INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-01 07:10 UTC

Q1 2026 Email Threat Landscape: 8.3 Billion Phishing Threats, QR Code Attacks Double, Tycoon2FA Disruption Yields Temporary Results

SECURITY ANALYSIS | **HIGH** | CVSS 7.5

SCC Item ID	SCC-STY-2026-0098
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Defender for Office 365, Microsoft Defender XDR, Microsoft Defender for Endpoint; broadly affects all enterprise email platforms and identity providers
Published	2026-04-30T15:00:00+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Microsoft Threat Intelligence detected 8.3 billion phishing threats in Q1 2026, with QR code attacks up 146% and CAPTCHA-gated phishing surging 125% in March alone, both techniques engineered to bypass automated security controls. Credential harvesting now accounts for 94% of payload-based attacks, signaling a deliberate shift by threat actors away from malware and toward identity theft as the primary entry point. A law enforcement disruption of the Tycoon2FA phishing-as-a-service platform produced only temporary relief, consistent with a broader pattern of PhaaS operators hardening their infrastructure against takedowns.

Technical Analysis

Microsoft's Q1 2026 email threat data reveals a threat landscape that has systematically adapted to defeat the controls most enterprises rely on. The 8.3 billion phishing detections represent not just volume growth but a qualitative evolution in evasion methods.

QR code phishing, up 146% quarter-over-quarter, exploits a structural gap in email security: most secure email gateways scan URLs and attachments, but QR codes are rendered as images. The malicious URL lives inside the image, invisible to link-scanning engines. Recipients scan the code on a personal mobile device, bypassing corporate endpoint controls entirely. The attack chain maps directly to MITRE T1566.001 (Spearphishing Attachment) and T1204.001 (Malicious Link), with the QR image functioning as the delivery mechanism.

CAPTCHA-gated phishing, surging 125% in March, addresses a different defensive layer: sandbox detonation. Automated sandboxes typically follow links and analyze page behavior passively. CAPTCHA gates interrupt that process, requiring human interaction before the credential harvesting page loads. Sandboxes fail silently; the security stack sees a CAPTCHA page and marks the URL clean. This technique aligns with T1056.003 (Web Portal Capture) and exploits the inherent limitation of behavioral analysis against interaction-dependent payloads.

The 94% credential phishing rate by March reflects a deliberate operational choice. Malware delivery creates endpoint artifacts, triggers EDR alerts, and exposes operators to takedown through payload infrastructure. Hosted credential harvesting, collecting usernames, passwords, and MFA tokens through adversary-in-the-middle (AiTM) frameworks, produces no endpoint footprint on the victim machine. The stolen session token (T1539) or captured OTP (T1111) is the product. This model directly underpins PhaaS platforms like Tycoon2FA, which provides operators with AiTM infrastructure, evasion tooling, and target templates as a subscription service.

The Tycoon2FA disruption is analytically significant precisely because it was temporary. Law enforcement and industry coordination dismantled infrastructure and reduced attack volume measurably, but consistent with every major PhaaS takedown in recent history, operators reconstituted within weeks. The platform's resilience reflects deliberate architectural choices: distributed hosting, rapid domain rotation (T1583.006), and modular infrastructure that separates the PhaaS control panel from the phishing front-ends. Defenders who treated the disruption as a resolution missed the operational pattern.

The aggregate picture is a threat ecosystem that has operationalized its evasion techniques against legacy email controls: CAPTCHA gates defeat sandboxes, QR codes defeat link scanners, AiTM defeats MFA, and PhaaS provides operational continuity against takedowns. Organizations still relying on perimeter email filtering as their primary credential defense have a structural gap this data makes explicit.

Action Checklist

1. Step 1: Assess exposure, audit your email security stack for QR code scanning capability; most legacy SEGs lack native QR code URL extraction and analysis, leaving that attack vector undetected at the gateway layer
2. Step 2: Review controls, verify that your secure email gateway or Microsoft Defender for Office 365 has CAPTCHA-aware URL detonation enabled; test whether your sandbox follows interactive page flows or stops at CAPTCHA prompts; confirm AiTM-resistant authentication (FIDO2/passkeys or certificate-based auth) is deployed for high-value accounts rather than TOTP-based MFA, which AiTM frameworks capture in real time
3. Step 3: Update threat model, add Tycoon2FA and generic PhaaS AiTM frameworks to your threat register; add detection rules for MFA interception (T1111), session token theft (T1539), and rapid domain infrastructure changes (T1583.006) to your SIEM and identity monitoring; assess whether your identity provider logs expose token replay or impossible-travel anomalies that would catch AiTM sessions post-credential capture
4. Step 4: Communicate findings, brief leadership that 8.3 billion phishing attempts in a single quarter represents a volume at which some will reach inboxes regardless of gateway efficacy; frame the conversation around post-delivery detection and identity resilience, not perimeter filtering alone; quantify the specific gap if QR code scanning is absent from your stack

