INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-01 07:09 UTC

AI Productivity Extensions Turn Browsers Into Insider Threats: How GenAI Lures Are Weaponizing Trusted Browser APIs

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0246
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Google Chrome, Chrome Web Store extensions (18 identified by Unit 42; 32-extension AiFrame cluster with 260,000+ installs identified by Socket/LayerX), Gmail, Outlook, ChatGPT browser sessions
Published	2026-04-30T22:00:57+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Attackers are distributing malicious Chrome extensions disguised as AI productivity tools, including email assistants and automation utilities, to steal corporate credentials, email content, and proprietary data entered into AI platforms like ChatGPT. Unit 42 identified 18 such extensions; parallel research by Socket and LayerX found a coordinated cluster of 32 additional extensions with over 260,000 combined installs. Any employee using Chrome-based AI workflow tools represents a potential attack surface for credential theft, email exfiltration, and corporate data loss without triggering traditional network-layer controls.

Technical Analysis

Unit 42 documented 18 malicious Chrome extensions impersonating GenAI productivity tools, including email assistants, prompt helpers, and Model Context Protocol (MCP) automation utilities. Socket and LayerX independently identified the AiFrame cluster (32 extensions, 260,000+ installs) and the CL Suite, confirming coordinated, multi-operator exploitation. Attack mechanics rely on legitimate Chrome extension permissions: DOM access, webRequest, and storage APIs. Once installed, extensions perform DOM-based email exfiltration from active Gmail and Outlook sessions, intercept ChatGPT prompt content, harvest credentials via form input capture (CWE-200, CWE-319), establish persistent C2 channels over standard HTTPS using trusted browser APIs (T1071.001, T1041), and in some cases deploy remote access trojan payloads. No CVE applies; this is an abuse-of-privilege pattern against Chrome's extension trust model (CWE-269, CWE-306, CWE-494). Threat

actors include the 2vk/VK Styles operator (GitHub-attributed by Koi Security with moderate confidence), an unattributed AiFrame cluster operator, and an unattributed CL Suite operator. MITRE coverage includes T1176 (browser extensions), T1056.004 (credential API hooking), T1539 (session cookie theft), T1557 (adversary-in-the-browser), T1567/T1020 (exfiltration), and T1185 (browser session hijacking). No patch exists; remediation is policy and control-based.

