Weaken Encryption: Disable Crypto Hardware, Sub-technique T1600.002 - Enterprise

Archived: 2026-04-05 13:15:02 UTC

Adversaries disable a network device’s dedicated hardware encryption, which may enable them to leverage weaknesses in software encryption in order to reduce the effort involved in collecting, manipulating, and exfiltrating transmitted data.

Many network devices such as routers, switches, and firewalls, perform encryption on network traffic to secure transmission across networks. Often, these devices are equipped with special, dedicated encryption hardware to greatly increase the speed of the encryption process as well as to prevent malicious tampering. When an adversary takes control of such a device, they may disable the dedicated hardware, for example, through use of Modify System Image, forcing the use of software to perform encryption on general processors. This is typically used in conjunction with attacks to weaken the strength of the cipher in software (e.g., Reduce Key Space). [1]

Source: https://attack.mitre.org/techniques/T1600/002