Detection of DNS Server, Detection Strategy DET0891

AN2023

Monitor for queried domain name system (DNS) registry data that may compromise third-party DNS servers that can be used during targeting. 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.
Monitor for logged domain name system (DNS) registry data that may compromise third-party DNS servers that can be used during targeting. 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.

Log Sources
