Ransomware: Hunting for Inhibiting System Backup or Recovery

cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

May 6, 2021

Ransomware continues to be a hot button issue for organizations around the world. APT actors, commodity malware operators and even attackers who had never used ransomware before started picking up the trend over the last several years. In years past, attackers turned to ransomware to exploit an organization's lack of a good backup plan, disaster recovery plan, or coax the victim into paying a ransom to maintain their operations and reduce downtime. However, an unfortunate fact of ransomware infections is how rare full recovery is, after payment occurs.

Given this fact, as well as several vendors and global government organizations highly recommending not paying and instead reverting to recovery options, ransomware infections were becoming less impactful when relying on data encryption alone. This is where the trend of stealing and holding a victim's confidential data for ransom has started to become prevalent amongst ransomware variants, sometimes referred to as 'doxware.' Ransomware "leak sites" are popping up regularly on the dark and clear webs. These leak sites publicly shame their victims and threaten to release sensitive information if their demands are not met. This makes ransomware an incredibly formidable foe, requiring organizations to focus more effort on detection and prevention.

Fortunately for defenders, there are many common calling cards of ransomware. Cyborg Security researchers performed research and analysis on more than twenty of the top variants of ransomware, many accounting for highly visible and damaging attacks. In the following section we'll break down one of the most common techniques employed by ransomware, how to detect the multiple variations that are deployed, give specific examples by variant and how to analyze and attribute observed activity back to the specific variant. Armed with this information defenders will be able to choose the best hunt for their organization that can cast a wide net with as little potential for false positives as possible.

Inhibiting System Recovery – *MITRE* ATT&CK Technique T1490

There are several methods that ransomware uses in order to inhibit system recovery, stop further recoveries, and corrupts or deletes available recovery points on a system. The most common method observed during Cyborg Security's research was the use of vssadmin to delete "Shadow Copies" from the system. Given this became nearly common place for ransomware, developers began exploring other options such as utilizing PowerShell, wmic, bcdedit, net.exe and wbadmin. The utilization of these built in Windows applications is so common in ransomware, it's nearly impossible to attribute the specific ransomware based solely on the method in which it prevents system backups.

Hypothesis

Dynamic analysis utilizing industry leading malware sandboxes, manual analysis, EDR and windows logging, it was noted in some cases, dependent on ransomware variant, process creation events were not logged for each application called within the cmd.exe or powershell.exe command. As such searching within the command line of a PowerShell or Command Shell execution must be performed to avoid missing potential attacks. During analysis it was found bcdedit, wmic, vssadmin, powershell and net were all used as a form of inhibiting a backup from being taken or utilized for system recovery. Although several

variants utilize the same technique with the same application it was found several utilized variations of commands or utilized the application completely different than another, which also needs to be accounted for within any generated logic.

Response

The majority of analyzed ransomware variants did not exhibit unique deployments of this technique. As such, analysts will need to review source processes, parent processes and related process executions or creation events for further signs of a ransomware infection and attribute the activity to a specific ransomware. The easiest method to attribute the ransomware variant, if it appears a successful infection is identified, is to search for file write events or analyze other data from the suspected host looking for files created or modified with abnormal extensions. Many ransomware variants make it easy and add the variant's name as the extension, while others use a randomized string and require other artifacts for attribution. Other methods can include reviewing services or processes stopped or deleted by the ransomware binary or script. Often each variant will choose a specific set of services to disable, stop, delete or uninstall applications. If these methods fail, identifying the directory and binary name (it's structure), combined with the already identified artifacts, can assist in final attribution.

In-scope Ransomware Variants

- Ako (Ranzy)
- Avaddon
- Conti
- Lockbit
- Maze
- Nemty (Nefilm)
- ProLock
- Ragnar
- RansomExx
- Ryuk
- Snatch
- Sodinokibi (REvil)
- Darkside
- Pysa (Mespinoza)
- Netwalker

Out-of-Scope Ransomware

MITRE ATT&CK also tracks a number of other ransomware families that use T1490, including

- BitPaymer (S0570)
- H1N1 (S0132)
- InvisiMole (S0260)
- JCry (S0389)
- MegaCortex S0576)
- Olympic Destroyer (S0365)
- RobbinHood (S0400)
- WannaCry (S0366)

However, for the purposes of this analysis, these malware families will remain out-of-scope.

