Ransomware Spotlight: Hive

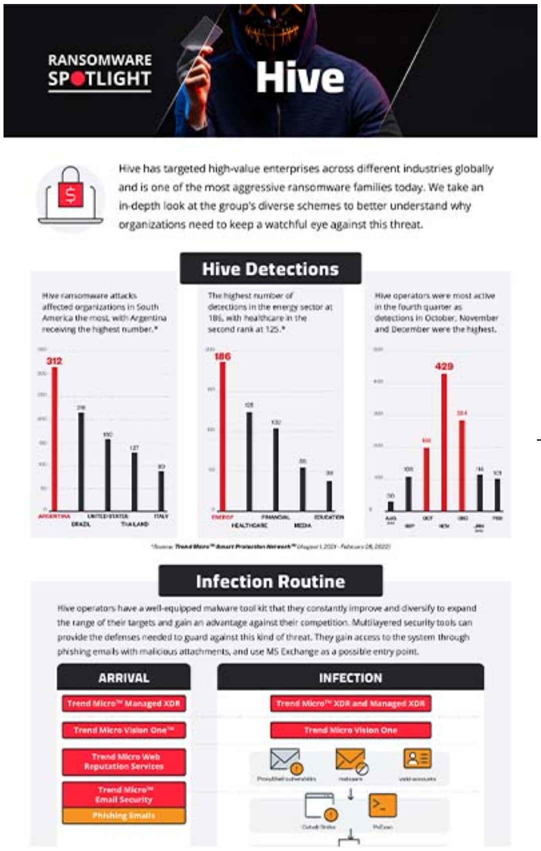
trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-hive

X

Hive

By Trend Micro Research

Hive ransomware is one of the new ransomware families in 2021 that poses significant challenges to enterprises worldwide. We take an in-depth look at the ransomware group’s operations and discuss how organizations can bolster their defenses against it.



Hive has targeted high-value enterprises across different industries globally and is one of the most aggressive ransomware families today. We take an in-depth look at the group's diverse schemes to better understand why organizations need to keep a watchful eye against this threat.

Hive Detections

Hive ransomware attacks affected organizations in South America the most, with Argentina receiving the highest number.*

The highest number of detections in the energy sector at 186, with healthcare in the second rank at 125.*

Hive operators were most active in the fourth quarter as detections in October, November and December were the highest.

*Source: Trend Micro™ Smart Protection Network™ (August 1, 2021 - February 08, 2022)

Infection Routine

Hive operators have a well-equipped malware tool kit that they constantly improve and diversify to expand the range of their targets and gain an advantage against their competition. Multilayered security tools can provide the defenses needed to guard against this kind of threat. They gain access to the system through phishing emails with malicious attachments, and use MS Exchange as a possible entry point.

_View infographic of "Ransomware Spotlight: Hive"

While some ransomware groups operating as ransomware-as-a-service (RaaS) networks claim to steer clear of targeting specific sectors such as hospitals or other critical industries to avoid causing harm to people, Hive's attacks against healthcare providers in 2021 showed that the operators behind it have no regard for such humanitarian considerations. A hospital in Missouri suffered a Hive ransomware attack three weeks after the same group hit the integrated systems of a healthcare provider that affected three hospitals and many outpatient clinics in two other US states. Hive ransomware has become one of the most active ransomware families since its discovery in June 2021. To defend against this threat, it is therefore crucial for companies to be acquainted with the various mechanisms that the infamous ransomware gang uses.

What do organizations need to know about Hive?

On August 15, 2021, Hive's ransomware attacks against a non-profit integrated health system severely disrupted the clinical and financial operations of three hospitals in Ohio and West Virginia. The attack resulted in emergency room diversions and cancelation of urgent surgical cases and radiology examinations. The encryption of files forced the hospital staff to use paper charts. Aside from the three hospitals, the affected non-profit also runs several outpatient service sites and clinics with a combined workforce of 3,000 employees.

Hive operators used double extortion techniques in this attack. Aside from the encryption of data, they also stole patient information that they threatened to publish on HiveLeaks, their dedicated leak site. The gang shares the list of victims that have not paid the ransom on their Tor site.

The incident prompted the FBI to issue an alert in late August that detailed Hive ransomware's indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs). According to the alert, Hive operators use phishing emails with malicious attachments to gain initial access to the system and Remote Desktop Protocol (RDP) to move laterally once on the network.

The motivation of those in the cyber-underground to expand their foothold inevitably leads to the incursion of uncharted paths. In late October 2021, threat researchers discovered that Hive has new malware tools specifically developed to encrypt Linux and FreeBSD systems. The report notes that Hive is among other ransomware operators that have set their sights on Linux servers. Other notorious ransomware groups have also been known to create their own Linux encryptors.

