INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-02 06:45 UTC

AccountDumpling: Vietnamese Phishing Ring Abuses Trusted Platforms to Harvest 30,000 Facebook Business Accounts

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0259
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Facebook Business accounts; abused delivery/hosting platforms: Google AppSheet, Netlify, Vercel, Google Drive, Canva, Telegram
Published	2026-05-01T14:09:00
Discovery Source	Rss

Executive Summary

A Vietnamese-linked threat group called AccountDumpling has compromised approximately 30,000 Facebook Business accounts by routing phishing emails through Google AppSheet's legitimate infrastructure, bypassing standard spam filters. The operation captures both passwords and two-factor authentication codes, then locks victims out and resells account access through an attacker-controlled storefront. Organizations using Facebook Business accounts for advertising, customer engagement, or revenue generation face direct financial loss and brand exposure if accounts are seized and their advertising credit is drained or audience data is sold.

Technical Analysis

AccountDumpling executes a multi-stage living-off-trusted-sites (LOTS) credential theft pipeline with no associated CVE. The attack chain exploits trust relationships rather than unpatched software. Delivery: phishing emails originate from Google AppSheet's legitimate email-sending infrastructure, defeating sender-reputation-based spam filters. Hosting: credential-harvesting pages are staged on Netlify, Vercel, Google Drive, and Canva, all high-reputation domains that bypass URL reputation controls. Collection: the harvesting pages capture both passwords and TOTP/SMS-based 2FA codes (CWE-287, improper authentication; CWE-1021, UI redress/overlay enabling credential interception). Exfiltration and resale: captured credentials are exfiltrated via Telegram channels and resold through an attacker-operated storefront, constituting a full commercial theft-to-resale pipeline (CWE-359, exposure of private information). MITRE

coverage: T1566.002 (spearphishing via link), T1598.003 (spearphishing for information via service), T1056.003 (web portal capture), T1539 (steal web session cookie), T1114 (email collection), T1071.001 (web protocols for C2), T1567 (exfiltration over web service), T1583.006 (acquire web services), T1608.005 (stage capabilities via link target), T1585.001 (establish social media accounts), T1078 (valid accounts). No patch exists; the attack exploits platform trust, not a vulnerability. Remediation centers on authentication hardening, user awareness, and platform-level abuse reporting.

Action Checklist

1. Containment: Audit all Facebook Business Manager accounts your organization owns: verify authorized administrators, remove unrecognized users, and revoke any third-party app permissions not explicitly sanctioned. If compromise is suspected, immediately use Facebook's Remove Account Access controls in Business Manager settings and report to Meta Business Support.
2. Detection: Review email gateway logs for messages originating from appsheet.com or *.appsheet.com that contain links to netlify.app, vercel.app, drive.google.com, or canva.com landing pages not provisioned by your organization. Query SIEM for login events to Facebook Business Manager from unexpected geolocations or IP ranges, particularly originating from Vietnam (VN) or anonymizing infrastructure. Look for session token reuse from new devices following credential entry.
3. Eradication: Enforce phishing-resistant MFA (FIDO2/hardware security keys) on all Facebook Business Manager accounts; SMS and TOTP-based 2FA is defeated by this campaign's real-time relay harvesting. Remove any harvesting page URLs identified from organization-controlled DNS blocklists and proxy/CASB deny lists. Report abusive infrastructure to Netlify, Vercel, and Google via their abuse reporting channels to accelerate takedown.
4. Recovery: After credential reset and MFA re-enrollment, verify that no unauthorized ad campaigns, payment method changes, or audience data exports occurred within the compromise window. Restore any modified Business Manager settings to known-good configurations. Enable Meta's login alerts and trusted device controls for all Business Manager users.
5. Post-Incident: This campaign exposed a control gap: reliance on sender-reputation filtering as a primary phishing defense is insufficient when attackers route through legitimate SaaS senders. Evaluate your email security stack's ability to inspect link destinations rather than sender domain alone. Implement a formal SaaS application inventory so links to unsanctioned hosting platforms (Netlify, Vercel) can be flagged contextually. Develop or update a social media account compromise playbook covering Facebook Business Manager specifically.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal and executive leadership if audit of the Meta Business Manager Audit Log confirms unauthorized ad spend against organizational payment methods, export of Custom Audience or customer PII, or if the number of compromised admin accounts suggests the organization's Meta Business Manager was resold through AccountDumpling's storefront — each of these conditions may trigger breach notification obligations under GDPR, CCPA, or state data protection statutes depending on the nature of audience data held in the account.

