iProov

Informe de inteligencia de amenazas 2025

Identidad remota bajo ataque

Contenido

Prólogo ejecutivo de Andrew Newell

El panorama de la verificación de identidad ha llegado a un punto de quiebre crítico. Durante el último año, hemos sido testigos de un enorme cambio, no solo en la sofisticación de los ataques, sino en la democratización fundamental de las capacidades de las amenazas. Lo que en el pasado era un campo dominado por actores altamente calificados, se ha transformado en un ecosistema accesible de herramientas y servicios que cualquier persona con la mínima experticia técnica puede aprovechar.

La escala de esta transformación es asombrosa. Por ejemplo, solo para un tipo de deepfake, el Face Swap, actualmente hemos detectado más de 120 herramientas de ataque activas; y los deepfakes mismos son solo una de las clases de imágenes que se pueden usar en los ataques de inyección. Al combinarlos con los diversos métodos de inyección y mecanismos de entrega, nos enfrentamos a más de 100.000 combinaciones posibles de ataques. Este crecimiento exponencial en las permutaciones de los ataques representa un desafío sin precedentes para los marcos de seguridad tradicionales.

Tal vez lo más preocupante es el salto en la calidad de los medios sintéticos. Antes el ojo humano podía detectar los deepfakes con certeza, pero esta certidumbre se ha erosionado. Los deepfakes ya no solo amenazan los sistemas biométricos, sino que representan desafíos fundamentales para cualquier sistema que dependa de imágenes para la verificación. Las implicaciones tienen un alcance que va más allá de los intentos de fraude individual, y posiblemente ponen en riesgo todo el marco de seguridad organizacional mediante un engaño sofisticado del personal.

El impacto financiero es igual de grave. Los datos del FBI señalan que solo durante el 2023, las actividades delictivas relacionadas con identidad generaron pérdidas de $8800 millones de dólares. Sin embargo, estas cifras solo cuentan parte de la historia. La transformación real recae en la naturaleza cambiante de estos ataques, que van desde incidentes aislados hasta sofisticadas campañas multivectoriales que corren el riesgo de pasar inadvertidas por meses, cuando no se ha implementado el monitoreo de amenazas adecuado.

Esta nueva realidad exige un replanteamiento fundamental de nuestro enfoque de la seguridad de la identidad. Contra las amenazas que evolucionan en tiempo real ya no es suficiente tener defensas estáticas y hacer actualizaciones periódicas. Para tener éxito, es necesario contar con monitoreo continuo, capacidades de adaptación rápidas, y lo más importante, la capacidad para detectar y responder a nuevos patrones de ataque antes de que se puedan explotar ampliamente.

A medida que exploramos este panorama en evolución, algo se hace evidente: el futuro pertenece a quienes se puedan adaptar y responder más rápido que las amenazas mismas. Este informe, además de ofrecer un análisis de las tendencias actuales, es una hoja de ruta para construir los marcos de seguridad resilientes y adaptables que se necesitan para afrontar estos desafíos emergentes.

Andrew Newell,
Chief Scientific Officer

Introducción:

Estado de la verificación de identidad remota: Amenazas e impacto económico (2024 - 2025)

El rápido crecimiento de la tecnologías basada en inteligencia artificial ha presentado nuevos retos para los sistemas de identificación remota. El fácil acceso a herramientas innovadoras ha permitido que los actores de amenazas se hagan más sofisticados de la noche a la mañana, generando una cantidad cada vez mayor de vectores de amenazas debido a las nuevas metodologías.

El creciente costo de las fallas de verificación de identidad

El crecimiento de nuevos vectores de ataque durante los últimos 24 meses ha afectado fuertemente a las organizaciones. El costo de no implementar de manera correcta la verificación de identidad remota tiene muchos aspectos. La Red de Vigilancia del Consumidor de la Comisión Federal de Comercio documentó un aumento del 45 % en los incidentes de robo de identidad a principios del 2024, con pérdidas consolidadas por fraude que exceden los $10.200 millones de dólares[1]. La segunda cantidad más alta de pérdidas reportada es por las estafas de impostores, con cerca de $2700 millones de dólares, lo que indica una trayectoria al alza en el impacto financiero.

Aunque las métricas tradicionales, como los costos y tiempos de detección de las vulneraciones siguen siendo indicadores importantes, solo cuentan parte de la historia. Lo más significativo es la naturaleza cambiante de estos ataques: de incidentes aislados a sofisticadas campañas multivector, que pueden permanecer sin detectarse durante meses. Este amplio periodo de tiempo hasta la detección, que, de acuerdo con IBM, frecuentemente supera los 270 días, crea oportunidades para que los actores de amenazas lleven a cabo esquemas de fraude complejos, lo que pone en riesgo, además de los activos inmediatos, sistemas de infraestructura digital completos.

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

El informe del costo de las vulneraciones de datos de IBM demuestra que las vulneraciones de seguridad relacionadas con identidad ahora cuestan un promedio de $4,24 millones de dólares por incidente, y el robo de credenciales corresponde al 19 % de los eventos registrados. Es importante que las organizaciones sepan que el tiempo promedio para la detección y contención llega hasta los 277 días, lo que crea un periodo de tiempo sustancial de vulnerabilidad para actividades de fraude descendente.

La gravedad de esta amenaza se ve reflejada en varios incidentes de alto perfil sucedidos en 2024:

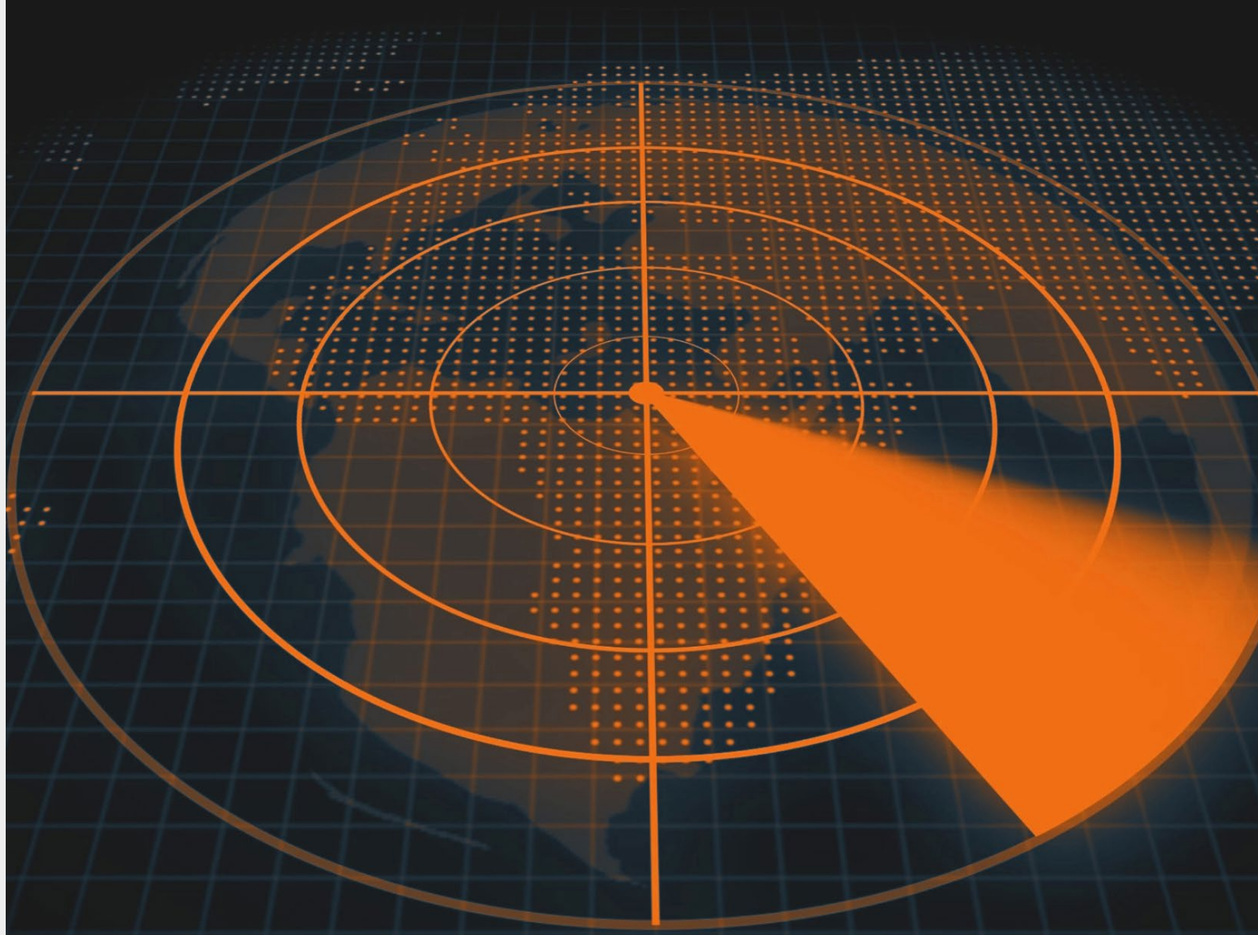
- T-Mobile (enero de 2024): Exposición de 37 millones de registros de usuarios, dando como resultado una conciliación por $350 millones de dólares[2]
- Microsoft (agosto de 2024): Los atacantes llevaron a cabo ataques con bots a gran escala contra sistemas CAPTCHA y los usaron para crear 750 millones de cuentas de Microsoft falsas[3]
- LoanDepot (enero de 2024): Incidente de ransomware que dio como resultado la filtración de datos de identificación de los clientes y perturbaciones sistémicas[4]

"Estos incidentes demuestran que hay un cambio crítico en la metodología de los ataques: los actores de amenazas ya no solo roban datos, ahora suplantan a personas confiables mediante herramientas de Face Swap, o crean identidades sintéticas nuevas para implementar estrategias de fraude a largo plazo". -

Andrew Newell, Chief Scientific Officer, iProov

Aunque el mercado reconoce que hay necesidad de medidas de seguridad mejoradas, las organizaciones afrontan retos significativos cuando se trata de seleccionar e implementar las soluciones adecuadas.

