INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-08 06:21 UTC

FBI IC3 2025 Annual Report: $21 Billion in U.S. Cybercrime Losses, New Enterprise Risk Baseline

SECURITY ANALYSIS | CRITICAL | CVSS 7.5

SCC Item ID	SCC-STY-2026-0050
Type	Security Analysis
Severity	CRITICAL
CVSS Base Score	7.5
Affected Products	No specific products or versions. Sectors affected: healthcare, manufacturing, financial services, information technology, government facilities, and broader critical infrastructure.
Published	2026-04-07T16:41:52
Discovery Source	Rss

Executive Summary

The FBI IC3 2025 Annual Report records nearly $21 billion in U.S. cybercrime losses, a 26% increase over 2024's $16.6 billion, driven by cryptocurrency investment fraud, AI-enabled social engineering, and business email compromise. Elder fraud and critical infrastructure attacks escalated sharply, with sectors including healthcare, financial services, and manufacturing absorbing disproportionate impact. For boards and CISOs, this report resets the enterprise risk baseline: the fraud and authentication-bypass techniques underlying these losses are no longer edge cases, they are the dominant threat pattern requiring calibrated investment in detection, awareness, and identity controls.

Technical Analysis

The IC3 2025 report is not a single incident post-mortem; it is a statistical portrait of the threat landscape across millions of complaints, and its findings carry significant operational weight for security teams building or validating their threat models.

Three loss drivers dominate. Cryptocurrency investment fraud, often called 'pig butchering,' accounts for the largest share of dollar losses. These schemes combine long-duration social engineering with fraudulent investment platforms, exploiting trust built over weeks or months before the financial extraction occurs. MITRE ATT&CK techniques T1598 (spearphishing for information), T1566 and T1566.002 (phishing and spearphishing via service), and T1656 (impersonation) map directly to the front-end of these campaigns. T1583.006 (web services acquisition) reflects the infrastructure these operators build or rent to host fraudulent platforms.

AI-enabled social engineering has materially lowered the barrier to convincing fraud. Attackers are using generative AI to produce high-quality phishing lures, deepfake voice and video for executive impersonation, and automated social media personas for relationship-building at scale. T1588.007 (artificial intelligence) appears in the technique set, signaling that AI is no longer a theoretical amplifier but an observed operational tool. CWE-1021 (UI redress and clickjacking patterns) reflects the delivery layer: fraudulent interfaces designed to obscure what a victim is actually authorizing.

Business email compromise remains a high-frequency, high-dollar attack category. The technique relies on CWE-287 authentication failures and account takeover, followed by T1534 (internal spearphishing) to extend compromise laterally within organizations. Once an email account is controlled, attackers redirect wire transfers, intercept invoice chains, or impersonate executives to authorize fraudulent payments. BEC losses are consistently undercounted because many organizations do not report, meaning the $21 billion figure likely understates actual impact.

Critical infrastructure targeting escalated, with healthcare, manufacturing, and government facilities among the most affected sectors. Ransomware remains the primary mechanism against these sectors, with groups including FIN7, Lazarus Group, and Scattered Spider named in threat actor attribution. Scattered Spider in particular has demonstrated a pattern of social engineering help desks to reset MFA and gain initial access, exploiting CWE-693 protection mechanism failures at the human layer rather than the technical one. T1204 and T1204.001 (user execution) and T1565 (data manipulation) round out the post-access phase.

For security teams, the report's CWE pattern tells a consistent story: attackers are not primarily exploiting novel zero-days. They are exploiting authentication gaps, human susceptibility, and inadequate fraud controls. The defensive implication is that MFA hardening, phishing-resistant authentication standards (FIDO2/passkeys), and user awareness programs targeting financial transaction verification carry outsized return on investment against the dominant loss categories documented here.

The report's priority score and flash designation reflect its value as a sector-wide calibration document. Security leaders who have not updated their threat models to incorporate AI-assisted fraud, cryptocurrency scam infrastructure, and BEC-specific detection logic are working from an outdated baseline.

