iProov

Relatório de Inteligência de Ameaças 2025

Identidade remota sob ataque

Conteúdo

Prefácio executivo por Andrew Newell

O cenário da verificação de identidade atingiu um ponto de inflexão crítico. No último ano, testemunhamos uma mudança significativa não apenas na sofisticação dos ataques, mas na democratização fundamental das capacidades de ameaças. O que antes estava no domínio de agentes altamente qualificados se transformou em um ecossistema acessível de ferramentas e serviços que podem ser exercidos por qualquer pessoa com conhecimento técnico mínimo.

A escala dessa transformação é impressionante. Como exemplo, para apenas um tipo de deepfake, a troca de rosto, rastreamos atualmente mais de 120 ferramentas de ataque ativas, e os próprios deepfakes são apenas uma classe de imagens que podem ser usadas em ataques de injeção. Ao combiná-los com vários métodos de injeção e mecanismos de entrega, passamos a lidar com mais de 100.000 combinações de ataques em potencial. Esse crescimento exponencial nas permutações de ataque representa um desafio sem precedentes para as estruturas de segurança tradicionais.

Talvez o mais preocupante seja o avanço da qualidade da mídia sintética. Não podemos mais confiar na capacidade do olho humano de detectar deepfakes. Os deepfakes não são mais apenas ameaças aos sistemas biométricos – eles representam desafios fundamentais para qualquer sistema que dependa de imagens para verificação. As implicações vão muito além das tentativas individuais de fraude, comprometendo potencialmente estruturas de segurança organizacionais inteiras por meio de enganos sofisticados à força de trabalho.

O impacto financeiro é igualmente preocupante. Os dados do FBI indicam que as atividades criminosas relacionadas à identidade geraram perdas de 8,8 bilhões de dólares apenas em 2023. No entanto, esses números contam apenas parte da história. A verdadeira transformação está na natureza mutável desses ataques – de incidentes isolados a campanhas sofisticadas e com múltiplos vetores que correm o risco de não serem detectados por meses se o monitoramento apropriado de ameaças não estiver em vigor.

Essa nova realidade exige o replanejamento fundamental de como abordamos a segurança da identidade. Defesas estáticas e atualizações periódicas não são mais suficientes contra ameaças que evoluem em tempo real. O sucesso requer monitoramento contínuo, recursos de adaptação rápida e, o mais importante, a capacidade de detectar e responder a novos padrões de ataque antes que eles possam ser amplamente explorados.

À medida que navegamos nesse cenário em evolução, algo fica claro: o futuro pertence àqueles que podem se adaptar e responder mais rápido do que as ameaças em si. Este relatório oferece não apenas uma análise das tendências atuais, mas também um roteiro para criar as estruturas de segurança resilientes e adaptáveis necessárias para enfrentar os desafios emergentes.

Andrew Newell,
Chief Scientific Officer,
iProov

Introdução:

Estado de verificação de identidade remota: ameaças e impacto econômico (2024-2025)

O rápido crescimento da tecnologia baseada em IA introduziu novos desafios aos sistemas de identidade remotos. Ferramentas inovadoras e facilmente acessíveis permitiram que os agentes de ameaças se tornassem mais sofisticados da noite para o dia, alimentando um número crescente de vetores de ameaças devido a novas metodologias.

O custo crescente das falhas de verificação de identidade

O crescimento de novos vetores de ataque nos últimos 24 meses impactou fortemente as organizações. O custo de não implementar adequadamente a verificação de identidade remota é múltiplo. A Rede Sentinela do Consumidor da Comissão Federal de Comércio documentou um aumento de 45% nos incidentes de roubo de identidade no início de 2024, com perdas agregadas de fraude superiores a 10,2 bilhões de dólares[1]. O segundo maior valor de perda relatado veio de golpes de impostores, com quase 2,7 bilhões de dólares em perdas relatadas, indicando uma trajetória ascendente significativa no impacto financeiro.

Embora as métricas tradicionais, como custos de violação e tempos de detecção, permaneçam indicadores importantes, elas contam apenas parte da história. O que é mais significativo é a natureza mutável desses ataques: de incidentes isolados a campanhas sofisticadas e com múltiplos vetore que podem persistir sem serem detectados por meses. A janela de detecção estendida – que, de acordo com a IBM, geralmente excede 270 dias – cria oportunidades para que os agentes de ameaças executem esquemas de fraude complexos, comprometendo não apenas ativos imediatos, mas sistemas de infraestrutura digital inteiros.

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

O Relatório de Custo de Violação de Dados da IBM demonstra que os compromissos de segurança relacionados à identidade agora incorrem em um custo médio de 4,24 milhões de dólares por incidente, com o roubo de credenciais representando 19% dos eventos registrados. É importante ressaltar que, para as organizações, o tempo médio de detecção e contenção se estende até 277 dias, criando janelas substanciais de vulnerabilidade para atividades de fraude a jusante.

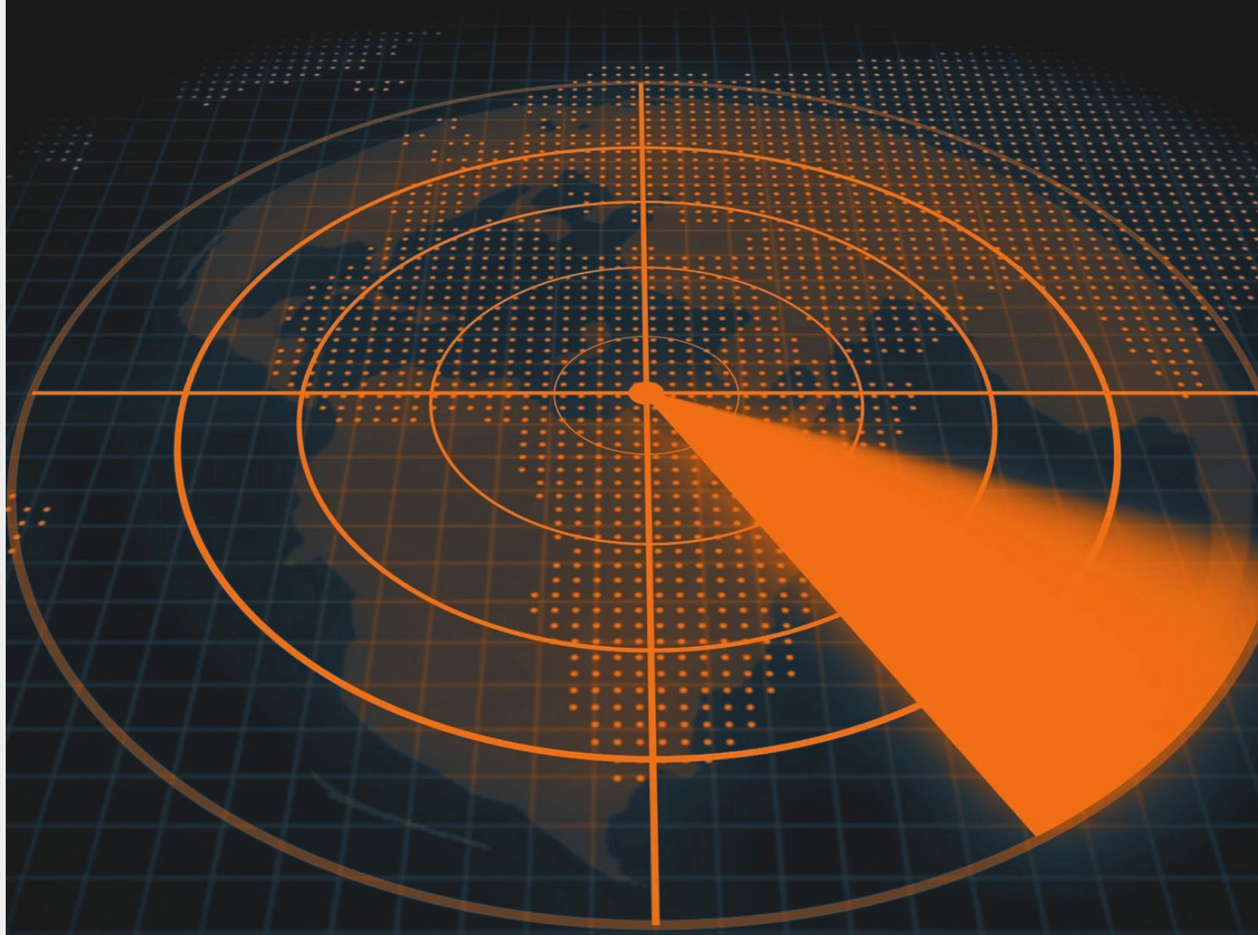
A gravidade dessa ameaça é ilustrada por vários incidentes de alto nível em 2024:

