INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-11 05:53 UTC

Silver Fox Deploys ValleyRAT via Fake OpenAI Model on Hugging Face, 244K Downloads in 18 Hours

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0301
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Hugging Face platform (Windows targets), Chromium/Gecko-based browsers, Discord, cryptocurrency wallet extensions, FileZilla
Published	2026-05-11T03:05:00
Discovery Source	Rss

Executive Summary

A typosquatted repository on the Hugging Face AI platform impersonated an OpenAI tool and delivered credential-stealing malware to approximately 244,000 systems within 18 hours before removal. The payload, attributed with medium confidence to Silver Fox, a Chinese threat actor, targets browser-stored passwords, cryptocurrency wallets, Discord tokens, and FTP credentials on Windows systems. Organizations with AI/ML developers who download models from Hugging Face face direct credential compromise and potential downstream supply chain exposure.

Technical Analysis

The malicious repository Open-OSS/privacy-filter masqueraded as OpenAI's legitimate Privacy Filter model on Hugging Face (T1036.005, Masquerading). A Rust-based loader executed on Windows, downloaded and ran a second-stage payload with SSL verification disabled (CWE-295) and no integrity checking (CWE-494). The payload is ValleyRAT (also tracked as Winos 4.0), a full-featured RAT with credential harvesting, screen capture (T1113), scheduled task persistence (T1053.005), UAC bypass (T1548.002), AMSI/ETW bypass (T1562.001), and C2 over HTTP/S (T1071.001). Dead-drop resolver infrastructure used JSON Keeper (T1583.006). Targeted data: Chromium and Gecko browser credential stores (T1555.003), Discord tokens (T1539), cryptocurrency wallet browser extensions (T1176), and FileZilla credentials (T1005). Six additional repositories using the same loader pattern were identified, confirming an active supply chain campaign (T1195.001). Attribution to Silver Fox is based on infrastructure overlap identified by HiddenLayer Research; independent corroboration from a

second threat intelligence source was not located in available reporting; treat attribution as medium confidence. No CVE has been assigned. Relevant CWEs: CWE-494, CWE-295, CWE-426.

Action Checklist

1. Containment: Immediately audit developer workstations and CI/CD pipeline environments for evidence of Open-OSS/privacy-filter installation. Isolate any system that pulled the repository. Block all network communication to C2 infrastructure associated with ValleyRAT/Winos 4.0 at the perimeter; IOCs from HiddenLayer Research (https://www.hiddenlayer.com/research/malware-found-in-trending-hugging-face-repository-open-oss-privacy-filter) should be pushed to EDR and firewall deny lists immediately.
2. Detection: Query endpoint logs for execution of Rust binaries downloaded from Hugging Face, scheduled tasks created in the 18-hour window around the campaign (confirm exact window with HiddenLayer's timeline), and PowerShell or cmd.exe activity spawned from unusual parent processes. Search browser credential stores for unexpected access events. Review EDR telemetry for AMSI or ETW tampering indicators and UAC bypass events (T1548.002, T1562.001). Check for JSON Keeper dead-drop resolver connections in proxy/DNS logs.
3. Eradication: Remove any instance of Open-OSS/privacy-filter from all environments, including cached model directories (common path: ~/.cache/huggingface/hub). Delete any scheduled tasks created by the malware. Remove persistence mechanisms identified by EDR tooling. Rotate all credentials stored in affected browsers; treat all browser-stored passwords, Discord tokens, and cryptocurrency wallet keys on affected systems as compromised.
4. Recovery: Rebuild affected systems from known-good images where feasible; do not trust credential rotation alone on a confirmed-infected host. Re-validate Hugging Face model sources against official OpenAI and vendor accounts before re-introducing any previously downloaded models. Confirm EDR and AMSI are fully operational post-remediation; the malware disables defensive tooling. Monitor for anomalous authentication activity on accounts whose credentials were stored in affected browsers for at least 30 days.
5. Post-Incident: Implement a policy requiring developer teams to verify Hugging Face repository authenticity (publisher account, download history, community flags) before any model download. Evaluate enforcing allowlist-based model sourcing for CI/CD pipelines. Address the control gap in software supply chain integrity: no process verified the downloaded code had not been tampered with (CWE-494). Consider integrating model hash verification and scanning into ML pipeline workflows. Map control gaps to NIST CSF ID.SC-3 and NIST SP 800-161 supply chain risk practices.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if any affected system had access to production credentials, customer PII, source code repositories, or cryptocurrency wallets with organizational funds, as Silver Fox credential exfiltration within the 18-hour exposure window may trigger breach notification obligations under applicable state privacy laws, GDPR, or financial regulations; also escalate if any CI/CD pipeline used the compromised environment to build and deploy production artifacts, as the supply chain compromise scope extends beyond the developer workstation.

