JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Product ID: AA24-242A

August 29, 2024

Co-Authored by:

#StopRansomware: RansomHub Ransomware

Summary

Note: *This joint Cybersecurity Advisory is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

Actions to take today to mitigate cyber threats from ransomware:

- Install updates for operating systems, software, and firmware as soon as they are released.
- Require phishing-resistant MFA (i.e., non-SMS text based) for as many services as possible.
- Train users to recognize and report phishing attempts.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Department of Health and Human Services (HHS) (hereafter referred to as the authoring organizations) are releasing this joint advisory to disseminate known RansomHub ransomware IOCs and TTPs. These have been identified through FBI threat response activities and third-party reporting as recently as August 2024. RansomHub is a ransomware-as-a-service variant—formerly known as Cyclops and Knight—that has established itself as an efficient and successful service model (recently attracting high-profile affiliates from other prominent variants such as LockBit and ALPHV).

Since its inception in February 2024, RansomHub has encrypted and exfiltrated data from at least 210 victims representing the water and wastewater, information technology, government services and facilities, healthcare and public health, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, and communications critical infrastructure sectors.

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. SLTT organizations should report incidents to MS-ISAC (866-787-4722 or SOC@cisecurity.org).

The affiliates leverage a double-extortion model by encrypting systems and exfiltrating data to extort victims. It should be noted that data exfiltration methods are dependent on the affiliate conducting the network compromise. The ransom note dropped during encryption does not generally include an initial ransom demand or payment instructions. Instead, the note provides victims with a client ID and instructs them to contact the ransomware group via a unique `.onion` URL (reachable through the Tor browser). The ransom note typically gives victims between three and 90 days to pay the ransom (depending on the affiliate) before the ransomware group publishes their data on the RansomHub Tor data leak site.

The authoring organizations encourage network defenders to implement the recommendations in the **Mitigations** section of this cybersecurity advisory to reduce the likelihood and impact of ransomware incidents.

For a downloadable copy of IOCs, see:

- AA24-242A-STIX XML (##KB)
- AA24-242A STIX JSON (##KB)

Table of Contents

Contents

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 15. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.

Initial Access

RansomHub affiliates typically compromise internet facing systems and user endpoints by using methods such as phishing emails [T1566], exploitation of known vulnerabilities [T1190], and password spraying [T1110.003]. Password spraying targets accounts compromised through data breaches. Proof-of-concept exploits are obtained from sources such as ExploitDB and GitHub [T1588.005]. Exploits based on the following CVEs have been observed:

- CVE-2023-3519 (CWE-94)
  - Citrix ADC (NetScaler) Remote Code Execution. A vulnerability exists within Citrix ADC that allows an unauthenticated attacker to trigger a stack buffer overflow of the NSPPE (NetScaler Packet Processing Engine) process by making a specially crafted HTTP GET request. Successful exploitation results in remote code execution as root.
- CVE-2023-27997 (CWE-787 | CWE-122)
  - A heap-based buffer overflow vulnerability in FortiOS version 7.2.4 and below, version 7.0.11 and below, version 6.4.12 and below, version 6.0.16 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below, version 1.2 all versions, version 1.1 all versions SSL-VPN may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.
- CVE-2023-46604 (CWE-502)
  - The Java OpenWire protocol marshaller, such as in Apache ActiveMQ, is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to open either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath. Upgrading both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 fixes this issue.
- CVE-2023-22515
  - A vulnerability in publicly accessible Confluence Data Center and Server instances that allows the creation of unauthorized Confluence administrator accounts and access to Confluence instances. Atlassian Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue.

- CVE-2023-46747 (CWE-306 | CWE-288)
  - Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. **Note:** Software versions which have reached End of Technical Support (EoTS) are not evaluated.
- CVE-2023-48788 (CWE-89)
  - An improper neutralization of special elements used in an SQL command (SQL injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2 and FortiClientEMS 7.0.1 through 7.0.10 allows attackers to execute unauthorized code or commands via specially crafted packets.
- CVE-2017-0144
  - The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, also known as "Windows SMB Remote Code Execution Vulnerability" [T1210].
- CVE-2020-1472
  - An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller using the Netlogon Remote Protocol (MS-NRPC).
- CVE-2020-0787
  - This vulnerability was also potentially exploited along with the Zerologon privilege escalation vulnerability.

