Malware Spotlight: **RansomHub Ransomware**

January 2025

Executive Summary

In 2024, Arete's Incident Response (IR) team responded to dozens of incidents attributed to the RansomHub threat actor group. Engagements attributed to RansomHub increased rapidly since Arete first observed them in May 2024, and the group quickly established itself as one of the top three threat actor groups since July 2024.

RansomHub has impacted multiple sectors across Arete engagements, including professional services, public services, healthcare, high technology, financial services, and manufacturing. The group has targeted several high-profile targets since its emergence, including telecom giant Frontier and British auction house Christie's. RansomHub also claimed to possess data stolen from Change Healthcare, which was the victim of an ALPHV/BlackCat ransomware attack in February 2024. RansomHub announced the sale of Change's data after leaking some of the alleged data a day beforehand.

Advertisements for the RansomHub Ransomware-as-a-Service (RaaS) appeared on cybercriminal forums on February 2, 2024, highlighting an encryptor developed using the C++ and Go programming languages. The use of Go makes it easier for ransomware groups to target a wide variety of operating systems without needing to rewrite significant portions of the malware, as Go allows developers to compile executables for Windows, Linux, and macOS platforms from a single codebase. These advertisements were accompanied by a new data leak site (DLS) under the RansomHub branding on the dark web.

RansomHub is suspected to be a re-brand of the "Knight" ransomware group, whose source code was listed for sale on the underground RAMP forum on February 18, 2024. From research, Arete can confirm various similarities between RansomHub and Knight's encryptors.

This spotlight explores the ransomware group's observed behavior, background information on the threat actor, and statistics from Incident Response engagements, along with a technical analysis of RansomHub's ransomware executable. Finally, we discuss security recommendations to better defend against this evolving cyber threat and mitigate the risk of financial and reputational losses.

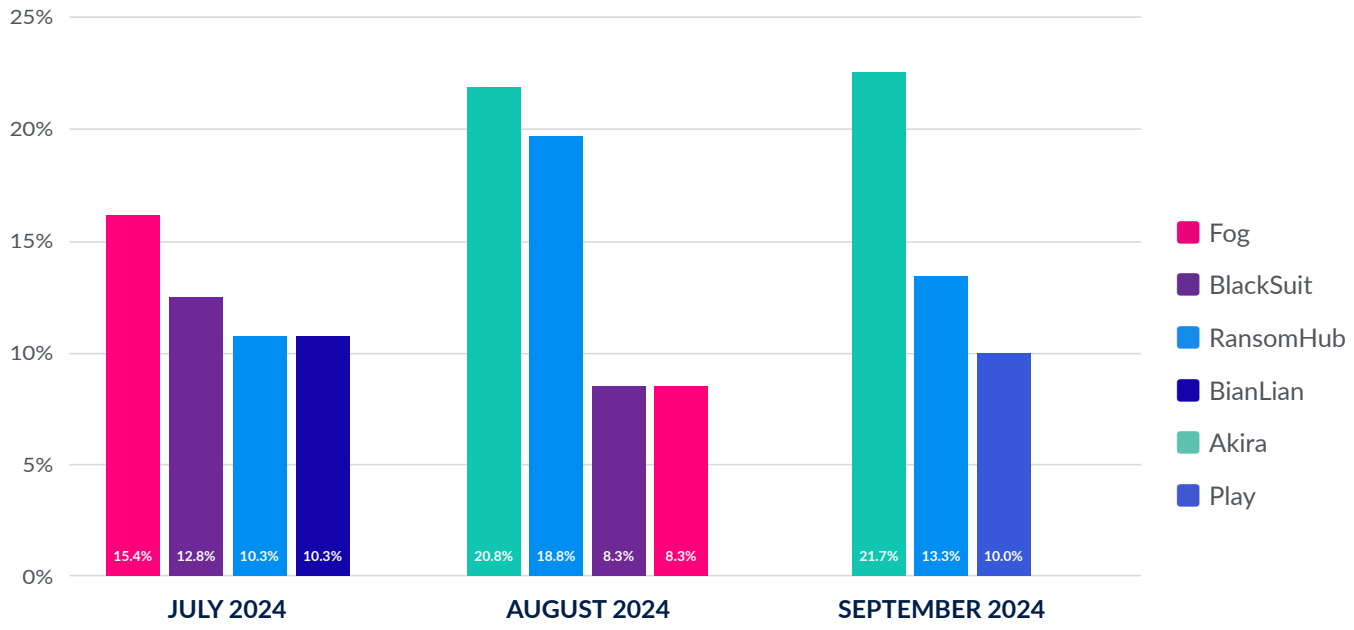
Incident Response Data on the RansomHub Ransomware Group

The information provided below is based on engagements involving the RansomHub threat actor group investigated by Arete in 2024. Our IR, Threat Intelligence, and Data Analytics teams work together to analyze key data points during every ransomware engagement and form real-time threat actor (TA) insights.

- Targeted sectors include professional services, public services, healthcare, high technology, financial services, and manufacturing.
- The median initial ransom demand is $900,000.
- The median ransom payment facilitated is $350,000.
- Tools and malware observed during investigations include SocGholish, CobaltStrike, Mimikatz, Rclone, Filezilla, WinSCP, PsExec, AnyDesk, PuTTY, WinSCP, Rclone, SoftPerfect Network Scanner, and TDSSKiller and EDRKillShifter to disable EDR software to evade detection.
- RansomHub-affiliated actors have exploited vulnerabilities in a variety of technologies, including Apache ActiveMQ, Atlassian Confluence, Citrix ADC, F5 BIG-IP, and Fortinet FortiOS.
- The group operates a data leak site (DLS) self-proclaimed as "RansomHub" and commonly threatens victims with releasing stolen data as a pressure tactic if a payment is not made.
- The file extension appended to encrypted files is created based on the first six characters of the Curve 25519 public key, and files are encrypted using a decrypted Curve 25519 public key and AES algorithms.
- The ransom note created self-identifies the group as RansomHub and references their data leak and chat negotiation sites. The filename of the ransom note is dependent on the encrypted file extension as a naming convention and follows this format: “README_<encrypte_file_extension>.txt”. For example: README_11f5ew.txt.
- In addition to encrypting files and creating a ransom note, the RansomHub ransomware needs a password to properly execute, supports various command line arguments, deletes volume shadow copies, clears the Windows Event Logs, and tries to stop virtual machines (VMs).

Background

RansomHub became a notable ransomware operation in 2024, and, alongside Akira, represented a very significant percentage of Arete Incident Response engagements in Q3 of 2024.



Source: Arete's Q3 2024 Crimeware Report

The group utilizes both Windows and Linux variants of encryptors, which increases its operational capability to target a wide range of victims of various sectors and sizes. RansomHub operates under a double extortion model, which involves exfiltrating sensitive data and encrypting the victims' systems to coerce a payment for a decryptor and data deletion.