Action Checklist

1. Step 1: Assess exposure, identify which of your user populations (finance teams, executives, employees nearing retirement) are most exposed to BEC, investment fraud, and AI-generated social engineering; these are your highest-risk segments per IC3 loss patterns
2. Step 2: Review controls, audit MFA deployment for completeness and phishing resistance; FIDO2 or hardware tokens are the appropriate control against BEC account takeover; SMS-based MFA does not adequately address the authentication failures (CWE-287) driving these losses
3. Step 3: Review controls, verify that wire transfer and payment authorization workflows require out-of-band confirmation; BEC losses persist because process controls are absent even when technical controls are in place
4. Step 4: Update threat model, incorporate AI-enabled social engineering as an active threat vector; update your phishing simulation program to include deepfake voice and video scenarios; add pig-butchering and investment fraud targeting of employees to your insider-risk-adjacent threat register
5. Step 5: Update threat model, map Scattered Spider, FIN7, and Lazarus Group TTPs to your current detection coverage using MITRE ATT&CK; prioritize gaps in T1566, T1598, T1534, and T1204 detection

logic

6. Step 6: Communicate findings, brief finance leadership and the board using the IC3 dollar figures as anchors; $21 billion in industry losses with a 26% year-over-year increase is a credible risk quantification argument for control investment

7. Step 7: Monitor developments, track IC3 complaint portal updates and CISA advisories for sector-specific follow-on reporting; the IC3 report is annual but CISA publishes interim alerts when campaign activity against specific sectors intensifies

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal, finance leadership, and external IR counsel if any wire transfer is identified that was authorized via email-only confirmation without out-of-band verification, if Microsoft 365 or Google Workspace audit logs show unauthorized MailItemsAccessed or forwarding rules on finance or executive accounts, or if an employee reports contact consistent with pig-butchering recruitment or AI voice impersonation of a senior executive — any of these conditions indicates active BEC campaign activity rather than preparatory exposure, and may trigger breach notification obligations under state privacy laws or GLBA/HIPAA depending on sector.
Recovery Notes	Following any confirmed BEC incident, immediately revoke and reissue all credentials for compromised accounts, audit and remove any inbox rules or OAuth application grants created during the intrusion window, and notify your financial institution within 24 hours to initiate a SWIFT recall or ACH reversal — the FBI's Internet Crime Complaint Center (IC3.gov) financial fraud kill chain requires rapid reporting to maximize fund recovery probability. Monitor the affected accounts and all accounts in the same department for anomalous authentication, mail access, and payment activity for a minimum of 30 days post-containment, as BEC actors frequently maintain persistent access through secondary footholds or re-compromise via the same social engineering vector. Conduct a structured lessons-learned review per NIST 800-61r3 §4 within two weeks of containment, specifically documenting whether the process control gaps identified in Step 3 were the proximate cause — this review should directly update your BEC playbook and wire transfer authorization policy.

Forensic Artifacts	Microsoft 365 Unified Audit Log — MailItemsAccessed, Send, UpdateInboxRules, and Add-MailboxPermission operations for finance and executive accounts: BEC actors establish forwarding rules and delegate access to maintain visibility into payment conversations; these operations are the primary forensic evidence of account compromise in M365 BEC campaigns | Email gateway logs (Exchange Transport Rules log or equivalent) — filter for messages with external reply-to headers that differ from the From address, lookalike sender domains (e.g., company-name with Unicode substitutions or transposed characters), and inbound messages containing wire transfer or banking change keywords targeting finance department recipients | Azure AD or Okta sign-in logs — authentication events with MFA not satisfied, token refresh anomalies, impossible travel (authentication from two geographically distant IPs within a short window), and legacy authentication protocol usage (IMAP, POP3, SMTP AUTH) which BEC actors use to bypass MFA via CWE-287 exploitation | Accounts payable system audit trail — all wire transfer and ACH requests received in the prior 12 months with authorization method documented; any transaction where vendor banking details were modified within 30 days of payment execution, and any transaction authorized exclusively via email with no documented callback confirmation, are primary forensic evidence of successful BEC payment fraud | VoIP or telephony call logs — for AI voice deepfake and vishing incidents: capture call detail records (CDRs) for calls received by finance staff and executives, including caller ID, call duration, and timestamps; cross-reference with any reported urgent payment requests to identify the social engineering contact event that preceded fraudulent wire transfer authorization

Per-Action IR Details

Step 1: Assess exposure — identify which of your user populations (finance teams, executives, employees nearing retirement) are most exposed to BEC, investment fraud, and AI-generated social engineering; these are your highest-risk segments per IC3 loss patterns

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and identifying high-risk asset/user populations before incidents occur