Discovery

RansomHub affiliates conduct network scanning with tools such as AngryIPScanner, Nmap, and PowerShell-based living off the land methods with PowerShell to conduct network scanning [T1018][T1046][T1059.001].

Defense Evasion

Cybersecurity researchers have observed affiliates renaming the ransomware executable with innocuous file names, such as Windows.exe, left on the user's desktop (C:\Users\%USERNAME%\Desktop) or downloads (C:\Users\%USERNAME%\Downloads) [T1036]. The affiliates have also cleared Windows and Linux system logs to inhibit any potential incident response [T1070]. Affiliates used Windows Management Instrumentation [T1047] to disable antivirus products. In some instances, RansomHub-specific tools were deployed to disable endpoint detection and response (EDR) tooling [T1562.001].

Privilege Escalation and Lateral Movement

Following initial access, RansomHub affiliates created user accounts for persistence [T1136], reenabled disabled accounts [T1098], and used Mimikatz [S0002] on Windows systems to gather credentials [T1003] and escalate privileges to SYSTEM [T1068]. Affiliates then moved laterally inside the network through methods including Remote Desktop Protocol (RDP) [T1021.001], PsExec [S0029], Anydesk

[T1219], Connectwise, N-Able, Cobalt Strike [S0154], Metasploit, or other widely used command-and-control (C2) methods.

Data Exfiltration

Data exfiltration methods depend heavily on the affiliate conducting the network compromise. The ransomware binary does not normally include any mechanism for data exfiltration. Data exfiltration has been observed through the usage of tools such as PuTTY [T1048.002], Amazon AWS S3 buckets/tools [T1537], HTTP POST requests [T1048.003], WinSCP, Rclone, Cobalt Strike, Metasploit, and other methods.

Encryption

RansomHub ransomware has typically leveraged an Elliptic Curve Encryption algorithm called Curve 25519 to encrypt user accessible files on the system [T1486]. Curve 25519 uses a public/private key that is unique to each victim organization. To successfully encrypt files that are currently in use, the ransomware binary will typically attempt to stop the following processes:

- *"vmms.exe"*
- *"msaccess.exe"*
- *"mspub.exe"*
- *"svchost.exe"*
- *"vmcompute.exe"*
- *"notepad.exe"*
- *"ocautoupds.exe"*
- *"ocomm.exe"*
- *"ocssd.exe"*
- *"oracle.exe"*
- *"onenote.exe"*
- *"outlook.exe"*
- *"powerpnt.exe"*
- *"explorer.exe"*
- *"sql.exe"*
- *"steam.exe"*
- *"synctime.exe"*
- *"vmwp.exe"*
- *"thebat.exe"*
- *"thunderbird.exe"*
- *"visio.exe"*
- *"winword.exe"*
- *"wordpad.exe"*

- *"xfssvccon.exe"*
- *"TeamViewer.exe"*
- *"agntsvc.exe"*
- *"dbsnmp.exe"*
- *"dbeng50.exe"*
- *"encsvc.exe"*

The ransomware binary will attempt to encrypt any files that the user has access to, including user files and networked shares.

RansomHub implements intermittent encryption, encrypting files in 0x100000 byte chunks and skipping every 0x200000 bytes of data in between encrypted chunks. Files smaller than 0x100000 bytes in size are completely encrypted. Files are appended with 58 (0x3A) bytes of data at the end. This data contains a value which is likely part of an encryption/decryption key. The structure of the appended 0x3A bytes is listed below with images from three different encrypted files.

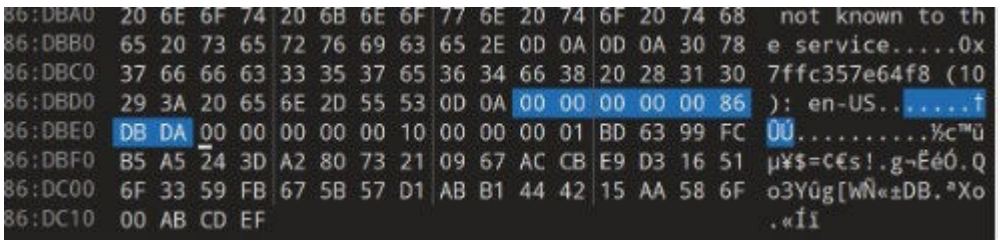

Figure 1: The first eight bytes are the size of the encrypted file.