- T-Mobile (janeiro de 2024): exposição de 37 milhões de registros de clientes, resultando em 350 milhões de dólares em custos de liquidação[2]
- Microsoft (agosto de 2024): os invasores executaram ataques de bot em grande escala contra sistemas CAPTCHA e os usaram para criar 750 milhões de contas falsas da Microsoft[3]
- LoanDepot (janeiro de 2024): incidente de ransomware que resultou na exposição de dados de identificação do cliente e interrupção sistêmica[4]

"Esses incidentes demonstram uma mudança crítica na metodologia de ataque: os agentes de ameaça não estão mais apenas roubando dados – eles estão se passando por indivíduos confiáveis por meio de ferramentas de troca de rosto ou criando novas identidades sintéticas para executar estratégias de fraude de longo prazo." - Andrew Newell, Chief Scientific Officer, iProov

Embora o mercado reconheça a necessidade de medidas de segurança aprimoradas, as organizações enfrentam desafios significativos na seleção e implementação de soluções apropriadas.

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/



Atenção, consumidor: a dupla de desafios da aquisição de tecnologia de segurança

As organizações enfrentam um duplo desafio ao proteger seus sistemas de verificação de identidade remotos. Primeiro, há uma lacuna de conhecimento fundamental em relação à compreensão e aquisição de tecnologias de verificação remota apropriadas com base em casos de uso e dados contextuais. Essa lacuna de conhecimento é claramente ilustrada no relatório ID IQ[5] da RSA de 2025, que constatou que quase metade de todos os entrevistados errou pelo menos metade das perguntas sobre conceitos básicos de segurança de identidade, com gerenciamento de identidade e acesso (IAM), com os especialistas em segurança cibernética surpreendentemente apresentando o pior desempenho.

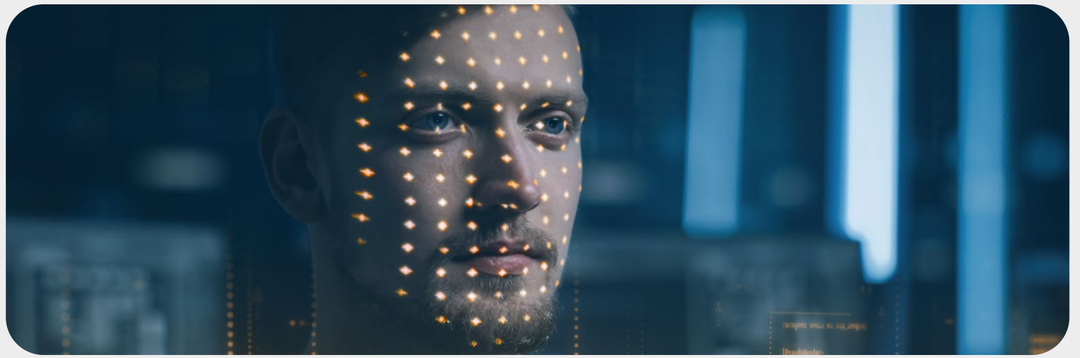
Em segundo lugar, e igualmente preocupante, é a prevalência de alegações infladas de fornecedores sobre recursos de segurança. Nossas descobertas no campo de inteligência de ameaças revelam que muitas soluções que reivindicam proteção abrangente contra ataques de mídia sintética não têm a base tecnológica para evitá-las. Essa disparidade entre os recursos comercializados e a proteção real deixa as organizações vulneráveis, criando uma falsa sensação de segurança.

O relatório da RSA destaca esse risco, usando o setor aeroespacial como exemplo. Apesar de ser o setor com maior probabilidade de sofrer graves violações relacionadas à identidade, custando mais de 10 milhões de dólares, as empresas aeroespaciais, paradoxalmente, relataram a maior confiança em sua capacidade de gerenciar os direitos de acesso dos usuários.

Esse cenário complexo exige uma abordagem mais diferenciada às compras de segurança. Indo além das garantias do fornecedor e das avaliações tradicionais focadas em conformidade, em direção a avaliações de segurança abrangentes que incluem:

- Verificação independente de compromissos de segurança – particularmente crucial, uma vez que 66% das organizações que sofreram violações relacionadas à identidade as classificaram como eventos graves
- Capacidade gerenciada de detecção e resposta
- Monitoramento contínuo com sistemas de detecção de ameaças em tempo real – especialmente importante, pois 42% das organizações relataram sofrer violações relacionadas à identidade em um período de três anos
- Capacidade comprovada de adaptação a vetores de ataque emergentes – crítica, pois 80% dos entrevistados acreditam que a IA afetará significativamente a segurança cibernética nos próximos cinco anos

Sem abordar a lacuna de conhecimento e os problemas de responsabilidade do fornecedor, as organizações correm o risco de implementar soluções que parecem robustas no papel, mas se mostram inadequadas contra ataques do mundo real. Este risco é quantificável:o relatório da RSA descobriu que 44% dos entrevistados estimaram que os custos de violação relacionados à identidade excederam os custos típicos de violação de dados, com 21% relatando custos acima de 10 milhões de dólares.



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

Principais conclusões

01 O cenário de ameaças se transformou profundamente

- Ferramentas de ataque foram democratizadas e comercializadas
- Mais de 100.000 combinações de ataque possíveis identificadas a partir de apenas três vetores
- As ferramentas de ataque individuais evoluíram para cadeias de ataque sofisticadas

02 As abordagens tradicionais de segurança não são mais suficientes

- As atualizações de segurança pontuais não conseguem acompanhar o ritmo das ameaças em evolução
- Os testes estáticos não conseguem captar a complexidade dos ataques modernos
- As organizações devem mudar de monitoramento de segurança periódico para contínuo

03 As capacidades de detecção humana são seriamente limitadas

- Apenas 0,1% das pessoas conseguem identificar com segurança todas as mídias sintéticas[6]
- O excesso de confiança nas habilidades de detecção cria riscos adicionais
- Soluções técnicas devem compensar a vulnerabilidade humana

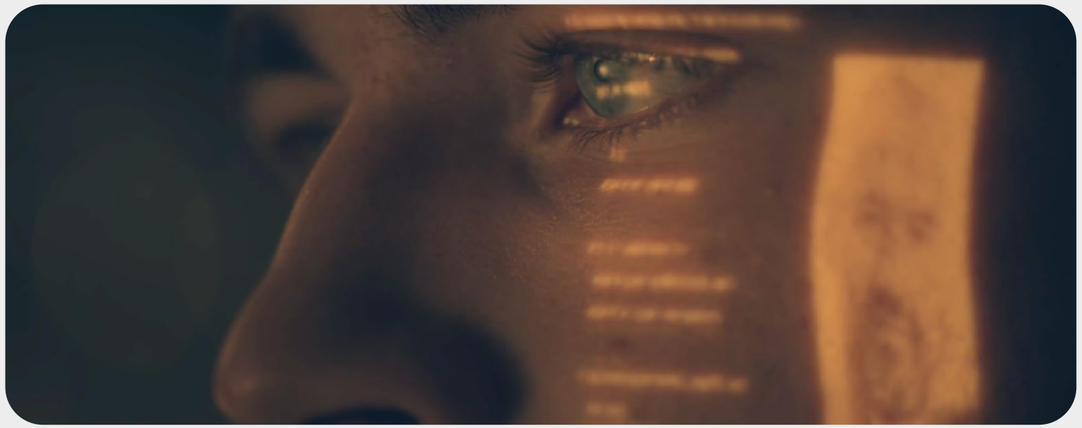
04 O sucesso da segurança requer uma abordagem multicamadas

- Recursos de detecção e resposta gerenciadas em tempo real são essenciais
- O monitoramento e a adaptação contínuos devem substituir as defesas estáticas
- A integração de sistemas automatizados com experiência humana é crucial

05 Padrões de ataque se tornaram mais sofisticados

- Os agentes de ameaças definem ativamente o perfil e compartilham informações sobre os alvos
- Taxas de ataque baixas geralmente indicam segurança forte em vez de redução das ameaças
- Os invasores mudam rapidamente o foco para alvos mais vulneráveis

Essas constatações ressaltam uma regra clara: as organizações devem replanejar completamente sua abordagem à segurança da identidade. O sucesso neste novo ambiente requer um compromisso com a evolução contínua da segurança, apoiada por inteligência robusta contra ameaças e recursos de detecção e resposta gerenciadas (MDR) em tempo real. O futuro pertence a fornecedores e organizações capazes de se adaptar e responder a novas ameaças, em vez daquelas que dependem de defesas estáticas.



