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

# Google Ads Weaponized to Intercept ManageWP Credentials in Real-Time 2FA Bypass Campaign

**THREAT CAMPAIGN** | **HIGH** | CVSS 7.5

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0283 |
| **Type** | Threat Campaign |
| **Severity** | HIGH |
| **CVSS Base Score** | 7.5 |
| **Affected Products** | GoDaddy ManageWP (all versions using portal login), WordPress sites managed via ManageWP plugin (1M+ sites at risk) |
| **Published** | 2026-05-06T17:36:06 |
| **Discovery Source** | Rss |

## Executive Summary

A threat actor is running a Google Ads campaign that intercepts ManageWP login credentials and multi-factor authentication codes in real time, allowing immediate account takeover without triggering standard MFA protections. GoDaddy's ManageWP platform is used to manage over one million WordPress sites; a single compromised account can expose every website under that account simultaneously. Organizations with staff who manage WordPress sites through ManageWP face significant risk of mass site defacement, malware injection, data theft, or ransomware deployment across their entire web property portfolio.

## Technical Analysis

This is an adversary-in-the-middle (AiTM) phishing campaign, not a software vulnerability, no CVE has been assigned. The threat actor purchases Google Ads placements targeting users searching for the ManageWP login page, presenting a sponsored result that redirects victims to a phishing proxy. The proxy transparently relays authentication traffic between the victim and the legitimate ManageWP portal, capturing both credentials and TOTP/2FA codes in real time before passing the session through. This defeats TOTP-based MFA entirely because the attacker authenticates to the real portal using the intercepted code within its validity window. According to Guardio Labs researchers cited by BleepingComputer, at least 200 victims were confirmed and attacker infrastructure was accessed, identifying a private, operator-driven phishing kit with Russian-language backend markers. The kit supports live operator monitoring, consistent with T1113 (Screen Capture/C2 observation). Relevant MITRE techniques: T1566 (Phishing), T1583.008 (Malvertising), T1557 (Adversary-in-the-Middle), T1078 (Valid Accounts), T1539 (Steal Web Session Cookie). Relevant CWEs:

CWE-287 (Improper Authentication), CWE-319 (Cleartext Transmission of Sensitive Information), CWE-384 (Session Fixation), CWE-1021 (UI Layer Rendering). No patch exists, this is an abuse-of-service attack. Mitigation requires procedural and architectural controls, not a software update.

## Action Checklist

1. Step 1: Containment, Audit all ManageWP accounts in your organization immediately. Identify any accounts with recent logins from unrecognized IPs or geolocations by reviewing the ManageWP activity log (dashboard: User Activity). Revoke active sessions for any account where compromise is suspected via ManageWP account settings > Active Sessions. Rotate credentials for all ManageWP accounts regardless of suspected compromise.
2. Step 2: Detection, Review ManageWP login history for anomalous authentication events: logins from IPs outside expected geography, rapid sequential logins suggesting session replay, or logins at unusual hours. Cross-reference against Google Workspace or SSO logs if ManageWP access is federated. Check managed WordPress sites for new admin user accounts, modified core files, injected scripts in theme/plugin files, or unexpected plugin installations by accessing each site's WordPress admin panel under Users > All Users and scanning files via ManageWP's site overview or using file integrity monitoring tools like Wordfence or Sucuri. These are indicators of post-compromise activity following account takeover.
3. Step 3: Eradication, This attack has no software patch. Remove the phishing vector by enforcing bookmark-only or direct-URL access to app.managewp.com for all staff, block access via search engine result clicks through endpoint DNS filtering or browser policy where feasible. Enroll all ManageWP accounts in hardware security key (FIDO2/passkey) authentication if supported by your ManageWP plan; if not yet available, request or advocate for this feature with GoDaddy and in the interim enforce hardware token or passkey authentication on upstream identity providers (SSO, Google Workspace) that feed ManageWP access. Note: TOTP-based 2FA does not protect against this attack.
4. Step 4: Recovery, For any confirmed compromised account: rotate ManageWP credentials, audit all connected WordPress sites for unauthorized admin accounts (via ManageWP's site overview or directly in each site's WordPress admin under Users > All Users), scan for injected malicious code using file integrity monitoring or plugins (e.g., Wordfence, Sucuri), and restore affected sites from a known-clean backup predating the compromise window. Confirm ManageWP account recovery email and phone are still under your control.
5. Step 5: Post-Incident, This campaign exposes a control gap in MFA architecture: TOTP is not phishing-resistant. Evaluate migration to FIDO2/passkey or hardware tokens for all privileged web application accounts, not just ManageWP. Add ManageWP and similar web management platforms to your phishing-resistant MFA policy scope. Implement a formal 'no sponsored search results for internal tools' policy and train staff to bookmark administrative portals directly. Review your Google Ads monitoring posture for brand impersonation and consider Google's ad complaint process for abusive sponsored placements targeting your managed tools.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |

| | |
|---|---|
| **Escalation Criteria** | Escalate to senior IR leadership, legal counsel, and data protection officer immediately if any compromised ManageWP account managed WordPress sites that process payment card data (PCI DSS breach notification), collect EU resident PII (GDPR 72-hour notification clock), or store PHI (HIPAA breach assessment required); secondary escalation trigger is confirmation that threat actor has deployed persistent webshells or backdoors across more than 10 managed WordPress sites, indicating automated post-exploitation at scale beyond the team's unaided remediation capacity. |
| **Recovery Notes** | After restoring WordPress sites from pre-compromise backups, maintain elevated monitoring of ManageWP User Activity logs and WordPress admin audit logs (via WP Activity Log plugin or equivalent) for a minimum of 30 days, specifically watching for re-appearance of unauthorized admin accounts or file modifications that would indicate a persistent backdoor survived the restoration. Verify that all ManageWP-connected WordPress sites have their wp-cron scheduled tasks audited (wp cron event list --format=table) for injected malicious cron jobs, as AiTM-enabled account takeovers frequently establish cron-based persistence to survive credential rotation. Confirm that no ManageWP Safe Updates, bulk plugin installations, or maintenance mode changes were queued by the threat actor during the compromise window, as ManageWP's bulk action capability allows site-wide changes that may execute after account recovery if not cancelled. |
| **Forensic Artifacts** | ManageWP User Activity log export (CSV): source IPs, session timestamps, and 2FA submission events for all accounts — the AiTM interception mechanism leaves a forensic signature of sub-60-second gaps between credential submission and TOTP entry followed by an immediate login from a distinct proxy IP, distinguishing real-time relay from legitimate authentication \| Browser history SQLite databases from all workstations used for ManageWP access (Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\History; Firefox: %APPDATA%\Mozilla\Firefox\Profiles*.default\places.sqlite) — query for any 'managewp' URL that does not originate from the canonical app.managewp.com domain, identifying which users clicked the malicious Google Ads placement and what AiTM relay domain was used \| WordPress wp_users and wp_usermeta database tables from all managed sites: administrator-capability rows created after the earliest suspected compromise timestamp represent accounts planted by the threat actor via ManageWP bulk user management during the post-AiTM account takeover window \| WordPress site filesystem snapshot focused on wp-content/uploads and wp-content/plugins directories: AiTM-enabled ManageWP account takeovers enable direct file manager access, and threat actors commonly stage PHP webshells in uploads (filenames matching regex [a-z0-9]{8,16}\.php) or inject base64-encoded eval() payloads into active theme functions.php files \| DNS query logs from endpoint resolvers or perimeter DNS forwarder covering 14 days prior to discovery: filter for any resolution of domains lexically similar to 'managewp' (Levenshtein distance ≤ 3 from 'managewp') that resolve to non-GoDaddy infrastructure ASNs — these records identify the AiTM proxy relay domains and establish which endpoints interacted with the phishing infrastructure before the credential interception occurred |

### Per-Action IR Details

**Step 1: Containment — Audit all ManageWP accounts in your organization immediately. Identify any accounts with recent logins from unrecognized IPs or geolocations by reviewing the ManageWP activity log (dashboard: User Activity). Revoke active sessions for any account where compromise is suspected via ManageWP account settings > Active Sessions. Rotate credentials for all ManageWP accounts regardless of suspected compromise.**

**NIST Phase:** Containment

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

**Controls:** NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

**Compensating:** Export ManageWP User Activity log as CSV via dashboard and run: awk -F',' '{print $3}' activity_export.csv | sort | uniq -c | sort -rn to surface repeated or outlier source IPs. Cross-check IPs against your known egress ranges using a free IP geolocation lookup (ip-api.com batch API — free tier supports 15 req/min). For session revocation confirmation without EDR, have users re-authenticate immediately after credential rotation and verify no active sessions persist in the ManageWP Active Sessions panel.

