INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 13:48 UTC

Phone Numbers as Trackable Infrastructure: How TOAD Campaigns Rotate, Recycle, and Evade Detection

THREAT CAMPAIGN | MEDIUM | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0279
Type	Threat Campaign
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	End users targeted via impersonation of PayPal, Geek Squad (Best Buy), McAfee, Norton LifeLock; VoIP/CPaaS providers abused: Sinch, Twilio, Bandwidth, RingCentral, Verizon, NUSO
Published	2026-05-06T10:00:12+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Cisco Talos research documents how scam call centers use phone numbers as rotating, reusable infrastructure to impersonate PayPal, Geek Squad, McAfee, and Norton LifeLock across email-delivered lure campaigns. Phone numbers persist for a median of 14 days, long enough to serve as durable tracking signals across multiple campaigns and brands. Organizations relying solely on email artifact detection are missing a cross-campaign IOC class that is actively exploited and largely absent from standard threat feeds.

Technical Analysis

Cisco Talos (research window February 26 to March 31, 2026) analyzed Telephone-Oriented Attack Delivery (TOAD) campaigns and identified phone numbers as semi-persistent infrastructure IOCs. Threat actors acquire sequential VoIP number blocks via CPaaS providers including Sinch, Twilio, Bandwidth, RingCentral, Verizon, and NUSO, then apply cool-down periods to evade reputation-based filtering before reactivating numbers across unrelated lure campaigns. Attachment formats include PDF, HEIC, and JPEG, expanding delivery surface beyond traditional document-based filtering. Median phone number lifespan: 14 days. Relevant MITRE ATT&CK techniques: T1566.001 (Spearphishing Attachment), T1566.002 (Spearphishing Link), T1583.008 (Acquire Infrastructure: Telephone Accounts), T1036.005 and T1036.007 (Masquerading), T1656 (Impersonation), T1598.002 and T1598.003 (Spearphishing for Information), T1204.002 (Malicious File).

CWE-184 (Incomplete List of Disallowed Inputs) and CWE-601 (URL Redirection to Untrusted Site) are referenced in classification. The primary detection gap is structural: phone numbers are not treated as first-class IOCs in standard SIEM ingestion pipelines or commercial threat feeds, leaving a durable, clusterable signal unmonitored.

Action Checklist

1. Step 1: Containment. Identify email gateways and SEGs in your stack and confirm whether phone number extraction from email body text is enabled. If not, configure message filtering to extract phone numbers and cross-reference them against TOAD-associated IOC lists. Block or quarantine messages containing sequential VoIP number clusters (e.g., +1-8XX-XXX-0001 through +1-8XX-XXX-0050 appearing in multiple campaigns within a 14-day window) pending analyst review.
2. Step 2: Detection. Query email logs for messages containing embedded phone numbers alongside impersonation lure keywords (PayPal, Geek Squad, McAfee, Norton LifeLock, subscription renewal, order confirmation). Search for HEIC and JPEG attachments delivered via email, as these formats bypass standard document-based filters. Correlate extracted phone numbers against the Cisco Talos blog IOC list (https://blog.talosintelligence.com/insights-into-the-clustering-and-reuse-of-phone-numbers-in-scam-emails/) for known number clusters.
3. Step 3: Eradication. Ingest phone number IOCs from the Cisco Talos research into your threat intelligence platform as first-class indicators alongside URL and hash IOCs. Configure your email security platform to extract and evaluate phone numbers from email body content. Add HEIC and JPEG to monitored attachment types if not already present.
4. Step 4: Recovery. Validate that phone number IOC ingestion is producing feed matches against incoming email traffic. Monitor for cool-down reactivation: numbers that appeared in prior campaigns going quiet for 7-14 days before re-emerging. Confirm VoIP provider abuse reports are being submitted to Sinch, Twilio, Bandwidth, RingCentral, Verizon, and NUSO via their abuse channels to accelerate number deactivation.
5. Step 5: Post-Incident. Document the detection gap this research exposed: phone numbers as unmonitored IOC class. Add phone number IOC ingestion as a formal requirement in your threat intel program. Review your email security vendor's roadmap for phone number extraction capability. Update phishing awareness training to include callback-scam mechanics, specifically that legitimate companies do not ask users to call numbers embedded in unsolicited emails.

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent if any user is confirmed to have called a TOAD-associated number and provided account credentials, payment card data, or remote access to a company-managed device, as this constitutes a social engineering breach with potential PII/financial data exposure triggering organizational breach notification assessment; also escalate if phone-number IOC feed matches against inbound traffic exceed 5 distinct numbers in a rolling 7-day window, indicating active targeting of your organization's user population.

