pellera

THREAT INTEL REPORT 2025

Prepared by: Pellera Threat Intel Team
pellera.com | 800.747.8585

OCTOBER

Driving Momentum. Accelerating Change. Empowering IT Transformation.

Pellera Technologies was born out of the combined expertise of Converge Technology Solutions and Mainline Information Systems, two industry leaders with over 35+ years of experience and a shared vision for innovation. Together, we empower businesses to achieve greater efficiency, adaptability, and growth for today and tomorrow.

Our commitment is to reshape what's possible with IT, offering advanced solutions in digital infrastructure, cloud, cybersecurity, and AI. We don't just deliver technology—we partner with you to build tailored strategies designed to simplify complexities, unlock opportunities, and drive transformational outcomes.

At Pellera, momentum builds here through collaborative, people-first technology designed to fuel progress and deliver measurable impact.

pellera

CONVERGE TECHNOLOGY SOLUTIONS + Mainline®

Observations for October 2025

The convergence of legislative failure, institutional paralysis, and rapidly advancing adversarial technology has created the most precarious period for U.S. cybersecurity in over a decade. The expiration of the Cybersecurity Information Sharing Act of 2015 (CISA 2015) on September 30, 2025—compounded by a concurrent government shutdown that **furloughed 65% of the Cybersecurity and Infrastructure Security Agency's (CISA) workforce**—has effectively dismantled the core framework of public-private cyber defense coordination.

This disruption removes key legal authorities that enabled real-time information sharing and network monitoring between the private sector and federal agencies, precisely as China's most aggressive cyber campaigns to date target U.S. telecommunications and critical infrastructure. The absence of statutory safe harbors and a depleted federal response capacity has opened an unprecedented window of vulnerability that adversaries are already poised to exploit.

This breakdown in institutional resilience comes amid escalating state-sponsored operations. Chinese threat groups Salt Typhoon and Volt Typhoon have compromised hundreds of organizations across 80 countries, including nine major U.S. telecommunications providers. These operations grant persistent access to lawful intercept systems and core infrastructure networks, enabling espionage and positioning China for potential disruption of U.S. communications, energy, and transportation sectors during future geopolitical conflict. **With CISA's operational workforce reduced from roughly 3,000 to 889 employees**, federal incident response, vulnerability coordination, and cross-sector collaboration are operating at critically degraded levels—leaving the private sector increasingly isolated against nation-state activity.

Simultaneously, the weaponization of artificial intelligence has transformed the cyber threat landscape from one of technical intrusion to one of cognitive manipulation. Deepfake technology—once a novelty—now drives a global disinformation and financial-fraud economy. Between 2022 and 2023, **reported deepfake incidents in North America surged 1,740%, resulting in over $200 million in losses during the first quarter of 2025 alone**. Attackers can fabricate realistic voice and video impersonations in under an hour using free software, collapsing the barrier to entry for sophisticated social engineering. The same state and criminal actors exploiting the current intelligence-sharing vacuum are leveraging deepfakes to erode trust in institutions, manipulate financial transactions, and undermine executive decision-making across the private sector.

Together, these developments illustrate a profound shift in the nature of cyber risk—from technical compromise to systemic erosion of trust, coordination, and information integrity. The United States now faces a dual crisis: the loss of institutional mechanisms designed to defend the nation's digital ecosystem, and the rapid democratization of AI-driven deception that amplifies the effectiveness of every adversary. Reauthorization of CISA 2015 and restoration of federal cyber capacity will be essential but insufficient; organizations must also harden internal intelligence-sharing networks, adopt behavioral analytics and AI-based verification systems, and treat digital authenticity as a core pillar of national and corporate security strategy in the months ahead.

Executive Overview

Audience

- CISO
- C-Suite Executives
- Board of Directors Audity & Risk Committees
- General Counsel & Legal Teams
- Government Relations Directors
- Compliance Officers
- Project Managers
- Cybersecurity Analysts
- Risk Management Professionals
- IT Managers

CISA 2015 EXPIRATION

HIGH

RISK

GEOGRAPHIC SCOPE

Organizations face $500K–$5M in legal costs or $10M–$50M+ in breach losses from choosing between data sharing risks and reduced access.

BUSINESS IMPACT

The September 30, 2025 expiration of CISA 2015 eliminates critical legal protections that enabled voluntary cybersecurity information sharing between the federal government and private sector entities for the past decade, directly weakening U.S. collective defense capabilities during an unprecedented surge in Chinese state-sponsored cyber operations. Organizations lose explicit authorization to monitor networks "notwithstanding any other provision of law"—exposing cybersecurity teams to potential liability under Federal Wiretap Act, Electronic Communications Privacy Act, and state privacy laws that previously carried CISA 2015 safe harbor protections. The simultaneous government shutdown reduced CISA's operational workforce by 1,651 employees (65% furlough rate), leaving just 889 personnel to maintain federal network defense, critical infrastructure coordination, vulnerability disclosure, and incident response capabilities. This workforce depletion follows approximately 1,000 DOGE-related staff reductions earlier in 2025, representing a 70% total reduction from CISA's mid-2024 staffing levels of approximately 3,000 employees.