Recovery Notes	Do not return any system to production on credential rotation alone — ValleyRAT's AMSI and ETW tampering means standard security tooling may have been blind during the infection window, leaving secondary persistence mechanisms undetected; full rebuild from known-good images is required for confirmed-infected hosts. Re-validate every Hugging Face model currently in use across all environments against the official publisher account before re-enabling CI/CD pipelines, and pin all future downloads to a verified commit SHA. Maintain enhanced authentication monitoring on all accounts whose credentials were browser-stored on affected systems for a minimum of 30 days, with specific attention to GitHub, cloud console, Discord, and any cryptocurrency exchange accounts targeted by Silver Fox.
Forensic Artifacts	Hugging Face hub cache directory at %USERPROFILE%\.cache\huggingface\hub\models--Open-OSS\ (Windows) or ~/.cache/huggingface/hub/models--Open-OSS/ (Linux CI/CD) — contains the downloaded Rust binaries and model files that constitute the primary payload delivery artifacts specific to this typosquatting campaign | Windows Scheduled Tasks XML files in C:\Windows\System32\Tasks\ created during the 18-hour campaign window — ValleyRAT establishes scheduled task persistence as its primary survival mechanism, and these XML files contain the exact command line, trigger, and run-as-user context needed to confirm compromise scope | Browser credential SQLite databases (Chrome/Edge: %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data; Firefox: %APPDATA%\Mozilla\Firefox\Profiles*.default\logins.json) and Discord LevelDB token store (%APPDATA%\discord\Local Storage\leveldb\) — Silver Fox ValleyRAT specifically targets these stores, and access timestamps on these files can confirm whether credential harvesting occurred | Microsoft-Windows-AMSI/Operational event log and ETW trace logs — ValleyRAT disables AMSI and tampers with ETW (T1562.001) as an early post-exploitation step; gaps or disable events in these logs corroborate active infection and bound the window during which other security tooling was blind | DNS resolver cache (ipconfig /displaydns) and proxy logs filtered for paste-site domains (pastebin.com, gist.github.com, paste.ee) — ValleyRAT's JSON Keeper component uses dead-drop resolver technique (T1102.001) to retrieve C2 addresses from public paste sites, making these DNS queries a unique network-layer indicator specific to this malware family's C2 architecture

Per-Action IR Details

Containment — Immediately audit developer workstations and CI/CD pipeline environments for evidence of Open-OSS/privacy-filter installation. Isolate any system that pulled the repository. Block all network communication to C2 infrastructure associated with ValleyRAT/Winos 4.0 at the perimeter; IOCs from HiddenLayer Research (https://www.hiddenlayer.com/research/malware-found-in-trending-hugging-face-repository-open-oss-privacy-filter) should be pushed to EDR and firewall deny lists immediately.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 13.4 (Perform Traffic Filtering Between Network Segments)

Compensating: Without EDR, run the following PowerShell on each developer workstation to detect the Hugging Face cache path and Rust binary presence: `Get-ChildItem -Path "$env:USERPROFILE\.cache\huggingface\hub" -Recurse -ErrorAction SilentlyContinue | Select FullName, LastWriteTime`. For network blocking, push ValleyRAT C2 IOC IP ranges and domains to Windows Firewall via: `netsh advfirewall firewall add rule name="Block ValleyRAT C2" dir=out action=block remoteip=`. For CI/CD hosts (Linux), use `iptables -A OUTPUT -d -j DROP`. Use Sysmon Event ID 3 (Network Connection) filtered on known-bad C2 domains to catch outbound beaconing before firewall rules propagate.

