INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-07 06:37 UTC

Organized TOAD Infrastructure Uses Sequentially Provisioned DID Blocks Across Brand Impersonation Callback Phishing Campaigns

THREAT CAMPAIGN | MEDIUM | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0284
Type	Threat Campaign
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Targeted users of PayPal, Geek Squad (Best Buy), McAfee, Norton LifeLock; abused VoIP/CPaaS providers: Sinch, Twilio, Bandwidth, Virtue, RingCentral, Verizon, NUSO
Published	2026-05-06T10:00:12+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

An organized criminal operation is running coordinated callback phishing campaigns that impersonate PayPal, Geek Squad, McAfee, and Norton LifeLock, tricking victims into calling fraudulent phone numbers staffed by fake support agents. Cisco Talos research reveals the attackers provision phone number blocks sequentially through commercial VoIP providers, rotate numbers every ~14 days, and reuse the same infrastructure across multiple brand lures, indicating a professionalized call-center backend rather than scattered individual scams. Organizations face credential theft, financial fraud, and social engineering losses that conventional email security tools cannot detect because the attack pivots on phone numbers, not malicious URLs or file hashes.

Technical Analysis

Cisco Talos formally classified phone numbers as a tracked IOC class after telemetry analysis of Telephone-Oriented Attack Delivery (TOAD) campaigns. Attackers provision Direct Inward Dialing (DID) number blocks sequentially through CPaaS providers, primarily Sinch, with secondary use of Twilio, Bandwidth, Virtue, RingCentral, Verizon, and NUSO. Median active lifespan per number is approximately 14 days before rotation; deliberate cool-down periods are engineered to evade reputation-based telephony filters. The same phone numbers appear across unrelated lure themes (PayPal billing fraud, Geek Squad renewal scams,

McAfee/Norton LifeLock subscription alerts) and across multiple attachment formats including PDFs. Cross-lure number reuse is not detectable via URL or file hash analysis, representing a blind spot in standard email security tooling. MITRE ATT&CK techniques involved include T1566.001 (Spearphishing Attachment), T1566.002 (Spearphishing Link), T1598.002 (Spearphishing via Service), T1598 (Phishing for Information), T1656 (Impersonation), T1036.007 (Masquerading, Double File Extension), T1583.006 (Acquire Infrastructure, Web Services), T1583.008 (Acquire Infrastructure, Malvertising), T1071.001 (Application Layer Protocol, Web Protocols), T1204.001 (User Execution, Malicious Link), and T1204.002 (User Execution, Malicious File). CWE-1021 (Improper Restriction of Rendered UI Layers) is associated with the UI deception component of lure delivery. Threat actors are unattributed organized TOAD call-center operators.