The timing amplifies consequences exponentially: Chinese Salt Typhoon operations compromised at least 200 companies across 80+ countries, including nine major U.S. telecommunications providers (Verizon, AT&T, T-Mobile), breaching lawful intercept systems used for government surveillance and accessing metadata for over one million users. Volt Typhoon maintains persistent pre-positioned access in U.S. critical infrastructure across communications, energy, transportation, and water sectors—access FBI Director Christopher Wray described as "the defining threat of our generation" designed to enable disruptive or destructive attacks during potential U.S.-China conflict over Taiwan. Detection and attribution of these distributed campaigns depend critically on cross-sector information sharing that CISA 2015 protections enabled—capabilities now severely degraded precisely when most needed.

READ MORE: CISA 2015 EXPIRATION

AI ENHANCED SOCIAL ENGINEERING

Audience

- CISO
- IT Operations Managers & Teams
- Risk Management Professionals
- Security Operations Team
- IT Managers
- Incident Response Teams
- System Administrators

HIGH
RISK

GLOBAL
GEOGRAPHIC SCOPE

AI-driven social engineering erodes trust by automating highly personalized attacks that bypass security controls and exploit employee trust.
INDUSTRY IMPACT

The weaponization of artificial intelligence for social engineering represents a paradigm shift in organizational risk that transcends traditional cybersecurity boundaries. Potential Financial Impact: Organizations face average losses of $4.88 million per phishing-related breach in 2025, with deepfake-enhanced attacks commanding premium success rates. Regulatory Exposure: SEC disclosure requirements, GDPR breach notification obligations, and emerging AI-specific legislation create immediate compliance risks for victimized organizations. Brand/ Reputation Risk: High-profile incidents like the $25.6 million Arup deepfake fraud have eroded stakeholder confidence in video communications and identity verification systems. Customer Impact: Service disruptions from successful attacks average 207 days to identify and 70 days to contain, affecting millions of customers globally.

READ MORE: AI ENHANCED SOCIAL ENGINEERING

RISE OF DEEPFAKES

Audience

- CISO
- IT Operations Managers & Teams
- Risk Management Professionals
- Security Operations Team
- Ai/Ml Development Teams
- Cloud Security Teams
- Software Development Teams

HIGH
RISK

GLOBAL
GEOGRAPHIC SCOPE

Organizations face average losses of $600,000 per deepfake incident and $4.88 million per phishing breach.
INDUSTRY IMPACT

The proliferation of deepfake technology has reached a critical inflection point where detection capabilities lag significantly behind creation tools, fundamentally undermining trust in digital communications. Global incidents of deepfake fraud increased by 1,740% in North America between 2022 and 2023, with financial losses exceeding $200 million in Q1 2025 alone. The barrier to entry has collapsed dramatically - voice cloning now requires just 20-30 seconds of audio, while convincing video deepfakes can be created in 45 minutes using freely available software like DeepFaceLab, which powers over 95% of all deepfake videos globally. This democratization of sophisticated deception tools has enabled a new class of threat actors who operate with impunity across international borders, targeting everything from corporate wire transfers to democratic elections.

READ MORE: RISE OF DEEPFAKES

CISA 2015 EXPIRATION

Overview & Impact

CISA 2015 operated through three core mechanisms that collectively reduced legal barriers to cybersecurity collaboration and provided explicit statutory authority for monitoring and defensive activities. First, the Act required the Director of National Intelligence, Secretary of Homeland Security, Secretary of Defense, and Attorney General to develop procedures facilitating classified and unclassified threat indicator sharing with private entities. Seven federal agencies subsequently adopted implementing procedures that dramatically increased government-to-industry information flow, with DHS sharing 12 million threat indicators in 2020 compared to 300,000 in 2017 (3,900% increase).

Second, the Act authorized private entities to monitor their own information systems and those of consenting partners for cybersecurity purposes "notwithstanding any other provision of law"—explicitly superseding Federal Wiretap Act, Electronic Communications Privacy Act, Pen Register and Trap and Trace Device statutes, and analogous state privacy laws. This authorization addressed longstanding concerns that cybersecurity monitoring activities could trigger criminal penalties or civil liability under communications surveillance laws.

Third, the Act established comprehensive protections for information sharing activities including: exemption from Freedom of Information Act and similar state sunshine laws; antitrust safe harbor allowing companies to share threat intelligence without fear of collusion allegations; protection from waiver of attorney-client privilege or trade secret protections; restrictions on regulatory use preventing federal agencies from using shared information to initiate enforcement actions; and liability limitations for entities that shared cyber threat indicators in good faith compliance with Act requirements.

Congressional failure to reauthorize CISA 2015 stemmed from political disputes substantially unrelated to the Act's cybersecurity mission. The government shutdown that began October 1, 2025, compounded CISA 2015 expiration by reducing CISA operational capacity by 65%, with 1,651 employees furloughed and 889 remaining to maintain essential functions.