5. Step 5: Monitor developments, track Microsoft Threat Intelligence blog and CISA advisories for follow-on Tycoon2FA infrastructure indicators as operators reconstitute; subscribe to PhaaS intelligence feeds covering platform re-emergence; watch for updated Defender for Office 365 policy guidance as Microsoft refines detections against CAPTCHA-gated and QR-delivered campaigns

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and identity platform owner if Entra ID Identity Protection surfaces a 'tokenIssuerAnomaly' or 'impossibleTravel' risk event for any account with access to sensitive data or privileged roles, if QR code scanning audit confirms zero gateway-layer URL extraction capability (leaving the entire QR attack vector undetected), or if a user reports completing an MFA prompt for a login they did not initiate — the latter is a near-certain AiTM session capture event requiring immediate token revocation across all sessions for that account.
Recovery Notes	If an AiTM session capture is confirmed via Tycoon2FA or a similar PhaaS framework, recovery requires more than password reset — all active refresh tokens and session tokens for the compromised account must be revoked immediately using 'Revoke-MgUserSignInSession -UserId ' in Microsoft Graph PowerShell or the Entra ID 'Revoke sessions' action, as stolen session tokens remain valid until expiry even after a password change. Post-revocation, monitor the affected account's Entra ID sign-in logs for a minimum of 14 days for signs of token replay from attacker-retained copies of the stolen session, and verify that the account's MFA method has been upgraded to FIDO2 or certificate-based authentication before re-enabling access. For any accounts where the attacker may have established persistence via OAuth app consent or registered a new MFA method, audit 'Get-MgUserAuthenticationMethod' and 'Get-MgUserAppRoleAssignment' outputs against the pre-incident baseline before returning the account to service.

Forensic Artifacts	Microsoft Entra ID Unified Audit Log — Operation: 'Add app role assignment to service principal' or 'Consent to application' events occurring within 30 minutes of a high-risk sign-in event indicate Tycoon2FA post-capture persistence via OAuth app consent grants, a common AiTM follow-on action to maintain access after session token expiry | Microsoft Defender for Office 365 Threat Explorer — filter by Delivery Action: 'Delivered' + Detection Technology: 'none' + Attachment FileType: 'png/jpeg/gif' to surface QR code phishing emails that transited the gateway without URL extraction analysis, establishing the undetected delivery corpus for this specific campaign vector | Microsoft Entra ID Sign-In Logs — filter for UserAgent strings associated with AiTM proxy frameworks (Evilginx2, Modlishka, Tycoon2FA relay servers commonly present generic or mismatched browser User-Agent headers) combined with ASN lookups showing hosting providers (OVH, Frantech, Serverius) commonly used for Tycoon2FA bulletproof infrastructure per T1583.006 | Microsoft Entra ID Identity Protection Risk Detections export — specifically the 'unfamiliarFeatures' detection type which fires when a sign-in originates from an IP, device, or location profile inconsistent with the user's history, the primary in-product signal for Tycoon2FA AiTM relay sessions where the attacker's proxy IP replaces the victim's legitimate IP in the authentication flow | Exchange Online Message Trace and Defender for Office 365 URL detonation logs — for emails where Safe Links verdict is 'Detonation unavailable' or 'Timeout', extract the original URL from the x-ms-exchange-organization-scl and X-Microsoft-Antispam headers in the raw message source to identify CAPTCHA-gated Tycoon2FA landing page domains that defeated sandbox analysis, then submit those domains to VirusTotal and cross-reference against ThreatFox for infrastructure confirmation

Per-Action IR Details

Step 1: Assess exposure — audit your email security stack for QR code scanning capability; most legacy SEGs lack native QR code URL extraction and analysis, leaving that attack vector undetected at the gateway layer

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Assessing and improving detection capability gaps before incidents occur