Technical Analysis

Malware analysis revealed that RansomHub ransomware:

- Supports multiple command-line arguments.
- Requires a password to properly execute and encrypt files.
- Encrypts files on the system and mounted shares.
- Creates a ransom note with the following filename: .README_<encrypted_file_extension>.txt
- Self-identifies the group as RansomHub in the ransom note.
- References a data leak site in the ransom note that, when accessed, self-identifies the group as RansomHub.
- Kills a list of processes and services.
- Maintains a list of whitelisted files and directories to make sure it will not render the system unusable, preventing recovery when running a decryptor.
- Attempts to prevent system recovery by deleting the system's volume shadow copies.
- Clears the Windows event logs.
- Creates a desktop wallpaper image in the "%temp%\" directory and later modifies a registry key to change desktop wallpaper.

Execution Pattern/Arguments

The RansomHub ransomware needs command line arguments to execute and encrypt files in the system. Command line arguments supported:

Command line arguments	Description
-cmd	CMD to be executed before encryption.
-disable-net	Disable network before running.
-fast	Fast encryption mode.
-file *value*	Only process file inside defined files. For example, -file C://1.txt, -file D://2.txt.
-host *value*	Only process net share inside defined hosts. -host 10.10.10.10 -host 10.10.10.11.
-only-local	Only encrypt local disks.
-pass *[SHA256 string]*	Password needed to execute the ransomware. A 64-character string.
-path *value*	Only process files inside defined paths. -path C:// -path D:// -path //10.10.10.10/d/
-safeboot	Reboot in Safe Mode before running.
-safeboot-instance	Run as Safe Mode instance.
-skip-vm *value*	Skip shutting down VMs. Example: -skip-vm "Ubuntu 22.04 LTS", -skip-vm "Windows Server 2012".
-sleep *[integer value]*	Sleep for a period of time to run (minute).
-verbose	Log to console.

Ransomware execution with the command line argument –help:

```
C:\Users\Akxy>C:\Users\Akxy\Desktop\RansomHub.exe -help
USAGE: C:\Users\Akxy\Desktop\RansomHub.exe [OPTIONS]
OPTIONS:
  -cmd string
        cmd to be executed before encryption
  -disable-net
        disable network before running
  -fast
        fast encryption mode
  -file value
        only process file inside defined files. -file C://1.txt -file D://2.txt
  -host value
        only process net share inside defined hosts. -host 10.10.10.10 -host 10.10.10.11
  -no-folder-filter
        *
  -only-local
        only encryption local disks
  -pass string
        run pass
  -path value
        only process files inside defined paths. -path C:// -path D:// -path //10.10.10.10/d/
  -safeboot
        reboot in Safe Mode before running
  -safeboot-instance
        run as Safe Mode instance
  -skip-vm value
        skip shutting down VMs. -skip-vm "Ubuntu 22.04 LTS" -skip-vm "Windows Server 2012"
  -sleep int
        sleep for a period of time to run (minute)
  -verbose
        log to console
```

Figure 1. Command line arguments supported by the ransomware

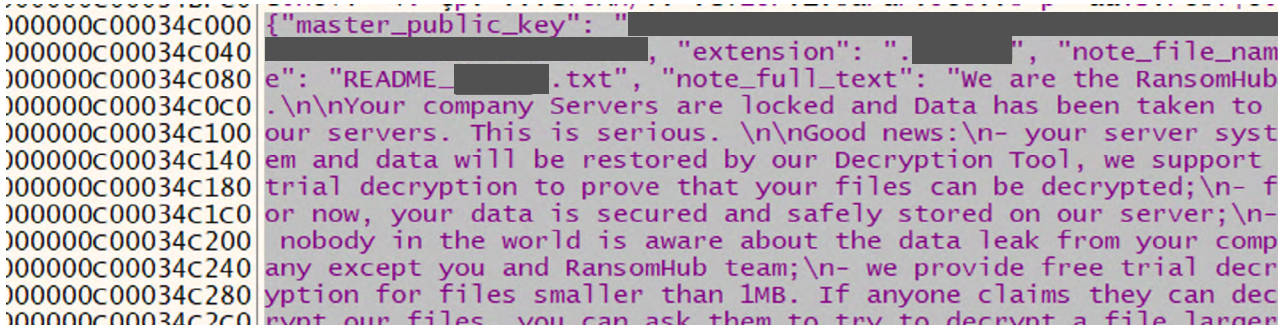
The ransomware will not execute in the system without the “-pass” argument followed by a SHA-256 value that is unique in each engagement.

Execution of ransomware to encrypt files:

```
RansomHub.exe -pass [SHA-256]

Example:
RansomHub.exe -pass
7ac8cd689f5d9f4c1ddca14ec84965ed42b17343ebe086076ba0e7a46a80f81f
```

Once the SHA-256 password value is provided, the ransomware will decrypt a JSON based ransomware configuration at the run time.



Decrypted JSON field name and descriptions:

Name	Description
master_public_key	Curve25519 public key used in the file encryption process.
extension	Extension added to encrypted files.
note_file_name	Ransom note file name, default value is .README<encrypted_file_extension>.txt
note_full_text	Ransom note content.
settings	Ransomware operation setting. Example: {"local_disks": true, "network_shares": true, "kill_processes": true, "kill_services": true, "set_wallpaper": true, "net_spread": true, "self_delete": false, "running_one": true}
credentials	Contains common or locally stolen credentials which are used for propagation and further infection.
kill_services	Terminates list of services.
kill_processes	Terminates list of processes.
white_folders	Excludes listed directories.
white_files	Excludes listed files.
white_hosts	Excludes listed hosts.

Stop Services and Processes

Before file encryption, the ransomware terminates a pre-determined list of processes and services to encrypt as many files as possible.

Process names:

"agntsvc.exe", "dbeng50.exe", "dbsnmp.exe", "encsvc.exe", "excel.exe", "firefox.exe", "infopath.exe", "isqlplussvc.exe", "msaccess.exe", "mspub.exe", "mydesktopqos.exe", "mydesktopservice.exe", "notepad.exe", "ocautoupds.exe", "ocomm.exe", "ocssd.exe", "onenote.exe", "oracle.exe", "outlook.exe", "powerpnt.exe", "sqbcoreservice.exe", "sql.exe", "steam.exe", "synctime.exe", "tbirdconfig.exe", "thebat.exe", "thunderbird.exe", "visio.exe", "winword.exe", "wordpad.exe", "xfssvccon.exe", "*sql*.exe", "bedbh.exe", "vxmon.exe", "benetns.exe", "bengien.exe", "pvlsvr.exe", "beserver.exe", "raw_agent_svc.exe", "vsnapvss.exe", "CagService.exe", "QBIDPService.exe", "QBDBMgrN.exe", "QBCFMonitorService.exe", "SAP.exe", "TeamViewer_Service.exe", "TeamViewer.exe", "tv_w32.exe", "tv_x64.exe", "CVMountd.exe", "cvd.exe", "cvfwd.exe", "CVODS.exe", "saphostexec.exe", "saposcol.exe", "sapstartsrv.exe", "avagent.exe", "avscc.exe", "DellSystemDetect.exe", "EnterpriseClient.exe", "VeeamNFSSvc.exe", "VeeamTransportSvc.exe", "VeeamDeploymentSvc.exe"