As enterprises slowly migrate to virtual machines to achieve better device management and optimize the use of resources, targeting virtual machines also makes good business sense for RaaS operators because it enables them to encrypt multiple servers simultaneously with just one command. Researchers pointed out that Hive's bespoke tool for Linux is not fully functional yet as it still cannot completely encrypt all files when the malware was deployed in an explicit path. However, one can expect Hive to keep refining their Linux encryptors to diversify and fortify its malware tool kit.

In January 2022, one of Europe's largest car dealers suffered a Hive ransomware attack. The Swiss company's name appeared as one of the victims on HiveLeaks in February. Targeting high-value enterprises has become a trend for ransomware operators as can be gleaned from the profile of the victim that reportedly generated US$3.29 billion in revenues for 2020.

Overview of Hive's operations

Hive operations are more prolific than their leak site might suggest. HiveLeaks only publishes the list of victims that have not settled the ransom, so it is tough to determine which — or how many — companies decided to pay the ransom. A report indicates that attack attempts by Hive affiliates hit an average of three companies per day since the group was first discovered in June 2021. The report also mentioned that security researchers who got access to information directly from the administrator panel of the Hive Tor site discovered that the number of enterprises whose systems had been compromised have reached 355 from September to December 2021.

Intelligence gathered by the researchers further revealed that the founders of the group deliberately put systems in place to achieve as much ease and transparency as possible particularly in the process of ransomware deployment and negotiations. Researchers also learned that the generation of malware versions by affiliates can be done within 15 minutes, while negotiations are coursed through the Hive ransomware administrators who relay the message to the victims in a chat window that the affiliates can see.

Researchers also shared that affiliates can see on the Hive administrator panel how much money was collected, the list of companies that paid, and those whose information was leaked.

The group's emphasis on operational efficiency and transparency is key to enticing new affiliates. It suggests that the group is aiming for sustainability by creating an environment that is conducive to building a bigger and stronger affiliate base.

Of note is that some enterprises complained about the decryption tool that Hive operators provided after settling the ransom. Reports said it lacked proper functionality and claimed that the Master Boot Records of their virtual machines were corrupted, rendering them incapable of booting.

Top affected countries and industries

This section cites Trend Micro™ Smart Protection Network™ (SPN) data on Hive's attempts to compromise organizations. Our detections show that Hive ransomware attack attempts against organizations were observed the most in South America, with Argentina receiving the highest number followed by Brazil. The United States takes the third spot, while the rest are spread across Europe, Asia, and the Middle East.

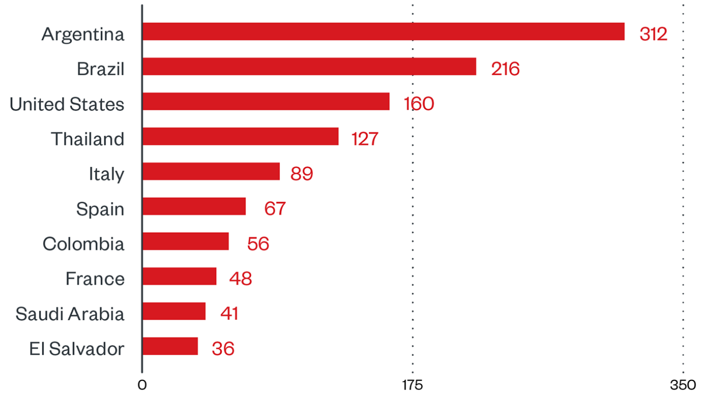


Figure 1. 10 countries with the highest number of attack attempts per machine for Hive ransomware (August 1, 2021 to February 28, 2022)
Source: Trend Micro Smart Protection Network

The energy sector had the highest number of attack attempts at 186; healthcare came in second at 125, followed by the financial sector with 102 detections.

