



| Profile |

RansomHub Ransomware

P-2025-02-28a

Classification: TLP:GREEN

Criticality: Medium

Intelligence Requirements: Deep Dark Web & Criminal Underground,
Ransomware, Threat Actor Targeting

February 28, 2025



Profile

RansomHub Ransomware

Report Date: February 28, 2025**Intelligence Cut-off:** 8:00 PM (EST) on
February 26, 2025

First Observed	February 2024
Origin	Russia
Former Aliases	Cyclops, Knights
Motivation	Financial Gain
Targeted Industries	Communication, Critical Infrastructure, Emergency Services, Finance, Food and Agriculture, Government, Healthcare, Information Technology (IT), Manufacturing, Transportation, Water and Wastewater <i>Note: This list should not be treated as exhaustive.</i>
Targeted Nations	Mexico, United States, Italy, Netherlands <i>Note: This list should not be treated as exhaustive.</i>
Tools	PuTTY, Amazon AWS S3 buckets/tools, HTTP POST requests, WinSCP, Rclone, Cobalt Strike, Metasploit, AngryIPScanner, Nmap, SoftPerfect, NetScan, Atera, Splashtop <i>Note: This list should not be treated as exhaustive.</i>

Actor Background

RansomHub (former aliases: Cyclops and Knight) is a ransomware-as-a-service (RaaS) variant initially launched in the predominantly Russian-speaking dark web forum RAMP. On February 20, 2024, ZeroFox published a report on the launch of the RansomHub RaaS, noting the group had established a partnership program and that user “koley” was using RAMP to recruit from other well-known ransomware operations like LockBit and ALPHV (Blackcat) after both groups were taken down by law enforcement. Koley claimed

RansomHub had created “the next generation of ransomware” and highlighted its numerous state-of-the-art features and benefits in a post dated February 2, 2024.¹



RAMP post by koley seeking RansomHub affiliates

Source: ZeroFox Intelligence

RansomHub demonstrated rapid success, encrypting and exfiltrating data from at least 210 victims between February and August 2024, and the group has since accumulated over 500 more possible victims. In August 2024, ZeroFox reported RansomHub’s activity was on an upward trajectory and had accounted for an estimated 2 percent of all attacks in the first quarter of 2024, 5 percent in the second quarter, and 14 percent in the third quarter. At that time, ZeroFox had also observed approximately 34 percent of RansomHub’s attacks targeted European-based organizations in comparison to 25 percent across the general threat landscape.² The group claims it avoids targeting Cuba, North Korea, China, and Commonwealth of Independent States (CIS).³

¹ <https://www.zerofox.com/intelligence-feed/the-underground-economist-volume-4-issue-4/>

²

<https://www.zerofox.com/intelligence-feed/ransomhub-extortion-attacks-on-sharp-upward-trajectory/>

³ [hXXps://thehackernews\[.\]com/2024/09/ransomhub-ransomware-group-targets-210.html](https://thehackernews[.]com/2024/09/ransomhub-ransomware-group-targets-210.html)

Tactics, Techniques, and Procedures (TTPs)

In its February 20, 2024, report, ZeroFox highlighted RansomHub's purported features:

- Native architecture with encryption software written in Go Programming (Golang) and C++, which the threat actor claims will create complications for anti-virus (AV) software.
- "Very fast" encryption speeds assisted by an adaptive algorithm change method.
- Supports Windows, ESXi, and Linux-based operating systems, as well as virtual machines (VM).
- Uses Abstract Syntax Trees (AST) structure to re-encrypt every day, maintaining obfuscation.
- Access to the ransomware's control panel, which offers affiliates a unique .onion domain. The panel is used to manage targets and log their accesses, use chat rooms, and create private blog pages that can be used for "proofing."
- Features to enable and encourage efficient communication and cooperation between affiliates, to include vouching for each other and sharing evidence of cooperation with other RaaS teams on previous projects.⁴

⁴ <https://www.zerofox.com/intelligence-feed/the-underground-economist-volume-4-issue-4/>

Panel

Each panel uses a separate onion domain, and the panels can manage targets and chat rooms.
The panel allows you to view the logs of target accesses and the last access time.
The panel supports Offline auto-reply for one message
The panel can create a private blog page, which can be very beneficial for proofing and negotiation.

Ticket

Affiliates who have joined our affiliate program to vouch for you.
ID of any well-known forums, the longer the registration time or have a certain deal as well as reputation.
Evidence of cooperation with other RaaS group (including, but not limited to, screenshots of payments received or balances at the receiving address.
The best and quickest way to join is to pay a deposit(Returned to you after first getting paid.)

