INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-14 18:26 UTC

Operation Riptide Dismantles Outsider Enterprise: A Blueprint for AI-Powered Phishing-as-a-Service at Scale

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0459
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Google (Android), AT&T, T-Mobile, Verizon, Shopify (storefront seized), Telegram (bot infrastructure), consumers targeted via major U.S. carrier SMS infrastructure
Published	2026-06-14T10:36:23
Discovery Source	Rss

Executive Summary

The FBI, Google, and Black Lotus Labs dismantled Outsider Enterprise, a Chinese-nexus Phishing-as-a-Service platform that operated approximately 9,000 fraudulent websites, stole 3.8 million payment card records, and caused an estimated $1.9 billion in financial losses since 2023. The platform abused Google Gemini APIs to generate convincing SMS phishing lures at industrial scale, delivered through abused U.S. carrier infrastructure at AT&T, T-Mobile, and Verizon. While the infrastructure has been disrupted, copycat operators and residual tooling remain active risks, and any organization whose customers receive SMS communications is an ongoing target.

Technical Analysis

Outsider Enterprise operated as a full-service PhaaS platform, providing affiliates with AI-generated smishing lures, fraudulent storefronts, payment harvesting infrastructure, and Telegram-based command-and-control. The platform abused Google Gemini APIs to produce high-volume, linguistically convincing SMS content that bypassed traditional signature-based phishing filters. Delivery exploited U.S. carrier SMS infrastructure (AT&T, T-Mobile, Verizon), with lures impersonating Google, financial institutions, and logistics providers. Approximately 9,000 fraudulent domains and over one million malicious URLs were in active use. Shopify storefronts were seized as part of takedown actions. Disruption included server seizures, domain sinkholing, Telegram bot infrastructure takeover, and civil litigation filed by Google. No discrete CVE applies; the attack chain maps to: CWE-345 (Insufficient Verification of Data Authenticity), CWE-1021 (Improper Restriction of Rendered UI

Layers), CWE-940 (Improper Verification of Source of a Communication Channel), and CWE-693 (Protection Mechanism Failure). MITRE ATT&CK techniques include T1583.001 (Acquire Infrastructure: Domains), T1598.003 (Phishing for Information: Spearphishing via Service), T1539 (Steal Web Session Cookie), T1557 (Adversary-in-the-Middle), T1598 (Phishing for Information), T1606.001 (Forge Web Credentials: Web Cookies), T1059 (Command and Scripting Interpreter), T1657 (Financial Theft), T1566.004 (Phishing: Spearphishing via SMS), T1588.004 (Obtain Capabilities: Digital Certificates), T1583.006 (Acquire Infrastructure: Web Services), and T1586 (Compromise Accounts). The infrastructure disruption is confirmed but residual tooling and affiliate operators remain unaccounted for.

