INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-13 06:39 UTC

Outsider Enterprise PhaaS Network Abuses Gemini AI for Mass Smishing Campaign; Google Sues, FBI Seizes Infrastructure

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0450
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Google Gemini AI (abused for phishing page generation), Android SMS/messaging surface, AT&T / T-Mobile / Verizon (carrier smishing delivery), Shopify (seized storefront infrastructure), Telegram (coordination and bot infrastructure)
Published	2026-06-12T14:59:32
Discovery Source	Rss

Executive Summary

A Chinese-operated phishing-as-a-service network called Outsider Enterprise weaponized Google's Gemini AI to mass-produce fraudulent websites and SMS lures, stealing an estimated 3.87 million credit cards and generating $1.9 billion in consumer financial losses across more than 100,000 confirmed victims, according to Google's federal lawsuit and FBI operational reporting. Google has filed a federal lawsuit and the FBI's Operation Ghost Hook seized thousands of fraudulent domains, approximately 9,000 fake websites, and $100,000 in cryptocurrency proceeds, with Operation Riptide continuing to dismantle remaining infrastructure. Organizations whose customers use SMS-based communications, e-commerce platforms, or AI-assisted content generation pipelines face elevated reputational and fraud liability as this campaign model scales.

Technical Analysis

Outsider Enterprise operated a PhaaS (phishing-as-a-service) platform that integrated Google Gemini AI to auto-generate convincing phishing page content and SMS lure messages at scale, bypassing the manual effort traditionally required in smishing operations. The attack chain combined AI-generated content (T1588.005, obtain AI tools; T1656, impersonation) with bulk SMS delivery (T1566.004, spearphishing via SMS) across AT&T, T-Mobile, and Verizon carrier surfaces. Command-and-control coordination ran over Telegram bots (T1071.001, application layer protocol), with domain infrastructure managed through registered fraudulent

domains (T1583.001) and web services (T1583.006). Shopify storefronts served as the fraudulent e-commerce layer. Credential and payment card harvesting was accomplished via keylogging/input capture (T1056.001) and session cookie theft (T1539). Exfiltration used web services (T1567). Proxy infrastructure (T1090.002, T1090.003) obscured operator attribution. No CVE is assigned; the attack exploits platform-level weaknesses rather than a patchable software vulnerability. Relevant CWEs: CWE-1021 (improper restriction of rendered UI layers, phishing page spoofing), CWE-345 (insufficient verification of data authenticity, SMS sender spoofing), CWE-693 (protection mechanism failure, bypass of platform abuse controls). CVSS base estimated at 9.5 reflecting network-accessible, low-complexity attack vector (AV:N, AC:L, PR:N) with demonstrated mass victim impact; this estimate is based on attack surface severity rather than a formal CVE scoring. EPSS is not applicable; no CVE is assigned. FBI seizures disrupted thousands of domains and ~9,000 fake sites; the broader network remains partially operational pending Operation Riptide.