Recovery Notes	Post-containment, maintain active monitoring of the ingested Talos phone-number IOC cluster for a minimum of 30 days given the documented 14-day cool-down reactivation cycle — a number going silent is not confirmation of deactivation. Verify with each relevant CPaaS provider (Sinch, Twilio, Bandwidth, RingCentral, Verizon, NUSO) that submitted abuse reports resulted in number deactivation, and re-add any reactivated numbers to the block list with updated first/last-seen timestamps. Confirm that HEIC and JPEG attachment monitoring is producing alerts and review the first two weeks of hits manually to tune for false positives before moving to automated quarantine.
Forensic Artifacts	Raw email files (.eml format) of delivered TOAD lures including full MIME structure — the image/heic or image/jpeg attachment part will contain a rendered invoice with the callback phone number as embedded text, bypassing text-extraction filters; preserve with `emlx` or `mbox` export before any remediation action | Email header `Received:` chain from all suspected lure messages — traces the originating CPaaS platform (Sinch, Twilio, Bandwidth, RingCentral, Verizon, or NUSO) via sending IP and HELO/EHLO domain, enabling provider-specific abuse reporting and infrastructure clustering consistent with Talos's sequential VoIP block methodology | SEG/MTA delivery logs for the 30-day window preceding detection, filtered for toll-free number regex patterns co-occurring with PayPal/Geek Squad/McAfee/Norton LifeLock keyword hits — establishes the full exposure window and identifies any users who received lures before controls were in place | EXIF metadata extracted from HEIC and JPEG attachments using `exiftool` — creation timestamps, software version, and GPS fields inconsistent with a legitimate corporate invoice are secondary indicators of lure fabrication and can corroborate campaign clustering | Time-series log of phone number first-seen and last-seen dates extracted from your email traffic, correlated against the Talos IOC cluster list — the 14-day median persistence and 7-14 day cool-down reactivation pattern documented by Talos, if replicated in your own logs, constitutes evidence of systematic infrastructure reuse and supports escalation of the threat classification

Per-Action IR Details

Step 1: Containment — Identify email gateways and SEGs in your stack and confirm whether phone number extraction from email body text is enabled. If not, block or quarantine messages containing known TOAD-associated number patterns (sequential VoIP blocks, +1 800/888/877/866 ranges appearing in invoice-style lures) pending analyst review.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST SI-10 (Information Input Validation), CIS 9.3 (Maintain and Enforce Network-Based URL Filters) — applied here to email body content pattern filtering as the closest IG1 analog for blocking lure delivery vectors, CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without enterprise SEG policy engines: deploy a Python script using the `imaplib` and `re` libraries to scan mailbox inboxes for regex patterns matching toll-free number formats (`\+?1[-\s]?(800|888|877|866|855|844|833)[-\s]?\d{3}[-\s]?\d{4}`) co-occurring with keywords like 'PayPal', 'Geek Squad', 'McAfee', 'Norton', 'subscription renewal', or 'order confirmation'. Quarantine matching messages to a review folder. Sample regex: `r'(?i)(paypal|geek.?squad|mcafee|norton).{0,300}\+?1[-.\s]?(800|888|877|866)'`. This is achievable with Python 3 standard libraries by a 2-person team in under two hours.

Evidence: Before reconfiguring SEG rules, export and preserve: (1) the current SEG policy configuration and any existing phone-number-related filter rules to document the detection gap baseline; (2) the raw email headers and body content of any already-delivered TOAD-pattern messages in quarantine or inbox, including X-Originating-IP, Return-Path, and Message-ID headers which will anchor the lure-to-infrastructure cluster; (3) delivery timestamps correlated against Cisco Talos's documented 14-day median number persistence window to identify whether any

numbers already received are still active. Do not alter mailbox state before preservation.

Step 2: Detection — Query email logs for messages containing embedded phone numbers alongside impersonation lure keywords (PayPal, Geek Squad, McAfee, Norton LifeLock, subscription renewal, order confirmation). Search for HEIC and JPEG attachments delivered via email, as these formats bypass standard document-based filters. Correlate against the Cisco Talos blog IOC list (https://blog.talosintelligence.com/insights-into-the-clustering-and-reuse-of-phone-numbers-in-scam-emails/) for known number clusters.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-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: use Microsoft 365 Compliance Center Message Trace (or Exchange Online PowerShell `Get-MessageTrace`) filtered by sender domain reputation and subject-line keywords. For on-prem Exchange or open-source MTA: parse MTA logs with `grep -E '(paypal|geek.?squad|mcafee|norton|renewal|order.?confirm)' /var/log/maillog` and pipe through a secondary `grep` for toll-free number patterns. For HEIC/JPEG attachment hunting: `grep -i 'Content-Type: image/heic\|Content-Type: image/jpeg' /var/log/maillog` or use `find /path/to/quarantine -name '*.heic' -o -name '*.jpg'` against your mail quarantine directory. Cross-reference extracted numbers against the Talos IOC list manually using a spreadsheet VLOOKUP or a simple Python `set.intersection()` comparison — this is a 1-hour task for one analyst.

