

# Detection of Proxy Execution via Trusted Signed Binaries Across Platforms, Detection Strategy DET0081

Archived: 2026-04-05 15:51:43 UTC

## AN0226

Execution of trusted, Microsoft-signed binaries such as `rundll32.exe`, `msiexec.exe`, or `regsvr32.exe` used to execute externally hosted, unsigned, or suspicious payloads through command-line parameters or network retrieval.

### Log Sources

### Mutable Elements

Field	Description
ParentProcessName	Used to profile unexpected parent-child relationships (e.g., <code>regsvr32.exe</code> not launched by <code>explorer.exe</code> )
SignedBinaryList	List of known signed binaries allowed for execution (e.g., <code>msiexec.exe</code> , <code>regsvr32.exe</code> )
CommandLineRegex	Regex to match suspicious arguments, such as URLs, script paths, or DLL entrypoints
RemoteDomainAllowlist	Filter to suppress activity contacting legitimate enterprise domains

## AN0227

Execution of trusted system binaries (e.g., `split`, `tee`, `bash`, `env`) used in uncommon sequences or chained behaviors to execute malicious payloads or perform actions inconsistent with normal system or script behavior.

### Log Sources

### Mutable Elements

Field	Description
TrustedBinaryList	Binaries like <code>`split`</code> , <code>`tee`</code> , <code>`env`</code> , <code>`awk`</code> , <code>`gzip`</code> , often used in benign scripts
AnomalyScore	Outlier model for process tree and command arguments

## AN0228

Use of system binaries such as `osascript` , `bash` , or `curl` to download or execute unsigned code or files in conjunction with application proxying.

### Log Sources

### Mutable Elements

Field	Description
TrustedUtilityList	macOS binary whitelist including <code>`usr/bin/osascript`</code> , <code>`bin/bash`</code> , <code>`usr/bin/curl`</code>
SignedToUnsignedTransition	Used to detect proxy execution from signed binary to unsigned payload

---

Source: <https://attack.mitre.org/detectionstrategies/DET0081#AN0228>