INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-26 06:31 UTC

Trusted Shopping App Weaponized for Callback Phishing, 50M Users at Risk from Fake Receipt Injection

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0575
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Shopify Shop app (iOS, Android); impersonated brands: Norton, McAfee, Apple, PayPal
Published	2026-06-25T15:45:48
Discovery Source	Rss

Executive Summary

Threat actors are injecting fraudulent purchase receipts into Shopify's Shop order-tracking app, a platform with 50 million installs on Google Play, to run callback phishing campaigns that harvest credentials, payment cards, and one-time passwords. The attack operates entirely within a trusted, authenticated mobile application, bypassing email security controls and exploiting the implicit trust users place in the app's order history. Organizations with BYOD policies or consumer-facing employees face elevated risk, as successful attacks can result in compromised accounts, unauthorized financial transactions, and remote access tool installation on personal devices that may also access corporate resources.

Technical Analysis

This campaign exploits Shopify's Shop order-tracking app (iOS and Android) to deliver TOAD (Telephone-Oriented Attack Delivery) phishing. Fraudulent order notifications appear within victims' legitimate, authenticated app sessions, the injection mechanism has not been publicly confirmed, creating significant defensive opacity. Upon seeing a fake receipt, victims are directed to call fraudulent support numbers impersonating Norton, McAfee, Apple, or PayPal. Attackers then harvest credentials, OTPs, and payment card data, or socially engineer victims into installing remote access tools (RATs). Relevant CWEs: CWE-287 (Improper Authentication, OTP and credential harvesting at the callback stage) and CWE-1021 (Improper Restriction of Rendered UI Layers, trust exploitation via the legitimate app surface). MITRE ATT&CK techniques include T1566.004 (Phishing: Spearphishing Voice / Vishing), T1598 (Phishing for Information), T1219 (Remote Access Software), T1056.001 (Input Capture: Keylogging via RAT), T1078 (Valid Accounts), T1204.002 (User

Execution: Malicious File), and T1539 (Steal Web Session Cookie). No CVE is assigned; no vendor-confirmed patch or remediation guidance has been published as of the reporting date. Sources are T3-tier community and news reporting; no vendor advisory confirmed.

Action Checklist

1. Containment: Issue immediate user awareness guidance to employees: do not call any phone number found in a Shop app order notification for orders not personally placed. Block known fraudulent callback numbers at telephony controls if your organization operates a corporate phone system or unified communications platform with call filtering capabilities.
2. Detection: Review mobile device management (MDM) logs for unapproved remote access tool installations (e.g., AnyDesk, TeamViewer, or similar) on BYOD or corporate devices enrolled in your MDM solution. Correlate against AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs): check authentication logs for anomalous OTP consumption, account takeover attempts, or credential reuse events following any reported user callback phone calls. No specific IOC signatures are confirmed from available T3 sources.
3. Eradication: No vendor-issued patch or configuration fix is available as of the reporting date; the receipt injection mechanism has not been publicly confirmed by Shopify. Eradication at the enterprise level requires preventing the attack outcome: enforce MFA for all corporate and externally-exposed applications per CIS 6.3 and CIS 6.5 to limit the value of harvested OTPs. Apply NIST AC-6 (Least Privilege) to limit what a compromised account can access. Remove any RATs discovered during detection review using your standard endpoint remediation process.
4. Recovery: Validate that no corporate credentials were reused on personal devices running the Shop app. Force re-authentication on accounts where anomalous OTP activity was detected. Confirm no unauthorized remote access sessions remain active by auditing remote access tool logs and active sessions per NIST AC-17 (Remote Access). Monitor authentication events for 30 days post-investigation for signs of lingering account compromise.
5. Post-Incident: This campaign exposes the control gap between enterprise email phishing defenses and mobile application trust surfaces. Conduct a BYOD risk review: assess which corporate systems are accessible from personal devices running consumer shopping applications. Document findings and update security awareness training to include mobile application phishing and callback-based social engineering, specifically TOAD-style attacks. Map improvements to NIST IR controls and CIS 7.1 (Establish and Maintain a Vulnerability Management Process) to ensure mobile threat vectors are included in your ongoing risk assessment cycle.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal and privacy counsel if any employee confirms they verbally provided corporate credentials, OTPs, or payment card data during a callback call, or if MDM logs confirm an active RAT session was established on a device with access to systems containing PII, PHI, or PCI-scoped data, as this may trigger breach notification obligations under GDPR, CCPA, HIPAA, or PCI DSS §12.10.