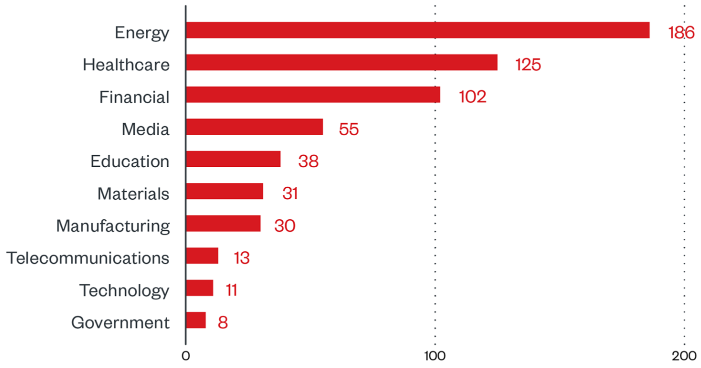


Figure 2. 10 industries with the highest number of attack attempts per machine for Hive ransomware (August 1, 2021 to February 28, 2022)
Source: Trend Micro Smart Protection Network

By breaking down the detections per month, our findings reveal that attack attempts peaked in November 2021 at 429. Hive operators were most active in the fourth quarter of 2021 as detections in December and October were the second and third highest numbers, respectively.

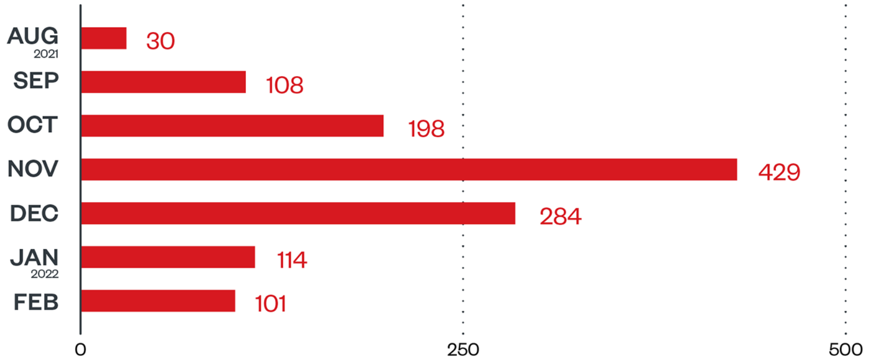


Figure 3. Monthly breakdown of detections per machine for Hive ransomware (August 1, 2021 to February 28, 2022)
Source: Trend Micro Smart Protection Network

Targeted regions and sectors according to Hive's leak site

An examination of the information that can be found on HiveLeaks reveals the number of successfully compromised companies that, as of this writing, have declined to pay the ransom. In our monitoring of their leak site from December 1, 2021 to February 28, 2022, attacks were highest in North America at 45.2% followed by Europe at 29% and Latin America at 12.9%.

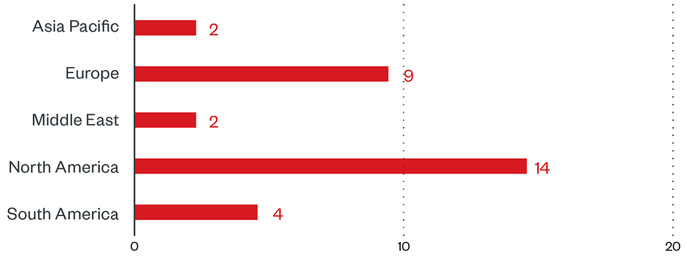


Figure 4. Regional distribution of Hive victims according to the group's leak site (December 1, 2021 to February 28, 2022)

Enterprises appear to be Hive's preferred targets estimated at almost 40%. Their victims were from a wide range of sectors, with technology at the top of the list having a victim count of 5. The healthcare and transportation sectors follow at 4 victims each. Other affected industries include construction, media and entertainment, professional services, retail, materials, automotive, apparel and fashion.

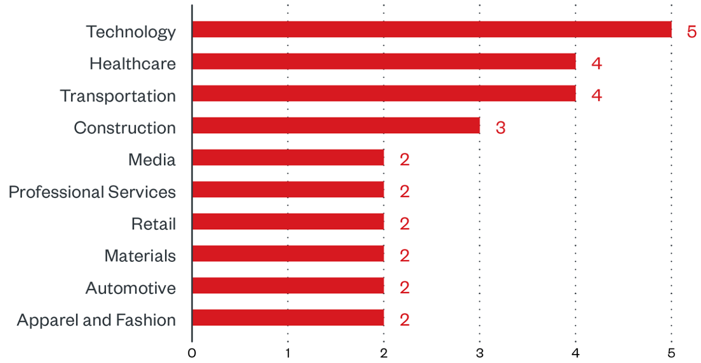


Figure 5. Sector distribution of Hive victims according to the group's leak site (December 1, 2021 to February 28, 2022)

Data observed in the same time frame showed that most of the attacks took place on weekdays as malicious activities on weekends comprise only 6.5%.

