INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-07 13:54 UTC

Beagle Backdoor Campaign Uses Fake Claude AI Site with DLL Sideloading and PlugX-Linked Infrastructure

THREAT CAMPAIGN | HIGH | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0286
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows systems; users targeted via typosquatted Anthropic Claude AI site; G Data NOVupdate.exe abused for DLL sideloading; Alibaba Cloud infrastructure used for C2; CrowdStrike, SentinelOne, and Trellix brands impersonated in delivery lures
Published	2026-05-07T06:02:35
Discovery Source	Rss

Executive Summary

A threat actor is running an active campaign that impersonates Anthropic's Claude AI, CrowdStrike, SentinelOne, and Trellix to trick Windows users into installing a new backdoor called Beagle. The malware uses a legitimate G Data security binary to load malicious code, evading many traditional defenses, and connects to attacker-controlled infrastructure on Alibaba Cloud for remote access. Organizations whose employees download security or AI tools from unverified sources are directly exposed; a successful infection gives attackers persistent, remote control of the affected system.

Technical Analysis

Beagle is a previously undocumented Windows backdoor delivered through a multi-stage infection chain. Initial access occurs via typosquatted sites impersonating Anthropic Claude AI, CrowdStrike, SentinelOne, and Trellix, at least four delivery variants observed since February 2026. The MSI installer drops and executes DonutLoader, which performs in-memory process injection (T1055) to load a malicious DLL (avk.dll) sideloaded through NOVupdate.exe, a legitimate signed binary from G Data security software (T1574.002, CWE-426). The downloader retrieves code without integrity verification (CWE-494), and the final payload constitutes embedded malicious code (CWE-506). Beagle provides full remote access: file upload/download (T1105), Windows command shell execution (T1059.003), and C2 communication over both TCP/443 with AES encryption (T1573.001, T1071.001) and UDP/8080 (T1095). Persistence is established via registry run keys or startup

folder (T1547.001). C2 infrastructure is hosted on Alibaba Cloud. Operational similarities to historical PlugX tooling have been noted by researchers; definitive actor attribution has not been established. No CVE assigned. Relevant CWEs: CWE-426, CWE-494, CWE-506. Sources: BleepingComputer, Security Affairs (T3).

Action Checklist

1. Containment, Block execution of NOVupdate.exe across the environment via application control policy (e.g., AppLocker, Windows Defender Application Control). NOVupdate.exe is a high-confidence IOC for this campaign when found outside a managed, IT-provisioned G Data installation. Isolate any system where it is found.
2. Detection, Hunt for NOVupdate.exe in process creation logs (Windows Event ID 4688 or Sysmon Event ID 1). Search EDR telemetry for avk.dll loaded by any process other than a verified G Data installation. Check DNS and proxy logs for connections to Alibaba Cloud IP ranges on TCP/443 and UDP/8080 from endpoints that are not cloud workloads. Review download logs for MSI files retrieved from domains typosquatting 'claude,' 'anthropic,' 'crowdstrike,' 'sentinelone,' or 'trellix.'
3. Eradication, On confirmed infected systems: terminate and remove NOVupdate.exe and avk.dll. Remove associated MSI installer artifacts. Purge registry run keys or startup folder entries added by the malware (T1547.001). Block identified C2 domains and IPs at the perimeter firewall and DNS resolver. No vendor patch applies, this is a campaign-based threat, not a software vulnerability.
4. Recovery, After removing artifacts, verify no additional persistence mechanisms remain using an EDR full-scan and manual review of HKCU/HKLM Run keys and startup folders. Monitor outbound connections from the previously infected host for 72 hours. Re-image if confidence in full eradication is low. Validate that no lateral movement or credential access occurred during the window of infection.
5. Post-Incident, This campaign exploited the absence of controls around unsigned software downloads (CWE-494) and unmanaged DLL loading (CWE-426). Evaluate whether software download policies restrict employees to approved sources. Implement or audit application allowlisting. Add brand-impersonation monitoring for your own vendors (CrowdStrike, SentinelOne, Trellix) to your threat intelligence feed. Update security awareness training to include AI tool impersonation as a current lure type.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to IR leadership, legal, and CISO immediately if any evidence of lateral movement (Security Event ID 4624 Type 3 from infected host), credential access (Event ID 4648, LSASS access in Sysmon Event ID 10), or data staging/exfiltration to Alibaba Cloud C2 is confirmed during the infection dwell window, as these conditions elevate the incident from initial access to potential breach requiring regulatory notification assessment.