Recovery Notes	After forcing re-authentication on affected accounts, validate recovery by confirming zero active sessions originating from IPs associated with known AnyDesk or TeamViewer relay infrastructure in your IdP logs, and verify no new RAT installations appear in MDM app inventory exports over the following 72 hours. Monitor all accounts that reported a callback interaction for anomalous authentication events — particularly MFA bypass attempts, new device registrations, and impossible-travel sign-ins — for a minimum of 30 days, as harvested credentials may be used in delayed account takeover attempts after initial scrutiny subsides. Update your BYOD acceptable-use policy to explicitly address consumer mobile application trust surfaces (including order-tracking apps such as Shopify Shop) and the risks of callback-based social engineering before closing the incident.
Forensic Artifacts	Shopify Shop app push notification metadata and in-app order history entries on affected employee devices — these contain the fraudulent order IDs, injected merchant names (impersonating Norton, McAfee, Apple, or PayPal), and embedded callback phone numbers that are the primary IOCs for this campaign | Corporate telephony CDRs or UCaaS call logs (e.g., Microsoft Teams PSTN call records, RingCentral logs) showing outbound calls from employee extensions to phone numbers embedded in fraudulent Shop app receipts — timestamps correlate directly to the social engineering window during which OTPs or credentials may have been disclosed | AnyDesk session trace log at %AppData%\AnyDesk\ad.trace (Windows) or equivalent Android app data, containing attacker-controlled AnyDesk Client IDs and session timestamps if a RAT was installed during the callback call — the Client ID can be submitted to AnyDesk's abuse team for attribution data | IdP authentication logs (Azure AD sign-in logs or Okta System Log) filtered for MFA challenge and OTP submission events in the 0–60 minute window following a reported callback call — anomalous OTP consumption (multiple MFA prompts in rapid succession, or MFA completion from a different IP than the device baseline) indicates successful OTP harvesting during the voice call | MDM application inventory snapshots showing installation timestamps for AnyDesk, TeamViewer, RustDesk, or similar remote access tools on enrolled devices, cross-referenced against the time of any reported callback interaction to establish whether RAT installation was directed during the social engineering call

Per-Action IR Details

Containment — Issue immediate user awareness guidance to employees: do not call any phone number found in a Shop app order notification for orders not personally placed. Block known fraudulent callback numbers at telephony controls if your organization operates a corporate phone system or unified communications platform with call filtering capabilities.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For teams without enterprise telephony controls: publish an internal advisory (email, Slack, Teams) with a screenshot of what a fraudulent Shop app receipt looks like, explicitly naming the impersonated brands (Norton, McAfee, Apple, PayPal) and instructing users to report any callback attempt to the security team. For unified communications platforms running on-prem (e.g., FreePBX, Asterisk), create an outbound call block list using a dialplan deny rule for any number identified in threat feeds. Use OSINT lookups (e.g., 800notes.com or TrueCaller) to cross-reference numbers reported by employees against known callback phishing registries.

Evidence: Before issuing communications or blocking numbers, capture: (1) any Shop app order notification screenshots or push notification metadata reported by employees, noting the fraudulent order IDs and embedded phone numbers; (2) corporate telephony call detail records (CDRs) showing any outbound calls placed by employees to numbers matching known fraudulent callback patterns; (3) mobile MDM enrollment records identifying which enrolled devices have the Shopify Shop app installed. This step does not alter live host state but CDR snapshots

should be preserved before carrier log retention windows expire (typically 30–90 days depending on carrier).

Detection — Review mobile device management (MDM) logs for unapproved remote access tool installations (e.g., AnyDesk, TeamViewer, or similar) on BYOD or corporate devices enrolled in your MDM solution. Correlate against AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs): check authentication logs for anomalous OTP consumption, account takeover attempts, or credential reuse events following any reported user callback phone calls. No specific IOC signatures are confirmed from available T3 sources.

NIST Phase: Detection Analysis

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

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

Compensating: Without SIEM: (1) Query MDM console (Jamf, Intune, or equivalent) for app inventory using bulk device report exports — filter installed app names containing 'AnyDesk', 'TeamViewer', 'AnyDesk', 'RustDesk', 'Zoho Assist', or 'SupRemo' on all enrolled iOS and Android devices. (2) For identity logs, pull Azure AD or Okta sign-in logs via CLI: in Azure AD use `az monitor activity-log list --filters 'status eq Failed'` filtered to the 24–72 hour window following any reported callback calls, looking for MFA challenge spikes or OTP submission events from new or unexpected geolocations. (3) On Android BYOD devices with ADB access, run `adb shell pm list packages` and diff against a known-good baseline to surface newly installed packages. For iOS, rely on MDM app inventory reports since direct package inspection is not available.

