Detection of Malware, Detection Strategy DET0872

Archived: 2026-04-05 14:06:23 UTC

AN2004

Consider analyzing malware for features that may be associated with the adversary and/or their developers, such as compiler used, debugging artifacts, or code similarities. Malware repositories can also be used to identify additional samples associated with the adversary and identify development patterns over time.
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.

Log Sources
