INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-08 18:51 UTC

AI Brand Impersonation as Attack Infrastructure: Structured Campaigns Targeting Credentials, Cards, and Code Developers

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0427
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	ChatGPT (OpenAI), Claude (Anthropic), Microsoft Copilot, DeepSeek, Microsoft Defender, Microsoft Entra ID, Microsoft Defender for Office 365
Published	2026-06-08T16:00:00+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Multiple threat actor groups are systematically using the brands of major AI platforms, ChatGPT, Claude, Microsoft Copilot, and DeepSeek, as lures in large-scale phishing, malvertising, and SEO poisoning campaigns. Microsoft Threat Intelligence documented (June 2026) a single-day wave of 100,000 phishing emails, with infections reaching tens to hundreds of thousands of endpoints; attackers have demonstrated the ability to deploy malware within 24 hours of major AI news events. The business risk is credential theft, financial fraud, and malware installation at scale, affecting any organization whose employees use web search, email, or install AI-related software.

Technical Analysis

Tracked campaigns exploit public interest in AI platforms through three primary delivery vectors: phishing email (T1566, T1566.001, T1566.002), malvertising via drive-by compromise (T1189), and SEO poisoning (T1608.006). A Trend Micro-documented campaign (June 2026) uses Claude Code branding as a lure, distributing payloads via GitHub Releases to abuse trusted hosting infrastructure and bypass URL-based filtering (T1583.008). Attack chains employ redirect chain abuse (CWE-1021) to obscure final payload destinations, embedded malicious code in delivered files (CWE-506), and credential harvesting through spoofed AI platform login pages (CWE-345). Additional observed techniques include AiTM web session cookie theft (T1550.004), DLL side-loading (T1574.002), code signing subversion (T1553.002), ScreenConnect abuse for remote access (T1219), and cryptojacking (T1496). Malware deployment has been confirmed within 24 hours of

high-profile AI news events, indicating deliberate news-cycle exploitation. Microsoft Defender for Office 365 and Microsoft Entra ID are identified as primary detection and mitigation surfaces. No CVE is assigned; CWEs include CWE-345, CWE-506, and CWE-1021.

