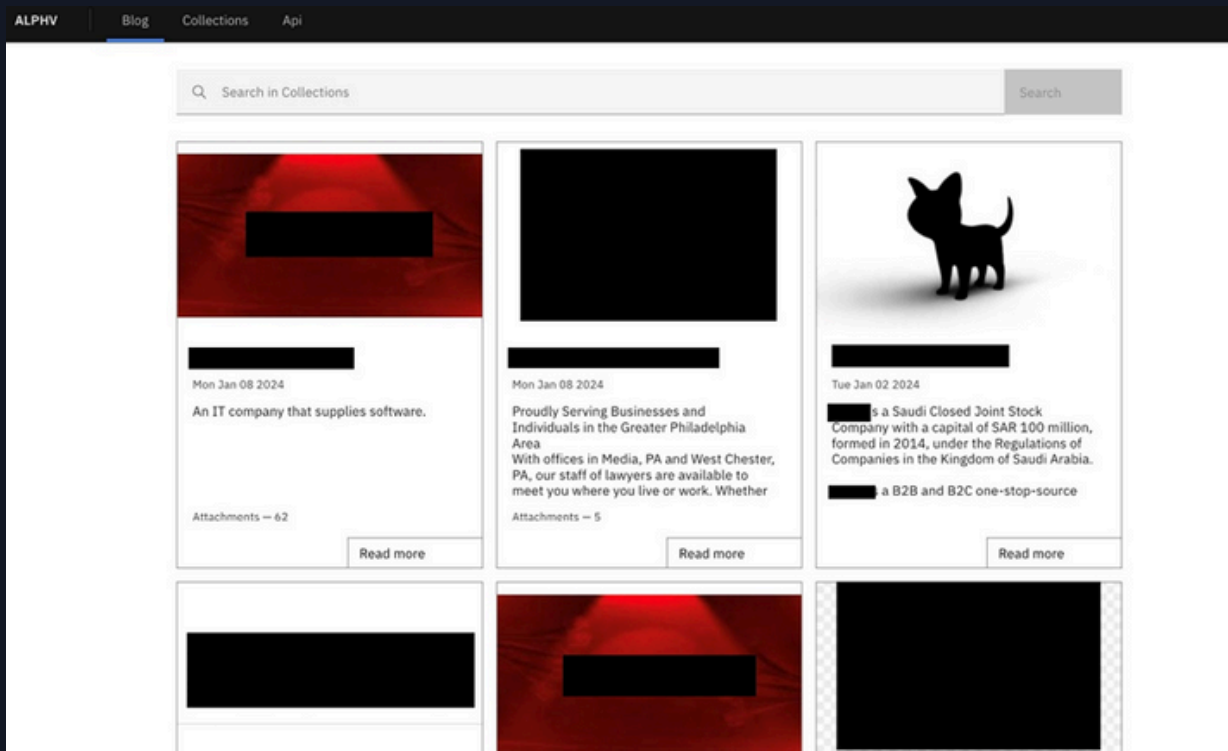


# Previous Targets: Alphv

Previous Victim HQ Regions from 01 Jul 2023 to 30 Jun 2024



# Data Leak Site: Alpv



[http://2cuqgeerjdba2rhdiviezodpu3lc4qz2sjf4qin6f7std2evleqlzjid\[.\]onion/](http://2cuqgeerjdba2rhdiviezodpu3lc4qz2sjf4qin6f7std2evleqlzjid[.]onion/)  
[http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad\[.\]onion/](http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad[.]onion/)  
[http://alphvuzxyxv6ylumd2ngp46xzq3pw6zflomrghvxeuks6kklberrbmyd\[.\]onion/](http://alphvuzxyxv6ylumd2ngp46xzq3pw6zflomrghvxeuks6kklberrbmyd[.]onion/)  
[http://vqifkltreqpudvulhbzmc5gocbeawl67uvs2pttswemdorbnhaddohyd\[.\]onion/](http://vqifkltreqpudvulhbzmc5gocbeawl67uvs2pttswemdorbnhaddohyd[.]onion/)



