Detection of Develop Capabilities, Detection Strategy DET0853

Archived: 2026-04-05 17:14:31 UTC

AN1985

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. 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 stages of the adversary lifecycle, such as during Defense Evasion or Command and Control.

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 related stages of the adversary lifecycle, such as during Defense Evasion or Command and Control.

Consider use of services that may aid in the tracking of capabilities, such as certificates, in use on sites across the Internet. In some cases it may be possible to pivot on known pieces of information to uncover other adversary infrastructure.[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 related stages of the adversary lifecycle, such as during Defense Evasion or Command and Control.

Log Sources