Action Checklist

1. Step 1: Containment. Audit outbound SMS and messaging workflows for abuse of carrier APIs; block known malicious domains via DNS sinkholes and enforce URL filtering on corporate mobile device management (MDM) profiles. Cross-reference any Telegram bot integrations against known Outsider Enterprise bot IDs when published by FBI or Black Lotus Labs via their official advisories. Restrict AI API usage (including Gemini and similar generative AI endpoints) to approved, monitored applications via policy (NIST AC-4, Information Flow Enforcement).
2. Step 2: Detection. Monitor security email/SMS gateways for anomalous outbound message volume or new sender IDs impersonating your brand. Query DNS resolver logs and web proxy logs for requests to newly registered domains (less than 30 days old) matching logistics, financial, or carrier brand patterns. Review authentication logs for session cookie theft indicators: concurrent sessions from geographically dispersed IPs, rapid session reuse after authentication events (NIST AU-6, Audit Record Review and Analysis; CIS 8.2, Collect Audit Logs). Behavioral indicator: users reporting unexpected carrier-branded SMS messages containing shortened URLs or redirects to login pages.
3. Step 3: Eradication. Submit fraudulent domains impersonating your brand to CISA's phishing takedown coordination and carrier abuse reporting portals (AT&T, T-Mobile, Verizon each maintain abuse intake). Rotate any API keys or service credentials exposed via compromised Shopify or similar e-commerce storefronts (NIST IA-4, Identifier Management). Revoke and reissue any digital certificates associated with impersonated domains. Enforce AI API key scoping and rate-limit policies to prevent generative AI abuse by unauthorized affiliates (NIST AC-6, Least Privilege).
4. Step 4: Recovery. Validate that brand-impersonating domains identified during triage are sinkholed or resolved to CISA/FBI-controlled addresses. Reconfirm SMS sender ID registrations through carrier programs (e.g., 10DLC registration) to establish baseline. Monitor payment card processors for anomalous chargebacks or fraud patterns in the 30-90 days following the campaign window. Implement post-incident session validation for high-value user accounts: require re-authentication after session anomalies (NIST AC-12, Session Termination; CIS 4.3, Configure Automatic Session Locking on Enterprise Assets).
5. Step 5: Post-Incident. Conduct a tabletop exercise simulating AI-generated phishing at scale targeting your customer-facing SMS channels. Review anti-phishing controls against AI-generated content specifically, as traditional signature and lexical filters are insufficient against Gemini-quality lures. Assess brand monitoring coverage: confirm you have active alerting on newly registered lookalike domains (CIS 7.1, Establish and Maintain a Vulnerability Management Process). Evaluate whether existing MFA implementations resist session cookie theft as a bypass path, and harden accordingly (NIST IA-2, Authentication; CIS 6.3, Require MFA for Externally-Exposed Applications).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal, compliance, and executive leadership if internal DNS/proxy logs confirm employee or customer devices resolved Outsider Enterprise domains, if Shopify or e-commerce API keys show unauthorized access consistent with credential harvesting, or if payment card processor data shows chargeback anomalies exceeding your organization's fraud threshold — any of these conditions triggers PCI DSS breach notification obligations and potentially state-level consumer data breach notification requirements depending on the volume of affected card records.
Recovery Notes	Verify recovery by confirming all identified Outsider Enterprise lookalike domains return NXDOMAIN or sinkhole IPs from your corporate resolvers and that no new certificate transparency log entries appear for brand-impersonating domains within 14 days post-takedown. Monitor payment card fraud and chargeback rates weekly for a minimum of 90 days post-campaign, as Outsider Enterprise's 3.8 million harvested card records may be monetized on a delayed schedule through secondary markets after the platform dismantlement. Revalidate 10DLC sender ID registrations with all three major U.S. carriers (AT&T, T-Mobile, Verizon) to confirm no residual Outsider Enterprise-registered sender IDs remain associated with your brand name in carrier systems.
Forensic Artifacts	DNS resolver query logs filtered for Outsider Enterprise's approximately 9,000 fraudulent domain patterns — specifically logistics, financial institution, and U.S. carrier brand lookalikes (att-, tmobile-, verizon-, shopify- prefixed domains registered within the campaign window 2023 to present) — to establish which internal hosts resolved adversary infrastructure | Web proxy and SMS gateway logs showing outbound POST requests to Telegram API endpoints (api.telegram.org) with bot token parameters, which would indicate internal systems were configured as unwitting nodes in Outsider Enterprise's Telegram-based C2 and lure delivery bot network | Google Cloud Audit Logs (cloudaudit.googleapis.com/data_access) for Gemini API (generativelanguage.googleapis.com) calls — specifically data_access log entries showing API key usage from unexpected source IPs or at volumes inconsistent with approved application usage, evidencing whether your organization's Gemini API credentials were stolen and weaponized for phishing lure generation at scale | Shopify Partners dashboard and storefront admin audit logs covering app installations, webhook endpoint registrations, and customer PII export events during the 2023-to-present campaign window — Outsider Enterprise's seizure of Shopify storefronts was a documented campaign tactic and these logs would show unauthorized admin actions or data exfiltration events preceding storefront compromise | Authentication server logs (Windows Security Event ID 4624 with Logon Type 3, or SAML/OAuth token issuance logs) cross-correlated with geolocation data, specifically looking for the same account authenticating from a legitimate IP and then reusing the resulting session token from an IP in a different ASN within 60–300 seconds — the primary forensic signature of Outsider Enterprise's adversary-in-the-middle session cookie harvesting via its reverse proxy phishing kit infrastructure

Per-Action IR Details

Step 1: Containment — Audit outbound SMS and messaging workflows for abuse of carrier APIs; block known malicious domains via DNS sinkholes and enforce URL filtering on corporate mobile device management (MDM) profiles. Cross-reference any Telegram bot integrations against known Outsider Enterprise bot IDs if shared by FBI or Black Lotus Labs. Restrict AI API usage (including Gemini and similar generative AI endpoints) to approved, monitored applications via policy (NIST AC-4 — Information Flow

Enforcement).

