blackpoint

THREAT PROFILE:

Hunters International Ransomware

TABLE OF CONTENTS

Executive Summary

First Identified:
2023

Operation style:
Hunters International operated as a ransomware-as-a-service (RaaS) until late 2024 when the group announced they would operate as an extortion-only group.

Extortion method:
Double extortion until late 2024 when the group announced a switch to extortion-only attacks.

Most frequently targeted industry:
- Industrials (Manufacturing)

Most frequently targeted victim HQ region:
- North America

Known Associations:
- Black Nevas Ransomware
- Gold Crescent
- Hive Ransomware
- Shift Scorpius
- Storm-0501
- Water Ouroboros
- WorldLeaks

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

Valid accounts, exploit external remote services, drive by compromise, exploit public-facing application, social engineering (MITRE ATT&CK: T1078, T1133, T1189, T1190, T1566)

Create or modify system process, boot or logon autostart execution (MITRE ATT&CK: T1543, T1547)

Remote services, lateral tool transfer (MITRE ATT&CK: T1021, T1570)

Description

Hunters International ransomware was first reported in October 2023 and operated in the double extortion method, where victim data is stolen and leaked via a data leak site if the ransom demand is not paid; however, the group reportedly dropped the encryption portion of their operation.

In November 2024, the Hunters International operators released an internal note to their partners that appeared to be a farewell letter. The statement indicated that the ransomware business has become too risky and unprofitable due to government attention and interruptions caused by ongoing geopolitics. However, a few weeks later, the administrator posted another notice that the group would be returning, and the group is still active as of March 2025.

Researchers report that Hunters International and Hive ransomware have multiple code overlaps and similarities, with at least a 60% match between two sets of code. Additionally, researchers have reported that affiliates and operators refer to Hunters International as хайв (Hive in Russian) and they have claimed that they were contacted by the Hunters International administrator using the same instant messaging account associated with Hive. However, Hunters International operators have claimed via their data leak site that they purchased the code and are not a rebrand.

For encryption, Hunters International embedded the encryption key within the encrypted files using ChaCha20-poly1305 and RSA OAEP combination. Hunters International does not always encrypt a victims' environment; sometimes opting for exfiltration and extortion instead. It is not known what factors contributed to the decision to encrypt or not to encrypt.

Hunters International and Hive ransomware are likely related, with at least 60% overlap in code.

Hunters International is written in Rust and targets both Windows and Linux environments for data encryption and exfiltration. The variant added a ".LOCKED" or ".lock" extension to the encrypted files on a victim machine, when encryption was used. Once the threat actors gain initial access, they attempt to kill processes and services. It then executes commands to delete backups and disable recovery mechanisms. It then reiterates through local and mapped drives, as well as shared drives found on the local network through the NetServerEnum and NetShareEnum APIs, encrypting files that are discovered.

In late 2024, Hunters International released a statement via their affiliate panel that no more ransom notes would be dropped, and the file extensions would no longer be changed. The group provided the reasoning that it is more likely to get a ransom payment if the people notified are the CEO and key staff members rather than dropping ransom notes everywhere - indicating the belief that the more people know, the less likely a ransom payment will be made.

In February 2024, security researchers identified that the domain "huntersinternational[.]org" was a legitimate active domain from 2017 to 2021 but then it was deactivated. The threat actors then reactivated the domain in January 2024 to launch the data leak site. The Hunters International group used a fake identity "Mihail Kolesnikov" to register the domain. This same name has been previously observed with Rilide Infostealer and Snatch ransomware phishing domains.

Description

In March 2024. a Hunters International administrator revealed a service for affiliates for 10% of the ransom payment. The service offered is an in-depth OSINT analysis on the targeted company, including all “managers, responsible persons, and their close relatives.”

In 2024, security researchers with Quorum Cyber reported a Hunters International custom backdoor, SharpRhino. SharpRhino reportedly has a valid code certificate and was masquerading as the legitimate tool, AngryIP. SharpRhino is an NSIS (Nullsoft Scriptable Installer System) packed executable.

Unlike other ransomware variants, Hunters International does not store stolen data on their infrastructure. The group reportedly maintains a tool, Software Storage, that sends information about files to the Hunters International server. Once a victim pays the ransom, they are reportedly given access to the disclosures configured by the affiliate where they can download and delete the data via an integrated file manager.

