iProov

Threat Intelligence Report 2025

Remote Identity Under Attack

Contents

Executive Foreword by Andrew Newell

The landscape of identity verification has reached a critical inflection point. Over the last year, we've witnessed a seismic shift not just in the sophistication of attacks, but in the fundamental democratization of threat capabilities. What was once the domain of highly skilled actors has transformed into an accessible ecosystem of tools and services that can be wielded by anyone with minimal technical expertise.

The scale of this transformation is staggering. As an example, for just one type of deepfake, the Face Swap, we currently track over 120 active attack tools; and deepfakes themselves are just one class of imagery that can be used in injection attacks. When combined with various injection methods and delivery mechanisms, we're facing over 100,000 potential attack combinations. This exponential growth in attack permutations represents an unprecedented challenge for traditional security frameworks.

Perhaps most concerning is the quality leap in synthetic media. Where the human eye could once reliably detect deepfakes, that certainty has eroded. Deepfakes aren't just threats to biometric systems anymore; they represent fundamental challenges to any system relying on imagery for verification. The implications extend far beyond individual fraud attempts to potentially compromising entire organizational security frameworks through sophisticated workforce deception.

The financial impact is equally sobering. FBI data indicates identity-related criminal activities generated losses of $8.8 billion in 2023 alone. Yet these numbers tell only part of the story.

The real transformation lies in the shifting nature of these attacks, from isolated incidents to sophisticated, multi-vector campaigns that risk being undetected for months, if appropriate threat monitoring is not in place.

This new reality demands a fundamental rethinking of how we approach identity security. Static defenses and periodic updates are no longer sufficient against threats that evolve in real-time. Success requires continuous monitoring, rapid adaptation capabilities, and most importantly, the ability to detect and respond to novel attack patterns before they can be widely exploited.

As we navigate this evolving landscape, one thing becomes clear: the future belongs to those who can adapt and respond faster than the threats themselves. This report offers not just an analysis of current trends, but a roadmap for building the resilient, adaptive security frameworks needed to meet these emerging challenges.

Andrew Newell,
Chief Scientific Officer,
iProov

Introduction:

State of Remote Identity Verification: Threats and Economic Impact (2024-2025)

The rapid growth of AI-based technology has introduced new challenges for remote identity systems. Innovative and easily accessible tools have allowed threat actors to become more sophisticated overnight, powering an increasing number of threat vectors due to new methodologies.

The Rising Cost of Identity Verification Failures

The growth of new attack vectors over the last 24 months has heavily impacted organizations. The cost of not properly implementing remote identity verification is manifold. The Federal Trade Commission's Consumer Sentinel Network documented a 45% increase in identity theft incidents in early 2024, with aggregate fraud losses exceeding $10.2 billion[1]. The second-highest reported loss amount came from imposter scams, with nearly $2.7 billion in reported losses, indicating a significant upward trajectory in financial impact.

While traditional metrics like breach costs and detection times remain important indicators, they tell only part of the story. What's more significant is the shifting nature of these attacks: from isolated incidents to sophisticated, multi-vector campaigns that can persist undetected for months. The extended detection window—which, according to IBM, often exceeds 270 days—creates opportunities for threat actors to execute complex fraud schemes, compromising not just immediate assets but entire digital infrastructure systems.

1. https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

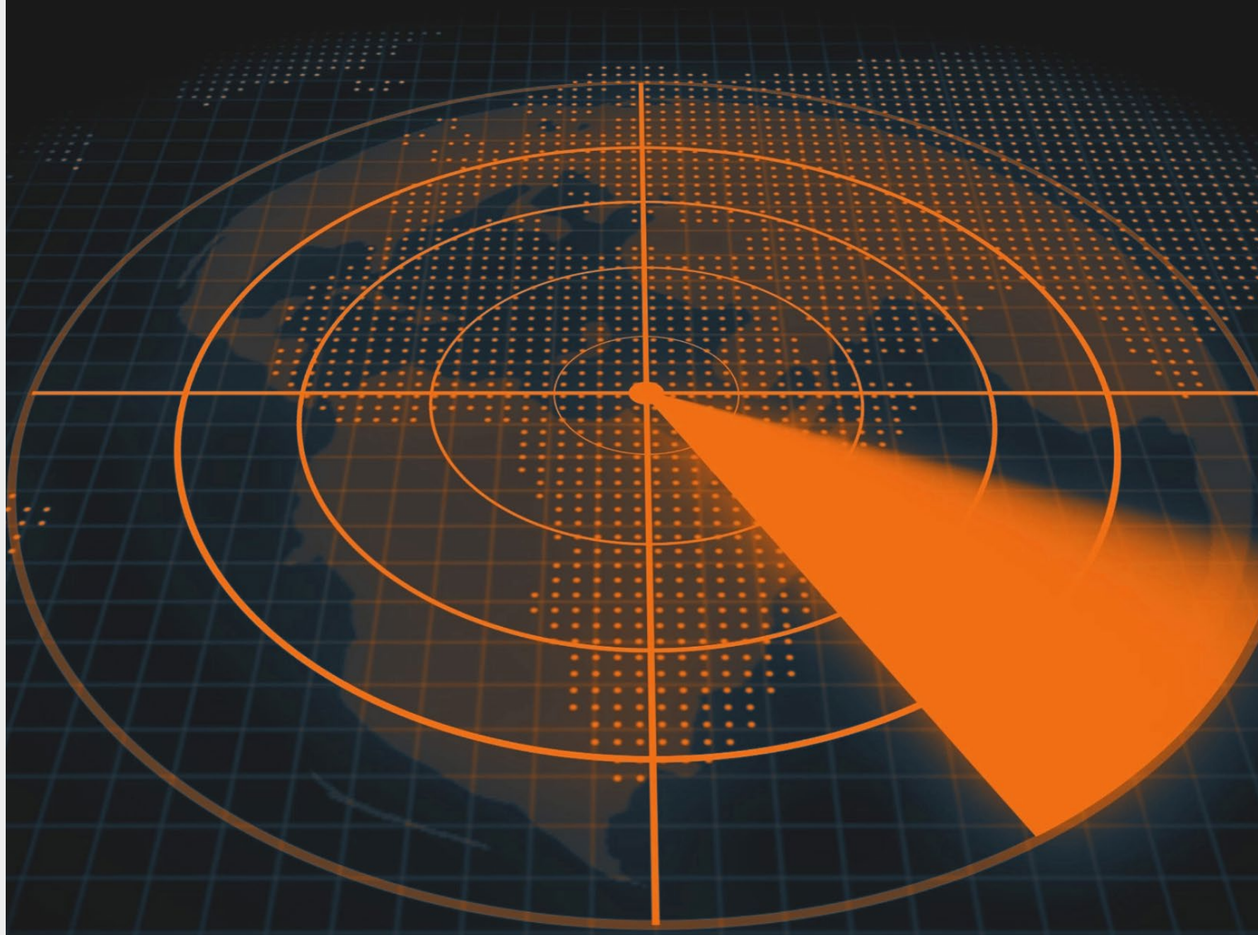
IBM's Cost of a Data Breach Report demonstrates that identity-related security compromises now incur an average cost of $4.24 million per incident, with credential theft accounting for 19% of recorded events. Importantly for organizations, the mean time to detection and containment extends to 277 days, creating substantial windows of vulnerability for downstream fraud activities.

The severity of this threat is illustrated by several high-profile incidents in 2024:

- T-Mobile (January 2024): Exposure of 37 million customer records, resulting in $350 million in settlement costs[2]
- Microsoft (August 2024): Attackers executed large-scale bot attacks against CAPTCHA systems and used them to create 750 million fake Microsoft accounts[3]
- LoanDepot (January 2024): Ransomware incident resulting in exposure of customer identification data and systemic disruption[4]

"These incidents demonstrate a critical shift in attack methodology: threat actors are no longer just stealing data—they're impersonating trusted individuals via Face Swap tools, or creating new synthetic identities to execute long-term fraud strategies." - Dr. Newell

While the market recognizes the need for enhanced security measures, organizations face significant challenges in selecting and implementing appropriate solutions.



2. https://www.forbes.com/sites/antoniopequenoiv/2024/08/14/t-mobile-will-pay-record-breaking-60-million-settlement-over-alleged-data-breach-violations/
3. https://www.darkreading.com/cyberattacks-data-breaches/cybercriminals-tap-greasy-opal-to-create-750m-fake-microsoft-accounts
4. https://www.cybersecuritydive.com/news/loandepot-ransomware-exposes-17M-people/705169/

Buyer Beware: The Twin Challenges of Security Technology Procurement

Organizations face a dual challenge when securing their remote identity verification systems. First, there is a fundamental knowledge gap regarding understanding and procuring appropriate remote verification technologies based on use cases and contextual data. This knowledge gap is starkly illustrated in the 2025 2025 RSA ID IQ[5] Report, which found that nearly half of all responders got at least half the questions wrong on basic identity security concepts, with identity and access management (IAM) and cybersecurity experts surprisingly performing the worst.