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/



Precauciones para el comprador: Dos desafíos de la compra de tecnología de la seguridad

Al proteger sus sistemas de verificación de identidad remota, las organizaciones enfrentan dos desafíos. El primero es que hay una brecha de conocimiento fundamental respecto a la comprensión y compra de tecnologías de verificación remota adecuadas basadas en casos de uso y datos contextuales. Esta brecha de conocimiento se ilustra claramente en el Informe ID IQ 2025 de RSA[5], que ha detectado que casi la mitad de los encuestados respondieron equivocadamente al menos la mitad de las preguntas relacionadas con conceptos básicos de seguridad de identidad, siendo los que peor desempeño tuvieron los expertos en gestión de identidad y acceso (IAM) y ciberseguridad.

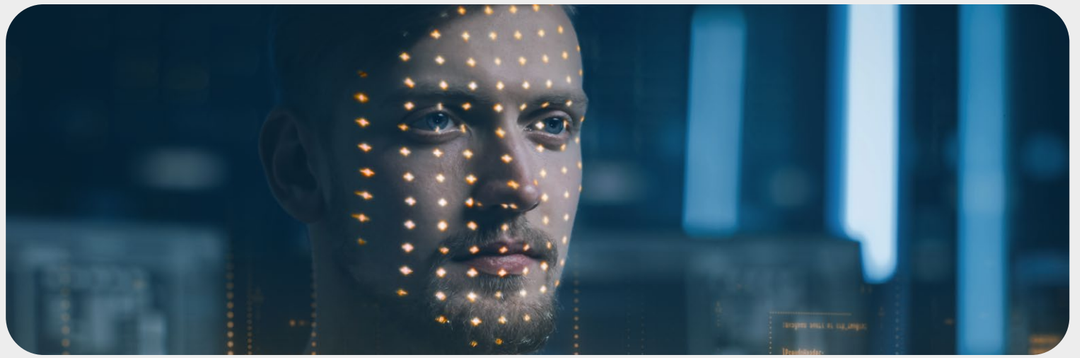
El segundo, que es igual de preocupante, es la prevalencia de afirmaciones exageradas de los proveedores sobre las capacidades de seguridad. Nuestros hallazgos de inteligencia de amenazas revelan que muchas soluciones que afirman ofrecer protección integral contra los ataques con medios sintéticos no tienen las bases tecnológicas para prevenirlos. Esta disparidad entre las capacidades ofrecidas y la protección real deja vulnerables a las organizaciones y crea un falso sentido de seguridad.

El informe de RSA destaca este riesgo usando como ejemplo a la industria aeroespacial. A pesar de ser el sector con mayor probabilidad de sufrir vulneraciones graves relacionadas con identidad, con costos de más de 10 millones de dólares, paradójicamente, las empresas aeroespaciales reportan tener la máxima confianza en su capacidad para manejar los derechos de acceso de los usuarios.

Este complejo panorama exige un enfoque más matizado a la compra de seguridad. Debe ir más allá de las garantías que hacen los proveedores y las evaluaciones tradicionales centradas en el cumplimiento para llegar a evaluaciones de seguridad integrales que incluyan:

- Verificación independiente de las afirmaciones de seguridad: es particularmente importante, dado que el 66 % de las organizaciones que sufrió vulneraciones relacionadas con identidad las calificó como eventos graves
- Capacidad de detección y respuesta gestionadas
- Monitoreo continuo con sistemas de detección de amenazas en tiempo real: es especialmente importante, ya que el 42 % de las organizaciones reportó que sufrieron vulneraciones relacionadas con identidad en un periodo de tres años
- Demostrar capacidad de adaptación a los vectores de ataque emergentes: es crítico, ya que el 80 % de los encuestados cree que la inteligencia artificial afectará significativamente la ciberseguridad durante los próximos cinco años

Al no abordar tanto la brecha de conocimiento como los problemas de responsabilidad de los proveedores, las organizaciones corren el riesgo de implementar soluciones que en papel parecen robustas, pero que demuestran ser insuficientes contra los ataques del mundo real. El riesgo es cuantificable: El informe de RSA encontró que el 44 % de los encuestados estima que los costos relacionados con las vulneraciones relacionadas con identidad, que el 21 % reportó que cuestan más de 10 millones de dólares, excede los costos de las vulneraciones de datos típicas.



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

Enseñanzas clave

01 El panorama de ataques se transformó fundamentalmente

- Las herramientas de ataque se han democratizado y comercializado
- Más de 100.000 posibles combinaciones de ataques se han identificado de solo tres vectores
- Las herramientas de ataque individuales han evolucionado para convertirse en cadenas de ataques sofisticadas

02 Los enfoques de seguridad tradicionales ya no son suficientes

- Las actualizaciones de seguridad periódicas ya no pueden mantener el ritmo de las amenazas en evolución
- Las pruebas estáticas no pueden capturar la complejidad de los ataques modernos
- Las organizaciones deben cambiar el monitoreo de seguridad periódico por uno continuo

03 Las capacidades de detección humanas tienen graves limitaciones

- Solo el 0,1 % de las personas pueden identificar todos los medios sintéticos con confianza[6]
- El exceso de confianza en las capacidades de detección crea riesgos adicionales
- Las soluciones técnicas deben compensar las vulnerabilidades de los humanos

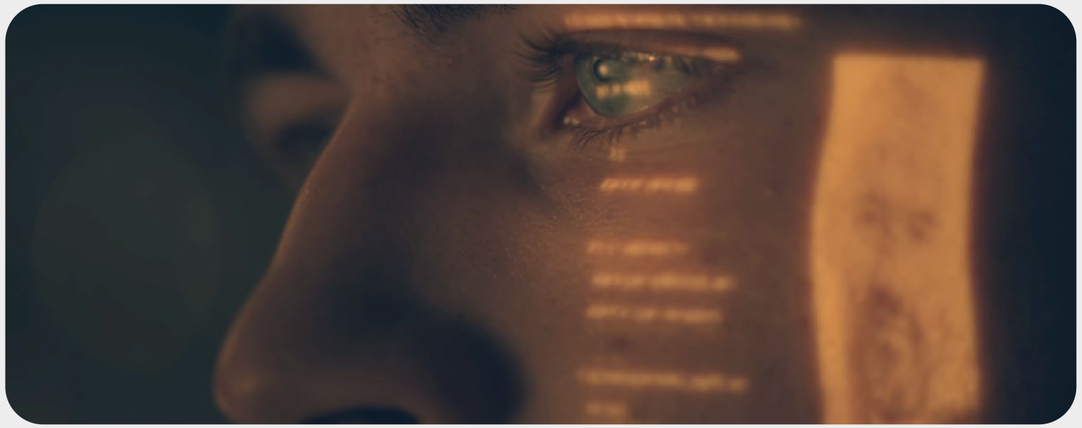
04 El éxito de la seguridad requiere un enfoque de varias capas

- Es fundamental contar con capacidades de detección y respuesta gestionadas en tiempo real
- El monitoreo y la adaptación continuos deben reemplazar las defensas estáticas
- La integración de los sistemas automatizados con la experticia humana es fundamental

05 Los patrones de ataque ahora son más sofisticados

- Los actores de amenazas perfilan activamente e intercambian inteligencia sobre sus objetivos
- Con frecuencia las tasas de ataque bajas son un indicador de una seguridad robusta, no de menos amenazas
- Los atacantes cambian rápidamente para centrarse en objetivos más vulnerables

Estos hallazgos destacan un imperativo claro: las organizaciones deben repensar su enfoque de seguridad de la identidad desde las bases. Tener éxito en este nuevo entorno exige comprometerse con la evolución continua de la seguridad, respaldada por inteligencia de amenazas robusta y capacidades de detección y respuesta gestionadas (MDR) en tiempo real. El futuro pertenece a los proveedores y organizaciones que puedan adaptarse y responder a las nuevas amenazas, en vez de confiar en defensas estáticas.



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

Informe de inteligencia de amenazas de iProov:
Metodología y alcance

El Informe de inteligencia de amenazas recoge los datos compilados del Centro de Operaciones de Seguridad de iProov (iSOC). Nuestro enfoque especial orientado por ciencia nos permite recopilar y analizar datos de ataques del mundo real, para ofrecer visibilidad sin precedentes de las amenazas emergentes que tienen como objetivo los sistemas de verificación remota.

