INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-04 06:47 UTC

# Pig Butchering Losses Hit $7.2B in 2025 as DOJ-Led Disruption Week Targets Southeast Asia Scam Infrastructure

**THREAT CAMPAIGN** | **HIGH** | CVSS 5.0

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0405 |
| **Type** | Threat Campaign |
| **Severity** | HIGH |
| **CVSS Base Score** | 5.0 |
| **Affected Products** | General population targeted via Facebook, Instagram, Microsoft accounts; Starlink/SpaceX kits used as communication infrastructure; Coinbase, Meta, Google, Apple platforms exploited as lure vectors, no specific software vulnerabilities identified |
| **Published** | 2026-06-04T02:06:25 |
| **Discovery Source** | Rss |

## Executive Summary

A U.S. government-led operation designated 'Disruption Week' (May 18, 2026) dismantled over 1.4 million criminal accounts tied to Southeast Asia-based pig butchering fraud networks, with participation from Meta, Microsoft, SpaceX, Coinbase, Google, and Apple. These scams, which manipulate victims into fraudulent cryptocurrency investments through fabricated relationships, cost U.S. victims $7.2 billion in 2025, a 24% increase year-over-year. The primary business risk is employee victimization through social engineering on platforms your organization uses daily, with secondary risk from reputational and financial exposure when employees or customers are targeted using your brand as a lure.

## Technical Analysis

Pig butchering (sha zhu pan) operations are fraud-as-a-service networks, not software exploits. No CVE is associated. The CWE-1021 classification (Improper Restriction of Rendered UI Layers) reflects the deceptive interface design of fraudulent cryptocurrency investment platforms that mimic legitimate exchanges. MITRE techniques observed: T1090 (Proxy), T1586 (Compromise Accounts), T1583.001 (Acquire Infrastructure: Domains), T1534 (Internal Spearphishing), T1585 (Establish Accounts), T1657 (Financial Theft), T1583.006 (Acquire Infrastructure: Web Services), T1566 (Phishing), T1531 (Account Access Removal). Operators used Starlink satellite kits to maintain connectivity from scam compounds in Southeast Asia, bypassing traditional ISP-level disruption. Fraudulent platforms were distributed via Meta, Instagram, and Microsoft platforms using

compromised and synthetic accounts. The operation froze $3.8 million in cryptocurrency and resulted in seven arrests in Thailand. Starlink IP ranges (AS14593) may appear in authentication logs if victims are contacted from scam compounds, but this indicator is low-confidence and high-noise; do not use for alerting or blocking without corroborating behavioral indicators. Patch status: not applicable, no software vulnerability to remediate.

## Action Checklist

1. Step 1: Awareness, brief your workforce on pig butchering social engineering patterns: unsolicited contact on LinkedIn, Facebook, Instagram, or WhatsApp leading to cryptocurrency investment platforms, often involving fabricated romantic or professional relationships. Focus on employees with financial authority or access to corporate accounts.
2. Step 2: Detection, monitor corporate email and collaboration platforms for inbound social engineering indicators: accounts created recently, unsolicited messages referencing cryptocurrency investment opportunities, and links to domains registered within the past 90 days. Query email gateway logs for domains impersonating Coinbase, Binance, or similar exchanges. Flag use of personal crypto wallets on corporate devices (NIST AC-3, AU-2).
3. Step 3: Eradication, if an employee has engaged with a suspected pig butchering platform, treat it as a social engineering incident: isolate any corporate accounts or credentials that may have been disclosed, revoke active sessions (NIST AC-12), rotate credentials (D3-CRO), and review financial transaction logs for unauthorized wire or crypto transfers.
4. Step 4: Recovery, verify no corporate financial accounts or credentials were compromised. Review access logs for anomalous authentication activity from the affected employee's accounts (NIST AU-6). Confirm MFA is enforced on all externally exposed applications (CIS 6.3) and administrative accounts (CIS 6.5). Validate that account inventory reflects current authorized users (CIS 5.1).
5. Step 5: Post-Incident, assess gaps in employee security awareness training specific to financial fraud and social engineering (NIST AC-1, AU-1 for policy). Evaluate whether your acceptable use policy addresses personal cryptocurrency activity on corporate devices. Consider adding pig butchering scenarios to tabletop exercises. Review third-party platform risk exposure for Meta, Microsoft, and Google services used in your environment (NIST AC-20).

