Detection of Malware, Detection Strategy DET0845

Archived: 2026-04-05 13:21:04 UTC

AN1977

Monitor for contextual data about a malicious payload, such as compilation times, file hashes, as well as watermarks or other identifiable configuration information. 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.
Consider analyzing malware for features that may be associated with malware providers, such as compiler used, debugging artifacts, code similarities, or even group identifiers associated with specific MaaS offerings. Malware repositories can also be used to identify additional samples associated with the developers and the adversary utilizing their services. Identifying overlaps in malware use by different adversaries may indicate malware was obtained by the adversary rather than developed by them. In some cases, identifying overlapping characteristics in malware used by different adversaries may point to a shared quartermaster.[1]

Log Sources