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-20 (Use Of External Systems), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Export MDM-enrolled device DNS query logs (or router syslog if no MDM) and grep for domains registered within the last 30 days using a free WHOIS bulk lookup script against your proxy egress logs. For Telegram bot cross-referencing, query your firewall/proxy logs for connections to api.telegram.org and correlate bot token substrings in HTTP POST bodies using Wireshark display filter: `http.request.method == "POST" && http.host contains "api.telegram.org"`. Block Gemini API endpoints (generativelanguage.googleapis.com) at the perimeter firewall for all non-whitelisted source IPs.

Evidence: Before modifying any DNS sinkhole entries or MDM URL-filter profiles, capture: (1) a full export of current DNS resolver cache from corporate resolvers (Windows: `ipconfig /displaydns > dns_cache_pre.txt`; Linux: `systemd-resolve --statistics` and journal logs); (2) active outbound HTTPS connection table from the MDM gateway (`netstat -ano` or `ss -tulnp`) to preserve any live Outsider Enterprise C2 domain resolutions in flight; (3) Telegram bot API session tokens visible in proxy logs before any block rule truncates log retention. These volatile artifacts confirm which Outsider Enterprise domains were actively resolving inside your environment prior to sinkholing.

Step 2: Detection — Monitor security email/SMS gateways for anomalous outbound message volume or new sender IDs impersonating your brand. Query DNS resolver logs and web proxy logs for requests to newly registered domains (less than 30 days old) matching logistics, financial, or carrier brand patterns. Review authentication logs for session cookie theft indicators: concurrent sessions from geographically dispersed IPs, rapid session reuse after authentication events (AU-6 — Audit Record Review, Analysis, and Reporting; CIS 8.2 — Collect Audit Logs). Behavioral indicator: users reporting unexpected carrier-branded SMS messages containing shortened URLs or redirects to login pages.

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), CIS 8.2 (Collect Audit Logs)

Compensating: Use osquery on authentication servers to query active user sessions: `SELECT user, host, time, pid FROM logged_in_users;` and diff against a baseline export to surface concurrent logins from disparate geos. For DNS, pipe your resolver query log through a bash one-liner filtering for domains with WHOIS creation dates under 30 days: use `whois $(awk '{print $5}' dns.log | sort -u)` piped through grep for 'Creation Date' and compare to today minus 30. Deploy the free Sigma rule set (SigmaHQ) rule `win_susp_web_request_cmd_and_arguments.yml` adapted to flag POST requests to newly registered domains from corporate endpoints. Flag any authentication event (e.g., Windows Security Event ID 4624 Type 3) followed within 60 seconds by a geographically impossible second 4624 from a different IP for the same account — indicative of stolen session cookie replay consistent with Outsider Enterprise's AiTM-harvested credential chain.

Evidence: No live-state alteration occurs in this detection step; evidence capture is the step itself. Preserve: (1) raw DNS resolver query logs with full timestamp and source IP before any log rotation fires; (2) web proxy access logs containing full URI strings for any requests to AT&T, T-Mobile, Verizon, or Shopify lookalike domains; (3) authentication server logs showing session token issuance (e.g., Windows Security Event ID 4769 Kerberos ticket grants or SAML assertion logs) for accounts that subsequently show concurrent geo-dispersed sessions — this is the primary forensic indicator of Outsider Enterprise's session cookie harvesting via its adversary-in-the-middle reverse proxy infrastructure.

Step 3: Eradication — Submit fraudulent domains impersonating your brand to CISA's phishing takedown coordination and carrier abuse reporting portals (AT&T, T-Mobile, Verizon each maintain abuse intake). Rotate any API keys or service credentials exposed via compromised Shopify or similar e-commerce storefronts (D3-CRO — Credential Rotation). Revoke and reissue any digital certificates associated with impersonated

domains. Enforce AI API key scoping and rate-limit policies to prevent generative AI abuse by unauthorized affiliates (NIST AC-6 — Least Privilege).

NIST Phase: Eradication

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

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For a 2-person team without a secrets management platform: enumerate all Shopify API keys and webhook signing secrets via `GET /admin/api/2024-01/api_permissions.json` (Shopify Admin REST API) and immediately delete any key not mapped to a documented integration. For Google Gemini API keys, audit via Google Cloud Console IAM → Service Accounts → Keys tab; revoke all keys older than 90 days or with no recent API call history. Document each revocation with a timestamp and the associated integration owner before rotating, so the post-incident review can confirm no re-issuance gap exists.