Recovery Notes	After credential reset, FIDO2 MFA enrollment, and Business Manager audit completion, monitor Meta Security Center login alerts daily for a minimum of 30 days, as AccountDumpling operators who successfully resell account access may attempt re-entry using purchased credentials before victims complete full eradication. Verify with Meta Business Support that no cloned or shadow Business Manager accounts were created using your organization's Page or ad account assets during the compromise window, as this is a documented post-compromise persistence technique in account resale operations. Maintain the pre-incident and post-incident Audit Log exports under legal hold for 12 months in the event of regulatory inquiry or civil liability from fraudulent ad spend.
Forensic Artifacts	Meta Business Manager Audit Log (Settings > Audit Log): primary forensic record of all AccountDumpling post-compromise actions including admin additions, payment method changes, ad campaign creation, and audience data exports — export full log for the 30-day window surrounding the incident and retain under legal hold | Email gateway message trace logs for sender domain *appsheet.com: extract raw headers (Received chain, x-originating-ip, DKIM signature results) to document how Google's legitimate AppSheet infrastructure was used to bypass sender-reputation filtering — these headers prove the trusted-platform abuse technique and are required for abuse reports to Google, Netlify, and Vercel | Meta Security Center > Active Sessions and Login History export: contains session token identifiers, IP addresses, ASN/geolocation, and device fingerprints for all authentication events — the real-time OTP relay attack will manifest as an attacker session originating from a Vietnamese or anonymizing IP appearing within seconds of a legitimate session from the victim's device, which is the smoking-gun artifact for this specific attack chain | Ads Manager campaign export (all statuses, full date range): documents any unauthorized ad campaigns created by AccountDumpling operators post-takeover, including targeting parameters, creative content, spend amounts, and associated payment instruments — required for financial fraud documentation and potential chargeback claims against unauthorized charges | DNS resolver query logs or proxy/CASB logs showing employee browser requests to netlify.app or vercel.app subdomains: the specific subdomain paths in these queries will contain victim-tracking tokens embedded by AccountDumpling's phishing kit, allowing you to correlate which employees received and clicked the phishing link and scope the full victim population within your organization

Per-Action IR Details

Containment — Audit all Facebook Business Manager accounts your organization owns: verify authorized administrators, remove unrecognized users, and revoke any third-party app permissions not explicitly sanctioned. If compromise is suspected, immediately use Facebook's 'Remove Account Access' controls and report to Meta Business Support.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected accounts and revoke attacker-controlled access vectors before eradication begins

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export Facebook Business Manager admin roster via Settings > People > Export and diff against your last known-good admin list (maintain this in a spreadsheet under version control). Use Meta's Business Account Activity log (Settings > Security Center > Recent Activity) to identify logins from unrecognized IPs. For third-party app permissions, navigate to Business Settings > Integrations > Connected Apps and screenshot the full list before revoking anything unrecognized — this preserves evidence before you destroy attacker access.

Evidence: Before revoking access, capture: (1) Full screenshot and CSV export of Business Manager People/Partners list showing all current admins and their email addresses, (2) Meta Business Security Center > Active Sessions export

showing session tokens, IP addresses, device fingerprints, and login timestamps for all active sessions — pay specific attention to sessions initiated from Vietnamese IP ranges (103.x.x.x, 27.x.x.x VNPT/Viettel blocks) or Mullvad/NordVPN exit nodes, (3) Meta Business Manager audit log export (Settings > Audit Log) covering the 30-day window prior to detection, documenting any permission escalations, ad account additions, or payment method changes added by AccountDumpling operators post-account takeover.

