datto

Hive Ransomware Group Threat Brief

Table of Contents

The Hive ransomware group has operated the Hive Ransomware-as-a-Service (RaaS) operation since at least June 2021.

Hive actors have been observed heavily targeting the US, with almost half of all victims published on Hive group's data leaks site, HiveLeaks, being US-based. Hive targets a range of industries, with manufacturing and health being the most targeted industries.

Hive's platform allows affiliates to perform all necessary actions from their web application to perform a ransomware attack end-to-end. This includes adding new victims, building ransomware kits on-demand, and checking payment status and cryptocurrency account balance. Hive's platform also consists of a "Sales Department" that is used for ransom negotiation between the victim and Hive actors.

Hive ransomware can encrypt Windows, Linux, FreeBSD, and ESXi systems. The binaries for all platforms are created each time an affiliate builds a new ransomware kit via Hive's platform. Although able to encrypt across various operating systems, victims have expressed issues with the decryption of virtual machines, with master boot records becoming corrupted and unrecoverable after decryption.

Motives

The Hive ransomware group is financially motivated and employs the double extortion method to maximize victim ransom payments. Double extortion is a popular tactic among ransomware gangs, where the attacker exfiltrates data from the victim network before encryption. The exfiltrated data is then threatened to be posted on Hive's public data leaks site if the ransom demand is not paid.

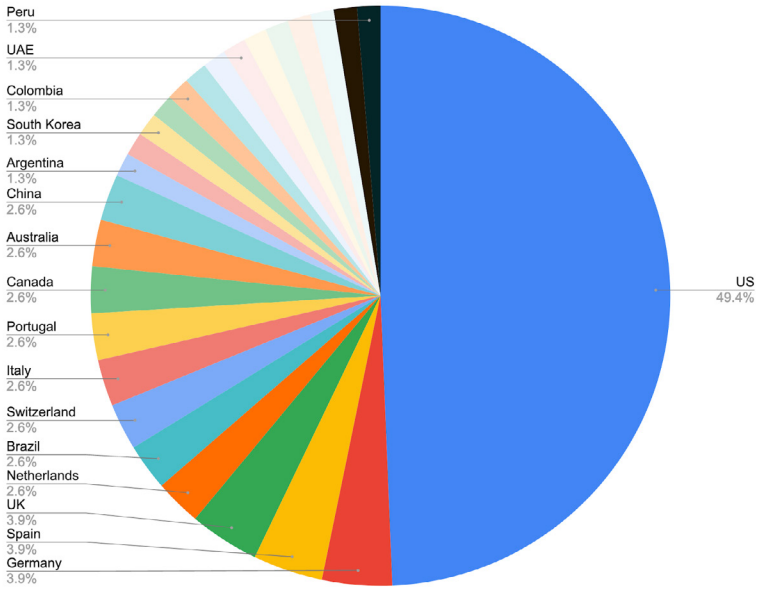
Victimology

Hive actors have been observed heavily targeting the US, with US victims making up over 49% of all victims published on HiveLeaks, Hive group's data leaks site.

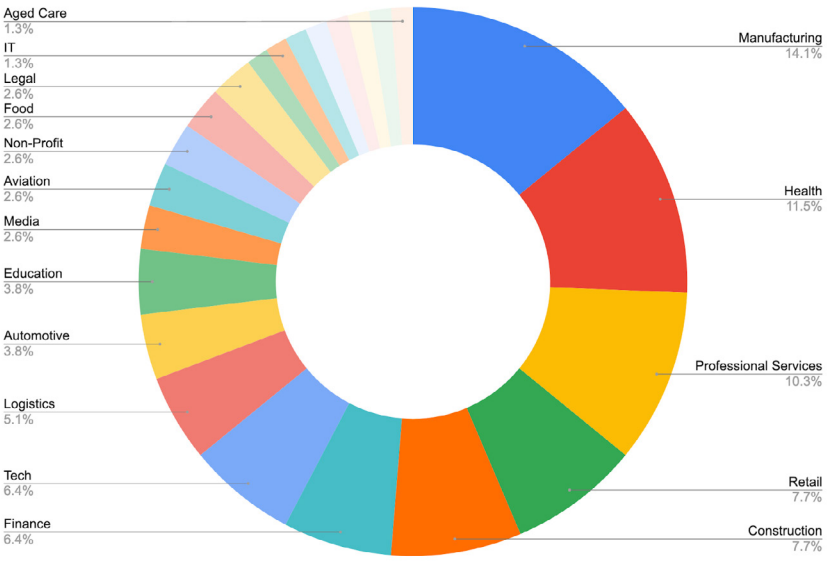
Hive actors target a range of industries, with victims from 23 industries posted to HiveLeaks. Victims from Manufacturing, Health, and Professional Services made up almost 36% of the total victims posted to HiveLeaks.

