Disk Wipe: Disk Structure Wipe, Sub-technique T1561.002 - Enterprise

Archived: 2026-04-05 17:17:17 UTC

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.[1][2][3][4][5] 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 may be performed in isolation, or along with Disk Content Wipe if all sectors of a disk are wiped.

On a network devices, adversaries may reformat the file system using Network Device CLI commands such as `format`.[6]

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, OS Credential Dumping, and SMB/Windows Admin Shares.[1][2][3][4]

Source: https://attack.mitre.org/techniques/T1561/002