# Known Exploited Vulnerabilities

## [CVE-2016-0099](#) (CVSS: 7.8)

Privilege Escalation Vulnerability

Product Affected: Microsoft Windows Secondary Logon Service

---

## [CVE-2018-13379](#) (CVSS: 9.8)

Credential Exposure Vulnerability

Product Affected: Fortinet FortiOS SSL VPN

---

## [CVE-2021-26857](#) (CVSS: 7.8)

Deserialization Vulnerability

Product Affected: Microsoft Unified Messaging

---

## [CVE-2021-26858](#) (CVSS: 7.8)

RCE Vulnerability

Product Affected: Microsoft Exchange Server

---

## [CVE-2021-27065](#) (CVSS: 9.8)

RCE Vulnerability

Product Affected: Microsoft Exchange Server

---

## [CVE-2021-27876](#) (CVSS: 8.8)

Remote Unauthorized Access Vulnerability

Product Affected: Veritas Backup Exec

---

## [CVE-2021-27877](#) (CVSS: 9.8)

Arbitrary Command Execution Vulnerability

Product Affected: Veritas Backup Exec

---

# Known Exploited Vulnerabilities

## [CVE-2021-27878](#) (CVSS: 8.1)

Arbitrary File Access Vulnerability

Product Affected: Veritas Backup Exec

---

## [ProxyLogon \(CVE-2021-26855\)](#) (CVSS: 9.8)

RCE Vulnerability

Product Affected: Microsoft Exchange

---

## [ProxyShell \(CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207\)](#) (CVSS: 9.8, 9.8, 7.2)

Pre-Auth Path Confusion, Privilege Escalation, Post-Auth RCE Vulnerabilities

Product Affected: Microsoft Exchange

---

# Associations: Alphv

## ALPHVM Ransomware

Alphv Alias

---

## BlackCat Ransomware

Alphv Alias

---

## Noberus Ransomware

Alphv Alias

---

## Sphynx

A variant of Alphv encryptor that was released in February 2023.

---

## FIN8

Affiliate of Alphv ransomware RaaS operation.

---

## FIN12

Affiliate of Alphv ransomware RaaS operation.

---

## DEV-0237

Affiliate of Alphv ransomware RaaS operation.

---

## DEV-0504

Affiliate of Alphv ransomware RaaS operation.

---

## Scattered Spider

Affiliate of Alphv ransomware RaaS operation.

---

## ShadowSyndicate

Affiliate of Alphv ransomware RaaS operation.

---

# Associations: Alphv

## UNC4466

Affiliate of Alphv ransomware RaaS operation.

---

## BlackMatter Ransomware

Multiple researchers have previously reported that Alphv is a rebranded version of the BlackMatter ransomware operation, previously known as DarkSide. However, Alphv representatives have stated they are not a rebrand but have employed affiliates associated with the former ransomware operations.

---

# Known Tools: Alphv

---

## 7zip

A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration.

---

## AdFind

A free command-line query tool that can be used for gathering information from Active Directory.

---

## AdRecon

A tool that gathers information about the Active Directory and generates a remote which can provide a holistic picture of the current state of the target AD environment.

---

## Advanced Port Scanner

A free network scanner allowing you to quickly find open ports on network computers and retrieve versions of programs running on the detected ports.

---

## bcdedit

A command line tool for managing Configuration Data; it can be used to create new stores, modify existing stores, and add boot menu options.

---

## cmd

A program used to execute commands on a Windows computer.

---

## CMSTPLUA COM interface

An interfaced used by multiple ransomware operations that allows the operators to elevate privileges and establish persistence by installing the ransomware as a service.

---

## Cobalt Strike

A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.

---

## ConnectWise

Formerly ScreenConnect. A self-hosted remote desktop software application that can be used to remotely access victim environments.

---

## Empire

An open source, cross-platform remote administration and post-exploitation framework that is publicly available on GitHub. While the tool itself is primarily written in Python, the post-exploitation agents are written in pure PowerShell for Windows and Python for Linux/macOS.

---

## ExMatter

A data exfiltration tool that is designed to steal user files, databases, and compressed file from multiple directories and then upload them to a preconfigured server via SFTP.

# Known Tools: Alphv

## FreeFileSync

A free open-source data backup software that can allow users to synchronize files and folders on devices.

---

## Koadic

A Windows post-exploitation framework and penetration testing tool that is publicly available on GitHub.

---

## LaZagne

An open-source application used to retrieve passwords stored on a local computer.

---

## Ligolo

A simple and lightweight tool for establishing SOCKS5 or TCP tunnels from a reverse connection in complete safety.

---

## LSASS

A Windows process that takes care of security policy for the OS.

---

## MEGASync

A cloud-based synchronization tool that is designed to work with the MEGA file-sharing service.

---

## MetaSploit

A tool that can be used by threat actors to probe systematic vulnerabilities on networks and servers.

---

## Mimikatz

An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.

---

## MobaXterm

An application that provides X-Server capability for the Microsoft Windows OS. It allows applications running in the Unix/Linux environment to display graphical user interfaces on the MS Windows desktop.

---

## Nanodump

A flexible tool that creates a minidump of the LSASS process.

---

## net

A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.

---

## PowerShell

A task automation and configuration management program that includes a command-line shell and the associated scripting language.

---

# Known Tools: Alphv

## Process Hacker

An open-source tool that allows users to see what processes are running on a device and identify network connections that are associated with a process.

---

## PsExec

A utility tool that allows users to control a computer from a remote location.

---

## Rclone

A command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.

---

## RevSocks

A cross-platform SOCKS5 proxy server program/library written in C that can also reverse itself over a firewall.