**Evidence:** Capture BEFORE revoking sessions: full screenshot and CSV export of ManageWP User Activity log showing timestamps, source IPs, and session tokens for the 72-hour window prior to discovery. Note any source IPs geolocating to residential proxy ranges or hosting ASNs (e.g., AS14061 DigitalOcean, AS16509 AWS) inconsistent with staff locations — AiTM proxy infrastructure typically resolves to these. Preserve browser history on any workstations where staff clicked a Google Ads result for 'ManageWP' or 'ManageWP login', as this captures the phishing relay URL (typically a lookalike domain proxying app.managewp.com). Document active session tokens before revocation for chain-of-custody records per NIST 800-61r3 §3.3.

**Step 2: Detection — Review ManageWP login history for anomalous authentication events: logins from IPs outside expected geography, rapid sequential logins suggesting session replay, or logins at unusual hours. Cross-reference against Google Workspace or SSO logs if ManageWP access is federated. Check managed WordPress sites for new admin user accounts, modified core files, injected scripts in theme/plugin files, or unexpected plugin installations — these are indicators of post-compromise activity following account takeover.**

**NIST Phase:** Detection Analysis

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

**Controls:** NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

**Compensating:** For WordPress site-level detection without enterprise tooling, run the following WP-CLI command across all managed sites to enumerate recently created admin accounts: wp user list --role=administrator --fields=user_login,user_registered,user_email --format=csv 2>/dev/null — flag any accounts registered after your earliest suspected compromise timestamp. For file integrity, run: find /var/www -name '*.php' -newer /var/www/wp-config.php -ls to identify PHP files modified after a reference date. For injected scripts in theme files, use: grep -rn --include='*.php' 'eval(base64_decode' /var/www/wp-content/ to detect common webshell obfuscation patterns left by post-AiTM compromise tooling. For Google Workspace log correlation, export Admin > Reports > Login Audit filtered by ManageWP's OAuth app identifier if SSO is configured.

**Evidence:** Preserve before analysis: ManageWP login history export for all accounts covering 14 days prior to discovery — specifically flag events where credential authentication and 2FA submission timestamps are separated by under 60 seconds, which is the AiTM relay window for real-time TOTP interception. In WordPress databases, query: SELECT user_login, user_registered, meta_value FROM wp_users JOIN wp_usermeta ON wp_users.ID = wp_usermeta.user_id WHERE meta_key='wp_capabilities' AND meta_value LIKE '%administrator%' ORDER BY user_registered DESC LIMIT 20; — capture output before any eradication. Preserve wp-content/uploads directory listing and modification timestamps, as threat actors commonly stage webshells or backdoors in uploads directories post-account takeover via ManageWP's bulk file manager. If Google Workspace SSO is in use, export SAML assertion logs for the compromise window.

**Step 3: Eradication — This attack has no software patch. Remove the phishing vector by enforcing bookmark-only or direct-URL access to app.managewp.com for all staff — block access via search engine result clicks through endpoint DNS filtering or browser policy where feasible. Enroll all ManageWP accounts in hardware security key (FIDO2/passkey) authentication if available, as this MFA method is not vulnerable to AiTM proxy interception. TOTP-based 2FA does not protect against this attack.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** NIST SI-2 (Flaw Remediation), NIST SC-20 (Secure Name/Address Resolution Service — Authoritative Source), NIST IA-5 (Authenticator Management), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.3 (Perform Automated Operating System Patch Management)

**Compensating:** Deploy a Pi-hole or pfBlockerNG DNS sinkhole with a custom blocklist targeting known ManageWP-lookalike domains (managewp-login[.]com, manage-wp[.]net patterns — query urlscan.io or URLhaus for current AiTM relay domains associated with this campaign). For browser policy enforcement without enterprise MDM, push a Chrome managed policy via Group Policy or registry key: HKLM\SOFTWARE\Policies\Google\Chrome\URLBlocklist = '*' scoped with a corresponding URLAllowlist = 'https://app.managewp.com/*' to prevent search-engine-click access paths. For FIDO2 enrollment without budget, register free passkeys via any FIDO2-compatible authenticator app (e.g., Google Authenticator passkey support, Bitwarden Passwordless) as an interim measure until hardware tokens are procured. Sigma rule reference: sigma/rules/web/proxy_generic/proxy_suspicious_managewp_lookalike.yml (community rules exist for AiTM proxy domain patterns; search the SigmaHQ GitHub repository for current AiTM detection rules applicable to this infrastructure pattern).

