blackpoint

THREAT PROFILE:

Ransomhub Ransomware

Table of Contents

Executive Summary 2

Description 3

Previous Targets: Ransomhub 4
- Previous Industry Targets
- Previous Victim HQ Regions

Data Leak Site: Ransomhub 6

Known Exploited Vulnerabilities 7

Associations: Ransomhub 8

Known Tools: Ransomhub 9

Observed Ransomhub Behaviors 11
- Windows
- Linux

MITRE ATT&CK® Mappings: Ransomhub 12

References 13

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:
- Technology

Most frequently targeted victim HQ region:
- North America

Known Associations:
- Koley
- Nothcy
- Alphv Ransomware
- Knight Ransomware
- Scattered Spider

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.

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 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.

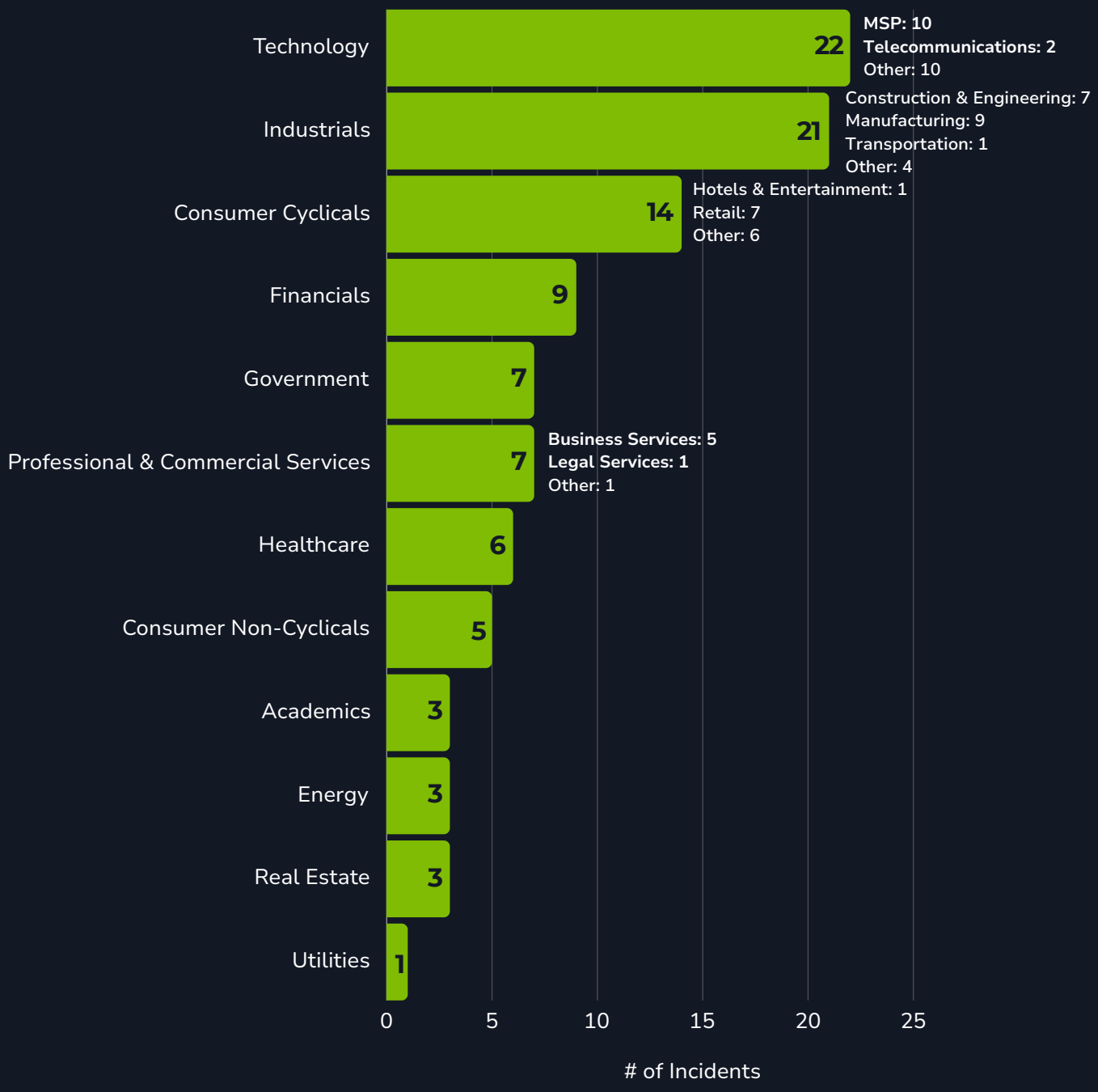
Ransomhub affiliates are offered 90% of ransom payments, with the core group taking a 10% commission.