Action Checklist

1. Step 1: Containment. Block known malicious redirect chains and GitHub Releases URLs associated with AI-branded lures at the proxy and email gateway. In Microsoft Defender for Office 365, enable Safe Links and Safe Attachments policies for all users and verify they are active (not in audit-only or disabled modes). Per the Microsoft advisory, Defender for Office 365 is a primary mitigation surface; confirm policies are enforced, not disabled.
2. Step 2: Detection. Query Microsoft Entra ID sign-in logs for session cookie reuse from anomalous IPs or geographies (indicator of AiTM activity, T1550.004). In Defender for Endpoint, hunt for processes spawned from GitHub Releases download paths and DLL side-loading patterns (T1574.002). Review email flow logs for high-volume AI-branded subject lines delivered in short time windows. Monitor DNS and proxy logs for domains spoofing ChatGPT, Claude, Copilot, and DeepSeek. Use NIST SP 800-53 Rev. 5, AU-6 (Audit Record Review, Analysis, and Reporting) cadence to ensure these log sources are reviewed at defined frequency.
3. Step 3: Eradication. Remove any software installed via AI-branded lures from affected endpoints; treat as untrusted regardless of apparent source, including files from GitHub Releases. Rotate credentials and invalidate active sessions for any account that authenticated to a spoofed AI platform login page. Revoke and reissue session tokens in Microsoft Entra ID for affected user populations. Disable or remove any unauthorized remote access software (ScreenConnect instances) discovered during investigation.
4. Step 4: Recovery. Validate that Defender for Office 365 Safe Links policies are rewriting and inspecting all URLs, including those pointing to github.com/releases paths. Confirm Entra ID Conditional Access policies enforce MFA for all remote and externally-exposed applications (CIS 6.3, CIS 6.4). Monitor affected endpoints for 30 days post-remediation for cryptojacking indicators (T1496): sustained high CPU, unexpected outbound connections to mining pools. Verify audit logging is active and storage capacity is sufficient per NIST SP 800-53 Rev. 5, AU-4.
5. Step 5: Post-Incident. This campaign exposes three control gaps: (a) user susceptibility to AI-branded social engineering, address with targeted awareness training focused on AI platform impersonation; (b) over-reliance on URL reputation filtering alone, bypassed by GitHub Releases abuse, supplement with file behavior analysis and file magic byte verification; (c) insufficient MFA coverage allowing AiTM session theft to succeed, audit all accounts against CIS 6.3, CIS 6.4, CIS 6.5 and enforce phishing-resistant MFA (FIDO2) where possible.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to CISO and legal counsel if Entra ID sign-in logs confirm successful AiTM session token theft for any account with access to PII, PHI, or financial data — this triggers breach notification assessment under GDPR Article 33 (72-hour window), HIPAA Breach Notification Rule, and applicable US state privacy laws; also escalate if ScreenConnect or cryptojacking artifacts are confirmed on more than 5 endpoints, indicating the campaign has achieved persistent access beyond initial phishing, or if any compromised account held Global Administrator privileges in Entra ID.
Recovery Notes	Validate recovery by re-running the Microsoft ORCA analyzer and `Get-SafeLinksPolicy` / `Get-SafeAttachmentPolicy` exports to confirm Defender for Office 365 is in enforced mode with no AI-brand or GitHub domain exclusions, and that all affected Entra ID accounts show clean sign-in history with no anomalous IP or geography patterns for 72 hours post-token revocation. Monitor all remediated endpoints for 30 days specifically for XMRig cryptomining indicators (sustained CPU above 80%, outbound connections to TCP 3333/4444/14444) and for ScreenConnect re-installation attempts, as this campaign class has demonstrated re-infection within 24 hours of new AI news events. Document all control gaps identified — particularly MFA coverage exceptions and Safe Links audit-mode configurations — in a formal remediation tracking record with assigned owners and deadlines, fulfilling NIST 800-61r3 §4 post-incident activity requirements.
Forensic Artifacts	Entra ID Sign-in Logs (Azure Portal > Entra ID > Monitoring > Sign-in logs): Filter for successful authentications preceded by interrupted MFA challenges from one IP followed by session activity from a geographically or ASN-distinct IP within the same refresh token lifetime — the specific forensic fingerprint of AiTM reverse-proxy credential interception (T1550.004) used in this campaign. | Windows Sysmon Event ID 1 (Process Create) and Event ID 7 (Image Loaded) logs: Filter for executables launched from %USERPROFILE%\Downloads\ or %LOCALAPPDATA%\Temp\ with names containing AI-brand strings (ChatGPT, Claude, Copilot, DeepSeek) as parent processes, and child DLL loads from co-located non-standard paths — the execution chain produced by GitHub Releases-hosted AI-branded lure installers performing DLL side-loading (T1574.002). | Windows System Event Log Event ID 7045 (New Service Installed) and Application Event Log entries: Identifies ScreenConnect (ConnectWise Control) service registration on endpoints post-infection — this campaign specifically deploys ScreenConnect as a persistent RAT following initial lure execution, and service installation is logged here even when the installer is named to appear as an AI client. | Proxy / Web Gateway Access Logs: Full URL-path logs (not just domain) filtered for requests to github.com/releases/* paths originating from endpoints shortly after delivery of AI-branded phishing emails — the timestamp correlation between email delivery and GitHub Releases download request is a high-fidelity indicator of successful lure execution specific to this campaign's delivery chain. | Windows Registry Export — HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\Software\Microsoft\Windows\CurrentVersion\Run: Captures persistence keys written by malware payloads dropped via AI-branded lure installers; XMRig cryptominer and ScreenConnect both establish Run key persistence, and these keys will reference the same %APPDATA% or %PROGRAMDATA% paths where the AI-branded installer deposited its payload.

