INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-01 07:11 UTC

Bluekit Phishing Kit Bundles AI Campaign Generation, Anti-Analysis Controls, and Full Lifecycle Management in Single Platform

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0250
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Microsoft Outlook, Hotmail, Gmail, Yahoo Mail, ProtonMail, iCloud, Apple ID, GitHub, Twitter, Zoho, Zara, Ledger (40+ brand templates)
Published	2026-04-30T14:58:50
Discovery Source	Rss

Executive Summary

Bluekit is a phishing-as-a-service platform that enables low-skill attackers to run credential-theft campaigns against over 40 major brands, including Microsoft, Google, Apple, and GitHub, with built-in tools to bypass multi-factor authentication. The platform integrates AI-assisted campaign generation using large language models (GPT-4 family, Claude, Llama), lowering the entry barrier for cybercriminals and accelerating campaign volume. Organizations relying on standard MFA as a primary control face elevated credential compromise risk, with downstream exposure to account takeover, data exfiltration, and unauthorized access to business-critical services.

Technical Analysis

Bluekit operates as a fully managed PhaaS platform consolidating domain registration, phishing page deployment, victim session monitoring, and real-time credential exfiltration into a single operator dashboard. The platform ships with 40+ brand-spoofing templates targeting Microsoft Outlook, Gmail, Apple ID, GitHub, ProtonMail, Ledger, and others. Core anti-analysis and evasion capabilities map to three CWEs: CWE-1021 (iframe overlay abuse to obstruct UI rendering and analysis tools), CWE-290 (authentication bypass via spoofed sender/context), and CWE-384 (session fixation/hijacking enabling AiTM-style 2FA bypass, stolen session tokens allow attackers to authenticate as the victim post-MFA completion). The AI assistant component integrates with large language models (GPT-4 family, Claude, Llama) to generate campaign skeletons, reducing operator skill requirements. MITRE coverage spans the full phishing lifecycle: spearphishing links (T1566.002),

internal spearphishing (T1534), email collection (T1114), web portal capture (T1056.003), adversary-in-the-middle (T1557), command scripting (T1059), browser session cookie theft (T1539), valid account abuse (T1078), spearphishing for information (T1598, T1598.003), proxy infrastructure (T1090.003), and account establishment (T1585.001). No CVE is assigned. No vendor patch applies, this is an attacker-controlled platform, not a vulnerability in a defender-controlled product. Threat actor attribution is unknown as of reporting date. Source quality score is 0.64 (T3 sources: BleepingComputer, Varonis, TechRadar, HackRead); no primary or secondary authority corroboration available. (Additional corroboration from CISA, law enforcement, or primary vendor threat research would elevate confidence.)

Action Checklist

1. Containment: Audit all SaaS application sign-in logs for the past 30 days for anomalous authentication events against Microsoft 365, Google Workspace, Apple ID, and GitHub. Prioritize accounts showing successful logins from unfamiliar IP ranges or geographies immediately following a link-click event in email logs. Suspend suspected compromised accounts pending review.
2. Detection: Query email gateway logs for messages containing links to recently registered domains (< 30 days old) spoofing the 40+ targeted brands. Cross-reference with proxy/DNS logs for user-initiated connections to those domains. Review identity provider logs for session token reuse from mismatched IP addresses, which indicates AiTM session hijacking (T1557, CWE-384). SIEM rule: alert on successful authentication events where the source IP differs from the IP that initiated the authentication flow.
3. Eradication: Migrate privileged and executive accounts (cloud admins, email admins, code repository maintainers) from TOTP/SMS-based MFA to phishing-resistant authentication (FIDO2 hardware security keys or passkeys) for all services targeted by Bluekit templates. Standard TOTP and push-based MFA do not prevent AiTM session hijacking. Revoke active sessions for any account confirmed or suspected to have authenticated through a phishing proxy.
4. Recovery: After session revocation, force re-authentication on phishing-resistant MFA. Audit OAuth application grants and API tokens on affected accounts, attackers who captured sessions may have issued persistent access tokens. Validate that email forwarding rules have not been added to compromised mailboxes (T1114). Monitor identity logs for 14 days post-remediation for recurrence.
5. Post-Incident: Document which accounts lacked phishing-resistant MFA and use findings to prioritize the rollout. Evaluate identity provider session anomaly detection policies (Azure Conditional Access, AWS GuardDuty session evaluation, Okta Adaptive MFA, or equivalent) to block authentication from anonymizing proxy infrastructure (T1090.003). Review security awareness training to include AiTM phishing scenarios where MFA prompts appear to complete normally. Submit observed phishing domains to your email gateway and threat intelligence platform for ongoing blocking.

