INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-29 19:06 UTC

Trusted Platform Abuse: ChatGPT Share Links, Claude Artifacts, and M365 Direct Send Weaponized for Malware and Phishing Delivery

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0382
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	OpenAI ChatGPT (chatgpt.com shared links), Anthropic Claude (Claude Artifacts), Microsoft 365 (Direct Send), Google Ads, macOS, Windows
Published	2026-05-29T14:21:36
Discovery Source	Rss

Executive Summary

Attackers are abusing legitimate features of ChatGPT, Claude, and Microsoft 365 to deliver malware and steal credentials without triggering standard security controls. Because the malicious content is hosted on trusted domains (chatgpt.com, claude.ai) or sent through authenticated internal mail infrastructure, blocklists and reputation-based defenses do not apply. Any organization whose employees use these platforms or rely on Microsoft 365 mail is exposed, and credential theft or malware infection may occur without any security alert firing.

Technical Analysis

Three structurally related campaigns exploit platform design features rather than software vulnerabilities, representing Living-off-Trusted-Sites (LoTS) tradecraft. (1) LLMShare (Push Security): Attackers create ChatGPT shared conversation links that render fake OpenAI outage pages on chatgpt.com, serving malware payloads from a domain that is broadly allowlisted. (2) Claude Artifacts (7ai): Anthropic's interactive content rendering feature is abused to host malicious pages or deliver malware via claude.ai infrastructure; MacSync macOS malware is one confirmed payload, distributed via Google Ads redirecting to Claude Artifacts. (3) M365 Direct Send (Varonis/BleepingComputer): Attackers leveraging Ukrainian-attributed IP infrastructure abuse Microsoft 365's Direct Send SMTP relay feature to inject email into victim organizations' mail flow. Because Direct Send uses the organization's own MX endpoint, messages pass SPF, DKIM, and DMARC checks and appear to originate from internal senders. No CVE is assigned; the attack surface is feature abuse. Relevant

CWEs: CWE-601 (Open Redirect), CWE-940 (Improper Verification of Source of Communication Channel), CWE-451 (UI Misrepresentation of Critical Information), CWE-289 (Authentication Bypass by Alternate Name), CWE-290 (Authentication Bypass by Spoofing). Note: CWE mapping reflects the design patterns exploited, not software vulnerabilities; no vendor patches are applicable. MITRE ATT&CK: T1566.002 (Spearphishing Link), T1608.005 (Link Target), T1036.005 (Match Legitimate Name or Location), T1204.002 (Malicious File), T1071.003 (Web Protocols), T1056.003 (Web Portal Capture), T1583.008 (Serverless Infrastructure), T1583.006 (Web Services), T1204.001 (Malicious Link), T1598.003 (Spearphishing Link for Credentials), T1534 (Internal Spearphishing), T1608.004 (Stage Capabilities via Drive-by Compromise), T1497.001 (Virtualization/Sandbox Evasion). Mitigations are defensive controls and user awareness.

