T1485 - Data Destruction

Description from ATT&CK

> Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016) (Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018)(Citation: Talos Olympic Destroyer 2018) Common operating system file deletion commands such as `del` and `rm` often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from [Disk Content Wipe](https://attack.mitre.org/techniques/T1561/001) and [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.
> Adversaries may attempt to overwrite files and directories with randomly generated data to make it irrecoverable.(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018) In some cases politically oriented image files have been used to overwrite data.(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)

> To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware designed for destroying data may have worm-like features to propagate across a network by leveraging additional techniques like Valid Accounts, OS Credential Dumping, and SMB/Windows Admin Shares.(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Talos Olympic Destroyer 2018).
>
> In cloud environments, adversaries may leverage access to delete cloud storage, cloud storage accounts, machine images, and other infrastructure crucial to operations to damage an organization or their customers.(Citation: Data Destruction - Threat Post)(Citation: DOJ - Cisco Insider)

Atomic Tests

- Atomic Test #1 - Windows - Overwrite file with Sysinternals SDelete
- Atomic Test #2 - macOS/Linux - Overwrite file with DD
- Atomic Test #3 - Overwrite deleted data on C drive

Atomic Test #1 - Windows - Overwrite file with Sysinternals SDelete

Overwrites and deletes a file using Sysinternals SDelete. Upon successful execution, "Files deleted: 1" will be displayed in the powershell session along with other information about the file that was deleted.

Supported Platforms: Windows

auto_generated_guid: 476419b5-aebf-4366-a131-ae3e8dae5fc2

Inputs:

Name	Description	Type	Default Value
sdelete_exe	Path of sdelete executable	Path	$env:TEMP\Sdelete\sdelete.exe
file_to_delete	Path of file to delete	Path	$env:TEMP\T1485.txt

Attack Commands: Run with `powershell`!

```
if (-not (Test-Path #{file_to_delete})) { New-Item #{file_to_delete} -Force }
Invoke-Expression -Command "#{sdelete_exe} -accepteula #{file_to_delete}"
```

Dependencies: Run with `powershell`!

Description: Secure delete tool from Sysinternals must exist on disk at specified location (#{sdelete_exe})

Check Prereq Commands:

```
if (Test-Path #{sdelete_exe}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Invoke-WebRequest "https://download.sysinternals.com/files/SDelete.zip" -OutFile "
Expand-Archive $env:TEMP\SDelete.zip $env:TEMP\Sdelete -Force
Remove-Item $env:TEMP\SDelete.zip -Force
```

Atomic Test #2 - macOS/Linux - Overwrite file with DD

Overwrites and deletes a file using DD. To stop the test, break the command with CTRL/CMD+C.

Supported Platforms: Linux, macOS

auto_generated_guid: 38deee99-fd65-4031-bec8-bfa4f9f26146

Inputs:

Name	Description	Type	Default Value
overwrite_source	Path of data source to overwrite with	Path	/dev/zero
file_to_overwrite	Path of file to overwrite and remove	Path	/var/log/syslog

Attack Commands: Run with `bash`!

```
dd of=#{file_to_overwrite} if=#{overwrite_source} count=$(ls -l #{file_to_overwrit
```

Atomic Test #3 - Overwrite deleted data on C drive

RansomEXX malware removes all deleted files using windows built-in cipher.exe to prevent forensic recover. This process is very slow and test execution may timeout.
https://www.cybereason.com/blog/cybereason-vs.-ransomexx-ransomware
https://support.microsoft.com/en-us/topic/cipher-exe-security-tool-for-the-encrypting-file-system-56c85edd-85cf-ac07-f2f7-ca2d35dab7e4

Supported Platforms: Windows

auto_generated_guid: 321fd25e-0007-417f-adec-33232252be19

Attack Commands: Run with `command_prompt`!

```
cipher.exe /w:C:
```