Detection Strategy for HTML Smuggling via JavaScript Blob + Dynamic File Drop, Detection Strategy DET0313

Archived: 2026-04-05 14:55:21 UTC

AN0872

Detection of browser-based or email client-driven file creation (often from temp directories) following navigation to or execution of HTML files containing JavaScript Blob APIs or base64 Data URLs, with follow-on execution of the dropped payload. Leveraging Sysmon EventID 15 to inspect Zone.Identifier ADS for HostUrl/ReferrerUrl indicators (e.g., HostUrl=about:internet). Optional: absence of a large HTTP download record for the same URL/client in proxy logs (suggests local assembly)

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time range between HTML file open and file drop + execution (e.g., 1–10 minutes)
DroppedFileExtensionWatchlist	Tunable list of file extensions of interest (e.g., .js, .hta, .exe)
ParentProcessName	Expected processes that may drop files (e.g., browser, Outlook); tune for normal behavior

AN0873

Detection of browser-based downloads from HTML sources that trigger file creation in temp or user directories followed by execution of new files within short timeframes and suspicious parent-child lineage.

Log Sources

Mutable Elements

Field	Description
DownloadPathRegex	Regular expressions for common download paths (e.g., /tmp/, ~/Downloads/)
ExecutableTriggerWindow	Tunable range for follow-up process execution from dropped file (e.g., 5–15 minutes)

AN0874

Detection of HTML-based downloads via Safari/Chrome that create obfuscated files (e.g., .zip, .app, .js) in user directories and are followed by suspicious executions from preview or launch services.

Log Sources

Mutable Elements

Field	Description
QuarantineFlagCheck	Whether downloaded file has a quarantine flag and is bypassed via Gatekeeper
BlobKeywordAlertList	JavaScript strings that may indicate smuggling: msSaveBlob, download.href, createObjectURL