Evidence: BEFORE isolating the system, capture: (1) Full disk image or at minimum a memory acquisition (WinPmem or Magnet RAM Capture) to preserve in-memory ValleyRAT/Winos 4.0 artifacts before shutdown destroys them. (2) Export Windows Scheduled Tasks via `schtasks /query /fo CSV /v > tasks_before_containment.csv` — ValleyRAT establishes persistence via scheduled tasks created during the 18-hour campaign window. (3) Export the Hugging Face hub cache directory listing at `%USERPROFILE%\.cache\huggingface\hub` and any pip/conda environment logs showing the Open-OSS/privacy-filter package install timestamp. (4) Pull active network connections via `netstat -anob > netstat_snapshot.txt` to capture live C2 connections before isolation severs them. (5) Export browser credential store metadata (do NOT decrypt on the compromised host) — SQLite DBs at `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data` and equivalent paths for Edge/Firefox to document what credentials were accessible.

Detection — Query endpoint logs for execution of Rust binaries downloaded from Hugging Face, scheduled tasks created in the 18-hour window around the campaign (confirm exact window with HiddenLayer's timeline), and PowerShell or cmd.exe activity spawned from unusual parent processes. Search browser credential stores for unexpected access events. Review EDR telemetry for AMSI or ETW tampering indicators and UAC bypass events (T1548.002, T1562.001). Check for JSON Keeper dead-drop resolver connections in proxy/DNS logs.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 10.1 (Deploy and Maintain Anti-Malware Software)

Compensating: Without a SIEM, use the following targeted queries: (1) Sysmon Event ID 1 (Process Create) — filter for processes where `ParentImage` contains `python.exe`, `pip.exe`, or `conda.exe` and `Image` ends in `.exe` within the `huggingface\hub` cache path, indicating a Rust binary spawned from the model-loading environment. (2) Windows Security Event Log Event ID 4698 (Scheduled Task Created) — filter for tasks created during the campaign window: `Get-WinEvent -FilterHashtable @{LogName='Security';Id=4698;StartTime='';EndTime=''}`. (3) For AMSI tampering (T1562.001), query Sysmon Event ID 13 (Registry Value Set) for writes to `HKLM\SOFTWARE\Microsoft\AMSI\Providers` or `HKCU\SOFTWARE\Microsoft\Windows Script\Settings\AmsiEnable`. (4) For JSON Keeper dead-drop resolver activity, run Wireshark or `tcpdump` filtering on DNS queries to Pastebin, GitHub Gist, or similar paste-site domains: `dns.qry.name contains "pastebin" or dns.qry.name contains "gist.github"`. (5) Deploy the Sigma rule for UAC bypass via fodhelper.exe or ComputerDefaults.exe (T1548.002) against Windows Security Event Log Event ID 4688 (Process Creation) with `ParentCommandLine` containing those binaries.

Evidence: Capture BEFORE analysis consumes or alters artifacts: (1) Windows Security Event Log Event ID 4688 (Process Creation with command line auditing enabled) — filter parent processes `pip.exe`, `python.exe`, or `huggingface-cli.exe` spawning unexpected child processes, which would reveal the Rust dropper execution chain. (2) PowerShell Script Block Logging (Event ID 4104) and Module Logging (Event ID 4103) from `HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell` — ValleyRAT uses PowerShell for post-exploitation; these logs capture obfuscated commands even when AMSI is subsequently disabled. (3) ETW provider logs — export `Microsoft-Windows-AMSI/Operational` event log before eradication to document exactly when and how AMSI was disabled by the malware. (4) DNS resolver cache (`ipconfig /displaydns > dns_cache.txt`) to capture JSON Keeper dead-drop resolver domains before network isolation clears the cache. (5) Browser SQLite access timestamps — use `sqlite3 "Login Data" "SELECT origin_url, username_value, date_last_used FROM logins ORDER BY date_last_used DESC LIMIT 50"` on a forensic copy to identify whether credential stores were accessed by a process other than the browser itself.