Action Checklist

1. Step 1: Containment, Immediately audit all Chrome extensions installed across managed endpoints. Cross-reference installed extension IDs against the 18 extensions identified in the Unit 42 report (see sources list for complete extension ID list). Remove any matching extensions via endpoint management tooling (Intune, Google Admin, Jamf). Enforce a browser extension allowlist via Group Policy or Chrome Enterprise policy to block unauthorized installs.
2. Step 2: Detection, Query endpoint telemetry and EDR logs for Chrome extension installation events from the Chrome Web Store outside an approved allowlist. Review proxy and CASB logs for outbound HTTPS connections to C2 infrastructure identified in Unit 42 IOC disclosures. In Gmail and Google Workspace environments, audit OAuth token grants and check for unexpected forwarding rules or delegated access. Monitor SIEM for high-volume DOM interaction events or anomalous browser process behavior correlating with webRequest API usage. Alert on extensions requesting permissions: tabs, webRequest, storage, and activeTab in combination.
3. Step 3: Eradication, Remove all identified malicious extensions from affected endpoints. Revoke active browser sessions and force re-authentication for users on affected systems, prioritizing accounts with access to email, corporate AI platforms, and sensitive data repositories. Enforce Chrome Enterprise extension allowlist policy to prevent reinstallation. Disable Chrome Web Store access for managed devices if allowlist enforcement is not immediately achievable.
4. Step 4: Recovery, After extension removal and session revocation, validate that no persistent forwarding rules, delegated mailbox access, or OAuth grants remain active for affected accounts. Review ChatGPT and other AI platform session logs for unauthorized access. Audit credential stores and password manager access logs for anomalous reads. Monitor outbound traffic patterns for 2-4 weeks post-remediation for residual C2 beacon activity. Confirm Chrome Enterprise extension policy is enforced and audit-logged.
5. Step 5: Post-Incident, This campaign exposes three control gaps: absence of a browser extension allowlist, lack of CASB or DLP coverage for AI platform data inputs, and insufficient employee guidance on GenAI tool vetting. Implement Chrome Enterprise managed browser policy with extension allowlisting. Extend DLP policy scope to cover data entered into browser-based AI interfaces. Establish a formal approval process for AI productivity tools that includes extension permission review. Classify browser-based AI platforms as a data handling surface subject to the same controls as SaaS applications.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to legal, privacy, and executive leadership immediately if forensic review of Gmail audit logs, proxy logs, or ChatGPT session data confirms exfiltration of PII, PHI, PCI-scope data, or trade secrets, as this triggers breach notification obligations under GDPR, HIPAA, or applicable state privacy laws; also escalate if affected accounts include privileged users (IT admins, executives, finance) whose credentials or session tokens were in scope of the webRequest interception.
Recovery Notes	After extension removal and OAuth revocation, verify clean state by re-running the osquery Chrome extension enumeration query daily for 30 days and confirming zero matches against the Unit 42 and Socket/LayerX IOC extension ID lists. Monitor outbound proxy logs for connections to C2 domains and IP ranges from Unit 42 IOC disclosures for a minimum of 4 weeks, as compromised OAuth refresh tokens not fully revoked may enable intermittent beacon activity. Validate Chrome Enterprise extension policy enforcement is audit-logged in endpoint management tooling (Intune compliance reports, Google Admin audit log event type `CHROME_OS_DEVICE_POLICY_CHANGED`) to confirm policy persistence and detect any policy rollback attempts.
Forensic Artifacts	Chrome Extension Manifests and Local Extension Settings LevelDB — `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\[MaliciousExtensionID]\[version]\manifest.json` and `Local Extension Settings\[ID]\` — confirm declared permissions (webRequest, tabs, storage, activeTab) and recover cached DOM-scraped credential fragments or intercepted email content stored locally before C2 transmission | Chrome Cookies and Login Data SQLite databases — `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies` and `Login Data` — establish which authenticated sessions (Google, ChatGPT, Outlook, corporate SSO) were active and accessible to the malicious extension's permission scope during the infection window, defining the credential theft blast radius | Google Workspace Admin Audit Log — events `token.request`, `EMAIL_FORWARDING_CHANGE`, `DELEGATED_ADMIN_SETTINGS_CHANGED`, and `OAUTH_ACCESS_TOKEN_GRANTED` filtered to the campaign timeframe — identify OAuth grants issued to attacker-controlled applications and persistence mechanisms (forwarding rules, delegated access) established by the extension's Gmail API abuse | Outbound Proxy / DNS Logs filtered on Unit 42 C2 IOC Domains and IPs — TLS SNI values and HTTPS CONNECT destinations from `chrome.exe` processes correlating with extension installation timestamps — confirm active C2 communication and identify the volume and timing of data exfiltration events from affected endpoints | Chrome Preferences File (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Preferences`) — the `extensions.settings` JSON object records each extension's install timestamp, update URL, and granted permissions, providing a tamper-evident installation timeline that can be correlated with proxy logs to establish when the malicious AI productivity extension began intercepting webRequest traffic

Per-Action IR Details

Step 1: Containment — Immediately audit all Chrome extensions installed across managed endpoints. Cross-reference installed extension IDs against the 18 extensions identified in the Unit 42 report (https://unit42.paloaltonetworks.com/high-risk-gen-ai-browser-extensions/) and the AiFrame/CL Suite extension lists published by Socket and LayerX. Remove any matching extensions via endpoint management tooling (Intune, Google Admin, Jamf). Enforce a browser extension allowlist via Group Policy or Chrome Enterprise policy to block unauthorized installs.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST SI-3 (Malicious Code Protection), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Without Intune or Google Admin, enumerate all installed Chrome extensions across endpoints using PowerShell: `Get-ChildItem 'C:\Users\*\AppData\Local\Google\Chrome\User Data\Default\Extensions\'` to extract extension folder IDs. On macOS/Linux, query `~/Library/Application Support/Google/Chrome/Default/Extensions/`. Cross-reference each extracted ID against the Unit 42 list of 18 malicious extension IDs and the Socket/LayerX AiFrame cluster of 32 IDs manually. Remove matches by deleting the extension folder and clearing corresponding entries from `Preferences` and `Secure Preferences` JSON files in the Chrome profile directory. Deploy a `managed_policies.json` Chrome enterprise policy file locally to enforce an ExtensionInstallBlocklist with wildcard `*` and an ExtensionInstallAllowlist for approved IDs — no MDM required.

