Behavioral Detection of Spoofed GUI Credential Prompts, Detection Strategy DET0521

Archived: 2026-04-05 16:40:06 UTC

AN1440

Detects suspicious use of PowerShell, .NET, or script interpreters to spawn processes that mimic UAC prompts, often with credential capture dialogue boxes invoked from non-standard parent processes.

Log Sources

Mutable Elements

Field	Description
CommandLine	Tunable to detect suspicious prompts like 'Enter your password' or 'CredentialRequired'
ParentProcessName	Tune to flag UI prompts spawned from unexpected processes like cmd.exe or user scripts
TimeWindow	Scope correlation of script execution and prompt appearance

AN1441

Detects GUI-based credential prompts invoked via zenity/kdialog/dialog or X11 APIs from non-user-facing scripts or background shell sessions, often with authentication-related text.

Log Sources

Mutable Elements

Field	Description
ExecutableName	Filter zenity/kdialog prompts launched from unexpected parent shells
PromptString	Look for 'password', 'authentication required', or similar tokens

AN1442

Detects AppleScript or Objective-C usage to generate fake authentication windows (e.g., using display dialog or NSAlert) from user-launched or persistence-related processes.

Log Sources

Mutable Elements

Field	Description
ScriptContent	AppleScript snippets like 'display dialog' or 'with hidden answer'
ProcessPath	Tune out Apple-signed and expected automation tasks

---

Source: https://attack.mitre.org/detectionstrategies/DET0521#AN1440