- **Statutory Protection Loss for Network Monitoring:** Organizations lose explicit Federal Wiretap Act and Electronic Communications Privacy Act exemptions for cybersecurity monitoring, forcing reliance on user consent mechanisms that may not provide equivalent legal protection
- **Automated Threat Indicator Sharing Platform Degradation:** CISA's Automated Indicator Sharing (AIS) platform faces potential discontinuation if monthly costs of approximately $1 million cannot be justified by declining indicator volumes
- **Cross-Sector Visibility Collapse:** Critical infrastructure sectors lose ability to correlate attack patterns across industry boundaries
- **Federal Cyber Defense Workforce Depletion:** The 65% CISA workforce furlough eliminates capacity for threat analysis, sector coordination, and vulnerability disclosure
- **Legal Review Bottleneck Introduction:** Organizations replacing automated processes with manual legal review introduce 48-96 hour delays
- **Government Intelligence Collection Gaps:** Federal agencies lose access to private sector telemetry covering 85% of U.S. critical infrastructure
- **Information Sharing and Analysis Center Uncertainty:** ISACs and ISAOs face legal uncertainty about antitrust protections
- **Small and Mid-Sized Organization Disproportionate Impact:** Entities lacking dedicated legal resources face binary choice between ceasing sharing or accepting unknown legal exposure
- **Third-Party Vendor Coordination Complexity:** Organizations face contractual uncertainty for sharing with managed service providers and cloud platforms

RETURN >>>

Tactical Guidance

- **Ransomware Detection and Response Degradation:** Affiliates benefit from extended indicator propagation time
- **Customer Trust and Service Availability Impact:** Elevated risk across telecommunications, financial services, healthcare, and critical infrastructure
- **Regulatory Compliance Tension:** Contradictory pressures to maintain regulatory compliance while managing increased legal exposure
- **Cyber Insurance Market Impact:** Insurers reassess risk models, potentially increasing premiums 15-25%
- **Financial Implications:** Competing cost pressures from legal review expenses, insurance premiums, breach costs, and regulatory fines
- **Reputational and Competitive Risk:** Organizations face shareholder questions and public criticism regardless of sharing decisions
- **Long-Term Collective Defense Erosion:** Decade of trust-building faces potential permanent degradation

Observations

- **Information Sharing Volume Degradation Metrics:** Industry estimates project 60-80% decline in voluntary threat indicator sharing within 30 days, with legal departments requiring 48-96 hour review cycles versus sub-second automated sharing
- **Federal Wiretap Act and ECPA Exposure Introduction:** Organizations lose "notwithstanding any other provision of law" authorization, forcing reliance on consent-based frameworks with potential litigation exposure
- **Automated Indicator Sharing Platform Sustainability Risk:** CISA's AIS platform incurs $1 million monthly operational costs that may not be justifiable if submission volumes decline 60-80%
- **Cross-Sector Correlation Capability Elimination:** Multi-industry campaigns face detection delays of 7-21 days when organizations cannot share indicators without protections
- **Government-to-Industry Intelligence Flow Continuity Uncertainty:** Seven federal agencies retain technical capability to share but may reduce prioritization without congressional direction
- **CISA Workforce Reduction Operational Impact:** The 65% furlough eliminates personnel producing Joint Cybersecurity Advisories, staffing sector coordination centers, and conducting vulnerability research
- **Threat Actor Operational Security Window Exploitation:** Chinese, Russian, Iranian, and North Korean actors gain 30-90 day operational security advantage
- **Legal Review Bottleneck Architecture:** Organizations face antitrust screening, FOIA exposure assessment, regulatory use analysis, and privilege protection evaluation requiring 24-72 hours per indicator category
- **Privacy and Civil Liberties Review Expansion:** Additional scrubbing and anonymization introduces 12-48 hour processing delays
- **Third-Party Vendor Information Sharing Contractual Ambiguity:** Managed service providers face uncertainty about continuing activities without statutory protections
- **State and Local Cybersecurity Grant Program Suspension:** Government shutdown suspends SLCGP grants funding security improvements for state, local, tribal, and territorial governments
- **Detection Engineering Capability Degradation:** Security operations centers lose access to government-shared adversary TTPs observed across federal threat landscape
- **Threat Hunting Hypothesis Development Impact:** Proactive hunting depends on intelligence primarily provided by federal agencies observing nation-state operations