Recovery Notes	After artifact removal, monitor the previously infected host's outbound network traffic for a minimum of 72 hours specifically filtering for connections to Alibaba Cloud ASN ranges (AS37963, AS45102) on TCP/443 and UDP/8080, as Beagle's PlugX-linked infrastructure may use multiple fallback C2 channels not identified in initial IOC sets. Validate integrity of any security tools (EDR agents, AV clients) installed on the infected host, as the campaign impersonated CrowdStrike, SentinelOne, and Trellix and the backdoor may have tampered with or replaced legitimate security software. Re-image any system where confidence in full eradication is below high, particularly if the system held privileged credentials or had access to sensitive data during the infection window.
Forensic Artifacts	NOVupdate.exe and avk.dll on disk: hash both files (SHA-256) and compare against known-good G Data binary hashes; presence of avk.dll outside 'C:\Program Files\G Data\AVK\' is definitive evidence of DLL sideloading (CWE-426) specific to this campaign | MSI installer file with Zone.Identifier alternate data stream intact: the ADS HostUrl field will contain the typosquatted domain used for delivery (e.g., a domain impersonating claude.ai, crowdstrike.com, sentinelone.com, or trellix.com), providing direct attribution to the Beagle campaign delivery vector | Windows DNS client event log (Microsoft-Windows-DNS-Client/Operational) and proxy logs: queries to Alibaba Cloud-hosted C2 domains on TCP/443 and UDP/8080 are the network-layer fingerprint of Beagle's command-and-control pattern, directly linked to the PlugX-associated infrastructure used in this campaign | Registry export of HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalent, plus Startup folder contents: Beagle establishes persistence via T1547.001 and these keys/folders will contain the specific entry pointing to NOVupdate.exe or a renamed variant, timestamped to the infection window | Sysmon Event ID 7 (ImageLoaded) logs showing avk.dll loaded by NOVupdate.exe: this is the highest-fidelity forensic artifact for DLL sideloading confirmation and distinguishes a Beagle-campaign infection from any legitimate G Data AVK installation, which would show the same DLL loaded only by G Data's own signed processes

Per-Action IR Details

Containment — Block execution of NOVupdate.exe across the environment via application control policy (e.g., AppLocker, Windows Defender Application Control). NOVupdate.exe is a high-confidence IOC for this campaign; its presence outside a managed G Data deployment has no legitimate explanation. Isolate any system where it is found.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality) — restrict execution to approved binaries only, CIS 2.3 (Address Unauthorized Software), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Without enterprise AppLocker/WDAC management, deploy a Sysmon configuration (SwiftOnSecurity baseline) with a rule to alert on NOVupdate.exe process creation: EventType 'ProcessCreate' where Image ends with 'NOVupdate.exe'. Immediately run: Get-Process | Where-Object {$_.Name -eq 'NOVupdate'} | Stop-Process -Force across all reachable endpoints via PowerShell remoting. Block the binary hash at the host firewall using: New-NetFirewallRule -DisplayName 'Block_Beagle_NOVupdate' -Action Block -Program 'C:\Path\NOVupdate.exe'. Use osquery to sweep: SELECT * FROM processes WHERE name = 'NOVupdate.exe'; across the fleet.

Evidence: Before isolating, capture: (1) full memory dump of the NOVupdate.exe process using ProcDump — 'procdump.exe -ma NOVupdate.exe novupdate_memdump.dmp' — to preserve the injected Beagle payload in memory before it is lost on reboot; (2) open network connections from the process via 'netstat -anob | findstr NOVupdate' to identify active Alibaba Cloud C2 IP and port; (3) loaded DLL list for the process — specifically confirm presence of avk.dll loaded from an anomalous path outside C:\Program Files\G Data\; (4) parent process tree from

Sysmon Event ID 1 or Windows Event ID 4688 to identify which MSI installer spawned NOVupdate.exe; (5) filesystem timestamps (Created, Modified, Accessed) on NOVupdate.exe and avk.dll using 'Get-Item | Select-Object Name, CreationTime, LastWriteTime, LastAccessTime'.

Detection — Hunt for NOVupdate.exe in process creation logs (Windows Event ID 4688 or Sysmon Event ID 1). Search EDR telemetry for avk.dll loaded by any process other than a verified G Data installation. Check DNS and proxy logs for connections to Alibaba Cloud IP ranges on TCP/443 and UDP/8080 from endpoints that are not cloud workloads. Review download logs for MSI files retrieved from domains typosquatting 'claude,' 'anthropic,' 'crowdstrike,' 'sentinelone,' or 'trellix.'