Los hallazgos que se presentan en este informe provienen de:

- Datos de detección de amenazas y respuesta en tiempo real del iSOC
- Recopilación de inteligencia de amenazas externas y monitoreo de la web oscura
- Campañas de pruebas de penetración del equipo rojo interno
- Investigación de seguridad biométrica avanzada e inteligencia de amenazas interna
- Análisis de patrones de los ataques detectados y prevenidos
- Evaluación técnica de las herramientas y metodologías de ataque emergentes

"En 2014, para crear identidades sintéticas era necesario tener experticia técnica extensa, equipos especializados y hacer una significativa inversión en tiempo. La inteligencia artificial ha revolucionado este ámbito, permitiendo la generación en tiempo real de medios sintéticos sofisticados". - *Andrew Newell, Chief Scientific Officer, iProov*

Mediante la continua detección de amenazas en tiempo real, nuestros expertos en seguridad defienden contra los ataques actuales e identifican los patrones de amenazas emergentes, haciendo posibles las mejoras de seguridad predictiva para nuestras defensas. Este informe ofrece análisis y reflexiones sobre los vectores de ataque emergentes y las tácticas de adversarios en evolución a medida que entramos en el panorama de verificación de identidad remota del 2025.

La evolución del engaño de identidad

Cronología e impacto de 2014 a 2024: Superado el punto de no retorno

El avance de las capacidades de engaño de identidad entre el 2014 y el 2025 representa un cambio fundamental tanto de tecnología como de accesibilidad. Esta cronología ilustra esta rápida transformación, de ataques complejos y especializados a herramientas y servicios ampliamente accesibles y disponibles.

Esta democratización ha sido acelerada por tres tendencias convergentes: avance tecnológico rápido, la emergencia de los mercados de crimen como servicio (CaaS), y la transición de los ataques con medios sintéticos de amenazas teóricas a delitos financieros documentados.

2014

Introducción a las redes GAN

2016

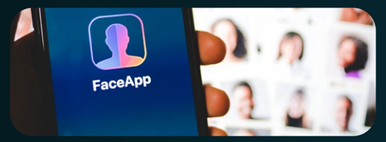
Los deepfakes emergieron con el surgimiento del aprendizaje profundo, cuyas primeras comunidades se formaron en Reddit.

2017

Primera herramienta generalizada para la creación deepfakes (FakeApp); Face Swap de calidad de limitada a deficiente en videos

2018

Primeros intercambios de rostros



2019

Modelo de gestos de primer orden (FOMM, por sus siglas en inglés)

2020

Los deepfakes de audio aparecieron al tiempo con herramientas como Descript Overdub y Wave2Lip

2021

Lanzamiento de DALL-E

2022

El surgimiento de la generación de imágenes accesible, la clonación de voces y los deepfakes en tiempo real llevaron a iProov a publicar su primer Informe de inteligencia de amenazas.

2023

Proliferación de intercambios de rostros; Deepfakes de audio de alta calidad; Lanzamiento de GPT-4

2024

Alta calidad Intercambios de rostros

De la investigación al impacto en el mundo real

La última parte de 2023 marcó un punto de quiebre crítico en esta evolución. Lo que principalmente había existido en laboratorios de investigación y demostraciones de pruebas de conceptos, se materializó en ataques sofisticados causantes de pérdidas financieras sustanciales.

Aunque se ha prestado mucha atención al fraude de identidad del consumidor, los ataques más importantes y costosos del 2024 fueron dirigidos a los sistemas de verificación de personal. Este cambio hacia atacar objetivos del sector corporativo revela una tendencia preocupante: los actores de amenazas sofisticados están explotando los procesos de trabajo remoto y los canales de comunicación corporativos para lograr el máximo impacto.

Un ejemplo de esto fue la estafa[7] con deepfake en Hong Kong por $25,6 millones de dólares, a una empresa multinacional en la cual los atacantes usaron medios sintéticos para suplantar a ejecutivos en llamadas de conferencia, eludiendo los protocolos tradicionales de verificación corporativos. Este incidente demostró que los ataques de identidad sintética pueden, además de arriesgar los activos financieros, llevar a vulneraciones de seguridad organizacional profundas mediante el aprovechamiento de la vulnerabilidad del personal.

Estos casos representan un cambio estratégico de los actores de amenazas, que han descubierto las vulnerabilidades críticas de los sistemas de verificación corporativos. Al fijar como objetivo los procesos de contratación de personal remota, las comunicaciones de los lugares de trabajo virtuales y las videoconferencias de ejecutivos, los atacantes están logrando obtener mayores beneficios que con el fraude al consumidor tradicional. Este cambio de objetivo, de las personas a las organizaciones, pone al descubierto una peligrosa brecha en la verificación de identidad de la fuerza laboral, algo que los marcos de seguridad corporativa actuales están teniendo dificultades para abordar.

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/

El informe del panorama de las amenazas a la seguridad de la identidad de 2024 de CyberArk[8] reveló que solo el año pasado el 93 % de las organizaciones sufrieron de dos o más vulneraciones relacionadas con la identidad. Estos incidentes validan las preocupaciones de larga data sobre el impacto potencial de los medios sintéticos.

Estos ataques exitosos demuestran varios desarrollos:

01 **Validación operacional:** Lo que antes era teórico ahora ha demostrado ser efectivo en escenarios del mundo real, proporcionando a los actores de amenazas metodologías documentadas e historias de éxito. Es probable que esta validación acelere la adopción de tácticas similares en todas las redes criminales.

02 **Vulneración tradicional de los sistemas de varias capas:** Estos ataques han tenido éxito invalidando varias capas de seguridad a la vez:

- Juicio humano en entornos profesionales
- Protocolos de seguridad corporativa
- Mecanismos de detección de fraude tradicionales

03 **Escalabilidad de los ataques:** El éxito comprobado de estos métodos, en combinación con la disponibilidad de plataformas de crimen como servicio crea el potencial para:

- Replicar rápidamente las metodologías de ataque exitosas
- Llevar a cabo ataques en paralelo contra varias organizaciones
- Enfocar los sectores vulnerables con automatización
- Permitir que actores con menos habilidades lleven a cabo patrones de ataque sofisticados

04 **Vulnerabilidad organizacional:** Estos ataques ponen al descubierto debilidades institucionales más amplias:

- Sobreexposición a métodos de verificación desactualizados
- Protocolos inadecuados para transacciones remotas de alto valor
- Capacidades limitadas de detección y respuesta gestionadas en tiempo real

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

Para desarrollar contramedidas efectivas contra las amenazas actuales y emergentes es fundamental entender esta progresión. La peligrosa combinación de las afirmaciones exageradas de los proveedores y nuestra convicción errada de que podemos detectar los deepfakes es una receta para el desastre.

Investigación del consumidor: Punto ciego de los deepfakes

El informe de investigación deepfakes de consumidor del 2025[9] de iProov presenta el panorama de una sociedad que en gran medida no está preparada para los desafíos que supone la tecnología de los deepfakes, con brechas significativas en la conciencia, las capacidades de detección y los mecanismos de respuesta.

Hallazgos clave:

- Tasa de éxito de la detección: Solo el 0,1 % de los participantes pudieron identificar correctamente todas las muestras de medios sintéticos.
- Vulnerabilidad del video: La tasa de éxito de la detección de deepfakes de video fue particularmente baja, con el 9 %.
- Vulnerabilidades relacionadas con la edad: Se encontró que las personas mayores de 55 años son particularmente vulnerables, ya que casi un tercio de ellas nunca había escuchado de los deepfakes, lo que limita la capacidad que tienen para identificar y protegerse contra esta tecnología.
- Brecha de confianza: Los más jóvenes, de 18 a 34 años, demostraron un peligroso exceso de confianza en sus capacidades de detección, a pesar de su bajo desempeño.

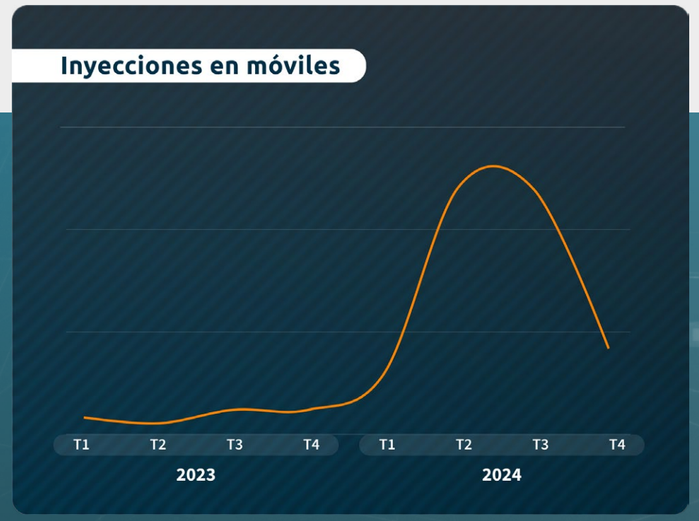
Capacidades de respuesta:

- 48 % de las personas no tienen conocimiento de los procedimientos adecuados para reportar los deepfakes
- 25 % de las personas verifica la información usando fuentes alternativas
- 11 % de las personas realiza análisis de fuentes crítico
- 29 % de las personas no hace nada cuando encuentra posibles deepfakes

Datos de iProov de 2023 en comparación con 2024 sobre tendencias de ataques clave año tras año

Ataques de inyección: Aumento del 783 %

Durante el 2024 se observó un rápido aumento en la frecuencia y escala de los vectores de ataque basados en inyección dirigidos a aplicaciones web móviles, lo que sugiere un cambio fundamental en las capacidades y accesibilidad de las herramientas de ataque.



