Detection of Code Signing Certificates, Detection Strategy DET0833

Archived: 2026-04-05 14:25:58 UTC

AN1965

Consider analyzing self-signed code signing certificates for features that may be associated with the adversary and/or their developers, such as the thumbprint, algorithm used, validity period, and common name. Malware repositories can also be used to identify additional samples associated with the adversary and identify patterns an adversary has used in crafting self-signed code signing certificates.
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 follow-on behavior, such as Code Signing or Install Root Certificate.

Log Sources
