User Execution – Malicious File via download/open → spawn chain (T1204.002), Detection Strategy DET0294

Archived: 2026-04-05 12:35:39 UTC

AN0819

User opens a file delivered by email, web, chat, or share. The handler application (Word/PDF reader/archiver) creates a file in user-controlled paths (Downloads, Temp, Desktop) and then spawns a new or unusual child process (e.g., powershell.exe, wscript.exe, cmd.exe, regsvr32.exe, rundll32.exe, msiexec.exe). Optional precursors include FileStreamCreated (URL/UNC) and Office → system32 batch writes.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Seconds/minutes to correlate file write to child spawn (e.g., 0–5m).
SuspiciousExtensions	Extensions and double-extension patterns to flag (exe,scr,lnk,pif,cpl,js,vbs,bat,cmd,ps1,hta,iso,lnk->cmd,docm,xlsm,pdf->exe, etc.).
UserPaths	Paths considered user-controlled (Downloads, Temp, Desktop, profile AppData staging).
ParentApps	List of user-facing apps that commonly open attachments for your org (reduce FPs or add weight).
SignerAllowList	Trusted code signers/publishers to suppress benign admin tools.

AN0820

User opens a downloaded document/installer leading to EndpointSecurity file create in ~/Downloads or ~/Library paths then an exec of a suspicious utility (osascript, bash/zsh, curl, chmod, open with -a Terminal). Correlates File Creation with subsequent process exec and, optionally, quarantine/LSQuarantine events.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	process_exec: image in {/bin/bash,/bin/zsh,/usr/bin/osascript,/usr/bin/python*,/usr/bin/curl,/usr/bin/ssh,/usr/bin/open} AND parent in {Preview, TextEdit, Microsoft Word, Microsoft Excel, AdobeReader, Archive Utility, Finder}
File Creation (DC0039)	macos:endpointsecurity	ES_EVENT_TYPE_NOTIFY_CREATE: path under /Users/*/(Downloads|Desktop|Library/*/Containers|Library/Group Containers) AND extension in SuspiciousExtensions

Mutable Elements

Field	Description
TimeWindow	Correlation window between file create and exec (e.g., ≤10m).
QuarantineRequired	Require com.apple.quarantine attribute present on the file for higher fidelity.

Field	Description
ParentApps	Approved document viewers/editors to anchor lineage.

AN0821

User or desktop application writes a new file to ~/Downloads, /tmp, or mounted removable media followed by execve of a risky interpreter/loader (bash, sh, python, perl, php, node, curl|wget piping to sh, ld.so, rdesktop, xdg-open - with unusual args). Uses auditd PATH+SYSCALL (open/creat/write/rename) with execve event linking.

Log Sources

Data Component	Name	Channel
File Creation (DC0039)	auditd:SYSCALL	open/create/rename: name in (/home/*/Downloads/*|/tmp/*|/run/user/*|/media/*) AND ext in SuspiciousExtensions
Process Creation (DC0032)	auditd:SYSCALL	execve: exe in {/bin/bash,/bin/sh,/usr/bin/python*,/usr/bin/perl,/usr/bin/php,/usr/bin/node,/usr/bin/curl,/usr/bin/wget,/ open,/usr/bin/ssh,/usr/bin/rundll32 (wine)} AND ppid process is a document viewer/browser

Mutable Elements

Field	Description
TimeWindow	Correlation window for audit events (e.g., ≤5m).
DesktopParentMap	Map common desktop apps (libreoffice, evince, firefox, chromium) for lineage anchoring.

Source: https://attack.mitre.org/detectionstrategies/DET0294#AN0820