Controls: NIST IR-4 (Incident Handling) — ensure incident handling capability accounts for fraud-vector incidents, not only technical intrusions, NIST RA-2 (Security Categorization) — classify user populations by risk exposure to BEC and social engineering consistent with IC3 loss patterns, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — account inventory must tag high-privilege financial approvers, executives, and retirement-age employees as elevated-risk segments for BEC targeting, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — map asset ownership to high-risk user segments so BEC exposure can be scoped to systems with payment authority

Compensating: Export Active Directory user list with department and title attributes using PowerShell: `Get-ADUser -Filter * -Properties Department,Title,EmailAddress | Export-Csv users.csv`. Cross-reference against finance, executive, and HR org charts to manually tag BEC-high-risk accounts. Use this list to scope awareness campaign and to prioritize MFA enforcement order — no SIEM required.

Evidence: Before conducting exposure assessment, capture a baseline of existing phishing simulation results and any historical email gateway logs showing BEC-pattern indicators: messages with lookalike sender domains (e.g., finance@c0mpany.com vs finance@company.com), external reply-to header mismatches, and urgency keywords ('wire transfer', 'invoice', 'CEO request'). On Microsoft 365 environments, query Unified Audit Log for MailItemsAccessed and Send operations by finance and executive accounts over the prior 90 days to establish a baseline before any attacker has reason to change behavior.

Step 2: Review controls — audit MFA deployment for completeness and phishing resistance; FIDO2 or hardware tokens are the appropriate control against BEC account takeover; SMS-based MFA does not adequately address the authentication failures (CWE-287) driving these losses

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Ensuring authentication controls are in place to reduce incident likelihood and impact for BEC-targeted accounts

Controls: NIST IA-2 (Identification and Authentication — Organizational Users) — enforce multi-factor authentication for all organizational users, with phishing-resistant methods required for high-risk roles, NIST IA-5 (Authenticator Management) — manage authenticator types; SMS OTP does not meet the bar for CWE-287 mitigation against adversary-in-the-middle and SIM-swap attacks used in BEC campaigns, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce MFA on all externally-exposed enterprise applications including Microsoft 365, Google Workspace, and VPN, prioritizing FIDO2 or hardware tokens for finance and executive accounts, CIS 6.5 (Require MFA for Administrative Access) — require phishing-resistant MFA for all administrative accounts without exception; Scattered Spider specifically targets help desk flows to bypass MFA

Compensating: Audit MFA enrollment gaps in Microsoft 365 without enterprise tooling using: `Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0} | Select-Object UserPrincipalName,Department | Export-Csv mfa_gaps.csv`. For Google Workspace, use the Admin SDK Reports API to export 2SV enrollment status. Free FIDO2 hardware tokens (e.g., YubiKey 5 Series) are approximately $25–$50 per unit; prioritize issuance to finance approvers and executives as the minimum viable deployment.

Evidence: Before remediating MFA gaps, document the current authentication state as forensic baseline: export Azure AD Sign-In Logs filtered for MFA not satisfied (authenticationRequirement: singleFactorAuthentication) and MFA interrupted (status: interrupted) for all finance and executive accounts over 90 days. Also capture any Conditional Access policy export to document what was enforced at time of any future incident. On-premises environments: collect Windows Security Event Log Event ID 4624 (logon success) with LogonType 3 (network) or 10 (remote interactive) for high-risk accounts — absence of MFA claim in token is your evidence of CWE-287 exposure.

Step 3: Review controls — verify that wire transfer and payment authorization workflows require out-of-band confirmation; BEC losses persist because process controls are absent even when technical controls are in place

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing process-level controls and verification procedures that reduce BEC fraud success rate independent of technical controls

Controls: NIST IR-4 (Incident Handling) — incident handling for BEC must include process control failures as a root cause category, not only technical compromise, NIST AC-3 (Access Enforcement) — enforce separation of duties in payment authorization workflows so no single compromised account can initiate and approve a wire transfer, NIST AC-5 (Separation of Duties) — require dual authorization for wire transfers above defined thresholds; a BEC actor with access to one account cannot unilaterally execute payment fraud, CIS 6.1 (Establish an Access Granting Process) — access to payment initiation and approval functions must be granted through a documented process that enforces role separation aligned to fraud-prevention requirements

Compensating: For teams without a formal GRC platform, document payment authorization workflows as a simple checklist enforced by finance policy: (1) all wire transfer requests received via email must be verbally confirmed via a pre-established phone number — not a number provided in the request email; (2) any change to vendor banking details requires dual approval and a 48-hour hold. Publish this policy to finance staff and log confirmation calls in a shared spreadsheet. This process control costs nothing and directly interrupts the IC3-documented BEC payment redirection pattern.

