User-Initiated Malicious Library Installation via Package Manager (T1204.005), Detection Strategy DET0252

Archived: 2026-04-05 15:56:49 UTC

AN0698

User-initiated installation of Python (pip), NodeJS (npm), or other language libraries, followed by unexpected network connections, credential access, or startup file modifications. Defender sees `pip install` or `npm install` commands run by a non-root user, followed shortly by new `.py`, `.sh`, or `.js` files in hidden directories, or interpreter-based execution during boot/login.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve: Execution of pip, npm, gem, or similar package managers
File Creation (DC0039)	auditd:PATH	New .py/.js/.sh files written to ~/.local/, ~/.cache/, or /tmp/ within 5 min of package install
Network Traffic Content (DC0085)	NSM:Flow	http::request: Network connection to package registry or C2 from interpreter shortly after install

Mutable Elements

Field	Description
PackageManagerList	Monitored package managers (e.g., pip, npm, gem, poetry, conda)
InstallWritePaths	Directories to watch for post-install execution artifacts (e.g., ~/.local/, /usr/lib/python3.8/site-packages/)
UserContextScope	Filter to focus on non-system accounts (e.g., interactive shell users)
TimeWindow	Correlate install command to subsequent network/file activity (default: 5 min)

AN0699

Execution of `pip.exe`, `npm.cmd`, or MSI installers within user context, followed by script interpreter startup (e.g., python.exe) or PowerShell with unusual child processes or file writes in `%APPDATA%`, `%TEMP%`, or

`%LOCALAPPDATA%`. Defender correlates command-line install tools with Sysmon and Event Logs to trace downstream behavior.

Log Sources

Mutable Elements

Field	Description
AllowedParentProcesses	Filter expected automation tools (e.g., enterprise installers, known IDEs)
InstallPathsToWatch	Suspicious post-install write paths (e.g., %APPDATA%, %TEMP%)
ExecutableEntropyThreshold	Used for evaluating if dropped files are packed/obfuscated

AN0700

Execution of Homebrew, pip3, npm, or manually downloaded PKGs from Terminal or shell, followed by the creation of startup agents, interpreter spawns, or outbound connections to unfamiliar domains. Defender links Terminal commands to plist creation, unsigned binary launches, and `python3` or `node` processes connecting to remote endpoints.

Log Sources

Mutable Elements

Field	Description
StartupAgentPaths	Filter user persistence plist directories like ~/Library/LaunchAgents
UnsignedBinaryAlerting	Enable alerting for new binaries lacking Apple or organization signature
InstallToNetWindow	Correlate install action to interpreter-based network behavior

---