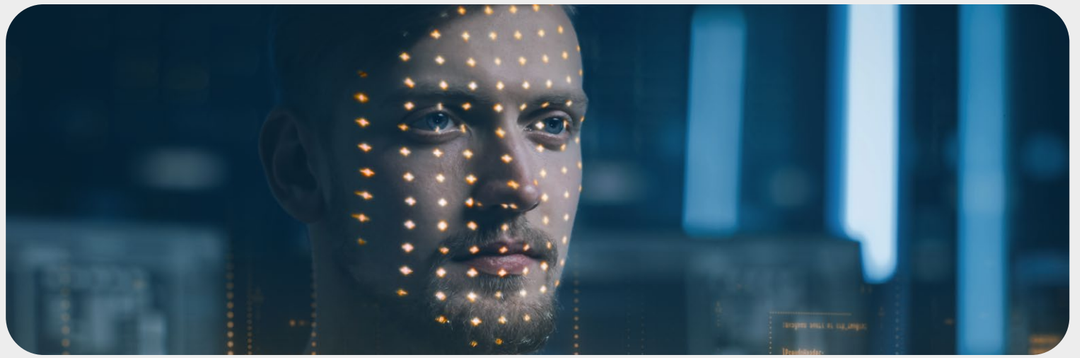
Second, and equally concerning, is the prevalence of inflated vendor claims about security capabilities. Our threat intelligence findings reveal that many solutions claiming comprehensive protection against synthetic media attacks lack the technological foundation to prevent them. This disparity between marketed capabilities and actual protection leaves organizations vulnerable while creating a false sense of security.

The RSA report highlights this risk by using the aerospace industry as an example. Despite being the most likely sector to suffer severe identity-related breaches costing over $10 million, aerospace companies paradoxically reported the highest confidence in their ability to manage user access entitlements.

This complex landscape demands a more nuanced approach to security procurement. Moving beyond vendor assurances and traditional compliance-focused evaluations toward comprehensive security assessments that include:

- Independent verification of security claims - particularly crucial given that 66% of organizations that experienced identity-related breaches rated them as severe events
- Managed detection & response capability
- Continuous monitoring with real-time threat detection systems – especially important as 42% of organizations reported experiencing identity-related breaches within a three-year period
- Demonstrated ability to adapt to emerging attack vectors - critical as 80% of respondents believe AI will significantly impact cybersecurity over the next five years

Without addressing both the knowledge gap and vendor accountability issues, organizations risk implementing solutions that appear robust on paper but prove inadequate against real-world attacks. This risk is quantifiable: The RSA report found that 44% of respondents estimated identity-related breach costs exceeded typical data breach costs, with 21% reporting costs over $10 million.



5. https://www.rsa.com/id-iq/

Key Takeaways

01 The Threat Landscape Has Fundamentally Transformed

- Attack tools have been democratized and commercialized
- Over 100,000 possible attack combinations identified from just three vectors
- Individual attack tools have evolved into sophisticated attack chains

02 Traditional Security Approaches Are No Longer Sufficient

- Point-in-time security updates can't keep pace with evolving threats
- Static testing fails to capture the complexity of modern attacks
- Organizations must shift from periodic to continuous security monitoring

03 Human Detection Capabilities Are Severely Limited

- Only 0.1% of people can reliably identify all synthetic media[6]
- Overconfidence in detection abilities creates additional risks
- Technical solutions must compensate for human vulnerability

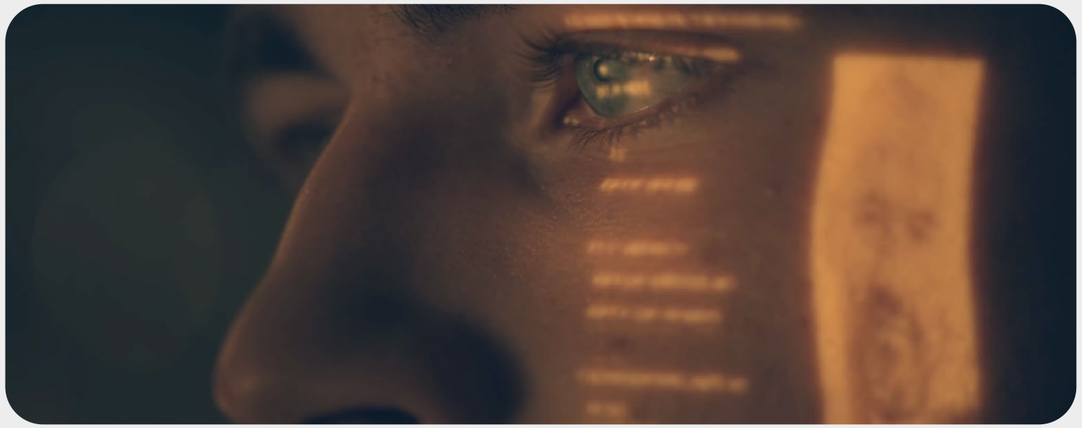
04 Security Success Requires a Multi-Layered Approach

- Real-time, managed detection and response capabilities are essential
- Continuous monitoring and adaptation must replace static defenses
- Integration of automated systems with human expertise is crucial

05 Attack Patterns Have Become More Sophisticated

- Threat actors actively profile and share intelligence about targets
- Low attack rates often indicate strong security rather than reduced threats
- Attackers rapidly shift focus to more vulnerable targets

These findings underscore a clear imperative: organizations must fundamentally rethink their approach to identity security. Success in this new environment requires a commitment to continuous security evolution backed by robust threat intelligence and real-time managed detection and response (MDR) capabilities. The future belongs to vendors and organizations that can adapt and respond to novel threats rather than those that rely on static defenses.



6. https://www.iproov.com/press/study-reveals-deepfake-blindspot-detect-ai-generated-content

iProov Threat Intelligence Report:
Methodology and Scope

This threat intelligence report draws from data collated from iProov's Security Operations Center (iSOC). Our unique science-led approach enables us to collect and analyze real-world attack data, providing unprecedented visibility into emerging threats targeting remote verification systems.

The findings presented in this report are derived from:

- Real-time threat detection and response data from iSOC
- External threat intelligence gathering and dark web monitoring
- Internal red team penetration testing campaigns
- Advanced biometric security research and internal threat intelligence
- Pattern analysis of detected and prevented attacks
- Technical evaluation of emerging attack tools and methodologies

"In 2014, creating synthetic identities required extensive technical expertise, specialized equipment, and significant time investment. Artificial intelligence has revolutionized this space, enabling the real-time generation of sophisticated synthetic media." *- Dr. Newell*

Through continuous real-time threat detection, our security experts defend against current attacks and identify emerging threat patterns, enabling predictive security improvements to our defenses. This report provides analysis and insights into the emerging attack vectors and evolving adversary tactics as we enter the 2025 remote identity verification landscape.

The Evolution of Identity Deception

2014 - 2024 Timeline and Impact: Past the Point of No Return

The progression of identity deception capabilities from 2014 to 2025 represents a fundamental shift in both technology and accessibility. This timeline illustrates the rapid transformation from complex, specialized attacks to widely accessible and available tools and services.

This democratization has been accelerated by three converging trends: rapid technological advancement, the emergence of Crime-as-a-Service (CaaS) marketplaces, and the transition of synthetic media attacks from theoretical threats to documented financial crimes.

2014

GANs introduction

2016

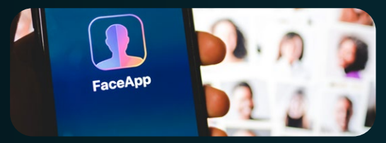
Deepfakes emerged with the rise of deep learning, with early communities forming on Reddit

2017

First widespread deepfake creation tool (FakeApp); Limited to poor quality Face Swaps in videos

2018

Early Face Swaps



2019

First Order Motion Models (FOMM)

2020

Audio deepfakes appeared alongside tools like Descript Overdub and Wave2Lip

2021

DALL-E release

2022

The rise of accessible image generation, voice cloning, and real-time deepfakes spurred iProov's first Threat Intelligence Report.

2023

Face Swap Proliferation; High quality audio deepfakes; GPT-4 release

2024

High quality Face Swaps

From Research to Real-World Impact

Late 2023 marked a critical turning point in this evolution. What had primarily existed in research labs and proof-of-concept demonstrations materialized into sophisticated attacks, resulting in substantial financial losses.