Rules

We are not allow to attack CIS as well as Cuba, North Korea, China and Romania.
Accounts that add false targets or have no activity for a certain period of time will be banned.
Repeated attacks on paid targets are not allowed, encryption of non-profit hospitals is not allowed but data ransom is allowed.
After the target pays, you must fulfill all the terms and agreements promised in the negotiations, otherwise you will be banned.
We do not forbid you to cooperate with other RaaS team at the same time, but you can not disclose our panel address and account password, when we find more than one user logging in and do not explain the situation, we will ban your account.

TOX 4D598799696AD5399FABF7D40C4D1BE9F05D74CFB311047D7391AC0BF64BED47B56EEE66A528

Last edited: Yesterday at 5:09 PM

RAMP post advertising new Ransomhub RaaS project

Source: ZeroFox Intelligence

RansomHub employs common ransomware TTPs like phishing and vulnerability exploitation and utilizes a double extortion model of exfiltrating information, deleting shadow volume copies and encrypting systems as a means of extorting its victims. RansomHub affiliates obtain initial access and disable Endpoint Detection and Response (EDR) solutions before conducting reconnaissance and network scanning using tools like AngryIPScanner, Nmap, SoftPerfect, NetScan, and living-off-the-land methods using PowerShell. The group also utilizes Remote Access Solutions, like Atera and Splashtop.

RansomHub has targeted environments through vulnerability exploits in Atlassian Confluence Data Center and Server Broken Access Control Vulnerability (CVE-2023-22515), Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability (CVE-2023-27997), Citrix ADC (CVE-2023-3519), Apache ActiveMQ Deserialization of Untrusted Data Vulnerability (CVE-2023-46604), F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability(CVE-2023-46747), and Fortinet FortiClient EMS SQL Injection Vulnerability (CVE-2023-48788) devices. The group has exploited older vulnerabilities as well, to include Event Manager And Tickets Selling Plugin For WooCommerce < 3.8.0 – Contributor+ Stored XSS (CVE-2023-0144) and RapidLoad Power-Up for Autooptimize Plugin for WordPress Cross-Site Request Forgery (CSRF) (CVE-2020-1472), also known as Microsoft ZeroLogon.

RansomHub affiliates have used tools like Remote Desktop Protocol (RDP), PsExec, Connectwise, N-Able, Cobalt Strike, Metasploit, PsExec, and AnyDesk to move laterally within networks. The group will either dump compromised credentials or conduct password spraying to enable user accounts for persistence, re-enable disabled accounts, and utilize Mimikatz on Windows OS to gather credentials and escalate privileges to SYSTEM.⁵

RansomHub affiliates use different methods for data exfiltration and have utilized tools like PuTTY, Amazon AWS S3 buckets/tools, HTTP POST requests, WinSCP, Rclone, Cobalt Strike, and Metasploit, amongst others. The group then encrypts the victim's system utilizing Curve 25519, an Elliptic Curve Encryption algorithm which uses a public/private key unique to a victim's respective organization. The ransomware binary successfully encrypts files currently in use and accessible by the victim user by stopping various processes such as vmms.exe, msaccess.exe, outlook.exe, oracle.exe, sql.exe, wordpad.exe, winword.exe, svchost.exe, powerpnt.exe, and explorer.exe.

RansomHub utilizes an intermittent encryption technique to encrypt files in 1,048,576-byte (0x100000) segments while leaving 2,097,152-byte (0x200000) gaps unencrypted between those segments. Files smaller than 1,048,576 bytes are fully encrypted. Additionally, an extra 58-bytes (0x3A) of data are appended to the end of encrypted files. The appended data appears to contain a value likely related to the encryption or decryption key.

RansomHub's ransomware program typically avoids encrypting executable files. It appends a randomly generated extension to affected file names and leaves a ransom note commonly named, "How To Restore Your Files.txt" on the compromised system. The ransomware often utilizes vssadmin.exe to delete volume shadow copies, making recovery more challenging.

5

[hXXps://www.cisa\[.\]gov/sites/default/files/2024-09/aa24-242a-stopransomware-ransomhub-ransomware_1.pdf](https://www.cisa.gov/sites/default/files/2024-09/aa24-242a-stopransomware-ransomhub-ransomware_1.pdf)

The group provides its victims a unique .onion URL on the encrypted system as a medium for communication. RansomHub threatens to release its victim's compromised data on a data leak site if the victim does not pay the prescribed ransom within a time frame ranging from three to 90 days.