RETURN >>>

Guidance

Strategic Intelligence

- **Threat Actor Context and Motivation Assessment**
  - Chinese state-sponsored groups conducting Volt Typhoon and Salt Typhoon campaigns demonstrate strategic preparation for potential conflict scenario over Taiwan, with cyber pre-positioning designed to complicate U.S. military response through disruption of critical infrastructure supporting force projection capabilities. FBI Director Christopher Wray's January 2024 testimony characterized Volt Typhoon as "the defining threat of our generation," emphasizing that pre-positioned access serves disruption rather than espionage objectives.
  - The timing of escalated Chinese operations concurrent with CISA 2015 expiration appears coincidental rather than coordinated, but Chinese intelligence services monitoring U.S. legislative processes will exploit the vulnerability window. Adversary operational planners demonstrating sophisticated understanding of U.S. cyber defense architecture will adjust campaign tempo to maximize impact during the October-December 2025 period.
  - Russian, Iranian, and North Korean threat actors gain operational security advantages during the CISA 2015 lapse and government shutdown that reduce their strategic disadvantages compared to Chinese capabilities, benefiting from degraded information sharing, reduced CISA workforce, and legal uncertainty.
  - Criminal ransomware groups operating affiliate models demonstrate acute awareness of defensive coordination mechanisms and will accelerate operations to exploit extended indicator propagation timelines. Groups rely on rapid operational cycles between initial access and encryption, with success dependent on moving faster than defender coordination.
- **Trend Analysis and Threat Landscape Evolution**
  - Cybersecurity legislation failures increasingly create exploitable operational windows as threat actors develop sophisticated understanding of U.S. policy processes and demonstrate ability to time campaigns for maximum impact during coordination disruptions. The CISA 2015 expiration follows a pattern of legislative gridlock on critical cyber issues.
  - Voluntary information sharing frameworks face persistent tension between legal risk management and collective security benefits, with corporate legal departments increasingly conservative when statutory protections are ambiguous, expired, or subject to political dispute.
  - The increasing sophistication of nation-state campaigns targeting distributed infrastructure amplifies consequences of information sharing disruptions exponentially compared to historical threat landscape. Unlike historical threats affecting individual organizations, contemporary campaigns span multiple sectors in coordinated operations invisible to individual defenders.
- **Contextual Insights and Historical Comparisons**
  - The CISA 2015 expiration occurred during the most active period of Chinese cyber operations against U.S. critical infrastructure in history, with Salt Typhoon representing the largest telecommunications sector compromise and Volt Typhoon demonstrating unprecedented patience for multi-year pre-positioning.
  - Previous temporary disruptions in cybersecurity coordination frameworks demonstrate measurable increases in successful intrusions during periods of degraded information sharing, with dwell time increasing 25-40% and detection probability declining 30-50% when coordination mechanisms are suspended.

RETURN >>>

- The financial services and telecommunications sectors face disproportionate exposure during the CISA 2015 lapse due to regulatory frameworks that previously assumed statutory protections would remain available and explicitly incorporated information sharing expectations into supervisory guidance.

- **Business Risk Mapping and Exposure Analysis**
  - Critical infrastructure operators in energy, telecommunications, water, and transportation face elevated breach risk during CISA 2015 lapse due to targeting by Chinese campaigns and dependence on cross-sector information sharing for distributed threat detection.
  - Financial institutions face complex legal exposure from contradictory pressures to maintain regulatory compliance through information sharing while managing antitrust risk, FOIA disclosure potential, and regulatory use concerns without CISA 2015 protections.
  - Healthcare organizations face elevated ransomware risk when affiliate activity accelerates combined with HIPAA Privacy Rule concerns about information sharing that may inadvertently disclose protected health information.
  - Managed security service providers, cloud platforms, cybersecurity vendors, and threat intelligence aggregators serving multiple clients face contractual disputes, service level agreement violations, and potential liability exposure from sharing decisions.
  - Publicly traded companies face shareholder litigation risk regardless of information sharing decisions during CISA 2015 lapse, with potential securities fraud claims, derivative lawsuits, and class actions creating legal exposure.

Operational Intelligence

- **Defense Effectiveness Assessment and Control Failures**
  - Organizations previously relying on automated consumption of government-shared threat indicators through CISA Automated Indicator Sharing (AIS) platform face complete workflow disruption requiring architectural decisions about continuing integration without statutory protections.
  - Cross-sector information sharing arrangements facilitated by Information Sharing and Analysis Centers and Organizations (ISACs/ISAOs) face legal uncertainty about antitrust protections for peer-to-peer threat intelligence sharing between competing organizations in the same industry.
  - Security controls dependent on timely threat intelligence—including threat-informed defense architectures, indicator of compromise blocking, proactive threat hunting, and security orchestration platforms—face degraded effectiveness ranging from 30-70% during CISA 2015 lapse.
  - Small and mid-sized organizations that lacked dedicated legal resources for evaluating information sharing decisions face disproportionate impact creating two-tier defensive posture where resource-rich enterprises maintain reduced sharing capabilities while smaller organizations withdraw entirely.

- **Monitoring & Detection Gaps**
  - Federal cybersecurity agencies lose visibility into threat activity affecting private sector critical infrastructure that owns and operates 85% of U.S. essential services, creating intelligence gaps for National Intelligence Estimates, Presidential Daily Briefings, and Strategic Intelligence Assessments.
  - Security operations centers face log coverage deficiencies for adversary infrastructure indicators when government agencies reduce sharing due to diminished recipient populations during CISA 2015 lapse, with government-originated indicators often providing sole-source intelligence about nation-state infrastructure.