While much attention has focused on consumer identity fraud, the most significant and costly attacks of 2024 targeted workforce verification systems. This shift toward corporate targets reveals a concerning trend: sophisticated threat actors are exploiting remote work processes and corporate communication channels for maximum impact.

An example is the $25.6 million Hong Kong-based deepfake scam[7] in which attackers used synthetic media to impersonate executives in conference calls, bypassing traditional corporate verification protocols. This incident demonstrated how synthetic identity attacks can compromise not just financial assets but also lead to deep organizational security breaches through workforce exploitation.'

These cases represent a strategic pivot by threat actors who have discovered critical vulnerabilities in corporate verification systems. By targeting remote hiring processes, virtual workplace communications, and executive video conferences, attackers are achieving significantly higher payouts than traditional consumer fraud. This shift from individual to organizational targets exposes a dangerous gap in workforce identity verification—one that current corporate security frameworks are struggling to address.

7. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
8. https://www.cyberark.com/threat-landscape/

CyberArk's 2024 Identity Security Threat Landscape Report[8] revealed that 93% of organizations had two or more identity-related breaches in the past year alone. These incidents validate long-held concerns about synthetic media's potential impact.

These successful attacks demonstrate several developments:

01 **Operational Validation:** What was once theoretical has now been proven effective in real-world scenarios, providing threat actors with documented methodologies and success stories. This validation will likely accelerate the adoption of similar tactics across criminal networks.

02 **Traditional Multi-Layer System Compromise:** These attacks have successfully bypassed multiple security layers simultaneously:

- Human judgment in professional settings
- Corporate security protocols
- Traditional fraud detection mechanisms

03 **Scalability of Attacks:** The proven success of these methods, combined with the availability of Crime-as-a-Service platforms, creates potential for:

- Rapid replication of successful attack methodologies
- Parallel attacks against multiple organizations
- Automated targeting of vulnerable sectors
- Lower-skilled actors executing sophisticated attack patterns

04 **Organizational Vulnerability:** These attacks expose broader institutional weaknesses:

- Overexposure to outdated verification methods
- Inadequate protocols for high-value remote transactions
- Limited real-time managed detection and response capabilities

9. https://www.iproov.com/press/study-reveals-deepfake-blindspot-detect-ai-generated-content

Understanding this progression is crucial for developing effective countermeasures against current and emerging threats. The dangerous combination of vendor-inflated claims and our misplaced conviction that we can spot a deepfake is a recipe for disaster.

Consumer Research: Deepfake Blindspot

A 2025 deepfake consumer research[9] report by iProov paints a picture of a society largely unprepared for the challenges posed by deepfake technology, with significant gaps in awareness, detection abilities, and response mechanisms.

Key Findings:

- Detection Success Rate: Only 0.1% of participants could identify all synthetic media examples correctly
- Video Vulnerability: Particularly low success rate (9%) for video deepfake detection
- Age-Related Vulnerabilities: Adults over 55 were found to be particularly vulnerable, as nearly one-third had never heard of deepfakes before, limiting their ability to identify and protect themselves against this technology
- Confidence Gap: Younger adults (18-34) displayed dangerous overconfidence in detection abilities despite poor performance

Response Capabilities:

- 48% lack knowledge of proper deepfake reporting procedures
- 25% verify information through alternative sources
- 11% conduct critical source analysis
- 29% take no action when encountering suspected deepfakes

iProov Data 2023 vs. 2024 Year-on-Year Key Attack Trends

Injection Attacks: 783% Increase

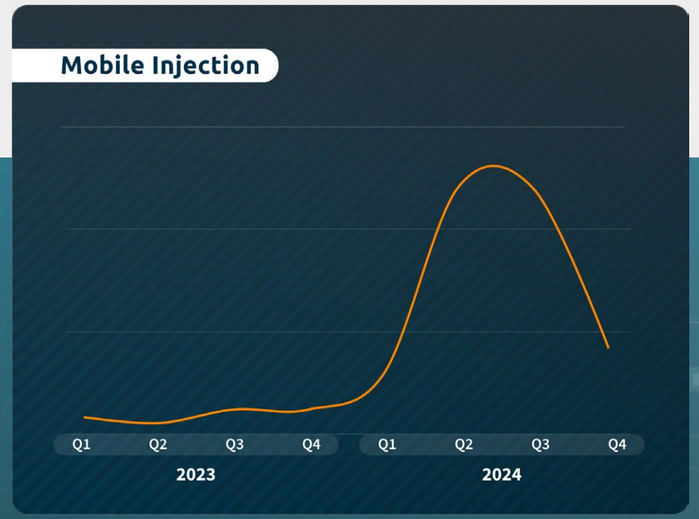
2024 saw a rapid escalation in the frequency and scale of injection-based attack vectors aimed at mobile web applications, suggesting a fundamental shift in the capabilities and accessibility of attack tools.

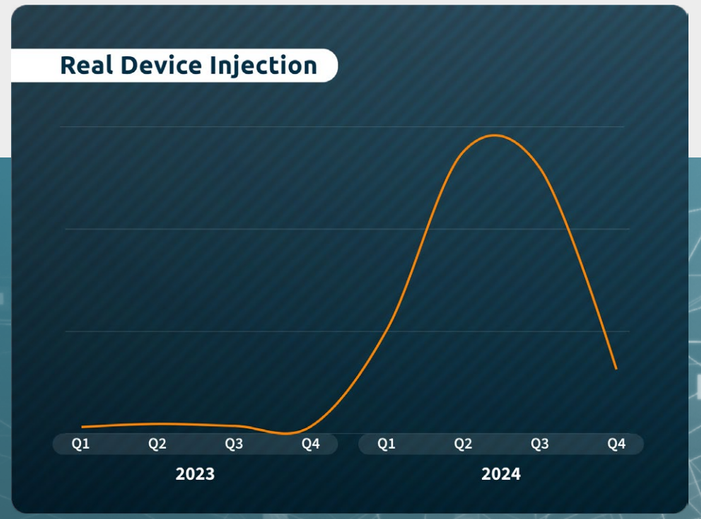
Native Virtual Cameras: 2665% Increase

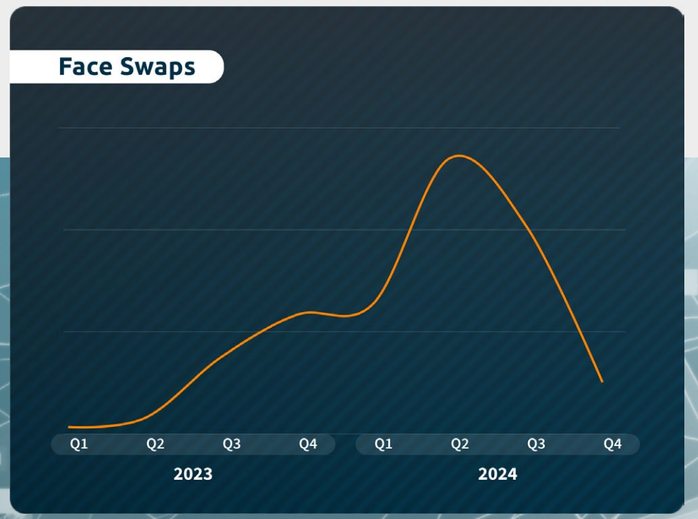
Perhaps one of the most significant events of 2024 was the dramatic reappearance of native virtual camera attacks and the speed with which they arrived. The chart demonstrates the need for real-time managed detection and response.

Face Swaps: 300% Increase

Already an alarming trend discovered in 2023, Face Swap attacks persisted in 2024 and spiked in Q2 of that year. We explore the nature of its evolution in the four Key Trends section of this report.







Emerging Threats

This section presents findings from iProov's threat intelligence team regarding the evolution of attack methodologies and their implications for contemporary identity verification frameworks.

