INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-25 06:03 UTC

Chinese PhaaS Ecosystem (Darcula/Lucid) Bypasses MFA and Tokenizes Stolen Payment Cards in Real Time

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0361
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Apple iMessage, RCS (Android), Google services, Amazon, PayPay, Rakuten Securities, Nomura Securities, Nintendo, Mercari, JA Bank, JCB Card, Alibaba domain services, unspecified digital wallet providers; Darcula PhaaS platform attributed to UNC5814
Published	2026-05-25T14:00:00+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Google's Threat Intelligence Group has documented a large-scale Chinese-language phishing-as-a-service operation, anchored by the Darcula platform (UNC5814), active across 119 countries and targeting financial institutions, e-commerce, and securities firms. The platform intercepts one-time passcodes in real time to defeat MFA, then automatically loads stolen payment card data into attacker-controlled digital wallets, enabling contactless fraud without the physical card. Any organization offering consumer-facing authentication or payment services faces direct exposure; the industrialized scale and MFA-bypass capability make this a material financial and reputational risk.

Technical Analysis

Darcula and related tooling (Lucid, tracked under UNC5814) operate as a subscription PhaaS ecosystem delivering smishing lures via Apple iMessage and Android RCS, channels that bypass carrier SMS filtering. Attack chain: (1) AI-generated brand-cloned phishing pages dynamically mimic target organizations, defeating signature-based detection; (2) real-time OTP interception (T1111, T1621) captures time-sensitive one-time passcodes at the moment of victim entry, defeating TOTP and SMS-OTP MFA; (3) stolen payment card data is provisioned into attacker digital wallets via NFC relay or tokenization abuse (T1185), enabling contactless fraud without physical card possession; (4) session cookie theft (T1539) extends unauthorized access beyond the initial OTP window. Delivery abuses iMessage and RCS trust models (T1566.004). Infrastructure leverages

registered domains (T1583.001) and link masquerading (T1608.005). Relevant CWEs: CWE-308 (use of single-factor authentication), CWE-287 (improper authentication), CWE-1390 (weak authentication over network), CWE-940 (improper verification of source of communication channel). No CVE assigned, this is a platform-level campaign, not a single software vulnerability. No vendor patch resolves this; mitigation requires architectural and detection controls. Source: Google GTIG (https://cloud.google.com/blog/topics/threat-intelligence/chinese-language-phishing-services/).