The following graphs summarize Hive victims published on HiveLeaks as of March 13, 2022. As the data is sourced from HiveLeaks, it's likely not a true reflection of all Hive victims, as victims may have paid the ransom before being published to the site.

Hive Victims by Country



Hive Victims by Industry



Tactics, Techniques, and Procedures (TTPs)

Hive actors have been observed gaining initial access to victim networks through phishing emails that drop Cobalt Strike beacon payloads. ConnectWise, a legitimate remote desktop application, has also been observed in use by Hive ransomware actors. Cobalt Strike and ConnectWise offer persistence and command and control to Hive actors.

Once persistence is established, Hive actors have been observed dumping credentials from LSASS memory using comsvcs.dll, which are then used to perform lateral movement through the victim network.

When Hive ransomware is executed, it will first stop system services, terminate processes that may conflict with the ransomware, and delete shadow copies if it's a Windows device before starting its encryption process.

After encrypting, Hive will also create large files of random data until disk space is full. The files are then deleted. This activity is possibly performed to prevent victims from attempting recovery via dumping raw disk space and carving files from the dump.

MITRE ATT&CK:

The following maps known Hive ransomware attack TTPs to MITRE ATT&CK:

Resource Development

- **Acquire Infrastructure (T1583) -** Hive actors utilize dedicated C2 infrastructure to perform ransomware attacks.

Initial Access

- **External Remote Services (T1133 -** Hive actors have used RDP software to gain initial access to victim networks.

Execution

- **Command and Scripting Interpreter: PowerShell (T1059.001) -** Hive actors have used PowerShell in ransomware attacks.
- **Command and Scripting Interpreter: Windows Command Shell (T1059.003) -** Hive actors have used the Windows command shell in ransomware attacks.
- **Command and Scripting Interpreter: Unix Shell (T1059.004) -** Hive actors have used the Unix shell in ransomware attacks.

Persistence

- **External Remote Services (T1133) -** Hive actors have used RDP software to maintain access to victim networks.

Defense Evasion

- **Indicator Removal on Host: File Deletion (T1070.004) -** Hive self-deletes after finishing encrypting victim files.
- **Obfuscated Files or Information: Software Packing (T1027.002) -** Hive ransomware group has used UPX to pack Hive ransomware binaries.
- **Modify Registry (T1112) -** Hive ransomware modifies the registry to disable Windows Defender.

Credential Access

- **OS Credential Dumping: LSASS Memory (T1003.001 -** Hive actors have dumped the LSASS process memory using the MiniDump function during ransomware attacks.

Discovery

- **System Service Discovery (T1007) -** Hive can discover running services.

Collection

- **Data from Local System (T1005) -** Hive actors manually collect data from the local systems for exfiltration.

Command and Control

- **Application Layer Protocol: Web Protocols (T1071.001) -** Hive ransomware group actors have used Cobalt Strike for HTTP-based C2 communications.
- **Remote Access Software (T1219 -** Hive ransomware group actors have used legitimate RDP software to perform command and control.

Exfiltration

- **Exfiltration Over C2 Channel (T1041) -** Maze actors has utilized Cobalt Strike and ConnectWise to exfiltrate data from victim networks before encryption.

Impact

- **Service Stop (T1489) -** Hive can stop processes and services.
- **Inhibit System Recovery (T1490) -** Hive can delete shadow copies.
- **Data Encrypted for Impact (T1486) -** Hive encrypts files that are part of a list of files.