Action Checklist

1. Step 1: Containment. Immediately review mail gateway rules for inbound messages using your own domain as the sending address originating from external IP ranges. Block or quarantine Direct Send traffic not originating from your authorized M365 tenant IP ranges. Per NIST SP 800-61 (Computer Security Incident Handling Guide), Preparation and Detection/Analysis phases, activate your incident response plan if suspicious M365 mail flow is detected. Cross-reference sending IPs against Ukrainian IP ranges flagged in published threat reports and apply conditional blocks at the mail gateway.
2. Step 2: Detection. Query email security logs for messages passing SPF/DKIM/DMARC that originated via Direct Send from non-standard IPs (NIST AU-6, CIS Controls v8 8.2). In endpoint detection tooling, search for process execution chains originating from browser child processes that downloaded from chatgpt.com shared-link paths (/share/) or claude.ai artifact paths. Flag MacSync-related indicators on macOS endpoints: look for unsigned binaries dropped to ~/Library or /tmp following browser activity on claude.ai. Review proxy or DNS logs for outbound connections to chatgpt.com/share/* and claude.ai/artifacts/* outside normal business application use.
3. Step 3: Eradication. For M365 Direct Send abuse: audit all connector configurations in the Exchange Admin Center; restrict Direct Send to explicitly authorized source IP ranges only (align with NIST CM-7, Least Functionality, and CIS Controls v8 4.2, Secure Configuration for Network Infrastructure). Disable Direct Send entirely if not operationally required. For ChatGPT/Claude exposure: block chatgpt.com/share/* and claude.ai/artifacts/* at the web proxy for endpoints that have no legitimate business requirement for these paths. For MacSync: quarantine and forensically examine any macOS endpoint that accessed Google Ads redirect URLs leading to claude.ai.
4. Step 4: Recovery. After Direct Send lockdown, validate by sending a test message from an unauthorized external IP using your domain; confirm it is rejected or quarantined. Verify DMARC policy is set to reject (p=reject), not quarantine or none. Re-examine any accounts that received suspicious internal-appearing email for credential compromise indicators, including unexpected MFA prompts or login anomalies (NIST AC-7, Unsuccessful Login Attempts). On macOS endpoints where MacSync activity is suspected, perform full malware scans, revoke and rotate affected credentials per organizational credential rotation policy, and validate integrity of browser credential stores.
5. Step 5: Post-Incident. This campaign exposes a structural gap: perimeter defenses calibrated to domain reputation do not protect against LoTS tradecraft. Conduct a control review against NIST SI-4 (System Monitoring) to ensure behavioral detection supplements reputation-based controls. Implement user awareness training specifically covering AI platform abuse scenarios; employees must understand that a chatgpt.com or claude.ai URL is not inherently safe. Review your DMARC posture across all domains (CIS Controls v8 6.2, Email Security). Consider deploying sandbox-based link analysis that evaluates content at

destination, not just domain reputation. Document this campaign in your threat model and update detection rules to cover future LoTS-pattern abuse of newly trusted platforms.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to legal, privacy officer, and executive leadership immediately if Microsoft 365 Unified Audit Log review confirms MailItemsAccessed or FileAccessed events from accounts targeted by Direct Send spoofed mail, or if MacSync keychain exfiltration is confirmed on any endpoint storing credentials to systems processing PII, PHI, or PCI data — both conditions may trigger breach notification obligations under GDPR Article 33, HIPAA 45 CFR §164.412, or applicable state privacy statutes within 72 hours of confirmed discovery.
Recovery Notes	After Direct Send lockdown and DMARC enforcement at p=reject, monitor Microsoft 365 Message Trace and Entra ID Sign-In Logs daily for a minimum of 30 days for re-attempt patterns, since this campaign's operators have demonstrated persistence and platform-switching behavior across ChatGPT, Claude, and M365. Any macOS endpoints from which MacSync was eradicated should be monitored via Unified Log collection for 14 days for LaunchAgent re-installation attempts, as stealer malware in this class commonly includes a re-installer stub. Credential rotation is not sufficient alone — validate that rotated accounts show no OAuth application grants or mail forwarding rules added during the exposure window, as these are common post-compromise persistence mechanisms in M365-targeting campaigns.
Forensic Artifacts	macOS Quarantine Events database at ~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2 (SQLite) — records the exact claude.ai artifact URL that served the MacSync binary, the download timestamp, and the browser bundle ID, directly linking the malware drop to the LoTS delivery chain. | Exchange Online Message Trace and full RFC-5322 headers for all messages where Authentication-Results shows SPF=pass or DMARC=pass but the originating IP (X-Originating-IP or top Received header) falls outside Microsoft's published M365 egress ranges — this is the forensic signature of Direct Send abuse passing authentication checks. | Microsoft 365 Unified Audit Log entries (record type MailItemsAccessed and FileAccessed) for accounts targeted by spoofed internal-appearing email, exportable via Search-UnifiedAuditLog -RecordType ExchangeItemAggregated, to determine whether credential phishing from Direct Send abuse resulted in account access. | macOS LaunchAgents directory contents at ~/Library/LaunchAgents/ and associated binary paths referenced in plist files — MacSync persistence is established here, and the plist will contain the executable path, run interval, and any C2 communication arguments that reconstruct the attacker's post-compromise command structure. | Web proxy or DNS resolver query logs filtered for chatgpt.com/share/* and claude.ai/artifacts/* with associated internal client IPs and timestamps — cross-referenced against the macOS Quarantine database timestamps, this correlation identifies every endpoint that accessed a weaponized shared link or artifact path and establishes the full scope of exposure.