RETURN >>>

- Alert correlation failures increase across organizations that previously used CISA AIS indicators to enrich security event logs with threat context, with manual legal review processes unable to sustain volume and velocity required for real-time alert enrichment.
- Threat hunting operations face significant capability degradation when organizations cannot access government-shared adversary tactics, techniques, and procedures without CISA 2015 protections, with proactive hunting depending on hypothesis development informed by current adversary behavior.

- **Time Analysis and Operational Tempo Impact**
  - Threat actor dwell time projected to increase 25-40% during CISA 2015 lapse as organizations lose early warning capabilities from cross-sector information sharing, with historical analysis showing mean dwell time of 16-21 days when coordination is optimal, compared to projected 20-30 days during degraded sharing.
  - Mean time to detect distributed threat campaigns will increase from 7-14 days to 21-45 days when organizations cannot correlate indicators across sector boundaries without legal protections, with campaigns invisible to individual organizations requiring multi-entity collaboration.
  - Response timeline for emerging threats extends 48-96 hours as organizations implement manual legal review processes for information sharing decisions previously executed through automated platforms, affecting both information consumption and production.
  - Attack velocity advantages accrue to adversaries during CISA 2015 lapse, with ransomware groups reducing time from initial access to encryption from 4-7 days to 2-4 days to exploit window before indicators propagate through manual sharing processes.

- **Response Actions and Stakeholder Coordination**
  - Some leading cybersecurity companies including CrowdStrike and Halcyon publicly committed to continuing threat intelligence sharing with government agencies despite loss of CISA 2015 protections, prioritizing collective defense over legal risk concerns.
  - Other cybersecurity vendors including Palo Alto Networks, Trellix, Google, and Microsoft declined to specify whether they would maintain information sharing activities, reflecting corporate legal departments evaluating competing priorities.
  - Federal agencies including CISA publicly communicated that the legislative lapse represents "a serious blow" to cyber defense capabilities and urged Congress to act swiftly on reauthorization, with agency statements emphasizing continued commitment to sharing indicators to extent possible under existing authorities.
  - The House of Representatives included 10-year CISA 2015 reauthorization in continuing resolution that passed House Homeland Security Committee unanimously on September 3, 2025, indicating strong bipartisan support with 435-0 vote demonstrating rare congressional consensus on cybersecurity policy.

Tactical Intelligence

- **Preventive Measures**
  - Organizations should establish diversified threat intelligence architectures incorporating multiple independent sources including government-shared indicators, commercial threat intelligence platforms, open-source intelligence feeds, industry consortium data, ISAC/ISAO information, peer bilateral sharing arrangements, and internal threat hunting capabilities.
  - General Counsel and cybersecurity leadership should jointly develop pre-approved frameworks for information sharing decisions during periods of regulatory uncertainty, establishing risk-based criteria specifying which indicators can be shared with which recipients under what circumstances.

RETURN >>>

Tactical Guidance

- Organizations should maintain comprehensive documentation of information sharing business justifications and security value to support potential future legal defense if actions taken during CISA 2015 lapse become subject to regulatory scrutiny, antitrust inquiry, shareholder litigation, or other legal challenges.
- Industry associations and sector-specific ISACs should develop model legal frameworks and contractual templates for peer-to-peer information sharing that operate independently of CISA 2015 protections, providing standardized approaches that reduce legal complexity.
- Organizations should establish direct relationships with federal cybersecurity agency personnel including CISA Hunt and Incident Response Teams, FBI Cyber Task Forces, and NSA Cybersecurity Collaboration Center to maintain communication channels during periods when statutory protections are unavailable.

Sources

- WilmerHale: Critical National Security Law, CISA 2015, Set to Expire at the End of the Month – September 15, 2025
- POLITICO: Government Flying Partially Blind to Threats After Key Cyber Law Expires – October 3, 2025
- Cybersecurity Dive: Landmark US Cyber-Information-Sharing Program Expires, Bringing Uncertainty – October 1, 2025
- Mayer Brown: Cybersecurity Information Sharing Act of 2015 Lapses – October 3, 2025
- Wiley Rein via JD Supra: Expiration of Critical Cyber Information Sharing Law Creates Confusion About Authorities and Liability Protections – October 2025
- A&O Shearman: Cybersecurity Sunset: Navigating the Expiration of CISA's Legal Protections – September 2025
- eSecurity Planet: CISA 2015 Lapse Leaves US Cybersecurity Exposed – October 4, 2025
- SC Media: Information Sharing Under CISA 2015 in Limbo After Government Shuts Down – October 1, 2025
- Data Protection Report: CISA 2015 Sunsets: Cyber Threat Sharing Without a Net – October 2025
- Infosecurity Magazine: US: CISA 2015 Safe Harbor at Risk as September 2025 Deadline Nears – September 2025
- Washington Post: Shutdown Guts CISA, Main U.S. Cybersecurity Agency, at a Perilous Time – October 2, 2025
- Cybersecurity Dive: CISA to Furlough 65% of Staff if Government Shuts Down This Week – September 30, 2025
- Infosecurity Magazine: US Government Shutdown to Slash Federal Cybersecurity Staff – October 3, 2025
- Federal News Network: Cyber Defenders on Edge Amid Shutdown Furloughs, Expired Authorities – October 2, 2025
- ITIF: Congress Needs to Shutdown-Proof CISA – October 3, 2025