Evidence: CRITICAL — before revoking any Shopify API credentials or Gemini API keys, capture: (1) full API key access logs from Google Cloud Audit Logs (Cloud Logging → `cloudaudit.googleapis.com/data_access`) showing which source IPs and user agents called the Gemini generativeLanguage API — this establishes whether Outsider Enterprise affiliates exfiltrated your API key and used it to generate phishing lures at scale; (2) Shopify Partners dashboard audit log export showing all storefront admin actions, app installations, and webhook endpoint changes within the campaign window (2023 to present); (3) CT log snapshot from crt.sh for your brand's domain names to document any fraudulent certificates issued during the Outsider Enterprise campaign period before revocation proceedings begin.

Step 4: Recovery — Validate that brand-impersonating domains identified during triage are sinkholed or resolved to CISA/FBI-controlled addresses. Reconfirm SMS sender ID registrations through carrier programs (e.g., 10DLC registration) to establish baseline. Monitor payment card processors for anomalous chargebacks or fraud patterns in the 30–90 days following the campaign window. Implement post-incident session validation for high-value user accounts: require re-authentication after session anomalies (NIST AC-12 — Session Termination; CIS 4.3 — Configure Automatic Session Locking on Enterprise Assets).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-12 (Session Termination), NIST AC-7 (Unsuccessful Logon Attempts), CIS 4.3 (Configure Automatic Session Locking on Enterprise Assets), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For teams without a commercial brand-monitoring service: set up daily automated crt.sh queries for your brand's domain variants using a cron job calling `curl -s 'https://crt.sh/?q=%25yourBrand%25&output=json'` and diff against prior day output to catch new fraudulent certificate issuances targeting your customers. For session anomaly enforcement without an enterprise IdP, use Apache/Nginx `ngx_http_limit_req_module` to rate-limit session token reuse velocity, and configure application-layer re-authentication triggers on any session where the client IP ASN changes mid-session — a reliable low-cost indicator of Outsider Enterprise's harvested cookie replay.

Evidence: Before forcing re-authentication on high-value accounts (which terminates live sessions and destroys in-memory session state), capture: (1) active session table from your application or IdP — specifically session tokens, associated IPs, user agents, and session creation timestamps for all accounts flagged during detection phase; (2) payment processor transaction logs for the 72 hours preceding recovery actions to establish a clean-state baseline for chargeback delta monitoring; (3) 10DLC campaign registration records from your carrier portal before any re-registration to document which sender IDs were legitimately yours versus which Outsider Enterprise operators registered lookalike IDs using your brand name.

Step 5: Post-Incident — Conduct a tabletop exercise simulating AI-generated phishing at scale targeting your customer-facing SMS channels. Review anti-phishing controls against AI-generated content specifically, as traditional signature and lexical filters are insufficient against Gemini-quality lures. Assess brand monitoring coverage: confirm you have active alerting on newly registered lookalike domains (CIS 7.1 — Establish and Maintain a Vulnerability Management Process). Evaluate whether existing MFA implementations resist

session cookie theft as a bypass path, and harden accordingly (D3-MFA — Multi-factor Authentication; CIS 6.3 — Require MFA for Externally-Exposed Applications).

NIST Phase: Post Incident

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

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Tabletop simulation for a 2-person team: use GoPhish (free, open source) configured with AI-generated lure text (generated internally for the exercise) sent via your own test SMS gateway to a volunteer user group — measure click rate and session cookie capture rate against your current controls to quantify the detection gap. For anti-phishing control assessment against AI-generated content, run your existing email/SMS filter ruleset against a corpus of Gemini-generated phishing messages and measure false-negative rate; document it as a risk finding. For MFA hardening against session cookie theft specifically, migrate at least admin accounts from TOTP/SMS OTP to FIDO2/WebAuthn passkeys, which are phishing-resistant by design and are not bypassable by Outsider Enterprise's AiTM reverse proxy session harvesting technique.