Service names:

"mepocs", "memtas", "veeam", "svc$", "backup", "sql", "vss", "sql$", "mysql", "mysql$", "sophos", "MSExchange", "MSExchange$", "WSBExchange", "PDVFSService", "BackupExecVSSProvider", "BackupExecAgentAccelerator", "BackupExecAgentBrowser", "BackupExecDiveciMediaService", "BackupExecJobEngine", "BackupExecManagementService", "BackupExecRPCService", "GxBlr", "GxVss", "GxCIMgrS", "GxCVD", "GxCIMgr", "GXMMM", "GxVssHWProv", "GxFWD", "SAPService", "SAP", "SAP$", "SAPD$", "SAPHostControl", "SAPHostExec", "QBCFMonitorService", "QBDBMgrN", "QBIDPService", "AcronisAgent", "VeeamNFSSvc", "VeeamDeploymentService", "VeeamTransportSvc", "MVArmor", "MVarmor64", "VSNAPVSS", "AcrSch2Svc"

The ransomware also tries to list and stop VMs by executing the following PowerShell command.

```
powershell.exe -Command PowerShell -Command "{ Get-VM | Stop-VM -Force }"
```

```
powershell.exe Get-VM | Stop-VM -Force -inputFormat xml -outputFormat text
```

File and Directory Exclusions

The ransomware excludes system-related files and folders, ransomware-related files, and whitelisted extensions during encryption.

Excluded file and extensions:

"NTUSER.DAT", "autorun.inf", "boot.ini", "desktop.ini", "thumbs.db", "*.deskthemepack", "*.themepack", "*.theme", "*.msstyles", "*.exe", "*.drv", "*.msc", "*.dll", "*.lock", "*.sys", "*.msu", "*.lnk", "*.ps1", "*.iso", "*.inf", "*.cab", "*.386"

Excluded directories:

```
"*\\$windows.~ws*", "*\\$windows.~bt*", "*\\windows\\*", "*\\windows.old*", "*\\system volume information*",
"*\\Boot*", "*\\PerfLogs*", "*\\AppData\\Local\\Temp*", "*\\AppData\\Local\\Microsoft\\GameDVR*", "*\\
AppData\\Local\\Microsoft\\Edge*", "*\\AppData\\Local\\Packages\\Microsoft.*", "*\\AppData\\Local\\Packages\\
MicrosoftWindows.*", "*\\AppData\\Local\\Packages\\Internet Explorer*", "*\\Program Files\\Common Files\\microsoft
shared*", "*\\Program Files\\Common Files\\Services*", "*\\Program Files\\Common Files\\System*", "*\\Program
Files\\Internet Explorer*", "*\\Program Files\\ModifiableWindowsApps*", "*\\Program Files\\Uninstall Information*",
"*\\Program Files\\Windows Defender*", "*\\Program Files\\Windows Mail*", "*\\Program Files\\Windows Media
Player*", "*\\Program Files\\Windows NT*", "*\\Program Files\\Windows Photo Viewer*", "*\\Program Files\\Windows
Portable Devices*", "*\\Program Files\\Windows Security*", "*\\Program Files\\Windows Sidebar*", "*\\Program Files\\
WindowsApps*", "*\\Program Files\\WindowsPowerShell*", "*\\Program Files (x86)\\Common Files*", "*\\Program Files
(x86)\\Common Files\\Microsoft Shared*", "*\\Program Files (x86)\\Common Files\\Services*", "*\\Program Files (x86)\\
Common Files\\System*", "*\\Program Files (x86)\\Internet Explorer*", "*\\Program Files (x86)\\Microsoft\\*Edge*",
"*\\Program Files (x86)\\Microsoft\\Temp*", "*\\Program Files (x86)\\Microsoft.NET*", "*\\Program Files (x86)\\
Windows Defender*", "*\\Program Files (x86)\\Windows Mail*", "*\\Program Files (x86)\\Windows Media Player*",
"*\\Program Files (x86)\\Windows Multimedia Platform*", "*\\Program Files (x86)\\Windows NT*", "*\\Program Files
(x86)\\Windows Photo Viewer*", "*\\Program Files (x86)\\Windows Portable Devices*", "*\\Program Files (x86)\\
Windows Security*", "*\\Program Files (x86)\\Windows Sidebar*", "*\\Program Files (x86)\\WindowsPowerShell*", "*\\
ProgramData\\ssh\\*", "*\\ProgramData\\USOPrivate*", "*\\ProgramData\\USOShared*", "*\\ProgramData\\Package
Cache*", "*\\ProgramData\\Microsoft\\Device Stage*", "*\\ProgramData\\Microsoft\\DeviceSync*", "*\\ProgramData\\
Microsoft\\Diagnosis*", "*\\ProgramData\\Microsoft\\DiagnosticLogCSP*", "*\\ProgramData\\Microsoft\\DRM*", "*\\
ProgramData\\Microsoft\\UEV*", "*\\ProgramData\\Microsoft\\EdgeUpdate*", "*\\ProgramData\\Microsoft\\Event
Viewer*", "*\\ProgramData\\Microsoft\\IdentityCRL", "*\\ProgramData\\Microsoft\\MapData*", "*\\ProgramData\\
Microsoft\\MF*", "*\\ProgramData\\Microsoft\\NetFramework*", "*\\ProgramData\\Microsoft\\Network*", "*\\
ProgramData\\Microsoft\\Provisioning*", "*\\ProgramData\\Microsoft\\Search*", "*\\ProgramData\\Microsoft\\
SmsRouter*", "*\\ProgramData\\Microsoft\\Spectrum*", "*\\ProgramData\\Microsoft\\Speech_OneCore*", "*\\
ProgramData\\Microsoft\\Storage Health*", "*\\ProgramData\\Microsoft\\User Account Pictures*", "*\\ProgramData\\
Microsoft\\Vault*", "*\\ProgramData\\Microsoft\\WDF*", "*\\ProgramData\\Microsoft\\Windows*", "*\\ProgramData\\
Microsoft\\Windows Defender*", "*\\ProgramData\\Microsoft\\Windows NT*", "*\\ProgramData\\Microsoft\\
Windows Security Health*", "*\\ProgramData\\Microsoft\\WinMSIPC*", "*\\ProgramData\\Microsoft\\WPD*", "*\\
ProgramData\\Packages\\USOPrivate*", "*\\ProgramData\\Packages\\USOShared*", "*\\ProgramData\\Packages\\
WindowsHolographicDevices*", "*\\ProgramData\\Packages\\MicrosoftWindows.*", "*\\ProgramData\\Packages\\
Microsoft.*"
```

Inhibit System Recovery

Windows operating systems contain features that can help fix corrupted system files, including shadow copies, which are backups of files created by the Volume Shadow Copy Service (VSS). By deleting shadow copies, the ransomware can prevent victims from restoring files from backups, making it more difficult for them to recover their data without paying the ransom.

The ransomware deletes volume shadow copies before file encryption by starting the following process:

```
powershell.exe -Command PowerShell -Command "\"Get-CimInstance Win32_ShadowCopy | Remove-CimInstance\""
```

System Network Connections Discovery

The ransomware can enumerate network-mounted shares by scanning the network interfaces.

