Disk Wipe: Disk Content Wipe, Sub-technique T1561.001 - Enterprise

Archived: 2026-04-02 12:00:29 UTC

Adversaries may erase the contents of storage devices on specific systems or in large numbers in a network to interrupt availability to system and network resources.

Adversaries may partially or completely overwrite the contents of a storage device rendering the data irrecoverable through the storage interface.[1][2][3] Instead of wiping specific disk structures or files, adversaries with destructive intent may wipe arbitrary portions of disk content. To wipe disk content, adversaries may acquire direct access to the hard drive in order to overwrite arbitrarily sized portions of disk with random data.[2] Adversaries have also been observed leveraging third-party drivers like RawDisk to directly access disk content.[1][2] This behavior is distinct from Data Destruction because sections of the disk are erased instead of individual files.

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware used for wiping disk content may have worm-like features to propagate across a network by leveraging additional techniques like Valid Accounts, OS Credential Dumping, and SMB/Windows Admin Shares.[2]

Source: https://attack.mitre.org/techniques/T1488