Data Destruction, Technique T0809 - ICS

Archived: 2026-04-05 18:04:35 UTC

Adversaries may perform data destruction over the course of an operation. The adversary may drop or create malware, tools, or other non-native files on a target system to accomplish this, potentially leaving behind traces of malicious activities. Such non-native files and other data may be removed over the course of an intrusion to maintain a small footprint or as a standard part of the post-intrusion cleanup process. [1]

Data destruction may also be used to render operator interfaces unable to respond and to disrupt response functions from occurring as expected. An adversary may also destroy data backups that are vital to recovery after an incident.

Standard file deletion commands are available on most operating system and device interfaces to perform cleanup, but adversaries may use other tools as well. Two examples are Windows Sysinternals SDelete and Active@ Killdisk.

Source: https://attack.mitre.org/techniques/T0809