Hypothesis Summaries

By Process Name

```
processName equals any of ("vssadmin.exe", "bcdedit.exe", "wmic.exe",
"powershell.exe", "wbadmin.exe")

AND

commandLine contains any of ("recoveryenabled no", "IgnoreAllFailures", "delete
shadows", "delete systemstatebackup", resize shadowstorage", "_ShadowCopy",
"safeboot minimal", "shadowcopy /nointeractive", "shadowcopy delete")
```

By Command Line

```
processName equals and of ("cmd.exe", "powershell.exe")

AND

commandLine contains any of ("vssadmin ", "vssadmin.exe ", "bcdedit ", "bcdedit.exe
", "wmic ", "wmic.exe ", "wbadmin ", "wbadmin.exe ", "Get-WmiObject ")

AND

commandLine contains any of ("recoveryenabled no", "IgnoreAllFailures", "delete
shadows", "delete systemstatebackup", resize shadowstorage", "_ShadowCopy",
"safeboot minimal", "shadowcopy /nointeractive", "shadowcopy delete")
```

Executions by Application and Variant

VSSAdmin

Families: Ako, Avaddon, Conti, Lockbit, Ragnar, Ryuk, Netwalker

```
vssadmin.exe Delete Shadows /All /Quiet
```

Families: Nemty, ProLock

```
"C:\Windows\System32\cmd.exe"  /c vssadmin resize shadowstorage /for=C: /on=C:
/maxsize=401MB

"C:\Windows\System32\cmd.exe"  /c vssadmin resize shadowstorage /for=C: /on=C:
/maxsize=unbounded
```

WMIC (WMI Command Line)

Families: Ako, Avaddon, Lockbit

```
wmic.exe SHADOWCOPY /nointeractive =
```

Families: Lockbit, Nemty, Ragnar, Ryuk

```
wmic  shadowcopy delete
```

Families: Maze
Analysis note: This command was a curious find as it's a defense evasion technique to break detections relying on the full path of wmic

```
C:\i\hhwq\jees\..\..\..\Windows\hpn\a\..\..\system32\s\p\..\..\wbem\vax\pq\..\..\wmic.
```

PowerShell

Families: Darkside, Nemty

Analysis note: Several samples analyzed of each of these variants utilized obfuscation of the PowerShell command. In some instances it was found deobfuscated in logging, specifically in PowerShell logging and EDR, but analysts should be aware its often obfuscated in the logs.

```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

BCDEdit

Families: Ako, Avaddon, Lockbit, Nemty, Ragnar, RansomExx, Ryuk, Sodinokibi

Analysis note: It is worth noting that the Ragnar ransomware did not perform the bcdedit command setting "recoveryenabled" to "no" in the samples analyzed. Additionally, in most of the samples analyzed across the variants noted below, the

commands were chained together with an ampersand (&) to run as one command, either utilizing powershell.exe or cmd.exe.

```
bcdedit  /set {default} bootstatuspolicy ignoreallfailures

bcdedit  /set {default} recoveryenabled no
```

Families: Snatch

```
c:\windows\System32\bcdedit.exe  /set {current} safeboot minimal
```

WBAdmin

Families: Ako, Avaddon, Lockbit, Ragnar

```
wbadmin DELETE SYSTEMSTATEBACKUP

wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
```

Families: Lockbit, Nemty

```
wbadmin delete catalog -quiet
```

Net

Families: Conti

```
net stop BackupExecAgentAccelerator /y

net stop BackupExecVSSProvider /y
```

Conclusion

Ransomware deploys a wide array of techniques, often making it difficult to effectively hunt for several variants at a time. This is especially true for the early stages of the infection chain, such as the Installation phase, to detect, identify and respond as quickly as possible to the potential threat. Hunting for ransomware attempting to inhibit a host's recovery ability is one of, if not the best methods for identifying potential ransomware attacks, post-delivery. This is largely due to the limited composition of the commands to carry out the technique, and its rarity of being observed for legitimate purposes. Although hunting for this technique may not make it readily apparent which ransomware variant is lurking in your organization, it's certainly one of the best bangs for your hunting and time.