Infection chain and techniques

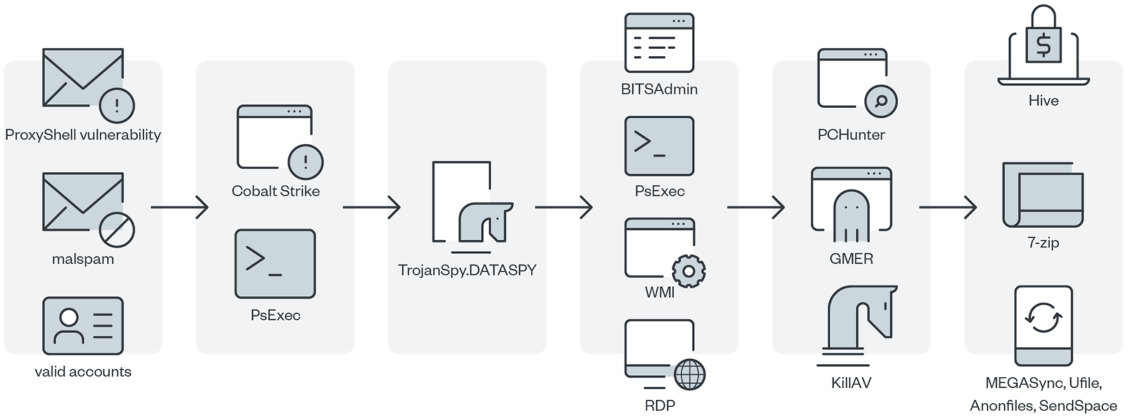


Figure 6. Infection chain of Hive ransomware

Initial Access

Hive operators breach systems through phishing emails with malicious attachments. We also observed Microsoft Exchange as a possible entry point for Hive ransomware based on our detection of the same post-exploitation scripts that can be found in the technique used to exploit ProxyShell-related vulnerabilities. These vulnerabilities were identified as CVE-2021-31207, CVE-2021-34473 and CVE-2021-34523.

Execution

Hive operators attempt to run the persistence technique for a Cobalt Strike beacon that can be used as a C&C method to accomplish lateral movement once they intrude into the system. Right after the attempt, Hive operators start to unload or uninstall antivirus (AV) products in the system so they can proceed to the download and execution of hacking tools such as PCHunter, GMER, and TrojanSpy.DATASPY. They use these tools to unload other AV products as a tactic to evade detection. We also observed the presence of WMI used to deploy uninstallation scripts and ransomware across the networks for lateral movement.

Defense Evasion, Discovery, and Credential Access

We observed the presence of PCHunter and GMER as their tools to discover and terminate services or processes to disable AV software. We also detected the use of TrojanSpy.DATASPY to gather information in the system such as machines in the network and the presence of specific AV products. In another attack, the threat actors deployed KillAV to terminate several AV products, also to avoid detection.

Lateral Movement, Command-and-Control

The Hive gang uses RDP and WMI to move laterally in the compromised network and deliver the payload remotely. We also detected the use of a BITSAdmin command for lateral movement. The threat actors also used PsExec to move laterally within the network.

Exfiltration

Our detections showed that the Hive operators use 7-Zip tool to archive stolen data for exfiltration. Moreover, the gang abuses anonymous file-sharing services such as MEGASync, AnonFiles, SendSpace, and uFile to exfiltrate data.

Impact

The ransomware payload proceeds with the encryption routine upon execution. The ransomware generates a random key that is used to encrypt based on RTLGenRandom API, which will be initially saved on the device's memory. The key is then used in what appears to be a custom implementation of the encryption process.

The key also encrypts through RSA via GoLang's implementation of RSA encryption. It accomplishes the RSA encryption through a list of public keys embedded in the binary. It is then saved as .key. on the encrypted drive.

The generated key will then be wiped from memory, leaving the encryption key as the only copy of the key for decryption.