Cámaras nativas virtuales: Aumento del 2665 %

Uno de los eventos más significativos del 2024 es tal vez la dramática reaparición de los ataques de cámaras nativas virtuales y la velocidad con la que llegaron. El cuadro demuestra la necesidad de contar con detección y respuesta gestionadas en tiempo real.

Intercambios de rostros: Aumento del 300 %

Los ataques de Face Swap, ya una tendencia alarmante al ser descubiertos en 2023, persistieron en 2024 y tuvieron un pico en el segundo trimestre de ese año. En la sección “Cuatro tendencias clave” de este informe exploramos la naturaleza de su evolución.

Tendencias emergentes

Esta sección presenta los hallazgos del equipo de inteligencia de amenazas de iProov respecto a la evolución de las metodologías de ataque y sus implicaciones para los marcos de verificación de identidad contemporáneos.

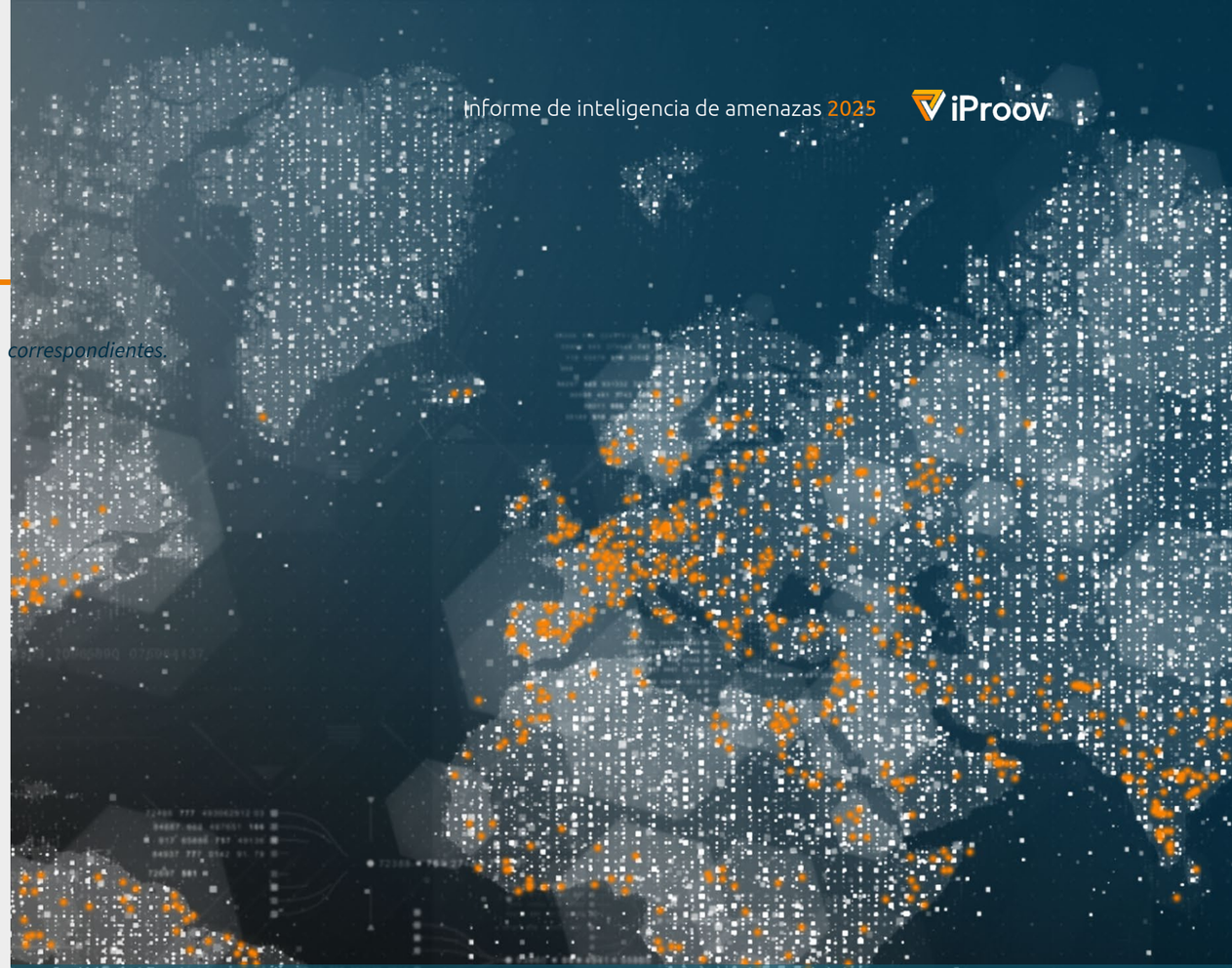
A finales del año pasado, el iSOC descubrió un grupo de la web obscura que había reunido una colección significativa de documentos de identidad con sus correspondientes imágenes faciales. Estas identidades fueron diseñadas específicamente para eludir los procesos de verificación de Conozca a su cliente (KYC). En cambio de ser adquiridos mediante robo tradicional, parece que las personas suministraron voluntariamente estas identidades a cambio de un pago.[10]

Descubrimiento: Una colección a gran escala de documentos de identidad e imágenes faciales legítimas
Método: Entrega voluntaria de las credenciales a cambio de un pago
Impacto: Creación de identidades falsas basadas en documentos genuinos para evadir la detección
Alcance geográfico: Fue identificado inicialmente en América Latina, y ahora está vinculado a redes de fraude europeas

Con el pico de ataques de intercambios de rostros y cámaras nativas virtuales, los adversarios pueden aprovechar documentos genuinos que no activan las alarmas de fraude para intercambiar el rostro de una identidad genuina superponiendo su rostro y verificándose remotamente mediante videoconferencias u otros medios de verificación facial del usuario remota.

Todas las actividades delictivas descubiertas por nuestro equipo son reportadas a las autoridades locales correspondientes.

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



"Las tecnologías de prueba de vida son cada vez más críticas para la defensa contra los deepfakes y la verificación de la presencia genuina de las personas".

2024 Gartner® Emerging Tech: El impacto de la inteligencia artificial en el informe de la verificación de identidad[11]

Cuatro tendencias para observar en 2025

Tendencia 1: Surgimiento de las cámaras nativas virtuales

Observaciones clave:

- Los ataques con cámaras nativas virtuales evolucionaron, de su fase experimental en 2023, para convertirse en una amenaza principal en 2024, con un pico de 785 ataques semanales durante el segundo trimestre.
- Lo más preocupante es que para estos ataques no es necesario tener dispositivos rooteados o con jailbreak, haciéndolos accesibles para actores de amenazas sin habilidades técnicas avanzadas.
- El descubrimiento de una aplicación de cámara maliciosa en una de las principales tiendas de aplicaciones demuestra cómo se pueden “democratizar” estos ataques con herramientas fáciles de usar.

Lo que empezó como un vector de amenaza experimental en 2023 evolucionó para convertirse en una de las tendencias más significativas del 2024, llegando a un pico de 785 ataques con cámara nativa semanales en el segundo trimestre. El descubrimiento de la aplicación de cámara maliciosa en una de las principales tiendas de aplicaciones reveló que para estos ataques no es necesario tener herramientas de hackeo sofisticadas ni dispositivos rooteados, haciendo que las medidas de ciberseguridad tradicionales, como la detección de rooteo, sean insuficientes. Aunque fue eliminada de la tienda oficial, la aplicación sigue disponible de otras fuentes, lo que permite el acceso fácil a los ataques de inyección.

Este desarrollo cuestiona la noción de que los ataques de inyección son únicamente amenazas biométricas o de ciberseguridad. La evidencia demuestra claramente que una defensa robusta requiere que las medidas de detección de prueba de vida robustas y la ciberseguridad trabajen al unísono. Los patrones de ataque observados sugieren que los actores de amenazas están explorando activamente este enfoque de doble vector.