Per-Action IR Details

Step 1: Containment — Block known malicious redirect chains and GitHub Releases URLs associated with AI-branded lures at the proxy and email gateway. In Microsoft Defender for Office 365, enable Safe Links and Safe Attachments policies for all users and verify they are not in audit-only mode. Per the Microsoft advisory, Defender for Office 365 is a primary mitigation surface — confirm policies are enforced, not permissive.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: For teams without Defender for Office 365: use Pi-hole or pfBlockerNG to sink DNS resolution for AI-spoofing domains (chatgpt-login[.]net pattern variants, deepseek-download[.]com pattern variants). Block github.com/releases/* paths at the proxy layer using Squid ACLs if GitHub access is not business-critical. Export the Microsoft Threat Intelligence IOC feed manually from CISA Known Exploited / MS advisories and push to firewall block lists via script. Use PowerShell on the email gateway: `Get-TransportRule | Where-Object {$_.State -eq 'Enabled'}` to audit whether existing transport rules are actively blocking vs. auditing.

Evidence: Before implementing blocks, capture: (1) proxy/web gateway logs showing full redirect chain URLs — specifically multi-hop redirectors terminating at GitHub Releases paths or spoofed AI login domains; (2) email gateway quarantine queue contents including full message headers, sender IPs, and subject lines containing 'ChatGPT', 'Claude', 'Copilot', 'DeepSeek' keywords delivered in burst windows; (3) current Defender for Office 365 policy configuration export via `Get-SafeLinksPolicy` and `Get-SafeAttachmentPolicy` PowerShell cmdlets to document pre-remediation state; (4) DNS query logs from the past 14 days filtered for AI-brand typosquats to establish scope of user exposure before the block is applied.

Step 2: Detection — Query Microsoft Entra ID sign-in logs for session cookie reuse from anomalous IPs or geographies (indicator of AiTM activity, T1550.004). In Defender for Endpoint, hunt for processes spawned from GitHub Releases download paths and DLL side-loading patterns (T1574.002). Review email flow logs for high-volume AI-branded subject lines delivered in short time windows. Monitor DNS and proxy logs for domains spoofing ChatGPT, Claude, Copilot, and DeepSeek. Use NIST AU-6 (Audit Record Review, Analysis, and Reporting) cadence to ensure these log sources are reviewed at defined frequency.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM or Defender for Endpoint: (1) Deploy Sysmon with SwiftOnSecurity config and filter Event ID 1 (Process Create) for parent processes matching *\AppData\Local\Temp* or *\Downloads* paths associated with GitHub Releases installer drops; additionally watch Sysmon Event ID 7 (Image Loaded) for DLL loads from non-standard paths co-located with AI-branded installer names. (2) Use `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' -FilterXPath "*[System[EventID=1] and EventData[Data[@Name='Image'] and (contains(Data,'ChatGPT') or contains(Data,'Copilot') or contains(Data,'DeepSeek'))]]"` to scope initial compromise. (3) Pull Entra ID sign-in logs via Microsoft Graph API free tier and filter for `tokenIssuedAt` vs. `signInActivity` delta exceeding 30 minutes from different IP ranges — a strong AiTM session replay indicator. (4) Apply publicly available Sigma rules mapped to T1550.004 using Chainsaw against Windows Security EVTX exports.

Evidence: Before concluding detection scope: (1) Entra ID sign-in logs (Azure Portal > Entra ID > Sign-in logs) filtered for interrupted MFA flows followed by successful authentication from a different IP within the same session — the AiTM (T1550.004) fingerprint specific to this campaign's Evilginx/reverse-proxy infrastructure; (2) Defender for Endpoint device timeline entries or Sysmon Event ID 1 logs showing process creation chains from `%USERPROFILE%\Downloads\[AI-brand]-installer.exe` or `%LOCALAPPDATA%\Temp\` spawning rundll32.exe, regsvr32.exe, or mshta.exe — DLL side-loading indicators specific to T1574.002; (3) Email message trace logs from Defender for Office 365 or Exchange showing delivery timestamps clustered within narrow windows (the Microsoft advisory documents a 100,000-email single-day wave) with AI-brand subject line patterns; (4) DNS query logs (Windows DNS debug log or resolver cache via `ipconfig /displaydns`) for domains matching chatgpt*, claude*, copilot*, deepseek* TLDs outside openai.com, anthropic.com, microsoft.com, and deepseek.com.