Data Encrypted for Impact

The ransomware initially finds available drives, then loads the files one by one using the Windows API “FindFirstFileW“ and “FindNextFileW”. The ransomware generates random keys to encrypt the files, and after encrypting them, the keys are encrypted using a public key. To encrypt files, the ransomware uses a combination of a decrypted Curve 25519 public key and AES algorithms.

The default extension value is the first six characters of the Curve 25519 public key.

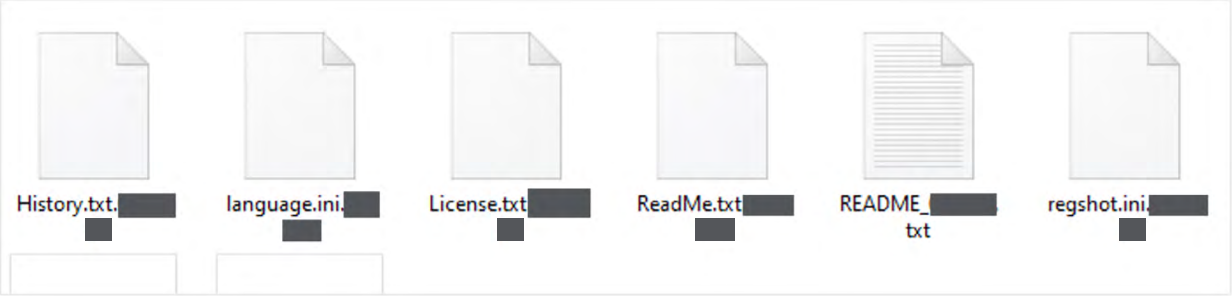


Figure 2. Extension added to the encrypted files

Files smaller than 0x100000 bytes are completely encrypted. If the file size is larger than 0x100000 bytes, the ransomware encrypts the file in 0x100000 bytes blocks and skips every 0x200000 bytes of data in between encrypted chunks.

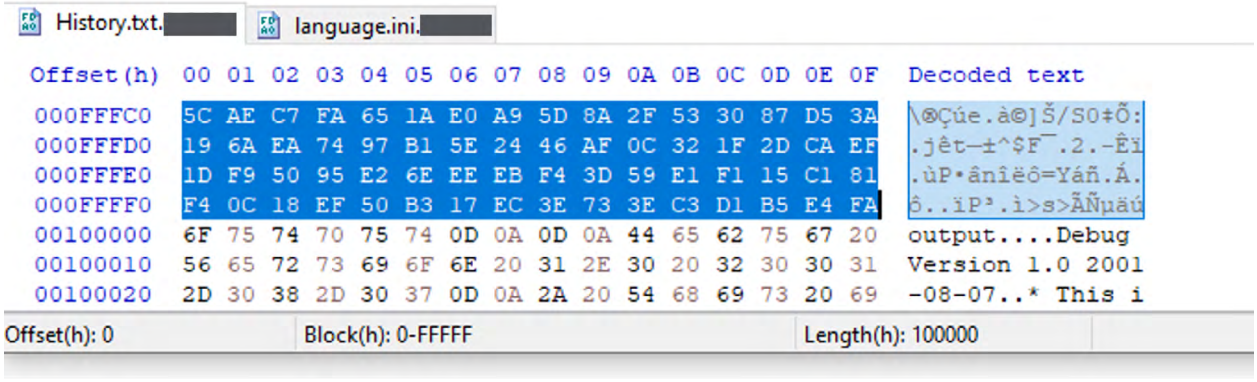


Figure 3. 0x100000 bytes encrypted file.

Upon successful execution, the ransomware creates ransom notes with the file name "README_<encrypted_file_extension>.txt"

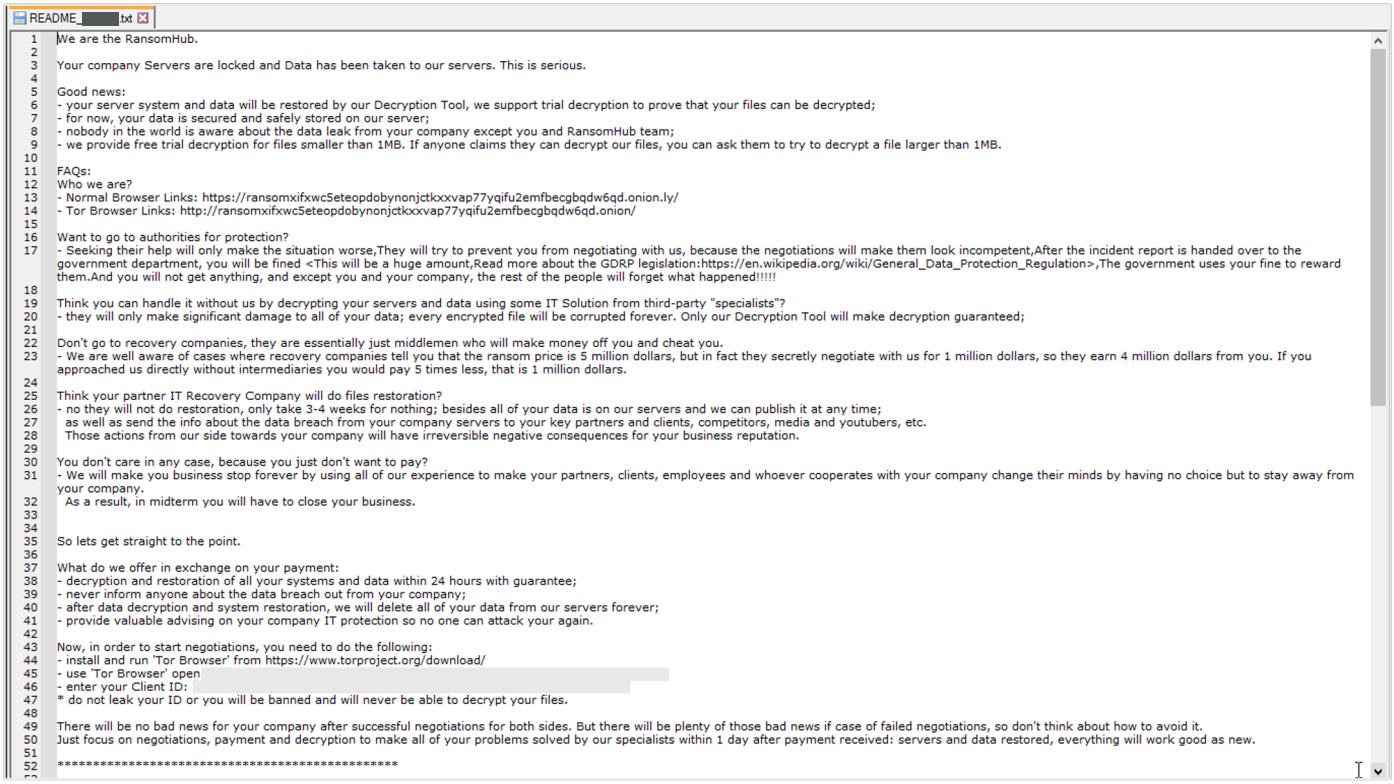


Figure 4. RansomHub ransom note

Ransom note content:

We are the RansomHub.