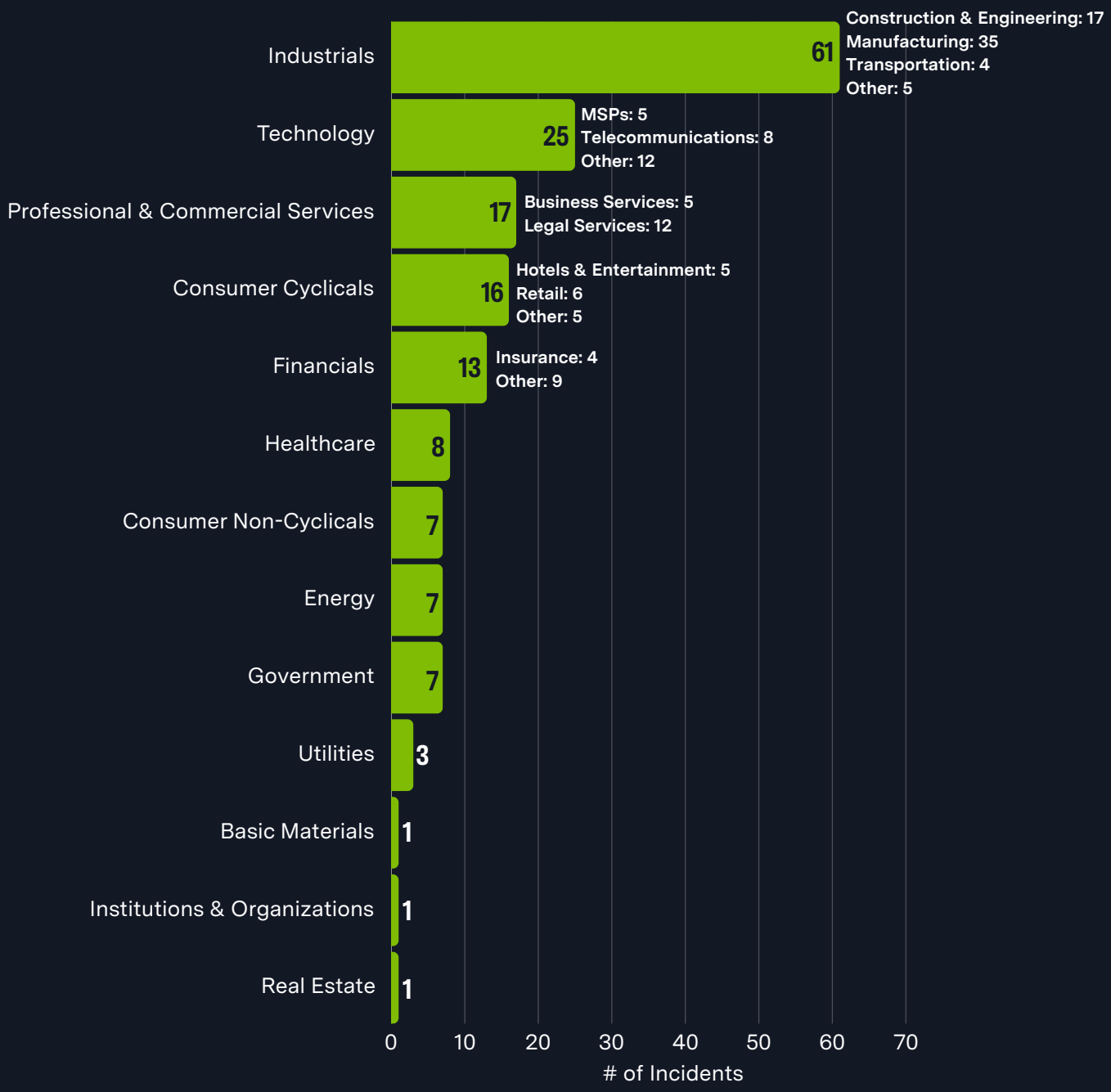
Hunters International has reportedly rebranded to “WorldLeaks”, with a focus on data exfiltration.

