Detection of Acquire Infrastructure, Detection Strategy DET0895

Archived: 2026-04-05 17:06:21 UTC

AN2027

Monitor for contextual data about an Internet-facing resource gathered from a scan, such as running services or ports that may buy, lease, or rent 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.
Once adversaries have provisioned infrastructure (ex: a server for use in command and control), internet scans may help proactively discover adversary acquired 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] Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.
Monitor for queried domain name system (DNS) registry data that may buy, lease, or rent 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 buy, lease, or rent 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.
Consider use of services that may aid in tracking of newly acquired infrastructure, such as WHOIS databases for domain registration information. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.

Log Sources