T1070 - Indicator Removal on Host

Description from ATT&CK

> Adversaries may delete or modify artifacts generated on a host system to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform.
> Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Atomic Tests

- Atomic Test #1 - Indicator Removal using FSUtil

Atomic Test #1 - Indicator Removal using FSUtil

Manages the update sequence number (USN) change journal, which provides a persistent log of all changes made to files on the volume. Upon execution, no output will be displayed. More information about fsutil can be found at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/fsutil-usn

Supported Platforms: Windows

auto_generated_guid: b4115c7a-0e92-47f0-a61e-17e7218b2435

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

```
fsutil usn deletejournal /D C:
```

Cleanup Commands:

```
fsutil usn createjournal m=1000 a=100 c:
```