Power Settings, Technique T1653 - Enterprise

Archived: 2026-04-05 17:23:25 UTC

Adversaries may impair a system's ability to hibernate, reboot, or shut down in order to extend access to infected machines. When a computer enters a dormant state, some or all software and hardware may cease to operate which can disrupt malicious activity.[1]

Adversaries may abuse system utilities and configuration settings to maintain access by preventing machines from entering a state, such as standby, that can terminate malicious activity.[2][3]

For example, `powercfg` controls all configurable power system settings on a Windows system and can be abused to prevent an infected host from locking or shutting down.[4] Adversaries may also extend system lock screen timeout settings.[5] Other relevant settings, such as disk and hibernate timeout, can be similarly abused to keep the infected machine running even if no user is active.[6]

Aware that some malware cannot survive system reboots, adversaries may entirely delete files used to invoke system shut down or reboot.[7]

Source: https://attack.mitre.org/techniques/T1653