Detection of Domain Generation Algorithms, Detection Strategy DET0669

Archived: 2026-04-02 12:23:14 UTC

AN1765

Monitor for pseudo-randomly generated domain names based on frequency analysis, Markov chains, entropy, proportion of dictionary words, ratio of vowels to other characters, and more.[1] Additionally, check if the suspicious domain has been recently registered, if it has been rarely visited, or if the domain had a spike in activity after being dormant.[2] Content delivery network (CDN) domains may trigger these detections due to the format of their domain names.

Log Sources

AN1766

Monitor for pseudo-randomly generated domain names based on frequency analysis, Markov chains, entropy, proportion of dictionary words, ratio of vowels to other characters, and more.[1] Additionally, check if the suspicious domain has been recently registered, if it has been rarely visited, or if the domain had a spike in activity after being dormant.[2] Content delivery network (CDN) domains may trigger these detections due to the format of their domain names.

Log Sources

Source: https://attack.mitre.org/detectionstrategies/DET0669