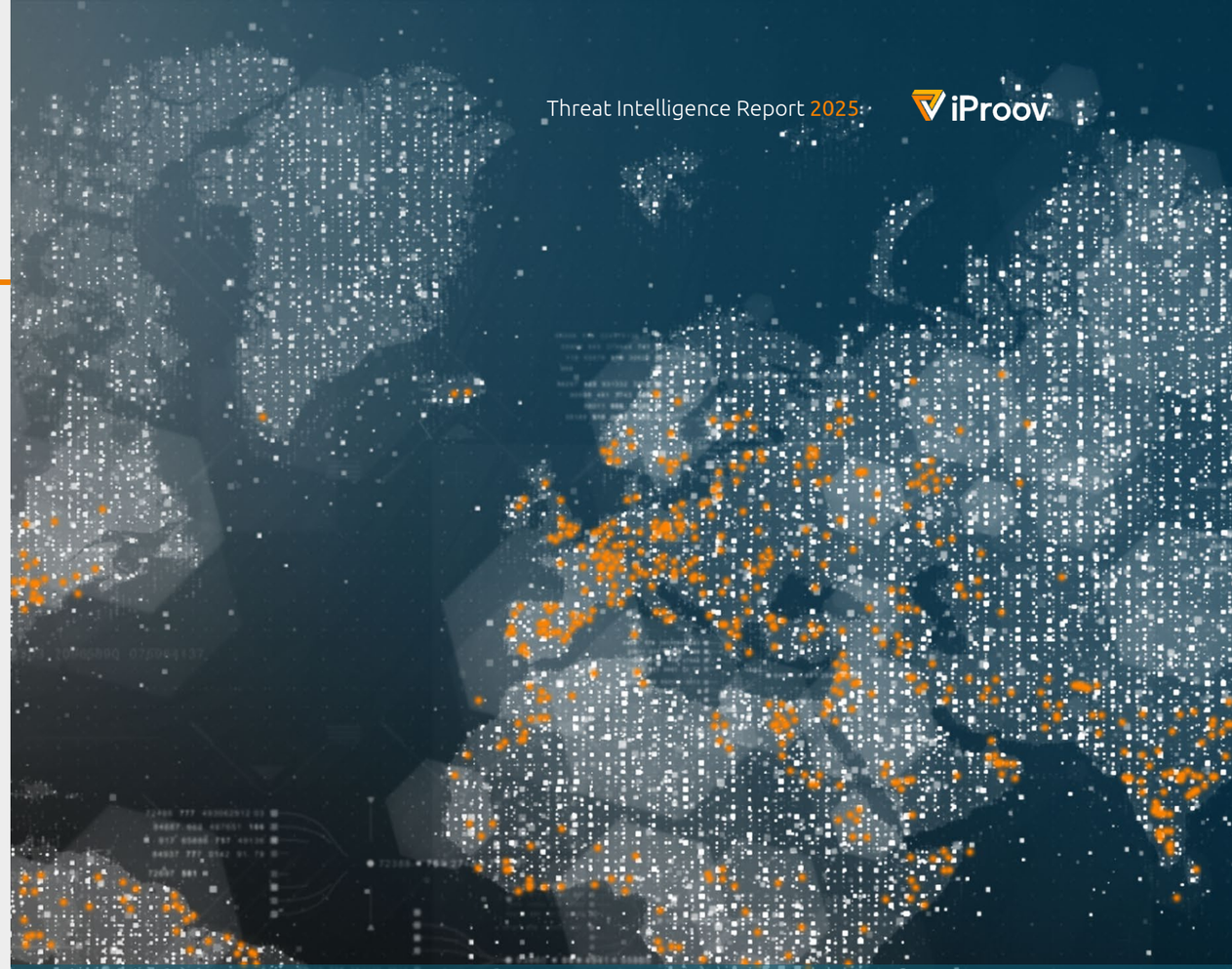
At the end of last year, iSOC uncovered a dark web group that had amassed a significant collection of identity documents and corresponding facial images. These identities were specifically designed to bypass Know Your Customer (KYC) verification processes. Instead of being acquired through traditional theft, it appears that individuals willingly provided these identities in exchange for payment.[10]

Discovery: Large-scale collection of legitimate identity documents and facial images
Method: Voluntary provision of credentials for payment
Impact: Creation of false identities based on genuine documents to evade detection
Geographic Scope: Initially identified in Latin America, now linked to European fraud networks

With Face Swaps and native camera attacks at their peak, bad actors can leverage genuine documents that do not ring any fraud alarm bells to create a Face Swap of a genuine identity to superimpose on their face and verify themselves remotely through video conferencing or other remote face verification means.

Any criminal activities discovered by our team are reported to the relevant local authorities.

10. https://www.iproov.com/press/discovers-major-dark-web-identity-farming-operation
11. https://www.iproov.com/reports/2024-gartner-emerging-tech-the-impact-of-ai-and-deepfakes-on-identity-verification



"Liveness detection technologies are becoming critical for defending against deepfakes and verifying the genuine presence of an individual."

2024 Gartner® Emerging Tech: The Impact of AI and Deepfakes on Identity Verification Report[11]

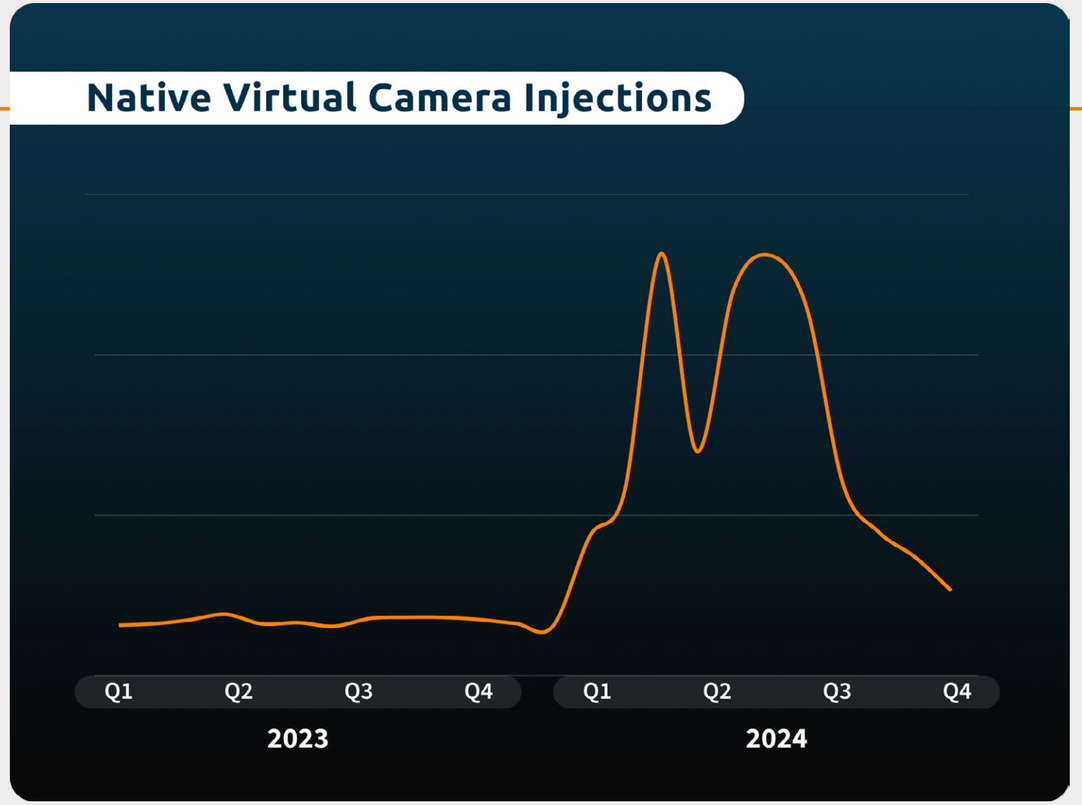
Four Trends to Watch in 2025

Trend 1: Rise of Native Virtual Cameras

Key Observations:

- Native virtual camera attacks evolved from their experimental phase in 2023 to become a major threat in 2024, peaking at 785 weekly attacks in Q2
- Most concerningly, these attacks don't require rooted or jailbroken devices, making them accessible to threat actors without advanced technical skills
- The discovery of a malicious camera app in a mainstream app store demonstrates how these attacks are being "democratized" through easy-to-use tools

What started as an experimental threat vector in 2023 evolved into one of the most significant trends in 2024, with native camera attacks peaking at 785 incidents per week in Q2. The discovery of a malicious camera app in a mainstream app store revealed these attacks don't require sophisticated hacking tools or rooted devices, making traditional cybersecurity measures like root detection insufficient. Though removed from the official store, the app remains available through third-party sources, enabling easy access to injection attacks.



This development challenges the notion that injection attacks are purely either a biometric or a cybersecurity threat. The evidence clearly shows that robust defense requires both strong biometric liveness detection and cybersecurity measures working in concert. The attack patterns we observed suggest threat actors are actively exploring this dual-vector approach.