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

Relatório de Inteligência de Ameaças iProov:
Metodologia e escopo

Este Relatório de Inteligência de Ameaças baseia-se em dados coletados do Centro de Operações de Segurança iProov (iSOC). Nossa abordagem única baseada na ciência nos permite coletar e analisar dados de ataques do mundo real, fornecendo visibilidade sem precedentes sobre as ameaças emergentes direcionadas a sistemas de verificação remota.

As constatações apresentadas neste relatório são obtidas de:

- Detecção de ameaças em tempo real e dados de resposta do iSOC
- Coleta de informações sobre ameaças externas e monitoramento da dark web
- Campanhas internas de teste de penetração da equipe vermelha
- Pesquisa avançada de segurança biométrica e inteligência interna de ameaças
- Análise de padrões de ataques detectados e evitados
- Avaliação técnica de ferramentas e metodologias de ataque emergentes

"Em 2014, a criação de identidades sintéticas exigiu ampla experiência técnica, equipamentos especializados e investimento significativo de tempo. A inteligência artificial revolucionou esse espaço, permitindo a geração de mídias sintéticas sofisticadas em tempo real." - *Andrew Newell, Chief Scientific Officer, iProov*

Por meio da detecção contínua de ameaças em tempo real, nossos especialistas em segurança realizam a defesa contra ataques atuais e identificam padrões de ameaças emergentes, permitindo melhorias preditivas de segurança em nossas defesas. Este relatório fornece análise e insights sobre os vetores de ataque emergentes e a evolução das táticas do adversário à medida que entramos no cenário de verificação de identidade remota de 2025.

A evolução da falsificação de identidade

Linha do tempo e impacto de 2014 a 2024: passado o ponto de não retorno

A progressão das capacidades de falsificação de identidade de 2014 a 2025 representa uma mudança fundamental tanto na tecnologia quanto na acessibilidade. Esta linha do tempo ilustra a rápida transformação de ataques complexos e especializados em ferramentas e serviços amplamente acessíveis e disponíveis.

Essa democratização foi acelerada por três tendências convergentes:o rápido avanço tecnológico, o surgimento de mercados de crime como serviço (CaaS) e a transição de ataques de mídia sintética de ameaças teóricas para crimes financeiros documentados.

2014

Introdução às GANs

2016

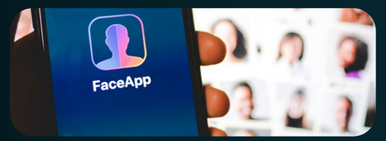
Os deepfakes surgiram com o aumento do deep learning, tendo as primeiras comunidades se formado no Reddit

2017

Primeira ferramenta de criação de deepfake generalizada (FakeApp); Limitada a trocas de rosto de baixa qualidade em vídeos

2018

Primeiras versões de trocas de rosto



2019

Modelo de movimento de primeira ordem (FOMM)

2020

Os deepfakes de áudio apareceram junto com ferramentas como Descript Overdub e Wave2Lip

2021

Lançamento do DALL-E

2022

A ascensão da geração de imagens acessíveis, clonagem de voz e deepfakes em tempo real estimulou o primeiro Relatório de Inteligência de Ameaças da iProov.

2023

Proliferação da troca de rosto; Deepfakes de áudio de alta qualidade; Lançamento do GPT-4

2024

Alta qualidade Trocas de rosto

Da pesquisa ao impacto no mundo real

O final de 2023 marcou um ponto de virada crítico nessa evolução. O que existia principalmente em laboratórios de pesquisa e demonstrações de prova de conceito se materializou em ataques sofisticados, resultando em perdas financeiras significativas.

Embora muita atenção tenha se concentrado na fraude de identidade do consumidor, os ataques mais significativos e caros de 2024 visaram os sistemas de verificação da força de trabalho. Essa mudança em direção às metas corporativas revela uma tendência preocupante:agentes de ameaça sofisticados estão explorando processos de trabalho remoto e canais de comunicação corporativa com máximo impacto.

Um exemplo é o golpe de deepfake[7] de 25,6 milhões de dólares com sede em Hong Kong em que os invasores usavam mídia sintética para se passar por executivos em teleconferências, ignorando os protocolos tradicionais de verificação corporativa. Esse incidente demonstrou como os ataques de identidade sintética podem comprometer não apenas os ativos financeiros, mas também levar a profundas violações de segurança organizacional por meio da exploração da força de trabalho.'

Esses casos representam um pivô estratégico por agentes de ameaças que descobriram vulnerabilidades críticas em sistemas de verificação corporativa. Através da segmentação dos processos de contratação remota, comunicações virtuais no local de trabalho e videoconferências executivas, os invasores estão obtendo resultados significativamente mais altos do que a fraude tradicional ao consumidor. Essa mudança de metas individuais para organizacionais expõe uma lacuna perigosa na verificação de identidade da força de trabalho – uma que as atuais estruturas de segurança corporativa estão lutando para resolver.

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/

Relatório do Panorama de Ameaças à Segurança de Identidade de 2024 da CyberArk[8] revelou que 93% das organizações tiveram duas ou mais violações relacionadas à identidade apenas no ano passado. Esses incidentes validam preocupações de longa data sobre o impacto potencial da mídia sintética.

Esses ataques bem-sucedidos demonstram vários desenvolvimentos:

01 **Validação operacional**: o que antes era teórico agora se mostrou eficaz em cenários do mundo real, fornecendo aos agentes de ameaça metodologias documentadas e histórias de sucesso. Essa validação provavelmente acelerará a adoção de táticas semelhantes em redes criminosas.

02 **Compromisso tradicional do sistema multicamada:** esses ataques contornaram com sucesso várias camadas de segurança simultaneamente:

- Julgamento humano em ambientes profissionais
- Protocolos de segurança corporativa
- Mecanismos tradicionais de detecção de fraudes

03 **Escalabilidade de ataques:** o sucesso comprovado desses métodos, combinado à disponibilidade de plataformas de Crime como Serviço, cria potencial para:

- Replicação rápida de metodologias de ataque bem-sucedidas
- Ataques paralelos contra várias organizações
- Direcionamento automatizado de setores vulneráveis
- Agentes menos qualificados executando padrões de ataque sofisticados

04 **Vulnerabilidade organizacional:** esses ataques expõem fraquezas institucionais mais amplas:

- Exposição excessiva a métodos de verificação desatualizados
- Protocolos inadequados para transações remotas de alto valor
- Recursos limitados de detecção e resposta gerenciadas em tempo real

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

Entender essa progressão é crucial para desenvolver estratégias de defesa eficazes contra ameaças atuais e emergentes. A combinação perigosa de alegações exageradas pelo fornecedor e nossa convicção equivocada de que podemos identificar um deepfake é uma receita para o desastre.

Pesquisa do consumidor: o ponto cego do deepfake

Uma pesquisa de consumidor de deepfake de 2025[9] da iProov retrata a imagem de uma sociedade amplamente despreparada para os desafios impostos pela tecnologia deepfake, com lacunas significativas na conscientização, habilidades de detecção e mecanismos de resposta.