Your company Servers are locked and Data has been taken to our servers. This is serious.

Good news:
- your server system and data will be restored by our Decryption Tool, we support trial decryption to prove that your files can be decrypted;
- for now, your data is secured and safely stored on our server;
- nobody in the world is aware about the data leak from your company except you and RansomHub team;
- we provide free trial decryption for files smaller than 1MB. If anyone claims they can decrypt our files, you can ask them to try to decrypt a file larger than 1MB.

FAQs:
Who we are?
- Normal Browser Links: https://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion.ly/
- Tor Browser Links: http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion/

Want to go to authorities for protection?
- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because the negotiations will make them look incompetent,After the incident report is handed over to the government department, you will be fined <This will be a huge amount,Read more about the GDRP legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward them.And you will not get anything, and except you and your company, the rest of the people will forget what happened!!!!!

Think you can handle it without us by decrypting your servers and data using some IT Solution from third-party "specialists"?
- they will only make significant damage to all of your data; every encrypted file will be corrupted forever. Only our Decryption Tool will make decryption guaranteed;

Don't go to recovery companies, they are essentially just middlemen who will make money off you and cheat you.
- We are well aware of cases where recovery companies tell you that the ransom price is 5 million dollars, but in fact they secretly negotiate with us for 1 million dollars, so they earn 4 million dollars from you. If you approached us directly without intermediaries you would pay 5 times less, that is 1 million dollars.

Think your partner IT Recovery Company will do files restoration?
- no they will not do restoration, only take 3-4 weeks for nothing; besides all of your data is on our servers and we can publish it at any time;
as well as send the info about the data breach from your company servers to your key partners and clients, competitors, media and youtubers, etc.
Those actions from our side towards your company will have irreversible negative consequences for your business reputation.

You don't care in any case, because you just don't want to pay?
- We will make you business stop forever by using all of our experience to make your partners, clients, employees and whoever cooperates with your company change their minds by having no choice but to stay away from your company.
As a result, in midterm you will have to close your business.

So lets get straight to the point.

What do we offer in exchange on your payment:
- decryption and restoration of all your systems and data within 24 hours with guarantee;
- never inform anyone about the data breach out from your company;
- after data decryption and system restoration, we will delete all of your data from our servers forever;
- provide valuable advising on your company IT protection so no one can attack your again.

Now, in order to start negotiations, you need to do the following:
- install and run 'Tor Browser' from https://www.torproject.org/download/
- use 'Tor Browser' open <TA_URL_removed_by_analyst>.onion/
- enter your Client ID: <ID_removed_by_analyst>
* do not leak your ID or you will be banned and will never be able to decrypt your files.

There will be no bad news for your company after successful negotiations for both sides. But there will be plenty of those bad news if case of failed negotiations, so don't think about how to avoid it.
Just focus on negotiations, payment and decryption to make all of your problems solved by our specialists within 1 day after payment received: servers and data restored, everything will work good as new.

****

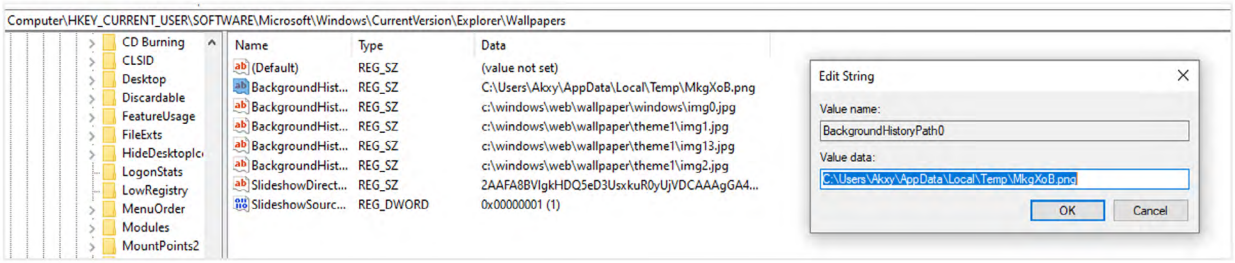
Modify Registry

The ransomware performs a registry key modification to change the desktop wallpaper.

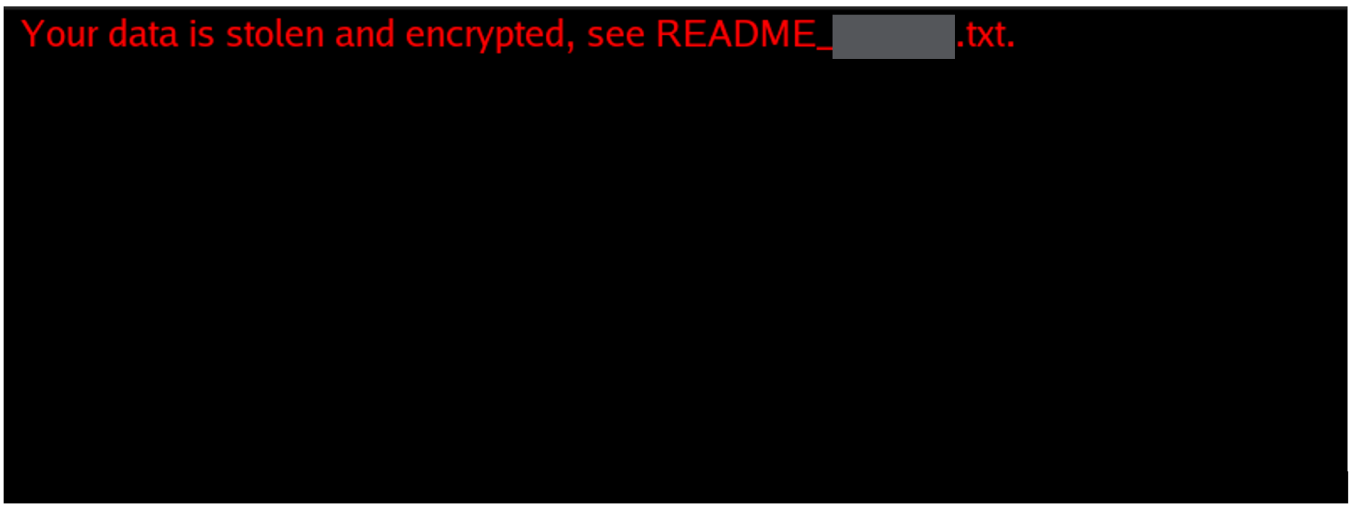
Registry key change:

Registry key	Value name	Value data
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers	BackgroundHistoryPath0	C:\Users\%USERNAME%\AppData\Local\Temp\MkgXoB.png

Screenshot showing the registry key modification:



Wallpaper image content from the C:\Users\%USERNAME%\AppData\Local\Temp\MkgXoB.png file:



Mutex

The mutex is the fundamental tool for managing shared resources between multiple threads or processes. Typically, ransomware uses a mutex to avoid reinfecting the victim system and causing multiple layers of encryption. The ransomware did not create a mutex during execution.