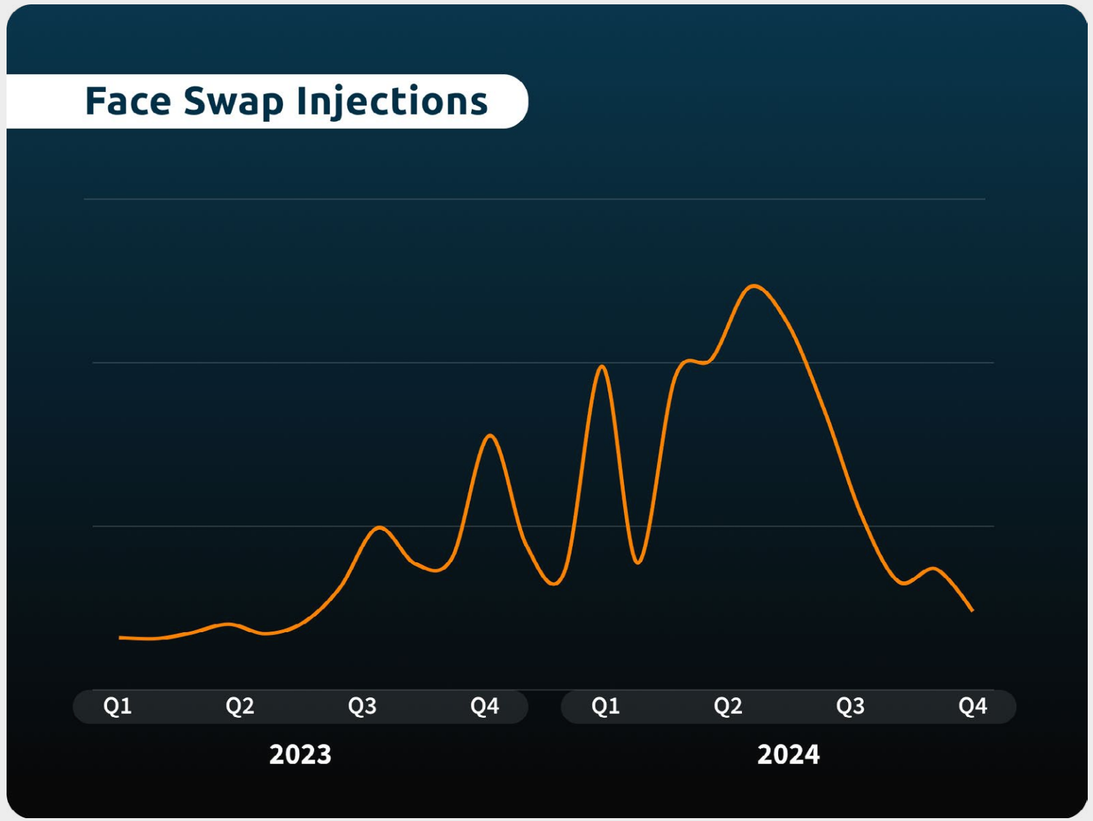
Trend 2: Face Swap Proliferation

Key Observations:

- In 2024, attack volumes surged by 300% compared to 2023
- The number of tools used in these attacks increased by 15.5%, rising from 110 to 127
- Threat actors leverage shared intelligence to exploit vulnerable systems using a variety of Face Swap tools

The landscape for Face Swap attacks grew significantly last year, with the number of tracked tools increasing from 110 to 127. The first quarter of 2024 revealed a clear pattern: threat actors adapted their tactics after initial widespread deployment. Notably, following the large scale experimentation stage in the first half of the year, intelligence sharing about system vulnerabilities effectively shifted their focus toward “low-hanging fruit.” Our observation saw them moving away from the iProov platform toward systems using active liveness detection that require users to follow specific actions or movements. These systems are easier to bypass since their challenge-response patterns can be replicated with pre-recorded or synthesized videos.

In 2024, discussions about Face Swap tools and techniques became more prominent in threat actor forums, driven by the sharing of information and tools among malicious communities.



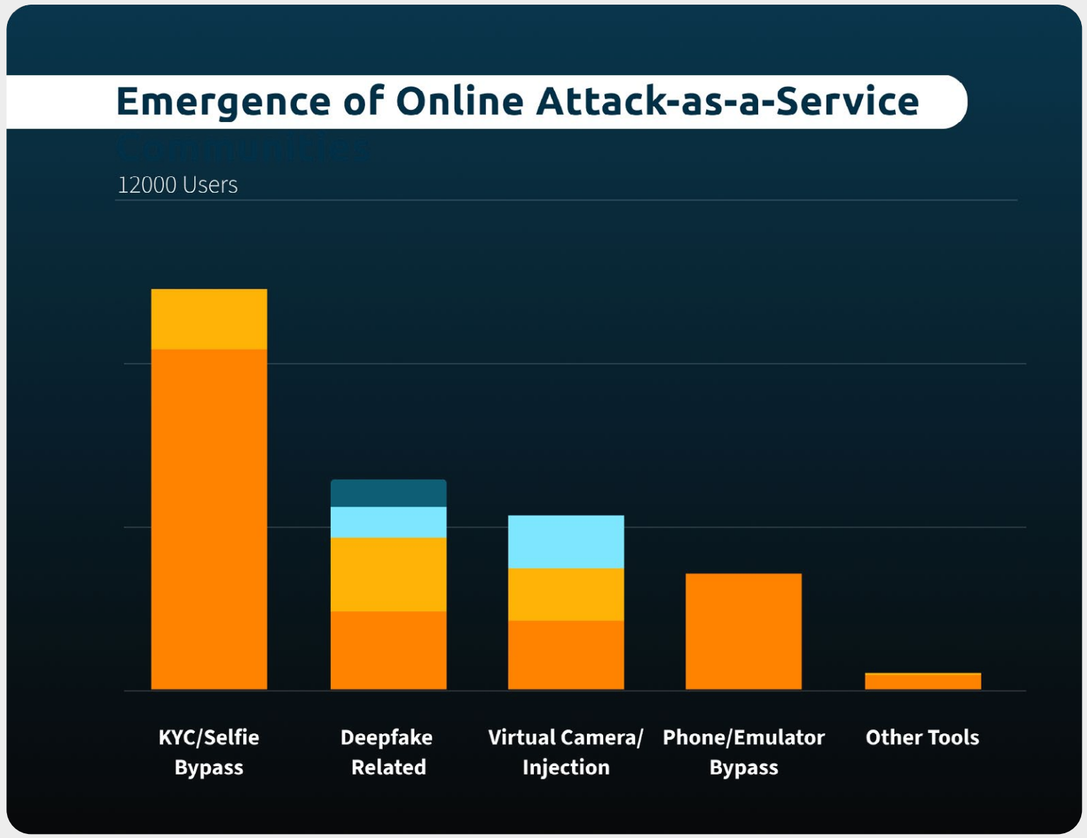
Trend 3: Online Attack-as-a-Service Communities

Key Observations:

- An additional 31 online threat actor groups were identified in 2024, the largest of which has 6,400 users
- Tool-selling groups serve 68% (23,698) of users, indicating their effectiveness and credibility
- Attack methods are increasingly focusing on KYC bypass, deepfakes, and Android-specific tools. These groups are moving towards comprehensive solutions instead of standalone services

In 2024, 31 additional online threat actor groups were identified, with 45% selling their own tools and 55% reselling or providing related services. This ecosystem encompasses 34,965 total users, with tool sellers attracting 23,698 users compared to 11,267 for non-sellers. Nine groups have over 1,500 users, with the largest reaching 6,400 members. Common discussions center on KYC bypass techniques, deepfake technology, and Android tools.

A significant focus is placed on mobile platforms, particularly Android, with some groups offering combined tools and services, while others specialize in areas like ID farming and cryptocurrency exchanges.



