Detection of Graphical User Interface, Detection Strategy DET0772

Archived: 2026-04-05 15:23:51 UTC

Analytics

- ICS

AN1904

Monitor for newly executed processes related to services specifically designed to accept remote graphical connections, such as RDP and VNC. Remote Services and Valid Accounts may be used to access a host's GUI.
Monitor executed commands and arguments related to services specifically designed to accept remote graphical connections, such as RDP and VNC. Remote Services and Valid Accounts may be used to access a host's GUI.
Monitor DLL file events, specifically creation of these binary files as well as the loading of DLLs into processes associated with remote graphical connections, such as RDP and VNC. Remote Services may be used to access a host's GUI.
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. Remote Services may be used to access a host's GUI.

Log Sources