Network Activity

The ransomware did not try to communicate with a remote server other than encrypting data from mounted shares.

Indicator Removal

The ransomware clears Windows Event Logs to hide its malicious activity. Windows Event Logs keep a record of a computer's alerts and notifications. The ransomware runs the following commands to clear the logs:

```
cmd.exe /c wevtutil cl security
cmd.exe /c wevtutil cl system
cmd.exe /c wevtutil cl application
```

File and Directory Permissions Modification

The ransomware uses the fsutil tool to redirect file system access to a different location after gaining access to a compromised network. The ransomware uses the following command line to redirect file system access, enabling remote to remote and remote to local symbolic links:

```
fsutil behavior set SymlinkEvaluation R2L:1
fsutil behavior set SymlinkEvaluation R2R:1
```

Indicators of Compromise

Indicator	Type	Context
de7913504efe4584bdd9dd1ec13c4de4152a84df5e1cb-c31d0dd8fe70c88b5e0 4ac0e6c804f638182ee8e23c37e0c474a22f8bc2b3eed5ac-c0a56764839e4106 83654c500c68418142e43b31ebbec040d9d36cfbbe08c7b9b-3dc90fabc14801a eaee06cb53ff473f32d02ad1aca38957812b394f69dd0a3d2af-16f2d923b10e3	SHA256 hash	RansomHub ransomware
README_<encrypted_file_extension>.txt	File name	RansomHub ransom note
powershell.exe -Command PowerShell -Command "{ Get-VM | Stop-VM -Force }"	Process	Retrieve information about VMs and forces a shutdown
powershell.exe -Command PowerShell -Command "\"Get-CimInstance Win32_ShadowCopy | Remove-CimIn-stance\"" cmd.exe /c "\"vssadmin.exe Delete Shadows /all /quiet\""	Process	Volume Shadow Copy deletion
cmd.exe /c wevtutil cl security cmd.exe /c wevtutil cl system cmd.exe /c wevtutil cl application	Process	Clearing Windows Event Logs
cmd.exe /c "\"fsutil behavior set SymlinkEvaluation R2L:1\"" cmd.exe /c "\"fsutil behavior set SymlinkEvaluation R2R:1\""	Process	Enable remote to remote and remote to local symbolic links

Key: Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers Value: BackgroundHistoryPath0 Data: C:\Users\%USERNAME%\AppData\Local\Temp\MkgXoB.png	Registry	Desktop wallpaper modification
ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecg-bqdw6qd[.]onion	URL	TA data leak site (DLS)

Ransomware Configuration

RansomHub decrypted configuration information extracted:

{"**master_public_key**": *<public_key_removed_by_analyst>*, "**extension**": ".*<extension_removed_by_analyst>*", "**note_file_name**": "README_*<encrypted_file_extension>*.txt", "**note_full_text**": "We are the RansomHub.\n\nYour company Servers are locked and Data has been taken to our servers. This is serious. \n\nGood news:\n- your server system and data will be restored by our Decryption Tool, we support trial decryption to prove that your files can be decrypted;\n- for now, your data is secured and safely stored on our server;\n- nobody in the world is aware about the data leak from your company except you and RansomHub team;\n- we provide free trial decryption for files smaller than 1MB. If anyone claims they can decrypt our files, you can ask them to try to decrypt a file larger than 1MB.\n\nFAQs:\nWho we are?\n- Normal Browser Links: https://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/\n- Tor Browser Links: http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/\n\nWant to go to authorities for protection?\n- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because the negotiations will make them look incompetent,After the incident report is handed over to the government department, you will be fined <This will be a huge amount,Read more about the GDRP legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward them.And you will not get anything, and except you and your company, the rest of the people will forget what happened!!!!!\n\nThink you can handle it without us by decrypting your servers and data using some IT Solution from third-party \"specialists\"?\n- they will only make significant damage to all of your data; every encrypted file will be corrupted forever. Only our Decryption Tool will make decryption guaranteed; \n\nDon't go to recovery companies, they are essentially just middlemen who will make money off you and cheat you. \n- We are well aware of cases where recovery companies tell you that the ransom price is 5 million dollars, but in fact they secretly negotiate with us for 1 million dollars, so they earn 4 million dollars from you. If you approached us directly without intermediaries you would pay 5 times less, that is 1 million dollars.\n\nThink your partner IT Recovery Company will do files restoration? \n- no they will not do restoration, only take 3-4 weeks for nothing; besides all of your data is on our servers and we can publish it at any time; \n as well as send the info about the data breach from your company servers to your key partners and clients, competitors, media and youtubers, etc. \n Those actions from our side towards your company will have irreversible negative consequences for your business reputation.\n\nYou don't care in any case, because you just don't want to pay? \n- We will make you business stop forever by using all of our experience to make your partners, clients, employees and whoever cooperates with your company change their minds by having no choice but to stay away from your company. \n As a result, in midterm you will have to close your business. \n\n\nSo lets get straight to the point.\n\nWhat do we offer in exchange on your payment:\n- decryption and restoration of all your systems and data within 24 hours with guarantee;\n- never inform anyone about the data breach out from your company;\n- after data decryption and system restoration, we will delete all of your data from our servers forever;\n- provide valuable advising on your company IT protection so no one can attack your again.\n\nNow, in order to start negotiations, you need to do the following: \n- install and run 'Tor Browser' from https://www.torproject.org/download/\n- use 'Tor Browser' open *<TA_URL_removed_by_analyst>* n- enter your Client ID: %s\n* do not leak your ID or you will be banned and will never be able to decrypt your files.\n\nThere will be no bad news for your company after successful negotiations for both sides. But there will be plenty of those bad news if case of failed negotiations, so don't think about how to avoid it.\nJust focus on negotiations, payment and decryption to make all of your problems solved by our specialists within 1 day after payment received: servers and data restored, everything will work good as new.\n\n**********\n**********\n", "**note_short_text**": "Your data is stolen and encrypted, see README_*<extension_*

removed_by_analyst>.txt.", "**settings**": {"**local_disks**": true, "**network_shares**": true, "**kill_processes**": true, "**kill_services**": true, "**set_wallpaper**": true, "**net_spread**": true, "**self_delete**": false, "**running_one**": true}, "**credentials**": [*<credentials_removed_by_analyst>*], "**kill_services**": ["mepocs", "memtas", "veeam", "svc$", "backup", "sql", "vss", "sql$", "mysql", "mysql$", "sophos", "MSExchange", "MSExchange$", "WSBExchange", "PDVFSService", "BackupExecVSSProvider", "BackupExecAgentAccelerator", "BackupExecAgentBrowser", "BackupExecDiveciMediaService", "BackupExecJobEngine", "BackupExecManagementService", "BackupExecRPCService", "GxBlr", "GxVss", "GxClMgrS", "GxCVD", "GxCIMgr", "GXMMM", "GxVssHWProv", "GxFWD", "SAPService", "SAP", "SAP$", "SAPD$", "SAPHostControl", "SAPHostExec", "QBCFMonitorService", "QBDBMgrN", "QBIDPService", "AcronisAgent", "VeeamNFSSvc", "VeeamDeploymentService", "VeeamTransportSvc", "MVArmor", "MVarmor64", "VSNAPVSS", "AcrSch2Svc"], "**kill_processes**": ["agntsvc.exe", "dbeng50.exe", "dbsnmp.exe", "encsvc.exe", "excel.exe", "firefox.exe", "infopath.exe", "isqlplussvc.exe", "msaccess.exe", "mspub.exe",