Step 3: Eradication — Remove any software installed via AI-branded lures from affected endpoints; treat as untrusted regardless of apparent source, including files from GitHub Releases. Rotate credentials and invalidate active sessions for any account that authenticated to a spoofed AI platform login page (D3-CRO:

Credential Rotation). Revoke and reissue session tokens in Microsoft Entra ID for affected user populations. Disable or remove any unauthorized remote access software (ScreenConnect instances) discovered during investigation.

NIST Phase: Eradication

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

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AC-12 (Session Termination), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without enterprise MDM or Intune for remote wipe: (1) Use PowerShell `Get-WmiObject Win32_Product | Where-Object {$_.Name -match 'ScreenConnect|ConnectWise|ChatGPT|DeepSeek'}` across endpoints via PSRemoting to enumerate unauthorized installs; uninstall via `msiexec /x {GUID} /quiet`. (2) Revoke all Entra ID refresh tokens for affected users via `Revoke-MgUserSignInSession -UserId ` (Microsoft Graph PowerShell, free) — this invalidates all existing session cookies acquired via AiTM proxy, directly neutralizing T1550.004 persistence. (3) For credential rotation without a PAM tool: force password reset via `Set-MgUserPassword` and simultaneously disable legacy authentication protocols in Entra ID (block Basic Auth) to prevent credential reuse over unprotected channels. (4) Run ClamAV with the freshest signatures against `%APPDATA%`, `%LOCALAPPDATA%\Temp`, and `%PROGRAMDATA%` on affected hosts to identify dropped malware payloads from AI-branded installer chains.

Evidence: Before eradicating, preserve: (1) Full disk image or at minimum targeted forensic collection of `%APPDATA%`, `%LOCALAPPDATA%\Temp`, `%PROGRAMDATA%`, and `C:\Users\[user]\Downloads` directories on affected endpoints — AI-branded lure installers dropped cryptominers and RATs to these paths per campaign reporting; (2) Registry export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` for persistence mechanisms established by the malware payload; (3) ScreenConnect installation artifacts: `%ProgramFiles(x86)\ScreenConnect*` directory contents, Windows Event Log Application entries showing ScreenConnect service registration (Event ID 7045 in System log), and network connection logs showing outbound connections to attacker-controlled ScreenConnect relay infrastructure; (4) Memory acquisition (via WinPmem, free) from any endpoint with active suspicious processes before termination — cryptojacking payloads for T1496 may be fileless or inject into legitimate processes.

Step 4: Recovery — Validate that Defender for Office 365 Safe Links policies are rewriting and inspecting all URLs, including those pointing to github.com/releases paths. Confirm Entra ID Conditional Access policies enforce MFA for all remote and externally-exposed applications (CIS 6.3, CIS 6.4). Monitor affected endpoints for 30 days post-remediation for cryptojacking indicators (T1496): sustained high CPU, unexpected outbound connections to mining pools. Verify audit logging is active and storage capacity is sufficient per NIST AU-4.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-4 (Audit Storage Capacity), NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without SIEM for 30-day post-recovery monitoring: (1) Deploy a scheduled PowerShell task on recovered endpoints that samples CPU utilization every 15 minutes via `Get-Counter '\Processor(_Total)\% Processor Time'` and logs sustained readings above 80% (cryptojacking T1496 baseline indicator) to a central share. (2) Use Wireshark or NetworkMiner in capture-only mode on a network tap or SPAN port to collect and flag outbound connections to known mining pool ports (3333, 4444, 14444, 45700) and domains (pool.minexmr.com, xmrpool.eu, etc.) — XMRig is the commonly deployed payload in this campaign class. (3) Validate Safe Links enforcement (not audit mode) using the Microsoft ORCA analyzer tool (free, PowerShell-based) which checks Defender for Office 365 policy posture and flags permissive configurations. (4) Set a Windows Task Scheduler job to run `auditpol /get /category:*` weekly and alert if audit subcategories are disabled — ensuring log collection for AU-4 compliance is not silently broken post-incident.