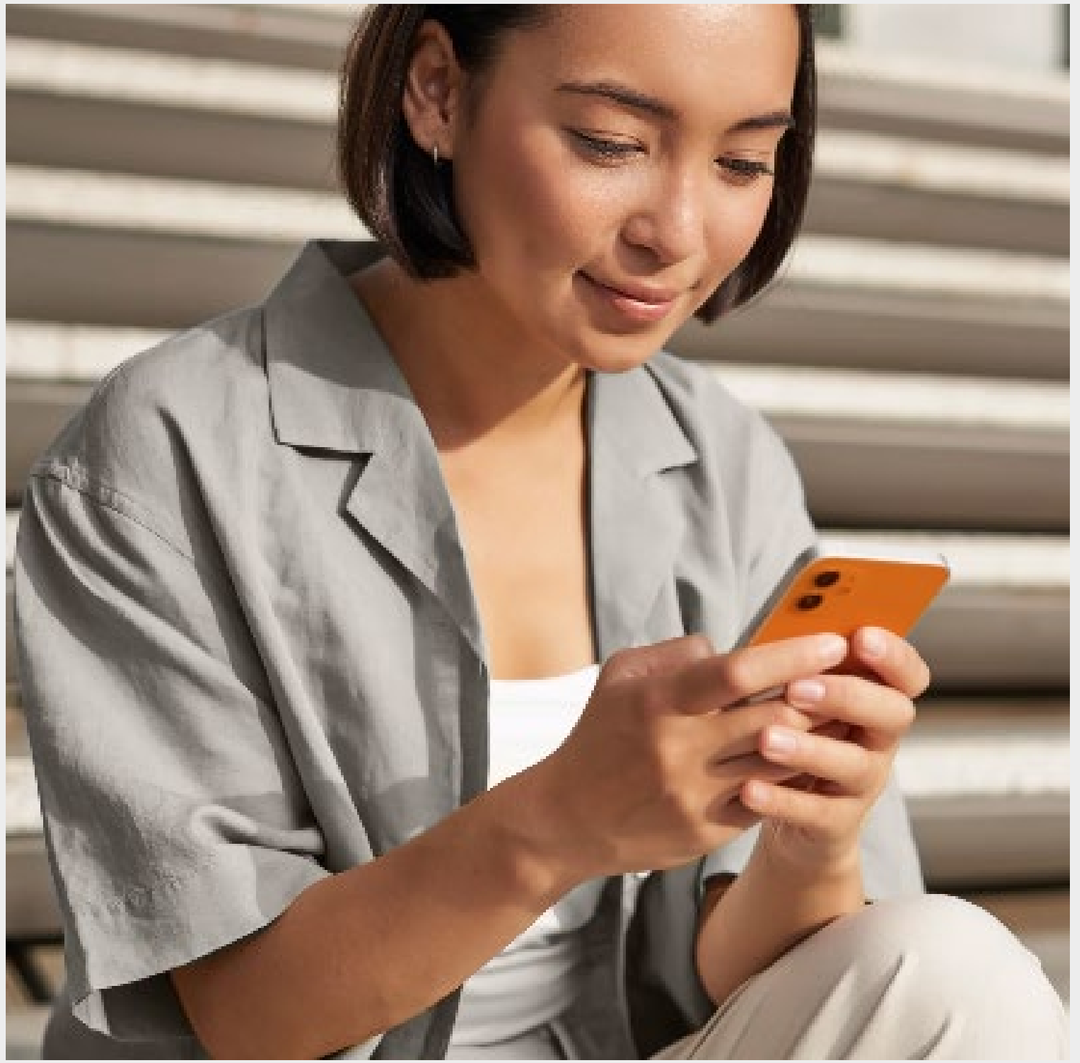
Trend 4: Image-to-Video Conversion
A New Synthetic Identity Attack Vector

Key Observations:

- Image-to-video conversion tools have reduced synthetic identity creation to a simple two-step process that requires minimal technical expertise
- Our testing shows these animated synthetic identities pose a significant threat to many liveness detection systems, including active challenge-response mechanisms
- The perfect nature of synthetic media output, lacking typical manipulation artifacts, makes them exceptionally difficult to detect once animated with fluid motion

These attacks proved ineffective against our Dynamic Liveness platform, which uses patented Flashmark technology[12] to verify genuine human presence through passive challenge-response mechanisms.

Our science team has identified a significant evolution in synthetic identity fraud through image-to-video conversion technology, first observed in an attack attempt against our platform in December 2024. This technique transforms static images into convincing video content that could pose very significant challenges for most remote identity verification systems. While synthetic identity attacks typically use Face Swaps, metadata manipulation, and camera bypasses, this new attack vector simplifies the process into two steps: threat actors obtain or create a synthetic face image, then utilize image-to-video conversion tools to animate it into fluid motion that closely mimics genuine video content.



12. https://www.iproov.com/biometric-encyclopedia/flashmark

Synthetic Identity Fraud (SIF) is the Fastest-Growing Type of Fraud

Synthetic identity fraud (SIF) is the fastest-growing type of fraud, with particularly alarming implications. This sophisticated scheme combines legitimate data (such as valid Social Security Numbers often stolen from children, elderly, or deceased individuals) with fabricated personal information to create convincing false identities. Fraudsters then methodically build credibility for these synthetic identities by establishing credit histories, opening multiple accounts across different institutions, and creating digital footprints that appear authentic.

What makes SIF especially challenging to combat is its ability to evade traditional fraud detection systems. Unlike conventional identity theft, where systems can flag stolen information based on reports from real victims, SIF creates entirely new identities that incorporate both real and fake elements. Without a real victim to raise the alarm, and with some components of the identity being legitimate, traditional detection methods often fail to recognize these synthetic fraud patterns.

Many remote identity verification systems struggle to detect manipulated images in videos because, unlike genuine images altered at the pixel level, synthetic faces do not exhibit these traditional signs of manipulation. When animated, these synthetic identities look incredibly lifelike, making detection challenging for the human eye. The accessibility and effectiveness of these tools suggest that the use of this technique will increase. This development marks a significant evolution in synthetic identity fraud, necessitating ongoing monitoring and research through 2025.

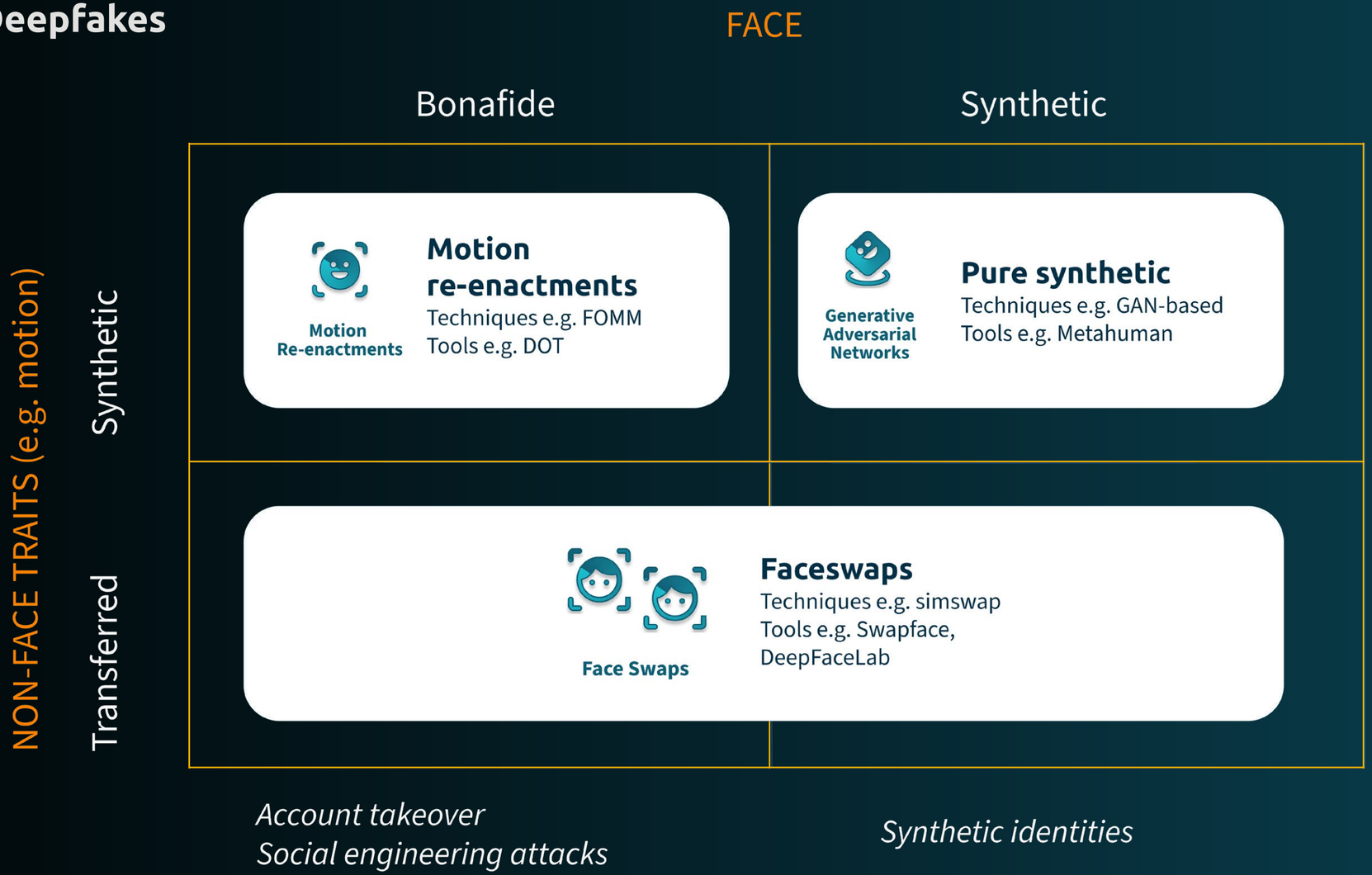
Attack Permutations:
The Exponential Threat Landscape

The complexity of remote identity verification attacks extends far beyond individual tools or techniques. Today's threat actors utilize sophisticated combinations of tools, creating an exponentially larger attack surface than many organizations realize and are equipped to protect. Understanding these permutations is crucial for comprehensive security testing and defense strategies.