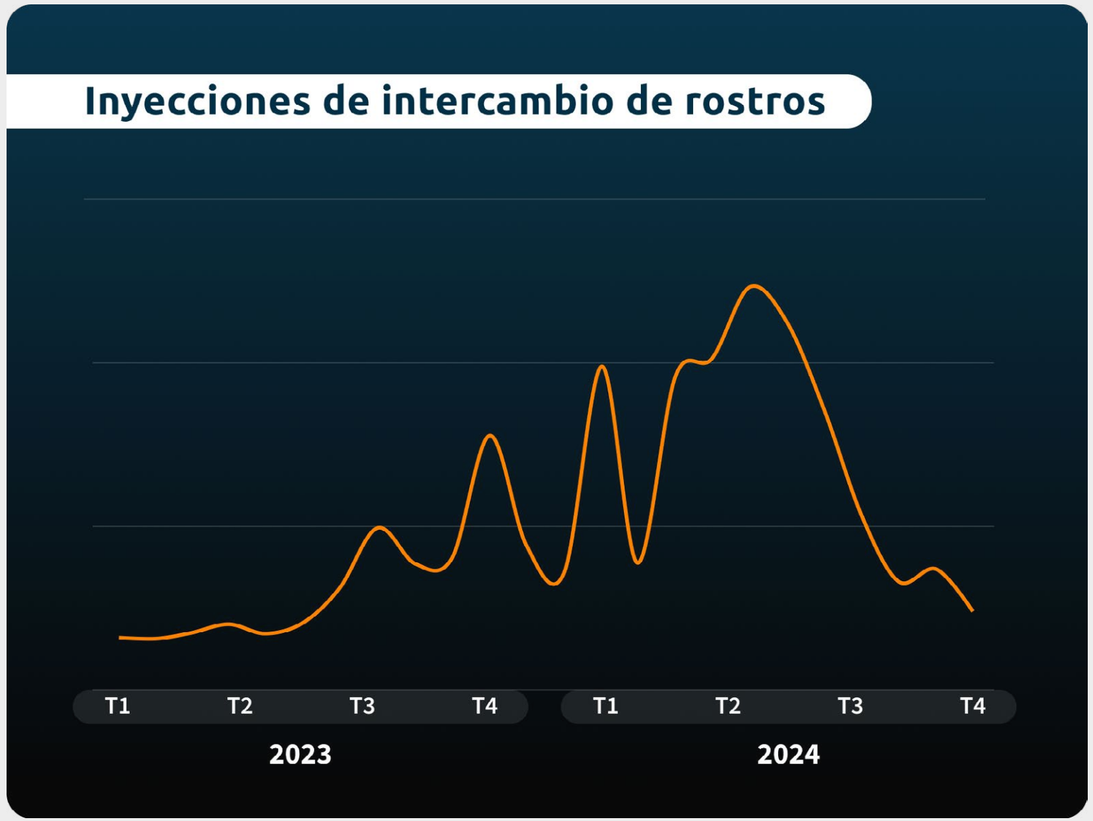
Tendencia 2: Proliferación de los intercambios de rostros

Observaciones clave:

- En 2024, el volumen de los ataques aumento un 300 % con respecto al 2023.
- La cantidad de herramientas usadas en estos ataques aumentó en 15,5 %, pasando de 110 a 127
- Los actores de amenazas aprovechan la inteligencia compartida para explotar sistemas vulnerables usando una diversidad de herramientas de Face Swap.

El panorama de los ataques de Face Swap aumentó significativamente el año pasado; y la cantidad de herramientas detectadas se incrementó de 110 a 127. El primer trimestre del 2024 reveló un patrón claro: los actores de amenazas adaptaron sus tácticas luego del despliegue generalizado inicial. Notablemente, luego de la etapa de experimentación a gran escala en la primera mitad del año, la inteligencia compartida sobre las vulnerabilidades del sistema cambió eficazmente su enfoque hacia la “presa más fácil”. Observamos que se alejaron de la plataforma iProov prefiriendo sistemas que usan detección de prueba de vida activa que pide a los usuarios hacer ciertas acciones o movimientos. Estos sistemas son más fáciles de eludir, ya que sus patrones de desafío-respuesta pueden replicarse con videos pregrabados y sintéticos.

En 2024, el debate sobre las herramientas y técnicas de Face Swap era más prominente en los foros de actores de amenazas, impulsado por el intercambio de información y herramientas entre las comunidades maliciosas.



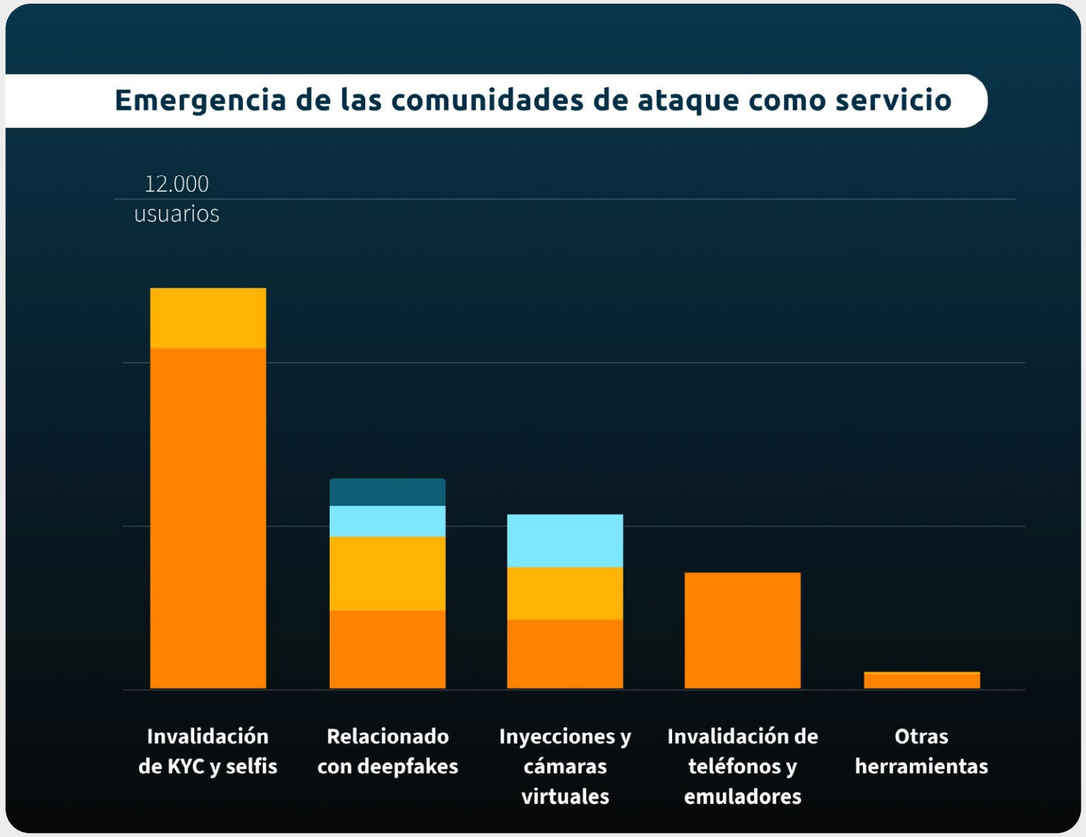
Tendencia 3: Comunidades de ataque como servicio en línea

Observaciones clave:

- En 2024 se identificaron otros 31 grupos de actores de amenazas en línea, y el más grande tenía 6400 usuarios.
- Los grupos que venden herramientas atienden al 68 % (23.698) de los usuarios, lo que es un indicador de su eficacia y credibilidad.
- Los métodos de ataque se enfocan cada vez más en eludir el NYC, los deepfakes y en herramientas específicas para Android. Estos grupos están cambiando hacia soluciones más integrales en vez de servicios independientes.

En 2024, se identificaron otros 31 grupos de actores de amenazas en línea, de los cuales el 45 % vendía sus propias herramientas y el 55 % revendía o prestaba servicios relacionados. Este ecosistema comprende 34.965 usuarios en total, y los vendedores de herramientas atraen a 23.698 usuarios, comparado con 11.267 para no vendedores. Hay nueve grupos con más de 1500 usuarios, y el más grande de estos llega a 6400 miembros. Los debates comunes se centran en las técnicas para eludir el NYC, la tecnología deepfake y las herramientas para Android.

El enfoque ha sido significativo en las plataformas móviles, especialmente en Android. Algunos grupos ofrecen paquetes de herramientas y servicios, mientras que otros están especializados en áreas como la recopilación sistemática de identificaciones (identity farming) y los mercados de criptomonedas.



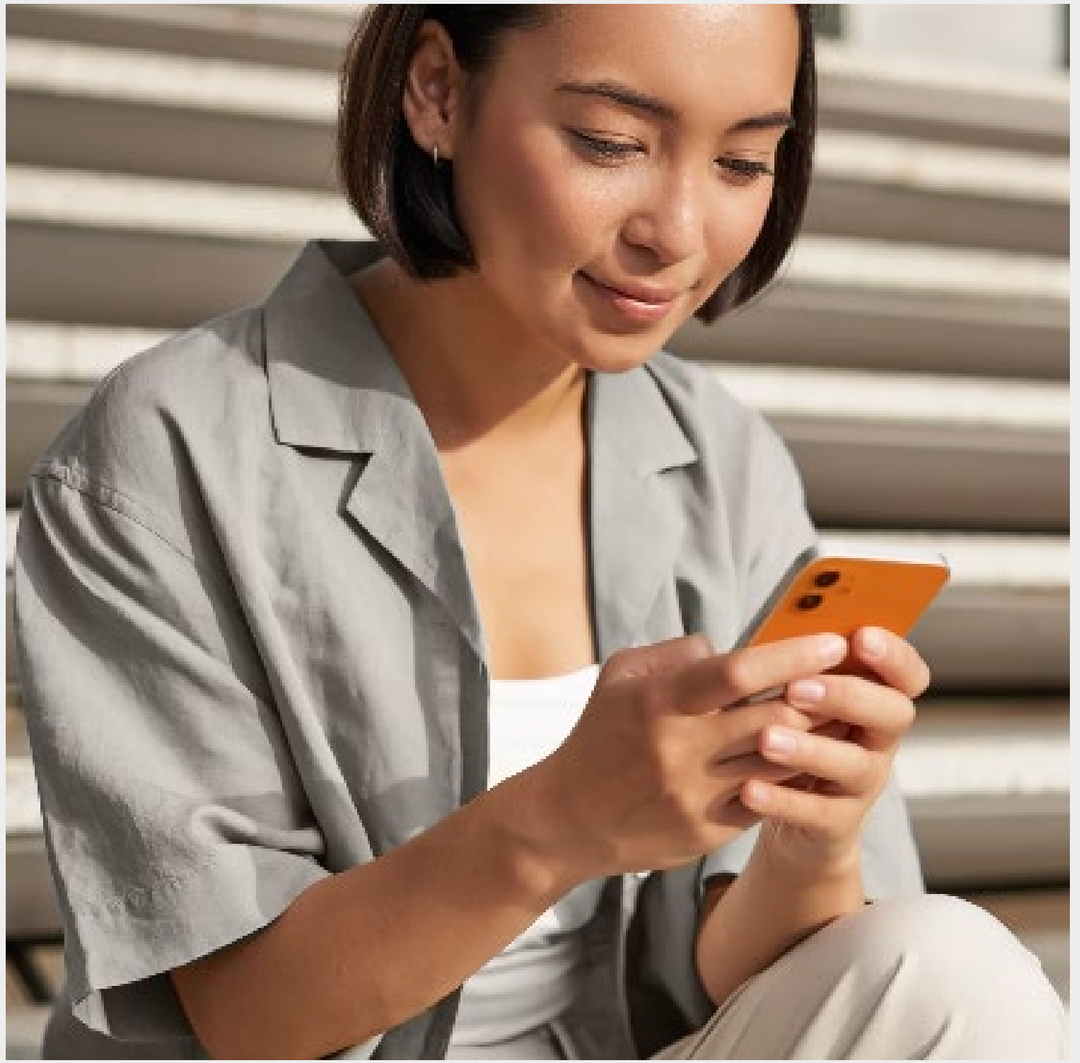
Tendencia 4: Conversión de imagen a video
Un nuevo vector de ataque con identidad sintética