Action Checklist

1. Containment: Deploy email security rules to flag or quarantine inbound messages containing phone numbers matching sequential DID block patterns (e.g., numerically adjacent numbers across multiple messages) from external senders. Block PDF attachments from first-time or low-reputation senders pending review, as PDFs are a confirmed delivery format in this campaign.
2. Detection: Query email gateway logs and SIEM for messages referencing PayPal, Geek Squad, Best Buy, McAfee, or Norton LifeLock in subject or body combined with embedded phone numbers. Cross-reference phone numbers appearing in multiple messages against Cisco Talos telemetry. Monitor for user-reported callback calls to numbers that match the known CPaaS provider ranges (Sinch, Twilio, Bandwidth, RingCentral, NUSO, Verizon, Virtue). Behavioral indicator: a single phone number appearing in lure emails across more than one brand theme is a high-confidence signal of shared infrastructure.
3. Eradication: Submit confirmed DID numbers as IOCs to your email security platform and telephony abuse reporting channels. File abuse reports with the relevant CPaaS providers (Sinch abuse reporting, Twilio trust and safety, Bandwidth abuse) for identified numbers. Update email filtering rules to flag numerically sequential phone number clusters embedded in billing-alert or subscription-renewal lure templates.
4. Recovery: Validate that updated IOC feeds and email rules are actively blocking or flagging messages containing confirmed DID numbers. For any user who called a fraudulent number, treat the call as a potential credential or financial compromise event: initiate a user interview, check for unauthorized account access or wire transfer requests, and escalate to HR and finance if social engineering success is suspected.
5. Post-Incident: Document the phone number IOC detection gap in your email security tooling. Evaluate whether your current platform supports phone number extraction and reputation scoring from email body content; if not, treat this as a control gap for the next vendor review cycle. Add TOAD-specific scenarios to security awareness training, emphasizing that legitimate vendors (PayPal, Best Buy, McAfee, Norton) do not send unsolicited billing alerts requiring a callback to an embedded phone number.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to HR, Legal, and Finance if any victim user confirms they granted remote access, provided account credentials, initiated a wire transfer, or purchased gift cards during a fraudulent callback call, as these outcomes indicate completed social engineering and potential financial fraud requiring breach notification assessment under applicable state consumer protection and financial regulations.
Recovery Notes	After blocking confirmed DID numbers and validating email rules, monitor email gateway quarantine queues and user-reported phishing submissions daily for a minimum of 30 days, as Cisco Talos research indicates this campaign rotates DID blocks approximately every 14 days — newly provisioned sequential numbers from the same CPaaS providers will appear and require the detection and containment cycle to repeat. For any user confirmed to have called a fraudulent number, maintain elevated monitoring on their accounts (email, financial systems, VPN) for 90 days, as TOAD actors may sell verified victim contact data to secondary fraud operators. Verify with your CPaaS abuse contacts whether deprovisioned numbers have been reassigned, as reassigned numbers in your blocklist could generate false positives against legitimate future communications.
Forensic Artifacts	Email gateway message trace logs: raw EML files with full Received headers for all messages matching TOAD lure keywords (invoice, subscription, renewal, billing) combined with impersonated brand names — headers will reveal CPaaS relay infrastructure (Sinch, Twilio, Bandwidth, RingCentral, NUSO) in the Received chain, confirming VoIP provider attribution | Extracted phone number corpus: structured list of all E.164 numbers appearing in flagged messages, annotated with brand impersonation theme (PayPal, Geek Squad, McAfee, Norton LifeLock) and message date — sequential numerical adjacency across entries is the primary infrastructure fingerprint identified by Cisco Talos for this campaign | PDF attachment binaries: SHA-256 hashes and full binary copies of any PDF attachments delivered with lure messages — TOAD campaign PDFs typically contain embedded phone numbers in invoice or receipt templates; static analysis with pdfid.py or pdf-parser.py will reveal embedded URIs or JavaScript that may accompany the callback number | Endpoint process execution logs for victim machines: Windows Security Event ID 4688 or Sysmon Event ID 1 filtered for remote access tool execution (AnyDesk.exe, TeamViewer.exe, msra.exe) and any scripting engine invocations (powershell.exe, wscript.exe, mshta.exe) within the window of a reported fraudulent callback call — TOAD actors conducting fake support sessions frequently use these vectors | User helpdesk and phishing report submissions: verbatim text of all user-reported suspicious emails or calls referencing the impersonated brands, with submission timestamps — this corpus establishes the first-known-delivery date, measures the detection lag against email gateway telemetry, and may contain victim-observed phone numbers not yet present in external threat feeds

Per-Action IR Details

Containment — Deploy email security rules to flag or quarantine inbound messages containing phone numbers matching sequential DID block patterns (e.g., numerically adjacent numbers across multiple messages) from external senders. Block PDF attachments from first-time or low-reputation senders pending review, as PDFs are a confirmed delivery format in this campaign.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: execute IR plan, categorize, contain, and mitigate; CSF [RS] function

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST SI-10 (Information Input Validation), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 9.4 — Restrict Email-Based Attachment Delivery (IG2/IG3) — apply sender-reputation thresholds for PDF delivery from first-contact external senders

Compensating: Without an enterprise email gateway: use Microsoft Exchange transport rules (New-TransportRule in PowerShell) or Postfix header_checks with a regex matching E.164 phone number patterns (e.g., \+?1?[2-9]\d{9}) in message body. For PDF blocking, configure a milter (e.g., amavisd-new with ClamAV) to quarantine PDF attachments from senders with no prior delivery history. Maintain a local blocklist text file of confirmed DID numbers and update the regex weekly using a cron job that ingests the Cisco Talos threat feed CSV.