Evidence: Before process control remediation, extract the complete wire transfer authorization audit trail from your accounts payable system for the prior 12 months: identify all transactions where the payment authorization was received exclusively via email with no documented out-of-band confirmation. Flag any transactions where vendor banking details were changed within 30 days of payment. In Microsoft 365 environments, query Exchange Message Trace for emails to finance staff containing keywords 'wire transfer', 'ACH', 'bank account change', 'urgent payment' from external senders to establish a baseline volume and identify any historical BEC attempts.

Step 4: Update threat model — incorporate AI-enabled social engineering as an active threat vector; update your phishing simulation program to include deepfake voice and video scenarios; add pig-butchering and investment fraud targeting of employees to your insider-risk-adjacent threat register

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Updating threat models and training programs to reflect active threat vectors identified in current threat intelligence (IC3 2025 report)

Controls: NIST IR-2 (Incident Response Training) — training must be updated to include AI-generated voice and video deepfake scenarios, pig-butchering recruitment patterns, and AI-assisted spear-phishing content that bypasses traditional awareness training cues, NIST SI-5 (Security Alerts, Advisories, and Directives) — the IC3 2025 Annual Report constitutes a formal threat advisory that should drive updates to the organizational threat model and training curriculum, NIST RA-3 (Risk Assessment) — risk assessment must be updated to reflect AI-enabled social engineering as an active, high-loss threat vector rather than an emerging or theoretical one; IC3 loss figures provide quantitative risk anchoring, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — vulnerability management scope must expand to include human-layer vulnerabilities exploited by AI social engineering, tracked in the threat register alongside technical CVEs

Compensating: Phishing simulation platforms with free tiers (GoPhish — fully open source, self-hosted) can be extended with AI-themed lure templates. Draft simulation scenarios that mimic: (1) a CFO voice message requesting urgent wire transfer (reference the IC3 pattern of AI voice cloning); (2) a LinkedIn message from a 'recruiter' proposing a cryptocurrency investment opportunity (pig-butchering entry vector). Add a threat register entry in a shared spreadsheet with columns: Threat Actor, TTP, IC3 Loss Category, Current Detection Coverage, Gap — populated from IC3 2025 data and MITRE ATT&CK mappings.

Evidence: Before updating the threat model, audit existing phishing simulation campaign results to establish the current human-layer susceptibility baseline: capture click rates, credential submission rates, and MFA bypass rates by department and role. Also pull any help desk tickets tagged as 'suspicious call', 'impersonation', or 'unusual request' from the prior 12 months — these are likely undocumented AI social engineering precursors. Document this baseline so post-training improvement can be quantified against the IC3 risk anchor.

Step 5: Update threat model — map Scattered Spider, FIN7, and Lazarus Group TTPs to your current detection coverage using MITRE ATT&CK; prioritize gaps in T1566, T1598, T1534, and T1204 detection logic

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Using threat intelligence to validate and improve detection coverage against known threat actor TTPs before and during active threat campaigns

Controls: NIST SI-4 (System Monitoring) — system monitoring must include detection logic mapped to T1566 (Phishing), T1598 (Phishing for Information), T1534 (Internal Spearphishing), and T1204 (User Execution) as used by Scattered Spider, FIN7, and Lazarus Group against IC3-identified sectors, NIST IR-5 (Incident Monitoring) — track and document detection gaps against specific threat actor TTPs; absence of coverage for Scattered Spider's help desk social engineering or Lazarus Group's spearphishing infrastructure is a documented risk, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — audit log review must be tuned to surface indicators specific to FIN7 macro-laced document delivery (T1204.002) and Lazarus Group's use of T1566.001 spearphishing attachments targeting financial sector employees, CIS 8.2 (Collect Audit Logs) — ensure audit log collection is enabled and centralized for email gateway, endpoint, and identity systems as the minimum telemetry required to detect T1566 and T1598 activity from Scattered Spider, FIN7, and Lazarus Group

Compensating: Use the free MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) to layer Scattered Spider (G1015), FIN7 (G0046), and Lazarus Group (G0032) technique heatmaps against your current detection rules. Export gaps as a prioritized list. For T1566 detection without a SIEM, deploy Sysmon with the SwiftOnSecurity config and write Sigma rules for: process creation from Office application child processes (T1204.002 — FIN7 macro execution), PowerShell with encoded command arguments launched from email client processes, and DNS queries to newly-registered domains (Lazarus Group C2 pattern). Sigma rules can be converted to Windows Event Log queries and run manually via PowerShell if no SIEM is available.