Per-Action IR Details

Step 1: Containment — Immediately review mail gateway rules for inbound messages using your own domain as the sending address originating from external IP ranges. Block or quarantine Direct Send traffic not originating from your authorized M365 tenant IP ranges. Per NIST IR-4 (Incident Handling), activate your incident response plan if suspicious M365 mail flow is detected. Cross-reference sending IPs against

Ukrainian IP ranges flagged in the Varonis report and apply conditional blocks at the mail gateway.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-4 (Information Flow Enforcement), NIST SC-5 (Denial of Service Protection), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Without an enterprise mail gateway appliance, use Exchange Online PowerShell to enumerate all inbound connectors: Get-InboundConnector | Select Name,SenderIPAddresses,Enabled. Then run Get-MessageTrace -StartDate (Get-Date).AddDays(-7) -EndDate (Get-Date) | Where-Object {$_.SenderAddress -like '*@yourdomain.com' -and $_.FromIP -notlike '52.100.*'} to surface Direct Send abuse using your own domain from external IPs. Block offending IPs via the Microsoft 365 Defender portal under Tenant Allow/Block List for a 2-person team with no on-prem gateway.

Evidence: Before blocking, preserve: (1) Exchange Online Message Trace logs (retention 90 days) capturing SenderAddress, FromIP, RecipientAddress, and MessageId for all messages where SenderAddress matches your domain but FromIP falls outside Microsoft's published M365 IP ranges (aka.ms/o365ips). (2) Mail gateway or MTA logs showing the SMTP EHLO/MAIL FROM sequence — Direct Send abuse will show MAIL FROM using your domain with an originating IP not in your SPF record. (3) Full RFC-5322 message headers from any suspicious messages, preserving the Received chain to reconstruct the true originating infrastructure.

Step 2: Detection — Query email security logs for messages passing SPF/DKIM/DMARC that originated via Direct Send from non-standard IPs (NIST AU-6, CIS 8.2). In endpoint detection tooling, search for process execution chains originating from browser child processes that downloaded from chatgpt.com shared-link paths (/share/) or claude.ai artifact paths. Flag MacSync-related indicators on macOS endpoints: look for unsigned binaries dropped to ~/Library or /tmp following browser activity on claude.ai. Review proxy or DNS logs for outbound connections to chatgpt.com/share/* and claude.ai/artifacts/* outside normal business application use.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: On macOS endpoints without EDR, use the built-in Unified Log to detect MacSync staging: log show --predicate 'process == "curl" OR process == "osascript"' --last 24h | grep -E '(Library|tmp)'. For unsigned binary detection, run: find ~/Library /tmp -newer /var/log/install.log -type f -exec spctl --assess --verbose {} \; 2>&1 | grep rejected. On Windows, deploy Sysmon with a config that logs Event ID 1 (Process Create) and Event ID 3 (Network Connection) and search for browser child processes (chrome.exe, msedge.exe, safari) spawning cmd.exe, powershell.exe, or curl.exe with network connections to chatgpt.com or claude.ai. Use the free Sigma rule community (github.com/SigmaHQ/sigma) and search for rules tagged 'lolbas' combined with browser parent process patterns.