Evidence: Before removing any extensions, capture the full Chrome extension manifest and permissions for each installed extension from `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\[ExtensionID]\[version]\manifest.json` — these manifests will confirm which permissions (webRequest, tabs, storage, activeTab) were declared and whether a remote `content_scripts` or `background` page URL points to attacker-controlled infrastructure. Also snapshot `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\` (LevelDB) for each suspect extension ID, which may contain intercepted credential fragments or exfiltrated DOM data cached locally before transmission. Export the Chrome `Preferences` file to preserve the `extensions.settings` object recording install timestamps, update URLs, and granted permissions for each extension ID prior to removal.

Step 2: Detection — Query endpoint telemetry and EDR logs for Chrome extension installation events from the Chrome Web Store outside an approved allowlist. Review proxy and CASB logs for outbound HTTPS connections to C2 infrastructure identified in Unit 42 IOC disclosures. In Gmail and Google Workspace environments, audit OAuth token grants and check for unexpected forwarding rules or delegated access. Monitor SIEM for high-volume DOM interaction events or anomalous browser process behavior correlating with webRequest API usage. Alert on extensions requesting permissions: tabs, webRequest, storage, and activeTab in combination.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST DE.AE-02 (Potentially adverse events are analyzed to better understand associated activities), NIST DE.AE-03 (Information is correlated from multiple sources), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM or CASB, use Sysmon (Event ID 1 — Process Create) to detect `chrome.exe` spawning unusual child processes or making network calls to non-Google domains shortly after extension installation events. Configure Sysmon with a rule filtering on `chrome.exe` as parent process and any child process with external network connections to C2 domains listed in Unit 42 IOC disclosures. For OAuth audit without Google Workspace admin tooling, have each affected user navigate to `myaccount.google.com/permissions` and export the list of third-party apps with account access; look for grants made during the extension installation window. Use Wireshark or `tshark` on a representative endpoint to capture outbound TLS SNI values from `chrome.exe` processes: `tshark -i eth0 -Y 'ssl.handshake.extensions_server_name and frame.protocols contains "tls"' -T fields -e ssl.handshake.extensions_server_name` — match SNI hostnames against Unit 42 C2 IOC domains. For forwarding rule detection without Workspace admin access, use the Gmail API with a service account: `GET https://gmail.googleapis.com/gmail/v1/users/{userId}/settings/forwardingAddresses` and `GET .../filters` for each affected user.

Evidence: Query Chrome's `History` SQLite database at `%LOCALAPPDATA%\Google\Chrome\User Data\Default\History` for visits to Chrome Web Store pages (`chrome.google.com/webstore/detail/`) timestamped within the campaign window to establish when each malicious extension was installed. Extract the Chrome `Network Action Predictor` and `Network Persistent State` files to identify domains pre-resolved by Chrome's prefetch on behalf of background extension scripts. Pull Windows DNS client cache (`ipconfig /displaydns`) and browser DNS-over-HTTPS logs to surface C2 domains contacted by the webRequest API interceptors. For Gmail-specific exfiltration, export Google Workspace Admin audit logs filtering on event type `EMAIL_FORWARDING_CHANGE`, `DELEGATED_ADMIN_SETTINGS_CHANGED`, and `OAUTH_ACCESS_TOKEN_GRANTED` for the incident

timeframe to detect credential and content theft artifacts left in the mail platform.

Step 3: Eradication — Remove all identified malicious extensions from affected endpoints. Revoke active browser sessions and force re-authentication for users on affected systems, prioritizing accounts with access to email, corporate AI platforms, and sensitive data repositories. Enforce Chrome Enterprise extension allowlist policy to prevent reinstallation. Disable Chrome Web Store access for managed devices if allowlist enforcement is not immediately achievable.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST CM-7 (Least Functionality), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without Google Workspace admin for bulk session revocation, use the Google Admin SDK Directory API to iterate user accounts and call `POST https://admin.googleapis.com/admin/directory/v1/users/{userKey}/signOut` for each affected user, forcing invalidation of all active Google session cookies including those potentially cloned by the malicious extension's webRequest interception of authentication flows. For Microsoft accounts (Outlook/M365), use `Revoke-AzureADUserAllRefreshToken -ObjectId ` via the AzureAD PowerShell module to invalidate all OAuth refresh tokens. To prevent Chrome Web Store reinstall without MDM, push a local Chrome policy file setting `ExtensionInstallBlocklist: ['*']` and an `ExtensionInstallSources` policy removing `https://chrome.google.com/webstore/*` from allowed sources, deployed via a startup script or GPO registry write to `HKLM\SOFTWARE\Policies\Google\Chrome\`.