Evidence: Before updating detection logic, export your current SIEM or endpoint detection rule inventory and cross-reference against the four prioritized ATT&CK technique IDs. For T1534 (Internal Spearphishing — Scattered Spider's post-compromise lateral phishing tactic), query Exchange or Google Workspace mail logs for emails sent between internal accounts that contain external-domain links or attachments — a pattern inconsistent with normal internal communication. For T1598 (Phishing for Information — credential harvesting), review proxy or DNS logs for user navigation to domains with high similarity scores to your company's SSO or Microsoft 365 login page (tools:

dnstwist for domain permutation analysis, free and open source).

Step 6: Communicate findings — brief finance leadership and the board using the IC3 dollar figures as anchors; $21 billion in industry losses with a 26% year-over-year increase is a credible risk quantification argument for control investment

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Using threat intelligence and loss data to drive organizational learning, risk communication, and control investment decisions

Controls: NIST IR-8 (Incident Response Plan) — the IR plan must include a stakeholder communication component; board and finance leadership briefings on IC3 loss data fulfill the risk communication requirement and support resource allocation for control gaps, NIST IR-6 (Incident Reporting) — while the IC3 report reflects industry-level incidents, this control's reporting culture should extend to proactive threat intelligence briefings that contextualize enterprise risk against observed loss patterns, NIST RA-3 (Risk Assessment) — IC3 2025 figures ($21B, 26% YoY increase, BEC as top loss category) provide authoritative external data points that must be incorporated into the organizational risk assessment to justify control investment, CIS 7.2 (Establish and Maintain a Remediation Process) — board-level risk communication using IC3 loss anchors directly supports the risk-based remediation prioritization process by providing quantitative justification for FIDO2 MFA, BEC process controls, and threat detection investment

Compensating: Construct a one-page board brief using only public IC3 data and your internal exposure assessment from Step 1. Structure: (1) IC3 2025 headline figures — $21B total loss, BEC as top loss category, 26% YoY increase; (2) your sector's specific IC3 loss ranking if applicable (healthcare, financial services, manufacturing are explicitly called out); (3) your organization's identified high-risk user segments and current control gaps from Steps 1–3; (4) proposed control investments with cost estimates. No enterprise reporting tool required — a well-structured slide deck or PDF is sufficient for this communication.

Evidence: Before the board briefing, document your organization's current BEC-relevant incident history: pull all help desk tickets, email gateway quarantine reports, and any finance-team-reported suspicious contact attempts from the prior 24 months. This internal incident data, combined with IC3 sector loss figures, constitutes a two-data-point risk argument — industry baseline plus organizational exposure — that is substantially more persuasive than IC3 figures alone. Retain this documentation as part of the risk assessment record per NIST RA-3 requirements.

Step 7: Monitor developments — track IC3 complaint portal updates and CISA advisories for sector-specific follow-on reporting; the IC3 report is annual but CISA publishes interim alerts when campaign activity against specific sectors intensifies

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Maintaining situational awareness through authoritative threat intelligence sources to enable continuous improvement of detection and response capability

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — formally subscribe to CISA advisories and IC3 public notices as organizational inputs to the security alert management process; sector-specific CISA alerts for healthcare, financial services, and manufacturing BEC/fraud campaigns qualify as directives requiring timely response, NIST IR-5 (Incident Monitoring) — continuous monitoring must include external threat intelligence feeds; IC3 complaint data trends and CISA sector-specific alerts are authoritative external indicators that should trigger re-evaluation of internal detection coverage, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — when CISA publishes a sector-specific BEC or fraud campaign alert, immediately cross-reference the published IOCs and TTPs against your audit log review queries and update detection thresholds accordingly, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — vulnerability management process must include a scheduled review cadence triggered by authoritative advisories; CISA alerts on BEC campaign intensification against your sector constitute a vulnerability management trigger event

Compensating: Subscribe to CISA alerts via the free CISA email notification service (us-cert.cisa.gov/mailing-lists-and-feeds) and the IC3 public notice RSS feed. Create a shared tracking document (spreadsheet or wiki page) with columns: Source, Date, Alert Title, Affected Sector, TTPs Referenced (ATT&CK IDs), IOCs Published, Detection Rule Update Required (Y/N), Date Actioned. Assign a named owner to review this log weekly — a two-person team can manage this in under 30 minutes per week. When a CISA alert references your

sector (healthcare, financial services, manufacturing), immediately re-run the detection gap analysis from Step 5 against the newly published TTPs.