The next eight bytes are the size of encrypted blocks. If the entire file is encrypted, this section is all zeros. In this example, each encrypted section is 0x100000 bytes long, with 0x100000 bytes between each encrypted block. This number was observed changing based on the size of the encrypted file.

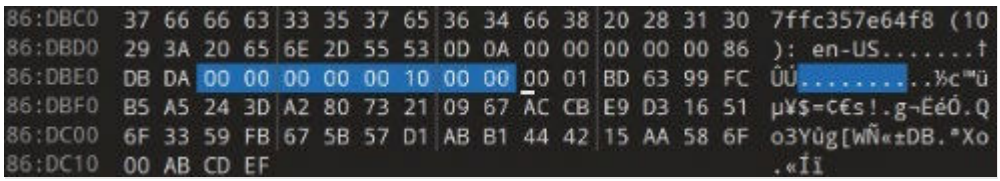

Figure 2: The size of encrypted blocks.

The next two bytes were always seen to be 0x0001.

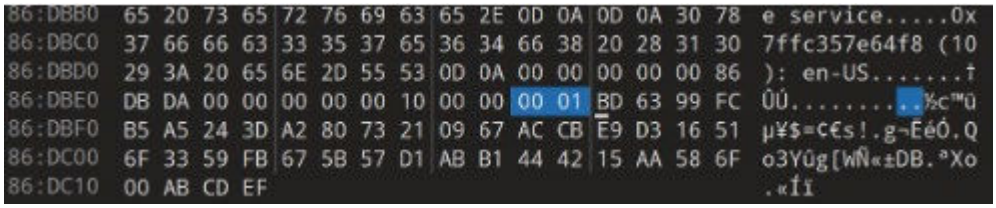

Figure 3: The next two bytes are always 0x0001.

The next 32 bytes are the public encryption key for the file.

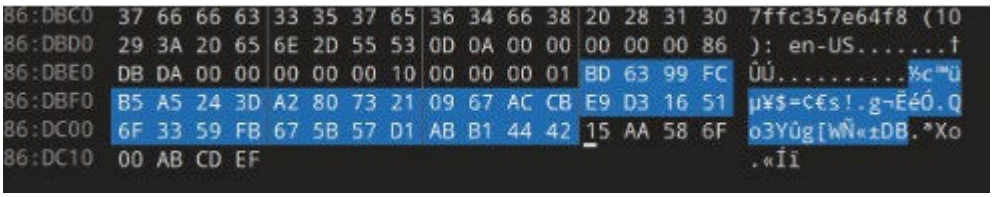

Figure 4: Public encryption key for the file.

The next four bytes are a checksum value.

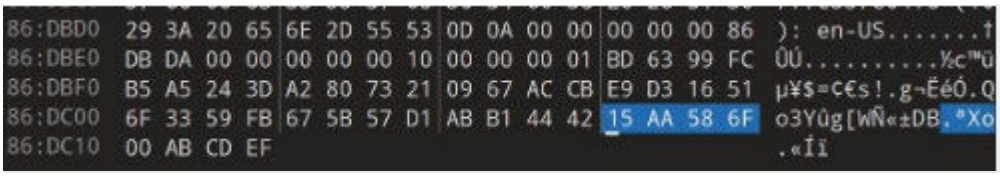

Figure 5: Checksum value.

The last four bytes are always seen to be the sequence 0x00ABCDEF.

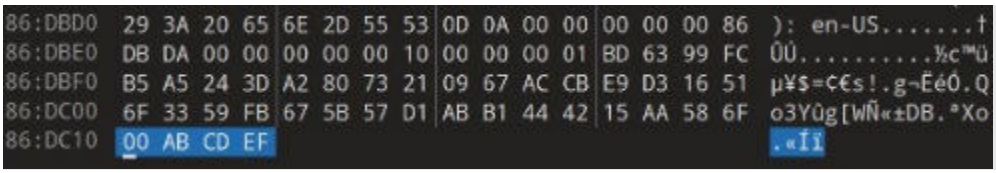

Figure 6: The last four bytes.