Controls: NIST SI-4 (System Monitoring) — verify monitoring tools cover QR-encoded URL extraction at the email gateway layer, NIST SI-5 (Security Alerts, Advisories, and Directives) — Microsoft Threat Intelligence Q1 2026 advisory documents 146% QR code attack increase as an active capability gap signal, NIST IR-4 (Incident Handling) — preparation sub-phase requires capability inventory aligned to known attack vectors, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — gap in QR code scanning is a detection control deficiency requiring formal tracking, CIS 8.2 (Collect Audit Logs) — confirm email gateway logs are capturing image attachment metadata and any extracted URLs; legacy SEGs frequently log only header-level data with no image content inspection

Compensating: For teams without enterprise SEG with QR decoding: use the free zbar-tools CLI (zbarimg) or Python pyzbar library in a script to batch-decode QR code images extracted from quarantined .eml files — run 'zbarimg --raw attachment.png' to extract the embedded URL, then submit that URL to VirusTotal's free API for reputation check. Create a mailbox rule to forward emails containing image-only bodies or single PNG/JPEG attachments with no text to a quarantine folder for manual QR decoding. Document the gap formally in your risk register as a compensating control limitation.

Evidence: Before auditing, preserve: (1) Email gateway quarantine logs showing image attachment delivery rates and file types (PNG, JPEG, GIF, SVG) for the past 90 days — QR phishing campaigns will show image-only or image-dominant email bodies with no URL in message headers; (2) Microsoft Defender for Office 365 Threat Explorer export filtered by 'Delivered' verdict + attachment type 'Image' to establish baseline of unscanned QR payloads that passed the gateway; (3) Microsoft 365 Message Trace logs for any emails containing single-image bodies from external senders in the past 30 days — these represent the undetected delivery window.

Step 2: Review controls — verify that your secure email gateway or Microsoft Defender for Office 365 has CAPTCHA-aware URL detonation enabled; test whether your sandbox follows interactive page flows or stops at CAPTCHA prompts; confirm AiTM-resistant authentication (FIDO2/passkeys or certificate-based auth) is deployed for high-value accounts rather than TOTP-based MFA, which AiTM frameworks capture in real time

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Validating that prevention and detection controls are correctly configured and tested against known attack techniques

Controls: NIST SI-4 (System Monitoring) — sandbox detonation must be verified to traverse CAPTCHA-gated pages representative of Tycoon2FA and similar PhaaS landing pages, not halt at the challenge layer, NIST IA-5 (Authenticator Management) — TOTP-based MFA is cryptographically insufficient against AiTM session relay; FIDO2/passkeys are origin-bound and defeat AiTM credential interception by design, NIST AC-17 (Remote Access) — enforce phishing-resistant MFA for all remote and privileged access pathways, explicitly replacing TOTP for high-value accounts, CIS 6.3 (Require MFA for Externally-Exposed Applications) — validate that FIDO2 or certificate-based auth is enforced on Microsoft 365, Azure AD, and any externally-exposed IdP endpoints targeted by AiTM frameworks, CIS 6.5 (Require MFA for Administrative Access) — administrative accounts are primary Tycoon2FA targets; TOTP on admin accounts is an active exploitable gap given real-time AiTM relay capability

Compensating: To test sandbox CAPTCHA traversal without enterprise tooling: manually submit known CAPTCHA-gated phishing page samples from PhishTank or URLhaus to your gateway's manual detonation interface and observe whether a verdict is returned or the analysis terminates with 'unable to analyze' or timeout — timeout/no-verdict is a confirmation that CAPTCHA gating is defeating your sandbox. For AiTM-resistant MFA on a limited budget: enroll high-value accounts in Microsoft Entra ID's free FIDO2 security key support (Windows Hello for Business is zero additional cost on existing M365 licensing) and use PowerShell 'Get-MgUserAuthenticationMethod -UserId ' to audit which accounts still have TOTP (Microsoft Authenticator OATH) as their only MFA method.

Evidence: Preserve before making configuration changes: (1) Microsoft Entra ID sign-in logs filtered by authentication method = 'OATH software token' or 'SMS' for all accounts with privileged roles or access to sensitive data — these represent the AiTM-capturable credential population; (2) Microsoft Defender for Office 365 Safe Links detonation logs showing URLs where verdict = 'Timeout' or 'Detonation unavailable' in the past 90 days — these are CAPTCHA-gated pages that bypassed sandbox analysis; (3) Conditional Access policy export from Entra ID showing which applications enforce which MFA methods — screenshot or JSON export before any policy changes for forensic baseline.