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | URGENT |
| **Escalation Criteria** | Escalate immediately to legal counsel, HR, and executive leadership if any corporate financial transaction (wire transfer, ACH, crypto transfer) was authorized by the affected employee during the engagement period, or if the employee disclosed credentials to corporate banking, payroll, or treasury systems — this triggers potential FinCEN SAR filing obligations and cyber insurance notification requirements; escalate to FBI IC3 if confirmed financial loss exceeds any threshold reportable under your cyber insurance policy. |

| | |
|---|---|
| **Recovery Notes** | Post-containment, monitor the affected employee's corporate accounts for 30 days for re-engagement attempts — pig butchering operators frequently re-contact victims posing as law enforcement or 'recovery scam' services offering to retrieve lost funds, which constitutes a second-stage fraud attempt. Verify with your financial institution that all outbound wire and ACH templates accessible to the affected employee's credentials have been audited and that no new beneficiaries were added during the engagement window. If the employee accessed the fraudulent platform from a corporate device, perform a browser artifact review (history, saved passwords, autofill data) to confirm no corporate credentials were stored in the fraudulent platform's login form. |
| **Forensic Artifacts** | Corporate email gateway logs (Exchange Message Trace, Google Workspace Admin Reports, or Proofpoint TRAP) showing inbound messages from newly registered domains impersonating Coinbase, Binance, or generic 'crypto investment' platforms — preserve with full headers and sender IP resolution before auto-purge window expires \| Azure AD or Google Workspace sign-in logs for affected employee covering 30–90 days prior to incident report — flag authentication events from IP ranges geolocating to Thailand, Myanmar, Cambodia, or Laos (primary DOJ-identified pig butchering operation locations) and any anomalous user agent strings indicating non-standard browser or mobile app access \| Corporate banking portal and ACH/wire transfer audit logs showing all outbound transfer authorizations, beneficiary additions, or template modifications made during the employee's engagement period with the fraudulent platform — required for FinCEN SAR filing and FBI IC3 referral \| Browser forensic artifacts from the employee's corporate device: Chrome SQLite history database at %LOCALAPPDATA%\Google\Chrome\User Data\Default\History and saved passwords at %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data — query for visits to the fraudulent crypto platform domain and check whether corporate credentials were autofilled into the platform's login form \| Screenshots and URL artifacts of the fraudulent investment platform itself, including the displayed wallet deposit address (Bitcoin, USDT/TRC-20, or ETH address) — submit these to the FBI IC3 Virtual Asset Unit and cross-reference against OFAC SDN cryptocurrency address lists and Chainalysis reactor (free tier) to determine if the wallet is linked to previously sanctioned pig butchering infrastructure identified during DOJ Disruption Week |

### Per-Action IR Details

**Step 1: Awareness — brief your workforce on pig butchering social engineering patterns: unsolicited contact on LinkedIn, Facebook, Instagram, or WhatsApp leading to cryptocurrency investment platforms, often involving fabricated romantic or professional relationships. Focus on employees with financial authority or access to corporate accounts.**

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2 — Preparation: Establishing IR Capability and Workforce Readiness

**Controls:** NIST AT-2 (Literacy Training and Awareness), NIST AT-3 (Role-Based Training), NIST IR-2 (Incident Response Training), NIST PM-14 (Testing, Training, and Monitoring), CIS 14.1 (Establish and Maintain a Security Awareness Program), CIS 14.2 (Train Workforce Members to Recognize Social Engineering Attacks)

**Compensating:** Distribute a one-page internal alert — formatted as a real phishing simulation debrief — describing the exact pig butchering contact sequence: initial unsolicited LinkedIn or Instagram DM, pivot to WhatsApp, introduction of a 'high-yield' crypto platform mimicking Coinbase or Binance, gradual trust-building before a large transfer request. Require acknowledgment via email reply. For financial-authority roles, conduct a 15-minute live walkthrough using screenshots from public DOJ Disruption Week press materials. No tooling required — calendar invite plus a shared drive PDF is sufficient for a 2-person team.