Observaciones clave:

- Las herramientas de conversión de imagen a video han simplificado la creación de identidades sintéticas hasta ser un proceso simple de dos pasos que solo requiere mínima experticia técnica.
- Nuestras pruebas muestran que las identidades sintéticas animadas suponen una amenaza significativa para muchos sistemas de prueba de vida, como los mecanismos de desafío-respuesta activos.
- La perfección de la naturaleza de la salida de medios sintéticos, sin los típicos artefactos de la manipulación, dificulta excepcionalmente la posibilidad de detectarlas una vez que están animadas con movimiento fluido.

Estos ataques han sido ineficaces contra nuestra plataforma Dynamic Liveness, que usa la tecnología patentada[12] Flashmark® para verificar la presencia humana genuina empleando mecanismos de desafío-respuesta pasivos.

Nuestro equipo científico identificó una evolución significativa en el fraude de identidad sintética mediante la tecnología de conversión de imagen a video, que se observó por primera vez en un intento de ataque contra nuestra plataforma en diciembre de 2024. Esta técnica transforma imágenes estáticas en contenido de video convincente que podría suponer desafíos muy significativos para la mayoría de los sistemas de verificación de identidad remota. Mientras los ataques de identidad sintética por lo general usan intercambios de rostros, manipulación de metadatos y vulneración de cámaras, este nuevo vector de ataque simplifica el proceso en dos pasos: los actores de amenazas obtienen o crean una imagen sintética de un rostro, y luego, utilizan herramientas de conversión de imagen a video para animarlas con un movimiento fluido que se imita fielmente el contenido de video genuino.



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

El fraude de identidad sintética (SIF) es el tipo de fraude con mayor crecimiento

El fraude de identidad sintética (SIF) es el tipo de fraude con mayor crecimiento, con implicaciones particularmente alarmantes. Este sofisticado esquema combina datos legítimos, como números de seguridad social válidos, frecuentemente robados a niños, adultos mayores o difuntos, con información personal fabricada para crear identidades falsas convincentes. Luego, los estafadores construyen la credibilidad de estas identidades sintéticas creando historiales crediticios, abriendo varias cuentas en diferentes instituciones y creando huellas digitales que parecen auténticas.

Su capacidad de evadir los sistemas de detección de fraude tradicionales es lo que hace que sea especialmente difícil combatir el fraude de identidad sintética. Al contrario del robo de identidad tradicional, donde los sistemas pueden alertar sobre la información robada con base en los informes de las víctimas reales, el fraude de identidad sintética crea entidades completamente nuevas que incorporan elementos tanto reales como falsos. Como no hay víctimas reales que alerten, y algunos de los componentes de la identidad son legítimos, los métodos de detección tradiciones con frecuencia no pueden reconocer estos patrones de fraude con identidad sintética.

Muchos sistemas de verificación de identidad remota tienen dificultades para detectar las imágenes manipuladas de los videos, porque al contrario de las imágenes genuinas que son alteradas a nivel de píxel, los rostros sintéticos no muestran estos signos de manipulación tradicionales. Al animarlas, estas identidades sintéticas parecen increíblemente vívidas, dificultando que el ojo humano pueda detectarlas. Las accesibilidad y eficacia de estas herramientas sugiere que el uso de la técnica aumentará. Este desarrollo marca una evolución significativa en el fraude de identidad sintética, por lo que será necesario monitorearlo e investigarlo durante el 2025.

Permutaciones de los ataques:
El panorama de amenazas exponencial

La complejidad de los ataques de verificación de identidad remota va más allá de herramientas o técnicas individuales. Hoy en día, los actores de amenazas utilizan sofisticadas combinaciones de herramientas, lo que crea una superficie de ataque exponencialmente mayor de la que muchas organizaciones conocen y están preparadas para proteger. Es fundamental comprender estas permutaciones para implementar pruebas de seguridad y estrategias de defensa integrales.

Fuente: This Person Does Not Exist

Fuente: iProov Threat Intelligence Library

Clases de deepfakes

Componentes básicos de los ataques y sus variables

01 Herramientas de manipulación de rostros

- Actualmente monitoreamos 127 diferentes aplicaciones de Face Swap
- Cada herramienta ofrece capacidades y calidad de salida diferentes
- Varios grados de capacidad de detección y sofisticación
- Van desde aplicaciones para nivel de consumidor hasta avanzadas soluciones con inteligencia artificial

02 Emuladores de dispositivos móviles

- Actualmente monitoreamos más de 10 nuevas tecnologías de emulación
- Algunas de las capacidades son la suplantación de ubicación y la manipulación de características del dispositivo
- Varias configuraciones de sistema operativo y hardware
- Capacidades de evasión de la detección con diferentes niveles

03 Software de cámara virtual

- Actualmente monitoreamos 91 herramientas de cámaras virtuales
- Van desde inyección básica de video hasta manipulación de transmisión sofisticada
- Varios métodos para eludir los controles de seguridad del dispositivo
- Diferentes capacidades de manipulación de metadatos

El efecto multiplicador

La verdadera escala de los posibles ataques surge cuando se combinan estas herramientas:

Cálculo básico:
127 herramientas de Face Swap
× 10 emuladores
× 91 cámaras virtuales
= 115.570 posibles combinaciones de ataques

Cada combinación representa un vector de ataque diferente para el cual se necesitan estrategias de detección y prevención específicas. Puesto que se introducen nuevas herramientas y actualizaciones, estas combinaciones aumentan constantemente. Por simplicidad, el ejemplo proporcionado en este informe calcula las tres combinaciones de ataque más representativas. Sin embargo, no se deben olvidar las herramientas disponibles de imágenes generadas por computador (CGI) y modelos de gestos de primer orden (FOMM), que también estamos monitoreando.

Puntos de entrada

Cámaras virtuales

- **Intercambios de rostros**
  - **Manipulación de metadatos**
    - Manipulación de los datos de los sensores del dispositivo
  - Deepfakes
  - CGI
  - Recreaciones
- Ataque de intermediario
  - Intercambios de rostros
  - Deepfakes
  - Medios sintéticos
- Reproducción
  - Intercambios de rostros
  - Ataques de empalme
  - Medios sintéticos

Permutaciones de los ataques:
El panorama de amenazas exponencial

Cada componente se puede combinar con los demás, lo que crea una matriz enorme de posibles vectores de ataque. Por ejemplo:

Una sola cámara virtual + una sola herramienta de Face Swap = un vector de ataque con rasgos únicos

Varias cámaras virtuales + varias herramientas de Face Swap + manipulación de metadatos = cientos de miles de posibles combinaciones con rasgos variables

Para evaluar eficazmente los nuevos vectores es necesario evaluar cuatro áreas clave:

01 **Factibilidad: analiza la integridad de la herramienta y su facilidad de uso**

02 **Novedad: examina los rasgos del vector de amenazas para evaluar qué tan nuevo o comunes son los métodos o herramientas**

03 **Transferibilidad: explora la disponibilidades y accesibilidad de la herramienta**

04 **Escalabilidad: predice la posible aceptación de la herramienta con base a lo anterior**

Las evaluaciones de seguridad convencionales no pueden captar adecuadamente la complejidad de las metodologías de ataque modernas. Cuando las organizaciones evalúan las afirmaciones que hacen los proveedores respecto a protecciones específicas, como las capacidades de detección de deepfakes, se deben formular preguntas críticas. Como demostramos, se debe probar la detección de 115.570 variantes de intercambios de rostros para respaldar esta afirmación, y hay que tener en cuenta que este vector de ataque no incluye todos los deepfakes.

