Detection of Tool, Detection Strategy DET0852

Archived: 2026-04-05 16:15:11 UTC

AN1984

Monitor for contextual data about a malicious payload, such as compilation times, file hashes, as well as watermarks or other identifiable configuration information. In some cases, malware repositories can also be used to identify features of tool use associated with an adversary, such as watermarks in Cobalt Strike payloads.[1] 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 post-compromise phases of the adversary lifecycle.

Log Sources

Source: https://attack.mitre.org/detectionstrategies/DET0852