Principais conclusões:

- Taxa de sucesso de detecção: apenas 0,1% dos participantes conseguiram identificar todos os exemplos de mídia sintética corretamente
- Vulnerabilidade de vídeo: taxa de sucesso particularmente baixa (9%) para detecção de deepfake de vídeo
- Vulnerabilidades relacionadas à idade: adultos com mais de 55 anos foram considerados particularmente vulneráveis, já que quase um terço nunca tinha ouvido falar de deepfakes antes, limitando sua capacidade de se identificar e se proteger contra essa tecnologia
- Lacuna de confiança: adultos mais jovens (18-34) apresentaram excesso de confiança perigosa nas habilidades de detecção, apesar do baixo desempenho

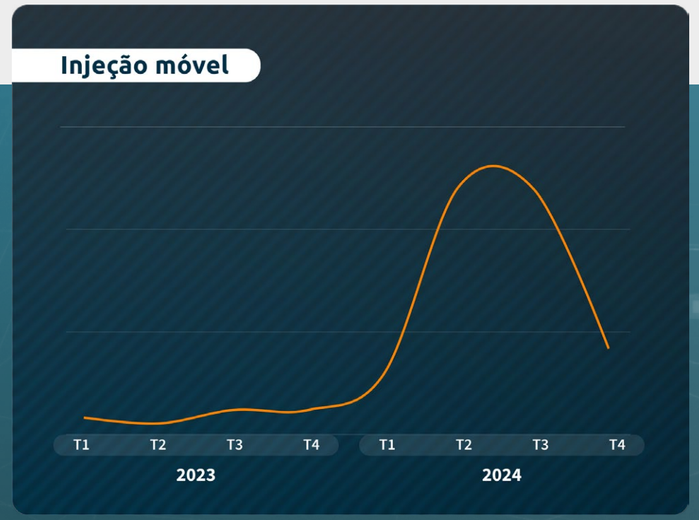
Recursos de resposta:

- 48% não conhecem os procedimentos adequados para relatar deepfakes
- 25% verificam informações através de fontes alternativas
- 11% realizam análise crítica da fonte
- 29% não tomam nenhuma medida ao encontrar suspeitas de deepfakes

Tendências principais de ataque do iProov, dados de 2023 vs. 2024, ano a ano

Ataques de injeção: Aumento de 783%

Em 2024, houve uma rápida escalada na frequência e na escala de vetores de ataque baseados em injeção voltados para aplicativos da Web para dispositivos móveis, sugerindo uma mudança fundamental nas capacidades e na acessibilidade das ferramentas de ataque.



Câmera virtuais nativas: Aumento de 2665%

Talvez um dos eventos mais significativos de 2024 tenha sido o reaparecimento dramático dos ataques de câmeras virtuais nativas e a velocidade com que chegaram. O gráfico demonstra a necessidade de detecção e resposta gerenciadas em tempo real.

Trocas de rosto: Aumento de 300%

Já uma tendência alarmante descoberta em 2023, os ataques de troca de rosto persistiram em 2024 e aumentaram no segundo trimestre daquele ano. Exploramos a natureza de sua evolução na seção 4 Tendências principais deste relatório.

Ameaças emergentes

Esta seção apresenta as constatações da equipe de inteligência de ameaças da iProov sobre a evolução das metodologias de ataque e suas implicações para as estruturas contemporâneas de verificação de identidade.

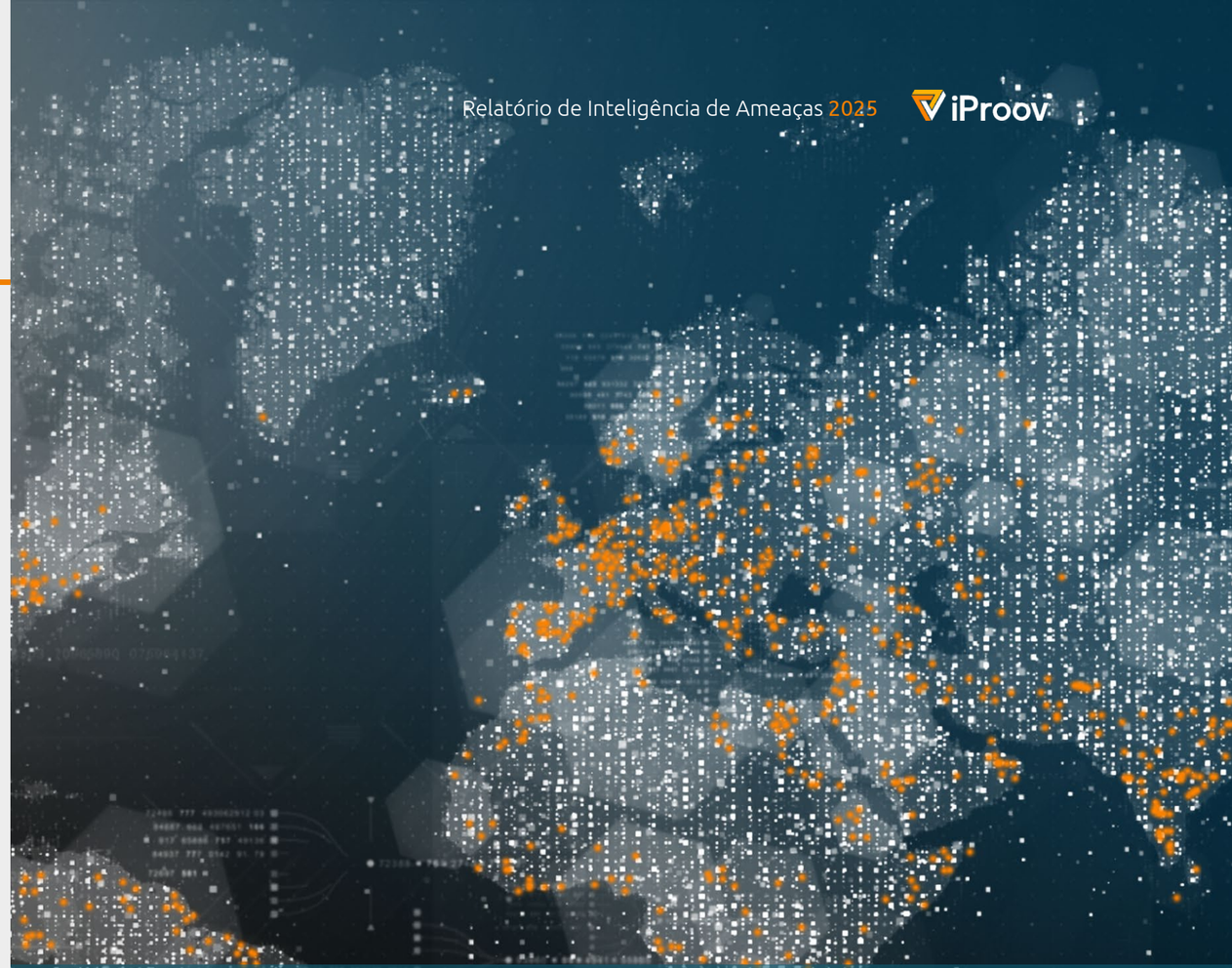
No final do ano passado, o iSOC descobriu um grupo da dark web que havia acumulado uma coleção significativa de documentos de identidade e imagens faciais correspondentes. Essas identidades foram projetadas especificamente para contornar os processos de verificação Know Your Customer (KYC, Conheça seu cliente). Em vez de serem adquiridas por meio de roubo tradicional, parece que os indivíduos forneceram voluntariamente essas identidades em troca de pagamento.[10]

Descoberta: coleta em grande escala de documentos de identidade e imagens faciais legítimos
Método: fornecimento voluntário de credenciais para pagamento
Impacto: criação de identidades falsas com base em documentos genuínos para evitar a detecção
Escopo geográfico: inicialmente identificado na América Latina, agora ligado a redes europeias de fraude

Com as trocas de rosto e os ataques de câmera nativos no seu auge, os agentes mal-intencionados podem aproveitar documentos genuínos que não soam nenhum alarme de fraude ao criar uma troca de rosto de uma identidade genuína para ser sobreposta ao rosto e ser verificada remotamente por meio de videoconferência ou outros meios de verificação remota de rosto.

