Detection Strategy for Content Injection, Detection Strategy DET0349

Archived: 2026-04-05 16:52:25 UTC

Analytics

- Windows
- Linux
- macOS

AN0992

Detect suspicious file creations and process executions triggered by browser activity (e.g., injected payloads written to %AppData% or Temp directories, then executed). Correlate network anomalies with subsequent local process creation or script execution.

Log Sources

Mutable Elements

Field	Description
MonitoredExtensions	File extensions to flag (exe, dll, js, vbs, sh, etc.).
SuspiciousParentProcesses	Browser processes (chrome.exe, firefox.exe, edge.exe, etc.) monitored as possible parents for malicious activity.
RedirectList	List of suspicious domains or URLs used for malicious redirects.

AN0993

Detect curl/wget commands saving executable/script payloads to /tmp or /var/tmp followed by execution. Monitor packet captures or IDS/IPS alerts for injected responses or mismatched content types.

Log Sources

Mutable Elements

Field	Description
TempDirectories	Directories such as /tmp and /var/tmp where injected files are often written.

AN0994

Monitor unified logs for processes spawned from Safari or other browsers that immediately load scripts or executables. Detect file drops in ~/Library/Caches or ~/Downloads that execute shortly after being written.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	Child processes of Safari, Chrome, or Firefox executing scripting interpreters
File Creation (DC0039)	macos:unifiedlog	File creation of unsigned binaries/scripts in user cache or download directories
Network Traffic Content (DC0085)	NSM:Flow	Content injection observed in HTTPS responses with mismatched certificates or altered payloads

Mutable Elements

Field	Description
MonitoredDirectories	macOS-specific directories where malicious payloads may be written.

Source: https://attack.mitre.org/detectionstrategies/DET0349#AN0994