Evidence: Volatile evidence to capture BEFORE any account lockout or session revocation actions that may follow detection: (1) Live authentication session tokens and active session listings from your IdP (Azure AD: `Get-AzureADAuditSignInLogs`; Okta: Admin console Sessions export) — these are invalidated upon forced logout; (2) MDM app inventory snapshot for all enrolled devices at point-in-time, as app state changes if the user uninstalls the RAT; (3) Any AnyDesk or TeamViewer session ID logs on the endpoint — on Windows, AnyDesk logs reside at `%AppData%\AnyDesk\ad.trace` and TeamViewer logs at `%ProgramFiles%\TeamViewer\TeamViewer15_Logfile.log`; on Android, RAT session artifacts may appear in `/data/data//files/` if device is rooted or MDM provides app data access; (4) Outbound network connection logs from MDM or endpoint showing connections to AnyDesk relay infrastructure (typically *.anydesk.com on TCP 7070 or 443) or TeamViewer relay servers (*.teamviewer.com on TCP 5938).

Eradication — No vendor-issued patch or configuration fix is available as of the reporting date; the receipt injection mechanism has not been publicly confirmed by Shopify. Eradication at the enterprise level requires preventing the attack outcome: enforce MFA for all corporate and externally-exposed applications per CIS 6.3 and CIS 6.5 to limit the value of harvested OTPs. Apply NIST AC-6 (Least Privilege) to limit what a compromised account can access. Remove any RATs discovered during detection review using your standard endpoint remediation process.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For RAT removal on BYOD Android devices without enterprise MDM wipe capability: instruct users to navigate to Settings > Apps > [AnyDesk/TeamViewer] > Uninstall, then verify removal by re-running `adb shell pm list packages` if ADB access is available. On Windows endpoints where a RAT was installed during a callback session, run `sc query` and `Get-Service` to identify and stop any installed RAT service, then use `reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` and `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` to remove persistence entries. For MFA enforcement without a commercial IdP: enable built-in MFA on Microsoft 365 via the admin portal (Security Defaults or per-user MFA) at no additional cost — this limits OTP harvest value even if a user was socially engineered into reading an OTP aloud during a callback call.

Evidence: Volatile evidence to capture BEFORE removing RATs or rotating credentials: (1) Full memory acquisition from any Windows endpoint on which a RAT was confirmed active during a callback session — use Magnet RAM

Capture (free) or WinPmem before terminating processes, as the attacker's active session state, injected code, and any credentials passed through the RAT channel exist only in live memory; (2) Run `Get-NetTCPConnection | Where-Object {$_.State -eq 'Established'}` and `netstat -ano` on Windows to capture active remote access connections before the RAT process is killed — record the remote IP, port, and owning PID; (3) Export AnyDesk session log (`ad.trace`) and TeamViewer connection log before uninstallation to preserve attacker-controlled relay node identifiers and session timestamps; (4) Screenshot or export the RAT's internal connection history if the UI is accessible, as session IDs may be traceable to the threat actor's device.

Recovery — Validate that no corporate credentials were reused on personal devices running the Shop app. Force re-authentication on accounts where anomalous OTP activity was detected. Confirm no unauthorized remote access sessions remain active by auditing remote access tool logs and active sessions per NIST AC-17 (Remote Access). Monitor authentication events for 30 days post-investigation for signs of lingering account compromise.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-17 (Remote Access), NIST AC-12 (Session Termination), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without a commercial PAM or SSO platform: (1) For Microsoft 365 environments, force token revocation for affected accounts using `Revoke-AzureADUserAllRefreshToken -ObjectId ` in PowerShell — this invalidates all active sessions including any the attacker may be maintaining post-callback; (2) For credential reuse validation on personal devices, issue a self-attestation survey to employees asking them to confirm whether their corporate email/password combination is also used on their personal Shopify Shop account or associated email — pair this with a HaveIBeenPwned Enterprise API check against corporate email domains if budget allows (free tier available); (3) For 30-day monitoring without SIEM, set up a recurring weekly export of Azure AD or Okta risky sign-ins reports and assign a team member to review for new anonymous proxy, unfamiliar location, or impossible travel flags tied to accounts involved in this incident.

Evidence: Volatile evidence to capture BEFORE forcing re-authentication or revoking sessions: (1) Export all active session listings from the IdP (Azure AD active sessions, Okta session management) showing current session origin IPs, device fingerprints, and session age — once revocation runs, this data is no longer queryable in its live state; (2) Capture authentication log exports covering the period from the earliest reported callback call to present, specifically filtering for OTP submission events (Azure AD: sign-in logs with authentication detail 'MFA completed' or 'MFA denied'), which establish the timeline of OTP harvesting attempts; (3) For any account flagged for anomalous OTP activity, export the full sign-in history before credential rotation to preserve the forensic baseline — password resets may trigger log truncation in some IdP configurations.