**Evidence:** Before conducting briefings, document the current baseline: capture a timestamped export of your HR roster identifying employees with wire transfer authority, corporate crypto wallet access, or access to treasury systems

— this establishes scope for downstream monitoring. Screenshot and archive any unsolicited social media messages already reported by employees referencing cryptocurrency investment opportunities, as these may constitute early-stage pig butchering contact attempts relevant to the DOJ Disruption Week campaign.

**Step 2: Detection — monitor corporate email and collaboration platforms for inbound social engineering indicators: accounts created recently (CIS 5.1), unsolicited messages referencing cryptocurrency investment opportunities, and links to domains registered within the past 90 days. Query email gateway logs for domains impersonating Coinbase, Binance, or similar exchanges. Flag use of personal crypto wallets on corporate devices (NIST AC-3, AU-2).**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis: Identifying Adverse Events and Precursors

**Controls:** NIST SI-3 (Malicious Code Protection), NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AC-3 (Access Enforcement), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 9.2 (Use DNS Filtering Services), CIS 13.3 (Deploy a URL Filter)

**Compensating:** Run the following PowerShell one-liner against Microsoft 365 Unified Audit Log to surface inbound messages referencing crypto investment terms: Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-30) -EndDate (Get-Date) -Operations 'Send,Receive' | Where-Object {$_.AuditData -match 'coinbase|binance|crypto|investment|wallet|usdt|btc'}. For domain-age checks on suspicious URLs extracted from email, query WHOIS via 'whois ' in bash or use the free MXToolbox WHOIS lookup to flag domains registered within 90 days. Use free Quad9 or Cloudflare Gateway DNS filtering to block known crypto-scam domains identified in DOJ Disruption Week takedown lists. For endpoint detection of personal crypto wallet installs (MetaMask browser extension, Exodus, Trust Wallet), run: Get-ItemProperty HKCU:\Software\Google\Chrome\Extensions -ErrorAction SilentlyContinue | Where-Object {$_.PSChildName -in @('nkbihfbeogaeaoehlefnkodbefgpgknn')} — the listed GUID is MetaMask's Chrome extension ID.

**Evidence:** Before actioning detections, preserve: (1) Full email headers and message body of any inbound messages referencing cryptocurrency investment platforms — export as .eml files from the mail gateway (Exchange Message Trace, Google Workspace Admin Audit, or Proofpoint logs) before auto-purge. (2) DNS query logs from corporate resolvers showing employee lookups of domains impersonating Coinbase (e.g., coinbase-pro[.]net, coinbasepro-login[.]com) or Binance — pull from Pi-hole query log at /var/log/pihole.log or from Windows DNS Server debug logs. (3) Browser history artifacts from corporate endpoints: Chrome history at %LOCALAPPDATA%\Google\Chrome\User Data\Default\History (SQLite), Firefox at %APPDATA%\Mozilla\Firefox\Profiles*.default\places.sqlite — query for visits to recently registered crypto-adjacent domains.

**Step 3: Eradication — if an employee has engaged with a suspected pig butchering platform, treat it as a social engineering incident: isolate any corporate accounts or credentials that may have been disclosed, revoke active sessions (NIST AC-12), rotate credentials (D3-CRO), and review financial transaction logs for unauthorized wire or crypto transfers.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication: Removing Threat and Preventing Reinfection

**Controls:** NIST AC-12 (Session Termination), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

**Compensating:** For Microsoft 365 environments, revoke all active sessions immediately via: Revoke-AzureADUserAllRefreshTokens -ObjectId followed by Set-AzureADUser -ObjectId -AccountEnabled $false if full lockout is warranted. For Google Workspace, use Admin Console > Users > [affected user] > Reset Sign-in Cookies. Force credential rotation by expiring the password immediately: Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText 'TempPass123!' -Force) then Set-ADUser -Identity -ChangePasswordAtLogon $true. Review corporate banking portal and ACH/wire transfer logs manually — contact your financial institution's fraud line to place a 24-hour hold on outbound wire transfers originating from the affected employee's authorized accounts while the review is in progress. No SIEM required — this is manual triage with native

admin consoles.