The ransomware executable does not typically encrypt executable files. A random file extension is added to file names and a ransom note generally titled How To Restore Your Files.txt is left on the compromised system. To further inhibit system recovery, the ransomware executable typically leverages the vssadmin.exe program to delete volume shadow copies [T1490].

Leveraged Tools

See **Table 1** for publicly available tools and applications used by RansomHub affiliates. This includes legitimate tools repurposed for their operations.

Table 1: Tools Used by RansomHub Affiliates

Disclaimer: Use of these tools and applications should not be attributed as malicious without analytical evidence to support threat actor use and/or control.

Tool Name	Description
BITSAdmin	A command-line utility that manages downloads/uploads between a client and server by using the Background Intelligent Transfer Service (BITS) to perform asynchronous file transfers.
Cobalt Strike [S0154]	A penetration testing tool used by security professionals to test the security of networks and systems. RansomHub affiliates have used it to assist with lateral movement and file execution.
Mimikatz [S0002]	A tool that allows users to view and save authentication credentials such as Kerberos tickets. RansomHub affiliates have used it to aid privilege escalation.
PSExec [S0029]	A tool designed to run programs and execute commands on remote systems.
PowerShell	Cross-platform task automation solution made up of a command line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS.
RClone	A command line program used to sync files with cloud storage services.
Sliver	A penetration testing toolset which allows for remote command and control of systems.
SMBExec	A tool designed to manipulate SMB services for remote code execution.
WinSCP	Windows Secure Copy is a free and open source SSH File Transfer Protocol, File Transfer Protocol, WebDAV, Amazon S3, and secure copy protocol client. Affiliates have used it to transfer data from a compromised network to actor-controlled accounts.
CrackMapExec	Pentest Toolset
Kerberoast	Kerberos Brute force and Exploitation Tool
AngryIPScanner	Network Scanner

Indicators of Compromise

Disclaimer: Several of these IP addresses were first observed as early as 2020, although most date from 2022 or 2023 and have been historically linked to QakBot. The authoring organizations recommend organizations investigate or vet these IP addresses prior to taking action (such as blocking).

See **Table 2–Table 5** for IOCs obtained from FBI investigations.

Table 2: Directory Structure TTPs

Filename	Description
C:\Users\%USERNAME%\AppData\Local\Programs\Python\Python311\Scripts\crackmapexec.exe	CrackMapExec
C:\Users\%USERNAME%\AppData\Local\Programs\Python\Python311\Scripts\kerbrute.exe	Kerberoasting
C:\Users\%USERNAME%\Downloads\Anydesk.exe	Anydesk C2
C:\Users\%USERNAME%\Desktop\IamBatMan.exe	Ransomware
C:\Users\backupexec\Desktop\stealer_cli_v2.exe	Info Stealer
C:\Users\%USERNAME%\Downloads\nmap-7.94-setup.exe	Nmap
C:\Program Files (x86)\Nmap\nmap.exe	Nmap
C:\Users\%USERNAME%\Downloads\mimikatz_trunk\x64\mimikatz.exe	Mimikatz
C:\Users\backupexec\Downloads\x64\mimikatz.exe	Mimikatz

Disclaimer: The authoring organizations recommend network defenders investigate or vet IP addresses prior to taking action, such as blocking. Many cyber actors are known to change IP addresses, sometimes daily, and some IP addresses may host valid domains.

Table 3: Known IPs Related to Malicious Activity (2023-2024)

IP Address
8.211.2[.]97
45.95.67[.]41
45.134.140[.]69
45.135.232[.]2

IP Address
89.23.96[.]203
188.34.188[.]7
193.106.175[.]107
193.124.125[.]78
193.233.254[.]21

Table 4: Known URLs Related to Malicious Activity (2023-2024)

Web Requests
http[:]//188.34.188[.]7/555
http[:]//188.34.188[.]7/555/
http[:]//188.34.188[.]7/555/amba16.ico
http[:]//188.34.188[.]7/555/bcrypt.dll
http[:]//188.34.188[.]7/555/CRYPTSP.dll
http[:]//188.34.188[.]7/555/en
http[:]//188.34.188[.]7/555/en-US
http[:]//188.34.188[.]7/555/NEWOFFICIALPROGRAMCAUSEOFNEWUPDATE.exe
http[:]//188.34.188[.]7/555/NEWOFFICIALPROGRAMCAUSEOFNEWUPDATE.exe.Config
http[:]//188.34.188[].7/555/NEWOFFICIALPROGRAMCAUSEOFNEWUPDATE.INI
http[:]//89.23.96[.]203/
http[:]//89.23.96[.]203/333
http[:]//89.23.96[.]203/333/
http[:]//89.23.96[.]203/333/1.exe
http[:]//89.23.96[.]203/333/1.exe.Config