Detection — Review email gateway logs for messages originating from appsheet.com or *.appsheet.com that contain links to netlify.app, vercel.app, drive.google.com, or canva.com landing pages not provisioned by your organization. Query SIEM for login events to Facebook Business Manager from unexpected geolocations or IP ranges, particularly originating from Vietnam (VN) or anonymizing infrastructure. Look for session token reuse from new devices following credential entry.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate email delivery artifacts with downstream authentication anomalies to establish the AccountDumpling kill chain

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, run this PowerShell one-liner against Microsoft 365 or Google Workspace email logs exported to CSV: `Import-Csv mail_log.csv | Where-Object {$_.SenderDomain -like '*appsheet.com' -and ($_.Body -like '*netlify.app*' -or $_.Body -like '*vercel.app*' -or $_.Body -like '*canva.com*')} | Select-Object Timestamp,Sender,Recipient,Subject,Links | Export-Csv hits.csv`. For session anomaly detection without SIEM, enable Meta's login alerts (Settings > Security > Login Alerts) and configure them to send to a monitored SOC mailbox. Use MXToolbox or AbuseIPDB CLI lookups against sender IPs extracted from email headers to flag Vietnamese ASNs (AS45899 VNPT, AS7552 Viettel). For link inspection, run suspicious URLs through urlscan.io API before clicking.

Evidence: Capture before analysis: (1) Raw email headers (including x-originating-ip, Received chain, and DKIM/DMARC results) from any appsheet.com-delivered messages — these will show Google's legitimate DKIM signature passing despite the phishing payload, confirming the trusted-platform abuse technique, (2) Email gateway quarantine logs showing messages with sender domain appsheet.com and embedded hyperlinks pointing to netlify.app or vercel.app subdomains — extract the full URL paths as these typically contain victim-specific tracking tokens that can scope the campaign, (3) Facebook Business Manager login history export (Meta Security Center) showing authentication events with device fingerprint changes immediately following credential submission to the harvesting page — the real-time relay attack means attacker login will appear within seconds to minutes of victim credential entry, (4) DNS query logs from your resolver for any employee lookups of netlify.app or vercel.app subdomains not matching your known application inventory.

Eradication — Enforce phishing-resistant MFA (FIDO2/hardware security keys) on all Facebook Business Manager accounts; SMS and TOTP-based 2FA is defeated by this campaign's real-time relay harvesting. Remove any harvesting page URLs identified from organization-controlled DNS blocklists and proxy/CASB deny lists. Report abusive infrastructure to Netlify, Vercel, and Google via their abuse reporting channels to accelerate takedown.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: eliminate the attacker's harvested credential utility by invalidating session tokens, blocking relay infrastructure, and closing the MFA bypass vector exploited by AccountDumpling's real-time OTP relay

Controls: NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For organizations without CASB: add identified netlify.app and vercel.app phishing subdomains to Windows Defender SmartScreen via Group Policy (Computer Configuration > Administrative Templates > Windows Components > Windows Defender SmartScreen) and to Pi-hole or your internal DNS RPZ blocklist. Use the free Quad9 DNS resolver (9.9.9.9) as upstream, which blocks known malicious domains by default. For FIDO2 enforcement without enterprise MDM: Meta Business Manager supports hardware security keys natively under Settings > Security >

Two-Factor Authentication — walk each admin through enrolling a YubiKey 5 (or free Google Titan key via their security key program) and then disable SMS 2FA at the account level. Document enforcement completion per user in a spreadsheet signed off by the account owner.