Evidence: Before deploying rules, capture: (1) raw EML headers of flagged messages — preserve the full Received chain to identify originating IP and CPaaS relay (look for Sinch, Twilio, Bandwidth, RingCentral, NUSO, Verizon, Virtue relay hostnames in Received headers); (2) embedded phone numbers extracted from message body and PDF attachments — document the full E.164 number, surrounding lure text (billing alert, subscription renewal), and impersonated brand (PayPal, Geek Squad, McAfee, Norton LifeLock); (3) sender envelope addresses and Reply-To headers, which in TOAD campaigns typically spoof legitimate brand domains while routing through disposable or lookalike domains; (4) PDF binary hash (SHA-256) of any attachment for IOC submission and detonation.

Detection — Query email gateway logs and SIEM for messages referencing PayPal, Geek Squad, Best Buy, McAfee, or Norton LifeLock in subject or body combined with embedded phone numbers. Cross-reference phone numbers appearing in multiple messages against Cisco Talos telemetry. Monitor for user-reported callback calls to numbers that match the known CPaaS provider ranges (Sinch, Twilio, Bandwidth, RingCentral, NUSO, Verizon, Virtue). Behavioral indicator: a single phone number appearing in lure emails across more than one brand theme is a high-confidence signal of shared infrastructure.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: correlate indicators, analyze adverse events, integrate CTI; CSF [DE] function — DE.AE-02, DE.AE-03, DE.AE-07

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM: run the following PowerShell one-liner against exported email gateway logs (CSV format) to surface multi-brand DID reuse — Import-Csv mail_log.csv | Where-Object { $_.Body -match '(PayPal|Geek Squad|McAfee|Norton)' -and $_.Body -match '\+?1?[2-9]\d{9}' } | Select-Object Sender, Subject, Body | Export-Csv toad_hits.csv. For cross-brand DID correlation without a SIEM, use a Python script with collections.Counter to identify phone numbers appearing in more than one brand-themed message across your log export. Subscribe to the free Cisco Talos threat intelligence blog RSS feed and manually cross-reference flagged numbers weekly. Use MXToolbox or similar free DNS/email header analyzers to identify CPaaS relay infrastructure in message headers.

Evidence: Before analyzing, collect and preserve: (1) email gateway message trace logs for the past 30 days filtered on subject keywords 'invoice', 'subscription', 'renewal', 'billing', 'alert' combined with impersonated brand names — TOAD lures consistently use subscription-expiry or billing-alert pretexts; (2) user helpdesk tickets or IT support emails reporting unexpected billing notifications or calls to support numbers — these are primary discovery vectors for TOAD campaigns since technical detection is often absent; (3) CPaaS provider ASN/IP ranges for Sinch (AS197157), Twilio (AS54208), Bandwidth (AS19624), and RingCentral — cross-reference outbound call records or VoIP logs if your organization operates a softphone or UCaaS platform; (4) any browser history or endpoint DNS query logs from users who may have visited a URL embedded alongside the callback number, as some TOAD lures include a landing page to reinforce legitimacy.

Eradication — Submit confirmed DID numbers as IOCs to your email security platform and telephony abuse reporting channels. File abuse reports with the relevant CPaaS providers (Sinch abuse reporting, Twilio trust and safety, Bandwidth abuse) for identified numbers. Update email filtering rules to flag numerically sequential phone number clusters embedded in billing-alert or subscription-renewal lure templates.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove threat from environment, verify eradication, notify external parties; CSF [RS] function

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, And Directives), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without an enterprise IOC management platform: maintain a plain-text IOC file (toad_dids.txt) versioned in a local Git repository, with one E.164 number per line. Use a bash cron job to diff the file daily and auto-push additions to your email gateway blocklist via API or config reload. For CPaaS abuse reporting without dedicated tooling, use the following direct channels: Twilio Trust & Safety at https://www.twilio.com/help/abuse (search-retrieved — validate before use); Bandwidth Abuse at abuse@bandwidth.com; Sinch Trust & Safety at trust@sinch.com (search-retrieved — validate before use). Document each submission with timestamp, number, campaign context, and confirmation receipt for audit purposes per NIST IR-6 (Incident Reporting).

