

Product ▾


Solutions ▾

Resources ▾

Open Source ▾


Enterprise ▾

Pricing





Sign in


Sign up

 redcanaryco / atomic-red-team


Public


 Notifications


 Fork 2.8k


 Star 9.7k


<> Code


 Issues 6


 Pull requests 5


 Actions


 Wiki


 Security


 Insights


 Files


 f339e7d





 Go to file


>  .github


>  atomic\_red\_team


>  atomics


>  Indexes


>  T1003.001


>  T1003.002


>  T1003.003


>  T1003.004


>  T1003.005


>  T1003.006


>  T1003.007


>  T1003.008


>  T1003


>  T1006


>  T1007


>  T1010


>  T1012


>  T1014


>  T1016


>  T1018


>  T1020


>  T1021.001


>  T1021.002


>  T1021.003


>  T1021.006


>  T1027.001


>  T1027.002


>  T1027.004


>  T1027


>  T1030


>  T1033

>  T1036.003


>  T1036.004


>  T1036.005


>  T1036.006

>  T1036


atomic-red-team / atomics / T1070 / T1070.md





 Atomic Red Team doc generat...

Generated docs from job=generate-d... 819934c · 2 years ago

 History


Preview


Code


Blame

44 lines (21 loc) · 1.83 KB

Raw







# 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:
```



- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039
- >  T1040