Evidence: Before eradication actions, preserve: (1) The full URLs of identified harvesting pages hosted on netlify.app or vercel.app, including any URL parameters (victim tracking tokens, campaign IDs) — these are forensic evidence of campaign infrastructure scope and should be submitted to abuse channels with full context, (2) Screenshot and HTTP response capture (using curl -I or Burp Suite in passive mode) of the phishing landing pages before reporting to hosting providers causes takedown — this documents the real-time OTP relay mechanism and is needed for abuse reports and law enforcement referrals, (3) List of all current Facebook Business Manager session tokens (visible in Security Center > Where You're Logged In) before forcing a global session invalidation — document IP, device, and timestamp of each active session to distinguish legitimate from attacker-controlled sessions.

Recovery — After credential reset and MFA re-enrollment, verify that no unauthorized ad campaigns, payment method changes, or audience data exports occurred within the compromise window. Restore any modified Business Manager settings to known-good configurations. Enable Meta's login alerts and trusted device controls for all Business Manager users.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: verify Business Manager integrity against pre-compromise baseline, confirm attacker persistence mechanisms are eliminated, and restore operational trust in the advertising account before resuming revenue-generating activity

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST AU-11 (Audit Record Retention), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Without a dedicated SaaS security tool, conduct the Business Manager integrity audit manually using Meta's Audit Log (Settings > Audit Log): filter by the compromise window and export to CSV, then grep for action types: 'ADD_PAYMENT_METHOD', 'CREATE_AD_CAMPAIGN', 'EXPORT_AUDIENCE', 'ADD_ADMIN', 'CHANGE_ROLE'. For each flagged event, verify the actor email matches a legitimate employee. Check active ad campaigns under Ads Manager for any with unfamiliar names, unusual targeting (geographic targeting of Vietnam, Southeast Asia), or payment against a card/account not belonging to your organization. Run `diff` against a prior export of Business Manager settings if one exists.

Evidence: Capture before recovery actions: (1) Full Meta Business Manager Audit Log export covering from 30 days pre-incident through current date — this is the authoritative record of what AccountDumpling operators did post-account takeover, including any ad spend, audience list access, or page permission changes, (2) Active Ads Manager campaign list export (all campaigns, all statuses) including spend-to-date, payment method associated, audience targeting parameters, and creative assets — unauthorized campaigns may be running charges against your payment method or harvesting your Custom Audience data, (3) Payment method list from Business Manager (Settings > Payments) with full card/account details masked but last-four documented — compare against authorized payment instruments to identify any attacker-added payment methods.

Post-Incident — This campaign exposed a control gap: reliance on sender-reputation filtering as a primary phishing defense is insufficient when attackers route through legitimate SaaS senders. Evaluate your email security stack's ability to inspect link destinations rather than sender domain alone. Implement a formal SaaS application inventory so links to unsanctioned hosting platforms (Netlify, Vercel) can be flagged contextually. Develop or update a social media account compromise playbook covering Facebook Business Manager specifically.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: document the AccountDumpling trusted-platform abuse technique as a lessons-learned finding, update email security controls and detection rules to address URL-destination inspection gaps, and formalize the Facebook Business Manager compromise playbook for future incidents

Controls: NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: For email link-destination inspection without enterprise SEG: deploy the free Sublime Security community edition or configure ProofPoint/Mimecast sandbox rules (if already licensed) to detonate links from appsheet.com senders. Write a Sigma rule targeting your email gateway logs: `title: AccountDumpling SaaS Phishing Relay | detection: keywords: ['appsheet.com'] AND url_domain: ['netlify.app','vercel.app','canva.com'] AND NOT url_domain in your_approved_saas_list` — submit to the SigmaHQ community repo. For the SaaS inventory, start a CSV tracking: platform name, business owner, approved use cases, known domains — Netlify and Vercel should now appear as 'unapproved hosting' unless your dev team uses them. Publish the Facebook Business Manager compromise runbook in your internal wiki and schedule a tabletop exercise.

