Detection of Domains, Detection Strategy DET0892

Archived: 2026-04-05 13:51:39 UTC

AN2024

Monitor logged domain name system (DNS) data for purchased domains that can be used during targeting. Reputation/category-based detection may be difficult until the categorization is updated. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access and Command and Control. Domain registration information is, by design, captured in public registration logs. Consider use of services that may aid in tracking of newly acquired domains, such as WHOIS databases and/or passive DNS. In some cases it may be possible to pivot on known pieces of domain registration information to uncover other infrastructure purchased by the adversary. Consider monitoring for domains created with a similar structure to your own, including under a different TLD. Though various tools and services exist to track, query, and monitor domain name registration information, tracking across multiple DNS infrastructures can require multiple tools/services or more advanced analytics.[1] Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access and Command and Control.
Monitor queried domain name system (DNS) registry data for purchased domains that can be used during targeting. Reputation/category-based detection may be difficult until the categorization is updated. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access and Command and Control.

Log Sources