Web Requests
http[:]//89.23.96[.]203/333/10.exe
http[:]//89.23.96[.]203/333/12.exe
http[:]//89.23.96[.]203/333/12.exe.Config
http[:]//89.23.96[.]203/333/2.exe
http[:]//89.23.96[.]203/333/2.exe.Config
http[:]//89.23.96[.]203/333/2wrRR6sW6XJtsXyPzuhWhDG7qwN4es.exe
http[:]//89.23.96[.]203/333/2wrRR6sW6XJtsXyPzuhWhDG7qwN4es.exe.Config
http[:]//89.23.96[.]203/333/3.exe
http[:]//89.23.96[.]203/333/3.exe.Config
http[:]//89.23.96[.]203/333/4.exe
http[:]//89.23.96[.]203/333/4.exe.Config
http[:]//89.23.96[.]203/333/5.exe
http[:]//89.23.96[.]203/333/5.exe.Config
http[:]//89.23.96[.]203/333/6.exe
http[:]//89.23.96[.]203/333/7.exe
http[:]//89.23.96[.]203/333/8.exe
http[:]//89.23.96[.]203/333/9.exe
http[:]//89.23.96[.]203/333/92.exe
http[:]//89.23.96[.]203/333/AmbaPDF.ico
http[:]//89.23.96[.]203/333/ambapdf.ico.DLL
http[:]//89.23.96[.]203/333/bcrypt.dll
http[:]//89.23.96[.]203/333/Cabinet.dll

Web Requests
http[:]//89.23.96[.]203/333/CRYPTBASE.DLL
http[:]//89.23.96[.]203/333/cryptnet.dll
http[:]//89.23.96[.]203/333/CRYPTSP.dll
http[:]//89.23.96[.]203/333/cv4TCGxUjvS.exe
http[:]//89.23.96[.]203/333/DPAPI.DLL
http[:]//89.23.96[.]203/333/en
http[:]//89.23.96[.]203/333/en/d%E5%AD%97%E5%AD%97.resources.dll
http[:]//89.23.96[.]203/333/en/d%E5%AD%97%E5%AD%97.resources.exe
http[:]//89.23.96[.]203/333/en/d%E5%AD%97%E5%AD%97.resources/d%E5%AD%97%E5%AD%97.resources.dll
http[:]//89.23.96[.]203/333/en/d%E5%AD%97%E5%AD%97.resources/d%E5%AD%97%E5%AD%97.resources.exe
http[:]//89.23.96[.]203/333/en-US
http[:]//89.23.96[.]203/333/en-US/d%E5%AD%97%E5%AD%97.resources.dll
http[:]//89.23.96[.]203/333/en-US/d%E5%AD%97%E5%AD%97.resources.exe
http[:]//89.23.96[.]203/333/en-US/d%E5%AD%97%E5%AD%97.resources/d%E5%AD%97%E5%AD%97.resources.dll
http[:]//89.23.96[.]203/333/en-US/d%E5%AD%97%E5%AD%97.resources/d%E5%AD%97%E5%AD%97.resources.exe
http[:]//89.23.96[.]203/333/iertutil.dll
http[:]//89.23.96[.]203/333/information.exe
http[:]//89.23.96[.]203/333/information.exe.Config
http[:]//89.23.96[.]203/333/information.INI
http[:]//89.23.96[.]203/333/IPHLPAPI.DLL

