

# Cross-Platform Behavioral Detection of Python Execution, Detection Strategy DET0063

Archived: 2026-04-02 12:31:00 UTC

## AN0172

Detects Python execution via python.exe or py.exe with anomalous parent lineage (e.g., Office macros, LOLBAS), execution from unusual directories, or chained network/PowerShell/system-level activity.

### Log Sources

### Mutable Elements

Field	Description
ParentProcess	Non-standard processes spawning python.exe (e.g., winword.exe, mshta.exe).
ScriptPath	Execution of .py from temp directories or user profile paths.
TimeWindow	Execution outside maintenance or patch windows.
UserContext	Execution by low-privileged or service accounts.
ChildProcess	Python spawning suspicious binaries or scripts (e.g., PowerShell, certutil).

## AN0173

Detects native Python or framework-based execution from Terminal, embedded apps, or launchd jobs. Flags network calls, persistence writes, or system enumeration after Python launch.

### Log Sources

### Mutable Elements

Field	Description
ExecutionPath	Detects python scripts from ~/Downloads/, /Volumes/, or /tmp/.
ScriptName	Obfuscated or high entropy script names.
SpawnChain	Chained behavior: Python → bash → curl or Python → osascript.

## AN0174

Detects Python execution from non-standard user contexts or cron jobs that invoke outbound traffic, access sensitive files, or perform process injection (e.g., ptrace or /proc memory maps).

**Log Sources**

**Mutable Elements**

Field	Description
ScriptDir	Script invoked from /tmp, /var/tmp, or .hidden/ folders.
ScheduledContext	Execution from user cron or systemd timers outside of approved scripts.
NetworkActivity	Python performing HTTP/HTTPS without package updates.

**AN0175**

Detects Python script or interpreter execution on ESXi hosts via embedded BusyBox shells, nested installations, or dropped files via SSH or datastore mount. Flags unusual scripting or post-compromise enumeration behavior.

**Log Sources**

**Mutable Elements**

Field	Description
ExecutionSource	Script loaded from mounted datastore, SSH upload, or dropped via guest-to-host tools.
HostUser	Python launched under root or unknown user.
InstallPath	Custom Python binaries or packages in non-default paths (/tmp/python/bin/python3).

---

Source: <https://attack.mitre.org/detectionstrategies/DET0063#AN0172>