Post-Incident — This campaign exposes the control gap between enterprise email phishing defenses and mobile application trust surfaces. Conduct a BYOD risk review: assess which corporate systems are accessible from personal devices running consumer shopping applications. Document findings and update security awareness training to include mobile application phishing and callback-based social engineering, specifically TOAD-style attacks. Map improvements to NIST IR controls and CIS 7.1 (Establish and Maintain a Vulnerability Management Process) to ensure mobile threat vectors are included in your ongoing risk assessment cycle.

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), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: For a 2-person team conducting the BYOD risk review without a dedicated GRC platform: (1) Create a simple asset-to-access matrix in a spreadsheet listing all corporate SaaS applications (M365, Salesforce, HR systems, etc.) and mark which are accessible via mobile browser or native app on personal devices — cross-reference against MDM enrollment gaps to identify unmanaged access paths; (2) Draft a one-page TOAD (Telephone-Oriented Attack Delivery) awareness brief using this campaign as the concrete example — specifically reference the Shopify Shop app

(50M installs), the impersonated brands (Norton, McAfee, Apple, PayPal), and the fake receipt injection mechanism — distribute via internal email and pin in team communication channels; (3) Add a mobile application phishing scenario to the next tabletop exercise, simulating a user receiving a fraudulent Shop app receipt notification and calling the embedded callback number, to test whether employees apply the awareness guidance under simulated social pressure.

Evidence: No live volatile evidence capture is required for this post-incident phase. Preserve for lessons-learned documentation: (1) All CDRs and MDM log exports gathered during detection and containment phases, retained per your AU-11 (Audit Record Retention) policy; (2) IdP sign-in log exports covering the full incident window, archived to read-only storage before retention window expiration; (3) A written timeline of the incident from first employee report through recovery validation, noting any detection gaps attributable to the mobile/non-email attack surface — this gap analysis is the primary deliverable for updating the BYOD policy and vulnerability management scope.

Detection Guidance

No confirmed network-layer IOCs (IPs, domains, hashes) are available from current T3 sources. Detection must focus on behavioral indicators. Monitor MDM and endpoint logs for installation of unsanctioned remote access software (AnyDesk, TeamViewer, UltraViewer, or similar) on devices enrolled in your program, align with CIS 8.2 (Collect Audit Logs). Review identity provider and SSO logs for OTP exhaustion patterns, rapid sequential authentication attempts, or account access from unexpected geolocations following any user-reported callback phone calls. Alert on NIST AU-6 (Audit Record Review, Analysis, and Reporting) triggers for anomalous authentication behavior. In SIEM, build correlation rules: (1) OTP accepted AND new device enrollment within the same session window; (2) RAT binary execution on a mobile-connected device within 24 hours of a user support call. User self-reporting is currently the highest-confidence detection signal, establish a clear, low-friction internal reporting path for employees who receive unexpected Shop app order notifications. D3FEND countermeasures applicable: D3-LAM (Local Account Monitoring) to detect unauthorized account activity, D3-MFA (Multi-factor Authentication) to reduce OTP harvest value, D3-UAP (User Account Permissions) to limit blast radius of compromised credentials.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1056** — Input Capture
- **T1598** — Phishing for Information
- **T1056.001** — Keylogging
- **T1566** — Phishing
- **T1566.004** — Spearphishing Voice
- **T1204** — User Execution
- **T1219** — Remote Access Tools
- **T1539** — Steal Web Session Cookie
- **T1204.002** — Malicious File

NIST-800-53R5

- **AC-2** — Account Management

- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1056	Input Capture	Collection
T1598	Phishing for Information	Reconnaissance
T1056.001	Keylogging	Collection
T1566	Phishing	Initial-Access

Technique ID	Technique Name	Tactic
T1566.004	Spearphishing Voice	Initial-Access
T1204	User Execution	Execution
T1219	Remote Access Tools	Command-And-Control
T1539	Steal Web Session Cookie	Credential-Access
T1204.002	Malicious File	Execution

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/order-tracking-app-s...	T3
Notification from the Shop (shopify) app of a purchase that I didn't ...	https://www.reddit.com/r/phishing/comments/1rr6qpt/notification_fro...	T3
The "Fake Shopify Notification" Scam Exposed - YouTube	https://www.youtube.com/watch?v=fB-W4K-7Kq0&vl=en	T3
Shopify Shop app users are seeing fake orders in purchase histories	https://cyberinsider.com/shopify-shop-app-users-are-seeing-fake-ord...	T3
Shopify security breach affects user's account - Facebook	https://www.facebook.com/groups/1911124516629079/posts/2091943931579...	T3

Generated 2026-06-26 06:31 UTC by TJS Security Command Center