While the group has remained active, the operators released a project titled “WorldLeaks” in January 2025 but took it down after identifying vulnerabilities in the infrastructure. Rather than operate in the double extortion method, the operation reportedly shifted to extortion-only attacks by using the Storage Software tool.

The data leak site for WorldLeaks is reportedly set to launch later this year; however, in the meantime, the Hunters International site has remained accessible.

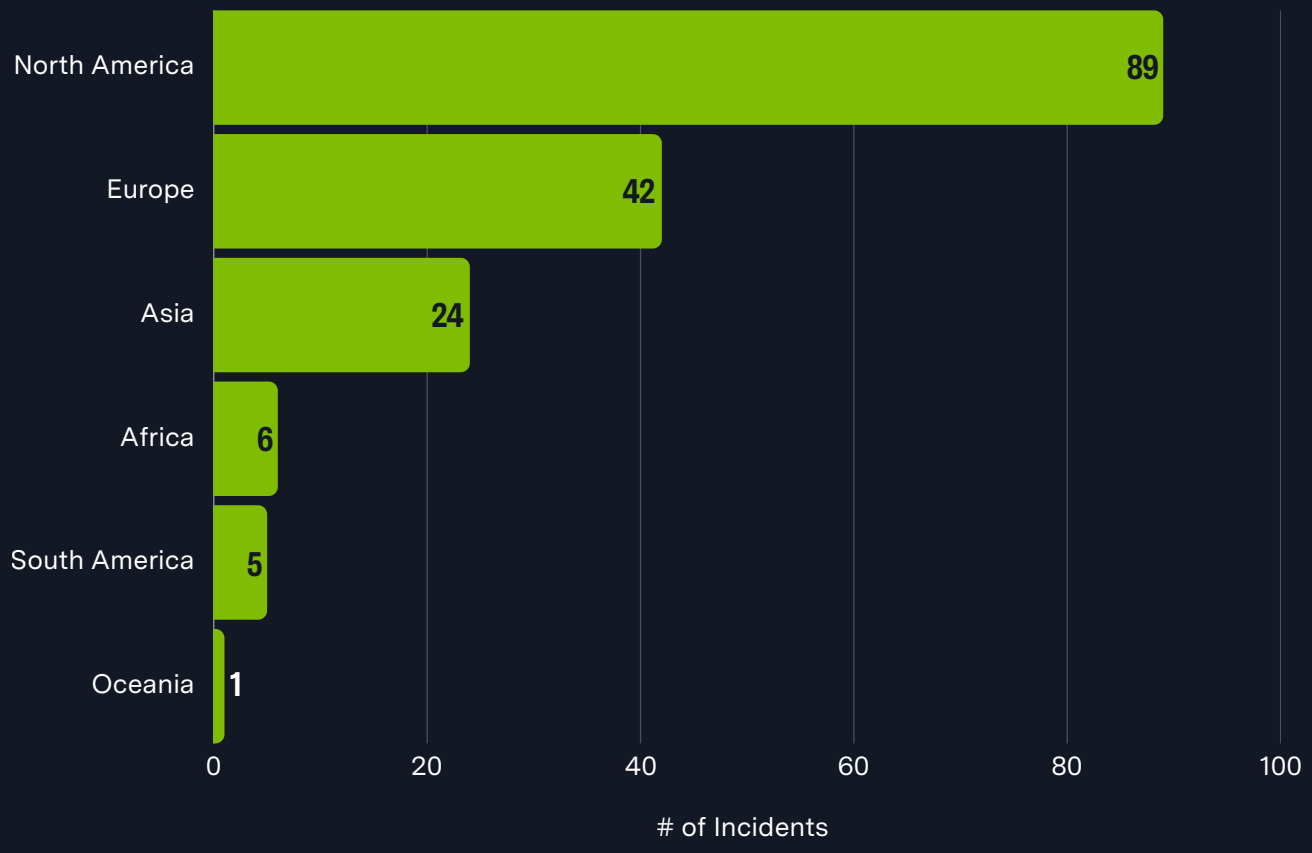
Previous Targets

Previous Industry Targets from 01 Jul 2024 to 30 Jun 2025

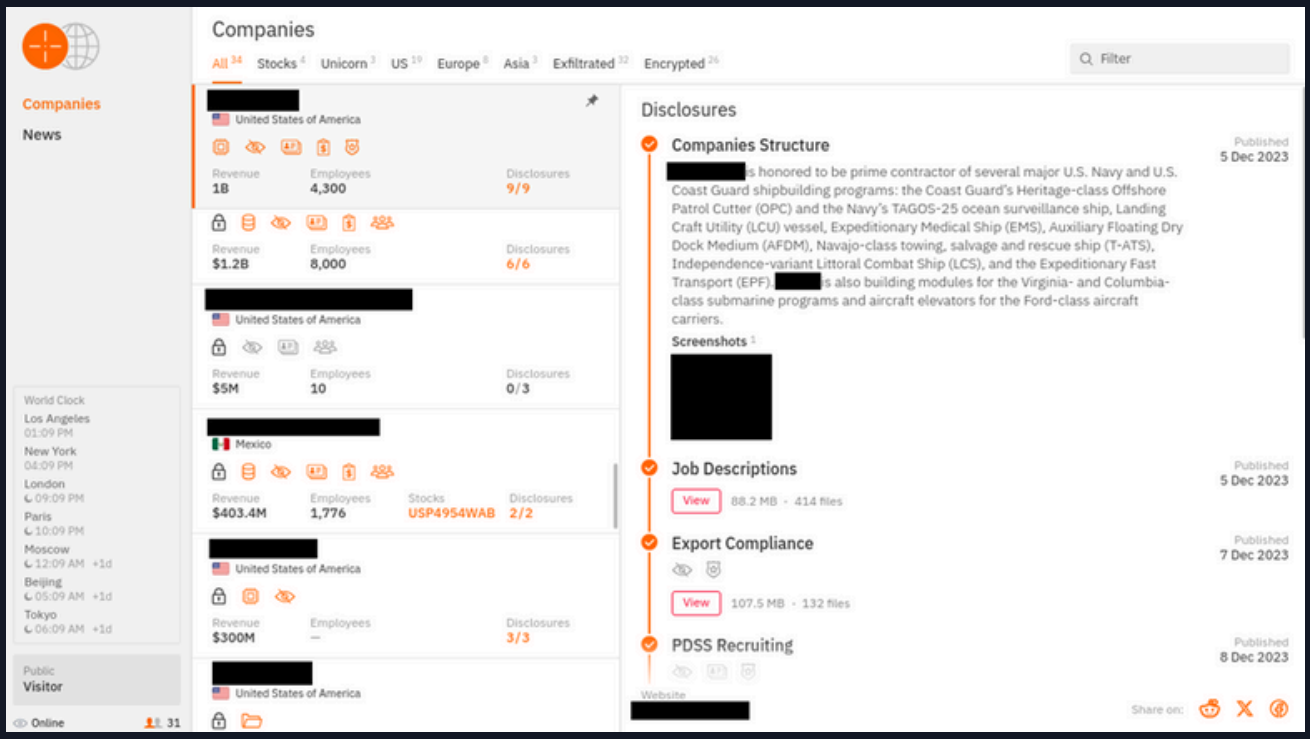


Previous Targets

Previous Victim HQ Regions from 01 Jul 2024 to 30 Jun 2025



Data Leak Site



hxxps://hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid[.]onion/
hxxps://hunters55atbdusuladzv7vzv6a423bkh6ksl2uftwrxyuarbzlfh7yd[.]onion/
hxxps://hunters33dootzzwybhxyh6xnmumopeoza6u4hkontdqu7awnhmix7ad[.]onion/
hxxps://hunters33mmcwww7ek7q5ndahul6nmzmrsumfs6aenicbqon6mxfiqyd[.]onion/

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CVE-2017-10271	RCE Vulnerability	Oracle WebLogic Server	9.8
CVE-2019-2725	Deserialization Vulnerability	Oracle WebLogic Server	9.8
CVE-2019-2729	Deserialization Vulnerability	Oracle WebLogic Server	9.8
CVE-2024-55591	Authentication Bypass Vulnerability	Fortinet FortiOS	9.8

Associations

Black Nevas Ransomware

Black Nevas is a ransomware operation that has been active since at least November 2024 and has reportedly claimed via their Telegram channel that they partner with multiple ransomware operations, including Hunters International.