Action Checklist

1. Step 1: Containment, Block known Outsider Enterprise infrastructure at the DNS and network perimeter. Cross-reference seized domain lists from FBI Operation Ghost Hook advisories against your DNS resolver logs, proxy logs, and firewall egress rules. Flag and block outbound connections to any matching domains. Notify your carrier account managers at AT&T, T-Mobile, or Verizon if you operate enterprise SMS programs, as smishing lures may spoof your brand.
2. Step 2: Detection, Query email and SMS gateway logs for inbound messages containing URL patterns consistent with the campaign: short-lived domains, newly registered TLDs, and Shopify subdomain abuse. Review AU-6 (audit record review and analysis) outputs for anomalous user authentication events following inbound SMS delivery windows. Behavioral indicators include credential submission to lookalike domains and session token reuse from unexpected geolocations. Search SIEM for Telegram C2 beacon patterns (T1071.001) from internal endpoints.
3. Step 3: Eradication, There is no software patch; this is a platform-abuse campaign. Eradication actions: (1) Submit abuse reports to Google (Gemini API misuse), Shopify (fraudulent storefronts), and Telegram (bot infrastructure) using their respective abuse portals. (2) If your brand was spoofed in lures, engage your legal team to file DMCA takedowns against active phishing domains. (3) Rotate any credentials or API keys that may have been exposed via compromised user sessions (D3-CRO, credential rotation).
4. Step 4: Recovery, Validate that user accounts showing anomalous post-smishing activity have had sessions terminated and passwords reset (D3-CH, credential hardening). Confirm MFA enrollment for all externally exposed applications (CIS 6.3, require MFA for externally-exposed applications). Review AU-11 (audit record retention) to ensure sufficient log history exists to scope any affected accounts. Monitor for resumed campaign activity using threat intelligence feeds referencing Outsider Enterprise IOCs.
5. Step 5: Post-Incident, Conduct a control gap review against CIS 6.3 and CIS 6.4 (MFA for externally-exposed applications and remote network access). Assess whether your organization's brand monitoring program covers SMS lure detection, not only email. Evaluate AI platform usage policies: establish controls to detect if internal AI tools are being abused for content generation at scale, referencing NIST AC-6 (least privilege) for API access scoping. Brief security awareness program on AI-generated smishing: synthetic lures are now indistinguishable from legitimate messages by grammar or formatting alone.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately if internal endpoint telemetry confirms Telegram C2 beacon activity (indicating an employee device was targeted and successfully compromised), if any enterprise application credential appears in Outsider Enterprise harvested data sets (cross-reference HaveIBeenPwned Enterprise or CISA advisories), or if PII or payment card data processed by your organization is within scope of the estimated 3.87 million compromised cards — triggering mandatory breach notification under PCI DSS 4.0 Requirement 12.10 and applicable state data breach statutes.
Recovery Notes	After session termination and MFA enforcement, monitor IdP sign-in logs daily for 30 days for any recurrence of impossible-travel authentication or credential-stuffing patterns against accounts that were in scope, as Outsider Enterprise harvested credentials may be resold to secondary threat actors and abused on a delayed timeline. Validate that any Shopify or third-party storefront integrations using API keys were rotated and that the old keys are confirmed deleted — not merely disabled — in the respective vendor consoles. Maintain a watchlist in your DNS resolver or threat intelligence feed for newly registered domains matching your brand's typosquat patterns, as Operation Ghost Hook seizures historically prompt rapid infrastructure replacement by the threat actor within days.
Forensic Artifacts	SMS gateway inbound message logs (MMS/SMS delivery headers and body URLs) for the 90-day window preceding detection — Outsider Enterprise lures use short-lived domains on .xyz, .top, .shop, and .vip TLDs with 6-10 character random path segments; these headers identify which employee phone numbers received lures and at what timestamps. | IdP authentication logs (Azure AD Sign-In Log Event ID 4624 / Okta System Log eventType session.start) filtered for successful logins occurring within 5 minutes of an inbound SMS delivery timestamp to the same user — this correlation fingerprints accounts where a user clicked a Gemini-generated phishing page and submitted credentials. | Proxy or web filter HTTP POST logs to Shopify subdomains (*.myshopify.com) and newly registered domains not matching your approved vendor list — Outsider Enterprise hosted credential harvesting forms on seized Shopify storefronts; POST requests to these endpoints confirm credential submission from internal devices. | DNS resolver query logs (Windows DNS debug log at C:\Windows\System32\dns\dns.log or Zeek dns.log) for resolutions of FBI Operation Ghost Hook seized domains — queries occurring after the seizure date indicate stale threat feeds or DNS caching and confirm internal hosts attempted contact with known adversary infrastructure. | Telegram process execution artifacts on Windows endpoints: Windows Security Event ID 4688 (Process Creation) with ParentProcessName matching a browser or email client spawning Telegram.exe or a Telegram web session initiating outbound TLS connections to 149.154.160.0/20 or 91.108.4.0/22 (Telegram's published ASN ranges) — indicative of a compromised user being directed from a smishing lure to a Telegram bot for further social engineering or data exfiltration.

Per-Action IR Details

Step 1: Containment — Block known Outsider Enterprise infrastructure at the DNS and network perimeter. Cross-reference seized domain lists from FBI Operation Ghost Hook advisories against your DNS resolver logs, proxy logs, and firewall egress rules. Flag and block outbound connections to any matching domains. Notify your carrier account managers at AT&T, T-Mobile, or Verizon if you operate enterprise SMS programs, as smishing lures may spoof your brand.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems and block adversary infrastructure to prevent further credential harvesting and lateral smishing delivery.

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: Export your Pi-hole or pfSense blocklist and ingest the FBI Operation Ghost Hook seized domain list as a flat-file block feed using pfBlockerNG or a simple cron-driven RPZ zone update. Cross-reference against Zeek/Suricata DNS logs with: `grep -Ff ghost_hook_domains.txt /var/log/zeek/dns.log` to surface prior resolutions. For outbound HTTP, add Squid ACL deny rules keyed to newly registered TLDs (.xyz, .top, .shop) seen in the campaign.