Web Requests
http[:]//89.23.96[.]203/333/mshtml.dll
http[:]//89.23.96[.]203/333/msi.dll
http[:]//89.23.96[.]203/333/SspiCli.dll
http[:]//89.23.96[.]203/333/TmsLA6kdcU8jxKzpMvbUVweTeF5YcR.exe
http[:]//89.23.96[.]203/333/TmsLA6kdcU8jxKzpMvbUVweTeF5YcR.exe.Config
http[:]//89.23.96[.]203/333/2wrRR6sW6XJtsXyPzuhWhDG7qwN4es.exe
http[:]//89.23.96[.]203/333/xwenxub285p83ecrzvft.exe
http[:]//89.23.96[.]203/333/cv4TCGxUjvS.exe
http[:]//89.23.96[.]203/333/urlmon.dll
http[:]//89.23.96[.]203/333/USERENV.dll
http[:]//89.23.96[.]203/333/webio.dll
http[:]//89.23.96[.]203/333/winhttp.dll
http[:]//89.23.96[.]203/333/WININET.dll
http[:]//89.23.96[.]203/333/WINMM.dll
http[:]//89.23.96[.]203/333/WINMMBASE.dll
http[:]//89.23.96[.]203/333/winnlsres.dll
http[:]//89.23.96[.]203/333/xwenxub285p83ecrzvft.exe
http[:]//89.23.96[.]203/333/xwenxub285p83ecrzvft.exe.Config
http[:]//temp.sh/KnCqD/superloop.exe
https[:]//grabify.link/Y33YXP
https[:]//i.ibb.co/2KBydfw/112882618.png
https[:]//i.ibb.co/4g6jH2J/2773036704.png

Web Requests
https[:]//i.ibb.co/b1bZBpg/2615174623.png
https[:]//i.ibb.co/Fxhyq6t/2077411869.png
https[:]//i.ibb.co/HK0jV1G/534475006.png
https[:]//i.ibb.co/nbMNnW4/2501108160.png
https[:]//i.ibb.co/p1RCtpy/2681232755.png
https[:]//i.ibb.co/SxQLwYm/1038436121.png
https[:]//i.ibb.co/v1bn9ZK/369210627.png
https[:]//i.ibb.co/V3Kj1c2/1154761258.png
https[:]//i.ibb.co/X2FR8Kz/2113791011.png
https[:]//i.ibb.com:443/V3Kj1c2/1154761258.png
https[:]//12301230[.]co/npm/module.tripadvisor/module.tripadvisor.css
https[:]//12301230[.]co/npm/module.external/jquery.min.js
https[:]//12301230[.]co/npm/module.external/moment.min.js
https[:]//12301230[.]co/npm/module.external/client.min.js
https[:]//12301230[.]co/npm/module.tripadvisor/module.tripadvisor.js
https[:]//samuelelena[.]co/npm/module.tripadvisor/module.tripadvisor.js
https[:]//samuelelena[.]co/npm/module.external/jquery.min.js
https[:]//samuelelena[.]co/npm/module.external/moment.min.js
https[:]//samuelelena[.]co/npm/module.external/client.min.js
https[:]//samuelelena[.]co/
http[:]//samuelelena[.]co/
https[:]//samuelelena[.]co/npm

Web Requests
https[:]//samuelelena[.]co/npm/module.tripadvisor/module.tripadvisor.js
http[:]//samuelelena[.]co/npm/
http[:]//samuelelena[.]co/npm/module.tripadvisor/module.tripadvisor.js
http[:]//samuelelena[.]co/npm/module.external/client.min.js
https[:]//samuelelena[.]co/npm/module.tripadvisor/module.tripadvisor.
https[:]//samuelelena[.]co/npm/module.external/jquery.min.js
https[:]//samuelelena[.]co/npm/module.external
https[:]//samuelelena[.]co/np
https[:]/samuelelena[.]co/npm/module.tripadvisor/module.tripadvisor.js
https[:]//samuelelena[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.]js
https[:]//samuelelena[.]co/npm/module[.]external/client.min.js
https[:]//samuelelena[.]co/npm/module.external/jquery.min.js
http[:]//samuelelena[.]co:443/
http[:]//samuelelena[.]co/npm/module.external/jquery.min.js
https[:]//40031[.]co/npm/module.tripadvisor/module.tripadvisor.css
https[:]//40031[.]co/npm/module.external/jquery.min.js
https[:]//40031[.]co/npm/module.external/moment.min.js
https[:]//40031[.]co/npm/module.external/client.min.js
https[:]//40031[.]co/npm/module.tripadvisor/module.tripadvisor.js

Table 5: Emails Related to RansomHub (2023-2024)

Email Addresses
brahma2023[@]onionmail.org

Email Addresses
<victim_organization_name>[@]protonmail.com

MITRE ATT&CK Tactics and Techniques

See **Table 6**–**Table 17** for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Table 6: Resource Development

Technique Title	ID	Use
Obtain Capabilities: Exploits	T1588.005	RansomHub affiliates may buy, steal, or download exploits that can be used during targeting.

