# TTP Detail – T1561.002

## TTP Information

Name: Disk Structure Wipe

Description: Adversaries may corrupt or wipe the disk data structures on a hard drive necessary to boot a system; targeting specific critical systems or in large numbers in a network to interrupt availability to system and network resources.

Adversaries may attempt to render the system unable to boot by overwriting critical data located in structures such as the master boot record (MBR) or partition table.(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018) The data contained in disk structures may include the initial executable code for loading an operating system or the location of the file system partitions on disk. If this information is not present, the computer will not be able to load an operating system during the boot process, leaving the computer unavailable. [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) may be performed in isolation, or along with [Disk Content Wipe](https://attack.mitre.org/techniques/T1561/001) if all sectors of a disk are wiped.

On a network devices, adversaries may reformat the file system using [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `format`.(Citation: format\_cmd\_cisco)

To maximize impact on the target organization, malware designed for destroying disk structures may have worm-like features to propagate across a network by leveraging other techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: impact

## Malware

* BFG Agonizer
* CaddyWiper
* DEADWOOD
* HermeticWiper
* KillDisk
* MultiLayer Wiper
* Shamoon
* StoneDrill
* WhisperGate
* ZeroCleare

## Tools

* RawDisk

## APTs (Intrusion Sets)

* APT37
* APT38
* Ember Bear
* Lazarus Group
* Sandworm Team