Detection of Indicator Removal on Host, Detection Strategy DET0750

Archived: 2026-04-05 16:40:27 UTC

AN1882

Monitor executed commands and arguments that may delete or alter generated artifacts on a host system, including logs or captured files such as quarantined malware.
Monitor for API calls that may delete or alter generated artifacts on a host system, including logs or captured files such as quarantined malware.
Monitor for changes made to Windows Registry keys or values that may delete or alter generated artifacts on a host system, including logs or captured files such as quarantined malware. For added context on adversary procedures and background see Indicator Removal and applicable sub-techniques.
Monitor for contextual file data that may show signs of deletion or alter generated artifacts on a host system, including logs or captured files such as quarantined malware.
Monitor Windows registry keys that may be deleted or alter generated artifacts on a host system, including logs or captured files such as quarantined malware. For added context on adversary procedures and background see Indicator Removal and applicable sub-techniques.
Monitor for a file that may delete or alter generated artifacts on a host system, including logs or captured files such as quarantined malware.
Monitor for changes made to a file may delete or alter generated artifacts on a host system, including logs or captured files such as quarantined malware.
Monitor for newly executed processes that may delete or alter generated artifacts on a host system, including logs or captured files such as quarantined malware.

Log Sources
