Detection of Server, Detection Strategy DET0871

Archived: 2026-04-05 13:08:40 UTC

AN2003

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.
Once adversaries have provisioned a server (ex: for use as a command and control server), internet scans may reveal servers that adversaries have acquired. Consider looking for identifiable patterns such as services listening, certificates in use, SSL/TLS negotiation features, or other response artifacts associated with adversary C2 software.[1][2][3]

Log Sources