RETURN >>>

AI ENHANCED SOCIAL ENGINEERING

Overview & Impact

The technical architecture of AI-enhanced social engineering attacks demonstrates sophisticated orchestration across multiple attack vectors. Threat actors initiate campaigns through automated reconnaissance using AI to analyze thousands of social media profiles, corporate websites, and public records within seconds. Large language models craft contextually perfect phishing messages that mirror organizational communication styles, eliminating traditional indicators like grammatical errors. Voice synthesis technology enables real-time impersonation during phone calls, with tools like Tacotron 2 and ElevenLabs producing indistinguishable voice clones. Video deepfakes leverage DeepFaceLab, responsible for over 95% of deepfake videos globally, to conduct fraudulent video conferences. These capabilities converge in multi-stage attacks where initial email contact escalates to voice verification and culminates in deepfake video calls for high-value authorization.

- **Disrupted systems:** Financial transaction platforms, email systems, VPN gateways
- **Bypassed controls:** Multi-factor authentication through real-time phishing proxies and voice cloning
- **Compromised workflows:** Help desk procedures, executive approval processes, vendor payment systems
- **Data exposure:** 60% of social engineering cases result in data exfiltration, 16 points higher than other vectors
- **Operational disruption:** Average 295 days to detect and contain phishing breaches
- **Financial losses:** Individual incidents ranging from $250,000 to $25.6 million per organization

Observations

- **Behavioral Patterns:** Attackers conduct 3-5 reconnaissance calls to help desks before executing MFA reset attacks, building rapport and gathering process intelligence
- **Attack Signatures:** Voice deepfakes exhibit consistent 100-200ms latency patterns and subtle pitch variations detectable through acoustic fingerprinting
- **Log Anomalies:** Geographical impossibility alerts triggered in 73% of successful account takeovers, but often dismissed as VPN-related false positives
- **Configuration Weaknesses:** 80% of compromised organizations lacked formal deepfake response protocols or voice authentication alternatives
- **MITRE ATT&CK TTPs:** T1566 (Phishing), T1656 (Impersonation), T1556 (Modify Authentication Process), T1078 (Valid Accounts)
- **Credential Misuse Patterns:** Lateral movement within 40 minutes of initial access, targeting administrative shares and cloud management consoles
- **Custom Tool Development:** AI-powered phishing kits incorporating real-time translation and dialect adaptation for global campaigns

Guidance

Strategic Intelligence

- **Threat Actor Motivation:** Financial gain drives 95% of AI-enhanced social engineering, with average monetization occurring within 48 hours of initial access
- **Sophistication Assessment:** Mid-tier cybercriminals now possess nation-state-level impersonation capabilities through commercially available AI tools

RETURN >>>

Tactical Guidance

- **Historical Patterns:** Evolution from Nigerian Prince scams to AI-generated CFO impersonations represents a 10,000% increase in success rates
- **Criminal Ecosystem:** Underground marketplaces offer deepfake-as-a-service for $500-5,000 per engagement, democratizing advanced capabilities
- **Industry Exposure:** Financial services face 28% of attacks, healthcare 19%, government 17%, creating sector-specific risk profiles
- **Supply Chain Impact:** Third-party vendor compromises through social engineering increased 300%, affecting downstream customers
- **Regulatory Landscape:** EU AI Act and pending US legislation will mandate AI content labeling by mid-2026
- **Predictive Analysis:** 70% probability of AI-powered attacks becoming primary threat vector by Q2 2026 (High Confidence

Operational Intelligence

- **Entry Vectors:** SEO poisoning delivers 35% of non-phishing social engineering, exploiting search result trust
- **C2 Infrastructure:** Attackers leverage Cloudflare Workers and Azure Functions to host phishing infrastructure, complicating takedowns
- **Tooling Evolution:** DeepFaceLab, FaceSwap, and First Order Motion Model comprise the primary deepfake toolkit
- **Operational Tempo:** Threat actors maintain 24/7 operations with AI handling initial engagement, humans intervening for high-value targets
- **Detection Gaps:** 60% of organizations lack voice biometric baselines, preventing deepfake voice detection
- **Security Control Failures:** Traditional email gateways detect only 11% of AI-generated phishing, requiring behavioral analysis
- **Dwell Time:** Attackers maintain presence for median 21 days in AI-initiated compromises before discovery
- **Response Delays:** Average 4.5 hours from initial alert to analyst review, allowing attacker entrenchment

Tactical Intelligence

- Enforce geographic impossibility blocks for authentication attempts
- Update incident response playbooks to include deepfake verification procedures
- Implement Identity Threat Detection and Response (ITDR) platform
- Deploy zero-trust architecture for privileged access management
- Alert on authentication attempts with >500ms latency variance from baseline
- Monitor for voice calls originating from VOIP providers to sensitive departments
- Flag email threads where sender writing style deviates >30% from historical baseline
- Detect unusual Graph API queries following successful authentication
- Track help desk password reset requests correlating with failed MFA attempts