Evidence: This phase does not alter live system state; no volatile pre-capture is required. Preserve as post-incident documentation: (1) full lessons-learned report referencing the specific Outsider Enterprise IOCs (domain list, Telegram bot IDs, campaign sender IDs) shared by Black Lotus Labs and FBI, used as the simulation baseline; (2) anti-phishing filter test results showing detection rate against AI-generated Gemini-quality lures versus traditional signature-matched phishing — this quantifies the residual risk for leadership reporting; (3) MFA audit output showing which externally-exposed applications still accept session cookies without binding them to a hardware-backed credential, prioritized by customer PII or payment card data exposure.

Detection Guidance

Primary detection focus: brand impersonation via SMS, session cookie theft, and adversary-in-the-middle activity against web sessions. Log sources to query: (1) DNS resolver logs, search for queries to domains registered within 30 days matching your brand name, carrier names (att, tmobile, verizon), or logistics providers (ups, fedex, usps) with unfamiliar TLDs or hyphenated patterns. (2) Web proxy and SIEM, correlate short-lived URL redirects with subsequent credential submission events; flag sessions where authentication is immediately followed by geographically inconsistent access from a different IP. (3) Email and SMS gateway logs, anomalous volume spikes in SMS delivery reports or unrecognized sender IDs associated with your brand's short codes. (4) Authentication platform logs, detect session token reuse from two or more distinct IP addresses within a short time window (indicative of T1539 cookie theft and T1557 adversary-in-the-middle). (5) AI API usage logs (if applicable), review Gemini or other generative AI API call logs for unauthorized applications generating high-volume text content matching phishing lure patterns. Behavioral IOC pattern: victims receive an SMS with a shortened or lookalike URL; click leads to a credential-harvesting page mimicking Google, a financial institution, or a carrier; session cookie is exfiltrated before any MFA challenge is presented. No confirmed technical IOCs (IPs, domains, hashes) are available from the provided sources; refer to FBI and Black Lotus Labs advisories for published indicators when released.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`~1,000,000+ malicious URLs across ~9,000 fraudulent domains (specific values not published in available sources)`	Outsider Enterprise PhaaS platform URLs used in smishing lures; refer to FBI and Black Lotus Labs advisories for published indicator lists	LOW
DOMAIN	`~9,000 fraudulent domains (specific values not published in available sources)`	Fraudulent domains impersonating Google, financial institutions, logistics providers, and carrier brands; sinkholed as part of Operation Riptide	LOW

Framework Mappings

MITRE-ATTACK

- **T1583.001** — Domains
- **T1598.003** — Spearphishing Link
- **T1539** — Steal Web Session Cookie
- **T1557** — Adversary-in-the-Middle
- **T1598** — Phishing for Information
- **T1606.001** — Web Cookies
- **T1059** — Command and Scripting Interpreter
- **T1657** — Financial Theft
- **T1566.004** — Spearphishing Voice
- **T1588.004** — Digital Certificates
- **T1583.006** — Web Services
- **T1586** — Compromise Accounts

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

OWASP-TOP10-2021

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

CIS-V8

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

HIPAA-SECURITY

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

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
T1583.001	Domains	Resource-Development
T1598.003	Spearphishing Link	Reconnaissance
T1539	Steal Web Session Cookie	Credential-Access
T1557	Adversary-in-the-Middle	Credential-Access
T1598	Phishing for Information	Reconnaissance
T1606.001	Web Cookies	Credential-Access
T1059	Command and Scripting Interpreter	Execution
T1657	Financial Theft	Impact
T1566.004	Spearphishing Voice	Initial-Access
T1588.004	Digital Certificates	Resource-Development
T1583.006	Web Services	Resource-Development
T1586	Compromise Accounts	Resource-Development

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/fbi-disrupts-massive...	T3
Outsider Enterprise PhaaS Network Abuses Gemini AI for Mass	https://techjacksolutions.com/scc-intel/outsider-enterprise-phaas-n...	T3
T-Mobile Fallout, ChatGPT abuse, and Shopify's Hardcoded API ...	https://www.traceable.ai/blog-post/cybersecurity-roundup-february-2...	T3

Source	URL	Tier
Android Zero-Day Vulnerability Under Active Attack| AT&T ThreatTraq	https://www.youtube.com/watch?v=Au6-GHeeUQs	T3
AT&T, T-Mobile, and Verizon spring into action after threat to texters ...	https://www.phonearena.com/news/email-to-text-bug-at-t-t-mobile-ver...	T3

Generated 2026-06-14 18:26 UTC by TJS Security Command Center