Recent Targeting

Mexico: In mid-November 2024, RansomHub carried out a ransomware attack targeting the Mexican government's legal affairs office, resulting in the alleged theft of 313 gigabytes of sensitive data. On November 15, 2024, RansomHub publicly listed the breach on its dark web data leak platform, claiming to have exfiltrated a substantial number of documents that included government contracts, financial records, and insurance data. The group included samples of the stolen data on its data breach site, which appeared to be a part of a government employee database that contained personal information. RansomHub stated it would publicly release the information if the Mexican government did not comply with its demands to pay an undisclosed sum of money within 10 days.

Mexican government officials suggested the sample data RansomHub published was potentially downloaded using a former employee's password and claimed to be reporting the attack.⁶ ZeroFox did not locate any public information regarding whether the Mexican government paid the ransom or the RansomHub group released the compromised information in accordance with its ultimatum.

⁶

[hXXps://apnews\[.\]com/article/mexico-president-hacking-attack-ransomhub-ransomware-a97fa044850ba05f574f71d2af3d67c8](https://apnews.com/article/mexico-president-hacking-attack-ransomhub-ransomware-a97fa044850ba05f574f71d2af3d67c8)

Italy: On November 9, 2024, RansomHub claimed responsibility for a ransomware attack that targeted the Bologna Football Club (FC) 1909. RansomHub alleged it had stolen data that consisted of sponsorship contracts and sponsor details, complete historical financial data of the FC, personal and confidential player data, medical records, commercial and strategic business plans, and data on young athletes. RansomHub stated it would publicly release the stolen data if Bologna FC did not comply with its ransom demands within two days.⁷ ZeroFox did not identify information to indicate whether RansomHub released the information or if Bologna FC complied with the demands.

Netherlands: In early September 2024, RansomHub launched a ransomware attack against Kawasaki Motors Europe (KME), claiming to have stolen 487 gigabytes of sensitive data. On September 5, 2024, the group listed Kawasaki on its dark web extortion site, demanding payment to prevent data leakage. KME opted to not engage with the ransom demands and instead attempted to isolate affected systems and mitigate the attack, but RansomHub released the stolen data on September 16, 2024. The leaked information reportedly contained business documents, financial records, and internal communications, posing significant security and reputational risks for the company.⁸⁹

United States: Intermountain Planned Parenthood of Montana, operating as Planned Parenthood of Montana (PPMT), identified a security breach within its computer network on August 28, 2024. On September 4, 2024, RansomHub published screenshot samples of administrative, financial, and legal documents to its data leak site as a method of legitimizing the claim it had exfiltrated 93 GBs of data from PPMT.¹⁰ RansomHub gave PPMT an ultimatum to respond within seven days to prevent full release of the compromised data.

7

[hXXps://www.bleepingcomputer\[.\]com/news/security/bologna-fc-confirms-data-breach-after-ransomhub-ransomware-attack/](https://www.bleepingcomputer.com/news/security/bologna-fc-confirms-data-breach-after-ransomhub-ransomware-attack/)

⁸ [hXXps://hackread\[.\]com/ransomhub-ransomware-group-kawasaki-europe-data-leak/](https://hackread.com/ransomhub-ransomware-group-kawasaki-europe-data-leak/)

9

[hXXps://www.bleepingcomputer\[.\]com/news/security/ransomhub-claims-kawasaki-cyberattack-threatens-to-leak-stolen-data/](https://www.bleepingcomputer.com/news/security/ransomhub-claims-kawasaki-cyberattack-threatens-to-leak-stolen-data/)

¹⁰ [hXXps://hackread\[.\]com/ransomhub-planned-parenthood-hack-steals-data/](https://hackread.com/ransomhub-planned-parenthood-hack-steals-data/)

On September 6, 2024, PPMT confirmed RansomHub gained unauthorized access to the network and had exfiltrated documents containing the personal health information of 18,003 patients. Specifically, the compromised documents contained “names, addresses, dates of birth, medical record numbers, health insurance information, clinical information, provider names(s), dates(s) of service, diagnosis of service, diagnosis information, treatment information, and prescription information.”¹¹ PPMT responded to the incident by implementing security measures and notifying patients of the data breach. ZeroFox did not locate any publicly available information regarding whether PPMT responded to RansomHub’s demands.

¹¹ <https://www.hipaajournal.com/planned-parenthood-ransomware-2024/>

Appendix A: Common Vulnerabilities and Exposures (CVEs)

Known CVEs Exploited by RansomHub Ransomware¹²

Note: This list should not be treated as exhaustive.