Action Checklist

1. Step 1: Containment, Audit all externally exposed applications for SMS/TOTP-only MFA and flag them as elevated risk. Per CIS 6.3, enforce MFA on all externally exposed applications; per NIST IA-2, ensure authentication mechanisms cannot be bypassed via OTP interception. Temporarily add additional authentication steps (step-up authentication, out-of-band confirmation) on high-value financial transactions and account changes while longer-term controls are evaluated.
2. Step 2: Detection, Query email and messaging security gateways for iMessage-origin and RCS-origin links resolving to newly registered domains (registered within 30 days). Review authentication logs (NIST AU-2, AU-6) for OTP submission sequences where the OTP is used within seconds of issuance and is immediately followed by account change, payment initiation, or wallet-linking events, this pattern is consistent with real-time relay. Alert on digital wallet provisioning events from unfamiliar devices or geolocations. Cross-reference against Darcula/Lucid infrastructure IOCs from GTIG reporting.
3. Step 3: Eradication, Migrate high-risk accounts from SMS/TOTP OTP to FIDO2/passkey authentication, which is phishing-resistant and not interceptable via relay (NIST IA-2(1), D3-MFA). Implement origin-binding for authentication sessions to detect relay attacks: the session origin presented to the relying party must match the origin presented during authentication. Block or scrutinize digital wallet provisioning requests that do not originate from a previously trusted device (D3-CH, D3-CRO). Revoke and rotate any credentials or session tokens associated with accounts flagged in detection step (NIST AC-2, D3-CRO).
4. Step 4: Recovery, After control changes, validate that phishing-resistant MFA is enforced end-to-end with no SMS/TOTP fallback path remaining (NIST IA-2, CIS 6.3, CIS 6.5). Confirm digital wallet provisioning workflows require device trust attestation. Monitor authentication logs (NIST AU-6) for residual relay-pattern anomalies for a minimum of 30 days post-remediation. Verify session binding controls are functioning by testing from a proxied session.
5. Step 5: Post-Incident, Conduct a gap assessment against NIST SP 800-53 IA-2 and AC-17 to identify remaining OTP-based authentication paths in production. Evaluate whether consumer-facing brand monitoring and typosquat detection (NIST AU-13) are in place to identify cloned pages before victims reach them. Document findings and update the authentication section of your incident response playbook to include PhaaS relay scenarios. Consider threat-sharing with sector peers via ISAC channels if your organization is in financial services, e-commerce, or securities.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to executive leadership, legal, and your card network contacts (Visa/Mastercard fraud ops) if authentication logs confirm any OTP relay pattern resulted in successful digital wallet provisioning, as this constitutes realized payment card fraud triggering PCI DSS Incident Response requirements (PCI DSS v4.0 Requirement 12.10) and potentially state breach notification obligations if cardholder PII was exposed.
Recovery Notes	Post-containment, validate that no SMS/TOTP fallback authentication path survives in any consumer-facing or high-value internal application, and confirm with your payment processor or card network that any network tokens provisioned to attacker-controlled wallets during the incident have been revoked at the tokenization service layer — this step is specific to Darcula's card-to-wallet automation and is often missed in standard credential reset procedures. Monitor authentication logs daily for a minimum of 30 days for recurrence of the OTP relay latency signature (OTP used within 15 seconds of issuance followed by wallet or account change event), as UNC5814-attributed infrastructure has demonstrated rapid retargeting of organizations after initial detection. Retain all forensic artifacts and logs for a minimum of 12 months to support any PCI DSS forensic investigation or law enforcement referral.
Forensic Artifacts	IdP/auth platform OTP issuance and submission timestamp logs: the sub-15-second OTP relay latency is the definitive behavioral signature of Darcula's real-time interception infrastructure — these logs are the primary forensic artifact linking observed account compromises to the PhaaS platform. | Digital wallet provisioning API logs from your payment processor or mobile wallet provider (e.g., Apple Pay, Google Pay provisioning events): these logs record the device ID, IP, geolocation, and network token ID assigned at provisioning — essential for identifying attacker-controlled devices and initiating token revocation with Visa/Mastercard. | DNS query logs and web proxy logs showing client resolution of and navigation to newly registered domains (under 30 days old) immediately following receipt of an iMessage or RCS deep-link — this reconstructs the victim's path from lure delivery through the Darcula phishing kit to OTP submission. | Web server access logs and WAF logs for your OTP submission endpoint: filter for POST requests where the Referer or Origin header matches an external, non-organizational domain — these indicate the OTP was submitted via a Darcula reverse-proxy page rather than your legitimate portal. | Card network tokenization service records for any network tokens (Visa Token Service / Mastercard Digital Enablement Service) provisioned to new devices in the incident window: Darcula's platform automates card-to-wallet loading, so token provisioning records at the network level may capture attacker device fingerprints not visible in your own logs.

Per-Action IR Details

Step 1: Containment — Audit all externally exposed applications for SMS/TOTP-only MFA and flag them as elevated risk. Per CIS 6.3, enforce MFA on all externally exposed applications; per NIST IA-2, ensure authentication mechanisms cannot be bypassed via OTP interception. Temporarily increase friction (step-up authentication, out-of-band confirmation) on high-value financial transactions and account changes while longer-term controls are evaluated.