Evidence: Before submitting IOCs and closing eradication, capture: (1) the complete sequential DID block pattern — document the numerical range (e.g., +1-800-XXX-0100 through +1-800-XXX-0120) to support abuse reports demonstrating organized provisioning rather than isolated misuse, which increases CPaaS provider response priority; (2) a mapping of which DID numbers were associated with which brand impersonation (PayPal vs. Geek Squad vs. McAfee vs. Norton LifeLock) and the approximate date range of use — Cisco Talos research indicates ~14-day rotation cycles, so date-stamp every number; (3) confirmation that all flagged messages have been removed from user mailboxes (for Exchange: Search-Mailbox or Purge-MailboxMessage targeting the identified sender domains and phone number strings); (4) CPaaS provider abuse report submission receipts or ticket numbers for chain-of-custody documentation.

Recovery — Validate that updated IOC feeds and email rules are actively blocking or flagging messages containing confirmed DID numbers. For any user who called a fraudulent number, treat the call as a potential credential or financial compromise event: initiate a user interview, check for unauthorized account access or wire transfer requests, and escalate to HR and finance if social engineering success is suspected.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: execute recovery plan, restore normal operations, verify integrity, communicate; CSF [RC] function

Controls: NIST IR-4 (Incident Handling), NIST IR-7 (Incident Response Assistance), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AC-2 (Account Management) — review and revoke any accounts or credentials disclosed during fraudulent call, CIS 6.2 (Establish an Access Revoking Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Without enterprise SIEM for rule validation: send a controlled test message containing a known-blocked DID number from an external account to an internal test mailbox and confirm quarantine behavior. For victim user interviews without a formal IR interviewing tool, use a structured question checklist: (1) Did the agent request remote access (AnyDesk, TeamViewer, Quick Assist)? (2) Did the agent request gift card purchase or wire transfer? (3) Were PayPal, bank, or subscription account credentials entered during or after the call? (4) Was any software downloaded or installed? Document responses verbatim. If remote access was granted, immediately isolate the endpoint and image it before any remediation — TOAD actors frequently install RATs or credential stealers during fake 'support' sessions.

Evidence: Before closing recovery: (1) review endpoint logs (Windows Event ID 4688 — Process Creation, or Sysmon Event ID 1) on any machine used by a victim who reported calling the fraudulent number, filtering for remote access tool execution (AnyDesk.exe, TeamViewer.exe, msra.exe for Quick Assist) within the call timeframe; (2) check Windows Event ID 4624 (Logon) and 4625 (Failed Logon) for anomalous authentication patterns on accounts belonging to victim users in the 24-hour window following the call; (3) review financial system access logs and wire transfer request queues for activity initiated by or on behalf of victim users — TOAD campaigns targeting PayPal and Norton impersonation frequently culminate in fraudulent refund transactions or gift card purchases; (4) verify email rule efficacy by querying email gateway delivery logs for any messages matching the blocked DID number patterns that were delivered post-rule-deployment.

Post-Incident — Document the phone number IOC detection gap in your email security tooling. Evaluate whether your current platform supports phone number extraction and reputation scoring from email body content; if not, treat this as a control gap for the next vendor review cycle. Add TOAD-specific scenarios to security awareness training, emphasizing that legitimate vendors (PayPal, Best Buy, McAfee, Norton) do not send unsolicited billing alerts requiring a callback to an embedded phone number.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned, update policies, improve detection, share intelligence; CSF [GV, ID] functions

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IR-2 (Incident Response Training), NIST IR-3 (Incident Response Testing), NIST SI-5 (Security Alerts, Advisories, And Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without a formal GRC platform to track control gaps: create a plain markdown or CSV gap register entry with fields: gap_id, date_identified, control_reference, description, current_state, target_state, owner, due_date. For TOAD-specific awareness training without an LMS, deliver a 10-minute tabletop scenario at the next all-hands or team meeting: present a realistic PayPal or Geek Squad billing-alert email with an embedded callback number and ask staff to identify the social engineering indicators. Document attendance. For ongoing phone number IOC detection without a commercial reputation service, evaluate the free PhoneInfoga tool (OSINT-based phone number reconnaissance) and integrate its output into your manual triage process for user-reported suspicious calls.

