Detection of Obtain Capabilities, Detection Strategy DET0850

Archived: 2026-04-05 14:38:31 UTC

AN1982

Consider use of services that may aid in the tracking of newly issued certificates and/or certificates in use on sites across the Internet. In some cases it may be possible to pivot on known pieces of certificate information to uncover other adversary infrastructure.[1] Some server-side components of adversary tools may have default values set for SSL/TLS certificates.[2] 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.
Monitor for logged network traffic in response to a scan showing both protocol header and body values that may buy and/or steal capabilities that can be used during targeting. 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 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 Malware-as-a-Service (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.[3] Malware repositories can also be used to identify features of tool use associated with an adversary, such as watermarks in Cobalt Strike payloads.[4]

Log Sources