User Execution – Malicious Copy & Paste (browser/email → shell with obfuscated one-liner) – T1204.004, Detection Strategy DET0340

Archived: 2026-04-05 15:42:04 UTC

AN0962

A user is socially engineered (web page, email, document) to open Run/PowerShell/CMD and paste an obfuscated one-liner. The chain is: (1) user context active in a browser/email/office app → (2) process creation of a command interpreter with suspicious arguments (base64/Invoke-Expression/web download/pipeline to shell) → (3) optional file drop in %TEMP% or %APPDATA% → (4) outbound network connection to an external domain. Events are correlated within a short window and with consistent user/session.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation horizon from parent app (browser/email/office) to interpreter spawn (e.g., 15 minutes).
ParentProcessAllowList	Legitimate automation that spawns PowerShell/CMD from Office/Email/Browser.
SuspiciousArgPatterns	List of command-line substrings indicating pasted one-liners (e.g., '-enc', 'FromBase64String', 'IEX(', 'DownloadString', 'Invoke-WebRequest', 'curl|wget.*|\s*(sh|bash|powershell)').
WritePaths	Directories treated as risky for first-stage drops (%TEMP%, %APPDATA%, %PUBLIC%).
OutboundCIDRBlockList	Internet ranges/domains to alert on for first-run egress.

AN0963

User pastes a multi-line or one-liner into a terminal (bash/zsh) that downloads/decodes and executes content. Chain: terminal exec of curl/wget/bash/sh with pipe to interpreter or base64-decode → transient file under /tmp|~/.cache → immediate outbound egress.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve: exe in (/usr/bin/bash,/usr/bin/sh,/usr/bin/zsh,/usr/bin/python*) AND cmdline matches '(curl|wget).*(||\s*sh|bash)|base64\s*-d|python\s*-c'
File Creation (DC0039)	auditd:SYSCALL	open: File creation under /tmp, /var/tmp, ~/.cache with executable bit or shell shebang
Network Connection Creation (DC0082)	NSM:Flow	New egress to Internet by the same UID/host shortly after terminal exec

Mutable Elements

Field	Description
TerminalProcessNames	Gui/tty terminals to monitor (gnome-terminal, konsole, iTerm2, tmux).
RiskyFilePaths	Temp/cache paths to watch for first-stage drops.
AnomalousUserSet	Users who should never run curl/wget or compilers.
TimeWindow	Exec → file → egress correlation window (e.g., 10 minutes).

AN0964

User pastes an obfuscated command into Terminal.app/iTerm2 that decodes or downloads code and executes. Detects Terminal/iTerm2 spawning bash/zsh/python with suspicious pipeline/base64 patterns followed by file writes in ~/Library or /tmp and outbound network connections.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	exec: ParentImage in (Terminal, iTerm2) AND Image in (/bin/zsh,/bin/bash,/usr/bin/python*) AND CommandLine matches '(curl|wget).*(||\s*sh|bash)|base64 -D|python -c'

Data Component	Name	Channel
Command Execution (DC0064)	macos:osquery	Interpreter exec with suspicious arguments as above
File Creation (DC0039)	macos:unifiedlog	create: New files in /tmp or ~/Library/Application Support/* with executable or script extensions
Network Traffic Content (DC0085)	NSM:Flow	Egress to non-approved networks from host after terminal exec

Mutable Elements

Field	Description
ParentAppScope	Terminal apps to treat as user-paste origins (Terminal, iTerm2, VSCode integrated terminal).
CommandPatternList	macOS-specific one-liner traits (pbpaste|base64 -D|curl ... | sh).
AllowListedDevUsers	Developers/automation accounts expected to run such commands.