**Evidence:** Before revoking sessions, capture a timestamped snapshot of: (1) Azure AD or Google Workspace sign-in logs for the affected employee covering the 30 days prior to incident report — export as CSV from Azure AD Sign-ins blade or Google Admin Reports API, preserving IP addresses, user agents, and authentication timestamps that may indicate adversary session hijacking or credential reuse by pig butchering operators. (2) Corporate financial platform audit trails — export transaction logs from the banking portal, payroll system, or AP platform showing all outbound wire, ACH, or crypto transfer authorizations tied to the affected employee's credentials. (3) Screenshot or export of the pig butchering platform itself (URL, wallet address displayed, account balance shown) before the employee's account is closed — this constitutes material evidence for FBI IC3 reporting and DOJ referral consistent with Disruption Week asset seizure procedures.

**Step 4: Recovery — verify no corporate financial accounts or credentials were compromised. Review access logs for anomalous authentication activity from the affected employee's accounts (NIST AU-6). Confirm MFA is enforced on all externally exposed applications (CIS 6.3) and administrative accounts (CIS 6.5). Validate that account inventory reflects current authorized users (CIS 5.1).**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery: Restoring Systems and Verifying Integrity

**Controls:** NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AC-2 (Account Management), NIST IA-2 (Identification and Authentication — Organizational Users), NIST IA-5 (Authenticator Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

**Compensating:** Pull the last 30 days of Microsoft 365 sign-in logs via PowerShell: Get-AzureADAuditSignInLogs -Filter "userPrincipalName eq '<user@domain>'" | Select-Object CreatedDateTime, IpAddress, ClientAppUsed, ConditionalAccessStatus | Export-Csv signin_review.csv — flag any IPs geolocating to Southeast Asia (Thailand, Myanmar, Cambodia, Laos — primary pig butchering operation locations per DOJ Disruption Week findings) using a free MaxMind GeoLite2 lookup. For MFA enforcement verification across all M365 accounts, run: Get-MsolUser -All | Where-Object {$_.StrongAuthenticationRequirements.Count -eq 0} | Select-Object UserPrincipalName — any returned accounts without MFA enforced are recovery gaps. Cross-reference against CIS 5.1 account inventory to confirm no accounts were created by the adversary during the social engineering engagement.

**Evidence:** Before declaring recovery complete, preserve: (1) The final sign-in log export for the affected employee showing the last 30–90 days of authentication events, annotated with any sessions originating from IP ranges associated with Southeast Asian scam infrastructure — this log is required for any subsequent FBI IC3 or FinCEN Suspicious Activity Report (SAR) filing. (2) A before/after screenshot comparison of the corporate account inventory (CIS 5.1) confirming no unauthorized accounts were provisioned. (3) MFA enrollment status report exported from your identity provider (Azure AD, Okta, or Google Workspace) as a dated artifact confirming post-incident enforcement state — required if the organization is subject to cyber insurance claims or regulatory notification obligations triggered by financial fraud losses.

**Step 5: Post-Incident — assess gaps in employee security awareness training specific to financial fraud and social engineering (NIST AC-1, AU-1 for policy). Evaluate whether your acceptable use policy addresses personal cryptocurrency activity on corporate devices. Consider adding pig butchering scenarios to tabletop exercises. Review third-party platform risk exposure for Meta, Microsoft, and Google services used in your environment (NIST AC-20).**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity: Lessons Learned and Program Improvement

**Controls:** NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AT-2 (Literacy Training and Awareness), NIST AC-20 (Use of External Systems), NIST AC-1 (Policy and Procedures), NIST PM-16 (Threat Awareness Program), CIS 14.1 (Establish and Maintain a Security Awareness Program), CIS 15.2 (Establish and Maintain a Process to Accept and Address Software Vulnerabilities)