---

## RDP

A protocol that provides a user with a graphical interface to connect to another computer over a network connection.

---

## SMB

A client-server communication protocol used for sharing access to files, printers, serial ports, and other resources on a network.

---

## SoftPerfect

A network scanner that can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices.

---

## Total Deployment Software

An administration tool that allows users to remotely deploy software, uninstall software, inventory software. Threat actors can use the tool to deploy malware payloads and additional tools.

---

## VSSAdmin

A Windows service that allows taking manual or automatic backup copies of computer files or volumes.

---

## Windows Task Scheduler

A tool that allows predefined actions to be automatically executed at predefined times or after specified time intervals.

---

## WinSCP

A free and open-source SFTP, FTP, WebDAV, S3, and SCP client for Windows that can be used to exfiltrate files to a remote server.

---

## WMIC

A utility that provides a command-line interface for Windows Management Instrumentation.

---

# Observed Alphy Behaviors: Windows

<p><b>Persistence</b></p>	<pre>net use \\[computer name] /user:[domain]\[user] [password] /persistent:no reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanman Server\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f cmd.exe /c "bcdedit /set {default}" cmd.exe /c "bcdedit /set {default} recoveryenabled No"</pre>
<p><b>Defense Evasion</b></p>	<pre>C:\Windows\system32\cmd.exe" /c "cmd.exe /c for /F \"tokens=*\" Incorrect function. in (' wevtutil.exe el ') DO wevtutil.exe cl \"Incorrect function. \" cmd.exe /c "vssadmin.exe Delete Shadows /all /quiet" cmd.exe /c "wmic.exe Shadowcopy Delete" cmd.exe /c "iisreset.exe /stop" cmd.exe /c "fsutil behavior set SymlinkEvaluation R2L:1" cmd.exe /c "fsutil behavior set SymlinkEvaluation R2R:1"</pre>
<p><b>Discovery</b></p>	<pre>whoami /all arp -a cmd.exe /c "wmic csproduct get UUID"</pre>
<p><b>Lateral Movement</b></p>	<pre>psexec.exe -accepteula \\&lt;TARGET_HOST&gt; -u &lt;USERNAME&gt; -p &lt;PASSWORD&gt; -s -d -f -c &lt;ALPHV_EXECUTABLE&gt; [FLAGS] [OPTIONS] -- access-token &lt;ACCESS_TOKEN&gt; [SUBCOMMAND]</pre>
<p><b>Impact</b></p>	<pre>HKEY_USERS\&lt;SID&gt;\Control Panel\Desktop\WallPaper = "C:\\Users\\ &lt;USERNAME&gt;\\Desktop\\RECOVER-&lt;ENCRYPTED_FILE_EXTENSION&gt;- FILES.txt.png" RECOVER-&lt;ENCRYPTED_FILE_EXTENSION&gt;-FILES.txt %USERPROFILE%\Desktop\RECOVER-&lt;ENCRYPTED_FILE_EXTENSION&gt;- FILES.txt.png</pre>



# Observed Alpv Behaviors: Linux

<b>Defense Evasion</b>	<pre>for i in `vim-cmd vmsvc/getallvms  awk '{print\$1}'`;do vim-cmd vmvc/snapshot.removeall \$i &amp; done awk -F "\",\"*" '{system("esxcli vm process kill --type=force --world- id=\"\$1\")}'</pre>
<b>Discovery</b>	<pre>esxcli --formatter=csv --format- param=fields=="WorldID,DisplayName" vm process list</pre>

# MITRE ATT&CK® Mappings: Alphv

<b>Reconnaissance</b>	
T1589: Gather Victim Identity Information	.001: Credentials
<b>Resource Development</b>	
T1583: Acquire Infrastructure	.003: Virtual Private Server
<b>Initial Access</b>	
T1078: Valid Accounts	.003: Local Accounts
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
<b>Execution</b>	
T1047: Windows Management Instrumentation	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell .006: Python
T1106: Native API	
T1569: System Services	.002: Service Execution
<b>Persistence</b>	
T1078: Valid Accounts	

# MITRE ATT&CK® Mappings: Alphv

Persistence	
T1505: Server Software Component	
T1543: Create or Modify System Process	.003: Windows Service
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder
Privilege Escalation	
T1078: Valid Accounts	
T1134: Access Token Manipulation	.001: Token Impersonation/Theft .002: Create Process with Token
T1548: Abuse Elevation Control Mechanism	.002: Bypass User Account Control
Defense Evasion	
T1027: Obfuscated Files or Information	.002: Software Packing .009: Embedded Payloads
T1036: Masquerading	
T1055: Process Injection	
T1070: Indicator Removal	.001: Clear Windows Event Logs .004: File Deletion
T1112: Modify Registry	
T1140: Deobfuscate/Decode Files or Information	
T1222: File and Directory Permissions Modification	.001: Windows File and Directory Permissions Modification

