- Clearing Windows Event Logs with wevtutil
  - MITRE ATT&CK™ Mapping
  - Query
  - Detonation
  - Contributors
- COM Hijack via Script Object
- Command-Line Creation of a RAR file
- Control Panel Items
- Creation of an Archive with Common Archivers
- Creation of Kernel Module
- Creation of Scheduled Task with schtasks.exe
- Creation or Modification of Systemd Service
- Credential Enumeration via Credential Vault CLI
- Delete Volume USN Journal with fsutil
- 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

Clearing Windows Event Logs with wevtutil

Identifies attempts to clear Windows event logs with the command `wevtutil`.

id:	5b223758-07d6-4100-9e11-238cfdd0fe97
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 == "wevtutil.exe" and command_line == "* cl *"
```

Detonation

Atomic Red Team: T1070

Contributors

- Endgame

Previous Next