Este desafío lo agravan las limitaciones de detección significativas:

- Muchos sistemas de verificación biométrica remota carecen de capacidades de monitoreo en tiempo real
- Los ataques exitosos habitualmente pasan desapercibidos hasta que los informan las organizaciones afectadas
- Los proveedores pueden seguir sin conocimiento de las intrusiones exitosas hasta después de que ocurran pérdidas financieras
- El largo tiempo transcurrido entre los ataques exitosos y su descubrimiento crea una exposición extendida
- La verdadera escala de los ataques exitosos probablemente no se informa por completo, ya que las organizaciones pueden atribuir las pérdidas a otras causas

Consideraciones críticas sobre las metodologías de pruebas de seguridad contemporáneas

La evidencia empírica reciente sugiere que hay una brecha significativa entre las capacidades de seguridad percibidas y reales con relación a los sistemas de verificación de identidad remota. El panorama de amenazas en evolución, que se caracteriza por vectores de ataques multiplicativos y avances tecnológicos veloces, hace necesario llevar a cabo una reevaluación de los marcos de prueba de seguridad tradicionales.

Las evaluaciones de seguridad convencionales no pueden captar adecuadamente la complejidad de las metodologías de ataque modernas. Cuando las organizaciones evalúan las afirmaciones que hacen los proveedores respecto a protecciones específicas, como las capacidades de detección de deepfakes, se deben formular preguntas críticas. Como demostramos, se debe probar la detección de 115.570 variantes de intercambios de rostros para respaldar esta afirmación, y hay que tener en cuenta que este vector de ataque no incluye todos los deepfakes.

El éxito documentado de los recientes ataques con medios sintéticos ha expuesto vulnerabilidades en varios sectores, que van desde pérdidas financieras hasta arriesgar la seguridad de la fuerza laboral. El incidente KnowBe4[13], que sucedió cuando una empresa de ciberseguridad, sin darse cuenta, contrató a una persona que utilizó imágenes sintéticas durante las entrevistas remotas, dándole acceso autorizado a los sistemas internos, demuestra cómo el fraude de identidad sintética se extiende más allá del robo financiero y supone amenazas internas graves mediante la suplantación de identidad del personal.

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

Dichos incidentes revelan que las medidas de protección actuales no abordan adecuadamente estas sofisticadas amenazas, lo que crea una peligrosa brecha entre las capacidades de seguridad percibidas y las reales. Esta disparidad representa un riesgo organizacional significativo que exige atención inmediata, especialmente porque la contratación remota de personal sigue siendo una práctica estándar.

Muchas organizaciones pueden tener un comprensión incompleta de su propia situación de seguridad. Dada la gran cantidad de maneras en que pueden ocurrir los ataques, es importante ir más allá de las pruebas de seguridad tradicionales y centrarse en el monitoreo y la adaptación continuos. Solo porque los ataques no se detectan no significa que no estén ocurriendo; esto puede deberse a que las capacidades de monitoreo son limitadas. Para mantenerse a la delantera, las organizaciones necesitan tener sistemas de monitoreo robustos y flexibles que puedan identificar y analizar los posibles ataques en tiempo real.

Liderazgo de iProov en las pruebas internacionales, referentes y marcos de seguridad

Aunque las certificaciones tradicionales del sector, de NIST y iBeta, definen importantes estándares de seguridad de referencia, el rápido cambio del panorama de amenazas requiere una perspectiva moderna. El nuevo programa de “Certificación de verificación facial” de FIDO Alliance evalúa la robustez e interoperabilidad de las soluciones biométricas, realizando pruebas específicas de su eficacia contra los deepfakes presentados en entornos controlados. Aunque esta certificación representa un avance en la estandarización de las pruebas de seguridad, es importante tener en cuenta que actualmente está centrada en los ataques de presentación en vez de todo el espectro de las posibles amenazas con deepfakes en todo el ciclo de vida de la identidad.

Nuestro compromiso con el avance de la seguridad biométrica ha llevado a rigurosas pruebas independientes de realizadas por la Dirección de Ciencia y Tecnología del Departamento de Seguridad Nacional de los Estados Unidos y líderes en ciberseguridad como Outflank, Jumpsec y Kroll Redscan, que han validado nuestras capacidades de defensa robustas contra los sofisticados ataques emergentes.

Mediante colaboraciones estratégicas, iProov participa activamente en dar forma al futuro de la seguridad biométrica. Trabajamos con MITRE para ampliar su marco ATLAS, contribuyendo con nuestra experticia en la detección de ataques con inteligencia artificial y las amenazas con medios sintéticos. Esta colaboración ayuda a crear enfoques estandarizados para la evaluación y defensa contra los vectores de ataques emergentes en sistemas de verificación de identidad remota.

Con nuestro enfoque basado en ciencia y un equipo de investigación líder en el sector, hemos logrado el reconocimiento como la autoridad científica más renombrada en el campo de la seguridad facial biométrica. Somos asesores habituales de gobiernos y organizaciones clave, como ENISA y MITRE, ayudando a concientizar sobre las amenazas del mundo real y a definir las mejores prácticas de la seguridad biométrica. Nuestras reflexiones impulsan los estándares y marcos del sector, más allá de las limitaciones de la pruebas periódicas tradicionales. Este enfoque integral garantiza que nuestras soluciones sigan siendo efectivas contra las amenazas actuales y emergentes, mientras ayudan a dar forma a los estándares internacionales para abordar la siguiente generación de desafíos de seguridad biométrica.

“La colaboración de iProov con MITRE ATLAS ha proporcionado información valiosa sobre el panorama de amenazas en evolución. Nuestro aporte a la documentación de los patrones ataque y las metodologías detección, descubiertas mediante los ataques del mundo real y evaluaciones de equipo rojo exhaustivas, ha contribuido a crear una comprensión más integral de la defensa contra las amenazas de verificación de identidad remota con uso de inteligencia artificial”. - *Panos Papadopoulos, Director del Equipo Rojo de iProov*

Profundización en el panorama de amenazas:
La paradoja de la tasa de ataques baja

Aunque al principio la reducción de las tasas de ataque parece indicar simplemente que hay menos interés de los actores de amenazas, nuestro análisis revela una dinámica de seguridad más matizada, que denominamos “la paradoja de la tasa de ataques baja”. Este fenómeno sucede cuando las medidas de seguridad robustas rechazan eficazmente los ataques, ocasionado que los actores de amenazas dejen de intentarlos y dirijan los recursos contra objetivos más vulnerables.

La inteligencia de amenazas demuestra que los atacantes perfilan activamente los sistemas de verificación y que en sus comunidades intercambian inteligencia sobre los sistemas que deben evitar, haciendo que las constantes tasas de ataque bajas sean un indicador importante sobre la eficacia de la seguridad, no de una menor actividad de amenazas. Comprender esto es fundamental para contextualizar nuestra postura de seguridad actual; el menor volumen de ataques valida nuestras mejoras de seguridad continuas y demuestra su efectividad continua con mantener una posición defensiva fuerte contra las amenazas en evolución.

Sistemas de seguridad robustos:
- Los ataques se abandonan rápidamente
- Los actores de amenazas advierten a otros miembros de sus comunidades
- Los recursos se redirigen hacia objetivos más fáciles
- Los intentos de ataque permanecen bajos

Sistemas vulnerables:
- Se convierten en objetivos con mayor frecuencia
- Experimentan campañas de ataques sostenidas

La importancia de la detección y respuesta gestionadas (MDR)
Este patrón demuestra por qué las organizaciones necesitan:

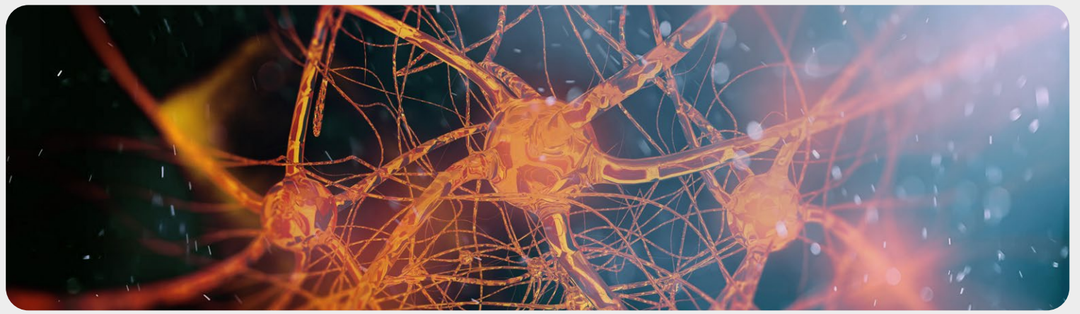
01 Medidas de seguridad preventiva robustas

02 Capacidades de monitoreo continuo

03 Recopilación de inteligencia de amenazas

04 Evaluaciones de seguridad periódicas

Incluso cuando las tasas de ataque son bajas, mantener una seguridad robusta es fundamental; son precisamente estas medidas las que mantienen bajas las tasas de ataque y protegen contra las amenazas en evolución.



Consideraciones del conjunto tecnológico:

Pasos útiles para la identidad moderna

El panorama de amenazas en evolución exige tener un enfoque de varias capas para la verificación de identidad. La clave es tener estrategias integrales que combinen la innovación tecnológica con la experticia humana, manteniendo la eficiencia operacional. El siguiente marco describe las áreas de enfoque para desarrollar medidas de seguridad resilientes.

