Detection of Remote Services, Detection Strategy DET0804

Archived: 2026-04-05 17:56:32 UTC

AN1936

Monitor network data for uncommon data flows (e.g., time of day, unusual source/destination address) that may be related to abuse of Valid Accounts to log into a service specifically designed to accept remote connections, such as RDP, Telnet, SSH, and VNC.
Monitor DLL file events, specifically creation of these files as well as the loading of DLLs into processes specifically designed to accept remote connections, such as RDP, Telnet, SSH, and VNC.
Monitor for user accounts logged into systems they would not normally access or abnormal access patterns, such as multiple systems over a relatively short period of time. Correlate use of login activity related to remote services with unusual behavior or other malicious or suspicious activity. Adversaries will likely need to learn about an environment and the relationships between systems through Discovery techniques prior to attempting Lateral Movement. For added context on adversary procedures and background see Remote Services and applicable sub-techniques.
Monitor for newly executed processes related to services specifically designed to accept remote connections, such as RDP, Telnet, SSH, and VNC. The adversary may use Valid Accounts to login and may perform follow-on actions that spawn additional processes as the user.
Monitor executed commands and arguments to services specifically designed to accept remote connections, such as RDP, Telnet, SSH, and VNC. The adversary may then perform these actions using Valid Accounts.
Monitor for newly constructed network connections into a service specifically designed to accept remote connections, such as RDP, Telnet, SSH, and VNC. Monitor network connections involving common remote management protocols, such as ports tcp:3283 and tcp:5900, as well as ports tcp:3389 and tcp:22 for remote logins. The adversary may use Valid Accounts to enable remote logins.
Monitor interactions with network shares, such as reads or file transfers, using remote services such as Server Message Block (SMB). For added context on adversary procedures and background see Remote Services and applicable sub-techniques.

Log Sources