Gold Crescent

A financially-motivated threat group purportedly behind the Hunters International operation.

Hive Ransomware

Hunters International and Hive ransomware reportedly have multiple code overlaps and similarities, with at least a 60% match between two sets of code. Additionally, researchers have reported that affiliates and operators refer to Hunters International as хайв (Hive in Russian) and they have claimed that they were contacted by the Hunters International administrator using the same instant messaging account associated with Hive. However, Hunters International operators have claimed via their data leak site that they purchased the code and are not a rebrand.

Shifty Scorpius

Hunters International alias named by Palo Alto Unit 42.

Storm-0501

A ransomware affiliate that has been attributed to multiple RaaS operations, including Hunters International.

Water Ouroboros

Hunters International alias named by Trend Micro.

WorldLeaks

Hunters International reportedly rebranded in 2025 to “WorldLeaks” after announcing the group would stop encrypting data and focus on exfiltration and extortion.

Known Tools

7zip	A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration.
AdFind	A free command-line query tool that can be used for gathering information from Active Directory.
Advanced IP Scanner	A fast and powerful network scanner with a user-friendly interface. It can locate all computers on your wired or wireless local network and scan their ports.
Advanced Port Scanner	A free network scanner allowing you to quickly find open ports on network computers and retrieve versions of programs running on the detected ports.
AnyDesk	An online file storage provider that allows users to store and share files anonymously.
bcdedit	A command line tool for managing Configuration Data; it can be used to create new stores, modify existing stores, and add boot menu options.
NirSoft	A collection of tools that include password recovery utilities, network monitoring tools, command-line utilities, and more.
PassView	A password recovery tool that reveals the passwords and other account details from Outlook Express and Microsoft Outlook 2000 (POP3 and SMTP Accounts Only).
PC Hunter	A toolkit for Windows with various powerful features for kernel structure viewing and manipulating.
Process Hacker	An open-source tool that allows users to see what processes are running on a device and identify network connections that are associated with a process.
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

SharpRhino	AKA Parcel RAT, ThunderShell, SMOKEDHAM. A RAT malware that has been observed in Hunters International ransomware attacks. The malware makes use of the C# programming language, is delivered through a typosquatting domain impersonating the legitimate tool, Angry IP Scanner.
Storage Software	A tool, compatible with both Windows and Linux, that allows users to share access to exfiltrated data, categorize documents, and make disclosures through the Hunters International website without a need to upload the data anywhere. This tool only sends information about the files, not the files themselves, to the group's system to be presented to the victims and disclose it on the data leak site.
VssAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes.
wbadmin	A command line utility that is used to back up and restore OS, drive volumes, files, folders, and applications from a command line interface.
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.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.

Observed Behaviors: Windows

Tactic	Commands Observed
Execution	-c -a / -attach / --attach -A / -no-aggressive / --no-aggressive -E / -no-extension / --no-extension -m / -min-size / --min-size
Defense Evasion	“C:\Windows\System32\wbem\WMIC.exe” shadowcopy delete “C:\Windows\System32\vssadmin.exe” delete shadows /all /quiet “C:\Windows\System32\wbadmin.exe” delete catalog-quiet “C:\Windows\System32\wbadmin.exe” delete systemstatebackup -keepVersions:3 “C:\Windows\System32\wbadmin.exe” delete systemstatebackup TerminateProcess ControlService
Discovery	NetServerEnum NetShareEnum EnumServicesStatusW CreateToolhelp32Snapshot
Impact	“C:\Windows\System32\bcdedit.exe” /set {default} recoveryenabled No “C:\Windows\System32\bcdedit.exe” /set {default} bootstatuspolicy ignoreallfailures

Observed Behaviors: Linux

Tactic	Commands Observed
Execution	-w, --wait: Number of seconds to sleep before execution -S, --no-stop: Do not stop running VMs -E, --no-erase: Do not erase free disk space

MITRE ATT&CK® Mappings

Reconnaissance	
T1595: Active Scanning	.002: Vulnerability Scanning
Initial Access	
T1078: Valid Accounts	
T1133: External Remote Services	
T1189: Drive-by Compromise	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment
Execution	
T1047: Windows Management Instrumentation	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1106: Native API	
T1129: Shared Modules	
T1204: User Execution	.002: Malicious File
Persistence	
T1543: Create or Modify System Process	.003: Windows Service
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder