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 AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), MITRE ATT&CK T1574.002 (DLL Side-Loading) — detection pivot for avk.dll loaded by NOVupdate.exe outside G Data install path, MITRE ATT&CK T1566.002 (Spearphishing Link) — typosquatted download delivery vector

Compensating: Without a SIEM, run this PowerShell query against Windows Security Event logs: Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -match 'NOVupdate.exe'}. For DLL sideloading detection without EDR, use Sysmon Event ID 7 (ImageLoaded) with a filter on ImageLoaded path containing 'avk.dll' AND process image NOT matching 'C:\Program Files\G Data\'. For DNS hunting without a proxy solution, parse Windows DNS client event log (Microsoft-Windows-DNS-Client/Operational) for queries matching regex pattern: /(claude|anthropic|crowdstrike|sentinelone|trellix)[^.]*\.(?!anthropic\.com|crowdstrike\.com|sentinelone\.com|trellix\.com)/i. Download and apply the community Sigma rule for PlugX-linked sideloading (search Sigma HQ repo for 'dll_sideloading_abused_tools') to parse collected Sysmon logs with sigma-cli.

Evidence: Collect before triaging: (1) Windows Event ID 4688 or Sysmon Event ID 1 records for NOVupdate.exe showing full command line and parent process — command-line logging must be enabled via Group Policy (Audit Process Creation + include command line); (2) Sysmon Event ID 7 records showing avk.dll loaded outside 'C:\Program Files\G Data\' — this is the forensic fingerprint of sideloading vs. legitimate G Data use; (3) DNS query logs filtered for typosquatted domains containing 'claude', 'anthropic', 'crowdstrike', 'sentinelone', or 'trellix' with non-canonical TLDs or subdomain prefixes; (4) proxy or web filter logs for HTTP GET/POST to Alibaba Cloud ASN (AS37963, AS45102) on TCP/443 or UDP/8080 from non-cloud endpoints; (5) browser download history and Windows Zone.Identifier alternate data streams on MSI files to confirm download origin URL — run: Get-Item *.msi -Stream Zone.Identifier | Get-Content.

Eradication — On confirmed infected systems: terminate and remove NOVupdate.exe and avk.dll. Remove associated MSI installer artifacts. Purge registry run keys or startup folder entries added by the malware (T1547.001). Block identified C2 domains and IPs at the perimeter firewall and DNS resolver. No vendor patch applies — this is a campaign-based threat, not a software vulnerability.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation) — applied here as artifact removal, not software patching, NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-7 (Least Functionality), CIS 2.3 (Address Unauthorized Software), MITRE ATT&CK T1547.001 (Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder) — specific persistence mechanism to remove

Compensating: Without EDR for guided remediation: (1) terminate process — Stop-Process -Name NOVupdate -Force; (2) remove files — Remove-Item -Force 'C:\[install path]\NOVupdate.exe', 'C:\[install path]\avk.dll', and MSI artifacts in %TEMP% and %APPDATA%\Local\Temp; (3) audit registry persistence — reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\Software\Microsoft\Windows\CurrentVersion\Run for any entry pointing to NOVupdate.exe or referencing the sideload path, then delete: reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v [BeagleEntry] /f; (4) check startup folder — Get-ChildItem 'C:\Users\[user]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup'; (5) block C2 at Windows Firewall — New-NetFirewallRule -DisplayName 'Block_Beagle_C2' -Direction Outbound -Action Block -RemoteAddress [Alibaba C2 IPs] -Protocol TCP -RemotePort 443.

Evidence: Before removing artifacts, preserve: (1) full forensic image or at minimum a targeted collection of NOVupdate.exe and avk.dll with SHA-256 hashes documented — use: Get-FileHash -Algorithm SHA256 NOVupdate.exe; (2) export all Run key contents before deletion — reg export HKCU\Software\Microsoft\Windows\CurrentVersion\Run C:\IR\RunKeys_HKCU.reg and same for HKLM; (3) capture contents of Startup folder — copy all LNK and executable files to IR evidence share before removal; (4) export Windows Event Log Security and Sysmon logs to offline storage before touching the system; (5) document all C2 IP and domain indicators from active netstat and DNS cache — ipconfig /displaydns > C:\IR\dns_cache.txt — to support perimeter block accuracy.