Adopción de la seguridad en tiempo real

Los sistemas de monitoreo y detección continuos que funcionan en tiempo real han dejado en el pasado a las actualizaciones de seguridad periódicas. Este cambio de paradigma permite el escalamiento automatizado de las defensas durante los momentos de alto riesgo y facilita el despliegue de los parches de seguridad. Los sistemas de seguridad en tiempo real funcionan como escudos y sensores, protegiendo contra las amenazas conocidas al tiempo que identifican los patrones de ataque emergentes. Este enfoque proactivo ayuda a identificar y abordar las posibles vulnerabilidades antes de que puedan ser explotadas a escala.

La convergencia entre la tecnología y la experticia

Para tener éxito es necesario contar con una combinación estratégica de sistemas y experticia humana. La detección de amenazas automatizada ofrece la velocidad y escala necesarias para abordar los intentos de verificación, mientras que los analistas expertos aportan reflexiones cruciales para lograr operaciones de seguridad eficaces. Esta sinergia permite tanto responder inmediatamente a las amenazas como identificar las vulnerabilidades de manera proactiva. Combinar científicos biométricos y capacidades informáticas crea un ciclo de retroalimentación donde los sistemas automatizados señalan patrones sospechosos que se deben evaluar, mientras que las reflexiones humanas refinan los algoritmos de detección para que identifiquen mejor los nuevos métodos de ataque.

Desarrollo de estrategias de seguridad adaptativas

Las medidas de seguridad efectivas evolucionan junto con el panorama de amenazas mediante la evaluación y desarrollo continuos de medidas de protección para anticipar los futuros vectores de ataque. Las estrategias exitosas son un equilibrio entre la seguridad robusta y la experiencia del usuario, mediante evaluaciones de riesgo sofisticadas para ajustar las medidas de seguridad de acuerdo al contexto y nivel de riesgo. Esto previene que el exceso de fricción aleje a los usuarios, llevándolos a alternativas menos seguras, mientras mantiene los niveles adecuados de protección.

Construcción de la defensa colaborativa

Las amenazas modernas exigen tener una combinación de experticia interna e inteligencia externa. Aliarse con expertos en seguridad, participar en redes de inteligencia de amenazas y tener conexiones en investigaciones especializadas ofrece acceso a un conocimiento especializado e inteligencia de amenazas más amplia. Compartir los patrones e indicadores de los ataques entre las organizaciones fortalece las capacidades de defensa colectivas más allá de lo que podría lograr las medidas de seguridad individuales.

Preparación para las futuras amenazas

Para crear una arquitectura de seguridad robusta hay que incorporar flexibilidad y escalabilidad desde las bases, apoyada por procesos de evaluación de amenazas claros y el despliegue rápido de nuevas medidas de seguridad. Mirar más allá de las amenazas actuales para evaluar el potencial de las tecnologías emergentes para los sistemas, tanto de ataque como de defensa, garantiza que los sistemas se puedan adaptar a los desafíos en evolución mientras se mantiene la escalabilidad para afrontar los volúmenes de ataques en aumento.

Conclusión:

Navegar la nueva realidad de la seguridad de la identidad

El panorama de la verificación de identidad ha llegado a un punto de quiebre crítico. Nuestro análisis de inteligencia de amenazas de 2025 revela un aumento en la sofisticación de los ataques, y una transformación fundamental es saber cómo el engaño de identidad se lleva a cabo y comercializa. Los avances en las herramientas de medios sintéticos, en combinación con los mercados de crimen como servicio, han creado un entorno democratizado que permite a actores con experticia técnica mínima llevar a cabo ataques complejos.

Varios desarrollos clave definen esta nueva realidad: La mera escala de las posibles combinaciones de ataques, que pueden ser más de 100.000 posibles combinaciones de tres vectores de ataque comunes, demuestra que las tradicionales medidas de seguridad estáticas ya no son suficientes. Las organizaciones deben adaptarse a un panorama de amenazas donde los atacantes pueden cambiar rápidamente sus tácticas y objetivos, haciendo fundamental contar con capacidades de detección y respuesta en tiempo real.

Nuestro análisis de los patrones de amenaza revela una paradoja crucial: Con frecuencia, los sistemas más seguros muestran las menores tasas de ataque, ya que los actores de amenazas rápidamente abandonan sus intentos de ataque contra defensas robustas, prefiriendo atacar objetivos más fáciles. Esta “paradoja de la tasa de ataques baja” demuestra la importancia de mantener medidas de seguridad robustas, incluso cuando es evidente que los niveles de ataque parecen disminuir.

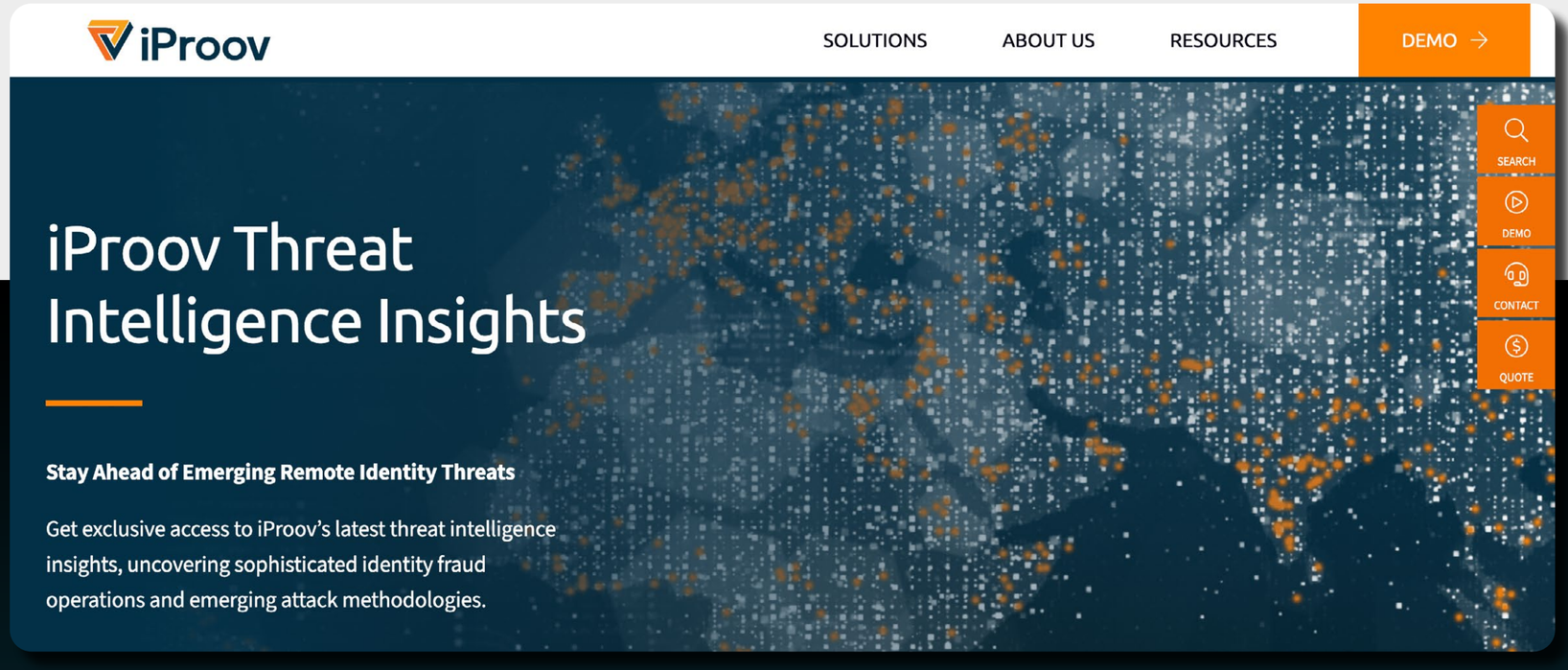
El factor de la detección humana continua siendo una vulnerabilidad crítica: Nuestra investigación de los deepfakes señala que solo el 0,1 % de las personas pueden identificar de manera confiable los medios sintéticos. Esta susceptibilidad generalizada, en combinación con la calidad cada vez mayor del contenido sintético, crea riesgos sin precedentes para los sistemas de verificación de identidad remota.

01 **Protección en tiempo real:** Cambio de las actualizaciones periódicas al monitoreo continuo y las capacidades de respuesta inmediatas

02 **Defensa dinámica:** Implementar medidas de seguridad que evolucionan a la par con las amenazas emergentes

03 **Colaboración humano-máquina:** La combinación de los sistemas de detección automatizados con el análisis de expertos en biometría y la caza de amenazas

El futuro de la seguridad de la identidad no recae en una sola tecnología o enfoque, sino en la integración de varias capas de defensa basadas en inteligencia de amenazas en tiempo real orientada por experticia científica profunda. Como enfrentamos un panorama de amenazas cada vez mayor y más complejo, el interrogante ya no es si las organizaciones afrontan ataques de identidad sofisticados, sino qué tan preparadas están para detectarlos y prevenirlos. Tener éxito en este nuevo entorno exige comprometerse con la evolución continua de la seguridad, respaldada por inteligencia de amenazas, capacidades de detección y respuesta gestionadas (MDR) en tiempo real y tecnologías de verificación remota que van más allá de la prueba de vida para validar la presencia de humanos genuinos.



¿Su organización necesita más información habitual sobre el panorama de amenazas de la verificación de identidad remota?

Registre su interés

Suscripción mensual al Informe de inteligencia de amenazas