Step 3: Update threat model — add Tycoon2FA and generic PhaaS AiTM frameworks to your threat register; map T1111 (MFA interception), T1539 (session token theft), and T1583.006 (web services infrastructure for rapid domain rotation) to your detection coverage; assess whether your identity provider logs expose token replay or impossible-travel anomalies that would catch AiTM sessions post-credential capture

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Establishing detection baselines and correlation logic specific to known adversary techniques to identify active AiTM sessions

Controls: NIST SI-4 (System Monitoring) — configure Microsoft Entra ID Identity Protection or equivalent IdP to alert on token replay indicators: same refresh token used from two geographically distinct IPs within a short window, a Tycoon2FA post-capture AiTM behavioral signature, NIST IR-5 (Incident Monitoring) — formally add Tycoon2FA infrastructure indicators (known proxy domains, ASNs associated with bulletproof hosting used for rapid domain rotation per T1583.006) to your IOC tracking system, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — Entra ID sign-in logs and Unified Audit Log must be reviewed for impossible-travel events and unfamiliar sign-in properties that indicate AiTM session hijacking post-TOTP capture, NIST RA-3 (Risk Assessment) — threat register update for Tycoon2FA and PhaaS AiTM is a formal risk assessment activity; document likelihood increase given Q1 2026 volume data from Microsoft Threat Intelligence, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — extend vulnerability management process to include PhaaS platform tracking as an emerging threat category alongside CVE-based vulnerabilities

Compensating: For teams without SIEM or commercial threat intel: (1) Use the free Microsoft Sentinel community Sigma rules mapped to T1539 — import the rule 'Suspicious Sign-in Activity Indicating AiTM' into your log analysis workflow even if running manual KQL queries against the free Entra ID log export; (2) Query Entra ID sign-in logs via

Microsoft Graph PowerShell: 'Get-MgAuditLogSignIn -Filter "riskEventTypes/any(t: t eq 'tokenIssuerAnomaly')" | Select UserPrincipalName,IPAddress,Location' — no SIEM required; (3) Subscribe to the free CISA Known Exploited Vulnerabilities feed and Microsoft Threat Intelligence blog RSS for Tycoon2FA reconstitution indicators; (4) Use the free ThreatFox API to query current Tycoon2FA-associated IOCs: 'curl https://threatfox-api.abuse.ch/api/v1/ -d {"query":"search_tag","tag":"Tycoon2FA"}'.

Evidence: Capture before updating threat model so you have a detection gap baseline: (1) Microsoft Entra ID Identity Protection risk detections export — filter for 'unfamiliarFeatures', 'impossibleTravel', and 'tokenIssuerAnomaly' event types for the past 90 days to establish pre-enrichment baseline of AiTM-consistent events that fired but were not correlated to Tycoon2FA; (2) Unified Audit Log export filtered by Operation = 'UserLoggedIn' where DeviceProperties contains no known device — these are browser-based AiTM relay sessions with no registered device fingerprint, a Tycoon2FA session characteristic; (3) DNS query logs or Entra ID sign-in IP records showing connections to domains registered within 7 days of use — Tycoon2FA's T1583.006 rapid domain rotation leaves a short domain-age signature in DNS telemetry.

Step 4: Communicate findings — brief leadership that 8.3 billion phishing attempts in a single quarter represents a volume at which some will reach inboxes regardless of gateway efficacy; frame the conversation around post-delivery detection and identity resilience, not perimeter filtering alone; quantify the specific gap if QR code scanning is absent from your stack

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Communicating lessons learned and capability gaps to leadership to drive resource and policy decisions; also maps to CSF [GV] Govern function for risk communication

Controls: NIST IR-6 (Incident Reporting) — leadership briefing on threat landscape data constitutes organizational risk communication; the Q1 2026 Microsoft Threat Intelligence volume data is the basis for escalating QR code and AiTM detection gaps, NIST IR-8 (Incident Response Plan) — leadership communication should drive update of the IR plan to explicitly include post-delivery phishing response procedures and AiTM session revocation steps, NIST SI-5 (Security Alerts, Advisories, and Directives) — Q1 2026 Microsoft Threat Intelligence report and CISA phishing advisories are the authoritative external inputs supporting the leadership briefing; cite these directly rather than generalizing, NIST RA-3 (Risk Assessment) — quantifying the QR code scanning gap in terms of unscanned email volume (extract from Defender for Office 365 Threat Explorer) converts an abstract capability gap into a risk metric leadership can act on, CIS 7.2 (Establish and Maintain a Remediation Process) — leadership briefing should produce a documented remediation decision: accept the QR code gap with compensating controls, or fund capability upgrade; either outcome must be documented

Compensating: For teams without a dedicated security communications function: build the leadership brief as a one-page risk summary using publicly available data — cite the Microsoft Q1 2026 Threat Intelligence report directly (available at Microsoft Security Blog), pull your own Defender for Office 365 Threat Explorer data for image-attachment delivery counts, and present a simple two-column table: 'Attack vector | Detection capability: present/absent.' For quantifying the AiTM gap without commercial tooling, run the PowerShell MFA audit from Step 2 and report the count of accounts with TOTP-only MFA as the at-risk identity population. This requires no budget and produces a concrete number leadership can act on.