Detection Guidance

Primary detection surface is identity provider and email gateway logs. Key behavioral indicators: (1) Authentication events where the initiating IP and the completing IP differ, indicates session proxying consistent with AiTM (T1557, CWE-384). (2) Successful logins immediately preceded by a user clicking a link in an email from an external sender, correlate email click telemetry with IdP sign-in timestamps. (3) DNS or proxy logs resolving domains that closely mimic targeted brand domains (typosquats, homoglyphs) registered within the last 60 days. (4) Browser session cookies appearing in multiple geographic locations within a short time window

(T1539). (5) New email forwarding rules or inbox filters created shortly after a suspicious authentication event (T1114). SIEM query approach: join email gateway click events with IdP authentication logs on user identity and timestamp within a 5-minute window; flag cases where the authentication source IP is not in the user's established baseline. For endpoint telemetry, look for T1059 execution patterns (script interpreter launches) that may indicate post-compromise automation. No confirmed IOCs (IPs, domains, hashes) are publicly attributed to Bluekit infrastructure in current T3 reporting; IOC data should be sourced directly from Varonis and BleepingComputer reports as they are updated.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Not publicly attributed in current reporting`	No confirmed Bluekit infrastructure IOCs (domains, IPs, hashes) are included in available T3 sources as of this item. Monitor Varonis and BleepingComputer publications for updates.	LOW

Framework Mappings

MITRE-ATTACK

- **T1566.002** — Spearphishing Link
- **T1534** — Internal Spearphishing
- **T1114** — Email Collection
- **T1056.003** — Web Portal Capture
- **T1557** — Adversary-in-the-Middle
- **T1059** — Command and Scripting Interpreter
- **T1539** — Steal Web Session Cookie
- **T1078** — Valid Accounts
- **T1598** — Phishing for Information
- **T1090.003** — Multi-hop Proxy
- **T1585.001** — Social Media Accounts
- **T1185** — Browser Session Hijacking
- **T1598.003** — Spearphishing Link

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
- **CM-7** — Least Functionality

- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.002	Spearphishing Link	Initial-Access
T1534	Internal Spearphishing	Lateral-Movement
T1114	Email Collection	Collection
T1056.003	Web Portal Capture	Collection
T1557	Adversary-in-the-Middle	Credential-Access
T1059	Command and Scripting Interpreter	Execution
T1539	Steal Web Session Cookie	Credential-Access
T1078	Valid Accounts	Defense-Evasion

Technique ID	Technique Name	Tactic
T1598	Phishing for Information	Reconnaissance
T1090.003	Multi-hop Proxy	Command-And-Control
T1585.001	Social Media Accounts	Resource-Development
T1185	Browser Session Hijacking	Collection
T1598.003	Spearphishing Link	Reconnaissance

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-bluekit-phishing...	T3
Meet Bluekit: The AI-Powered All-in-One Phishing Kit - Varonis	https://www.varonis.com/blog/bluekit	T3
Researchers discover new all-in-one 'Bluekit' phishing kit capable of ...	https://www.techradar.com/pro/security/researchers-discover-new-all...	T3
New AI-Powered Bluekit Phishing Kit Targets Major Platforms with ...	https://hackread.com/bluekit-phishing-kit-targets-platforms-mfa-byp...	T3
Attackers use Apple's Own Servers to Send Phishing Emails	https://www.youtube.com/watch?v=dtV76FL_9WI	T3

Generated 2026-05-01 07:11 UTC by TJS Security Command Center