Evidence: Preserve before querying: (1) raw HEIC and JPEG attachment files from suspected lure emails — these image-based invoices contain the callback number rendered as text-in-image to evade OCR-less filters, and the image EXIF metadata (tool: `exiftool`) may reveal creation timestamps inconsistent with the purported sender; (2) full email header chains including all `Received:` hops to trace the originating CPaaS infrastructure (Sinch, Twilio, Bandwidth, RingCentral, Verizon, or NUSO sending domains); (3) SEG/MTA delivery logs with timestamps for all messages matching lure keywords, preserving the original message-IDs for chain-of-custody; (4) a snapshot of your current TIP/threat intel platform's phone-number IOC coverage (likely empty) to document the detection gap at time of analysis.

Step 3: Eradication — Ingest phone number IOCs from the Cisco Talos research into your threat intelligence platform as first-class indicators alongside URL and hash IOCs. Configure your email security platform to extract and evaluate phone numbers from email body content. Add HEIC and JPEG to monitored attachment types if not already present.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IR-4 (Incident Handling), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without a commercial TIP: create a structured phone-number IOC list in MISP (free, open-source) using the `phone-number` object type, or maintain a flat CSV with columns: number, first_seen, last_seen, associated_brand, source (Talos), campaign_cluster. Automate daily comparison against inbound email logs using a cron job running the Python `re` + `csv` pattern above. For HEIC/JPEG monitoring without enterprise DLP: configure a Postfix `content_filter` or `milter` hook to invoke a shell script that runs `file --mime-type` on all attachments and rejects or flags `image/heic` and `image/jpeg` types arriving from external senders with invoice-style subjects. YARA rule targeting toll-free number strings co-located with impersonation brand keywords within image-bearing email MIME parts can be deployed via `yara-python` as a milter.

Evidence: Before modifying SEG attachment policies or TIP configurations, document and preserve: (1) the pre-change SEG attachment filter policy configuration (screenshot or exported config) to establish a change baseline for audit purposes under NIST AU-9 (Protection of Audit Information); (2) a deduplicated list of all phone numbers already observed in delivered lure emails in your environment, timestamped, to seed your TIP and establish your

organization's specific exposure window relative to the Talos 14-day median persistence figure; (3) confirmation of which CPaaS providers (Sinch, Twilio, Bandwidth, RingCentral, Verizon, NUSO) appear in the originating infrastructure of messages already delivered, as this determines which abuse reporting channels are relevant in Step 4.

Step 4: Recovery — Validate that phone number IOC ingestion is producing feed matches against incoming email traffic. Monitor for cool-down reactivation: numbers that appeared in prior campaigns going quiet for 7-14 days before re-emerging. Confirm VoIP provider abuse reports are being submitted to Sinch, Twilio, Bandwidth, RingCentral, Verizon, and NUSO via their abuse channels to accelerate number deactivation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST IR-6 (Incident Reporting), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Without automated feed-match alerting: implement a daily cron job that diffs your phone-number IOC list against the previous 24 hours of parsed email logs and emails a summary to the security team — flag any number appearing for the first time or reappearing after a gap of 7 or more days (the Talos-documented cool-down window). For abuse reporting without a ticketing system: maintain a tracking spreadsheet with columns: number, provider, abuse_email (Twilio: abuse@twilio.com; Sinch: abuse@sinch.com; Bandwidth: abuse@bandwidth.com; RingCentral: trust@ringcentral.com), date_reported, date_confirmed_deactivated. Submit abuse reports within 24 hours of IOC confirmation. Use `whois` or the FCC's number lookup tools to confirm CPaaS provider attribution before routing reports.

Evidence: During recovery validation, collect and retain: (1) feed-match hit logs from your TIP or cron-based comparison tool showing which ingested Talos phone-number IOCs triggered on inbound traffic and on what dates — this validates detection coverage and documents dwell time; (2) VoIP provider abuse submission confirmations (email receipts or ticket numbers) as evidence of third-party coordination per NIST IR-6 (Incident Reporting) and NIST 800-61r3 §3.5; (3) a time-series log of any numbers that reappear after a 7-14 day silence window, which Talos identifies as a characteristic cool-down reactivation behavior — this pattern, if observed in your own traffic, constitutes evidence of targeted reuse against your user population specifically.