Evidence: Before declaring recovery complete, confirm: (1) Entra ID Conditional Access policy report showing zero accounts with MFA exceptions or exclusions for externally-exposed apps — gaps here are the specific control failure exploited by this campaign's AiTM infrastructure; (2) Defender for Office 365 configuration report (`Get-SafeLinksPolicy

| Select Name,IsEnabled,DoNotRewriteUrls,ScanUrls`) confirming `DoNotRewriteUrls` list does not contain github.com or any AI-brand domains that could re-permit the lure delivery vector; (3) Network flow records or endpoint telemetry from recovered hosts showing absence of outbound connections to XMRig pool infrastructure or ScreenConnect relay domains for a 72-hour clean period before broader recovery declaration; (4) Audit log storage utilization report confirming log retention capacity is not exhausted — this campaign's scale (100,000 emails in a single day) can spike log volume and silently fill AU-4 storage allocations, causing log loss during the investigation window.

Step 5: Post-Incident — This campaign exposes three control gaps: (a) user susceptibility to AI-branded social engineering — address with targeted awareness training focused on AI platform impersonation; (b) over-reliance on URL reputation filtering alone, bypassed by GitHub Releases abuse — supplement with file behavior analysis (D3-SFA: System File Analysis, D3-FMBV: File Magic Byte Verification); (c) insufficient MFA coverage allowing AiTM session theft to succeed — audit all accounts against CIS 6.3, CIS 6.4, CIS 6.5 and enforce phishing-resistant MFA (FIDO2) where possible (D3-MFA).

NIST Phase: Post Incident

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AC-7 (Unsuccessful Logon Attempts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: For teams without security awareness platforms or MFA enforcement tooling: (1) Conduct a tabletop exercise specifically using AI-brand impersonation scenarios — show employees side-by-side pixel-perfect spoofs of ChatGPT and DeepSeek login pages versus legitimate sites; document the exercise per NIST 800-61r3 §4 lessons-learned requirements. (2) Deploy a YARA rule scanning `%USERPROFILE%\Downloads` and `%TEMP%` at login via Group Policy logon script to flag files whose magic bytes (file header) do not match their declared extension — directly addressing the GitHub Releases abuse vector where malicious executables are named to appear as AI client installers. Free YARA Windows binary from VirusTotal GitHub is sufficient. (3) For FIDO2 enforcement without Entra ID P2 licensing: enable Windows Hello for Business (built into Windows 10/11, no additional license) as a phishing-resistant MFA alternative for domain-joined endpoints — it is not proxiable by AiTM reverse-proxy infrastructure, directly closing the T1550.004 session theft gap. (4) Submit campaign IOCs (spoofed domains, GitHub Releases URLs, ScreenConnect relay IPs) to CISA's automated indicator sharing (AIS) program and to the Microsoft Defender Threat Intelligence community — free, and directly informs detection for peer organizations facing the same campaign.

Evidence: For the lessons-learned record, preserve and document: (1) Timeline reconstruction from Entra ID sign-in logs showing the delta between AI news event publication (the 24-hour deployment window cited in the advisory) and first observed phishing delivery in your environment — this validates whether your detection cadence is sufficient to catch news-reactive campaigns; (2) Complete list of affected user accounts, scope of credential exposure (password only vs. session token theft), and whether any accounts lacked MFA — this documents the specific control gap (CIS 6.3/6.4/6.5 deficiency) for remediation tracking; (3) Any ScreenConnect or RAT C2 communication logs preserved from network captures, to be used as hunt signatures for future campaigns using the same remote access infrastructure; (4) Final count of endpoints where AI-branded lure installers executed vs. were blocked — this ratio quantifies the effectiveness of the pre-incident Defender for Office 365 policy posture and justifies the policy enforcement changes made in Steps 1 and 4.

Detection Guidance

Primary detection surfaces are Microsoft Defender for Office 365, Microsoft Entra ID sign-in logs, endpoint process telemetry, and proxy/DNS logs. Key behavioral indicators: (1) Email: high volumes of messages referencing ChatGPT, Claude, Copilot, or DeepSeek brand names with embedded links or attachments; URLs that traverse multiple redirects before reaching a final destination (redirect chain abuse, CWE-1021). (2) AiTM credential theft: Entra ID sign-in logs showing token reuse from IPs inconsistent with the user's normal