Source: This Person Does Not Exist

Source: iProov Threat Intelligence Library

Classes of Deepfakes



Core Attack Components and Their Variations

01 Facial Manipulation Tools

- Currently tracking 127 distinct Face Swap applications
- Each tool offers different capabilities and output qualities
- Varying degrees of detectability and sophistication
- Range from consumer-grade apps to advanced AI-powered solutions

02 Mobile Emulators

- Currently tracking over 10 new emulator technologies
- Capabilities include location spoofing, device characteristic manipulation
- Various operating system and hardware configurations
- Different levels of detection evasion capabilities

03 Virtual Camera Software

- Currently tracking 91 virtual camera tools
- Ranging from basic video injection to sophisticated stream manipulation
- Various methods of bypassing device security controls
- Different capabilities for metadata manipulation

The Multiplication Effect

The true scale of potential attacks emerges when these tools are combined:

Basic Calculation:
127 Face Swap tools
× 10 emulators
× 91 virtual cameras
= 115,570 potential attack combinations

Each combination represents a unique attack vector requiring specific detection and prevention strategies. As new tools and updates are introduced, combinations are constantly increasing. For simplicity, the example provided in this report calculates the three most notorious attack combinations. However, it should not detract from the available Computer-generated imagery (CGI) and First Order Motion Model (FOMM) tools, which we are also tracking.

Entry Points

Virtual Cameras

- **Face Swaps**
  - **Metadata Manipulation**
  - Device Sensor Data Manipulation
- Deepfakes
- CGI
- Re-enactments

- Man in the Middle
  - Face Swaps
  - Deepfakes
  - Synthetic Media

- Replay
  - Face Swaps
  - Splice Attacks
  - Synthetic Media

Attack Permutations:
The Exponential Threat Landscape

Each component can be combined with others, creating a vast matrix of possible attack vectors. For example:

Single Virtual Camera + Single Face Swap Tool = An attack vector with unique traits

Multiple Virtual Cameras + Multiple Face Swap Tools + Metadata Manipulation = Hundreds of thousands of potential combinations with varying traits

Effective evaluation of new vectors requires examining four key areas:

01 **Feasibility - Examines the integrity of the tool and its ease of use**

02 **Novelty - Looks at the traits of the threat vector to assess how new/common the tools and methods are**

03 **Transferability - Explores the availability and accessibility of the tool**

04 **Scalability - Predicts the likely uptake of the tool based on the above**

Conventional security assessments do not adequately capture the complexity of modern attack methodologies. When organizations evaluate vendor claims regarding specific protections, such as deepfake detection capabilities, critical questions need to be asked. As demonstrated, 115,570 variations would need to be proven to back a claim of Face Swap detection, and this threat vector doesn't fully encapsulate all deepfakes.

This challenge is compounded by significant detection limitations:

- Many remote biometric verification systems lack real-time attack monitoring capabilities
- Successful attacks often go undetected until reported by impacted organizations
- Vendors may remain unaware of successful bypasses until after financial losses occur
- The delay between successful attacks and their discovery creates extended exposure
- The true scale of successful attacks is likely underreported, as organizations may attribute losses to other causes

Critical Considerations in Contemporary Security Testing Methodologies

Recent empirical evidence suggests a significant gap between perceived and actual security capabilities in remote identity verification systems. The evolving threat landscape, characterized by multiplicative attack vectors and rapid technological advancement, necessitates a reassessment of traditional security testing frameworks.

Conventional security assessments do not adequately capture the complexity of modern attack methodologies. When organizations evaluate vendor claims regarding specific protections, such as deepfake detection capabilities, critical questions need to be asked. As demonstrated, 115,570 variations would need to be proven to back a claim of Face Swap detection, and this threat vector doesn't fully encapsulate all deepfakes.

The documented success of recent synthetic media attacks has exposed vulnerabilities across multiple sectors, from financial losses to compromised workforce security. The KnowBe4 incident[13], where a cybersecurity company inadvertently hired someone using synthetic imagery during remote interviews, granting them authorized access to internal systems, demonstrates how synthetic identity fraud extends beyond financial theft to pose serious insider threats through workforce identity deception.

13. https://www.iproov.com/blog/knowbe4-deepfake-wake-up-call-remote-hiring-security

Such incidents reveal that current protection measures aren't adequately addressing these sophisticated threats, creating a dangerous gap between perceived and actual security capabilities. This disparity represents a significant organizational risk requiring immediate attention, particularly as remote hiring continues to be standard practice.

Many organizations might have an incomplete understanding of their security situation. Given the numerous ways attacks can occur, it's important to move beyond traditional security tests and focus on continuous monitoring and adaptation. Just because attacks aren't detected doesn't mean they aren't happening; it may be due to limited monitoring capabilities. To stay ahead, organizations need strong, flexible monitoring systems that can identify and analyze potential attacks in real time.

iProov's Leadership in International Testing, Benchmarking, and Security Frameworks

While traditional industry certifications from U.S. National Institute of Standards and Technology (NIST) and iBeta Quality Assurance establish important baseline security standards, the rapidly changing threat landscape requires a modern perspective. The FIDO Alliance's new "Face Verification Certification" program evaluates the robustness and interoperability of biometric solutions, specifically testing their effectiveness against presented deepfakes in controlled environments. While this certification represents progress in standardizing security testing, it's important to note that it currently focuses on presentation attacks rather than the full spectrum of potential deepfake threats throughout the identity lifecycle.

Our commitment to advancing biometric security has led to rigorous independent testing by the U.S. Department of Homeland Security's Science and Technology Directorate (DHS S&T) and cybersecurity leaders like Outflank, Jumpsec, and Kroll Redscan, validating our robust defense capabilities against emerging sophisticated attacks.

iProov actively shapes the future of biometric security through strategic collaborations. We are working with MITRE to expand their ATLAS framework, contributing our expertise in AI-powered attack detection and synthetic media threats. This collaboration helps establish standardized approaches for evaluating and defending against emerging attack vectors in remote identity verification systems.

Through our science-based approach and industry-leading research team, we have gained recognition as the most reputable scientific authority in facial biometric security. We regularly advise key organizations and governments, such as the European Union Agency for Cybersecurity (ENISA) and MITRE, helping raise awareness of real-world threats and establishing best practices for biometric security. Our insights drive industry standards and frameworks beyond traditional point-in-time testing limitations. This comprehensive approach ensures that our solutions remain effective against current and emerging threats while helping shape international standards for the next generation of biometric security challenges.

"iProov's collaboration with MITRE ATLAS has provided valuable insights into the evolving threat landscape. Our contribution to the documentation of attack patterns and detection methodologies—discovered through real-world attacks and comprehensive red teaming assessments—have helped create a more comprehensive understanding in the defense against AI based remote identity verification threats." - *Panos Papadopoulos, Head of Red Team, iProov*

Deeper Dive into the Threat Landscape:
The Low Attack Rate Paradox

While drop-off in attack rates may initially appear to simply indicate reduced threat actor interest, our analysis reveals a more nuanced security dynamic we term the "Low Attack Rate Paradox." This phenomenon occurs when robust security measures effectively deter attacks, causing threat actors to abandon their efforts and redirect resources toward more vulnerable targets.

Threat intelligence shows that attackers actively profile verification systems and share intelligence within their communities about which systems to avoid, making persistently low attack rates a strong indicator of security efficacy rather than reduced threat activity. This understanding is crucial for contextualizing our current security posture – the reduced attack volumes validate our ongoing security enhancements and demonstrate their continued effectiveness in maintaining a strong defensive position against evolving threats.

