FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

25 AUG 2021

Alert Number

MC-000150-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Indicators of Compromise Associated with Hive Ransomware

Summary

Hive ransomware, which was first observed in June 2021 and likely operates as an affiliate-based ransomware, employs a wide variety of tactics, techniques, and procedures (TTPs), creating significant challenges for defense and mitigation. Hive ransomware uses multiple mechanisms to compromise business networks, including phishing emails with malicious attachments to gain access and Remote Desktop Protocol (RDP) to move laterally once on the network.

After compromising a victim network, Hive ransomware actors exfiltrate data and encrypt files on the network. The actors leave a ransom note in each affected directory within a victim's system, which provides instructions on how to purchase the decryption software. The ransom note also threatens to leak exfiltrated victim data on the Tor site, "HiveLeaks."

Technical Details

Hive ransomware seeks processes related to backups, anti-virus/anti-spyware, and file copying and terminates them to facilitate file encryption. The encrypted files commonly end with a .hive extension. The Hive ransomware then drops a hive.bat script into the directory, which enforces an execution timeout delay of one second in order to perform cleanup after the encryption is finished by deleting the Hive executable and the hive.bat script. A second file, shadow.bat, is dropped into the directory to delete shadow copies, including disc backup copies or snapshots, without notifying the victim and then deletes the shadow.bat file. During the encryption process, encrypted files are renamed with the double final extension of `*.key.hive` or `*.key.*`. The ransom note, "`HOW_TO_DECRYPT.txt`" is dropped into each affected directory and states the `*key.*` file cannot be modified, renamed, or deleted, otherwise the encrypted files cannot be recovered. The note contains a "sales department" link, accessible through a TOR browser, enabling victims to contact the actors through a live chat. Some victims reported receiving phone calls from Hive actors requesting payment for their files. The initial deadline for payment fluctuates between 2 to 6 days, but actors have prolonged the deadline in response to contact by the victim company. The ransom note also informs victims that a public disclosure or leak site, accessible on a TOR browser, contains data exfiltrated from victim companies who do not pay the ransom demand.

Indicators of Compromise

The following indicators were leveraged by the threat actors during Hive ransomware compromises. Some of these indicators might appear as applications within your enterprise supporting legitimate purposes; however, these applications can be used by threat actors to aid in further malicious exploration of your enterprise. The FBI recommends removing any application not deemed necessary for day-to-day operations.

Hive Tor Domain
http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion

Winlo.exe	
MD5	b5045d802394f4560280a7404af69263
SHA256	321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a78bdac06868136b72c
File Path Observed	C:\Windows\SysWOW64\winlo.exe
Description	Drops `7zG.exe`
`7zG.exe`	
MD5	04FB3AE7F05C8BC333125972BA907398
Description	This is a legitimate 7zip, version 19.0.0 Drops `Winlo_dump_64_SCY.exe`
`Winlo_dump_64_SCY.exe`	
MD5	BEE9BA70F36FF250B31A6FDF7FA8AFEB
Description	Encrypts files with *.key.* extension Drops `HOW_TO_DECRYPT.txt`
`HOW_TO_DECRYPT.txt`	
Description	Stops and disables Windows Defender Deletes all Windows Defender definitions Removes context menu for Windows Defender Stops the following services and disables them from restart LanmanWorkstation SamSs SDRSVC SstpSVc UI0Detect Vmicvss Vmss VSS Wbengine Unistoresvc Attempts to delete Volume Shadow Copies (vssadmin and wmic) Deletes Windows Event Logs -> System, Security, Application and powershell Uses notepad++ to create key file Changes bootup to ignore errors and not attempt recovery Drops PowerShell script

Other IOCs
*.key.hive
.key.
HOW_TO_DECRYPT.txt
hive.bat
shadow.bat
vssadmin.exe delete shadows /all /quiet
wmic.exe SHADOWCOPY /nointeractive
wmic.exe shadowcopy delete
wevtutil.exe cl system
wevtutil.exe cl security
wevtutil.exe cl application
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe /set {default} recoveryenabled no

Anonymous File Sharing Links
https://anonfiles.com
https://mega.nz
https://send.exploit.in
https://ufile.io
https://www.sendspace.com

Sample Ransom Note

Your network has been breached and all data were encrypted.
Personal data, financial reports and important documents are ready to disclose.

To decrypt all the data or to prevent exfiltrated files to be disclosed at http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion/ you will need to purchase our decryption software.

Please contact our sales department at:

REDACTED

Login: REDACTED
Password: REDACTED

To get access to .onion websites download and install Tor Browser at: https://www.torproject.org/ (Tor Browser is not related to us)

Follow the guidelines below to avoid losing your data:

- Do not shutdown or reboot your computers, unmount external storages.
- Do not try to decrypt data using third party software. It may cause irreversible damage.
- Do not fool yourself. Encryption has perfect secrecy and it's impossible to decrypt without knowing the key.
*- Do not modify, rename or delete *.key.k6thw files. Your data will be undecryptable.*
- Do not modify or rename encrypted files. You will lose them.
- Do not report to authorities. The negotiation process will be terminated immediately and the key will be erased.
- Do not reject to purchase. Your sensitive data will be publicly disclosed.

Information Requested

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. Regardless of whether you or your organization decide to pay the ransom, the FBI urges you to report ransomware incidents to your local field office. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under US law, and prevent future attacks.

The FBI may seek the following information that you determine you can legally share, including:

- Recovered executable files
- Live memory (RAM) capture
- Images of infected systems
- Malware samples
- IP addresses identified as malicious or suspicious
- Email addresses of the attackers
- A copy of the ransom note
- Ransom amount
- Bitcoin wallets used by the attackers
- Bitcoin wallets used to pay the ransom
- Post-incident forensic reports

Recommended Mitigations

- Back-up critical data offline.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
- Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.
- Use two-factor authentication with strong passwords, including for remote access services.

- Monitor cyber threat reporting regarding the publication of compromised VPN login credentials and change passwords/settings if applicable.
- Keep computers, devices, and applications patched and up-to-date.
- Install and regularly update anti-virus or anti-malware software on all hosts.
- Review the following additional resources.
    - The joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity provides additional guidance when hunting or investigating a network and common mistakes to avoid in incident handling.
    - The Cybersecurity and Infrastructure Security Agency-Multi-State Information Sharing & Analysis Center Joint Ransomware Guide covers additional best practices and ways to prevent, protect, and respond to a ransomware attack.
    - StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

If your organization is impacted by a ransomware incident, the FBI and CISA recommend the following actions.

- **Isolate the infected system.** Remove the infected system from all networks, and disable the computer's wireless, Bluetooth, and any other potential networking capabilities. Ensure all shared and networked drives are disconnected, whether wired or wireless.
- **Turn off other computers and devices.** Power-off and segregate (i.e., remove from the network) the infected computer(s). Power-off and segregate any other computers or devices that share a network with the infected computer(s) that have not been fully encrypted by ransomware. If possible, collect and secure all infected and potentially infected computers and devices in a central location, making sure to clearly label any computers that have been encrypted. Powering-off and segregating infected computers and computers that have not been fully encrypted may allow for the recovery of partially encrypted files by specialists.
- **Secure your backups.** Ensure that your backup data is offline and secure. If possible, scan your backup data with an antivirus program to check that it is free of malware.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey