INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-25 13:42 UTC

Chinese PhaaS Ecosystem Moves Beyond Credential Theft, Real-Time OTP Interception and Digital Wallet Tokenization Redefine the Threat

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0362
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Apple iMessage, RCS, Google services, PayPay, Amazon Japan, Nintendo, Rakuten Securities, Nomura Securities, Mercari, JCB Card, Alibaba domain services, users across 119 countries; Darcula PhaaS platform (UNC5814)
Published	2026-05-25T14:00:00+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Google Threat Intelligence Group has documented a maturing Chinese-language phishing-as-a-service ecosystem, led by the Darcula platform (UNC5814), that now intercepts one-time passcodes in real time and converts stolen payment card data directly into mobile wallet tokens, bypassing traditional fraud controls without ever exposing raw card numbers. The campaign targets consumers and financial services customers across 119 countries, with concentrated activity against Japanese financial platforms including Rakuten Securities, Nomura Securities, PayPay, and JCB Card. Organizations relying on SMS-based MFA, static phishing page detection, or IOC blocklists cannot defend against this threat model.

Technical Analysis

UNC5814 operates the Darcula PhaaS platform, which delivers adversary-in-the-middle (AiTM) session relay using Puppeteer-based browser automation to intercept live OTP tokens during active authentication sessions, rendering TOTP and SMS MFA ineffective against real-time interception. Phishing lures are delivered via Apple iMessage and RCS, circumventing carrier-level SMS filtering entirely. Page variants defeat signature-based detection by producing structurally unique HTML per session, consistent with automated generation techniques. Monetization has shifted from credential resale to digital wallet tokenization: stolen card data is provisioned into Apple Pay or Google Pay equivalents, enabling contactless fraud without exposing primary account numbers (PANs). Targeted brands include PayPay, Amazon Japan, Nintendo, Rakuten Securities, Nomura Securities,

Mercari, and JCB Card. Relevant CWEs: CWE-940 (Improper Verification of Source of Communication Channel), CWE-287 (Improper Authentication), CWE-308 (Use of Single-Factor Authentication). MITRE ATT&CK techniques include T1566 (Phishing), T1557 (Adversary-in-the-Middle), T1111 (MFA Interception), T1539 (Steal Web Session Cookie), T1056 (Input Capture), T1566.004 (Spearphishing via Service, iMessage/RCS), T1583/T1584 (Acquire/Compromise Infrastructure), T1621 (MFA Request Generation), and T1647 (Plist File Modification). No CVE is assigned; this is a platform capability evolution, not a discrete software vulnerability. Source: Google Threat Intelligence Group (cloud.google.com/blog/topics/threat-intelligence/chinese-language-phishing-services/).

Action Checklist

1. Step 1: Containment (Immediate). Audit authentication flows for all customer-facing applications relying on SMS OTP or TOTP. Identify services exposed to phishing via iMessage or RCS by reviewing inbound phishing reports and mobile threat logs. Block known Darcula infrastructure at the perimeter using IOCs from the Google Threat Intelligence report. Migrate to FIDO2/WebAuthn phishing-resistant authentication on all externally exposed applications, prioritizing financial and payment systems (NIST IA-2, CIS 6.3).
2. Step 2: Detection. Query email and messaging security gateway logs for iMessage and RCS-sourced phishing delivery (T1566.004). In your SIEM, build detection for AiTM session relay patterns: look for successful MFA authentication immediately followed by session token use from a distinct IP/ASN with no prior history for that account AND rapid subsequent financial transaction attempts, indicative of T1557 session relay. Monitor for anomalous card-not-present tokenization requests to Apple Pay or Google Pay provisioning APIs, especially high-velocity provisioning from new devices (T1111). Ensure authentication and payment logs are ingested and reviewed per NIST AU-6 (Audit Record Review) and CIS 8.2 (Collect Audit Logs). Behavioral IOC: successful login followed immediately by wallet provisioning from a new device warrants immediate step-up verification.
3. Step 3: Eradication. Replace SMS OTP and standard TOTP MFA with FIDO2/WebAuthn (phishing-resistant) across all externally exposed applications, prioritizing financial, payment, and privileged access workflows. This directly addresses CWE-308 and T1111. Disable or restrict new device wallet provisioning without explicit out-of-band owner verification. Enforce NIST IA controls requiring hardware-bound authenticators for high-value transactions. Update phishing detection tooling to move beyond static signature matching; deploy behavioral or AI-assisted page analysis capable of flagging dynamically generated lure pages.
4. Step 4: Recovery. After MFA migration, validate that no active session tokens from the suspect period remain valid; force re-authentication across affected user populations. Review payment processor logs for unauthorized tokenization events during the exposure window and initiate card issuer notification workflows per your incident response playbook. Confirm NIST AU-9 (Protection of Audit Information) controls are intact; AiTM actors may attempt to tamper with session and authentication logs. Monitor for renewed phishing lure delivery targeting the same brands in your supply chain or customer base for at least 30 days post-response. Apply NIST IR-4 (Incident Handling) procedures for post-containment validation.
5. Step 5: Post-Incident. Conduct a control gap assessment against NIST AC-7 (Unsuccessful Logon Attempts) and AC-12 (Session Termination) to ensure session anomaly thresholds are tuned for AiTM patterns. Document the gap between your prior phishing detection capability (signature-based) and the page evasion techniques used; update detection engineering runbooks accordingly. Review third-party and affiliate authentication dependencies; the PhaaS affiliate model means exposure can originate from

lower-security partners. Brief leadership on the digital wallet tokenization monetization path, as traditional fraud monitoring focused on raw card number exposure will not flag provisioning-based fraud. Map residual gaps to CIS 7.1 (Establish and Maintain a Vulnerability Management Process) and schedule a tabletop exercise simulating AiTM phishing against your current MFA stack.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to executive leadership, legal, and your card network/payment processor contacts if forensic review of payment processor logs confirms any unauthorized Apple Pay or Google Pay DPAN tokenization events during the exposure window, as this constitutes confirmed financial fraud with potential PCI DSS breach notification obligations and — for organizations serving Japanese financial platform customers — triggers notification requirements under Japan's Act on the Protection of Personal Information (APPI) and FSA incident reporting rules.
Recovery Notes	After forcing session revocation and completing MFA migration to FIDO2/WebAuthn, validate recovery by running a synthetic authentication test from a new device against each migrated application to confirm SMS OTP fallback paths have been fully disabled and cannot be re-enabled by an authenticated user without out-of-band verification. Continuously monitor your payment processor's provisioning API logs and your identity provider's new device enrollment events for at least 30 days post-remediation, as UNC5814 affiliates operating under the Darcula PhaaS model have demonstrated persistence by re-targeting the same brand ecosystems with freshly generated lure pages after initial takedowns. Engage your card issuer relationships to enable enhanced fraud rules specifically flagging card-not-present provisioning from devices with no transaction history, as traditional raw-PAN fraud controls will not surface the DPAN-based monetization path used by this actor.

Forensic Artifacts	Identity provider sign-in logs (Azure AD Sign-in logs, Okta System Log, or equivalent) filtered for successful MFA completions where the source IP ASN does not match the user's historical geolocation baseline — the Darcula AiTM reverse proxy relays authenticated sessions through hosting provider IP ranges that are geographically inconsistent with the victim's device location | Apple Pay IDMS push provisioning API request logs or Google Pay push provisioning API logs showing FPAN-to-DPAN tokenization events — specifically the device_id, device_ip, and provisioning_timestamp fields for any provisioning initiated within 5 minutes of a successful login event, which is the behavioral signature of automated AiTM-to-wallet-tokenization conversion | iMessage and RCS delivery metadata from Apple Business Register phishing reports or carrier abuse systems — Darcula lures are delivered via iMessage using registered Apple IDs and via RCS using virtual SIM pools, and delivery receipts contain sender Apple ID hashes or RCS sender identifiers that can be cross-referenced against known UNC5814 infrastructure | Web server or reverse proxy access logs (Apache access.log, Nginx access.log, or cloud WAF logs) from any customer-facing application targeted in the Darcula campaign — look specifically for POST requests to authentication endpoints where the User-Agent string matches mobile browser patterns but the TLS fingerprint (JA3 hash) matches known Darcula kit automation, as the kit auto-submits stolen OTPs programmatically rather than through a real browser | Payment processor webhook and dispute logs covering the full exposure window showing card-not-present transaction attempts and chargeback initiations linked to cards whose DPAN provisioning timestamps fall within the Darcula activity window — this artifact set establishes the financial impact scope and is the primary evidence required for PCI DSS forensic investigation and card issuer breach notification workflows

Per-Action IR Details

Step 1: Containment — Immediately audit authentication flows for all customer-facing and employee-facing applications that rely on SMS OTP or TOTP. Identify services exposed to iMessage or RCS-delivered lures by reviewing inbound phishing reports and mobile threat logs. Block known Darcula-associated infrastructure at the perimeter; consult the Google Threat Intelligence report for current IOC sets. Apply NIST AC-17 (Remote Access) controls to enforce phishing-resistant authentication on all externally exposed applications. Implement CIS 6.3 (Require MFA for Externally-Exposed Applications) using FIDO2/WebAuthn rather than SMS or TOTP where supported.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-7 (Unsuccessful Logon Attempts), 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)

Compensating: For teams without enterprise IAM tooling: export authentication logs from your identity provider (Okta, Azure AD, or on-prem LDAP) and run a PowerShell query — 'Get-AzureADAuditSignInLogs | Where-Object {$_.MfaDetail.AuthMethod -eq "SMS"}' — to enumerate all accounts still using SMS OTP. For RCS/iMessage lure identification without a mobile threat defense platform, manually triage your abuse@ inbox and Apple Business Manager phishing reports for domains matching Darcula's known naming pattern (brand-name + random string + .top/.xyz). Use pfSense or iptables to block IOC IP ranges published in the Google GTIG report using a deny-all rule on perimeter interfaces.

Evidence: Before executing any authentication reconfiguration, preserve: (1) raw authentication gateway logs showing OTP delivery timestamps and receiving phone numbers — these establish which accounts received Darcula lures and at what time; (2) mobile carrier SMS delivery receipts or iMessage delivery confirmation metadata if accessible through your MDM platform; (3) a full export of your current MFA method enrollment per account from your identity provider, timestamped, to create a pre-remediation baseline for later comparison against unauthorized TOTP/SMS re-enrollment attempts by threat actors attempting to maintain persistence; (4) perimeter firewall connection logs showing outbound

connections to Darcula reverse-proxy infrastructure, which will appear as HTTPS sessions to newly registered domains (sub-30-day registration age) on non-standard CDN ASNs.

Step 2: Detection — Query email and messaging security gateway logs for iMessage and RCS-sourced phishing delivery (T1566.004). In your SIEM, build detection for AiTM session relay patterns: look for rapid session token reuse from geographically inconsistent IPs immediately following successful MFA events (T1557, T1539). Monitor for anomalous card-not-present tokenization requests to Apple Pay or Google Pay provisioning APIs — especially high-velocity provisioning from new devices (T1111). Review AU-6 (Audit Record Review, Analysis, and Reporting) cadence; ensure authentication and payment logs are ingested and reviewed. Apply CIS 8.2 (Collect Audit Logs) to confirm logging is active on all identity and payment processing endpoints. Behavioral IOC: successful login followed immediately by wallet provisioning from a new device warrants immediate step-up verification.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use Elastic SIEM free tier or Graylog Open to ingest identity provider sign-in logs and payment processor webhook logs. Build a Sigma rule targeting the AiTM behavioral pattern: correlate successful MFA event followed within 60 seconds by a session token used from a source IP in a different ASN/country than the authenticating device — exportable as a Splunk SPL or Elastic EQL query from SigmaHQ. For Apple Pay and Google Pay tokenization anomalies without API-level monitoring, request daily provisioning reports from your payment processor (Stripe, Adyen, or direct card network) and flag any provisioning events where the device fingerprint is new AND the cardholder has not initiated a transaction in the prior 72 hours. Use Wireshark with a capture filter on your payment gateway's IP range ('host and port 443') to capture provisioning handshake metadata without decrypting payload.

Evidence: Before tuning detections, capture and preserve: (1) raw HTTPS access logs from your identity provider's sign-in endpoint showing User-Agent strings and source IPs for all successful MFA completions in the prior 30 days — Darcula's AiTM proxy will inject sessions from hosting provider ASNs (e.g., Cloudflare Workers, BuyVM, or Chinese CDN nodes) that will be inconsistent with the user's historical IP geolocation; (2) Apple Pay IDMS provisioning logs or Google Pay push provisioning API request logs — look specifically for 'FPAN to DPAN' tokenization requests where the device ID (device_id field) is not present in the cardholder's prior device history; (3) MITRE T1557 artifacts — session cookie values from your application's auth layer that were used from more than one concurrent IP within the same session window, extractable from Apache/Nginx access logs via 'awk' filtering on session cookie header values.

Step 3: Eradication — Replace SMS OTP and standard TOTP MFA with FIDO2/WebAuthn (phishing-resistant) across all externally exposed applications, prioritizing financial, payment, and privileged access workflows. This directly addresses CWE-308 and T1111. Apply D3-MFA (Multi-factor Authentication with phishing-resistant factors) and D3-CH (Credential Hardening). Disable or restrict new device wallet provisioning without explicit out-of-band owner verification. Enforce NIST IA controls requiring hardware-bound authenticators for high-value transactions. Update phishing detection tooling to move beyond static signature matching — deploy behavioral or AI-assisted page analysis capable of flagging dynamically generated lure pages.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-2 (Identification and Authentication — Organizational Users), NIST IA-5 (Authenticator Management), NIST AC-3 (Access Enforcement), NIST SI-2 (Flaw Remediation), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams that cannot immediately deploy hardware FIDO2 keys (YubiKey, Google Titan): enable passkey support in your identity provider as an interim step — both Okta and Azure AD free tiers support device-bound passkeys that are phishing-resistant without hardware token cost. To restrict wallet provisioning without a commercial

fraud platform, submit a request to your card network (Visa, Mastercard) or payment processor to enable 'step-up authentication required' flags on all new device provisioning events for your issued cards — this is a policy flag, not a software deployment. For phishing page detection without a commercial sandbox, deploy the free URLScan.io API against your abuse@ reported URLs and compare DOM structure hashes against Darcula's known lure template fingerprints (kit generates dynamic subdomains but reuses consistent HTML scaffold patterns documented in the Google GTIG report).

Evidence: Before executing MFA migration and provisioning restrictions, preserve: (1) a complete TOTP/SMS enrollment export from your identity provider showing authenticator device IDs and enrollment timestamps — any device enrolled during the Darcula exposure window that the account owner cannot verify should be treated as adversary-controlled authenticator persistence (T1098.005); (2) payment processor tokenization logs for the full exposure window showing Device Primary Account Number (DPAN) issuance events, cardholder device IDs, and IP addresses — this is your primary evidence set for card issuer notification and potential regulatory reporting; (3) Darcula kit artifacts if any lure pages were hosted on infrastructure you control or can request from your hosting provider — the kit's server-side OTP relay component communicates in real time with target bank APIs and will leave outbound connection traces in hosting provider logs to bank OTP verification endpoints.

Step 4: Recovery — After MFA migration, validate that no active session tokens from the suspect period remain valid; force re-authentication across affected user populations. Review payment processor logs for unauthorized tokenization events during the exposure window and initiate card issuer notification workflows per your incident response playbook. Confirm AU-9 (Protection of Audit Information) controls are intact — AiTM actors may attempt to tamper with session and authentication logs. Monitor for renewed phishing lure delivery targeting the same brands in your supply chain or customer base for at least 30 days post-response. Apply NIST IR-4 (Incident Handling) procedures for post-containment validation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-9 (Protection of Audit Information), NIST AU-11 (Audit Record Retention), NIST AC-12 (Session Termination), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: To force session invalidation without enterprise SIEM automation: use your identity provider's bulk session revocation API — Azure AD 'Revoke-AzureADUserAllRefreshToken' or Okta's '/api/v1/users/{id}/sessions' DELETE endpoint — scoped to all users whose sign-in logs show a successful authentication within the Darcula exposure window followed by an anomalous session IP. For audit log integrity verification without a log management platform, compute SHA-256 hashes of your authentication log files immediately after collection ('Get-FileHash -Algorithm SHA256' on Windows or 'sha256sum' on Linux) and store the hash manifest on write-once storage (S3 Object Lock, or simply email the manifest to a separate mailbox) to establish tamper evidence baseline. For 30-day phishing re-emergence monitoring without commercial threat intel, configure free Google Safe Browsing API alerts for your brand terms and monitor URLScan.io's public feed for newly submitted scans matching your targeted brand names (PayPay, Rakuten, JCB, etc.).

Evidence: Before closing the recovery phase, capture and archive: (1) complete session token validity audit from your application layer — export all active session records from your session store (Redis, database) and cross-reference against the token issuance timestamps from the exposure window to confirm none remain active post-forced-revocation; (2) payment processor dispute and chargeback data linked to cards identified in unauthorized provisioning events — this dataset is required for card issuer notification letters and may be required for PCI DSS incident reporting obligations; (3) audit log integrity verification artifacts (file hashes and access timestamps) for all authentication and payment logs from the exposure window, as Darcula's operators have demonstrated operational security awareness and AiTM infrastructure may have attempted log manipulation on compromised application layers.

Step 5: Post-Incident — Conduct a control gap assessment against NIST AC-7 (Unsuccessful Logon Attempts) and AC-12 (Session Termination) to identify whether session anomaly thresholds are tuned for AiTM patterns. Document the gap between your prior phishing detection capability (signature-based) and the AI-generated page evasion technique; update detection engineering runbooks accordingly. Review third-party and affiliate authentication dependencies — the PhaaS affiliate model means exposure can originate from

lower-security partners. Brief leadership on the digital wallet tokenization monetization path, as traditional fraud monitoring focused on raw card number exposure will not flag provisioning-based fraud. Map residual gaps to CIS 7.1 (Establish and Maintain a Vulnerability Management Process) and schedule a tabletop exercise simulating AiTM phishing against your current MFA stack.

NIST Phase: Post Incident

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

Controls: NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-12 (Session Termination), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For the AiTM tabletop exercise without a commercial red team: use the open-source Evilginx3 framework (freely available on GitHub) in an isolated lab environment to simulate the Darcula reverse-proxy AiTM technique against your own applications — this will reveal which of your session token lifetimes, concurrent session controls, and device fingerprinting policies would have blocked or detected the attack. For the third-party affiliate authentication review without a vendor risk platform, distribute a targeted questionnaire to all partners with SSO or API access to your systems, specifically asking: (1) MFA method in use, (2) session token lifetime configured, and (3) whether FIDO2 is supported — score responses against your own post-incident baseline. Publish internal Sigma detection rules for AiTM session relay behavior to SigmaHQ or your internal rule repository to operationalize the lessons-learned output.

Evidence: Post-incident documentation must include: (1) a lessons-learned report comparing pre-incident phishing detection rule coverage against the specific evasion characteristics of Darcula's AI-generated lure pages (dynamic DOM generation, no static URL patterns, brand-accurate visual cloning) — this gap document drives your detection engineering roadmap; (2) a third-party authentication dependency map showing every affiliate or partner with access to your identity or payment systems and their current MFA posture, which serves as the risk register input for the next assessment cycle; (3) a timeline artifact correlating the first observed Darcula phishing lure delivery (from iMessage/RCS abuse reports) through to the first unauthorized wallet provisioning event — this attack-chain timeline is the core artifact for executive briefing and is required if regulatory notification obligations were triggered.