Evidence: Before revoking sessions, export the Chrome `Cookies` SQLite database from `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies` to preserve evidence of which authenticated sessions (Google, ChatGPT, Outlook) were active and potentially accessible to the malicious extension's `tabs` and `webRequest` permission scope — these cookie records establish the blast radius of potential session hijacking. Capture the Chrome `Login Data` SQLite database at the same profile path to determine whether the extension's `storage` API access may have exposed locally cached credentials. Document all active extension permissions from `chrome://extensions/` (screenshot or policy export) before policy enforcement removes visibility into what was previously installed.

Step 4: Recovery — After extension removal and session revocation, validate that no persistent forwarding rules, delegated mailbox access, or OAuth grants remain active for affected accounts. Review ChatGPT and other AI platform session logs for unauthorized access. Audit credential stores and password manager access logs for anomalous reads. Monitor outbound traffic patterns for 2-4 weeks post-remediation for residual C2 beacon activity. Confirm Chrome Enterprise extension policy is enforced and audit-logged.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), NIST SI-7 (Software, Firmware, and Information Integrity), NIST DE.CM-09 (Computing hardware and software, runtime environments, and their data are monitored), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Without a CASB to inspect AI platform traffic, configure outbound proxy logging (Squid or similar) to capture all HTTPS CONNECT requests to `chatgpt.com`, `chat.openai.com`, `outlook.office365.com`, and `mail.google.com` and alert on any authenticated sessions originating from service accounts or non-human user agents, which could indicate residual OAuth token use by attacker infrastructure. For Gmail forwarding rule validation without Workspace admin, script the Gmail API call `GET https://gmail.googleapis.com/gmail/v1/users/me/settings/filters` and `GET .../forwardingAddresses` for each affected user and compare output against a pre-incident baseline. Use osquery on each affected endpoint with the query `SELECT * FROM chrome_extensions WHERE identifier IN ('');` scheduled daily for the 4-week monitoring window to catch reinstallation attempts. For password manager audit without enterprise logging, check browser-integrated password manager sync logs in the Chrome `Sync Data` LevelDB store for anomalous read timestamps correlating

with the malicious extension's active period.

Evidence: Pull Google Workspace Admin Reports API event type `token.request` and `token.revoke` for all affected users covering 90 days prior to detection to establish the full OAuth grant timeline and identify any third-party applications that received access tokens during the campaign window — these represent potential data exfiltration paths beyond just the extension itself. Export ChatGPT usage logs from `chatgpt.com/settings` (session history) or OpenAI API logs for any API keys exposed to browser sessions on affected devices to determine whether proprietary data entered into ChatGPT prompts was accessible to the extension's DOM-scraping `content_scripts`. Retain Chrome `Network Persistent State` and proxy logs for the 4-week post-remediation monitoring period as a baseline comparison dataset for detecting residual C2 beacon patterns matching the periodicity and destination profiles in Unit 42 IOC disclosures.

Step 5: Post-Incident — This campaign exposes three control gaps: absence of a browser extension allowlist, lack of CASB or DLP coverage for AI platform data inputs, and insufficient employee guidance on GenAI tool vetting. Implement Chrome Enterprise managed browser policy with extension allowlisting. Extend DLP policy scope to cover data entered into browser-based AI interfaces. Establish a formal approval process for AI productivity tools that includes extension permission review. Classify browser-based AI platforms as a data handling surface subject to the same controls as SaaS applications.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AU-2 (Event Logging), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Without CASB or commercial DLP, deploy a free browser extension policy using Chrome's `URLBlocklist` managed policy to block `chrome.google.com/webstore` for non-admin users and require IT-reviewed allowlist additions via a lightweight change request form. Write a Sigma rule targeting proxy logs to alert on POST requests exceeding 10KB to `chatgpt.com/backend-api/conversation` or `api.openai.com/v1/chat/completions` from endpoints not in an approved AI-access list, as a compensating DLP control for data entered into ChatGPT. Publish an internal one-page GenAI tool vetting checklist (minimum: extension permissions review, developer identity verification, privacy policy review for data retention) and distribute via security awareness tooling or email — this addresses the employee guidance gap identified in the campaign at zero cost. Subscribe the security team to Unit 42, Socket, and CISA vulnerability advisories via RSS to receive future AI-lure extension campaign disclosures without requiring a paid threat intel feed.