**Evidence:** Before enforcing DNS blocks, capture: full DNS query logs from endpoint resolvers or your perimeter DNS forwarder for the 14-day lookback window, filtering for any resolution of domains resembling 'managewp' that are NOT app.managewp.com or managewp.com — these are the AiTM proxy relay domains and constitute primary evidence of staff interaction with the phishing infrastructure. Preserve browser history from all workstations used for ManageWP access: target the Chrome history SQLite database at %LOCALAPPDATA%\Google\Chrome\User Data\Default\History and query the urls table for any domain containing 'managewp' that does not match the canonical app.managewp.com origin. This distinguishes which users clicked a sponsored result versus used a bookmark.

**Step 4: Recovery — For any confirmed compromised account: rotate ManageWP credentials, audit all connected WordPress sites for unauthorized admin accounts (wp_users table or Users > All Users in WP admin), scan for injected malicious code using a file integrity monitoring tool or plugin (e.g., Wordfence, Sucuri), and restore affected sites from a known-clean backup predating the compromise window. Confirm ManageWP account recovery email and phone are still under your control.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST IR-4 (Incident Handling), NIST CP-9 (System Backup), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.2 (Establish and Maintain a Remediation Process)

**Compensating:** Run Wordfence CLI (free tier) or Sucuri SiteCheck (free, no install required) against each affected WordPress site URL to identify injected scripts and modified core files before backup restoration. For wp_users auditing without WP admin access, connect directly to the WordPress MySQL/MariaDB database: mysql -u wpuser -p wpdb -e "SELECT user_login, user_email, user_registered FROM wp_users JOIN wp_usermeta ON wp_users.ID=wp_usermeta.user_id WHERE meta_key='wp_capabilities' AND meta_value LIKE '%administrator%';" — remove any unrecognized admin rows before restoring from backup to avoid re-persisting backdoor accounts. For file integrity verification post-restoration, use WP-CLI: wp core verify-checksums and wp plugin verify-checksums --all to confirm core and plugin files match WordPress.org repository hashes. Verify ManageWP recovery email ownership by triggering a test password reset to the registered address and confirming delivery.

**Evidence:** Before beginning any restoration, preserve: a complete file system snapshot or tarball of the compromised WordPress site's wp-content directory, including uploads — threat actors using ManageWP bulk access frequently drop PHP webshells in wp-content/uploads (e.g., files named with random alphanumeric strings ending in .php or .php.jpg). Capture the wp_options table entry for 'siteurl' and 'home' to detect URL hijacking redirects. Export the wp_usermeta table filtered on capability = administrator to document all unauthorized accounts created during the compromise window. This evidence must be preserved in immutable storage before any recovery action modifies the filesystem, per NIST 800-61r3 §3.5 and NIST IR-4 (Incident Handling) evidence preservation requirements.

**Step 5: Post-Incident — This campaign exposes a control gap in MFA architecture: TOTP is not phishing-resistant. Evaluate migration to FIDO2/passkey or hardware tokens for all privileged web application accounts, not just ManageWP. Add ManageWP and similar web management platforms to your phishing-resistant MFA policy scope. Implement a formal 'no sponsored search results for internal tools'**

**policy and train staff to bookmark administrative portals directly. Review your Google Ads monitoring posture for brand impersonation and consider Google's ad complaint process for abusive sponsored placements targeting your managed tools.**

**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 IA-5 (Authenticator Management), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

**Compensating:** For brand impersonation monitoring without a commercial service, set up a free Google Alerts query for 'ManageWP' + 'login' and review weekly for suspicious sponsored content patterns; supplement with manual spot-checks of Google search results for 'ManageWP login' from a clean browser session monthly. To enforce bookmark-only access policy without MDM, distribute a pre-configured browser bookmarks HTML file to all staff via shared drive and document in your acceptable use policy that clicking search ads for administrative tools is a policy violation. For FIDO2 migration planning, reference CISA's Phishing-Resistant MFA guidance (cisa.gov — search 'phishing-resistant MFA fact sheet') as a free policy justification document. Submit a Google Ads policy complaint via ads.google.com/intl/en_us/home/resources/adsense-spam-report/ referencing the impersonating advertiser to request takedown of the malicious ad placement.

