# TTP Detail – T1562.001

## TTP Information

Name: Disable or Modify Tools

Description: Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. This may take many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning or reporting information. Adversaries may also disable updates to prevent the latest security patches from reaching tools on victim systems.(Citation: SCADAfence\_ransomware)

Adversaries may also tamper with artifacts deployed and utilized by security tools. Security tools may make dynamic changes to system components in order to maintain visibility into specific events. For example, security products may load their own modules and/or modify those loaded by processes to facilitate data collection. Similar to [Indicator Blocking](https://attack.mitre.org/techniques/T1562/006), adversaries may unhook or otherwise modify these features added by tools (especially those that exist in userland or are otherwise potentially accessible to adversaries) to avoid detection.(Citation: OutFlank System Calls)(Citation: MDSec System Calls) Alternatively, they may add new directories to an endpoint detection and response (EDR) tool’s exclusion list, enabling them to hide malicious files via [File/Path Exclusions](https://attack.mitre.org/techniques/T1564/012).(Citation: BlackBerry WhisperGate 2022)(Citation: Google Cloud Threat Intelligence FIN13 2021)

Adversaries may also focus on specific applications such as Sysmon. For example, the “Start” and “Enable” values in <code>HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Microsoft-Windows-Sysmon-Operational</code> may be modified to tamper with and potentially disable Sysmon logging.(Citation: disable\_win\_evt\_logging)

On network devices, adversaries may attempt to skip digital signature verification checks by altering startup configuration files and effectively disabling firmware verification that typically occurs at boot.(Citation: Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation)(Citation: Analysis of FG-IR-22-369)

In cloud environments, tools disabled by adversaries may include cloud monitoring agents that report back to services such as AWS CloudWatch or Google Cloud Monitor.

Furthermore, although defensive tools may have anti-tampering mechanisms, adversaries may abuse tools such as legitimate rootkit removal kits to impair and/or disable these tools.(Citation: chasing\_avaddon\_ransomware)(Citation: dharma\_ransomware)(Citation: demystifying\_ryuk)(Citation: doppelpaymer\_crowdstrike) For example, adversaries have used tools such as GMER to find and shut down hidden processes and antivirus software on infected systems.(Citation: demystifying\_ryuk)

Additionally, adversaries may exploit legitimate drivers from anti-virus software to gain access to kernel space (i.e. [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068)), which may lead to bypassing anti-tampering features.(Citation: avoslocker\_ransomware)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Agent Tesla
* Avaddon
* Babuk
* Bazar
* BlackByte Ransomware
* Brave Prince
* Bundlore
* Carberp
* ChChes
* Clop
* Cobalt Strike
* Conficker
* DarkComet
* DarkGate
* Diavol
* EKANS
* Ebury
* Egregor
* Gold Dragon
* Goopy
* Grandoreiro
* H1N1
* HDoor
* Hildegard
* JPIN
* KOCTOPUS
* LockBit 2.0
* LockBit 3.0
* LockerGoga
* Lumma Stealer
* Mango
* Maze
* MegaCortex
* Metamorfo
* Meteor
* MultiLayer Wiper
* NanHaiShu
* NanoCore
* Netwalker
* POWERSTATS
* Proton
* Pysa
* QakBot
* REvil
* Ragnar Locker
* Raspberry Robin
* RobbinHood
* RunningRAT
* Ryuk
* SUNBURST
* ShrinkLocker
* Skidmap
* SslMM
* StrongPity
* ThiefQuest
* TinyZBot
* TrickBot
* Unknown Logger
* WarzoneRAT
* WhisperGate
* XLoader
* ZIPLINE
* ZxShell
* macOS.OSAMiner

## Tools

* Donut
* Imminent Monitor
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT38
* Agrius
* Akira
* Aquatic Panda
* BRONZE BUTLER
* BlackByte
* Ember Bear
* FIN6
* Gamaredon Group
* Gorgon Group
* INC Ransom
* Indrik Spider
* Kimsuky
* Lazarus Group
* Magic Hound
* MuddyWater
* Play
* Putter Panda
* Rocke
* Saint Bear
* TA2541
* TA505
* TeamTNT
* Turla
* Velvet Ant
* Wizard Spider