geography or device; Conditional Access failures followed by successful authentications from new devices. (3) GitHub Releases payload delivery: process creation events where the parent is a browser or download manager and the child executable originates from a path containing github.com/releases; DLL load events (T1574.002) from non-standard directories adjacent to newly downloaded binaries. (4) ScreenConnect abuse: presence of ScreenConnect or ConnectWise binaries not in authorized software inventory (CIS 2.1, CIS 2.3); outbound connections to ScreenConnect relay infrastructure from endpoints without an authorized remote support use case. (5) Cryptojacking: sustained CPU utilization above baseline on endpoints post-infection; outbound connections to known mining pool ports (3333, 4444, 14444) detected at the firewall or proxy layer. (6) SEO poisoning: DNS or proxy logs showing users navigating to domains closely resembling official AI platform domains (typosquats, homoglyph substitutions). Align log collection to NIST SP 800-53 Rev. 5, AU-2 (Event Logging) and AU-12 (Audit Record Generation) to ensure these event types are captured. Per Local Account Monitoring recommendations, review local account activity on endpoints where infections are confirmed.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.trendmicro.com/en_us/research/26/d/weaponizing-trust-claude-code-lures-and-github-release-payloads.html`	Trend Micro research article documenting Claude Code lure campaign with GitHub Releases payload delivery — check report for specific IOCs published by Trend Micro	HIGH
URL	`https://www.microsoft.com/en-us/security/blog/2026/06/08/ai-brands-as-bait-how-threat-actors-are-using-the-ai-hype-in-social-engineering/`	Microsoft Threat Intelligence advisory documenting AI brand impersonation campaigns — primary IOC source; consult for specific domains, hashes, and IP indicators	HIGH
URL	`https://www.microsoft.com/en-us/security/blog/2026/05/26/poisoned-search-results-gpu-mining-cryptojacking-campaign-abusing-screenconnect-microsoft-net-utilities/`	Microsoft advisory on SEO poisoning, cryptojacking, and ScreenConnect abuse campaign — additional IOC source	HIGH

Framework Mappings

MITRE-ATTACK

- **T1598.003** — Spearphishing Link
- **T1598** — Phishing for Information
- **T1583.008** — Malvertising
- **T1496** — Resource Hijacking
- **T1566** — Phishing
- **T1566.002** — Spearphishing Link
- **T1189** — Drive-by Compromise

- **T1566.001** — Spearphishing Attachment
- **T1056.003** — Web Portal Capture
- **T1553.002** — Code Signing
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1608.006** — SEO Poisoning
- **T1588.006** — Vulnerabilities
- **T1574.002** — DLL Side-Loading
- **T1550.004** — Web Session Cookie
- **T1036** — Masquerading
- **T1204.002** — Malicious File
- **T1195** — Supply Chain Compromise
- **T1219** — Remote Access Tools

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

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

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1598.003	Spearphishing Link	Reconnaissance
T1598	Phishing for Information	Reconnaissance
T1583.008	Malvertising	Resource-Development
T1496	Resource Hijacking	Impact
T1566	Phishing	Initial-Access
T1566.002	Spearphishing Link	Initial-Access
T1189	Drive-by Compromise	Initial-Access
T1566.001	Spearphishing Attachment	Initial-Access
T1056.003	Web Portal Capture	Collection
T1553.002	Code Signing	Defense-Evasion
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1608.006	SEO Poisoning	Resource-Development
T1588.006	Vulnerabilities	Resource-Development
T1574.002	DLL Side-Loading	Persistence
T1550.004	Web Session Cookie	Defense-Evasion
T1036	Masquerading	Defense-Evasion
T1204.002	Malicious File	Execution
T1195	Supply Chain Compromise	Initial-Access
T1219	Remote Access Tools	Command-And-Control

Sources

Source	URL	Tier
Microsoft Security Blog	https://www.microsoft.com/en-us/security/blog/2026/06/08/ai-brands-...	T1
	https://www.microsoft.com/en-us/security/blog/2026/06/08/ai-brands-...	T1
	https://www.trendmicro.com/en_us/research/26/d/weaponizing-trust-cl...	T3
	https://www.microsoft.com/en-us/security/blog/2026/05/26/poisoned-s...	T1
Microsoft Purview data security and compliance protections for ...	https://learn.microsoft.com/en-us/purview/ai-microsoft-purview	T1

Generated 2026-06-08 18:51 UTC by TJS Security Command Center