Evidence: For the lessons-learned record, preserve: (1) the full incident timeline from first user report through rule deployment, including lag time between initial delivery and detection — this gap measurement is the primary metric for the detection control gap finding; (2) a sample of 3-5 representative lure emails with headers intact (anonymized for user PII) to anchor the awareness training materials with real campaign artifacts rather than hypothetical examples; (3) CPaaS abuse report submission records and any provider responses, noting whether numbers were actually deprovisioned — this informs the effectiveness assessment of the telephony abuse reporting channel as a defensive action; (4) a count of users who received vs. users who reported the lure emails, to establish a baseline report rate for measuring training effectiveness in future TOAD campaign encounters.

Detection Guidance

Primary detection pivot is the phone number, not the URL or file hash. Extract all phone numbers from inbound email body content and PDFs at the email gateway or SIEM layer. Flag messages where: (1) the same phone number appears across multiple sender addresses or lure themes; (2) phone numbers are numerically sequential across a batch of inbound messages (indicating DID block provisioning); (3) lure themes match known TOAD brands, PayPal, Geek Squad/Best Buy, McAfee, Norton LifeLock, combined with billing-alert or subscription-renewal language. Cross-reference extracted numbers against Cisco Talos published IOC feeds. Monitor endpoint logs for users who received flagged emails and then placed outbound calls to the embedded numbers (correlate email timestamps with telephony logs if available). PDF attachments from first-time senders carrying phone numbers and billing-alert language should trigger analyst review. MITRE T1566.001 and T1566.002 detection rules in your SIEM are applicable starting points but will not surface the phone-number pivot without custom content extraction logic.

Indicators of Compromise

Type	Value	Context	Confidence
OTHER	`Sequential DID number blocks provisioned through Sinch, Twilio, Bandwidth, Virtue, RingCentral, Verizon, NUSO`	Phone numbers provisioned in numerically adjacent blocks through CPaaS providers; median active lifespan ~14 days per number before rotation; same numbers reused across PayPal, Geek Squad, McAfee, Norton LifeLock lure themes	HIGH

Type	Value	Context	Confidence
OTHER	`PDF attachments embedding callback phone numbers with billing-alert or subscription-renewal lure content`	Confirmed delivery format in Cisco Talos TOAD campaign analysis; cross-lure reuse of phone numbers across PDF and non-PDF attachment formats indicates shared backend	HIGH
OTHER	`Brand impersonation lure themes: PayPal billing fraud, Geek Squad renewal scams, McAfee subscription alerts, Norton LifeLock subscription alerts`	Confirmed lure themes per Cisco Talos telemetry; same infrastructure used across all four brand themes	HIGH

Framework Mappings

MITRE-ATTACK

- **T1071.001** — Web Protocols
- **T1566.001** — Spearphishing Attachment
- **T1598.002** — Spearphishing Attachment
- **T1656** — Impersonation
- **T1583.006** — Web Services
- **T1204.002** — Malicious File
- **T1598** — Phishing for Information
- **T1566.002** — Spearphishing Link
- **T1204.001** — Malicious Link
- **T1036.007** — Double File Extension
- **T1583.008** — Malvertising

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection

CIS-V8

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071.001	Web Protocols	Command-And-Control
T1566.001	Spearphishing Attachment	Initial-Access
T1598.002	Spearphishing Attachment	Reconnaissance
T1656	Impersonation	Defense-Evasion
T1583.006	Web Services	Resource-Development
T1204.002	Malicious File	Execution
T1598	Phishing for Information	Reconnaissance
T1566.002	Spearphishing Link	Initial-Access
T1204.001	Malicious Link	Execution
T1036.007	Double File Extension	Defense-Evasion
T1583.008	Malvertising	Resource-Development

Sources

Source	URL	Tier
Cisco Talos Blog	https://blog.talosintelligence.com/insights-into-the-clustering-and...	T3
	https://blog.talosintelligence.com/insights-into-the-clustering-and...	T3
	https://gbhackers.com/cybercrime-group-in-vietnam/	T3
	https://blog.talosintelligence.com/pdfs-portable-documents-or-perfe...	T3
We Identified Sinch AB as the Leading Enabler of Scam and ...	https://grizzlyreports.com/sinch/	T3

Generated 2026-05-07 06:37 UTC by TJS Security Command Center