Evidence: Compile a lessons-learned report documenting the specific extension IDs removed, the number of affected users per extension, the OAuth grants revoked, and any confirmed data exfiltration indicators from proxy and Gmail audit logs — this record satisfies NIST IR-5 (Incident Monitoring) documentation requirements and provides the baseline for measuring improvement at the next tabletop exercise. Retain all forensic artifacts (Chrome profile snapshots, OAuth grant exports, proxy logs, Sysmon captures) for a minimum of 12 months per NIST AU-11 (Audit Record Retention) to support potential regulatory breach notification inquiries if PII or regulated data was confirmed in scope of the exfiltrated email content or ChatGPT session data.

Detection Guidance

Primary detection signal: Chrome extension installations outside an approved allowlist, particularly extensions requesting DOM access, webRequest, storage, and activeTab permissions in combination. Query EDR telemetry for Chrome extension install events (Windows: look for new subdirectories under AppData\Local\Google\Chrome\User Data\Default\Extensions; macOS: ~/Library/Application Support/Google/Chrome/Default/Extensions). Cross-reference extension IDs against the Unit 42 published IOC list. In proxy and firewall logs, look for low-volume, periodic HTTPS POST requests to uncommon domains

originating from Chrome renderer processes, consistent with C2 beacon behavior (T1071.001). In Google Workspace: audit Apps Script and OAuth grants for recently authorized third-party applications. In Microsoft 365/Outlook environments: review mailbox audit logs for unexpected delegate access or forwarding rule creation. Behavioral indicator: users who installed a GenAI Chrome extension within the past 90 days and subsequently had email forwarding rules created or OAuth tokens issued to unrecognized applications. MITRE techniques to hunt: T1176, T1539, T1185, T1056.002, T1056.004, T1020.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://unit42.paloaltonetworks.com/high-risk-gen-ai-browser-extensions/`	Unit 42 primary research report containing extension IDs and IOC disclosures for the 18 identified malicious extensions	HIGH
DOMAIN	`See Unit 42 report for C2 domain list`	C2 infrastructure domains are published in the Unit 42 technical report; specific values not reproduced here to avoid transcription error	HIGH

Framework Mappings

MITRE-ATTACK

- **T1090** — Proxy
- **T1176** — Software Extensions
- **T1567** — Exfiltration Over Web Service
- **T1056.004** — Credential API Hooking
- **T1204.001** — Malicious Link
- **T1557** — Adversary-in-the-Middle
- **T1113** — Screen Capture
- **T1539** — Steal Web Session Cookie
- **T1059.007** — JavaScript
- **T1020** — Automated Exfiltration
- **T1564.001** — Hidden Files and Directories
- **T1056.002** — GUI Input Capture
- **T1185** — Browser Session Hijacking
- **T1071.001** — Web Protocols
- **T1041** — Exfiltration Over C2 Channel

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection

- **SI-4** — System Monitoring
- **SC-8** — Transmission Confidentiality and Integrity
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **AC-6** — Least Privilege
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **3.10** — Encrypt Sensitive Data in Transit
- **6.3** — Require MFA for Externally-Exposed Applications
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security
- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1090	Proxy	Command-And-Control
T1176	Software Extensions	Persistence

Technique ID	Technique Name	Tactic
T1567	Exfiltration Over Web Service	Exfiltration
T1056.004	Credential API Hooking	Collection
T1204.001	Malicious Link	Execution
T1557	Adversary-in-the-Middle	Credential-Access
T1113	Screen Capture	Collection
T1539	Steal Web Session Cookie	Credential-Access
T1059.007	JavaScript	Execution
T1020	Automated Exfiltration	Exfiltration
T1564.001	Hidden Files and Directories	Defense-Evasion
T1056.002	GUI Input Capture	Collection
T1185	Browser Session Hijacking	Collection
T1071.001	Web Protocols	Command-And-Control
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
Unit 42	https://unit42.paloaltonetworks.com/high-risk-gen-ai-browser-extens...	T3
	https://unit42.paloaltonetworks.com/high-risk-gen-ai-browser-extens...	T3
	https://www.nytimes.com/2026/04/06/technology/ai-cybersecurity-hack...	T2
	https://thehackernews.com/2026/02/malicious-chrome-extensions-caugh...	T3
Advanced URL Filtering - Palo Alto Networks	https://www.paloaltonetworks.com/network-security/advanced-url-filt...	T3

Generated 2026-05-01 07:09 UTC by TJS Security Command Center