Detection of Compromise Accounts, Detection Strategy DET0876

Archived: 2026-04-02 11:55:19 UTC

AN2008

Consider monitoring social media activity related to your organization. Suspicious activity may include personas claiming to work for your organization or recently modified accounts making numerous connection requests to accounts affiliated with your organization.
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 Initial Access (ex: Phishing).
Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

Log Sources