Strong Security Systems:
- Attacks are quickly abandoned
- Threat actors warn others in their communities
- Resources are redirected to easier targets
- Attack attempts remain low

Vulnerable Systems:
- Become frequent targets
- Experience sustained attack campaigns

Importance of Managed Detection and Response (MDR)
This pattern demonstrates why organizations need:

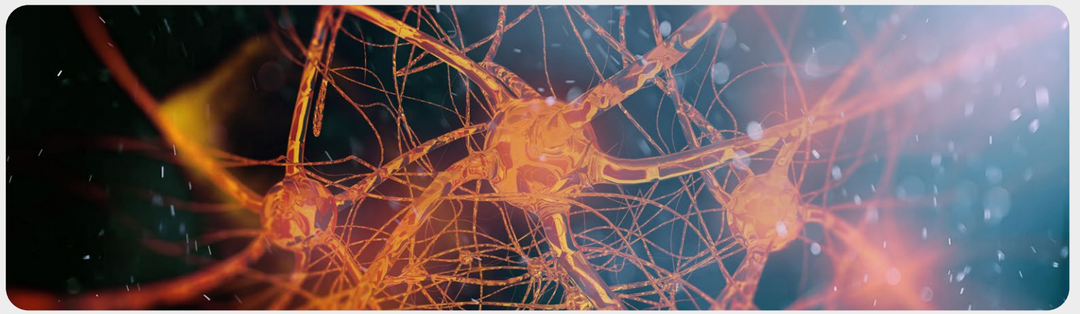
01 Strong preventative security measures

02 Continuous monitoring capabilities

03 Threat intelligence gathering

04 Regular security assessments

Even when attack rates are low, maintaining robust security remains critical - it's precisely these measures that keep attack rates low and protect against evolving threats.



Tech Stack Considerations:

Actionable Steps for Modern Identity

The evolving threat landscape demands a multi-layered approach to identity verification. The key is comprehensive strategies that combine technological innovation with human expertise while maintaining operational efficiency. The following framework outlines areas of focus for developing resilient security measures.

Embracing Real-Time Security

The era of periodic security updates has given way to continuous monitoring and detection systems operating in real time. This paradigm shift enables automated scaling of defenses during high-risk periods and seamless security patch deployment. Real-time security systems act as both shields and sensors, simultaneously protecting against known threats while identifying emerging attack patterns. This proactive approach helps identify and address potential vulnerabilities before they can be exploited at scale.

The Technology-Expertise Convergence

Success requires a strategic blend of automated systems and human expertise. Automated threat detection provides the speed and scale needed to manage verification attempts, while expert analysis delivers crucial insights for effective security operations. This synergy enables both immediate threat response and proactive vulnerability identification. Combining biometric scientists and machine capabilities creates a feedback loop where automated systems flag suspicious patterns for evaluation while human insights refine detection algorithms to better identify novel attack methods.

Developing Adaptive Security Strategies

Effective security measures evolve alongside the threat landscape through continuous evaluation and development of protective measures that anticipate future attack vectors. Successful strategies balance robust security with user experience, using sophisticated risk assessment to adjust security measures based on context and risk level. This prevents excessive friction from driving users toward less secure alternatives while maintaining appropriate protection levels.

Building a Collaborative Defense

Modern threats demand a combination of internal expertise and external intelligence. Partnerships with security experts, participation in threat intelligence networks, and dedicated research connections provide access to specialized knowledge and broader threat intelligence. Cross-organizational sharing of attack patterns and indicators strengthens collective defense capabilities beyond what individual security measures can achieve alone.

Preparing for Future Threats

A robust security architecture incorporates flexibility and scalability from the ground up, supported by clear processes for threat evaluation and rapid deployment of new security measures. Looking beyond current threats to consider emerging technologies' potential for both attack and defense ensures systems can adapt to evolving challenges while maintaining scalability for increasing attack volumes.

Conclusion:

Navigating the New Reality of Identity Security

The identity verification landscape has reached a critical inflection point. Our 2025 threat intelligence analysis reveals an increase in attack sophistication and a fundamental transformation in how identity deception is executed and commercialized. The advances in synthetic media tools, combined with thriving Crime-as-a-Service marketplaces, have created a democratized environment where complex attacks can be launched by actors with minimal technical expertise.

Several key developments define this new reality: The sheer scale of potential attack combinations—with over 100,000 possible permutations of just three common attack vectors—demonstrates that traditional, static security measures are no longer sufficient. Organizations must adapt to a threat landscape where attackers can rapidly switch tactics and targets, making real-time detection and response capabilities essential.

Our analysis of attack patterns reveals a crucial paradox: The most secure systems often show the lowest attack rates, as threat actors quickly abandon attempts against robust defenses in favor of easier targets. This “Low Attack Rate Paradox” underscores the importance of maintaining strong security measures even when apparent threat levels seem to decrease.

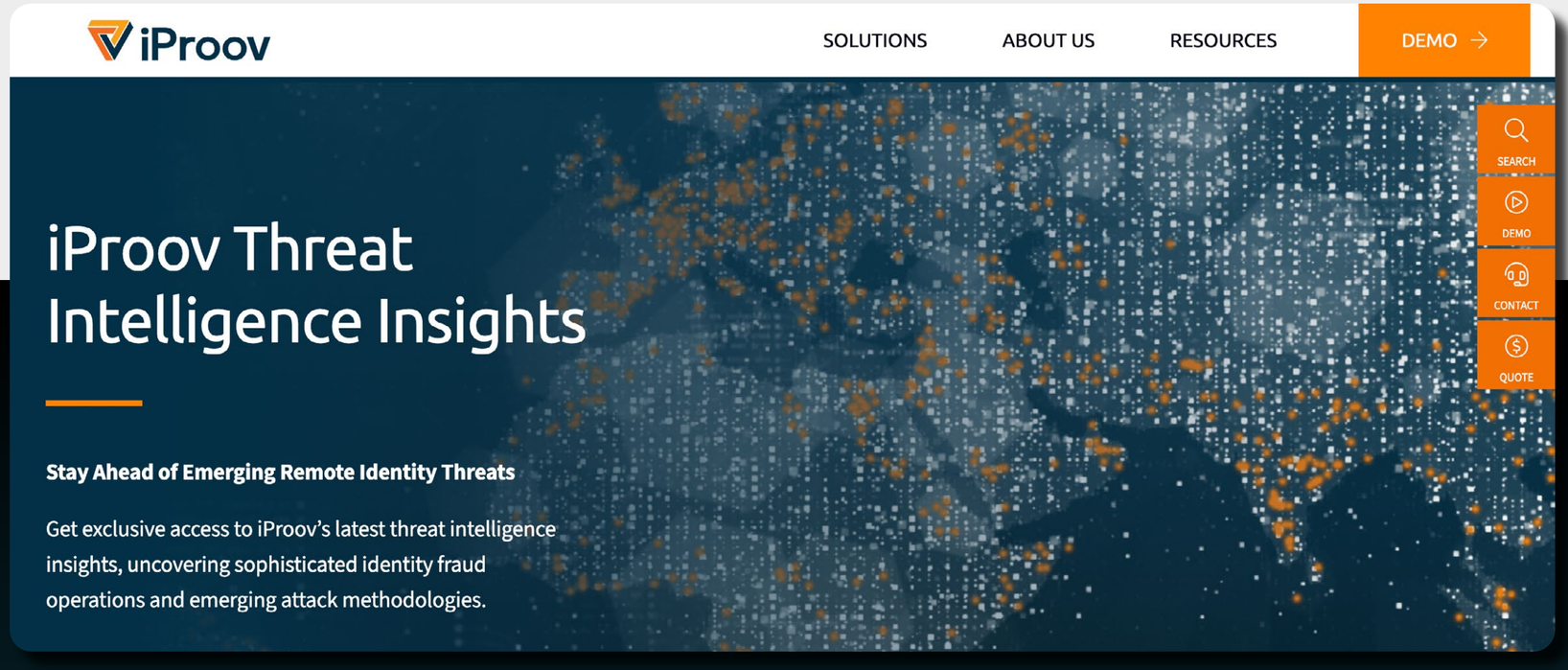
The human detection factor remains a critical vulnerability: Our deepfake research shows that only 0.1% of people can reliably identify synthetic media. This widespread susceptibility, combined with the increasing quality of synthetic content, creates unprecedented risks for remote identity verification systems.

01 **Real-Time Protection:** Moving beyond periodic updates to continuous monitoring and instant response capabilities

02 **Dynamic Defense:** Implementing security measures that evolve alongside emerging threats

03 **Human-Machine Collaboration:** Combining automated detection systems with biometric expert analysis and threat-hunting

The future of identity security lies not in any single technology or approach but in integrating multiple defensive layers powered by real-time threat intelligence and guided by deep scientific expertise. As we face a growing and increasingly complex threat landscape, the question is no longer whether organizations will face sophisticated identity attacks but how well they are prepared to detect and prevent them. Success in this new environment requires a commitment to continuous security evolution backed by threat intelligence, real-time MDR capabilities, and remote verification technology that goes beyond liveness detection to validate genuine human presence.



Need more comprehensive, regular insights into the remote threat landscape?

Register Your Interest

Threat Intelligence Monthly Subscription Report