INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-16 18:58 UTC

ATHR Platform Automates End-to-End Vishing Attacks Using AI Voice Agents, Targeting Google, Microsoft, and Crypto Accounts

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0180
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Google, Microsoft, Coinbase, Binance, Gemini, Crypto.com, Yahoo, AOL, account holders on these platforms
Published	2026-04-16T10:09:11
Discovery Source	Rss

Executive Summary

A cybercrime group is selling an AI-powered platform called ATHR that fully automates voice phishing (vishing) attacks against users of Google, Microsoft, and major cryptocurrency exchanges including Coinbase and Binance. The platform removes the need for skilled human attackers by chaining spoofed emails with AI-generated phone calls to steal account credentials at scale. Organizations whose employees or customers hold accounts on these platforms face increased risk of account takeover, unauthorized access, and financial loss, with no technical vulnerability to patch.

Technical Analysis

ATHR is a cybercrime-as-a-service (CaaS) platform that automates telephone-oriented attack delivery (TOAD) by integrating AI voice agents into a phishing-to-vishing pipeline. The attack chain operates in three stages: (1) spoofed email lures sent to targets impersonating Google, Microsoft, Coinbase, Binance, Gemini, Crypto.com, Yahoo, or AOL; (2) AI-generated voice calls that autonomously engage the target and apply social engineering pressure; (3) automated credential harvesting. No CVE is associated, this is threat actor tooling, not a software vulnerability. Applicable CWEs: CWE-287 (Improper Authentication) and CWE-1390 (Weak Authentication), reflecting exploitation of authentication trust assumptions rather than a discrete code flaw. MITRE ATT&CK techniques include T1566 (Phishing), T1566.002 (Spearphishing Link), T1566.004 (Spearphishing Voice), T1598 (Phishing for Information), T1598.004 (Phishing for Information: Spearphishing Voice), T1621 (Multi-Factor Authentication Request Generation), T1656 (Impersonation), T1534 (Internal Spearphishing),

T1539 (Steal Web Session Cookie), and T1110 (Brute Force). The platform is sold on underground forums for approximately $4,000 plus a 10% commission. The primary defensive gap is human authentication trust; MFA bypass via social engineering is a core capability.

Action Checklist

1. Step 1: Containment, Identify employees with accounts on targeted platforms (Google Workspace, Microsoft 365, Coinbase, Binance, Gemini, Crypto.com) and verify MFA enrollment. Disable SMS-based MFA where possible; enforce phishing-resistant MFA (FIDO2/hardware keys) for high-value accounts immediately.
2. Step 2: Detection, Review telephony and email gateway logs for spoofed sender domains impersonating Google, Microsoft, or listed crypto platforms. Monitor authentication logs for MFA prompt floods (T1621) and failed login spikes (T1110). Flag inbound calls from spoofed caller IDs referencing account security or suspicious activity. Alert on out-of-hours or geographically anomalous authentication attempts following inbound call events.
3. Step 3: Eradication, No patch exists; this is a social engineering campaign. Block known spoofed sender domains at the email gateway. Enforce DMARC, DKIM, and SPF on all owned domains to limit spoofing of your organization's identity in outbound lures. Restrict callback number verification to out-of-band, organization-controlled channels only.
4. Step 4: Recovery, Audit accounts on targeted platforms for unauthorized access, session token reuse (T1539), or profile changes following any reported suspicious call. Revoke active sessions for any account where credential compromise is suspected. Validate MFA re-enrollment for affected users before restoring access.
5. Step 5: Post-Incident, Conduct a user awareness exercise specifically covering AI voice impersonation. Employees should understand that voice calls can be synthetically generated and should never confirm credentials or MFA codes verbally. Review authentication policy gaps exposed by this campaign: SMS MFA susceptibility, lack of step-up authentication for sensitive actions, and absence of call verification protocols.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to executive leadership, legal counsel, and affected platform security teams (Google, Microsoft, or exchange trust-and-safety) immediately if any employee confirms they verbally provided an MFA code or credentials during an inbound call, if unauthorized API key issuance or cryptocurrency withdrawal activity is discovered on exchange accounts, or if the volume of targeted employees exceeds 5% of workforce — any of these conditions may trigger breach notification obligations under applicable state privacy laws or financial regulations.