Recovery — After removing artifacts, verify no additional persistence mechanisms remain using an EDR full-scan and manual review of HKCU/HKLM Run keys and startup folders. Monitor outbound connections from the previously infected host for 72 hours. Re-image if confidence in full eradication is low. Validate that no lateral movement or credential access occurred during the window of infection.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CP-10 (System Recovery and Reconstitution), CIS 5.1 (Establish and Maintain an Inventory of Accounts) — validate no accounts created or modified during infection window, MITRE ATT&CK T1003 (OS Credential Dumping) — validate no credential access tools executed during Beagle dwell time, MITRE ATT&CK T1021 (Remote Services) — validate no lateral movement from infected host

Compensating: Without EDR for post-eradication validation: (1) run Autoruns (Sysinternals) with 'Check VirusTotal' enabled to scan all persistence points including Run keys, scheduled tasks, services, and startup folders; (2) check for scheduled tasks created during infection window — Get-ScheduledTask | Where-Object {$_.Date -gt [infection_start_timestamp]}; (3) for lateral movement validation, review Windows Security Event ID 4624 (Logon) and 4648 (Explicit Credential Logon) from the infected host to other systems using: Get-WinEvent -ComputerName [host] -FilterHashtable @{LogName='Security';Id=4624;StartTime=[infection_start]} | Where-Object {$_.Message -match 'Logon Type.*3'}; (4) deploy Wireshark or tcpdump on the recovered host's network segment for 72 hours filtering on Alibaba Cloud ASN egress traffic.

Evidence: Before closing out recovery: (1) collect Windows Security Event ID 4648 (explicit credential use) and 4768/4769 (Kerberos TGT/TGS requests) from the infected host during the dwell window to assess if Beagle facilitated credential theft for lateral movement; (2) review Security Event ID 4624 logon events from other hosts showing origination from the infected system's IP/hostname during infection window; (3) export Scheduled Tasks XML — Export-ScheduledTask — for any task created during infection timeframe; (4) collect a final Autoruns snapshot post-remediation as documented evidence of clean state; (5) capture a post-remediation netstat baseline — netstat -anob > C:\IR\post_remediation_netstat.txt — timestamped, to serve as the clean-state reference for the 72-hour monitoring window.

Post-Incident — This campaign exploited the absence of controls around unsigned software downloads (CWE-494) and unmanaged DLL loading (CWE-426). Evaluate whether software download policies restrict employees to approved sources. Implement or audit application allowlisting. Add brand-impersonation monitoring for your own vendors (CrowdStrike, SentinelOne, Trellix) to your threat intelligence feed. Update security awareness training to include AI tool impersonation as a current lure type.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling) — update playbook to include DLL sideloading via abused security vendor binaries, NIST IR-8 (Incident Response Plan) — revise to address brand-impersonation delivery vectors, NIST SI-7 (Software, Firmware, and Information Integrity) — enforce code signing verification for all downloaded executables, NIST SA-22 (Unsupported System Components) — policy basis for restricting unapproved software sources, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — establish recurring hunt for sideloading patterns, CIS 2.1 (Establish and Maintain a Software Inventory) — unauthorized NOVupdate.exe would be caught by inventory gap analysis, CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability

Management Process) — extend to include campaign-based threats, not just CVEs, CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without a commercial TI feed: (1) subscribe to CISA's Known Exploited Vulnerabilities feed and free threat intel sharing via ISAC relevant to your sector; (2) create a free dnstwist (open source) scheduled scan against your own vendor brand names (crowdstrike, sentinelone, trellix, anthropic, claude) to detect newly registered typosquatted domains — run: dnstwist --registered crowdstrike.com weekly via cron; (3) create a YARA rule targeting the NOVupdate.exe + avk.dll sideloading pattern and deploy via ClamAV on email gateway and shared drives; (4) build a Sigma rule for Sysmon Event ID 7 where ImageLoaded matches 'avk.dll' and process is not in the G Data install path, and run it as a scheduled hunt against archived Sysmon logs using sigma-cli; (5) add a mandatory acknowledgment step to the software download SOP requiring employees to verify URLs against a pinned approved-sources list before downloading any security or AI tooling.