Threat Hunting Hypotheses

Deepfake Voice Reconnaissance

Hypothesis: Threat actors conduct voice sampling calls to executives before launching deepfake campaigns

Investigation Steps

- **Patterns:** Sub-3-minute calls to executives from unknown numbers, followed by no callback
- **Expected Baseline:** <5 unsolicited executive calls per week

RETURN >>>

- **Correlation:** Match call timing with subsequent phishing campaigns or fraud attempts
- **Success Criteria:** Identify 3+ reconnaissance calls preceding known incidents
- **Potential Findings:** Pre-attack intelligence gathering patterns enabling prevention

MFA Bypass Through Social Engineering

Hypothesis: Attackers systematically target help desk staff during shift changes

Investigation Steps

- **Patterns:** Password reset requests within 30 minutes of shift change
- **Expected Baseline:** 2-3 legitimate shift-change resets per week
- **Correlation:** Match successful resets with subsequent anomalous logins
- **Success Criteria:** Identify temporal clustering of suspicious requests
- **Potential Findings:** Vulnerable time windows requiring enhanced verification

Sources

- Deepfake Attacks & AI-Generated Phishing: 2025 Statistics – August 29, 2025
- Deepfakes and AI-Powered Phishing Scams – April 28, 2025
- AI-Generated Phishing: The Top Enterprise Threat of 2025
- The Rise of AI-Powered Phishing 2025 – February 20, 2025
- Deepfake Statistics & Trends 2025 – October 6, 2025
- AI Phishing Attacks: How Big is the Threat? – April 24, 2025
- The Anatomy of a Deepfake Voice Phishing Attack – August 6, 2025
- Detecting dangerous AI is essential in the deepfake era – July 2025
- Cybercrime: Lessons learned from a $25m deepfake attack – February 2025
- Why is Deepfake Phishing Becoming a 2025 Problem? – April 2, 2025
- 2025 Unit 42 Global Incident Response Report: Social Engineering Edition – August 2, 2025
- The 13 Most Common Types of Social Engineering Attacks in 2025 – July 30, 2025
- Social Engineering Statistics 2025 – June 20, 2025
- 60+ Social Engineering Statistics 2025 – December 31, 2024
- Social Engineering Statistics 2025: The Human Hack – September 7, 2025
- 10 Types of Social Engineering Attacks to Watch for in 2025
- Hackers target Workday in social engineering attack – August 19, 2025
- List of Recent Data Breaches in 2025 – October 5, 2025
- 100+ Latest Social Engineering Statistics 2025 – August 22, 2025
- The Human Factor 2025: Vol. 1 Social Engineering – September 17, 2025

RISE OF DEEPFAKES

Overview & Impact

The technical sophistication of deepfake attacks in 2025 encompasses three primary vectors: video, audio, and hybrid multi-modal operations. Video deepfakes utilize generative adversarial networks (GANs) trained on publicly available footage to create photorealistic impersonations. Audio deepfakes leverage neural voice synthesis, requiring minimal input data - as little as 3-5 seconds for basic cloning or 20-30 seconds for high-fidelity reproduction. Hybrid attacks combine both technologies, exemplified by the Hong Kong incident where criminals created an entire fake video conference with multiple deepfaked participants. The infrastructure supporting these attacks includes cloud-based rendering farms, distributed C2 networks, and cryptocurrency money laundering chains that can move funds within minutes of successful fraud.

- **Service disruptions:** Call center operations, help desk services, executive decision-making processes
- **Financial losses:** Single incidents ranging from $25,000 to $25.6 million (Arup case)
- **Trust erosion:** 42% of businesses only "somewhat confident" in detecting deepfakes
- **Compliance violations:** GDPR, SEC disclosure requirements, KYC/AML regulations
- **Psychological impact:** Employee hesitation to trust legitimate instructions, operational friction
- **Sector-specific damage:** Crypto firms averaging $440,000 losses, 57% hit rate in 2024

Observations

- **Generation Patterns:** Deepfake creation follows predictable GPU usage patterns, with 4-6 hour processing windows for high-quality output
- **Acoustic Signatures:** Voice deepfakes exhibit micro-artifacts at 8-16 kHz frequencies, detectable through spectral analysis
- **Visual Anomalies:** Inconsistent eye movement patterns, temporal flickering at 0.1-0.3 second intervals in 73% of deepfakes
- **Behavioral Inconsistencies:** Mismatched breathing patterns with speech, unnatural pause distributions
- **Infrastructure Indicators:** Heavy use of cloud GPU instances, particularly AWS p3 and Google Cloud V100 deployments
- **Distribution Networks:** Leveraging CDNs and legitimate video platforms to host and distribute deepfake content
- **Tool Signatures:** DeepFaceLab artifacts in metadata, characteristic compression patterns from specific encoders