Recovery Notes	After revoking sessions and enforcing FIDO2 MFA, monitor Microsoft Entra ID and Google Workspace sign-in logs daily for 30 days for re-appearance of geographically anomalous logins or new OAuth application grants on previously affected accounts, as ATHR-assisted takeovers may have resulted in persistent OAuth backdoors that survive password and session resets. For any employee whose crypto exchange account was active during the suspected vishing window, require the employee to independently verify withdrawal address whitelists and API key inventory directly through the exchange's authenticated web portal — do not rely on email confirmation. Validate that DMARC aggregate reports (rua) confirm zero unauthorized use of your organization's sending domains in the 14 days following eradication controls.
Forensic Artifacts	Microsoft Entra ID Sign-In Logs (JSON via MS Graph /auditLogs/signIns): capture authenticationDetails array showing MFA method used, MFA result, and conditionalAccessStatus for each authentication event in the 72-hour window surrounding reported vishing calls — MFA prompt flood pattern (T1621) and 'MFA denied, user declined' results are primary indicators of ATHR-driven real-time phishing relay. | Email gateway message headers for inbound lure emails: full RFC 5322 headers including Authentication-Results (SPF/DKIM/DMARC verdict), X-Originating-IP, and From/Reply-To display name spoofing google.com, microsoft.com, coinbase.com, or binance.com — ATHR chains a spoofed email immediately before the AI voice call, so lure emails will precede vishing call CDR timestamps by minutes. | PBX/UCaaS call detail records (CDRs): inbound caller ID, call duration, and call timestamp for all inbound calls to employee direct numbers referencing account security — ATHR uses spoofed caller IDs mimicking Google (650-253-0000), Microsoft (800-642-7676), or exchange support lines; short-duration calls (under 3 minutes) with MFA event correlation within 5 minutes are high-confidence ATHR automation indicators. | Google Workspace Admin Reports API — token events: OAuth application grants made by affected users in the 30-day window prior to detection, specifically any app granted 'https://www.googleapis.com/auth/gmail.readonly' or 'https://www.googleapis.com/auth/drive' scopes — ATHR-assisted account takeover may establish persistent OAuth access that survives credential reset. | Cryptocurrency exchange account security/activity logs: API key creation timestamps, withdrawal whitelist modification events, and login session records from Coinbase, Binance, Gemini, or Crypto.com account activity pages — unauthorized API keys or whitelist additions made within 30 minutes of a reported vishing call constitute confirmed compromise indicators and should be preserved as screenshots before any remediation action alters the audit trail.

Per-Action IR Details

Step 1: Containment — Identify employees with accounts on targeted platforms (Google Workspace, Microsoft 365, Coinbase, Binance, Gemini, Crypto.com) and verify MFA enrollment. Disable SMS-based MFA where possible; enforce phishing-resistant MFA (FIDO2/hardware keys) for high-value accounts immediately.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST IA-2 (Identification and Authentication — Organizational Users), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Export Azure AD / Google Workspace user lists via CLI (gcloud identity groups memberships list or az ad user list) and cross-reference against a manually maintained spreadsheet of known high-value accounts (finance, IT admins, executives). Use Google Admin SDK Reports API or Microsoft 365 compliance center Sign-In Logs (exported as CSV, no SIEM required) to identify accounts with SMS MFA enrolled: filter on 'authenticationMethodUsed = sms' in the M365 Sign-In Log export. For Google, pull Security > 2-Step Verification report from Admin Console. Prioritize

hardware key enforcement for any account with crypto platform SSO or access to wire transfer workflows.