Evidence: For lessons learned documentation: (1) timeline reconstruction showing first MSI download event (browser history or proxy log) through to C2 beacon establishment — this establishes dwell time and scope for the post-incident report; (2) the Zone.Identifier ADS contents from the original MSI file confirming the typosquatted download URL; (3) the full list of C2 indicators (Alibaba Cloud IPs and domains) observed in DNS/proxy logs — these become permanent block entries and TI feed submissions; (4) Sysmon Event ID 7 records showing avk.dll sideloading as the definitive forensic proof of the DLL hijack technique for the after-action report; (5) any Security Event ID 4688 or Sysmon Event ID 1 records of unusual child processes spawned by NOVupdate.exe to characterize full Beagle backdoor capability observed in this environment.

Detection Guidance

Primary IOC: presence of NOVupdate.exe on any system not running a managed, IT-provisioned G Data installation. Secondary IOCs: avk.dll loaded outside a verified G Data process tree; MSI installers downloaded from domains containing 'claude,' 'anthropic,' or typosquats of major security vendor names. Behavioral indicators: DonutLoader-style in-memory injection events in EDR (unsigned shellcode executed from memory); outbound connections on UDP/8080 to Alibaba Cloud IP space from endpoint systems; encrypted C2 beaconing on TCP/443 with irregular intervals from recently installed processes. Sysmon rules: alert on ImageLoad events where ImageLoaded matches avk.dll and the parent process is not a verified G Data binary path. MITRE coverage gaps to check: T1574.002 (DLL sideloading), T1055 (process injection), T1095 (non-application layer C2). C2 IPs and domains should be obtained from current threat intelligence feeds (BleepingComputer, Security Affairs, and OSINT sources tracking Alibaba Cloud abuse).

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Typosquatted Anthropic/Claude AI domains (specific domains not confirmed in available T3 sources)`	Initial delivery sites impersonating Anthropic Claude AI brand; deliver malicious MSI installer	MEDIUM
DOMAIN	`Typosquatted CrowdStrike, SentinelOne, Trellix domains (specific domains not confirmed in available T3 sources)`	Secondary delivery lures observed since February 2026; same infection chain	MEDIUM

Type	Value	Context	Confidence
URL	`Alibaba Cloud-hosted C2 infrastructure (specific IPs/URLs not confirmed in available T3 sources)`	Beagle backdoor C2 communications over TCP/443 (AES-encrypted) and UDP/8080	MEDIUM
HASH	`NOVupdate.exe (specific file hash not confirmed in available T3 sources — flag any instance outside verified G Data deployment)`	Legitimate signed G Data binary abused for DLL sideloading; high-confidence IOC when found outside managed G Data installation	HIGH
HASH	`avk.dll (specific file hash not confirmed in available T3 sources)`	Malicious DLL sideloaded via NOVupdate.exe; delivers Beagle backdoor	HIGH

Framework Mappings

MITRE-ATTACK

- **T1547.001** — Registry Run Keys / Startup Folder
- **T1574.002** — DLL Side-Loading
- **T1095** — Non-Application Layer Protocol
- **T1071.001** — Web Protocols
- **T1055** — Process Injection
- **T1566** — Phishing
- **T1204.002** — Malicious File
- **T1105** — Ingress Tool Transfer
- **T1027** — Obfuscated Files or Information
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1583.001** — Domains
- **T1059.003** — Windows Command Shell
- **T1573.001** — Symmetric Cryptography

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-8** — Spam Protection
- **CM-7** — Least Functionality

- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1574.002	DLL Side-Loading	Persistence
T1095	Non-Application Layer Protocol	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1055	Process Injection	Defense-Evasion
T1566	Phishing	Initial-Access
T1204.002	Malicious File	Execution
T1105	Ingress Tool Transfer	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1583.001	Domains	Resource-Development
T1059.003	Windows Command Shell	Execution
T1573.001	Symmetric Cryptography	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/fake-claude-ai-websi...	T3

Source	URL	Tier
Fake Claude AI installer abuses DLL sideloading to deploy PlugX	https://securityaffairs.com/190754/malware/fake-claude-ai-installer...	T3
Fake Claude Website Distributes New 'Beagle' Malware - SecNews	https://www.secnews.gr/en/707510/claude-fake-site-beagle-malware/	T3
Fake Claude site installs malware that gives attackers access to your ...	https://securityboulevard.com/2026/04/fake-claude-site-installs-mal...	T3
Three high-risk AI vulnerabilities discovered in Claude.ai - TechRadar	https://www.techradar.com/pro/security/three-high-risk-ai-vulnerabi...	T3

Generated 2026-05-07 13:54 UTC by TJS Security Command Center