NIST Phase: Containment

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

Controls: NIST IA-2 (Identification and Authentication — Organizational Users), NIST IA-2(1) (Identification and Authentication — Multi-Factor Authentication to Privileged Accounts), NIST AC-7 (Unsuccessful Logon Attempts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams without an IAM platform: export your IdP or application user directory and run a grep/PowerShell audit against MFA enrollment records — e.g., in Azure AD use `Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0}` to enumerate accounts with no MFA enrolled. For SMS/TOTP-enrolled

accounts you cannot immediately migrate, enable step-up prompts by adding conditional access rules (if free-tier Azure AD, use Security Defaults) that require re-authentication on wallet-linking or payment initiation events. Document all flagged accounts in a shared spreadsheet with owner and remediation deadline.

Evidence: Before implementing friction changes, snapshot the current MFA enrollment state for all externally exposed apps: export IdP MFA enrollment reports, capturing each account's enrolled factor type (SMS, TOTP app, FIDO2, push). Collect authentication event logs for the 30 days preceding action, filtering for sessions originating from Apple iMessage or RCS deep-link referrers (check web server access logs and auth platform logs for Referer headers and user-agent strings consistent with iOS Messages or Android Messages apps). Preserve these logs to establish a pre-containment baseline for Darcula/Lucid relay-pattern comparison.

Step 2: Detection — Query email and messaging security gateways for iMessage-origin and RCS-origin links resolving to newly registered domains (registered within 30 days). Review authentication logs (NIST AU-2, AU-6) for OTP submission sequences where the OTP is used within seconds of issuance and is immediately followed by account change, payment initiation, or wallet-linking events — this pattern is consistent with real-time relay. Alert on digital wallet provisioning events from unfamiliar devices or geolocations. Cross-reference against Darcula/Lucid infrastructure IOCs from GTIG reporting.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM: use `jq` or Python pandas to parse raw authentication JSON/CSV logs and calculate OTP issuance-to-use delta times — flag any OTP used in under 15 seconds followed within 60 seconds by a wallet-link or account-change event. For domain age checks on URLs observed in gateway logs, script bulk WHOIS lookups using `python-whois` against extracted domains and flag registrations under 30 days old. Pull Darcula/Lucid IOC lists from GTIG's public reporting and load into a local Pi-hole or firewall ACL for blocking. Use Wireshark with a display filter of `http.request.method == POST && http.host matches ""` on egress taps to catch relay callbacks if network monitoring is available.

Evidence: Capture the following before tuning detection rules: (1) Full authentication event logs from your IdP or app auth layer showing OTP issuance timestamps and OTP submission timestamps — essential for calculating relay latency specific to Darcula's real-time interception model. (2) DNS query logs from your resolver showing lookups for domains registered within 30 days that were accessed immediately after an iMessage or RCS link click (correlate with mobile device management or proxy logs). (3) Digital wallet provisioning API logs or payment gateway logs showing device fingerprint, geolocation, and provisioning timestamp for all wallet-link events in the preceding 60 days. (4) Any WAF or reverse proxy logs showing POST requests to OTP submission endpoints with anomalously short time-to-submit values.

Step 3: Eradication — Migrate high-risk accounts from SMS/TOTP OTP to FIDO2/passkey authentication, which is phishing-resistant and not interceptable via relay (NIST IA-2(1), D3-MFA). Implement origin-binding for authentication sessions to detect relay attacks: the session origin presented to the relying party must match the origin presented during authentication. Block or scrutinize digital wallet provisioning requests that do not originate from a previously trusted device (D3-CH, D3-CRO). Revoke and rerotate any credentials or session tokens associated with accounts flagged in detection step (NIST AC-2, D3-CRO).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-2(1) (Identification and Authentication — Multi-Factor Authentication to Privileged Accounts), NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST SC-8 (Transmission Confidentiality and Integrity), 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: For teams without an enterprise IAM rollout budget: use WebAuthn/passkey libraries (e.g., `py_webauthn` for Python backends or `SimpleWebAuthn` for Node.js) to add FIDO2 support to consumer-facing portals at low cost — both are open source. For origin-binding enforcement without a WAF, implement server-side checks in your auth handler that compare the `Origin` header on OTP submission requests against the registered origin for the session and reject mismatches with a 403. To revoke compromised sessions at scale, script forced session invalidation using your IdP's API (e.g., Azure AD `Revoke-AzureADUserAllRefreshToken`, or Keycloak admin REST API `DELETE /sessions/{id}`) for all accounts flagged in Step 2.

Evidence: Before revoking sessions and rotating credentials, preserve: (1) A full export of active session tokens and refresh tokens for flagged accounts from your IdP, including device ID, IP, and session creation timestamp — this establishes what the attacker may have harvested via Darcula's relay infrastructure. (2) Digital wallet provisioning records for flagged accounts including the tokenized card data references (PAN tokens, network token IDs from Visa/Mastercard tokenization services) so you can notify the relevant card networks to revoke those tokens. (3) Logs of any account changes (email, phone, password reset) made by flagged accounts in the window between OTP relay and detection — these are the downstream actions Darcula's platform automates post-interception.

Step 4: Recovery — After control changes, validate that phishing-resistant MFA is enforced end-to-end with no SMS/TOTP fallback path remaining (NIST IA-2, CIS 6.3, CIS 6.5). Confirm digital wallet provisioning workflows require device trust attestation. Monitor authentication logs (NIST AU-6) for residual relay-pattern anomalies for a minimum of 30 days post-remediation. Verify session binding controls are functioning by testing from a proxied session.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IA-2 (Identification and Authentication — Organizational Users), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), NIST CA-7 (Continuous Monitoring), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without automated compliance tooling: manually test for SMS/TOTP fallback paths by attempting account recovery flows, password resets, and new device enrollment from a clean browser session — document every path that still allows OTP as a factor. For proxied-session relay testing, use Burp Suite Community Edition (free) to intercept an authentication session and manually modify the `Origin` header on the OTP submission request — a correctly implemented origin-binding control must reject this with a 403. For 30-day post-remediation monitoring without a SIEM, schedule a daily cron job that runs your OTP relay latency detection script (from Step 2) against the previous day's auth logs and emails the output to the security team.

Evidence: During recovery validation, collect: (1) Screenshots and session recordings of each tested authentication flow confirming no SMS/TOTP fallback path survives — these serve as audit evidence of remediation completeness. (2) Web server and auth platform logs from proxied-session relay tests showing the 403 rejection of mismatched-origin OTP submissions — confirms origin-binding is enforced. (3) Ongoing daily auth log snapshots for the 30-day monitoring window, specifically the OTP relay latency dataset, preserved as evidence of post-remediation clean baseline for any future regulatory inquiry or PCI DSS audit related to the compromised payment card data.

Step 5: Post-Incident — Conduct a gap assessment against NIST SP 800-53 IA-2 and AC-17 to identify remaining OTP-based authentication paths in production. Evaluate whether consumer-facing brand monitoring and typosquat detection (NIST AU-13) are in place to identify cloned pages before victims reach them. Document findings and update the authentication section of your incident response playbook to include PhaaS relay scenarios. Consider threat-sharing with sector peers via ISAC channels if your organization is in financial services, e-commerce, or securities.

NIST Phase: Post Incident

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

Controls: NIST IA-2 (Identification and Authentication — Organizational Users), NIST AC-17 (Remote Access), NIST AU-13 (Monitoring for Information Disclosure), 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 brand monitoring without a commercial service: set up free Google Alerts for your organization's name combined with terms like 'login', 'verify', 'payment', 'OTP', and 'account' to catch indexed phishing pages. Use `dnstwist` (open source, pip-installable) to generate typosquat permutations of your domain and run weekly WHOIS lookups against the list — flag any newly registered permutation for manual review. For ISAC sharing without a formal membership, FS-ISAC and the Retail and Hospitality ISAC both publish public threat advisories; submit IOCs from your investigation via their public intake portals. Document the Darcula/Lucid relay attack chain in your playbook using MITRE ATT&CK T1557 (Adversary-in-the-Middle), T1566.002 (Spearphishing Link via messaging), and T1111 (Multi-Factor Authentication Interception) as the canonical technique references.