Evidence: Before modifying MFA configuration, snapshot the current MFA enrollment state: export Google Admin Console 2-SV enrollment report and Microsoft Entra ID (Azure AD) Authentication Methods Activity report as timestamped CSVs. Capture Microsoft Unified Audit Log entries for MFA registration events (Operation: 'Update user' or 'Register security info') and any recent MFA method changes made within 72 hours of a reported suspicious call — these may indicate the attacker already completed an MFA swap during the vishing call. Preserve telephony records (call logs, inbound caller ID data) from the corporate PBX or UCaaS platform for any calls referencing 'account security', 'suspicious activity', or impersonating Google/Microsoft/Coinbase support.

Step 2: Detection — Review telephony and email gateway logs for spoofed sender domains impersonating Google, Microsoft, or listed crypto platforms. Monitor authentication logs for MFA prompt floods (T1621) and failed login spikes (T1110). Flag inbound calls from spoofed caller IDs referencing account security or suspicious activity. Alert on out-of-hours or geographically anomalous authentication attempts following inbound call events.

NIST Phase: Detection Analysis

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

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

Compensating: Email gateway: query mail transfer agent logs (Postfix: /var/log/mail.log; Exchange message tracking logs via Get-MessageTrackingLog) for inbound messages with From/Reply-To domains spoofing google.com, microsoft.com, coinbase.com, binance.com, gemini.com, crypto.com — use regex: '(google|microsoft|coinbase|binance|gemini|crypto)\.com' against envelope-sender where SPF/DKIM result is 'fail' or 'softfail'. Authentication: export Microsoft 365 Sign-In Logs (Entra ID > Sign-ins, filter RiskState != none or MFA result = 'MFA denied') as CSV; for Google, use Admin Reports API > login events filtered on 'login_failure' and 'login_challenge'. For MFA prompt flood detection (T1621) without SIEM, write a PowerShell script to count MFA push/OTP events per user per hour from the M365 Sign-In Log export and alert when count exceeds 5 within 60 minutes. Correlate timestamps of inbound calls from the PBX call detail records (CDRs) against authentication log timestamps manually — ATHR chains the email lure with a follow-up AI voice call within minutes, so a failed login spike within 15 minutes of an inbound spoofed-caller-ID call is a high-confidence indicator.

Evidence: Capture before analysis: (1) Email gateway message headers for all inbound messages from domains visually similar to google.com, microsoft.com, coinbase.com — preserve full RFC 5322 headers including Received chain, Authentication-Results (SPF/DKIM/DMARC verdict), and X-Originating-IP. (2) Microsoft Entra ID Sign-In Logs for the 7 days preceding detection: export JSON via MS Graph API (GET /auditLogs/signIns) filtering on userPrincipalName for affected users — retain fields: ipAddress, location, conditionalAccessStatus, authenticationDetails, riskEventTypes. (3) PBX/UCaaS CDRs showing inbound caller ID, call duration, and timestamp for any calls from numbers spoofing +1-800 ranges associated with Google, Microsoft, or exchange support lines. (4) ATHR-generated vishing calls use AI voice synthesis — if call recording is enabled on the PBX, preserve audio files as forensic evidence of synthetic voice characteristics.

Step 3: Eradication — No patch exists; this is a social engineering campaign. Block known spoofed sender domains at the email gateway. Enforce DMARC, DKIM, and SPF on all owned domains to limit spoofing of your organization's identity in outbound lures. Restrict callback number verification to out-of-band, organization-controlled channels only.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST SC-8 (Transmission Confidentiality and Integrity), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 9.2 (Ensure Only Approved Ports, Protocols, and Services Are Running)

Compensating: Email gateway blocklist: add sender domains and display-name spoofs to your MTA blocklist (Postfix: /etc/postfix/access with 'REJECT' action; Exchange: New-TenantBlockedSenderAddress or content filter rules). For

DMARC enforcement on owned domains: publish a DMARC TXT record at _dmarc.yourdomain.com with p=reject and rua/ruf reporting addresses — validate current SPF/DKIM/DMARC status using the free MXToolbox DMARC check (mxtoolbox.com/dmarc.aspx) or dmarcian.com free tier. Publish SPF with hard-fail (-all). For callback verification: draft and distribute a one-page policy requiring employees to terminate unsolicited inbound calls claiming to be from Google/Microsoft/exchange support and call back only using numbers sourced from the official platform website — no verbal confirmation of MFA codes under any circumstance. This is the primary eradication control since ATHR has no patchable software component.