Evidence: Before applying firewall or DNS block rules that would sever active connections: capture a netflow or pcap snapshot of current egress traffic to document any endpoints already communicating with Outsider Enterprise infrastructure — use `tcpdump -i eth0 -w outsider_pre_block_$(date +%s).pcap` at the perimeter. Preserve DNS resolver cache (`rndc dumpdb -cache` on BIND, or export Windows DNS debug log at C:\Windows\System32\dns\dns.log) to establish which internal hosts resolved Operation Ghost Hook domains prior to blocking. These records are overwritten on resolver restart.

Step 2: Detection — Query email and SMS gateway logs for inbound messages containing URL patterns consistent with the campaign: short-lived domains, newly registered TLDs, and Shopify subdomain abuse. Review AU-6 (audit record review and analysis) outputs for anomalous user authentication events following inbound SMS delivery windows. Behavioral indicators include credential submission to lookalike domains and session token reuse from unexpected geolocations. Search SIEM for Telegram C2 beacon patterns (T1071.001) from internal endpoints.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate multi-source indicators (SMS gateway telemetry, authentication logs, proxy logs) to scope victim accounts that submitted credentials to Outsider Enterprise Gemini-generated phishing pages.

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

Compensating: Without a SIEM, use PowerShell against Azure AD or on-prem AD sign-in logs: `Get-AzureADAuditSignInLogs | Where-Object {$_.RiskLevelDuringSignIn -ne 'none' -or $_.Location.CountryOrRegion -notin @('US')} | Export-Csv suspicious_logins.csv`. For SMS gateway log analysis (no SIEM), use `grep -E '\.(xyz|top|shop|vip|ltd)/[a-z0-9]{6,}' /var/log/sms-gateway/inbound.log` to surface Outsider Enterprise-style short-path lure URLs. Deploy the free Sigma rule `proc_creation_win_telegram_susp_child_process` via Chainsaw against Windows event logs to detect Telegram beacon child processes on endpoints.

Evidence: This is an analytical step — no live state is altered. Collect and preserve before analysis activity overwrites retention windows: (1) Export SMS gateway delivery receipts and message headers for the trailing 90 days (Outsider Enterprise campaigns operate persistently); (2) Pull IdP/SSO authentication logs (Okta System Log, Azure AD Sign-In Log, or Windows Security Event ID 4624/4625) filtered for the 30 minutes following inbound SMS delivery timestamps to correlate credential submission timing; (3) Extract proxy or web filter logs (Squid access.log, Palo Alto URL filtering logs) for HTTP POST requests to Shopify subdomains (*.myshopify.com paths not matching your own storefronts) and newly registered domains resolved within the campaign window.

Step 3: Eradication — There is no software patch; this is a platform-abuse campaign. Eradication actions: (1) Submit abuse reports to Google (Gemini API misuse), Shopify (fraudulent storefronts), and Telegram (bot infrastructure) using their respective abuse portals. (2) If your brand was spoofed in lures, engage your legal team to file DMCA takedowns against active phishing domains. (3) Rotate any credentials or API keys that may have been exposed via compromised user sessions (D3-CRO — credential rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove threat actor footholds by disabling compromised credentials, eliminating adversary-controlled infrastructure referencing your brand, and reporting platform abuse to terminate Gemini-generated phishing page hosting.

Controls: NIST AC-2 (Account Management), NIST IA (Identification and Authentication) — no single IA control in the knowledge base maps to credential rotation; AC-2 governs account lifecycle actions including disabling and resetting compromised accounts, CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access

Revoking Process)

Compensating: For credential rotation without PAM tooling: generate a prioritized list of accounts that authenticated from unexpected geolocations or submitted credentials during the smishing window using `Search-ADAccount -PasswordExpired | Select Name,LastLogonDate` and force-reset via `Set-ADAccountPassword` with the `-Reset` flag. For API key rotation (Google, Shopify integrations), use each platform's CLI: `gcloud iam service-accounts keys create` (new key) followed by immediate deletion of the exposed key ID. Document each rotation with timestamp and actor in your incident ticket before proceeding.