Evidence: For the post-incident lessons-learned record, preserve: (1) The complete gap assessment output listing every OTP-based authentication path found in production, with owning system, user population size, and remediation status — this is the baseline for IA-2 compliance tracking. (2) Any Darcula/Lucid phishing kit artifacts or cloned page screenshots collected during the incident, which can be submitted to Google Safe Browsing and FS-ISAC for broader protection. (3) A documented timeline from first phishing link observed to OTP relay to wallet provisioning event, specific to your environment — this dwell-time and attack-velocity data is critical for calibrating future detection thresholds for PhaaS relay patterns.

Detection Guidance

Primary behavioral indicators: (1) OTP relay pattern, authentication log entries where an OTP is submitted within 2-5 seconds of issuance, immediately followed by a high-privilege action (payment, wallet link, account update); log sources: identity provider authentication logs, application-layer transaction logs per NIST AU-2 and AU-3. (2) Digital wallet provisioning from unrecognized devices or atypical geolocations, payment platform and mobile wallet provisioning logs. (3) Smishing delivery indicators, iMessage and RCS links to domains registered within the last 30 days, particularly those resolving to dynamic brand-clone pages; sources: DNS query logs, proxy/web gateway logs. (4) Session anomalies suggesting cookie theft (T1539), same session token used from two distinct IP addresses within a short window; sources: web application and load balancer access logs. NIST AU-6 mandates regular log review and analysis for exactly these behavioral patterns. CIS 8.2 requires audit log collection to be enabled across enterprise assets as a prerequisite. IOC enrichment: cross-reference domain and infrastructure indicators published in the GTIG report (source URL above) and Netcraft's Darcula tracking. Label any matches as medium confidence pending behavioral corroboration.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Darcula/Lucid infrastructure domains — see GTIG report for current list`	Dynamically generated brand-clone phishing domains used in smishing delivery; rotate frequently	MEDIUM
URL	`https://cloud.google.com/blog/topics/threat-intelligence/chinese-language-phishing-services/`	GTIG primary source — current IOC list published here; retrieve directly for up-to-date indicators	HIGH

Framework Mappings

MITRE-ATTACK

- **T1621** — Multi-Factor Authentication Request Generation
- **T1598.004** — Spearphishing Voice
- **T1185** — Browser Session Hijacking
- **T1608.005** — Link Target
- **T1556** — Modify Authentication Process
- **T1566.004** — Spearphishing Voice
- **T1056.003** — Web Portal Capture
- **T1111** — Multi-Factor Authentication Interception
- **T1539** — Steal Web Session Cookie
- **T1583.001** — Domains
- **T1566** — Phishing
- **T1557** — Adversary-in-the-Middle

NIST-800-53R5

- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **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
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1598.004	Spearphishing Voice	Reconnaissance
T1185	Browser Session Hijacking	Collection
T1608.005	Link Target	Resource-Development
T1556	Modify Authentication Process	Credential-Access
T1566.004	Spearphishing Voice	Initial-Access
T1056.003	Web Portal Capture	Collection
T1111	Multi-Factor Authentication Interception	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1583.001	Domains	Resource-Development
T1566	Phishing	Initial-Access
T1557	Adversary-in-the-Middle	Credential-Access

Sources

Source	URL	Tier
Threat Intelligence	https://cloud.google.com/blog/topics/threat-intelligence/chinese-la...	T3
'darcula' iMessage and RCS smishing attacks target USPS ... - Netcraft	https://www.netcraft.com/blog/darcula-smishing-attacks-target-usps-...	T2

Source	URL	Tier
Dracula Phishing Attacks Targets Organizations Worldwide	https://fidelissecurity.com/threatgeek/threat-intelligence/darcula-...	T3
Darcula Phishing Network Leveraging RCS and iMessage to Evade ...	https://thehackernews.com/2024/03/darcula-phishing-network-leveragi...	T3
'Lucid' Phishing Tool Exploits Faults in iMessage, RCS - Dark Reading	https://www.darkreading.com/threat-intelligence/lucid-phishing-expl...	T3

Generated 2026-05-25 06:03 UTC by TJS Security Command Center