Evidence: Before blocking domains, archive the full list of blocked indicators (sender domains, display names, originating IPs extracted from message headers) in a timestamped IOC log for potential law enforcement referral and for enriching future detection rules. Verify that DMARC reporting (rua) is collecting aggregate XML reports from major mailbox providers — these reports will confirm whether your domain is being spoofed in ATHR lure emails targeting your employees' personal accounts. Preserve any voicemail recordings or transcripts from AI-generated vishing calls as evidence of synthetic voice cadence and scripted social engineering language specific to the ATHR platform's known scripts.

Step 4: Recovery — Audit accounts on targeted platforms for unauthorized access, session token reuse (T1539), or profile changes following any reported suspicious call. Revoke active sessions for any account where credential compromise is suspected. Validate MFA re-enrollment for affected users before restoring access.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST AU-11 (Audit Record Retention), NIST IA-5 (Authenticator Management), CIS 6.2 (Establish an Access Revoking Process), CIS 5.3 (Disable Dormant Accounts)

Compensating: Google Workspace: use Admin Console > Reports > User Activity to review login events, session activity, and profile changes (recovery email/phone additions, OAuth app grants) for each affected user; revoke active sessions via Admin Console > Users > [user] > Reset Sign-in Cookies. Microsoft 365: run Revoke-AzureADUserAllRefreshToken (PowerShell, Az module) for suspected accounts and review Unified Audit Log for 'Set user password', 'Update user', 'Add app role assignment' operations within 30 days of the suspected call. For crypto accounts (Coinbase, Binance, Gemini, Crypto.com): instruct affected employees to check API key issuance logs and withdrawal whitelist changes — these platforms expose this in account security activity logs; unauthorized API keys created during the vishing window should be treated as a confirmed compromise indicator and reported to the exchange's trust and safety team. Validate MFA re-enrollment by requiring FIDO2 hardware key registration before restoring platform access.

Evidence: Before revoking sessions or resetting credentials, capture: (1) Microsoft Entra ID token issuance logs for the suspected compromise window — export via MS Graph /auditLogs/signIns filtering on the user and time range, preserving refreshTokenIssuedTime and sessionId fields to establish session token lineage (T1539). (2) Google Workspace Admin Reports API > token events for OAuth grants made by the affected user — ATHR-assisted account takeover may result in the attacker granting a malicious OAuth app persistent access that survives password reset. (3) For crypto platform accounts: screenshot or export the full account activity/security log before any administrative action — exchange support teams will need this for their own investigation and potential asset recovery. (4) Profile change audit trail: any recovery email, recovery phone, or trusted device additions made within 24 hours of the vishing call are high-confidence indicators of attacker persistence.

Step 5: Post-Incident — Conduct a user awareness exercise specifically covering AI voice impersonation — employees should understand that voice calls can be synthetically generated and should never confirm credentials or MFA codes verbally. Review authentication policy gaps exposed by this campaign: SMS MFA susceptibility, lack of step-up authentication for sensitive actions, and absence of call verification protocols.

NIST Phase: Post Incident

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

Controls: NIST IR-2 (Incident Response Training), NIST IR-8 (Incident Response Plan), NIST AT-2 (Literacy Training and Awareness), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Awareness exercise: develop a one-page scenario brief using actual ATHR campaign characteristics — AI voice calling on behalf of 'Google Security Team', referencing a real-looking spoofed email the employee just received, requesting MFA code verbally to 'verify identity'. Deliver via all-hands email or 10-minute team briefing; no simulation platform required. Include a concrete decision rule: hang up on any unsolicited inbound call requesting credentials or MFA codes, regardless of how convincing the voice sounds, and report it to the security team via a dedicated reporting alias or Slack channel within 15 minutes. Policy gap review: document findings in a lessons-learned register covering (1) which accounts had SMS MFA still enabled, (2) which sensitive actions (wire transfers, API key creation, OAuth grants) lacked step-up authentication, and (3) which teams lacked a call verification protocol — assign remediation owners and 30-day deadlines for each gap. Share sanitized IOCs (spoofed domains, caller ID patterns, email lure characteristics) with your sector ISAC.