Evidence: Credential rotation and session revocation alter live authentication state — capture before acting: (1) Export a full active session list from your IdP (Okta Admin Console → Reports → System Log filtered for `session.start` events, or Azure AD Sign-In logs) to document all live sessions associated with potentially compromised accounts; (2) Retrieve any OAuth tokens or API keys currently active in your Google Cloud project (`gcloud iam service-accounts keys list --iam-account=`) and preserve the key IDs and creation timestamps as evidence of the exposure window; (3) If Telegram beacon activity was detected in Step 2, capture process memory and active network connections (`Get-NetTCPConnection | Where-Object State -eq 'Established' | Where-Object RemotePort -in @(443,80,5222)`) from implicated endpoints before session kill.

Step 4: Recovery — Validate that user accounts showing anomalous post-smishing activity have had sessions terminated and passwords reset (D3-CH — credential hardening). Confirm MFA enrollment for all externally exposed applications (CIS 6.3 — require MFA for externally-exposed applications). Review AU-11 (audit record retention) to ensure sufficient log history exists to scope any affected accounts. Monitor for resumed campaign activity using threat intelligence feeds referencing Outsider Enterprise IOCs.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore user accounts to a verified-clean state, enforce MFA to defeat stolen credential reuse from Outsider Enterprise harvesting, and confirm log retention depth supports ongoing scope validation.

Controls: NIST AU-11 (Audit Record Retention), NIST AC-12 (Session Termination), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: Without enterprise MDM or IdP bulk-enrollment tooling: audit MFA enrollment status in Google Workspace via `gam report users fields accounts:is_2sv_enrolled` or in Microsoft 365 via `Get-MsolUser -All | Where-Object {$_.StrongAuthenticationRequirements.Count -eq 0} | Select UserPrincipalName`. For session termination without SOAR: in Azure AD use `Revoke-AzureADUserAllRefreshToken -ObjectId ` per affected account; in Google Workspace use `gam user signout`. Monitor Outsider Enterprise IOC feeds via the free CISA Known-Exploited Vulnerabilities catalog and OTX AlienVault pulse 'Outsider Enterprise PhaaS' for resumed domain registration activity.

Evidence: Session termination alters live authentication state — before revoking, document: (1) All active refresh tokens and their issuance timestamps from your IdP to establish the credential-theft window precisely (Azure AD: `Get-AzureADAuditSignInLogs` filtered by affected UPNs; Okta: System Log API `eventType eq session.start`); (2) Verify AU-11 retention depth covers the estimated campaign start date — Outsider Enterprise has operated persistently, so log gaps before 90 days would leave scope blind spots; (3) Preserve a snapshot of MFA enrollment state per account before remediation so the pre-incident baseline is documented for regulatory or legal purposes.

Step 5: Post-Incident — Conduct a control gap review against CIS 6.3 and CIS 6.4 (MFA for externally-exposed applications and remote network access). Assess whether your organization's brand monitoring program covers SMS lure detection, not only email. Evaluate AI platform usage policies: establish controls to detect if internal AI tools are being abused for content generation at scale, referencing NIST AC-6 (least privilege) for API access scoping. Brief security awareness program on AI-generated smishing: synthetic lures are now indistinguishable from legitimate messages by grammar or formatting alone.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons-learned review to close the MFA and brand-monitoring gaps Outsider Enterprise exploited, update detection playbooks for AI-generated smishing, and restrict internal Gemini/LLM API access under least-privilege principles to prevent insider abuse of the same weaponization vector.

Controls: NIST AC-6 (Least Privilege), NIST AU-13 (Monitoring For Information Disclosure), 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: For brand monitoring without a commercial DRPS: configure Google Alerts for your brand name combined with terms like 'verify', 'account suspended', 'delivery', and common smishing pretexts; supplement with free dnstwist (`dnstwist yourdomain.com --format json`) run weekly via cron to detect lookalike domain registrations targeting your brand. For AI API access scoping without PAM: audit Google Cloud IAM bindings monthly (`gcloud projects get-iam-policy --format=json | jq '.bindings[] | select(.role | contains("aiplatform"))'`) and remove Gemini API roles from accounts that do not require them, enforcing least-privilege per NIST AC-6.

Evidence: Post-incident review is non-destructive — no volatile capture required at this phase. Preserve as institutional artifacts: (1) Final scoped account list with credential-compromise determination and evidence basis; (2) Timeline reconstruction mapping FBI Operation Ghost Hook seizure dates against your DNS resolver logs to determine whether any infrastructure was queried after seizure (indicating stale IOC feeds or DNS caching gaps); (3) Inventory of internal Gemini API key holders and their access scopes as of the incident date, establishing the baseline for least-privilege remediation; (4) Lessons-learned report per NIST 800-61r3 §4 covering detection latency, MFA enrollment gaps, and brand monitoring blind spots, to be shared with carrier account managers and legal counsel.

