Weaken Encryption: Reduce Key Space, Sub-technique T1600.001 - Enterprise

Archived: 2026-04-05 14:58:26 UTC

Adversaries may reduce the level of effort required to decrypt data transmitted over the network by reducing the cipher strength of encrypted communications.[1]

Adversaries can weaken the encryption software on a compromised network device by reducing the key size used by the software to convert plaintext to ciphertext (e.g., from hundreds or thousands of bytes to just a couple of bytes). As a result, adversaries dramatically reduce the amount of effort needed to decrypt the protected information without the key.

Adversaries may modify the key size used and other encryption parameters using specialized commands in a Network Device CLI introduced to the system through Modify System Image to change the configuration of the device. [2]

Source: https://attack.mitre.org/techniques/T1600/001