Evidence: Compile the post-incident evidence package: (1) Timeline reconstruction correlating email lure delivery timestamps, inbound call CDR timestamps, and authentication event timestamps for each affected user — this establishes the ATHR platform's automation chain and dwell time. (2) Aggregate MFA audit report showing pre- and post-incident MFA method distribution (SMS vs. TOTP vs. FIDO2) to quantify exposure reduction from containment actions. (3) Final IOC set (spoofed domains, originating IPs, caller ID ranges) formatted as a STIX 2.1 bundle or simple CSV for sharing with sector ISAC and for import into email gateway blocklists. (4) Record of any unauthorized API keys, OAuth grants, or withdrawal whitelist changes discovered during recovery — retain for potential law enforcement referral if financial loss occurred on crypto platforms.

Detection Guidance

No signature-based detection applies; ATHR exploits human behavior, not software flaws. Focus detection on behavioral indicators: (1) Email gateway: inbound messages spoofing Google, Microsoft, Coinbase, Binance, Gemini, Crypto.com, Yahoo, or AOL with mismatched SPF/DKIM/DMARC alignment; (2) Authentication logs: MFA push floods or OTP request spikes (T1621) correlated with inbound phone activity; unusual login times or locations following a reported suspicious call; (3) Telephony: inbound calls with spoofed caller IDs referencing account security, flag calls claiming to be from Google, Microsoft, or crypto platform support; (4) Session anomalies: new session tokens issued from unexpected IPs or devices after a call event (T1539); (5) User reports: treat employee reports of unexpected account-security calls as potential active attack indicators and triage immediately. No public IOCs (IPs, domains, hashes) were confirmed in available sources as of this report.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs available`	No IPs, domains, hashes, or URLs associated with ATHR infrastructure were confirmed in available sources as of this report. Treat absence of IOCs as expected for a CaaS platform with dynamic infrastructure.	LOW

Framework Mappings

MITRE-ATTACK

- **T1534** — Internal Spearphishing
- **T1539** — Steal Web Session Cookie
- **T1598.004** — Spearphishing Voice
- **T1566.002** — Spearphishing Link
- **T1598** — Phishing for Information
- **T1566.004** — Spearphishing Voice
- **T1656** — Impersonation
- **T1566** — Phishing
- **T1621** — Multi-Factor Authentication Request Generation
- **T1110** — Brute Force

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
- **CA-7** — Continuous Monitoring
- **AC-7** — Unsuccessful Logon Attempts
- **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
- **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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1534	Internal Spearphishing	Lateral-Movement
T1539	Steal Web Session Cookie	Credential-Access
T1598.004	Spearphishing Voice	Reconnaissance
T1566.002	Spearphishing Link	Initial-Access
T1598	Phishing for Information	Reconnaissance
T1566.004	Spearphishing Voice	Initial-Access
T1656	Impersonation	Defense-Evasion
T1566	Phishing	Initial-Access
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1110	Brute Force	Credential-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-athr-vishing-pla...	T3
Open source is collapsing under AI-powered threats | Cal.com	https://finance.yahoo.com/sectors/technology/articles/open-source-c...	T3
'AI-based super attacker' threat looms as top crypto exchanges ...	https://finance.yahoo.com/markets/crypto/articles/ai-based-super-at...	T3
Microsoft Finds Vulnerability Exposing Millions of Android Crypto ...	https://www.securityweek.com/microsoft-finds-vulnerability-exposing...	T3
Android API exposure, Acrobat zero-day, Bitcoin Depot attack	https://cisoseries.com/cybersecurity-news-android-api-exposure-acro...	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 2026-04-16 18:58 UTC by TJS Security Command Center