Quaisquer atividades criminosas descobertas por nossa equipe são relatadas às autoridades locais relevantes.

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



"As tecnologias de detecção de vivacidade estão se tornando críticas para a defesa contra deepfakes e a verificação da presença genuína de um indivíduo."

2024 Gartner® Emerging Tech: O impacto da IA e dos deepfakes no relatório de verificação de identidadet[11]

Quatro tendências a serem observadas em 2025

Tendência 1: Aumento de câmeras virtuais nativas

Observações principais:

- Os ataques de câmeras virtuais nativas evoluíram de sua fase experimental em 2023 para se tornar uma grande ameaça em 2024, chegando a 785 ataques semanais no segundo trimestre
- É mais preocupante ainda o fato de que esses ataques não exigem dispositivos enraizados ou desbloqueados, tornando-os acessíveis a agentes de ameaças sem habilidades técnicas avançadas
- A descoberta de um aplicativo de câmera mal-intencionado em uma loja de aplicativos convencional demonstra como esses ataques estão sendo "democratizados" por meio de ferramentas fáceis de usar

O que começou como um vetor de ameaças experimental em 2023 evoluiu para uma das tendências mais significativas em 2024, com ataques de câmeras virtuais nativas atingindo 785 incidentes por semana no segundo trimestre. A descoberta de um aplicativo de câmera mal-intencionado em uma loja de aplicativos convencional revelou que esses ataques não exigem ferramentas de hacking sofisticadas ou dispositivos enraizados, tornando insuficientes as medidas tradicionais de segurança cibernética, como a detecção de raiz. Embora removido da loja oficial, o aplicativo permanece disponível por meio de fontes de terceiros, permitindo acesso fácil a ataques de injeção.

Esse desenvolvimento desafia a noção de que os ataques de injeção sejam puramente uma ameaça biométrica ou de segurança cibernética. As evidências mostram claramente que uma defesa robusta requer forte detecção de vivacidade biométrica e medidas de segurança cibernética trabalhando em conjunto. Os padrões de ataque que observamos sugerem que os agentes de ameaça estão explorando ativamente essa abordagem de vetor duplo.

Tendência 2: Proliferação da troca de rosto

Observações principais:

- Em 2024, os volumes de ataque aumentaram 300% em comparação com 2023
- O número de ferramentas usadas nesses ataques aumentou 15,5%, passando de 110 para 127
- Os agentes de ameaças aproveitam a inteligência compartilhada para explorar sistemas vulneráveis, usando uma variedade de ferramentas de troca de rosto

O cenário dos ataques de troca de rosto cresceu significativamente no ano passado, tendo o número de ferramentas rastreadas aumentado de 110 para 127. O primeiro trimestre de 2024 revelou um padrão claro: os agentes de ameaça adaptaram suas táticas após a implantação generalizada inicial. Notavelmente, após o estágio de experimentação em grande escala na primeira metade do ano, o compartilhamento de informações sobre as vulnerabilidades do sistema efetivamente mudou seu foco para "frutas fáceis de apanhar". Nossa observação fez com que eles se afastassem da plataforma da iProov em direção a sistemas que usam detecção de vivacidade ativa que exigem que os usuários sigam ações ou movimentos específicos. Esses sistemas são mais fáceis de contornar, pois seus padrões de desafio-resposta podem ser replicados com vídeos pré-gravados ou sintetizados.

Em 2024, as discussões sobre ferramentas e técnicas de troca de rosto tornaram-se mais proeminentes nos fóruns de agentes de ameaças, impulsionadas pelo compartilhamento de informações e ferramentas entre as comunidades mal-intencionadas.

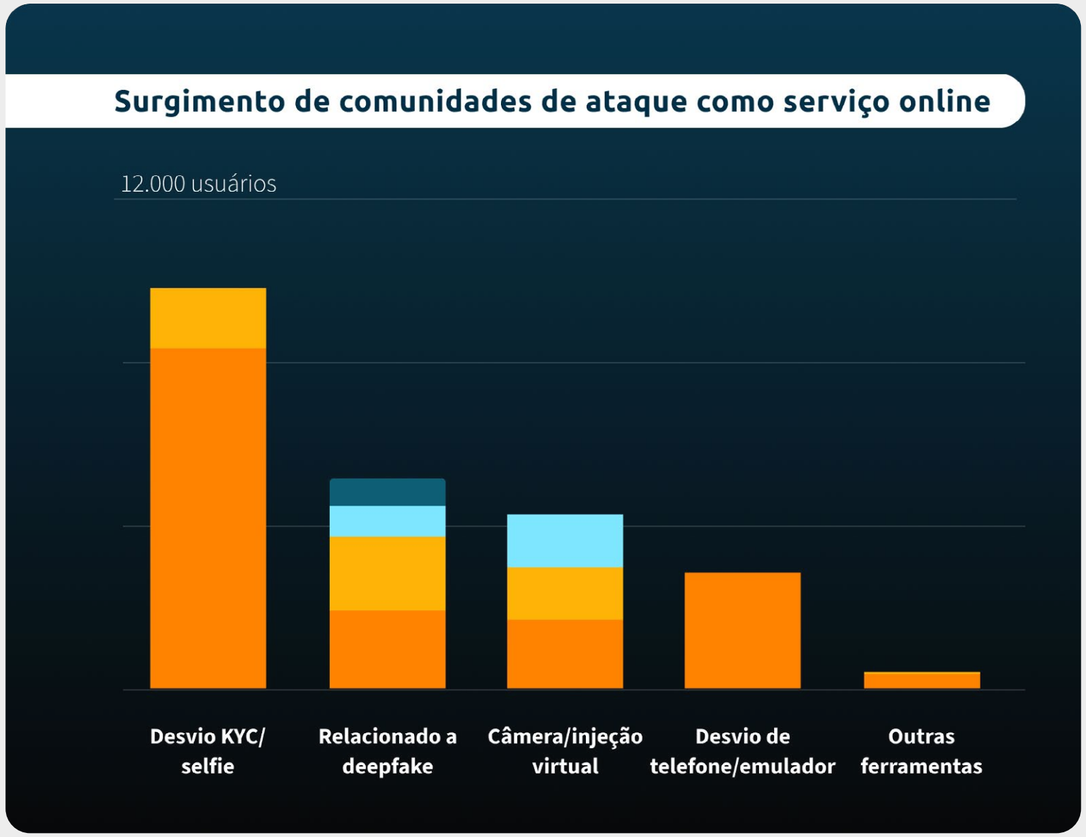
Tendência 3: Comunidades online de ataque como serviço

Observações principais:

- Outros 31 grupos de agentes de ameaças online foram identificados em 2024, o maior deles tem 6.400 usuários.
- Os grupos de venda de ferramentas atendem 68% (23.698) dos usuários, indicando sua eficácia e credibilidade.
- Os métodos de ataque estão cada vez mais focados no desvio de KYC, deepfakes e ferramentas específicas do Android.Esses grupos estão se movendo em direção a soluções abrangentes, em vez de serviços independentes.

Em 2024, foram identificados 31 grupos adicionais de agentes de ameaças online, com 45% vendendo suas próprias ferramentas e 55% revendendo ou fornecendo serviços relacionados. Esse ecossistema abrange 34.965 usuários totais, com os vendedores de ferramentas atraindo 23.698 usuários, em comparação com 11.267 para os não vendedores. Nove grupos têm mais de 1.500 usuários, com o maior chegando a 6.400 membros. As discussões comuns se concentram nas técnicas de desvio de KYC, na tecnologia deepfake e nas ferramentas do Android.

Um foco significativo é colocado em plataformas móveis, particularmente o Android, com alguns grupos oferecendo ferramentas e serviços combinados, enquanto outros se especializam em áreas como agricultura de identificação e câmbio de criptomoedas.



O monitoramento atual indica que 60% dos principais bancos ocidentais estão sendo alvo, embora esse número seja provavelmente maior e deva crescer conforme a cobertura do fórum se expande.