Evidence: Capture before analysis: (1) macOS Unified Logs (log collect --output /tmp/incident.logarchive) preserving browser download events and any curl/osascript execution within 30 minutes of claude.ai visits. (2) macOS Quarantine database at ~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2 — this SQLite file records every file downloaded via browser including the originating URL, timestamp, and bundle ID, directly linking MacSync drops to claude.ai artifact paths. (3) Web proxy or DNS resolver logs filtered for chatgpt.com/share/* and claude.ai/artifacts/* with associated client IPs and timestamps. (4) Windows Sysmon Event ID 1 logs for browser child process spawns correlating to chatgpt.com or claude.ai network connections (Event ID 3). (5) Exchange Online message headers from any email that passed SPF/DKIM/DMARC authentication but originated via Direct Send, preserving the Authentication-Results header to document the authentication pass that enabled delivery.

Step 3: Eradication — For M365 Direct Send abuse: audit all connector configurations in the Exchange Admin Center; restrict Direct Send to explicitly authorized source IP ranges only (align with NIST CM-7, Least Functionality, and CIS 4.2, Secure Configuration for Network Infrastructure). Disable Direct Send entirely if not operationally required. For ChatGPT/Claude exposure: block chatgpt.com/share/* and claude.ai/artifacts/* at

the web proxy for endpoints that have no legitimate business requirement for these paths. For MacSync: quarantine and forensically examine any macOS endpoint that accessed Google Ads redirect URLs leading to claude.ai.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST CM-7 (Least Functionality), NIST AC-17 (Remote Access), NIST SI-3 (Malicious Code Protection), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 2.3 (Address Unauthorized Software)

Compensating: For teams without enterprise proxy, implement path-level blocking using Windows Firewall with Advanced Security (WFAS) or DNS Response Policy Zones (RPZ) on an internal resolver — add CNAME wildcard blocks for chatgpt.com and claude.ai subpaths where no business need exists; this is blunt but effective for small teams. For macOS MacSync eradication without MDM, use a shell script deployed via SSH: find / -name 'MacSync' -o -name '.MacSync' 2>/dev/null; launchctl list | grep -i sync; then remove persistence via: launchctl remove com.[suspiciouslabel] and delete associated plist from ~/Library/LaunchAgents/. Run ClamAV (brew install clamav) with freshclam update against the ~/Library and /tmp paths on each suspect endpoint.

Evidence: Before eradicating MacSync from macOS endpoints, image or collect: (1) Full contents of ~/Library/LaunchAgents/ and /Library/LaunchDaemons/ to document persistence mechanism plist files (MacSync typically persists via LaunchAgent for user-context execution). (2) The MacSync binary itself — hash with sha256sum and submit to VirusTotal or your threat intel platform before deletion. (3) macOS keychain access logs if available, as MacSync targets credential stores; run security dump-keychain -d ~/Library/Keychains/login.keychain-db and preserve output. (4) Network capture (tcpdump -i en0 -w /tmp/macsync_c2.pcap) run for 10–15 minutes on a sandboxed duplicate to capture C2 callback patterns before eradication on production systems.

Step 4: Recovery — After Direct Send lockdown, validate by sending a test message from an unauthorized external IP using your domain; confirm it is rejected or quarantined. Verify DMARC policy is set to reject (p=reject), not quarantine or none. Re-examine any accounts that received suspicious internal-appearing email for credential compromise indicators, including unexpected MFA prompts or login anomalies (NIST AC-7, Unsuccessful Logon Attempts; D3-LAM, Local Account Monitoring). On macOS endpoints where MacSync activity is suspected, perform full malware scans, revoke and rotate affected credentials (D3-CRO, Credential Rotation), and validate integrity of browser credential stores.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-7 (Unsuccessful Logon Attempts), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.3 (Disable Dormant Accounts), CIS 6.5 (Require MFA for Administrative Access)

Compensating: DMARC validation without commercial tooling: use MXToolbox DMARC checker (mxtoolbox.com/dmarc.aspx) or Google Admin Toolbox (toolbox.googleapps.com/apps/checkmx/) — both free. For Direct Send lockdown validation, use swaks (Swiss Army Knife for SMTP, free): swaks --to victim@yourdomain.com --from spoof@yourdomain.com --server [your-MX-record] and confirm rejection. For credential compromise review on M365 without SIEM, run: Get-MgAuditLogSignIn -Filter "userPrincipalName eq 'user@yourdomain.com'" | Where-Object {$_.RiskLevelDuringSignIn -ne 'none'} using the free Microsoft Graph PowerShell SDK. For macOS browser credential store integrity, check for unauthorized keychain access in Unified Logs: log show --predicate 'subsystem == "com.apple.securityd"' --last 48h | grep -i 'keychain'.