Table of Contents

Mitigations/Defenses

Implementing a strong foundation of security controls is recommended to defend your network against Hive ransomware actors.

The Center for Internet Security (CIS) Controls are a prioritized set of safeguards designed to defend against cyber attacks. The CIS Controls has three tiers, known as Implementation Groups, that build on each other.

The following table maps Hive's MITRE ATT&CK techniques to CIS v8 Safeguards:

MITRE ATT&CK	CIS Safeguards
External Remote Services (T1133)	**IG1** 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 6.3: Require MFA for Externally-Exposed Applications 6.4: Require MFA for Remote Network Access 6.5: Require MFA for Administrative Acces
Command and Scripting Interpreter: PowerShell (T1059.001)	**IG1** 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates
Command and Scripting Interpreter: Windows Command Shell (T1059.003)	**IG2** 22.5: Allowlist Authorized Software
Command and Scripting Interpreter: Unix Shell (T1059.004)	**IG2** 2.5: Allowlist Authorized Software
Obfuscated Files or Information: Software Packing (T1027.002)	**IG1** 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates
Modify Registry (T1112)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process

— IG1 — IG2 — IG3

OS Credential Dumping: LSASS Memory (T1003.001)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 14.1: Establish and Maintain a Security Awareness Program 14.3: Train Workforce Members on Authentication Best Practices
Application Layer Protocol: Web Protocols (T1071.001)	**IG2** 13.3: Deploy a Network Intrusion Detection Solution
Remote Access Software (T1219)	**IG1** 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers
Exfiltration Over C2 Channel (T1041)	**IG2** 13.3: Deploy a Network Intrusion Detection Solution
Service Stop (T1489)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Inhibit System Recovery (T1490)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data
Data Encrypted for Impact (T1486)	**IG1** 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data

— IG1 — IG2 — IG3

Detection Opportunities

The following detection opportunities are mapped to MITRE ATT&CK v9 methods, CIS v8 Safeguards, and provide appropriate Red Canary Atomic Red Team tests to undertake for validation:

Detection Opportunity 1: Detect Hive's ESXi-targeting variant

MITRE ATT&CK: T1059.004

CIS Control(s): 2.5

Red Canary Atomic Red Team Test(s): N/A

Like other ransomware groups, Hive developers have written an ESXi-specific variant of Hive ransomware. ESXi is a popular hypervisor and often runs critical components of the business, making it a very lucrative target for ransomware actors.

Hive's ESXi-targeting variant runs the following shell command to power off virtual machines before starting the encryption process:

vim-cmd vmsvc/getallvms | grep -o -E '^[0-9]+' | xargs -r -n 1 vim-cmd vmsvc/power.off

By creating alerts for the above command being run in your environment, you will be able to detect potential deployment of Hive ransomware and be able to prevent the next stages of execution.

Detection Opportunity 2: Detect AnyDesk

MITRE ATT&CK: T1219

CIS Control(s): 4.2, 4.4

Red Canary Atomic Red Team Test(s): Atomic Test #2 - *AnyDesk* Files Detected Test on Windows

AnyDesk is legitimate desktop support and remote access tool that has been used by various malicious actors, including Hive actors. Hive actors have been observed installing *AnyDesk* on victim devices to establish persistence and use as a Command-and-Control tool during ransomware attacks.

By regularly auditing endpoints in your network for the installation of *AnyDesk* you are preventing unauthorized access to your network from malicious actors, including Hive affiliates. Given *AnyDesk* is a legitimate tool, it is important to understand whether the application is installed for legitimate reasons before removing it from endpoints.

Red Canary's T1219 Atomic Test #2 - AnyDesk Files Detected Test on Windows is a helpful and easy-to-run validation to ensure your detection for *AnyDesk* installations is functioning properly.

References/Appendix/Resources

https://www.ic3.gov/Media/News/2021/210825.pdf

https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/

https://blog.group-ib.com/hive

https://www.netskope.com/blog/hive-ransomware-actively-targeting-hospitals

https://blog.malwarebytes.com/ransomware/2022/02/hive-ransomware-researchers-figure-out-a-method-to-decrypt-files/