Table 7: Initial Access

Technique Title	ID	Use
Phishing	T1566	RansomHub affiliates used mass phishing and spear-phishing emails to obtain initial access.
Exploit Public-Facing Application	T1190	RansomHub affiliates may exploit known vulnerabilities to obtain initial access.

Table 8: Execution

Technique Title	ID	Use
Command and Scripting Interpreter	T1059.001	RansomHub affiliates used PowerShell and Scripts to quickly run and automate intrusion.
Windows Management Instrumentation	T1047	RansomHub affiliates may abuse Windows Management Instrumentation to execute malicious commands and payloads.

Table 9: Persistence

Technique Title	ID	Use
Command and Scripting Interpreter	T1059.001	RansomHub affiliates used PowerShell and Scripts to quickly run and automate intrusion.

Technique Title	ID	Use
Create Account	T1136	RansomHub affiliates may create an account to maintain access to victim systems.

Table 10: Privilege Escalation

Technique Title	ID	Use
Account Manipulation	T1098	RansomHub affiliates may manipulate accounts to maintain and/or elevate access to victim systems.
Remote Services: Remote Desktop Protocol	T1021.001	RansomHub affiliates may log onto systems using the Remote Desk Protocol, then perform actions as the logged-on user.

Table 11: Defense Evasion

Technique Title	ID	Use
Masquerading	T1036	RansomHub affiliates may hide binaries by renaming executable names.
Indicator Removal on Host	T1070	RansomHub affiliates may remove logs to inhibit cybersecurity response.
Impair Defenses: Disable or Modify Tools	T1562.001	RansomHub affiliates may disable endpoint detection and response (EDR) tooling to avoid detection.

Table 12: Credential Access

Technique Title	ID	Use
OS Credential Dumping	T1003	RansomHub affiliates used Mimikatz on Windows systems to gather credentials.
Brute Force: Password Spraying	T1110.003	RansomHub affiliates may use password spraying to obtain initial access.

Table 13: Discovery

Technique Title	ID	Use
Remote System Discovery	T1018	RansomHub affiliates may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system.
Network Service Discovery	T1046	RansomHub affiliates may attempt to get a listing of services running on remote hosts and local network infrastructure devices.

Table 14: Lateral Movement

Technique Title	ID	Use
Exploitation of Remote Services	T1210	RansomHub affiliates may exploit remote services to gain unauthorized access to internal systems once inside of a network.

Table 15: Command and Control

Technique Title	ID	Use
Remote Access Software	T1219	RansomHub affiliates may use Anydesk, a legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks.

Table 16: Exfiltration

Technique Title	ID	Use
Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	T1048.002	RansomHub affiliates may steal data by exfiltrating it over an asymmetrically encrypted network protocol other than that of the existing command and control channel.
Transfer Data to Cloud Account	T1537	RansomHub affiliates may exfiltrate data by transferring the data, including through sharing/syncing and creating backups of cloud environments, to another cloud account they control on the same service.

Technique Title	ID	Use
Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Unencrypted Non-C2 Protocol	T1048.003	RansomHub affiliates may steal data by exfiltrating it over an un-encrypted network protocol other than that of the existing command and control channel.

Table 17: Impact

Technique Title	ID	Use
Data Encrypted for Impact	T1486	RansomHub affiliates used encryption for ransomware operations.
Inhibit System Recovery	T1490	RansomHub ransomware deleted volume shadow copies and affiliates removed backups for ransomware operations.

Incident Response

If compromise is detected, organizations should:

1. Quarantine or take potentially affected hosts offline.
2. Reimage compromised hosts.
3. Provision new account credentials.
4. Collect and review artifacts such as running processes/services, unusual authentications, and recent network connections.
5. Report the compromise to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870). State, local, tribal, or territorial government entities can also report to the Multi-State Information Sharing and Analysis Center (MS-ISAC) (SOC@cisecurity.org or 866-787-4722).

