Drive-by Compromise — Behavior-based, Multi-platform Detection Strategy (T1189), Detection Strategy DET0176

Archived: 2026-04-05 17:42:49 UTC

AN0498

Correlated evidence of anomalous browser/network behavior (suspicious external resource fetches and script injection patterns) followed by atypical child processes, ephemeral execution contexts, memory modification or process injection, and unexpected file drops. Defender sees network requests to previously unseen/suspicious domains or resources + browser process spawning unusual children or loading unsigned modules + file writes or registry changes shortly after those requests.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation time window between suspicious network fetch and subsequent process/file events. Tweak for environment latency and caching; default 2 minutes.
KnownGoodDomainsList	Allowlist of high-volume, benign domains used by corporate sites or CDNs to reduce false positives.
PayloadEntropyThreshold	Entropy threshold for downloaded script/binary content to surface likely obfuscated/packed payloads.
UserContext	Exclude or treat differently known administrative service accounts or build machines versus end-user contexts.

AN0499

Correlated evidence of browser or webview fetches to uncommon domains or mutated JS resources (proxy/NGFW logs + Zeek/HTTP logs) followed by unexpected interpreters or script engines executing (python, ruby, sh) spawned from browser processes or user sessions, rapid on-disk staging in /tmp, and outbound connections that deviate from baseline. Defender sees: uncommon resource fetch → short-lived child process executions from user browser context → file writes in temp directories → anomalous outbound C2-like connections.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve: execve calls where a browser/webview process is parent and child is interpreter (python, sh, ruby) or downloader (curl, wget)
Application Log Content (DC0038)	linux:syslog	Application or browser logs (webview errors, plugin enumerations) indicating suspicious script evaluation or plugin loads
Network Traffic Content (DC0085)	NSM:Flow	http::response: HTTP responses with suspicious content-type for scripts, long obfuscated javascript bodies, or redirects to exploit kit domains
File Creation (DC0039)	linux:Sysmon	New files in /tmp, /var/tmp, $HOME/.cache, executed within TimeWindow after browser HTTP fetch
Network Connection Creation (DC0082)	NSM:Connections	Outbound connections from newly spawned child processes or from the browser to uncommon endpoints or on anomalous ports

Mutable Elements

Field	Description
TempPathPatterns	Paths used for staging differ by distro and package manager; tune to include company-specific temp paths or exclude known benign build machines.
UserShellWhitelist	Whitelist known server/service accounts or CI/CD runners where shell executions are expected.
DomainRarityThreshold	Threshold for flagging domains based on internal popularity vs global rarity.

AN0500

Correlated evidence where Safari/Chrome/WebKit-based processes issue network requests for uncommon or obfuscated JS resources followed by spawning of script interpreters, launchd or ad-hoc binaries, unusual child processes, or dynamic library loads into browser processes. Defender sees: proxy/HTTP logs with suspicious resource content + unifiedlogs/ASL showing browser/plugin crashes or extension loads + process events indicating child process creation and file writes to /var/folders or /tmp shortly after the fetch.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	macos:unifiedlog	Logs from unifiedlogging that show browser crashes, plugin enumerations, extension installs or errors around the same time as suspicious network fetches
Process Creation (DC0032)	macos:unifiedlog	process_create: Process creation where parent is Safari/Google Chrome and child is script interpreter or signed-but-unusual helper binary
File Creation (DC0039)	macos:unifiedlog	New files written to /var/folders, /tmp, ~/Library/Caches, or ~/Downloads by browser context or its children
Network Traffic Content (DC0085)	NSM:Flow	HTTP/HTTPS requests for script resources flagged by content inspection (excessive obfuscation, eval usage, unusual redirects)
Process Modification (DC0020)	macos:unifiedlog	Anomalous dyld dynamic library loads or RWX memory mappings in browser process

Mutable Elements

Field	Description
SleepyUserThreshold	Volume thresholds for interactive user browsing vs. automated systems (e.g., shared kiosks) — tune to reduce FP in heavy-browsing employees.
ExtensionInstallPolicy	Policy setting that influences how extension installs are treated: strict policy reduces FP from known extension behavior.

AN0501

Post-compromise identity & session anomalies that follow a drive-by compromise: token reuse from new/unfamiliar IPs, anomalous sign-in patterns for previously inactive users, unexpected consent/grant events, or provisioning changes. Defender sees an endpoint/browser compromise (network + endpoint signals) followed by unusual IdP events: new refresh token issuance, consent/consent-grant events, odd MFA bypass patterns, or unusual OAuth client registrations.

Log Sources

Data Component	Name	Channel
User Account Authentication (DC0002)	azure:signinlogs	SignIn: Sign-ins flagged as atypical (new geographic region, unfamiliar device id) shortly after correlated endpoint/browser compromise times

Data Component	Name	Channel
Application Log Content (DC0038)	m365:unified	Application Consent grants, new OAuth client registrations, or unusual admin-level activities executed by a user account shortly after suspected drive-by compromise
User Account Metadata (DC0013)	saas:auth	Refresh token issuance or refresh token usage from new IPs or user agents
Logon Session Creation (DC0067)	AWS:CloudTrail	ConsoleLogin: If IdP backed by cloud provider, Console login from new IP/agent after correlated endpoint compromise

Mutable Elements

Field	Description
IdpAlertWindow	Time window to correlate IdP events to endpoint compromise alerts (default 30 minutes to 2 hours).
HighRiskCountryList	List of countries/IP zones considered high risk for sign-ins; used to tune geo-anomalies.
DeviceTrustLevel	Device trust scoring thresholds that influence whether a sign-in is considered suspicious.

Source: https://attack.mitre.org/detectionstrategies/DET0176#AN0500