CVE ID	Vulnerability	Description
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection Vulnerability	An improper neutralization of special elements used in an SQL command (SQL injection) in Fortinet FortiClientEMS versions 7.2.0 through 7.2.2 and FortiClientEMS versions 7.0.1 through 7.0.10 allow attackers to execute unauthorized code or commands via specially crafted packets.
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to a BIG-IP system to execute arbitrary system commands. Note: Software versions which have reached the End of Technical Support (EoTS) are not evaluated.
CVE-2023-46604	Apache Active MQ Deserialization of Untrusted Data Vulnerability	The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath. Users are recommended to upgrade both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3, which fixes this issue.

¹² Vulnerability names and descriptions taken from the CVE Program, the NIST National Vulnerability Database, and CISA's KEV Catalog, when available.

CVE-2023-27997	Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability	A heap-based buffer overflow vulnerability [CWE-122] in FortiOS (version 7.2.4 and below, version 7.0.11 and below, version 6.4.12 and below, and version 6.0.16 and below) and FortiProxy (version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below, all 1.2 versions, and all 1.1 versions) SSL-VPNs may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.
CVE-2023-22515	Atlassian Confluence Data Center and Server Broken Access Control Vulnerability	Atlassian has been made aware of an issue reported by a handful of customers where external attackers may have exploited a previously unknown vulnerability in publicly accessible Confluence Data Center and Server instances to create unauthorized Confluence administrator accounts and access Confluence instances. Atlassian Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian[.]net domain, it is hosted by Atlassian and is not vulnerable to this issue.
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Unauthenticated remote code execution.
CVE-2023-0144	Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)	The Event Manager and Tickets Selling Plugin for WooCommerce WordPress plugin before 3.8.0 does not validate and escape some of its post meta before outputting them back in a page/post, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
CVE-2020-1472	ZeroLogon - Microsoft Netlogon Privilege Escalation Vulnerability	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a

		domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network. To exploit the vulnerability, an unauthenticated attacker would be required to use MS-NRPC to connect to a domain controller to obtain domain administrator access. Microsoft is addressing the vulnerability in a phased two-part rollout. These updates address the vulnerability by modifying how Netlogon handles the usage of Netlogon secure channels. For guidelines on how to manage the changes required for this vulnerability and more information on the phased rollout, see "How to manage the changes in Netlogon secure channel connections" associated with CVE-2020-1472 (updated September 28, 2020). When the second phase of Windows updates become available in Q1 2021, customers will be notified via a revision to this security vulnerability. If you wish to be notified when these updates are released, we recommend that you register for the security notifications mailer to be alerted of content changes to this advisory. See Microsoft Technical Security Notifications.
--	--	--

Appendix B: MITRE Codes

T-Code	Description
T1059.001	Command and Scripting Interpreter: PowerShell
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1486	Data Encrypted for Impact
T1083	File and Directory Discovery
T1222.002	File and Directory Permissions Modification: Linux and Mac
T1222.001	File and Directory Permissions Modification: Windows
T1490	Inhibit System Recovery
T1027.001	Obfuscated Files or Information: Binary Padding
T1018	Remote System Discovery
T1082	System Information Discovery
T1007	System Service Discovery
T1204.002	User Execution: Malicious File
T1497.001	System Checks
T1047	Windows Management Instrumentation
T1498	Network Denial-of-Service
T1566	Phishing
T1566.004	Phishing: Spearphishing Voice
T1566.003	Phishing: Spearphishing via Service
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1140	Deobfuscate/Decode Files or Information
T1056.001	Input Capture: Keylogging
T1033	System Owner/User Discovery
T1570	Lateral Tool Transfer
T1070.001	Indicator Removal: Clear Windows Event Logs
T1562	Impair Defenses: Disable or Modify Tools

T1489	Service Stop
T1190	Exploit Public-Facing Applications
T1110.003	Brute Force: Password Spraying
T1588.005	Obtain Capabilities: Exploits
T1078	Compromised Credentials
T1547.001	Registry Run Keys/Startup Folder
T1053.005	Scheduled Tasks
T1003	OS Credential Dumping
T1068	Exploitation for Privilege Escalation
T1562.001	Impair Defenses: Disable or Modify Tools
T1480.001	Execution Guardrails: Environmental Keying
T1003.001	OS Credential Dumping: LSASS Memory
T1056.001	Input Capture: Keylogging
T1046	Network Service Discovery
T1083	File and Directory Discovery
T1021.001	Remote Desktop Protocol
T1021.002	Remote Services: SMB/Windows Admin Shares
T1490	Inhibit System Recovery
T1491.001	Internal Defacement
T1567.002	Exfiltration to Cloud Storage
T1659	Content Injection

| Appendix C: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix D: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%