Eradication — Remove any instance of Open-OSS/privacy-filter from all environments, including cached model directories (common path: ~/.cache/huggingface/hub). Delete any scheduled tasks created by the malware. Remove persistence mechanisms identified by EDR tooling. Rotate all credentials stored in affected browsers — treat all browser-stored passwords, Discord tokens, and cryptocurrency wallet keys on affected systems as compromised.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IA-5 (Authenticator Management), CIS 2.3 (Address Unauthorized Software), CIS 5.2 (Use Unique Passwords)

Compensating: Without EDR-guided artifact removal: (1) Uninstall via pip: `pip uninstall open-oss privacy-filter -y` followed by `pip cache purge` to remove cached wheel files. (2) Manually delete the Hugging Face hub cache: `Remove-Item -Recurse -Force "$env:USERPROFILE\.cache\huggingface\hub\models--Open-OSS*"` on Windows or `rm -rf ~/.cache/huggingface/hub/models--Open-OSS*` on Linux CI/CD. (3) Delete malware-created scheduled tasks identified in detection phase: `schtasks /delete /tn "" /f`. (4) Scan residual files using ClamAV with the latest signatures (`clamscan -r --infected --remove %USERPROFILE%\.cache\huggingface`) and a YARA rule targeting ValleyRAT/Winos 4.0 strings — check public YARA rules from MalwareBazaar or the HiddenLayer report. (5) For credential rotation, use `browserpass` or manual export to enumerate all credentials stored in Chrome/Edge/Firefox before rotating — prioritize corporate SSO, GitHub/GitLab, AWS/Azure/GCP console, and any cryptocurrency exchange accounts, as Silver Fox specifically targets these.

Evidence: Capture BEFORE eradication destroys artifacts: (1) Full forensic copy of scheduled task XML definitions from `C:\Windows\System32\Tasks\` — preserves the exact persistence mechanism including trigger conditions, run-as user context, and command line used by ValleyRAT. (2) Registry export of Run/RunOnce keys: `reg export HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run run_keys_before_eradication.reg` and the equivalent HKLM path — ValleyRAT/Winos 4.0 may establish registry-based persistence in addition to scheduled tasks. (3) Hash (SHA-256) all files in `%USERPROFILE%\.cache\huggingface\hub\models--Open-OSS*` before deletion: `Get-FileHash -Algorithm SHA256 -Path (Get-ChildItem -Recurse "").FullName` — these hashes are needed for post-incident IOC sharing and to confirm eradication. (4) Export the full list of installed pip packages from affected environments: `pip freeze > pip_env_snapshot.txt` to identify any secondary malicious dependencies the Rust dropper may have installed. (5) Copy Discord `%APPDATA%\discord\Local Storage\leveldb\` directory — ValleyRAT harvests Discord tokens from LevelDB; this directory documents what token material was accessible and to which accounts.

Recovery — Rebuild affected systems from known-good images where feasible; do not trust credential rotation alone on a confirmed-infected host. Re-validate Hugging Face model sources against official OpenAI and vendor accounts before re-introducing any previously downloaded models. Confirm EDR and AMSI are fully operational post-remediation; the malware disables defensive tooling. Monitor for anomalous authentication activity on accounts whose credentials were stored in affected browsers for at least 30 days.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Without enterprise imaging infrastructure: (1) Use Windows Reset (`Settings > Recovery > Reset this PC > Remove everything`) as a minimum viable rebuild for developer workstations where full reimaging is not feasible — document the decision and residual risk. (2) Verify AMSI is re-enabled post-rebuild by running `[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils')` in PowerShell — if it returns a type without error and AMSI events reappear in `Microsoft-Windows-AMSI/Operational`, the provider is functional. (3) Re-validate Hugging Face model sources by cross-referencing the repository publisher account against the official OpenAI organization page at `huggingface.co/openai` — typosquatted repos will show a different account with a recent creation date and anomalously high short-term download counts. (4) For 30-day anomalous auth monitoring without a SIEM, configure Microsoft 365 or Google Workspace audit log email alerts for impossible-travel logins and new OAuth application grants, and set calendar reminders to manually review GitHub audit logs weekly for the affected developer accounts.