Evidence: Before credential rotation, preserve: (1) Microsoft Entra ID (Azure AD) Sign-In Logs for all accounts that received Direct Send-spoofed messages — export via Get-MgAuditLogSignIn filtered to the incident timeframe, capturing IPAddress, ClientAppUsed, ConditionalAccessStatus, and RiskDetail fields. (2) Microsoft 365 Unified Audit Log entries (Search-UnifiedAuditLog) for MailItemsAccessed, FileAccessed, and UserLoggedIn operations from accounts targeted by spoofed mail, to determine if credential phishing succeeded. (3) macOS browser credential store files prior to rotation: Chrome stores credentials at ~/Library/Application Support/Google/Chrome/Default/Login Data (SQLite); Safari at ~/Library/Keychains/ — copy these for forensic review before any credential rotation invalidates the

forensic baseline.

Step 5: Post-Incident — This campaign exposes a structural gap: perimeter defenses calibrated to domain reputation do not protect against LoTS tradecraft. Conduct a control review against NIST SI-4 (System Monitoring) to ensure behavioral detection supplements reputation-based controls. Implement user awareness training specifically covering AI platform abuse scenarios — employees must understand that a chatgpt.com or claude.ai URL is not inherently safe. Review your DMARC posture across all domains (CIS 6.3 analog for mail authentication). Consider deploying sandbox-based link analysis that evaluates content at destination, not just domain reputation. Document this campaign in your threat model and update detection rules to cover future LoTS-pattern abuse of newly trusted platforms.

NIST Phase: Post Incident

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

Controls: NIST SI-4 (System Monitoring), NIST AT-2 (Literacy Training and Awareness), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For sandbox-based link analysis without commercial budget, deploy URLScan.io API (free tier) integrated with a Python script that auto-submits URLs from email headers before delivery confirmation — this evaluates chatgpt.com/share/* destination content, not just domain reputation. Write Sigma rules (free, github.com/SigmaHQ/sigma) targeting browser process spawning executables from %TEMP% or ~/Library following navigation to chatgpt.com or claude.ai, and deploy via Sysmon + Windows Event Forwarding to a free ELK stack. For awareness training on a zero budget, create a one-page brief with actual screenshots of this campaign's ChatGPT share link and Claude artifact delivery mechanism — specificity dramatically outperforms generic phishing awareness in behavioral change.

Evidence: Post-incident documentation must capture: (1) All Sigma or detection rules created or modified during this incident, versioned in Git, as the authoritative record of detection coverage improvement. (2) The full kill chain reconstruction mapping attacker actions to MITRE ATT&CK techniques — specifically T1566.002 (Spearphishing Link) for chatgpt.com/claude.ai delivery, T1071.003 (Web Protocols — mail) for Direct Send abuse, and T1539 (Steal Web Session Cookie) if MacSync targeted browser credential stores — this document becomes the threat model update. (3) DMARC aggregate (rua) and forensic (ruf) reports from the incident period, which provide independent third-party evidence of Direct Send abuse attempts across your domain that can be used for lessons-learned reporting and regulatory documentation if PII was exposed.