MITRE ATT&CK® Mappings

Privilege Escalation	
T1078: Valid Accounts	.002: Domain Accounts
T1134: Access Token Manipulation	
T1543: Create or Modify System Process	.003: Windows Service
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder
Defense Evasion	
T1027: Obfuscated Files or Information	.002: Software Packing .004: Compile After Delivery .008: Stripped Payloads
T1036: Masquerading	.001: Invalid Code Signature
T1480: Execution Guardrails	
T1497: Virtualization/Sandbox Evasion	.003: Time Based Evasion
T1562: Impair Defenses	.001: Disable or Modify Tools
T1622: Debugger Evasion	
Credential Access	
T1003: OS Credential Dumping	.002: Security Account Manager
Discovery	
T1018: Remote System Discovery	

MITRE ATT&CK® Mappings

Discovery	
T1057: Process Discovery	
T1069: Permission Groups Discovery	.002: Domain Groups
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	
T1135: Network Share Discovery	
T1497: Virtualization/Sandbox Evasion	.001: System Checks
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1090: Proxy	.003: Multi-hop Proxy
T1105: Ingress Tool Transfer	

MITRE ATT&CK® Mappings

Command and Control
T1573: Encrypted Channel
Exfiltration
T1020: Automated Exfiltration
T1041: Exfiltration Over C2 Channel
Impact
T1486: Data Encrypted for Impact
T1489: Service Stop
T1490: Inhibit System Recovery
T1657: Financial Theft

References

- Boulrice, Ryan (2023, November 14) Netizen: “The Evolution from Hive to Hunters International: Ransomware Gangs Leveraging Peer Innovations.” https://blog.netizen.net/2023/11/14/the-evolution-from-hive-to-hunters-international-ransomware-gangs-leveraging-peer-innovations/
- Broadcom (2024, January 09) “Protection Highlight: Hunters International Ransomware.” https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-hunters-international-ransomware
- Forret, Michael (2024, August 02) Quorum Cyber: “SharpRhino – New Hunters International RAT identified by Quorum Cyber.” https://www.quorumcyber.com/insights/sharprhino-new-hunters-international-rat-identified-by-quorum-cyber/
- Group-IB (2025, April 02) “The beginning of the end: the story of Hunters International.”
- HC3 (2024, April 05) “HC3’s Top 10 Most Active Ransomware Groups.” https://www.group-ib.com/blog/hunters-international-ransomware-group/ https://www.hhs.gov/sites/default/files/hc3-top-10-most-active-ransomware-groups-analyst-note-tlpclear-r.pdf
- Krishnan, Rakesh (2024, February 05) Netenrich: “Identity Behind Hunters International Ransomware Group’s Dedicated Leak Site Exposed.” https://netenrich.com/blog/hunters-international-group-dls-identity-exposure
- Quorum Cyber (2023, November) “Threat Intelligence Hunters International Ransomware.” https://www.quorumcyber.com/wp-content/uploads/2023/11/QC-Hunters-International-Ransomware-Report-TI.pdf
- SOCRadar (2024, February 20) “Dark Web Profile: Hunters International.” https://socradar.io/dark-web-profile-hunters-international/
- Swagler, Chris (2023, November 15) Speartip: “New Hunters International Ransomware Group Emerged as Possible Hive Rebrand.” https://www.speartip.com/new-hunters-international-ransomware-group-emerged/
- ThreatIntelReport (2023, November 22) “Threat Actor Profile: Hunters International Ransomware Group.” https://www.threatintelreport.com/2023/11/22/threat_actor_profiles/threat-actor-profile-hunters-international-ransomware-group/
- Trend Research (2025, March 05) “Ransomware Spotlight: Water Ouroboros.” https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-water-ouroboros
- Vectra (n.d.) “Hunters.” https://www.vectra.ai/threat-actors/hunters
- Zugec, Martin (2023, November 09) Bitdefender: “Hive Ransomware's Offspring: Hunters International Takes the Stage.” https://www.bitdefender.com/blog/businessinsights/hive-ransomwares-offspring-hunters-international-takes-the-stage/

Adversary Pursuit Group

blackpoint