Evidence: Capture BEFORE returning systems to production: (1) Post-rebuild AMSI operational verification log — export `Microsoft-Windows-AMSI/Operational` after a controlled test (attempt to run EICAR string via PowerShell) to confirm AMSI is generating scan result events, proving the malware's defensive disabling was reversed. (2) Baseline Sysmon event log immediately after rebuild and EDR re-enrollment — this establishes a clean-state reference for the

30-day anomalous authentication monitoring period. (3) Screenshot or export of the rebuilt system's scheduled tasks list (`schtasks /query /fo LIST /v > tasks_post_rebuild.txt`) to confirm no ValleyRAT persistence tasks survived the rebuild process. (4) Authentication logs from GitHub, Hugging Face, AWS/Azure/GCP, and Discord for the 30-day monitoring window — request log exports from each platform's admin console at T+0 (rebuild date) so the baseline is established before any post-compromise activity occurs.

Post-Incident — Implement a policy requiring developer teams to verify Hugging Face repository authenticity (publisher account, download history, community flags) before any model download. Evaluate enforcing allowlist-based model sourcing for CI/CD pipelines. Address the control gap in software supply chain integrity: no process verified the downloaded code had not been tampered with (CWE-494). Consider integrating model hash verification and scanning into ML pipeline workflows. Map control gaps to NIST CSF ID.SC-3 and NIST SP 800-161 supply chain risk practices.

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-7 (Software, Firmware, and Information Integrity), NIST SA-12 (Supply Chain Protection), NIST RA-3 (Risk Assessment), 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)

Compensating: Without a commercial supply chain security tool: (1) Implement `huggingface_hub` Python library's built-in hash verification — use `snapshot_download(repo_id, revision='')` pinned to a specific commit SHA rather than floating `main` to prevent silent swaps. (2) Build a lightweight CI/CD gate using a pre-download shell script that queries the Hugging Face API (`curl https://huggingface.co/api/models/`) and fails the pipeline if `createdAt` is within the past 30 days, `downloads` spiked more than 10,000% in 24 hours, or the author account has fewer than 3 other repositories. (3) Add ClamAV and a YARA scan step (`yara -r valleyrat_rules.yar ~/.cache/huggingface/hub/`) to CI/CD pipelines using published ValleyRAT/Winos 4.0 YARA rules from MalwareBazaar as a compensating integrity check. (4) For model allowlisting without enterprise tooling, maintain a plain-text `approved_models.txt` in the repo and add a pre-commit hook that fails if any `huggingface_hub` download call references a model not in the approved list — reviewable via standard pull request process.

Evidence: Capture for lessons-learned and policy documentation: (1) Full timeline reconstruction of which developer accounts authenticated to Hugging Face and downloaded the Open-OSS/privacy-filter repository — pull from Hugging Face account access logs and correlate with CI/CD pipeline run logs to determine the blast radius across build environments. (2) Gap analysis documentation: export the current CI/CD pipeline configuration files (GitHub Actions YAML, Jenkinsfile, etc.) to formally document the absence of model hash verification, YARA scanning, or publisher allowlisting controls — this becomes the evidence base for the CWE-494 remediation task. (3) Post-incident IOC report compiled from all forensic artifacts collected during detection/eradication phases — including SHA-256 hashes of ValleyRAT Rust binaries, scheduled task names, C2 domains/IPs, and JSON Keeper paste-site URLs — formatted for sharing with Hugging Face security team and optionally submitted to CISA via their reporting portal.