Step 5: Post-Incident — Document the detection gap this research exposed: phone numbers as unmonitored IOC class. Add phone number IOC ingestion as a formal requirement in your threat intel program. Review your email security vendor's roadmap for phone number extraction capability. Update phishing awareness training to include callback-scam mechanics, specifically that legitimate companies do not ask users to call numbers embedded in unsolicited emails.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IR-2 (Incident Response Training), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AU-2 (Event Logging), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Without a formal TIP or security awareness platform: document the detection gap in a one-page after-action memo that includes: (a) the IOC class previously uncovered (phone numbers), (b) the Talos-documented 14-day persistence and cool-down reactivation behavior that makes this class durable and cross-campaign, (c) the specific brands impersonated (PayPal, Geek Squad, McAfee, Norton LifeLock) and attachment types abused (HEIC, JPEG). For training, add a single slide to your existing phishing awareness deck showing a real-format TOAD lure invoice with the callback number highlighted and the caption: 'PayPal, Geek Squad, McAfee, and Norton LifeLock do not ask you to call a number embedded in an unsolicited email — this is always a scam.' Distribute via email to all staff within 30 days and log completion under NIST IR-2 (Incident Response Training).

Evidence: Post-incident documentation package should include and preserve: (1) the full after-action report referencing the Cisco Talos research as the triggering intelligence source, the specific detection gap identified (phone-number IOC class absent from TIP and SEG policy), and the timeline from Talos publication to your organization's detection capability being operational — this gap duration is a program maturity metric; (2) the pre- and

post-change SEG policy configurations showing HEIC/JPEG attachment monitoring and phone-number extraction additions as evidence of control improvement; (3) records of all user reports (if any) of suspected TOAD-style callback scam emails received before detection controls were in place, which may indicate whether any users interacted with scammer infrastructure and require follow-up social engineering exposure assessment.

Detection Guidance

Primary signal: email messages containing embedded phone numbers combined with impersonation lure content (subscription renewal, order confirmation, refund notice) referencing PayPal, Geek Squad, McAfee, or Norton LifeLock. Secondary signals: HEIC or JPEG attachments in unsolicited email, which bypass document-type filters. Phone number clustering: sequential VoIP number blocks (e.g., +1-8XX-XXX-0001 through 0050) appearing across multiple sender addresses or campaigns within a 14-day window indicate infrastructure reuse. Use regex pattern \+?1?[\s.-]?\(?[2-9]\d{2}\)?[\s.-]?\d{3}[\s.-]?\d{4} as a first-pass extraction rule. Apply secondary correlation with impersonation lure keywords to reduce false positives. Cross-reference extracted numbers against the Cisco Talos campaign IOC list. Behavioral indicator: a user who called a number embedded in a lure email and was asked to install remote access software or provide payment should be treated as an active TOAD incident. SIEM teams should build a parsing rule to extract phone numbers from email body fields and feed them to a reputation lookup or watchlist.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://blog.talosintelligence.com/insights-into-the-clustering-and-reuse-of-phone-numbers-in-scam-emails/`	Cisco Talos primary research post; contains campaign IOC list including known TOAD phone number clusters	HIGH
DOMAIN	`VoIP number blocks via Sinch, Twilio, Bandwidth, RingCentral, Verizon, NUSO (sequential +1 8XX ranges)`	CPaaS providers abused for number acquisition; specific number values in Talos IOC list	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1566.001** — Spearphishing Attachment
- **T1583.008** — Malvertising
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1656** — Impersonation
- **T1566.002** — Spearphishing Link
- **T1598.003** — Spearphishing Link
- **T1204.002** — Malicious File
- **T1598.002** — Spearphishing Attachment

- **T1036.007** — Double File Extension

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

- **8.2** — Collect Audit Logs

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.001	Spearphishing Attachment	Initial-Access
T1583.008	Malvertising	Resource-Development
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1656	Impersonation	Defense-Evasion
T1566.002	Spearphishing Link	Initial-Access
T1598.003	Spearphishing Link	Reconnaissance
T1204.002	Malicious File	Execution
T1598.002	Spearphishing Attachment	Reconnaissance
T1036.007	Double File Extension	Defense-Evasion

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

Source	URL	Tier
New FTC Data Shed Light on Companies Most Frequently ...	https://www.ftc.gov/news-events/news/press-releases/2024/05/new-ftc...	T1

Generated 2026-05-06 13:48 UTC by TJS Security Command Center