MITRE tactics and techniques

Initial Access	**Execution**	**Persistence**	**Defense Evasion**	**Discovery**	**Lateral Movement**	**Collection**	**Command and Control**
T1566.001 - Phishing: Spear-phishing attachment *Arrives via phishing emails.* **T1190** - Exploit public-facing application *Arrives via any the following exploits:• CVE-2021-34473• CVE-2021-34523• CVE-2021-31207* **T1078** - Valid accounts *Has been reported to make use of compromised accounts to access victims via RDP*	**T1106** - Native API *Uses native API to execute various commands /routines* **T1059.003** - Command and scripting interpreter: Windows Command Shell *The ransomware accepts various command-line arguments upon execution.* **T1059.001** - Command and scripting interpreter: PowerShell *Cobalt executes a PowerShell command to run the persistence technique.* **T1053.005** - Scheduled Task/Job: Scheduled Task*Registers and executes malicious tasks* **T1204** - User execution *User execution is needed to carry out the payload from the spear phishing link/attachments* **T1047** - Windows Management Instrument *Used WMI to deploy uninstallation scripts and ransomware.*	**T1053.005** - Boot or logon autostart execution *Scheduled Task/Job: Scheduled Task* **T1068** - Exploitation for Privilege Escalation *Makes use of CVE-2021-34523 to escalate privilege.*	**T1562.001** - Impair Defenses: Disable or Modify Tools *Uses several tools to disable security related software by terminating them*	**T1083** - File and directory discovery *Searches for specific files and directories related to its encryption* **T1018** - Remote system discovery *Makes use of tools for network scans* **T1057** - Process discovery *Discovers certain processes for process termination* **T1063** - Security software discovery *Discovers security software for reconnaissance and termination* **T1049** - System Network Connections Discovery *Uses TrojanSpy.DATASPY to gather information about the connected machines in the network.* **T1135** - Network Share Discovery *List all available machines in the network via SMB*	**T1570** - Lateral tool transfer *Can make use of RDP to transfer the Ransomware or tools within the network* **T1021.002** - Remote services: SMB/Windows admin shares *Uses RDP to transfer and execute ransomware payload and other tools.* **T1021.006** - Remote Services: Windows Remote Management *Uses WMI to execute and deploy uninstallation scripts and the ransomware payload.*	**T1005** - Data from local system *May make use of RDP to manually search for valuable files or information* **T1560.001** - Archive Collected Data: Archive via Utility *Uses a tool to archive stolen information for exfiltration*	**T1105** - Ingress Toc Transfer *Executes BitsAdmin Command to deliver the ransomwar on other machines i the networl*

Summary of malware, tools, and exploits used

Security teams can watch out for the presence of the following malware tools and exploits that are typically used in Hive attacks:

Initial Access	Execution	Discovery	Lateral Movement	Defense Evasion	Exfiltration
Phishing emails with malicious attachments Exoitpls: • **CVE-2021-34473** Pre-auth path confusion vulnerability to bypass access control • **CVE-2021-34523** Privilege elevation vulnerability in the Exchange PowerShell backend • **CVE-2021-31207** Post-auth remote code execution via arbitrary file write	• **PsExec** 3rd Party Tool to execute process or command-line on a remote computer • **WMI** Administration feature that provides a uniform environment to access Windows system components. This was used for remote execution of files for lateral movement. • **Cobalt Strike**	**TrojanSpy.DATASPY** Trojan that collects AV related processes and services running in the system as well as connected machines within the network	• **PSExec** Command-line utility built for Windows to allow programs to run on remote machines • **RDP** Spread across machines in the network using RDP connection • **BitsAdmin** Command-line tool that is used to create download or upload jobs and monitor their progress • **WMI** Administration feature that provides a uniform environment to access Windows system components. This was used for remote execution of files for lateral movement.	• **PCHunter** Third party tool that can be used to disable security tools • **GMER** Third party tool that can be used to disable security tools • **KillAV** Used to terminate AV processes	• **7-Zip** A file archiver with a high compression ratio. • **MEGASync** Third party cloud storage tool abused for data exfiltration • **uFile.io** ◦ A free file hosting website where people can upload and share files to other users ◦ Abused for data exfiltration • **SendSpace** Third party cloud storage tool abused for data exfiltration • **AnonFiles** ◦ An online file storage provider that provides an anonymous working environment ◦ Abused for data exfiltration

Recommendations

Despite being relatively new, Hive ransomware has already made its mark as one of the most prolific and aggressive ransomware families today. Our detections of their malicious activities show that their operations are robust, thus providing an incentive for new affiliates to join them. Hive operators are also known to constantly refine and diversify their TTPs, so it is important for companies to stay vigilant and be well-informed of potential threats. An organization stands a better chance of addressing ransomware threats if they implement strong defenses early on.

To protect systems against similar threats, organizations can establish security frameworks that allocate resources systematically for establishing a strong defense strategy against ransomware.

Here are some best practices that organizations can consider:

Audit and inventory

- Take an inventory of assets and data
- Identify authorized and unauthorized devices and software
- Audit 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 allowlist 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 possible entry points into their system (endpoint, email, web, and network). Security solutions can detect malicious components and suspicious behavior, which can help protect enterprises.

- Trend Micro Vision One™ provides multilayered protection and behavior detection, which helps block questionable behavior and tools before the ransomware can do any damage.
- Trend Micro Cloud One™ Workload Security protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™ offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise (IOCs)

The IOCs for this article can be found here. Actual indicators might vary per attack.

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.