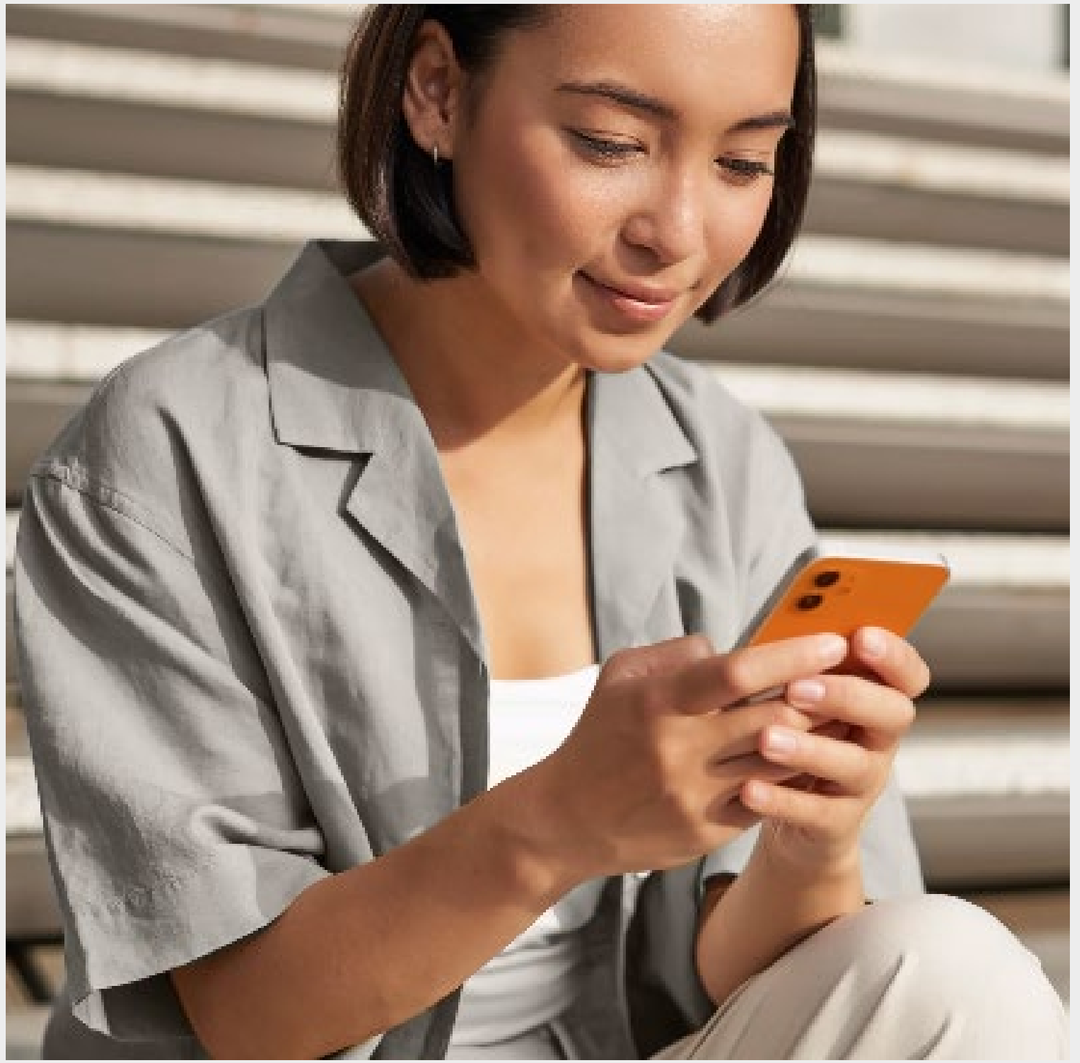
Tendência 4: Conversão de imagem para vídeo
Um novo vetor de ataque de identidade sintética

Observações principais:

- As ferramentas de conversão de imagem para vídeo reduziram a criação de identidade sintética a um processo simples de duas etapas que requer conhecimento técnico mínimo
- Nossos testes mostram que essas identidades sintéticas animadas representam uma ameaça significativa para muitos sistemas de detecção de vivacidade, incluindo mecanismos ativos de desafio-resposta
- A natureza perfeita da saída de mídia sintética, sem artefatos de manipulação típicos, os torna excepcionalmente difíceis de detectar uma vez animados com movimento fluido

Esses ataques se mostraram ineficazes contra nossa plataforma Dynamic Liveness, que usa a tecnologia[12] patenteada Flashmark para verificar a presença humana genuína por meio de mecanismos passivos de desafio-resposta.

Nossa equipe de ciência identificou uma evolução significativa na fraude de identidade sintética por meio da tecnologia de conversão de imagem para vídeo, observada pela primeira vez em uma tentativa de ataque contra nossa plataforma em dezembro de 2024. Essa técnica transforma imagens estáticas em conteúdo de vídeo convincente que pode representar desafios muito significativos para a maioria dos sistemas de verificação de identidade remotos. Embora os ataques de identidade sintética normalmente usem trocas de rosto, manipulação de metadados e desvios de câmera, esse novo vetor de ataque simplifica o processo em duas etapas:os agentes de ameaça obtêm ou criam uma imagem de rosto sintética e, em seguida, utilizam ferramentas de conversão de imagem para vídeo para animá-la em movimento fluido que imita de perto o conteúdo de vídeo genuíno.



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

Fraude de identidade sintética (SIF) é o tipo de fraude que mais cresce

A fraude de identidade sintética (SIF) é o tipo de fraude que mais cresce, com implicações particularmente alarmantes. Esse esquema sofisticado combina dados legítimos (como números de documentos de identidade válidos, muitas vezes roubados de crianças, idosos ou indivíduos falecidos) com informações pessoais fabricadas para criar identidades falsas convincentes. Os fraudadores criam metodicamente credibilidade para essas identidades sintéticas, estabelecendo históricos de crédito, abrindo várias contas em diferentes instituições e criando pegadas digitais que parecem autênticas.

O que torna a SIF especialmente desafiadora de combater é sua capacidade de escapar dos sistemas tradicionais de detecção de fraudes. Ao contrário do roubo de identidade convencional, em que os sistemas podem sinalizar informações roubadas com base em relatórios de vítimas reais, a SIF cria identidades inteiramente novas que incorporam elementos reais e falsos. Sem uma vítima real para disparar o alarme, e com alguns componentes da identidade sendo legítimos, os métodos de detecção tradicionais muitas vezes não conseguem reconhecer esses padrões de fraude sintéticos.

Muitos sistemas de verificação de identidade remotos lutam para detectar imagens manipuladas em vídeos porque, ao contrário das imagens genuínas alteradas no nível de pixel, os rostos sintéticos não exibem esses sinais tradicionais de manipulação. Quando animadas, essas identidades sintéticas parecem incrivelmente realistas, tornando a detecção desafiadora para o olho humano. A acessibilidade e a eficácia dessas ferramentas sugerem que o uso dessa técnica só aumentará. Esse desenvolvimento marca uma evolução significativa na fraude de identidade sintética, exigindo monitoramento e pesquisa contínuos até 2025.

Permutações de ataque:
O cenário de ameaças exponenciais

A complexidade dos ataques de verificação de identidade remotos vai muito além de ferramentas ou técnicas individuais. Os agentes de ameaças de hoje utilizam combinações sofisticadas de ferramentas, criando uma superfície de ataque exponencialmente maior do que muitas organizações percebem e estão equipadas para proteger. Entender essas permutações é crucial para estratégias abrangentes de teste e defesa de segurança.

