Detection of User Execution, Detection Strategy DET0791

Archived: 2026-04-05 12:40:31 UTC

AN1923

Monitor for newly executed processes that depend on user interaction, especially for applications that can embed programmatic capabilities (e.g., Microsoft Office products with scripts, installers, zip files). This includes compression applications, such as those for zip files, that can be used to Deobfuscate/Decode Files or Information in payloads. For added context on adversary procedures and background see User Execution and applicable sub-techniques.
Monitor for application logging, messaging, and/or other artifacts that may rely upon specific actions by a user in order to gain execution.
Monitor for newly constructed web-based network connections that are sent to malicious or suspicious destinations (e.g., destinations attributed to phishing campaigns). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments (e.g., monitor anomalies in use of files that do not normally initiate network connections or unusual connections initiated by regsvr32.exe, rundll.exe, SCF, HTA, MSI, DLLs, or msiexec.exe).
Anti-virus can potentially detect malicious documents and files that are downloaded and executed on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the file is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning PowerShell).
Monitor for newly executed processes that depend on user interaction, especially for applications that can embed programmatic capabilities (e.g., Microsoft Office products with scripts, installers, zip files). This includes compression applications, such as those for zip files, that can be used to Deobfuscate/Decode Files or Information in payloads.
Monitor and analyze traffic patterns and packet inspection associated with web-based network connections that are sent to malicious or suspicious destinations (e.g., destinations attributed to phishing campaigns). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments (e.g., monitor anomalies in use of files that do not normally initiate network connections or unusual connections initiated by regsvr32.exe, rundll.exe, SCF, HTA, MSI, DLLs, or msiexec.exe).

Log Sources