"mydesktopqos.exe", "mydesktopservice.exe", "notepad.exe", "ocautoupds.exe", "ocomm.exe", "ocssd.exe", "onenote.exe", "oracle.exe", "outlook.exe", "powerpnt.exe", "sqbcoreservice.exe", "sql.exe", "steam.exe", "synctime.exe", "tbirdconfig.exe", "thebat.exe", "thunderbird.exe", "visio.exe", "winword.exe", "wordpad.exe", "xfssvccon.exe", "*sql*.exe", "bedbh.exe", "vxmon.exe", "benetns.exe", "bengien.exe", "pvlsvr.exe", "beserver.exe", "raw_agent_svc.exe", "vsnapvss.exe", "CagService.exe", "QBIDPService.exe", "QBDBMgrN.exe", "QBCFMonitorService.exe", "SAP.exe", "TeamViewer_Service.exe", "TeamViewer.exe", "tv_w32.exe", "tv_x64.exe", "CVMountd.exe", "cvd.exe", "cvfwd.exe", "CVODS.exe", "saphostexec.exe", "saposcol.exe", "sapstartsrv.exe", "avagent.exe", "avscc.exe", "DellSystemDetect.exe", "EnterpriseClient.exe", "VeeamNFSSvc.exe", "VeeamTransportSvc.exe", "VeeamDeploymentSvc.exe"], "**white_folders**": ["*\\$windows.~ws*", "*\\$windows.~bt*", "*\\windows*", "*\\windows.old*", "*\\system volume information*", "*\\Boot*", "*\\PerfLogs*", "*\\AppData\\Local\\Temp*", "*\\AppData\\Local\\Microsoft\\GameDVR*", "*\\AppData\\Local\\Microsoft\\Edge*", "*\\AppData\\Local\\Packages\\Microsoft.*", "*\\AppData\\Local\\Packages\\MicrosoftWindows.*", "*\\AppData\\Local\\Packages\\Internet Explorer*", "*\\Program Files\\Common Files\\microsoft shared*", "*\\Program Files\\Common Files\\Services*", "*\\Program Files\\Common Files\\System*", "*\\Program Files\\Internet Explorer*", "*\\Program Files\\ModifiableWindowsApps*", "*\\Program Files\\Uninstall Information*", "*\\Program Files\\Windows Defender*", "*\\Program Files\\Windows Mail*", "*\\Program Files\\Windows Media Player*", "*\\Program Files\\Windows NT*", "*\\Program Files\\Windows Photo Viewer*", "*\\Program Files\\Windows Portable Devices*", "*\\Program Files\\Windows Security*", "*\\Program Files\\Windows Sidebar*", "*\\Program Files\\WindowsApps*", "*\\Program Files\\WindowsPowerShell*", "*\\Program Files (x86)\\Common Files*", "*\\Program Files (x86)\\Common Files\\Microsoft Shared*", "*\\Program Files (x86)\\Common Files\\Services*", "*\\Program Files (x86)\\Common Files\\System*", "*\\Program Files (x86)\\Internet Explorer*", "*\\Program Files (x86)\\Microsoft*Edge*", "*\\Program Files (x86)\\Microsoft\\Temp*", "*\\Program Files (x86)\\Microsoft.NET*", "*\\Program Files (x86)\\Windows Defender*", "*\\Program Files (x86)\\Windows Mail*", "*\\Program Files (x86)\\Windows Media Player*", "*\\Program Files (x86)\\Windows Multimedia Platform*", "*\\Program Files (x86)\\Windows NT*", "*\\Program Files (x86)\\Windows Photo Viewer*", "*\\Program Files (x86)\\Windows Portable Devices*", "*\\Program Files (x86)\\Windows Security*", "*\\Program Files (x86)\\Windows Sidebar*", "*\\Program Files (x86)\\WindowsPowerShell*", "*\\ProgramData\\ssh*", "*\\ProgramData\\USOPrivate*", "*\\ProgramData\\USOShared*", "*\\ProgramData\\Package Cache*", "*\\ProgramData\\Microsoft\\Device Stage*", "*\\ProgramData\\Microsoft\\DeviceSync*", "*\\ProgramData\\Microsoft\\Diagnosis*", "*\\ProgramData\\Microsoft\\DiagnosticLogCSP*", "*\\ProgramData\\Microsoft\\DRM*", "*\\ProgramData\\Microsoft\\UEV*", "*\\ProgramData\\Microsoft\\EdgeUpdate*", "*\\ProgramData\\Microsoft\\Event Viewer*", "*\\ProgramData\\Microsoft\\IdentityCRL", "*\\ProgramData\\Microsoft\\MapData*", "*\\ProgramData\\Microsoft\\MF*", "*\\ProgramData\\Microsoft\\NetFramework*", "*\\ProgramData\\Microsoft\\Network*", "*\\ProgramData\\Microsoft\\Provisioning*", "*\\ProgramData\\Microsoft\\Search*", "*\\ProgramData\\Microsoft\\SmsRouter*", "*\\ProgramData\\Microsoft\\Spectrum*", "*\\ProgramData\\Microsoft\\Speech_OneCore*", "*\\ProgramData\\Microsoft\\Storage Health*", "*\\ProgramData\\Microsoft\\User Account Pictures*", "*\\ProgramData\\Microsoft\\Vault*", "*\\ProgramData\\Microsoft\\WDF*", "*\\ProgramData\\Microsoft\\Windows*", "*\\ProgramData\\Microsoft\\Windows Defender*", "*\\ProgramData\\Microsoft\\Windows NT*", "*\\ProgramData\\Microsoft\\Windows Security Health*", "*\\ProgramData\\Microsoft\\WinMSIPC*", "*\\ProgramData\\Microsoft\\WPD*", "*\\ProgramData\\Packages\\USOPrivate*", "*\\ProgramData\\Packages\\USOShared*", "*\\ProgramData\\Packages\\WindowsHolographicDevices*", "*\\ProgramData\\Packages\\MicrosoftWindows.*", "*\\ProgramData\\Packages\\Microsoft.*"], "**white_files**": ["NTUSER.DAT", "autorun.inf", "boot.ini", "desktop.ini", "thumbs.db", "*.deskthemepack", "*.themepack", "*.theme", "*.msstyles", "*.exe", "*.drv", "*.msc", "*.dll", "*.lock", "*.sys", "*.msu", "*.lnk", "*.ps1", "*.iso", "*.inf", "*.cab", "*.386"], "**white_hosts**": []}

