# TTP Detail – T1070.001

## TTP Information

Name: Clear Windows Event Logs

Description: Adversaries may clear Windows Event Logs to hide the activity of an intrusion. Windows Event Logs are a record of a computer's alerts and notifications. There are three system-defined sources of events: System, Application, and Security, with five event types: Error, Warning, Information, Success Audit, and Failure Audit.

With administrator privileges, the event logs can be cleared with the following utility commands:

\* <code>wevtutil cl system</code>
\* <code>wevtutil cl application</code>
\* <code>wevtutil cl security</code>

These logs may also be cleared through other mechanisms, such as the event viewer GUI or [PowerShell](https://attack.mitre.org/techniques/T1059/001). For example, adversaries may use the PowerShell command <code>Remove-EventLog -LogName Security</code> to delete the Security EventLog and after reboot, disable future logging. Note: events may still be generated and logged in the .evtx file between the time the command is run and the reboot.(Citation: disable\_win\_evt\_logging)

Adversaries may also attempt to clear logs by directly deleting the stored log files within `C:\Windows\System32\winevt\logs\`.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Apostle
* BlackCat
* BlackEnergy
* DUSTTRAP
* FinFisher
* HermeticWiper
* HermeticWizard
* Hydraq
* KillDisk
* LockBit 2.0
* LockBit 3.0
* Lucifer
* Mafalda
* Meteor
* MultiLayer Wiper
* NotPetya
* Olympic Destroyer
* RansomHub
* RunningRAT
* ShrinkLocker
* SynAck
* ZxShell
* gh0st RAT

## Tools

* Pupy
* Wevtutil

## APTs (Intrusion Sets)

* APT28
* APT32
* APT38
* APT41
* Aquatic Panda
* Chimera
* Dragonfly
* FIN5
* FIN8
* HAFNIUM
* Indrik Spider
* Play
* Volt Typhoon