Evidence: Before the briefing, pull and preserve: (1) Microsoft Defender for Office 365 Threat Explorer 90-day export showing phishing emails with 'Delivered' verdict broken down by delivery reason — this is your evidence that gateway filtering does not achieve 100% interception and supports the 'some will reach inboxes' framing; (2) Entra ID Identity Protection risk summary report showing count of high-risk sign-in events in the past quarter — this quantifies the post-delivery identity threat surface that leadership must understand; (3) Screenshot or export of current MFA method distribution across user population from Entra ID — the proportion of accounts using TOTP vs. FIDO2/CBA is the quantified AiTM exposure metric for the briefing.

Step 5: Monitor developments — track Microsoft Threat Intelligence blog and CISA advisories for follow-on Tycoon2FA infrastructure indicators as operators reconstitute; subscribe to PhaaS intelligence feeds covering platform re-emergence; watch for updated Defender for Office 365 policy guidance as Microsoft refines detections against CAPTCHA-gated and QR-delivered campaigns

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Continuous intelligence monitoring for reconstituted threat actor infrastructure following law enforcement disruption; maps to CSF [ID] Identify function for sustained threat awareness

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — establish a formal process to ingest Microsoft Threat Intelligence blog and CISA advisories as authoritative external intelligence sources for Tycoon2FA reconstitution indicators, NIST IR-5 (Incident Monitoring) — track and document Tycoon2FA infrastructure re-emergence as a continuous monitoring activity; PhaaS platforms historically reconstitute within weeks of disruption, requiring sustained monitoring not a one-time check, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — schedule recurring review of Entra ID Identity Protection and Defender for Office 365 alerts specifically tuned to updated Tycoon2FA IOCs as Microsoft publishes revised detection signatures, NIST IR-8 (Incident Response Plan) — update the IR plan's indicator watchlist section with new Tycoon2FA infrastructure IOCs as they are published; reconstitution indicators must be operationalized into detection rules within 24 hours of publication, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — PhaaS platform re-emergence monitoring should be integrated into the vulnerability management process as a recurring threat intelligence review cadence

Compensating: For teams without commercial threat intel subscriptions: (1) Set up a free RSS feed monitor (such as Feedly free tier) tracking Microsoft Security Blog, CISA Alerts (https://www.cisa.gov/news-events/cybersecurity-advisories), and the MITRE ATT&CK changelog for T1111/T1539 technique updates; (2) Use the free abuse.ch ThreatFox feed — configure a daily cron job running 'curl https://threatfox.abuse.ch/export/json/recent/' and grep for 'Tycoon' or 'AiTM' tags to catch newly published Tycoon2FA IOCs; (3) When new Tycoon2FA domains or IPs are published, immediately add them to Entra ID Named Locations as blocked IPs and to Microsoft Defender for Office 365 tenant allow/block list as blocked URLs — both are free, no SIEM required.

Evidence: Establish a monitoring baseline now by preserving: (1) Current Defender for Office 365 tenant allow/block list export — this is your pre-reconstitution IOC baseline; any Tycoon2FA indicators added post-disruption should be version-controlled against this export to track response velocity; (2) Entra ID Named Locations configuration export — documents current blocked IP ranges so Tycoon2FA infrastructure IPs can be added incrementally and tracked; (3) Defender for Office 365 'Campaigns' view export filtered to the current quarter — Microsoft's campaign clustering will surface Tycoon2FA re-emergence as a new campaign cluster, providing an in-product early warning mechanism that requires no external tooling.

Detection Guidance

Detection for this threat cluster requires coverage across three distinct attack surfaces that most email security stacks address unevenly.