Data Leak Site

The RansomHub ransom note contains a data leak site (DLS) that displayed the following page, self-identifying the group as RansomHub:

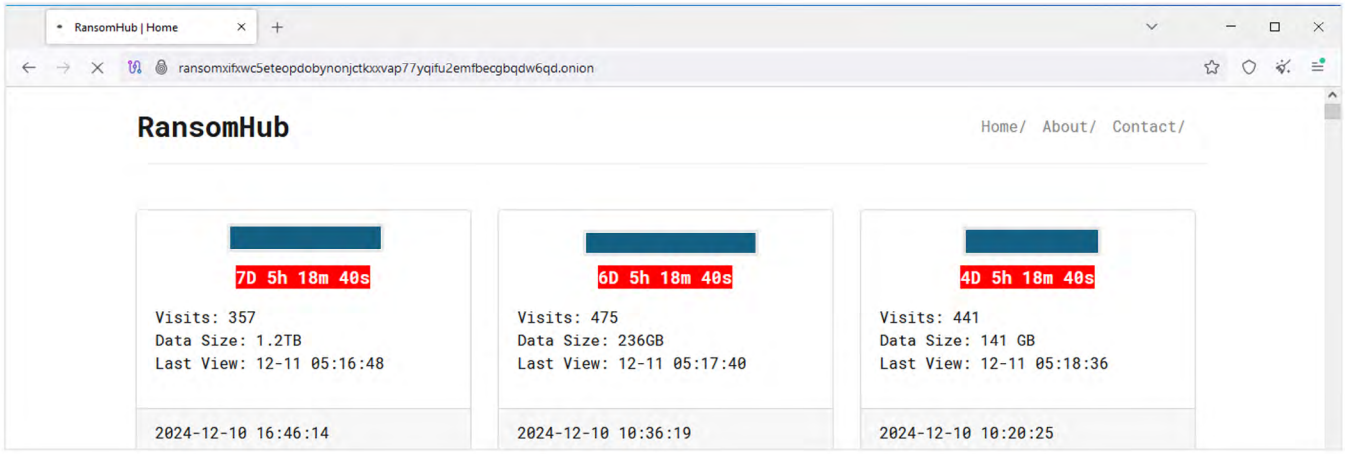


Figure 5. TOR DLS

Similarities with Other Ransomware

During our analysis, we observed some similarities between RansomHub, ALPHV/BlackCat, and Knight ransomware executables.

The following table highlights some of the similarities:

Malware family	Common Arguments	Password	JSON Configuration
RansomHub	pass safeboot safeboot-instance path help verbose fast path sleep	SHA256 strings value	extension note_file_name note_full_text note_short_text kill_processes kill_services credentials
ALPHV/BlackCat	--access-token (similar to -pass in RansomHub and Knight) safeboot safeboot-instance paths help verbose	SHA256 strings value	extension note_file_name note_full_text note_short_text kill_processes kill_services credentials

Knight	pass path verbose fast path sleep	SHA256 strings value	extension note_file_name note_full_text note_short_text kill_processes kill_services credentials

Detection Mechanisms

Custom Detections and Blocking with Arete's Arsinal

SentinelOne S1QL 1.0 query syntax (STAR rule):

RansomHub Ransomware

EndpointOS = "windows" **AND** EventType = "Process Creation" **AND** TgtProcCmdLine RegExp "\.exe\s{1,3}[A-Za-z0-9-]{0,20}\s{0,3}-pass\s[A-Za-z0-9]{64}"

Volume Shadow Copy Deletion

EndpointOS = "windows" **AND** EventType = "Process Creation" **AND** TgtProcCmdLine Contains Anycase "powershell.exe" **AND** TgtProcCmdLine Contains Anycase "-Command" **AND** TgtProcCmdLine Contains Anycase "Get-CimInstance" **AND** TgtProcCmdLine Contains Anycase "Win32_ShadowCopy"

Windows Event Log Cleared

EndpointOS = "windows" **AND** ObjectType = "process" **AND** TgtProcCmdLine Contains Anycase "wevtutil" **AND** TgtProcCmdLine Contains Anycase " cl " **AND** TgtProcCmdLine In Contains Anycase ("Application", "Security", "System")

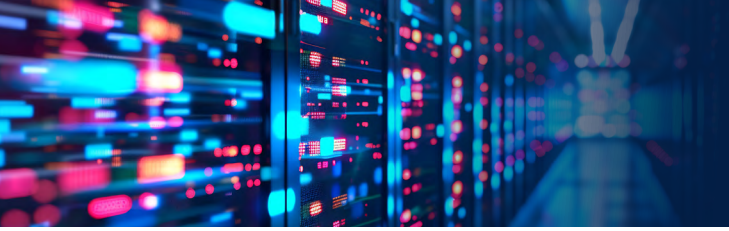
Note: These threat hunting queries may need to be tuned for your specific network environment.

Yara

```
rule RansomHub_ransomware_executable
{
    meta:
        author = "areteir.com"
        description = "Detects the RansomHub ransomware executable"
        target = "Windows systems"
        file_type = "exe"
        copyright = "Copyright © 2024 by Arete Advisors, LLC."
        distribution = "No re-distribution without Arete Advisors, LLC consent."

    strings:
        $s1 = "json:\"local_disks\""
        $s2 = "json:\"running_one\""
        $s3 = "json:\"self_delete\""
        $s4 = "json:\"white_files\""
        $s5 = "json:\"white_hosts\""
        $s6 = "json:\"credentials\""
        $s7 = "json:\"kill_services\""
        $s8 = "json:\"set_wallpaper\""
        $s9 = "json:\"white_folders\""
        $s10 = "json:\"note_file_name\""
        $s11 = "json:\"note_full_text\""
        $s12 = "json:\"kill_processes\""
        $s13 = "json:\"network_shares\""
        $s14 = "json:\"note_short_text\""
        $s15 = "json:\"master_public_key\""

    condition:
        ((uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550)) and
        (9 of ($s*))
}
```



Recommended Mitigations

- Utilize an endpoint detection and response (EDR) solution with the capability to halt detected processes and isolate systems on the network based on identified conditions.
- Block any known attacker C2s in the firewall.
- Implement multi-factor authentication on RDP and VPN to restrict access to critical network resources.
- Eliminate unnecessary RDP ports exposed to the internet.
- Block a high number of SMB connection attempts from one system to others in the network over a short period of time.
- Perform periodic dark web monitoring to verify if data is available for sale on the black market.
- Perform penetration tests.
- Periodically patch systems and update tools.
- Monitor connections to the network from suspicious locations.
- Monitor downloads and uploads of files to file-sharing services outside standard work hours.
- Monitor file uploads from domain controllers to the internet.
- Monitor network scans from uncommon servers (e.g., RDP server).

Organizations can find the full list of US government-recommended ransomware prevention and mitigation guidance here: https://www.cisa.gov/stopransomware/ransomware-guide.

References

https://areteir.com/report/aretes-q3-2024-crimeware-report/
https://areteir.com/solutions/managed-services/#arsinal-threat-management
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
https://areteir.com/article/ransomhub-raas-group-zerologon-exploits/