⊟ **Delete Volume USN Journal with fsutil**

MITRE ATT&CK™ Mapping

Query

Detonation

Contributors

Disconnecting from Network Shares with net.exe

Discovery and Enumeration of System Information via Rundll32

Discovery of a Remote System's Time

Discovery of Domain Groups

Discovery of Network Environment via Built-in Tools

Discovery of Network Environment via Built-in Tools

DLL Search Order Hijacking with known programs

Domain Trust Discovery

Domain Trust Discovery via Nltest.exe

Encoding or Decoding Files via CertUtil

Enumeration of Local Shares

Enumeration of Mounted Shares

Enumeration of Remote Shares

Enumeration of System Information

Enumeration of System Information

Executable Written and Executed by Microsoft Office Applications

Execution of a Command via a SYSTEM Service

Execution of Existing Service via Command

Execution via cmstp.exe

HH.exe execution

Host Artifact Deletion

Image Debuggers for Accessibility Features

Incoming Remote PowerShell Sessions

Indirect Command Execution

Installation of Port Monitor

Installation of Security Support Provider

Installation of Time Providers

Installing Custom Shim Databases

InstallUtil Execution

Interactive AT Job

Launch Daemon Persistence

Loading Kernel Modules with kextload

Local Job Scheduling Paths

Local Job Scheduling Process

Logon Scripts with

Delete Volume USN Journal with fsutil

Identifies use of the fsutil command to delete the volume USNJRNL. This technique is used by attackers to eliminate evidence of files created during post-exploitation activities.

id:	c91f422a-5214-4b17-8664-c5fcf115c0a2
categories:	detect
confidence:	low
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Defense Evasion
techniques:	T1070 Indicator Removal on Host

Query

```
process where subtype.create and
  process_name == "fsutil.exe" and command_line == "* usn *" and command_line == "* deletej
```

Detonation

Atomic Red Team: T1070

Contributors

- Endgame

Previous Next