Detection Guidance

M365 Direct Send Abuse: Query Exchange message trace logs for inbound messages where the sender domain matches your organization's domain but the source IP is not in your authorized M365 sending IP ranges. In Microsoft Defender or your SIEM, create an alert rule with the following logic: Example query: sender_domain = [your domain] AND source_ip NOT IN [your authorized M365 IP list] AND auth_results includes SPF=pass. Flag any message passing authentication checks that originated via an MX-targeted SMTP connection from an unrecognized IP. ChatGPT Share Link Abuse: In web proxy logs, alert on user access to chatgpt.com/share/* URLs where the next HTTP action is a file download or redirect to a non-OpenAI domain. Behavioral indicator: browser child process spawning an executable or script following navigation to a chatgpt.com/share/ path. Claude Artifacts Abuse / MacSync: In DNS or proxy logs, flag access to claude.ai/artifacts/* that results in a file download. On macOS endpoints, monitor for new unsigned binaries created in ~/Library/Application Support, /tmp, or ~/Downloads following browser-initiated downloads from claude.ai. MacSync-specific: look for persistence mechanisms including LaunchAgent plist creation in ~/Library/LaunchAgents after a claude.ai session. Google Ads redirect chain: look for ad-network redirect chains (doubleclick.net, googleadservices.com) terminating at claude.ai rather than an expected commercial destination. General LoTS detection: Implement

content inspection at the proxy layer that evaluates page content and download behavior, not just domain reputation. NIST AU-6 (Audit Record Review) and CIS Controls v8 8.2 (Collect Audit Logs) provide the logging baseline required to support these queries.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`chatgpt.com/share/*`	ChatGPT shared conversation link path pattern used by LLMShare campaign to host fake OpenAI outage pages and serve malware; wildcard pattern — specific URLs vary per campaign instance.	HIGH
URL	`claude.ai/artifacts/*`	Claude Artifacts path pattern used to host malicious interactive content and deliver MacSync and other malware; specific artifact URLs vary per campaign instance.	HIGH
DOMAIN	`claude.ai`	Legitimate Anthropic domain abused as delivery infrastructure; flag unexpected file downloads or executable drops originating from sessions on this domain.	MEDIUM
DOMAIN	`chatgpt.com`	Legitimate OpenAI domain abused via shared link feature; flag downloads or redirects to non-OpenAI domains following access to /share/ paths.	MEDIUM
IP	`Ukrainian IP ranges (unspecified)`	Varonis attributed M365 Direct Send abuse campaign to Ukrainian IP infrastructure; specific IPs not publicly disclosed in available sources — consult Varonis report for IOC detail.	LOW

Framework Mappings

MITRE-ATTACK

- **T1566.002** — Spearphishing Link
- **T1608.005** — Link Target
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1204.002** — Malicious File
- **T1071.003** — Mail Protocols
- **T1056.003** — Web Portal Capture
- **T1583.008** — Malvertising

- **T1583.006** — Web Services
- **T1204.001** — Malicious Link
- **T1598.003** — Spearphishing Link
- **T1534** — Internal Spearphishing
- **T1608.004** — Drive-by Target
- **T1497.001** — System Checks

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **SR-2** — Supply Chain Risk Management Plan

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.002	Spearphishing Link	Initial-Access
T1608.005	Link Target	Resource-Development
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion

Technique ID	Technique Name	Tactic
T1204.002	Malicious File	Execution
T1071.003	Mail Protocols	Command-And-Control
T1056.003	Web Portal Capture	Collection
T1583.008	Malvertising	Resource-Development
T1583.006	Web Services	Resource-Development
T1204.001	Malicious Link	Execution
T1598.003	Spearphishing Link	Reconnaissance
T1534	Internal Spearphishing	Lateral-Movement
T1608.004	Drive-by Target	Resource-Development
T1497.001	System Checks	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/chatgpt-share-links-...	T3
	https://www.bleepingcomputer.com/news/security/microsoft-365-direct...	T3
Claude Fraud - When Trusted Tools Become the Attack Surface - Blog	https://blog.7ai.com/claude-fraud-malware-campaign-ai-developer-tools	T3
MacSync is spreading through Google ads that lead directly to ...	https://www.facebook.com/ethical.hack.group/posts/macsync-is-spread...	T3
Claude.ai Malware Campaign via Google Ads - LinkedIn	https://www.linkedin.com/posts/the-cyber-security-hub_hackers-abuse...	T3

Generated 2026-05-29 19:06 UTC by TJS Security Command Center