Guidance

Strategic Intelligence

- **Market Evolution:** Deepfake-as-a-Service economy valued at $2.1 billion in 2023, projected $25.6 billion by 2033
- **Threat Actor Sophistication:** Convergence of cybercriminal and nation-state capabilities in deepfake operations
- **Geopolitical Implications:** 77% of voters encountered political deepfakes before 2024 US elections
- **Technology Proliferation:** Open-source tools reducing technical barriers, enabling script-kiddie level actors
- **Industry Targeting:** Financial services (28%), healthcare (19%), government (17%) comprise 64% of targets
- **Criminal ROI:** Average 2,400% return on investment for successful deepfake fraud campaigns

RETURN >>>

- **Detection Technology Gap:** 65% success rate for current detection tools versus 95%+ for creation tools
- **Legislative Response:** 17 countries implementing deepfake-specific legislation by end of 2025

Operational Intelligence

- **Creation Infrastructure:** Primary reliance on Google Colab, Kaggle, and local GPU farms for rendering
- **Distribution Channels:** YouTube (49% of deepfakes), social media platforms, encrypted messaging apps
- **Monetization Methods:** Wire transfers (45%), cryptocurrency (35%), gift cards (20%)
- **Operational Timing: 68% of attacks occur Tuesday-Thursday, 14:00-16:**00 victim local time
- **Actor Collaboration:** Evidence of Scattered Spider and ShinyHunters groups sharing deepfake capabilities
- **Tool Evolution:** Monthly updates to DeepFaceLab, FaceSwap indicating active development
- **Detection Evasion:** Attackers using adversarial training to defeat known detection algorithms
- **Campaign Duration:** Average deepfake campaign runs 17 days before detection or objective completion

Tactical Intelligence

- Monitor for sudden increases in GPU utilization on user workstations
- Alert on video calls originating from virtual cameras or OBS Studio
- Flag voice calls with consistent 100-200ms processing delays
- Detect downloads of deepfake tools through endpoint monitoring
- Analyze metadata for signs of video manipulation or re-encoding

Threat Hunting Hypotheses

Internal Deepfake Generation

Hypothesis: Insider threats may use corporate resources to generate deepfakes

Investigation Steps

- **Patterns:** Extended GPU usage, downloads from AI model repositories
- **Expected Baseline:** <5% GPU utilization for non-developer workstations
- **Correlation:** Match GPU spikes with external data transfers
- **Success Criteria:** Identify unauthorized AI model training or inference
- **Potential Findings:** Insider threat indicators or compromised workstation

Executive Voice Harvesting

Hypothesis: Attackers systematically collect executive voice samples before attacks

Investigation Steps

- **Patterns:** Searches for executive names + "interview" or "presentation"
- **Expected Baseline:** <10 searches per month for executive content
- **Correlation:** Match searches with subsequent vishing attempts
- **Success Criteria:** Identify reconnaissance pattern preceding attacks
- **Potential Findings:** Pre-attack indicators enabling proactive defense

RETURN >>>

Tactical Guidance

Deepfake C2 Communications

Hypothesis: Deepfake tools may contain backdoors for attacker control

Investigation Steps

- **Patterns:** Connections to known deepfake tool infrastructure
- **Expected Baseline:** Zero connections for non-media organizations
- **Correlation:** Match with suspicious authentication events
- **Success Criteria:** Identify compromised deepfake tools in environment
- **Potential Findings:** Supply chain compromise through AI tools

Sources

- Deepfake Statistics & Trends 2025 – October 6, 2025
- The Anatomy of a Deepfake Voice Phishing Attack – August 6, 2025
- Detecting dangerous AI is essential in the deepfake era – July 2025
- Deepfake Attacks & AI-Generated Phishing: 2025 Statistics – August 29, 2025
- AI-Generated Phishing: The Top Enterprise Threat of 2025
- 2025 Unit 42 Global Incident Response Report: Social Engineering Edition – August 2, 2025
- Deepfakes and AI-Powered Phishing Scams – April 28, 2025
- The Rise of AI-Powered Phishing 2025 – February 20, 2025
- AI Phishing Attacks: How Big is the Threat? – April 24, 2025
- Cybercrime: Lessons learned from a $25m deepfake attack – February 2025
- Why is Deepfake Phishing Becoming a 2025 Problem? – April 2, 2025
- Social Engineering Statistics 2025 – June 20, 2025
- The 13 Most Common Types of Social Engineering Attacks in 2025 – July 30, 2025
- Social Engineering Statistics 2025: The Human Hack – September 7, 2025
- List of Recent Data Breaches in 2025 – October 5, 2025
- 100+ Latest Social Engineering Statistics 2025 – August 22, 2025
- 60+ Social Engineering Statistics 2025 – December 31, 2024
- 10 Types of Social Engineering Attacks to Watch for in 2025
- Hackers target Workday in social engineering attack – August 19, 2025
- The Human Factor 2025: Vol. 1 Social Engineering – September 17, 2025

RETURN >>>

Contact the Pellera Threat Intel Group at getsecure@pellera.com

pellera.com

A PELLERA PODCAST

Edge of I.T.