Mitigations

Network Defenders

The authoring organizations recommend organizations implement the mitigations below to improve cybersecurity posture based on RansomHub's activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).
- **Require all accounts** with password logins (e.g., service accounts, admin accounts, and domain admin accounts) to comply with National Institute for Standards and Technology (NIST) standards for developing and managing password policies.
  - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length;
  - Store passwords in hashed format using industry-recognized password managers;
  - Add password user "salts" to shared login credentials;
  - Avoid reusing passwords;
  - Implement multiple failed login attempt account lockouts;
  - Disable password "hints"; and
  - Refrain from requiring password changes more frequently than once per year.

    Note: NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
  - Require administrator credentials to install software.
- **Keep all operating systems, software, and firmware up to date** [CPG 1.E]. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities in internet-facing systems.
- **Require Phishing-Resistant multifactor authentication to administrator accounts** [CPG 2.H] and require standard MFA for all services to the extent possible (particularly for webmail, virtual private networks, and accounts that access critical systems).
- **Segment networks** [CPG 2.F] to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool** [CPG 3.A]. To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Install, regularly update, and enable real time detection for antivirus software on all hosts.**
- **Implement Secure Logging Collection and Storage Practices** [CPG 2.T]. Learn more about logging best practices by referencing CISA's Logging Made Easy resources.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts.
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege.

- **Disable unused ports.**
- **Implement and enforce email security policies** [CPG 2.M].
- **Disable macros by default** [CPG 2.N].
- **Consider adding an email banner to emails** received from outside your organization.
- **Disable hyperlinks in received emails.**
- **Implement time-based access for accounts set at the admin level and higher.** For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- **Disable command-line and scripting activities and permissions.** Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- **Maintain offline backups of data, and regularly maintain backup and restoration** [CPG 2.R]. By instituting this practice, the organization ensures they will not be severely interrupted, and/or only have irretrievable data.
- **Ensure all backup data is encrypted,** immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure.

Software Manufacturers

The above mitigations apply to enterprises and critical infrastructure organizations with on-premises or hybrid environments. Recognizing that insecure software is the root cause of many of these flaws and that the responsibility should not be on the end user, CISA urges software manufacturers to implement the following to reduce the prevalence of identified or exploited issues (e.g., misconfigurations, weak passwords, and other weaknesses identified and exploited through the assessment team):

- **Embed security into product architecture** throughout the entire software development lifecycle (SDLC).
- **Mandate MFA, ideally phishing-resistant MFA, for privileged users** and make MFA a default, rather than opt-in, feature.

These mitigations align with tactics provided in the joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. CISA urges software manufacturers to take ownership of improving the security outcomes of their customers by applying these and other secure by design tactics. By using secure by design tactics, software manufacturers can make their product lines secure "out of the box" without requiring customers to spend additional resources making configuration changes, purchasing security software and logs, monitoring, and making routine updates.

For more information on secure by design, see CISA's Secure by Design webpage.

Validate Security Controls

In addition to applying mitigations, CISA recommends exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring organizations recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 6–Table 17**).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA, FBI, MS-ISAC, and HHS recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Resources

- #StopRansomware is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- Resource to reduce the risk of a ransomware attack: #StopRansomware Guide.
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment.
- Health and Human Services HPH Cybersecurity Gateway hosts the HPH CPGs and links to HHS cybersecurity resources.

References

1. Ransomware Roundup - Knight | FortiGuard Labs (fortinet.com)
2. Knight Ransomware - X-Industry - Red Sky Alliance
3. Cyclops Ransomware and Stealer Combo: Exploring a Dual Threat (uptycs.com)
4. Knight ransomware distributed in fake Tripadvisor complaint emails (bleepingcomputer.com)

Reporting

Your organization has no obligation to respond or provide information to the FBI in response to this joint advisory. If, after reviewing the information provided, your organization decides to provide information to the FBI, reporting must be consistent with applicable state and federal laws.

The FBI is interested in any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with threat actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

Additional details of interest include a targeted company point of contact, status and scope of infection, estimated loss, operational impact, transaction IDs, date of infection, date detected, initial attack vector, and host- and network-based indicators.

The authoring organizations do not encourage paying a ransom, as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to the FBI's Internet Crime Complain Center (IC3), a local FBI Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center (report@cisa.gov) or by calling 1-844-Say-CISA (1-844-729-2472).

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring organizations.