



# RANSOMHUB

## THREAT ACTOR

## PROFILE

AUG 22ND, 2025

**TLP:GREEN** Free version

Stay updated: subscribe to our intelligence feeds for real-time updates on APT activity and emerging cyber threats. Reach out to our team at [commercial@malwarepatrol.net](mailto:commercial@malwarepatrol.net) or visit our website: <https://malwarepatrol.net/>

### STATUS

Very Active

### ATTRIBUTION AND ASSOCIATIONS

- **Links to Knight Ransomware:** RansomHub is directly linked to the Knight ransomware family, with evidence suggesting the repurposing of Knight's source code.
- **Recruitment from ALPHV and LockBit:** Recruitment of affiliates from prominent ransomware groups suggests a connection and potential overlap in infrastructure or personnel.
- **Suspected Origin:** No information available.

### OPERATIONAL MODEL

- **Ransomware-as-a-Service (RaaS):** RansomHub operates on a RaaS model, allowing affiliates to deploy its ransomware in exchange for a percentage of the ransom payment.
- **Affiliates:** Actively recruits affiliates from other ransomware groups, including ALPHV and LockBit, to expand its reach and attack capabilities.
- **Collaborations:** No information available on specific collaborations with other threat actors beyond affiliate recruitment.



RansomHub is a cyber threat actor specializing in ransomware attacks, operating as a Ransomware-as-a-Service (RaaS) model. It emerged in February 2024 and has rapidly become one of the largest currently operating, known for its aggressive tactics and links to other ransomware variants.



### HISTORICAL CONTEXT

- **February 2024:** RansomHub emerges as a new RaaS platform, quickly gaining traction and becoming one of the largest ransomware groups. The group begins listing victims.
- **Mid-February 2024:** The group lists its first victims.
- **February - June 2024:** RansomHub rapidly accumulates victims and demonstrates strategic acumen through recruitment from groups like ALPHV and LockBit.
- **2024-06-18:** CYFIRMA releases a report detailing RansomHub's tactics and techniques, including its connection to the Knight ransomware source code.
- **Recent Activity:** Ongoing - RansomHub continues to be prolific, consistently adding new victims to its leak site.



### TECHNICAL PROFILE

#### Malware and Tools

- **RansomHub Ransomware:** Written primarily in Go, utilizing Gobfuscate for obfuscation, although early versions sometimes lacked this obfuscation. It appends random characters to filenames during encryption. Ransom notes are in a file named README\_[random\_string].txt.
- **Knight Ransomware (Precursor):** Source code was initially sold and then repurposed into RansomHub. Similar code base and functionalities.
- **Dual-Use Tools:** Atera, Splashtop, and NetScan are employed for remote access and network discovery.
- **IIS Services Halting:** iisreset.exe and iisrstas.exe are used to halt Internet Information Services (IIS) services.

#### Infrastructure

- **Tor Network:** RansomHub utilizes the Tor network for hosting its leak site, communication, and facilitating ransom payment instructions.
- **Online Infrastructure:** General use of online infrastructure for command and control and data dissemination.

#### Tactics, Techniques, and Procedures (TTPs)

- **Command and Scripting Interpreter (T1059):** Utilizing command-line tools for various operations.
- **Hijack Execution Flow: DLL Side-Loading (T1574.002):** Employed for persistence and defense evasion.
- **Privilege Escalation (T1574.002):** Utilizing DLL side-loading techniques.
- **Defense Evasion (T1574.002):** Utilizing DLL side-loading techniques.
- **System Information Discovery (T1082):** Gathering information about targeted systems.
- **Software Discovery: Security Software Discovery (T1518.001):** Identifying and potentially disabling security software.
- **Application Layer Protocol (T1071):** Used for command and control communication.
- **Non-Application Layer Protocol (T1095):** Also used for command and control communication.
- **Data Encrypted for Impact (T1486):** Employing double extortion tactics.

## RECENT DEVELOPMENTS

- **June 2024:** CYFIRMA releases a report detailing RansomHub's tactics and techniques and its connection to Knight ransomware.
- **Ongoing Affiliate Recruitment:** RansomHub continues to actively recruit affiliates from other ransomware operations.
- **Prolific Attacks:** RansomHub remains consistently active, regularly adding victims to its leak site.

## INTELLIGENCE GAPS

- **Origin and Attribution:** The origin and specific actors behind RansomHub remain unknown.
- **Affiliate Structure:** A detailed understanding of the affiliate structure and their individual capabilities is lacking.
- **Long-Term Strategy:** The long-term strategic goals of RansomHub and its potential evolution remain unclear.

## KNOWN ALIASES

No information available.



