Detection of Compromise Infrastructure, Detection Strategy DET0885

Archived: 2026-04-05 14:47:17 UTC

AN2017

Once adversaries have provisioned compromised infrastructure (ex: a server for use in command and control), internet scans may help proactively discover compromised infrastructure. 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]
Consider monitoring for anomalous changes to domain registrant information and/or domain resolution information that may indicate the compromise of a domain. Efforts may need to be tailored to specific domains of interest as benign registration and resolution changes are a common occurrence on the internet.
Monitor for queried domain name system (DNS) registry data that may compromise third-party infrastructure that can be used during targeting. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.
Monitor for logged domain name system (DNS) data that may compromise third-party infrastructure that can be used during targeting. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.
Monitor for contextual data about an Internet-facing resource gathered from a scan, such as running services or ports that may compromise third-party infrastructure that can be used during targeting. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.

Log Sources