Detection of Network Connection Enumeration, Detection Strategy DET0770

Archived: 2026-04-05 17:12:05 UTC

AN1902

Monitor executed commands and arguments that may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Also monitor executed commands and arguments that may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.
Monitor for executed processes (such as ipconfig/ifconfig and arp) with arguments that may look for details about the network configuration and settings, such as IP and/or MAC addresses. Also monitor for executed processes that may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.
Monitor for any suspicious attempts to enable script execution on a system. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.
Monitor for API calls (such as GetAdaptersInfo() and GetIpNetTable()) that may gather details about the network configuration and settings, such as IP and/or MAC addresses. Also monitor for API calls that may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. For added context on adversary procedures and background see System Network Configuration Discovery and System Network Connections Discovery.

Log Sources
