blackpoint

THREAT PROFILE:

Hunters International Ransomware

Table of Contents

Executive Summary

First Identified:
2023

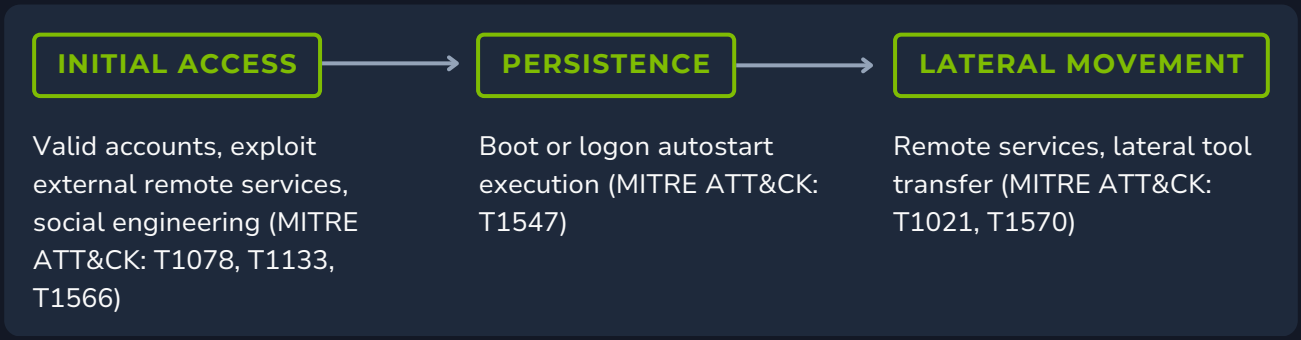
Operation style:
Ransomware-as-a-Service (RaaS), affiliate payment structure is unknown; however, it is likely similar to other RaaS operations – 80/20 split.

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:
- Industrials (Manufacturing)

Most frequently targeted victim HQ region:
- United States, North America

Known Associations:
- Hive Ransomware



Description

Hunters International ransomware was first reported in October 2023 and operates in the double extortion method, where victim data is stolen and leaked via a data leak site if the ransom demand is not paid. Hunters International is written in the Rust language. Researchers report that Hunters International and the former Hive ransomware operation are likely related – a possible rebranding – with at least a 60% overlap in code. However, the Hunters International operators have announced via their data leak site that they are not a rebrand of the Hive operation but rather purchased the code from the former group.

For encryption, Hunters International embeds 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 contribute to the decision to encrypt or not encrypt.

Hunters International targets both Windows and Linux environments for data encryption and exfiltration and adds a ".LOCKED" or ".lock" extension to the encrypted files on a victim machine, when encryption is 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.

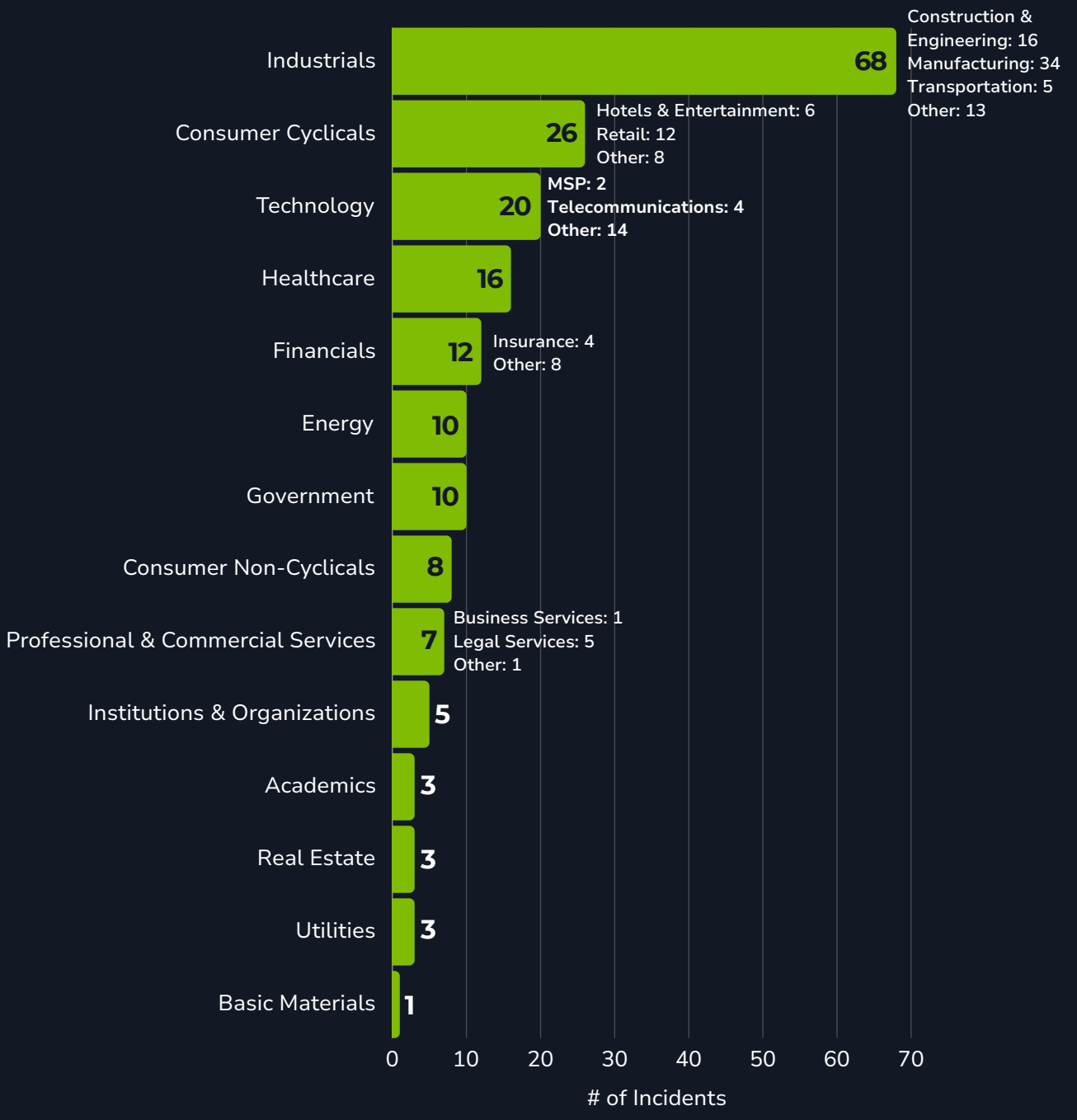
Hunters International and Hive ransomware are likely related, with at least 60% overlap in code.

