Data Destruction, Technique T1485 - Enterprise

Archived: 2026-04-05 13:51:21 UTC

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.[1][2][3][4][5][6] Common operating system file deletion commands such as `del` and `rm` often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from Disk Content Wipe and Disk Structure Wipe because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.

Adversaries may attempt to overwrite files and directories with randomly generated data to make it irrecoverable.[4][5] In some cases politically oriented image files have been used to overwrite data.[2][3][4]

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware designed for destroying data 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.[1][2][3][4][6]

In cloud environments, adversaries may leverage access to delete cloud storage objects, machine images, database instances, and other infrastructure crucial to operations to damage an organization or their customers.[7][8] Similarly, they may delete virtual machines from on-prem virtualized environments.

Source: https://attack.mitre.org/techniques/T1485