Evidence: Establish a forward-looking evidence collection baseline now so that when a CISA sector advisory is published, you have historical telemetry to search against: ensure email gateway logs, DNS query logs, and authentication logs are retained for a minimum of 90 days (365 days preferred per NIST AU-11). When a new IC3 or CISA advisory is received, the first forensic action is to query retained logs for the published IOCs retroactively — this determines whether a campaign that CISA just flagged has already touched your environment. Without adequate log retention, this retroactive hunt is impossible.

Detection Guidance

BEC detection: Monitor for email rule creation (inbox forwarding to external addresses), login events from unfamiliar geolocations or ASNs immediately followed by email access, and changes to payment account details in finance systems. Correlate Microsoft 365 or Google Workspace audit logs against user behavior baselines. Anomalous OAuth application consent grants are a secondary indicator of account compromise used as BEC staging.

AI-enabled phishing: Standard URL and attachment filtering remains necessary but insufficient. Look for phishing lures with unusually high linguistic quality and low typo rates, which can indicate AI-generated content. Voice phishing (vishing) attempts impersonating executives should be flagged when callers request credential resets or fund transfers; train help desk staff to treat any such request as a social engineering attempt requiring callback verification to a known number.

Cryptocurrency fraud infrastructure: For organizations with employees who may be targeted individually, the attack surface is primarily personal. However, organizations in financial services and technology should monitor for internal communications referencing unsolicited investment opportunities or urgent fund transfer requests to cryptocurrency addresses. T1583.006 infrastructure (web services used for fraud platforms) typically involves newly registered domains; threat intelligence feeds with domain age and registration pattern data are relevant here.

Ransomware and critical infrastructure: Hunt for T1566 phishing delivery followed by T1204 user execution patterns in endpoint telemetry. Scattered Spider specifically targets help desk MFA reset workflows; audit your MFA reset process for identity verification strength. Monitor for anomalous lateral movement following authentication events, particularly during off-hours. T1565 data manipulation indicators include unexpected changes to database records or file integrity alerts in monitored directories.

Log sources to prioritize: identity provider authentication logs, email platform audit logs, endpoint detection telemetry for execution chain anomalies, and network flow data for unexpected outbound connections to newly registered domains or cryptocurrency-related infrastructure.

Framework Mappings

MITRE-ATTACK

- **T1598** — Phishing for Information
- **T1566.002** — Spearphishing Link
- **T1204** — User Execution
- **T1534** — Internal Spearphishing

- **T1566** — Phishing
- **T1588.007** — Artificial Intelligence
- **T1656** — Impersonation
- **T1204.001** — Malicious Link
- **T1647** — Plist File Modification
- **T1583.006** — Web Services
- **T1565** — Data Manipulation

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

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1598	Phishing for Information	Reconnaissance
T1566.002	Spearphishing Link	Initial-Access
T1204	User Execution	Execution

Technique ID	Technique Name	Tactic
T1534	Internal Spearphishing	Lateral-Movement
T1566	Phishing	Initial-Access
T1588.007	Artificial Intelligence	Resource-Development
T1656	Impersonation	Defense-Evasion
T1204.001	Malicious Link	Execution
T1647	Plist File Modification	Defense-Evasion
T1583.006	Web Services	Resource-Development
T1565	Data Manipulation	Impact

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/fbi-americans-lost-a...	T3
Critical Infrastructure Sectors - CISA	https://www.cisa.gov/topics/critical-infrastructure-security-and-re...	T1
The United States' 16 Critical Infrastructure Sectors - Bredemarket	https://bredemarket.com/2026/02/09/the-united-states-16-critical-in...	T3
Cybersecurity vulnerability analysis of medical devices purchased ...	https://pmc.ncbi.nlm.nih.gov/articles/PMC10636100/	T1
Risk management, legacy tech pose major threats to healthcare ...	https://www.cybersecuritydive.com/news/healthcare-cybersecurity-ris...	T3

Generated 2026-04-08 06:21 UTC by TJS Security Command Center