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.

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.

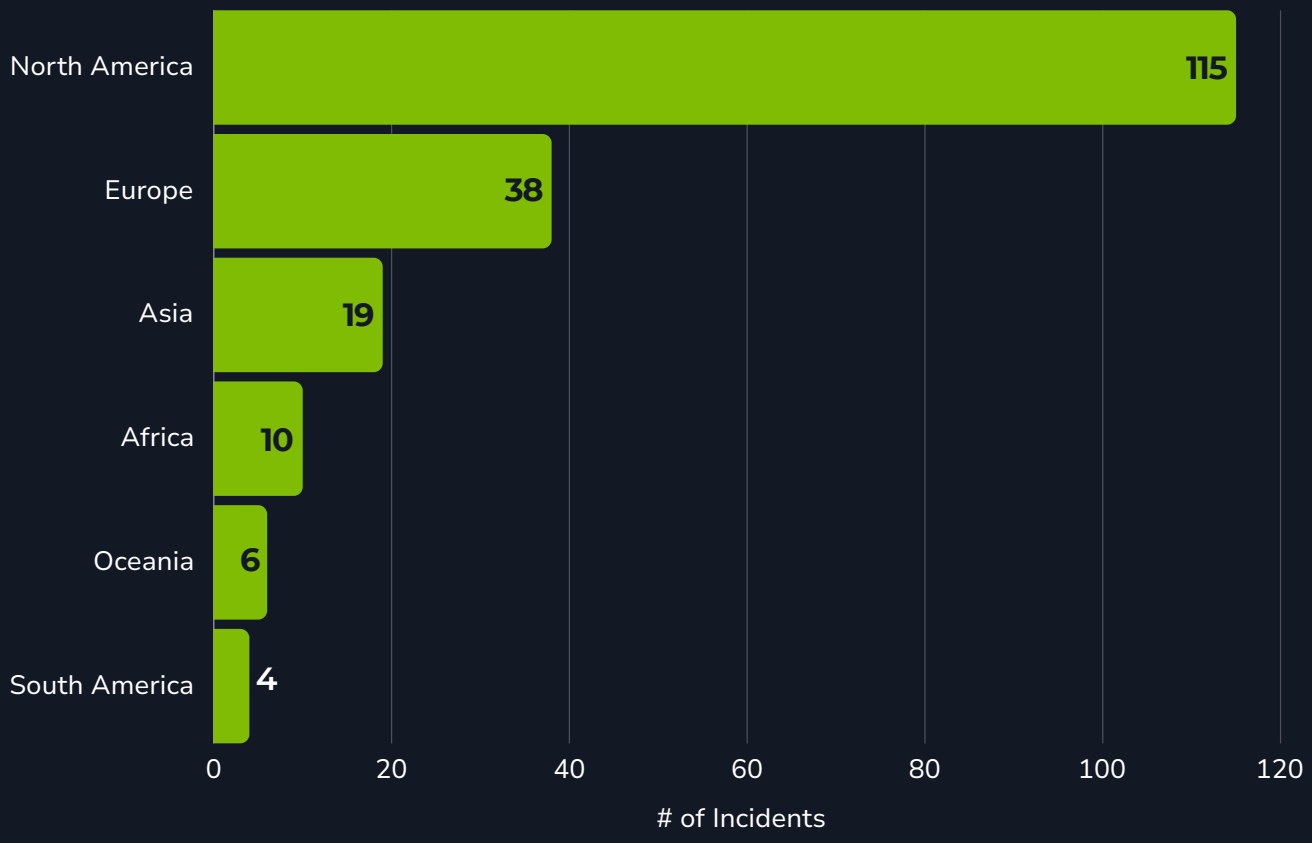
Previous Targets: Hunters International

Previous Industry Targets from 01 Oct 2023 to 30 Sep 2024

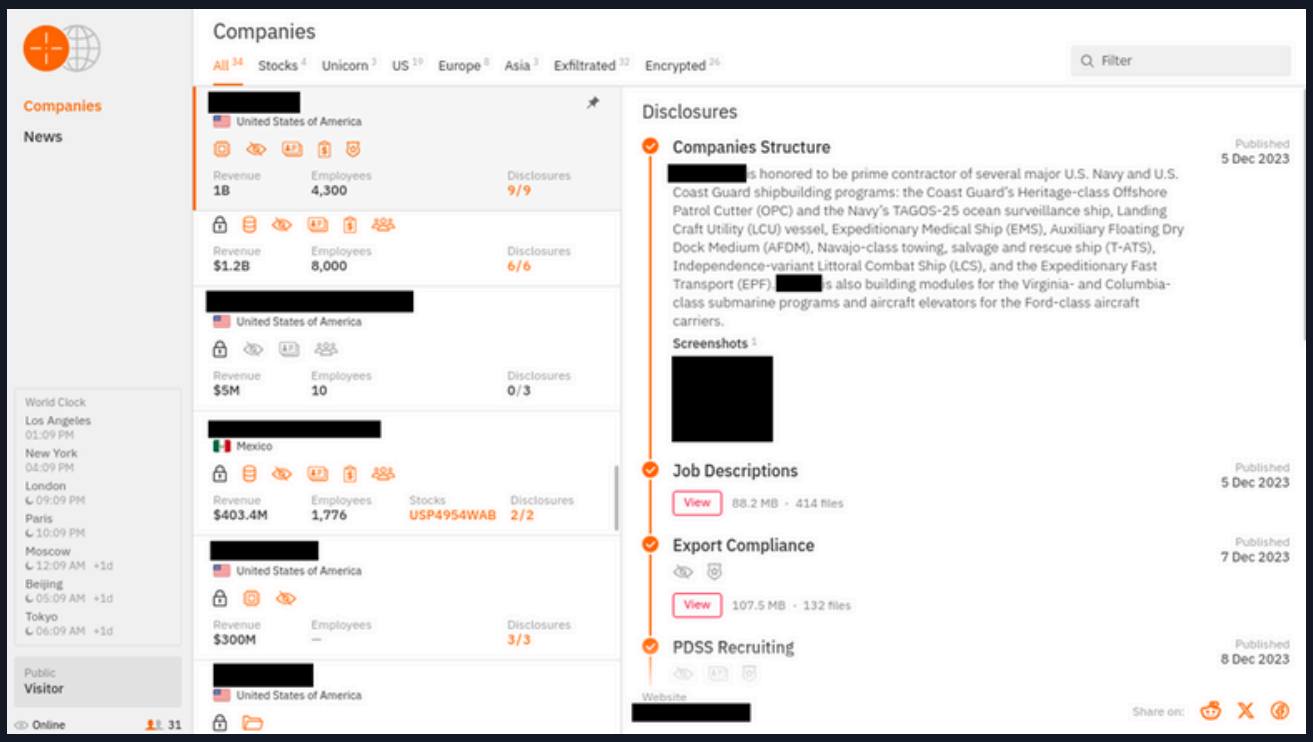


Previous Targets: Hunters International

Previous Victim HQ Regions from 01 Oct 2023 to 30 Sep 2024



Data Leak Site: Hunters International



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

Associations: Hunters International

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. However, Hunters International operators have claimed via their data leak site that they purchased the code and are not a rebrand.

Known Tools: Hunters International

7zip	A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration.
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.
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.
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.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.

Observed Windows Behaviors: Windows

Execution	-c -a / -attach / --attach -A / -no-aggressive / --no-aggressive -E / -no-extension / --no-extension -m / -min-size / --min-size
Defense Evasion	exe shadowcopy delete exe delete shadows /all /quiet exe delete catalog-quiet exe delete systemstatebackup -keepVersions:3 exe delete systemstatebackup
Discovery	NetServerEnum NetShareEnum
Impact	exe /set {default} recoveryenabled No exe /set {default} bootstatuspolicy ignoreallfailures

MITRE ATT&CK® Mappings: Hunters International

Initial Access	
T1078: Valid Accounts	
T1133: External Remote Services	
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	
Persistence	
T1543: Create or Modify System Process	.003: Windows Service
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder
Privilege Escalation	
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

MITRE ATT&CK® Mappings: Hunters International

Defense Evasion	
T1027: Obfuscated Files or Information	.002: Software Packing .004: Compile After Delivery
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	
Discovery	
T1057: Process Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1135: Network Share Discovery	
T1497: Virtualization/Sandbox Evasion	.001: System Checks
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol
T1570: Lateral Tool Transfer	

MITRE ATT&CK® Mappings: Hunters International

Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1573: Encrypted 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/
- 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/
- 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