**Compensating:** Conduct a 60-minute tabletop exercise specifically scripted around the pig butchering attack chain documented in DOJ Disruption Week materials: scenario begins with an employee receiving a LinkedIn connection

request from a fabricated financial advisor persona, progresses through WhatsApp pivot, fake Coinbase-lookalike platform onboarding, and culminates in a wire transfer request to a Southeast Asia-controlled wallet. Use free CISA tabletop templates (available at cisa.gov/resources-tools/resources/tabletop-exercise-packages) as the exercise framework. Update the Acceptable Use Policy with an explicit clause prohibiting access to personal cryptocurrency trading platforms, wallet applications, or investment platforms from corporate devices or accounts — reference the $7.2B 2025 U.S. victim loss figure from DOJ Disruption Week reporting as the documented threat basis in the policy rationale section. For third-party platform risk under NIST AC-20, document which Meta (Facebook/Instagram), Microsoft (LinkedIn/Teams), and Google (Gmail/Chat) services are sanctioned in your environment and add pig butchering social engineering as an explicit risk scenario in your third-party risk register.

**Evidence:** For the lessons learned record required by NIST 800-61r3 §4, preserve and attach: (1) The original employee report or complaint that initiated the incident, including any screenshots of the pig butchering operator's social media profile and the fraudulent investment platform UI — these document the specific campaign TTPs for future threat intelligence use. (2) Timeline reconstruction showing first contact date, escalation to corporate account access or financial transaction risk, and detection date — gap between first contact and detection is the key metric for awareness program effectiveness measurement. (3) If financial loss occurred, file FBI IC3 report at ic3.gov and retain the submission confirmation number — this directly supports DOJ Disruption Week successor operations targeting the Southeast Asia scam networks responsible for the $7.2B in 2025 U.S. losses.

## Detection Guidance

No exploit-based IOCs are available for this campaign type. Detection focuses on behavioral and social engineering indicators. Monitor for: (1) inbound messages from newly created or recently compromised social media accounts referencing cryptocurrency investments, cross-reference account creation dates against contact initiation dates; (2) DNS queries or proxy logs showing access to cryptocurrency platforms not on your approved vendor list (NIST AC-4, AU-2); (3) financial system anomalies, wire transfers or ACH transactions to cryptocurrency exchanges initiated by individual employees without standard approval workflows; (4) account takeover indicators on corporate Microsoft or Meta-connected accounts: login from new geography, new device, or unusual time (NIST AU-9, D3-LAM). No confirmed domain, IP, or hash IOCs are available for this campaign from any source; detection must focus on behavioral and account indicators.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| URL | `Not available` | No confirmed IOC list has been published from the Disruption Week operation at the T3 source quality available. Do not act on unverified IOC lists circulating informally. | LOW |

## Framework Mappings

**MITRE-ATTACK**

- **T1090** — Proxy
- **T1586** — Compromise Accounts
- **T1583.001** — Domains

- **T1534** — Internal Spearphishing
- **T1585** — Establish Accounts
- **T1657** — Financial Theft
- **T1583.006** — Web Services
- **T1566** — Phishing
- **T1531** — Account Access Removal

**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

**CIS-V8**

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1090 | Proxy | Command-And-Control |
| T1586 | Compromise Accounts | Resource-Development |
| T1583.001 | Domains | Resource-Development |
| T1534 | Internal Spearphishing | Lateral-Movement |
| T1585 | Establish Accounts | Resource-Development |
| T1657 | Financial Theft | Impact |
| T1583.006 | Web Services | Resource-Development |
| T1566 | Phishing | Initial-Access |
| T1531 | Account Access Removal | Impact |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://thehackernews.com/2026/06/doj-disrupts-southeast-asia-crypt... | T3 |

| Source | URL | Tier |
|---|---|---|
| **SpaceX, FBI Crack Down on Scammers Using Starlink to ...** | https://www.pcmag.com/news/spacex-fbi-crack-down-on-scammers-using-... | T3 |
| **Meta Took Down Over A Million Scam Accounts In Joint ...** | https://www.engadget.com/2186397/meta-took-down-over-a-million-scam... | T3 |
| **Now cybersecurity researchers are working to release a list ...** | https://www.facebook.com/forbes/posts/now-cybersecurity-researchers... | T3 |
| **Data Breach 2025: Meta, Coinbase, AT&T, Google, Apple ...** | https://www.trendlife.com/en-us/blog/2025/05/22/meta-coinbase-att-g... | T3 |



Generated 2026-06-04 06:47 UTC by TJS Security Command Center