# MITRE ATT&CK® Mappings: Alphv

Defense Evasion	
T1484: Domain Policy Modification	.001: Group Policy Modification
T1497: Virtualization/Sandbox Evasion	.001: System Checks
T1562: Impair Defenses	.001: Disable or Modify Tools .009: Safe Mode Boot
T1564: Hide Artifacts	.010: Process Argument Spoofing
T1574: Hijack Execution Flow	.011: Services Registry Permissions Weakness
T1620: Reflective Code Loading	
T1622: Debugger Evasion	
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory
T1552: Unsecured Credentials	
T1555: Credentials from Password Stores	.003: Credentials from Web Browsers
Discovery	
T1007: System Service Discovery	
T1012: Query Registry	
T1016: System Network Configuration Discovery	
T1018: Remote System Discovery	

# MITRE ATT&CK® Mappings: Alphv

Discovery	
T1033: System Owner/User Discovery	
T1046: Network Service Discovery	
T1057: Process Discovery	
T1069: Permission Groups Discovery	.002: Domain Groups
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.001: Local Account .002: Domain Account
T1135: Network Share Discovery	
T1482: Domain Trust Discovery	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares .004: SSH
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1039: Data from Network Shared Data	

# MITRE ATT&CK® Mappings: Alphv

Collection	
T1074: Data Staged	
T1119: Automated Collection	
T1213: Data from Information Repositories	
T1560: Archive Collected Data	.010: Archive via Utility
Exfiltration	
T1020: Automated Exfiltration	
T1030: Data Transfer Size Limits	
T1041: Exfiltration Over C2 Channel	
T1048: Exfiltration Over Alternative Protocol	.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage
Impact	
T1485: Data Destruction	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	

# MITRE ATT&CK® Mappings: Alphv

Impact	
T1491: Defacement	.001: Internal Defacement
T1498: Network Denial of Service	
T1529: System Shutdown/Reboot	
T1561: Disk Wipe	.001: Disk Content Wipe
T1657: Financial Theft	

# References

- Deyalsingh, Jason; Smith, Nick; Mattos, Eduardo; McLellan, Tyler (2023, April 03) Mandiant: “ALPHV Ransomware Affiliate Targets Vulnerable Backup Installations to Gain Initial Access.” <https://www.mandiant.com/resources/blog/alphv-ransomware-backup>
- ETDA (2023, June 22) “Tool: BlackCat.” <https://apt.etcha.or.th/cgi-bin/listgroups.cgi?t=BlackCat&n=1>
- FBI (2022, April 19) “BlackCat/ALPHV Ransomware Indicators of Compromise.” <https://www.ic3.gov/Media/News/2022/220420.pdf>
- Hill, Jason (2023, April 14) Varonis: “BlackCat Ransomware (ALPHV).” <https://www.varonis.com/blog/blackcat-ransomware>
- IBM Security X-Force Team (2023, May 30) “BlackCat (ALPHV) ransomware levels up for stealth, speed and exfiltration.” <https://securityintelligence.com/x-force/blackcat-ransomware-levels-up-stealth-speed-exfiltration/>
- Microsoft Threat Intelligence (2022, June 13) “The many lives of BlackCat ransomware.” <https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/>
- MITRE (2023, June 15) “BlackCat.” <https://attack.mitre.org/software/S1068/>
- SecurityScorecard (n.d.) A Deep Dive Into ALPHV/BlackCat Ransomware. <https://securityscorecard.com/research/deep-dive-into-alphv-blackcat-ransomware/>
- StoneFly (n.d.) “BlackCat/Alphv Ransomware: In-Depth Analysis and Mitigation.” <https://stonefly.com/blog/blackcat-alphv-ransomware-analysis-and-mitigation/>
- Trend Micro Research (2022, October 27) “Ransomware Spotlight: BlackCat.” <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat>
- Yuceel, Huseyin Can (2022, August 22) Picus Security: “BlackCat Ransomware Gang.” <https://www.picussecurity.com/resource/black-cat-ransomware-gang>
- Zhdanov, Andrey (2022, June 29) Group IB: “Fat Cats: An analysis of the BlackCat ransomware affiliate program.” <https://www.group-ib.com/blog/blackcat/>
- Zohdy, Mahmoud; Magdy, Sherif; Fahmy, Mohamed; Yamany, Bahaa (2023, May 22) Trend Micro: “BlackCat Ransomware Deploys New Signed Kernel Driver.” [https://www.trendmicro.com/en\\_us/research/23/e/blackcat-ransomware-deploys-new-signed-kernel-driver.html](https://www.trendmicro.com/en_us/research/23/e/blackcat-ransomware-deploys-new-signed-kernel-driver.html)





Adversary Pursuit Group