Detection Guidance

Primary detection surface is endpoint and EDR telemetry on Windows developer workstations and build systems. Key indicators: (1) Rust binary execution following a Hugging Face model download event; (2) scheduled task creation (Event ID 4698) in the campaign window from unusual parent processes; (3) PowerShell (T1059.001) or cmd.exe (T1059.003) spawned from model-loading processes; (4) AMSI provider tamper events or ETW session stops (T1562.001); (5) UAC bypass attempts (T1548.002, look for process elevation without user prompt). Network indicators: DNS or HTTP requests to JSON Keeper infrastructure (dead-drop resolver), outbound connections to ValleyRAT C2 endpoints. For confirmed IOC values (hashes, domains, IPs), reference HiddenLayer Research's published report directly. IOCs extracted from secondary reporting carry higher transcription risk. Browser credential store access from non-browser processes is a

behavioral indicator for T1555.003 and T1539. Cryptocurrency wallet extension data access outside browser context is a supplemental signal. Apply YARA rules for ValleyRAT/Winos 4.0 if available from your threat intelligence platform.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://huggingface.co/Open-OSS/privacy-filter`	Typosquatted Hugging Face repository delivering ValleyRAT payload — repository disabled but URL retained for log matching	HIGH
DOMAIN	`json.extendsclass.com`	JSON Keeper dead-drop resolver used for ValleyRAT C2 resolution (T1583.006) — verify against HiddenLayer report before blocking as this is a shared service	MEDIUM
HASH	`[see HiddenLayer Research report for verified hash values]`	Rust-based loader and ValleyRAT payload hashes — not reproduced here to avoid transcription error; retrieve directly from primary source	HIGH

Framework Mappings

MITRE-ATTACK

- **T1036.005** — Match Legitimate Resource Name or Location
- **T1005** — Data from Local System
- **T1059.003** — Windows Command Shell
- **T1562.001** — Disable or Modify Tools
- **T1053.005** — Scheduled Task
- **T1071.001** — Web Protocols
- **T1027** — Obfuscated Files or Information
- **T1204.002** — Malicious File
- **T1113** — Screen Capture
- **T1548.002** — Bypass User Account Control
- **T1176** — Software Extensions
- **T1555.003** — Credentials from Web Browsers
- **T1059.001** — PowerShell
- **T1539** — Steal Web Session Cookie
- **T1583.006** — Web Services
- **T1566** — Phishing
- **T1195.001** — Compromise Software Dependencies and Development Tools

- **T1497** — Virtualization/Sandbox Evasion
- **T1041** — Exfiltration Over C2 Channel

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **CM-3** — Configuration Change Control
- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates
- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **3.10** — Encrypt Sensitive Data in Transit
- **6.3** — Require MFA for Externally-Exposed Applications
- **15.1** — Establish and Maintain an Inventory of Service Providers

HIPAA-SECURITY

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

SOC2-TSC

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

NIST-CSF-2

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

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1005	Data from Local System	Collection
T1059.003	Windows Command Shell	Execution
T1562.001	Disable or Modify Tools	Defense-Evasion
T1053.005	Scheduled Task	Execution
T1071.001	Web Protocols	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1204.002	Malicious File	Execution
T1113	Screen Capture	Collection
T1548.002	Bypass User Account Control	Privilege-Escalation
T1176	Software Extensions	Persistence
T1555.003	Credentials from Web Browsers	Credential-Access
T1059.001	PowerShell	Execution
T1539	Steal Web Session Cookie	Credential-Access
T1583.006	Web Services	Resource-Development
T1566	Phishing	Initial-Access
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access
T1497	Virtualization/Sandbox Evasion	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/fake-openai-privacy-filter-repo-h...	T3

Source	URL	Tier
Malware Found in Trending Hugging Face Repository "Open-OSS ...	https://www.hiddenlayer.com/research/malware-found-in-trending-hugg...	T3
Fake OpenAI repository on Hugging Face pushes infostealer malware	https://www.bleepingcomputer.com/news/security/fake-openai-reposito...	T3
WARNING: Open-OSS/privacy-filter MALWARE : r/LocalLLaMA	https://www.reddit.com/r/LocalLLaMA/comments/1t6febk/warning_openos.. .	T3
Fake OpenAI repository on Hugging Face pushes infostealer malware	https://x.com/cybernewslive/status/2053364711144477020	T3

Generated 2026-05-11 05:53 UTC by TJS Security Command Center