Detection Guidance

Primary behavioral indicators center on AiTM session relay and anomalous wallet provisioning rather than static IOCs. In your SIEM or XDR platform, prioritize these detection patterns: (1) Successful MFA authentication event immediately followed by session token use from a distinct IP/ASN with no prior authentication history for that account AND rapid subsequent financial transaction attempts, indicative of T1557 session relay via Puppeteer proxy. (2) High-velocity Apple Pay or Google Pay device provisioning requests from accounts that completed MFA within the prior 60 seconds, indicative of tokenization fraud post-interception. (3) Inbound phishing lures delivered via iMessage or RCS (T1566.004); these bypass traditional email security. Review mobile device management (MDM) logs and carrier threat feeds for RCS-sourced malicious link delivery. (4) Phishing pages will not match static signatures; instead, hunt for pages with structurally novel HTML impersonating target brands (PayPay, JCB, Rakuten, Nomura, Amazon Japan, Mercari, Nintendo) using OSINT and threat intelligence feeds with behavioral page classification. (5) Monitor for OTP interception timing anomalies: if a TOTP or SMS code is consumed milliseconds after generation and a concurrent session from a foreign IP appears, treat as confirmed AiTM. Log sources: IdP/SSO authentication logs, payment processor provisioning APIs, MDM/UEM mobile threat logs, web proxy and DNS logs for newly registered domains mimicking target brands (T1583.001). Reference NIST AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting) to ensure these log sources are configured and reviewed. Apply NIST SI-4 (Information System Monitoring) and SI-7 (Software, Firmware, and Information Integrity) for endpoint-side session artifact review.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`darcula[.]com (platform infrastructure — representative)`	Darcula PhaaS platform domain associated with UNC5814 infrastructure; treat as indicator class rather than single domain — operators register large volumes of lookalike domains	MEDIUM
URL	`https://cloud.google.com/blog/topics/threat-intelligence/chinese-language-phishing-services/`	Google Threat Intelligence Group primary source report containing current IOC sets and infrastructure details — consult directly for updated indicator lists	HIGH

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1557** — Adversary-in-the-Middle
- **T1583** — Acquire Infrastructure
- **T1588.002** — Tool
- **T1656** — Impersonation
- **T1598** — Phishing for Information
- **T1588** — Obtain Capabilities
- **T1647** — Plist File Modification
- **T1111** — Multi-Factor Authentication Interception
- **T1584** — Compromise Infrastructure
- **T1621** — Multi-Factor Authentication Request Generation
- **T1583.001** — Domains
- **T1566.004** — Spearphishing Voice
- **T1539** — Steal Web Session Cookie
- **T1056** — Input Capture

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
- **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	Phishing	Initial-Access
T1557	Adversary-in-the-Middle	Credential-Access
T1583	Acquire Infrastructure	Resource-Development
T1588.002	Tool	Resource-Development
T1656	Impersonation	Defense-Evasion
T1598	Phishing for Information	Reconnaissance
T1588	Obtain Capabilities	Resource-Development
T1647	Plist File Modification	Defense-Evasion
T1111	Multi-Factor Authentication Interception	Credential-Access
T1584	Compromise Infrastructure	Resource-Development

Technique ID	Technique Name	Tactic
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1583.001	Domains	Resource-Development
T1566.004	Spearphishing Voice	Initial-Access
T1539	Steal Web Session Cookie	Credential-Access
T1056	Input Capture	Collection

Sources

Source	URL	Tier
Threat Intelligence	https://cloud.google.com/blog/topics/threat-intelligence/chinese-la...	T3
The Evolution of Chinese-language Phishing Services - Google Cloud	https://cloud.google.com/blog/topics/threat-intelligence/chinese-la...	T3
Japan investigates Google for alleged antitrust violations in search	https://www.cnbc.com/2023/10/23/japan-investigates-google-for-alleg...	T3
FAQ: Malware that Targets Mobile Devices and How to Protect Them	https://blogs.jpcert.or.jp/en/2022/02/mobile-malwarefaq.html	T3
Google sues Chinese scam ring over E-ZPass, USPS phishing texts	https://www.nbcnews.com/tech/security/google-sues-chinese-scam-ring...	T3

Generated 2026-05-25 13:42 UTC by TJS Security Command Center