## TARGETING AND VICTIMS

- **Targeted Industries:** Accounting, Business Services, Construction, E-commerce, Education, Energy, Finance, FMCG, Government, Healthcare, Manufacturing, Media, Real Estate, Retail, Software, Telecommunications, and Transportation.
- **Targeted Technologies:** MS Windows.
- **Geographic Distribution:** Australia, Brazil, Canada, Colombia, Egypt, El Salvador, France, Honduras, Indonesia, Italy, Japan, Libya, Norway, Romania, Slovakia, South Africa, Spain, Sri Lanka, Sweden, UAE, United Kingdom, United States, and Vietnam.
- **Shifts in Targeting:** While initially broad, RansomHub appears to be targeting economically rich nations.



## DEFENSE AND MITIGATION GUIDANCE

- **Network Segmentation:** Limit the impact of a breach by isolating critical systems and data.
- **Regular Backups:** Ensure data can be restored in case of encryption.
- **Endpoint Detection and Response (EDR):** Implement EDR solutions to detect and respond to malicious activity.
- **Application Control:** Restrict the execution of unauthorized applications.
- **Patch Management:** Maintain up-to-date security patches to address vulnerabilities.
- **TTPs:** Employ techniques to mitigate Command and Scripting Interpreter (T1059), Hijack Execution Flow: DLL Side-Loading (T1574.002), Privilege Escalation (T1574.002), Defense Evasion (T1574.002), System Information Discovery (T1082).



## DETECTION GUIDANCE

- **Monitor Tor Network Traffic:** Identify connections to known RansomHub leak sites.
- **Analyze Command-Line Activity:** Detect the use of iisreset.exe and iisrstas.exe.
- **Endpoint Monitoring:** Detect unusual file modifications and encryption activity.
- **Network Traffic Analysis:** Identify patterns associated with data exfiltration.
- **TTPs:** Monitor Command and Scripting Interpreter (T1059), Hijack Execution Flow: DLL Side-Loading (T1574.002), Privilege Escalation (T1574.002), Defense Evasion (T1574.002), System Information Discovery (T1082).

**IOCS - INDICATORS OF COMPROMISE**

FULL LIST OF IOCS AVAILABLE TO  
MALWARE PATROL CUSTOMERS ONLY

**IOCS - INDICATORS OF COMPROMISE**

FULL LIST OF IOCS AVAILABLE TO  
MALWARE PATROL CUSTOMERS ONLY



**IOCS - INDICATORS OF COMPROMISE**

FULL LIST OF IOCS AVAILABLE TO  
MALWARE PATROL CUSTOMERS ONLY





## IOCS - INDICATORS OF COMPROMISE

IOCS 001	...
IOCS 002	...
IOCS 003	...
IOCS 004	...
IOCS 005	...
IOCS 006	...
IOCS 007	...
IOCS 008	...
IOCS 009	...
IOCS 010	...
IOCS 011	...
IOCS 012	...
IOCS 013	...
IOCS 014	...
IOCS 015	...
IOCS 016	...
IOCS 017	...
IOCS 018	...
IOCS 019	...
IOCS 020	...
IOCS 021	...
IOCS 022	...
IOCS 023	...
IOCS 024	...
IOCS 025	...
IOCS 026	...
IOCS 027	...
IOCS 028	...
IOCS 029	...
IOCS 030	...
IOCS 031	...
IOCS 032	...
IOCS 033	...
IOCS 034	...
IOCS 035	...
IOCS 036	...
IOCS 037	...
IOCS 038	...
IOCS 039	...
IOCS 040	...
IOCS 041	...
IOCS 042	...
IOCS 043	...
IOCS 044	...
IOCS 045	...
IOCS 046	...
IOCS 047	...
IOCS 048	...
IOCS 049	...
IOCS 050	...

**FULL LIST OF IOCS AVAILABLE TO  
MALWARE PATROL CUSTOMERS ONLY**

**IOCS - INDICATORS OF COMPROMISE**

IOCS 001	...
IOCS 002	...
IOCS 003	...
IOCS 004	...
IOCS 005	...
IOCS 006	...
IOCS 007	...
IOCS 008	...
IOCS 009	...
IOCS 010	...
IOCS 011	...
IOCS 012	...
IOCS 013	...
IOCS 014	...
IOCS 015	...
IOCS 016	...
IOCS 017	...
IOCS 018	...
IOCS 019	...
IOCS 020	...
IOCS 021	...
IOCS 022	...
IOCS 023	...
IOCS 024	...
IOCS 025	...
IOCS 026	...
IOCS 027	...
IOCS 028	...
IOCS 029	...
IOCS 030	...
IOCS 031	...
IOCS 032	...
IOCS 033	...
IOCS 034	...
IOCS 035	...
IOCS 036	...
IOCS 037	...
IOCS 038	...
IOCS 039	...
IOCS 040	...
IOCS 041	...
IOCS 042	...
IOCS 043	...
IOCS 044	...
IOCS 045	...
IOCS 046	...
IOCS 047	...
IOCS 048	...
IOCS 049	...
IOCS 050	...

**FULL LIST OF IOCS AVAILABLE TO  
MALWARE PATROL CUSTOMERS ONLY**





 [MALWAREPATROL.NET](https://malwarepatrol.net)

 +1 813 321 0987