**Evidence:** Compile a lessons-learned document per NIST 800-61r3 §4 capturing: the specific Google Ads creative and relay domain used in this campaign (preserved from browser history forensics in Step 3), a timeline from first staff click to account compromise to detection, the number of WordPress sites exposed per compromised ManageWP account (blast radius metric), and the delta between TOTP submission and AiTM session replay (establishing the real-time interception window). This document supports both internal control improvement and any regulatory breach notification assessment if compromised WordPress sites processed PII or payment data. Submit campaign IOCs (relay domains, phishing URLs) to CISA's automated indicator sharing program and Google Safe Browsing report portal to protect the broader community.

## Detection Guidance

Primary detection surface is ManageWP's own activity log, look for authentication events from IPs inconsistent with your team's known locations, multiple successful logins within short intervals from different IPs (session relay pattern), and logins immediately followed by bulk site actions. For WordPress sites under managed accounts: query wp_users for accounts created after a suspicious login window; scan for base64-encoded strings injected into active theme files (functions.php, header.php); check for unauthorized plugin installations via wp_options (active_plugins). At the network/DNS layer: monitor for DNS queries or outbound connections to domains mimicking 'managewp' or 'godaddy' that are not the canonical app.managewp.com. If you run an email security gateway, flag any inbound messages referencing ManageWP login links, the campaign may use secondary phishing lures. No public IOC list has been confirmed from Guardio Labs' disclosure; treat any sponsored Google search result for ManageWP as a potential lure until Google removes the abusive placements.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| URL | `app.managewp.com (canonical — verify all login URLs match exactly)` | Phishing proxies mimic this URL; any sponsored Google search result claiming to lead here should be treated as suspect until campaign is confirmed removed | HIGH |

## Framework Mappings

### MITRE-ATTACK

- **T1566** — Phishing
- **T1078** — Valid Accounts
- **T1583.008** — Malvertising
- **T1557** — Adversary-in-the-Middle
- **T1539** — Steal Web Session Cookie
- **T1598.003** — Spearphishing Link
- **T1113** — Screen Capture
- **T1566.003** — Spearphishing via Service

### NIST-800-53R5

- **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
- **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)
- **SC-8** — Transmission Confidentiality and Integrity

### OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A02:2021** — Cryptographic 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

- **3.10** — Encrypt Sensitive Data in Transit
- **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
- **164.312(e)(1)** — Transmission Security
- **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

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1566 | Phishing | Initial-Access |
| T1078 | Valid Accounts | Defense-Evasion |
| T1583.008 | Malvertising | Resource-Development |
| T1557 | Adversary-in-the-Middle | Credential-Access |
| T1539 | Steal Web Session Cookie | Credential-Access |
| T1598.003 | Spearphishing Link | Reconnaissance |
| T1113 | Screen Capture | Collection |
| T1566.003 | Spearphishing via Service | Initial-Access |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.bleepingcomputer.com/news/security/hackers-abuse-google... | T3 |
| **Hackers abuse Google ads for GoDaddy ManageWP login phishing** | https://x.com/TheCyberSecHub/status/2052140498815738305 | T3 |

| Source | URL | Tier |
|---|---|---|
| **All my ManageWP websites are hacked : r/Wordpress - Reddit** | https://www.reddit.com/r/Wordpress/comments/1i78uwp/all_my_managewp... | T3 |
| **GoDaddy exposes fake WordPress plugin scam operation - LinkedIn** | https://www.linkedin.com/posts/godaddy_help-tds-and-its-malicious-p... | T3 |
| **GoDaddy Announces Security Incident Affecting Managed ...** | https://aboutus.godaddy.net/newsroom/company-news/news-details/2021... | T3 |

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

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