Exfiltration Over Command and Control Channel Mitigation, Mitigation T1041 - Enterprise

Archived: 2026-04-05 17:11:26 UTC

Mitigations for command and control apply. Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.

Source: https://attack.mitre.org/mitigations/T1041