Evidence: Preserve for lessons-learned documentation: (1) Full timeline of AccountDumpling TTPs observed in this incident mapped to MITRE ATT&CK: T1566.002 (Spearphishing Link), T1557 (Adversary-in-the-Middle for OTP relay), T1078.004 (Valid Accounts: Cloud Accounts for post-compromise Business Manager access), T1583.006 (Acquire Infrastructure: Web Services for Netlify/Vercel hosting) — document which techniques your existing controls detected and which they missed, (2) Email gateway efficacy report showing that appsheet.com sender passed DMARC/DKIM/SPF checks — this documents the specific control gap for the board-level incident report and justifies investment in URL sandboxing, (3) Metrics on compromise window: time from phishing email delivery to account takeover, time from takeover to detection, time from detection to containment — these feed your MTTD and MTTR KPIs per NIST 800-61r3 §4 recommendations.

Detection Guidance

Email gateway: alert on messages where the sending domain is appsheet.com or a subdomain thereof and the embedded URLs resolve to netlify.app, vercel.app, drive.google.com, or canva.com. These domain pairings have no legitimate business use case in most organizations. CASB/proxy: flag or block outbound authentication POST requests to pages hosted on netlify.app, vercel.app, or canva.com that are not in your approved SaaS inventory. Facebook Business Manager audit log: query for admin role additions, payment method changes, or ad account ownership transfers not initiated by known users, particularly during off-hours. SIEM behavioral: correlate Facebook Business login events from new device fingerprints immediately following a user clicking a link from an AppSheet-originated email. Threat intelligence: IOCs from this campaign have not been publicly confirmed in structured feeds as of this item's sourcing date; monitor T3 sources (The Hacker News, CyberSecurityNews) for published IOC drops. Optional: Threat intelligence teams monitoring Telegram-based threat markets may search for AccountDumpling storefront listings referencing Facebook Business account sales.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`appsheet.com`	Legitimate Google AppSheet domain abused as phishing email sender to bypass reputation filters; not inherently malicious — flag unexpected emails from this domain containing external links	HIGH
DOMAIN	`netlify.app`	Legitimate hosting platform abused to stage credential-harvesting pages in this campaign	MEDIUM

Type	Value	Context	Confidence
DOMAIN	`vercel.app`	Legitimate hosting platform abused to stage credential-harvesting pages in this campaign	MEDIUM
DOMAIN	`canva.com`	Legitimate design/hosting platform abused for phishing page staging	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1114** — Email Collection
- **T1539** — Steal Web Session Cookie
- **T1598.003** — Spearphishing Link
- **T1566.002** — Spearphishing Link
- **T1071.001** — Web Protocols
- **T1567** — Exfiltration Over Web Service
- **T1583.006** — Web Services
- **T1608.005** — Link Target
- **T1056.003** — Web Portal Capture
- **T1585.001** — Social Media Accounts
- **T1078** — Valid Accounts

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
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **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
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **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.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1114	Email Collection	Collection
T1539	Steal Web Session Cookie	Credential-Access
T1598.003	Spearphishing Link	Reconnaissance
T1566.002	Spearphishing Link	Initial-Access
T1071.001	Web Protocols	Command-And-Control
T1567	Exfiltration Over Web Service	Exfiltration
T1583.006	Web Services	Resource-Development
T1608.005	Link Target	Resource-Development
T1056.003	Web Portal Capture	Collection
T1585.001	Social Media Accounts	Resource-Development
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/30000-facebook-accounts-hacked-vi...	T3
Attackers Abuse Google AppSheet, Netlify, and Telegram in ...	https://cybersecuritynews.com/attackers-abuse-google-appsheet-netli...	T3
Google AppSheet Phishing Breaches 30K Facebook Accounts	https://cybertechnologyinsights.com/cyberattacks-data-breaches/goog...	T3
Google AppSheet abused to compromise 30,000 Facebook accounts	https://cyberinsider.com/google-appsheet-abused-to-compromise-30000...	T3
Key Vulnerability Used to Steal Facebook Accounts & More	https://www.cloudhesive.com/news/the-key-vulnerability-hackers-use-...	T3

Generated 2026-05-02 06:45 UTC by TJS Security Command Center