

# Detection Strategy for Hidden Windows, Detection Strategy DET0128

Archived: 2026-04-05 17:18:06 UTC

## AN0360

Suspicious use of scripting parameters or registry edits to hide process windows (e.g., powershell.exe - WindowStyle Hidden, or registry modifications pushing window positions off screen). Defender view: correlation of hidden execution with anomalous process lineage or hVNC-like CreateDesktop API calls.

### Log Sources

### Mutable Elements

Field	Description
HiddenProcessScope	Restrict to processes where hidden execution is unexpected (e.g., PowerShell, cmd, wscript).
ParentProcessCorrelation	Correlate hidden execution with suspicious parent processes to reduce false positives.

## AN0361

Suspicious invocation of GUI utilities or scripts with suppressed or redirected windowing options. Defender view: detection of X11 or Wayland calls to spawn windows that do not appear on active displays, or use of nohup/screen/tmux to mask interactive shells.

### Log Sources

### Mutable Elements

Field	Description
DisplayScope	Restrict monitoring to interactive GUI contexts rather than server/headless processes.

## AN0362

Modification of plist files to set apple.awt.UIElement or similar flags hiding app icons and windows, and dscl/command-line activity that suppresses visibility. Defender view: correlation of plist modifications with unexpected hidden user applications.

## Log Sources

## Mutable Elements

Field	Description
PlistScope	Restrict detection to application plists where UIElement flag is unexpected.
UserContext	Correlate plist modifications with the creating/modifying user to tune results.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0128#AN0360>