

# Detection Strategy for T1546.016 - Event Triggered Execution via Installer Packages, Detection Strategy DET0330

Archived: 2026-04-05 16:16:55 UTC

## AN0938

Correlation of package install event with execution of postinstall scripts containing unknown binaries or abnormal CLI usage. Look for `/usr/sbin/installer` execution followed by child processes originating from postinstall script.

### Log Sources

Data Component	Name	Channel
<a href="#">Process Creation (DC0032)</a>	macos:unifiedlog	Execution of /usr/sbin/installer spawning child process from within /private/tmp or package contents
<a href="#">File Creation (DC0039)</a>	macos:unifiedlog	Creation or modification of postinstall scripts within .pkg or .mpkg contents

### Mutable Elements

Field	Description
ScriptLocation	Path to postinstall script varies depending on .pkg packaging and user temp directories.
ParentProcessName	Installers may vary (e.g., /usr/sbin/installer, Jamf, Munki).

## AN0939

Detection of maintainer scripts (e.g., postinst, preinst) being modified or executed during dpkg or rpm operations. Watch for script content that spawns additional processes or writes outside package scope.

### Log Sources

### Mutable Elements

Field	Description
ScriptName	May be postinst, preinst, prerm, or postrm depending on packaging system

Field	Description
PackageManager	Depends on system: dpkg, apt, rpm, yum, etc.

## AN0940

Detection of msiexec.exe running installer packages that result in anomalous process creation. Look for unexpected binaries executed by msiexec or custom action DLLs in the temp directory.

### Log Sources

### Mutable Elements

Field	Description
InstallerParent	Could be msiexec.exe or third-party wrapper like setup.exe.
ChildImagePath	Payload paths vary based on where installer extracts to (e.g., %TEMP%, C:\Users\Public).
ExecutionTimeWindow	Threshold for how soon a payload must run after msiexec to be considered related.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0330#AN0938>