Detection Guidance

Primary detection surface is DNS and proxy egress logs. Query for connections to newly registered domains (registration age under 30 days) combined with URL paths containing checkout, verify, confirm, or update patterns consistent with fake e-commerce flows. Review SMS gateway or mobile device management (MDM) logs for inbound messages delivering short URLs resolving to Shopify subdomains or lookalike brand domains not in your approved vendor list. In your SIEM, correlate: (1) inbound SMS delivery timestamp, (2) subsequent user authentication attempt within 10 minutes, (3) authentication source IP inconsistent with user's normal geolocation - this three-event chain is a strong behavioral indicator of smishing-to-credential-harvest success. Monitor for Telegram API endpoints (api.telegram.org) in outbound proxy logs from endpoints not authorized for Telegram use (T1071.001 C2 indicator). Review AU-2 (event logging) configurations to confirm SMS gateway events and authentication logs are captured. IOC enrichment: cross-reference FBI Ghost Hook public domain seizure lists (published in official advisories), Google's complaint exhibits (available via PACER Federal Court Records if your organization has access), and threat intelligence platforms for Outsider Enterprise infrastructure indicators.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`See FBI Operation Ghost Hook seized domain list`	Thousands of fraudulent domains used for smishing lure delivery and fake e-commerce pages; specific domain list available via FBI and Google's federal complaint filing	HIGH
URL	`Shopify subdomain infrastructure (pattern: *.myshopify.com storefronts flagged in complaint)`	Outsider Enterprise used Shopify storefronts as fraudulent e-commerce surfaces; specific subdomain list not yet publicly enumerated in available sources	MEDIUM

Type	Value	Context	Confidence
URL	`api.telegram.org`	Telegram used for C2 coordination and bot operations; outbound connections to Telegram API from non-authorized endpoints are a behavioral indicator	MEDIUM
HASH	`Not available in current source reporting`	No file hashes have been published in the sources available for this item; monitor threat intelligence platforms for Outsider Enterprise malware artifact updates	LOW

Framework Mappings

MITRE-ATTACK

- **T1090.003** — Multi-hop Proxy
- **T1056.001** — Keylogging
- **T1585.002** — Email Accounts
- **T1071.001** — Web Protocols
- **T1566.004** — Spearphishing Voice
- **T1567** — Exfiltration Over Web Service
- **T1598** — Phishing for Information
- **T1583.006** — Web Services
- **T1588.002** — Tool
- **T1539** — Steal Web Session Cookie
- **T1090.002** — External Proxy
- **T1583.001** — Domains
- **T1496** — Resource Hijacking
- **T1656** — Impersonation
- **T1588.005** — Exploits

OWASP-TOP10-2021

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

NIST-800-53R5

- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness

CIS-V8

- **2.5** — Allowlist Authorized Software
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1090.003	Multi-hop Proxy	Command-And-Control
T1056.001	Keylogging	Collection
T1585.002	Email Accounts	Resource-Development
T1071.001	Web Protocols	Command-And-Control
T1566.004	Spearphishing Voice	Initial-Access
T1567	Exfiltration Over Web Service	Exfiltration
T1598	Phishing for Information	Reconnaissance
T1583.006	Web Services	Resource-Development
T1588.002	Tool	Resource-Development
T1539	Steal Web Session Cookie	Credential-Access
T1090.002	External Proxy	Command-And-Control
T1583.001	Domains	Resource-Development
T1496	Resource Hijacking	Impact
T1656	Impersonation	Defense-Evasion
T1588.005	Exploits	Resource-Development

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/google-sues-chinese-smishing-netw...	T3
Google sues scam ring that used Gemini AI to build fraud sites - TNW	https://thenextweb.com/news/google-gemini-outsider-enterprise-scam-...	T3

Source	URL	Tier
Scammers Used Gemini AI to Help Build Spam Messages, Google ...	https://www.insurancejournal.com/news/national/2026/06/12/873591.htm	T3
Google Sues to Stop Chinese Cybercrime Group from Using Its A.I.	https://www.nytimes.com/2026/06/12/technology/google-lawsuit-china-...	T2
A massive Chinese cybercrime operation just hijacked Google's ...	https://x.com/Unveiled_ChinaX/status/2065440554054525400/photo/1	T3

Generated 2026-06-13 06:39 UTC by TJS Security Command Center