Fonte: This Person Does Not Exist

Fonte: iProov Threat Intelligence Library

Classes de deepfakes

Componentes de ataque principais e suas variações

01 Ferramentas de manipulação facial

- Atualmente rastreando 127 aplicativos de troca de rosto distintos
- Cada ferramenta oferece diferentes capacidades e qualidades de saída
- Graus variados de detectabilidade e sofisticação
- Gama de aplicativos de nível de consumidor a soluções avançadas alimentadas por IA

02 Emuladores móveis

- Atualmente rastreia mais de 10 novas tecnologias de emulador
- Os recursos incluem falsificação de localização, manipulação de características do dispositivo
- Várias configurações de sistema operacional e hardware
- Diferentes níveis de recursos de evasão de detecção

03 Software de câmera virtual

- Atualmente rastreia 91 ferramentas de câmera virtual
- Variando da injeção de vídeo básica até a manipulação de fluxo sofisticada
- Vários métodos para contornar os controles de segurança do dispositivo
- Recursos diferentes para manipulação de metadados

O efeito de multiplicação

A verdadeira escala de ataques potenciais surge quando essas ferramentas são combinadas:

Cálculo básico:
127 ferramentas de troca de rosto
× 10 emuladores
× 91 câmeras virtuais
= 115.570 combinações de ataques em potencial

Cada combinação representa um vetor de ataque único que requer estratégias específicas de detecção e prevenção. À medida que são introduzidas novas ferramentas e atualizações, as combinações aumentam constantemente. Por simplicidade, o exemplo fornecido neste relatório calcula as três combinações de ataque mais notórias. No entanto, isso não deve prejudicar as ferramentas disponíveis de imagens geradas por computador (CGI) e modelo de movimento de primeira ordem (FOMM), que também estamos rastreando.

Pontos de entrada

Câmeras virtuais

- **Trocas de rosto**
  - **Manipulação de metadados**
    - Manipulação de dados de sensor de dispositivo
  - Deepfakes
  - CGI
  - Reencenações
- “Man in the Middle”
  - Trocas de rosto
  - Deepfakes
  - Mídias sintéticas
- Reprodução
  - Trocas de rosto
  - Ataques de emenda
  - Mídias sintéticas

Permutações de ataque:
O cenário de ameaças exponenciais

Cada componente pode ser combinado com outros, criando uma vasta matriz de possíveis vetores de ataque. Por exemplo:

Câmera virtual única + ferramenta de troca de rosto única = um vetor de ataque com características únicas

Múltiplas câmeras virtuais + ferramentas de troca de rosto múltipla + manipulação de metadados = centenas de milhares de combinações potenciais com características variadas

A avaliação eficaz de novos vetores requer o exame de quatro áreas fundamentais:

01 **Viabilidade: examina a integridade da ferramenta e sua facilidade de uso**

02 **Novidade: analisa as características do vetor de ameaça para avaliar o quanto as ferramentas e os métodos são novos ou comuns**

03 **Transferibilidade: explora a disponibilidade e a acessibilidade da ferramenta**

04 **Escalabilidade: prevê a provável aceitação da ferramenta com base no exposto acima**

As avaliações de segurança convencionais não capturam adequadamente a complexidade das metodologias de ataque modernas. Quando as organizações avaliam os compromissos dos fornecedores em relação a proteções específicas, como recursos de detecção de deepfake, algumas perguntas críticas precisam ser feitas. Como demonstrado, 115.570 variações precisariam ser comprovadas para dar respaldo a uma reivindicação de detecção de “troca de rosto”, e esse vetor de ameaça não encapsula totalmente todos os deepfakes.

Este desafio é agravado por limitações de detecção significativas:

- Muitos sistemas de verificação biométrica remota não possuem recursos de monitoramento de ataques em tempo real
- Os ataques bem-sucedidos geralmente passam despercebidos até serem relatados pelas organizações afetadas
- Os fornecedores podem permanecer inconscientes de desvios bem-sucedidos até que ocorram perdas financeiras
- O atraso entre ataques bem-sucedidos e sua descoberta cria uma exposição prolongada
- A verdadeira escala de ataques bem-sucedidos é provavelmente subnotificada, pois as organizações podem atribuir perdas a outras causas

Considerações críticas nas metodologias de teste de segurança contemporâneas

Evidências empíricas recentes sugerem uma lacuna significativa entre as capacidades de segurança percebidas e reais em sistemas de verificação de identidade remotos. O cenário de ameaças em evolução, caracterizado por vetores de ataque multiplicativos e rápido avanço tecnológico, requer uma reavaliação das estruturas tradicionais de teste de segurança.

As avaliações de segurança convencionais não capturam adequadamente a complexidade das metodologias de ataque modernas. Quando as organizações avaliam os compromissos dos fornecedores em relação a proteções específicas, como recursos de detecção de deepfake, algumas perguntas críticas precisam ser feitas. Como demonstrado, 115.570 variações precisariam ser comprovadas para dar respaldo a uma reivindicação de detecção de “troca de rosto”, e esse vetor de ameaça não encapsula totalmente todos os deepfakes.

O sucesso documentado dos recentes ataques de mídia sintética expôs vulnerabilidades em vários setores, desde perdas financeiras até comprometimento da segurança da força de trabalho. O incidente KnowBe4[13], em que uma empresa de segurança cibernética contratou inadvertidamente alguém que usava imagens sintéticas durante entrevistas remotas, concedendo-lhe acesso autorizado a sistemas internos, demonstra como a fraude de identidade sintética se estende além do roubo financeiro para representar sérias ameaças internas por meio do engano da identidade da força de trabalho.

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

Tais incidentes revelam que as medidas de proteção atuais não estão abordando adequadamente essas ameaças sofisticadas, criando uma lacuna perigosa entre as capacidades de segurança percebidas e reais. Essa disparidade representa um risco organizacional significativo que exige atenção imediata, particularmente porque a contratação remota continua a ser uma prática padrão.

Muitas organizações podem ter uma compreensão incompleta sobre sua situação de segurança. Dadas as inúmeras maneiras pelas quais os ataques podem ocorrer, é importante ir além dos testes de segurança tradicionais e se concentrar no monitoramento e na adaptação contínuos. Só porque os ataques não são detectados não significa que eles não estejam acontecendo; isso pode ser devido a recursos de monitoramento limitados. Para se manterem à frente, as organizações precisam de sistemas de monitoramento fortes e flexíveis que possam identificar e analisar possíveis ataques em tempo real.

Liderança da iProov em testes internacionais, benchmarking e estruturas de segurança

Embora as certificações tradicionais do setor do NIST e do iBeta estabeleçam padrões de segurança de linha de base importantes, o cenário de ameaças em rápida mudança requer uma perspectiva moderna. O novo programa de "Certificação de Verificação Facial" da FIDO Alliance avalia a robustez e a interoperabilidade das soluções biométricas, testando especificamente sua eficácia em relação aos deepfakes apresentados em ambientes controlados. Embora essa certificação represente um progresso na padronização de testes de segurança, é importante notar que atualmente ela se concentra em ataques de apresentação, e não em todo o espectro de possíveis ameaças deepfake ao longo do ciclo de vida da identidade.

Nosso compromisso com o avanço da segurança biométrica levou a testes independentes rigorosos pela Diretoria de Ciência e Tecnologia do Departamento de Segurança Nacional dos EUA e líderes de segurança cibernética como Outflank, Jumpsec e Kroll Redscan, validando nossas capacidades de defesa robustas contra ataques sofisticados emergentes.

A iProov molda ativamente o futuro da segurança biométrica por meio de colaborações estratégicas. Estamos trabalhando com a MITRE para expandir sua estrutura ATLAS, contribuindo com nossa experiência em detecção de ataques alimentados por IA e ameaças de mídia sintética. Essa colaboração ajuda a estabelecer abordagens padronizadas para a avaliação e defesa contra vetores de ataque emergentes em sistemas de verificação de identidade remotos.

Através de nossa abordagem baseada na ciência e da equipe de pesquisa líder do setor, ganhamos reconhecimento como a autoridade científica mais respeitável em segurança biométrica facial. Aconselhamos regularmente organizações e governos importantes, como a ENISA e a MITRE, ajudando a aumentar a conscientização sobre as ameaças do mundo real e estabelecendo as melhores práticas para a segurança biométrica. Nossos insights impulsionam padrões e estruturas do setor além das limitações tradicionais de teste "point-in-time". Essa abordagem abrangente garante que nossas soluções permaneçam eficazes contra ameaças atuais e emergentes, ao mesmo tempo em que ajudam a moldar padrões internacionais para a próxima geração de desafios de segurança biométrica.