QR Code Detection: Enable or validate QR code URL extraction in your email security platform. Microsoft Defender for Office 365 provides QR code detonation as part of Safe Links; confirm it is active and not scoped out by policy exceptions. In logs, look for emails with image-only bodies and no hyperlinks, a structural signature of QR phishing. Hunt for QR-delivered URLs resolving to newly registered domains (under 30 days) or domains using CAPTCHA redirectors.

CAPTCHA-Gated Pages: Legacy sandbox verdicts on CAPTCHA-fronted URLs are unreliable. Cross-reference email delivery timestamps against proxy or DNS logs for user-initiated browsing to domains that appeared in email within a short time window. A clean sandbox verdict followed by a user visit to the same domain within minutes is a hunting hypothesis worth building. Look for browser sessions that resolve a domain, hit a CAPTCHA, and then POST credentials to a third-party endpoint; proxy logs showing an unusual POST to a domain with no prior history are a signal.

AiTM Session Capture: Review Azure AD / Entra ID sign-in logs for token replay indicators: successful authentication from one IP followed immediately by resource access from a geographically distinct IP using the

same session token. Enable continuous access evaluation (CAE) in Entra ID to reduce session token validity windows. Alert on MFA prompt completions where the originating IP differs from the session continuation IP. MITRE T1539 and T1528 (token theft and OAuth abuse) should be mapped to specific detection rules in your SIEM.

PhaaS Infrastructure: Monitor threat intelligence feeds for Tycoon2FA re-emergence domains. MITRE T1583.006 (web service infrastructure acquisition) means operators will reuse hosting providers and registrars; if you have prior Tycoon2FA domain patterns, pivot on registrar, nameserver, and hosting ASN to identify reconstituted infrastructure before campaigns launch.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Tycoon2FA PhaaS platform`	Adversary-in-the-middle phishing-as-a-service platform leveraged via subscribed threat operators to intercept credentials and MFA tokens in real time through hosted reverse-proxy infrastructure; platform reconstituted after law enforcement disruption	HIGH
URL	`Pending — refer to Microsoft Security Blog (https://www.microsoft.com/en-us/security/blog/2026/04/30/email-threat-landscape-q1-2026-trends-and-insights/) for published indicators`	Microsoft Threat Intelligence report references campaign infrastructure indicators including QR code delivery domains, CAPTCHA-gated phishing URLs, and Tycoon2FA-associated hosting patterns; specific IOC values not reproduced in the provided source text	LOW

Framework Mappings

MITRE-ATTACK

- **T1566.002** — Spearphishing Link
- **T1534** — Internal Spearphishing
- **T1566** — Phishing
- **T1583.006** — Web Services
- **T1566.001** — Spearphishing Attachment
- **T1056.003** — Web Portal Capture
- **T1204.001** — Malicious Link
- **T1111** — Multi-Factor Authentication Interception
- **T1557** — Adversary-in-the-Middle
- **T1528** — Steal Application Access Token
- **T1539** — Steal Web Session Cookie

- **T1598** — Phishing for Information
- **T1585.001** — Social Media Accounts
- **T1585** — Establish Accounts
- **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
- **CA-7** — Continuous Monitoring
- **IA-2** — Identification and Authentication (Organizational Users)
- **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
- **8.2** — Collect Audit Logs

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

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

Technique ID	Technique Name	Tactic
T1534	Internal Spearphishing	Lateral-Movement
T1566	Phishing	Initial-Access
T1583.006	Web Services	Resource-Development
T1566.001	Spearphishing Attachment	Initial-Access
T1056.003	Web Portal Capture	Collection
T1204.001	Malicious Link	Execution
T1111	Multi-Factor Authentication Interception	Credential-Access
T1557	Adversary-in-the-Middle	Credential-Access
T1528	Steal Application Access Token	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1598	Phishing for Information	Reconnaissance
T1585.001	Social Media Accounts	Resource-Development
T1585	Establish Accounts	Resource-Development
T1598.003	Spearphishing Link	Reconnaissance

Sources

Source	URL	Tier
Microsoft Security Blog	https://www.microsoft.com/en-us/security/blog/2026/04/30/email-thre...	T1
	https://www.microsoft.com/en-us/security/blog/2026/04/30/email-thre...	T1
	https://sqmagazine.co.uk/microsoft-q1-2026-phishing-threats/	T3
	https://www.scworld.com/news/microsoft-qr-code-captcha-gated-phishi...	T3
Microsoft Defender for Office 365 | Microsoft Security	https://www.microsoft.com/en-us/security/business/siem-and-xdr/micr...	T1

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 2026-05-01 07:10 UTC by TJS Security Command Center