Ransomhub initial access methods likely vary depending on the affiliate deploying the ransomware. It is likely that the affiliates gain access using tried-and-true methods such as social engineering, vulnerability exploitation, valid accounts, and initial access brokers (IABs).

Little is known about the inner workings of the Ransomhub operation as the group is new to the landscape. However, the group has proven they are capable and pose a credible threat to organizations and it is likely that additional analysis will be completed over the next 12 months.

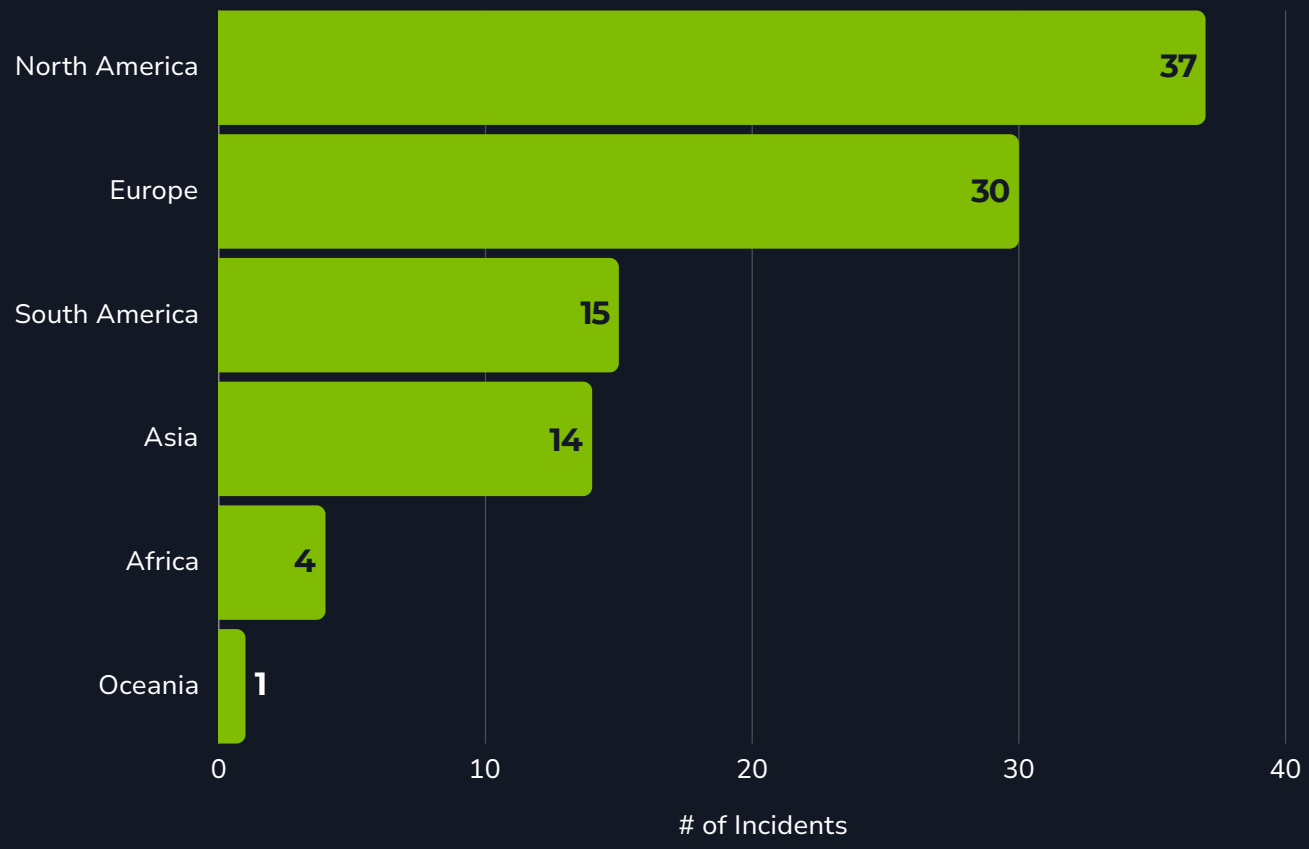
Previous Targets: Ransomhub

Previous Industry Targets from 01 Feb 2024 to 30 Jun 2024

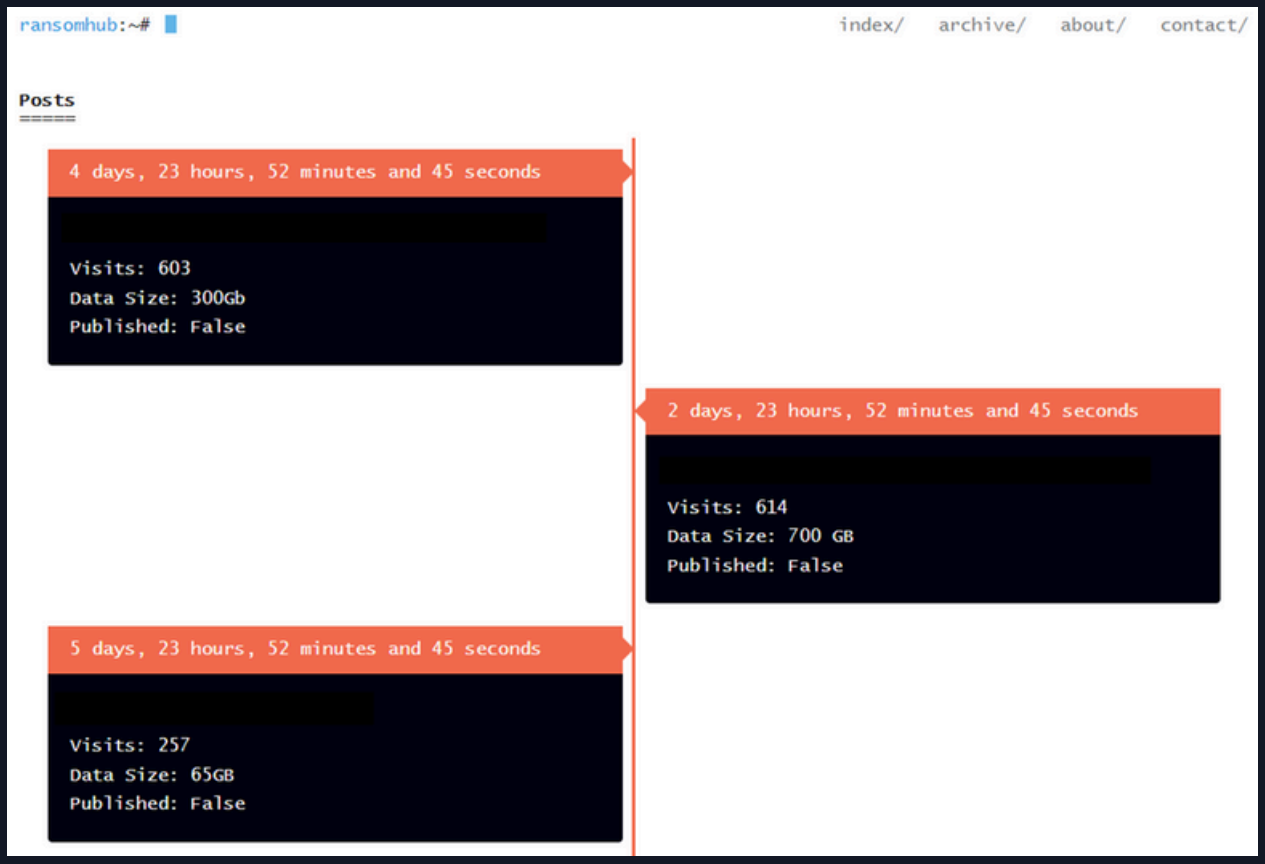


Previous Targets: Ransomhub

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



Data Leak Site: Ransomhub



hxxp://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion

Known Exploited Vulnerabilities

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

Privilege Escalation Vulnerability
Product Affected: Netlogon

Associations: Ransomhub

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.

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

Atera	A remote monitoring and network discovery tool that provides a comprehensive security scan and complete view of all your end-user networks and devices.
cmd	A program used to execute commands on a Windows computer.
EDRKillShifter	A tool designed to terminate endpoint protection software.
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.
iisrstas.exe	An Internet Information Services reset control.
NetScan	A utility that scans within a subnet or IP range to check for devices.
POORTRY	A Windows driver that implements process termination and requires a userland utility to initiate the functionality.
PsExec	A utility tool that allows users to control a computer from a remote location.
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.
TOR	An open-source software for enabling anonymous communication, making it more difficult to trace a user's internet activity.

Known Tools: Ransomhub

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

Observed Ransomhub Behaviors: Windows

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

MITRE ATT&CK® Mappings: Ransomhub

Execution	
T1047: Windows Management Instrumentation	
T1059: Command and Scripting Interpreter	.003: Windows Command Shell
Defense Evasion	
T1070: Indicator Removal	.001: Clear Windows Event Logs
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
- 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/
- 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
- 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