"A colaboração da iProov com a MITRE ATLAS já forneceu informações valiosas sobre o cenário de ameaças em evolução. Nossa contribuição para a documentação de padrões de ataque e metodologias de detecção - descobertos por meio de ataques reais e avaliações abrangentes de red teaming - ajudou a criar uma compreensão mais ampla da defesa contra ameaças à verificação remota de identidade baseadas em IA."- *Panos Papadopoulos, Chefe da Equipe Red Team, iProov*

Aprofunde-se no cenário de ameaças:
O paradoxo da baixa taxa de ataque

Embora a queda nas taxas de ataque possa inicialmente parecer simplesmente indicar um interesse reduzido dos agentes de ameaça, nossa análise revela uma dinâmica de segurança mais sutil que chamamos de “paradoxo da baixa taxa de ataque”. Esse fenômeno ocorre quando medidas de segurança robustas efetivamente impedem ataques, fazendo com que os agentes de ameaças abandonem seus esforços e redirecionem recursos para alvos mais vulneráveis.

A inteligência contra ameaças mostra que os invasores definem ativamente os sistemas de verificação e compartilham informações dentro de suas comunidades sobre quais sistemas evitar, fazendo com que taxas de ataque persistentemente baixas sejam um forte indicador de eficácia de segurança, em vez de uma atividade de ameaças reduzida. Essa compreensão é crucial para contextualizar nossa postura de segurança atual – os volumes de ataque reduzidos validam nossos aprimoramentos de segurança contínuos e demonstram sua eficácia contínua em manter uma forte decisão defensiva contra as ameaças em evolução.

Sistemas de segurança fortes:
- Os ataques são rapidamente abandonados
- Agentes de ameaças alertam outras pessoas em suas comunidades
- Os recursos são redirecionados para alvos mais fáceis
- As tentativas de ataque permanecem baixas

Sistemas vulneráveis:
- Tornam-se alvos frequentes
- Passam por campanhas de ataque sustentadas

Importância da detecção e resposta gerenciadas (MDR)
Esse padrão demonstra por que as organizações precisam de:

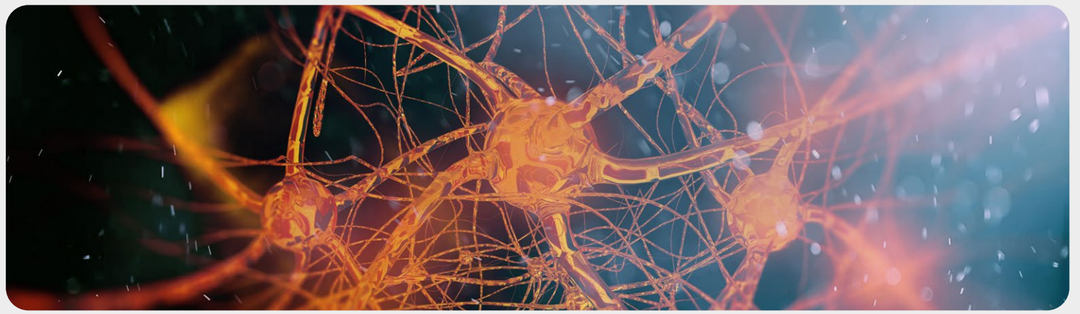
01 Medidas de segurança preventivas fortes

02 Recursos de monitoramento contínuo

03 Coleta de informações sobre ameaças

04 Avaliações de segurança regulares

Mesmo quando as taxas de ataque são baixas, a manutenção de uma segurança robusta permanece crítica – são precisamente essas medidas que mantêm as taxas de ataque baixas e protegem contra ameaças em evolução.



Considerações sobre a pilha técnica:

etapas acionáveis para a identidade moderna

O cenário de ameaças em evolução exige uma abordagem em várias camadas para a verificação de identidade. A chave são estratégias abrangentes que combinem inovação tecnológica com experiência humana, mantendo a eficiência operacional. A estrutura a seguir descreve as áreas de foco para o desenvolvimento de medidas de segurança resilientes.

Adoção da segurança em tempo real

A era das atualizações periódicas de segurança deu lugar a sistemas de monitoramento e detecção contínuos que operam em tempo real. Essa mudança de paradigma permite o dimensionamento automatizado de defesas durante períodos de alto risco e a implantação perfeita de patches de segurança. Os sistemas de segurança em tempo real atuam como escudos e sensores, protegendo simultaneamente contra ameaças conhecidas e identificando padrões de ataque emergentes. Essa abordagem proativa ajuda a identificar e abordar possíveis vulnerabilidades antes que elas possam ser exploradas em escala.

A convergência entre tecnologia e experiência

O sucesso requer uma mistura estratégica de sistemas automatizados e experiência humana. A detecção automatizada de ameaças fornece a velocidade e a escala necessárias para gerenciar as tentativas de verificação, enquanto a análise de especialistas fornece informações cruciais para operações de segurança eficazes. Essa sinergia permite a resposta imediata a ameaças e a identificação proativa de vulnerabilidades. A combinação de cientistas biométricos e recursos automáticos cria um ciclo de feedback em que os sistemas automatizados sinalizam padrões suspeitos para avaliação, enquanto as percepções humanas refinam os algoritmos de detecção para melhor identificar novos métodos de ataque.

Desenvolvimento de estratégias de segurança adaptáveis

As medidas de segurança eficazes evoluem ao lado do cenário de ameaças por meio da avaliação contínua e do desenvolvimento de medidas de proteção que antecipam futuros vetores de ataque. As estratégias bem-sucedidas equilibram a segurança robusta com a experiência do usuário, usando uma avaliação de risco sofisticada para ajustar as medidas de segurança com base no contexto e no nível de risco.Isso evita que o atrito excessivo leve os usuários a alternativas menos seguras, mantendo os níveis de proteção apropriados.

Criação de uma defesa colaborativa

As ameaças modernas exigem uma combinação de experiência interna e inteligência externa. Parcerias com especialistas em segurança, participação em redes de inteligência de ameaças e conexões de pesquisa dedicadas fornecem acesso a conhecimento especializado e inteligência de ameaças mais ampla. O compartilhamento interorganizacional de padrões e indicadores de ataque fortalece as capacidades de defesa coletiva além do que as medidas de segurança individuais podem alcançar sozinhas.

Preparação para ameaças futuras

Uma arquitetura de segurança robusta incorpora flexibilidade e escalabilidade a partir do zero, apoiada por processos claros para a avaliação de ameaças e a rápida implantação de novas medidas de segurança. Olhar além das ameaças atuais para considerar o potencial das tecnologias emergentes para ataque e defesa garante que os sistemas possam se adaptar aos desafios em evolução, mantendo a escalabilidade para aumentar os volumes de ataque.

Conclusão:

Navegação pela nova realidade da segurança de identidade

O cenário de verificação de identidade atingiu um ponto de inflexão crítico. Nossa análise de inteligência contra ameaças de 2025 revela um aumento da sofisticação do ataque e uma transformação fundamental na forma como a fraude de identidade é executada e comercializada. Os avanços nas ferramentas de mídia sintética, combinados com mercados prósperos de Crime como Serviço, criaram um ambiente democratizado onde ataques complexos podem ser lançados por agentes com conhecimento técnico mínimo.

Vários desenvolvimentos importantes definem essa nova realidade: A grande escala de combinações de ataques potenciais – com mais de 100.000 permutações possíveis de apenas três vetores de ataque comuns – demonstra que as medidas de segurança tradicionais e estáticas não são mais suficientes. As organizações devem se adaptar a um cenário de ameaças em que os invasores são capazes de alternar rapidamente táticas e alvos, o que torna os recursos de detecção e resposta em tempo real essenciais.

Nossa análise dos padrões de ataque revela um paradoxo crucial: Os sistemas mais seguros geralmente mostram as taxas de ataque mais baixas, pois os agentes de ameaças abandonam rapidamente as tentativas contra defesas robustas em favor de alvos mais fáceis. Esse “paradoxo da baixa taxa de ataque” ressalta a importância de manter medidas de segurança fortes, mesmo quando os níveis de ameaça aparentes parecem diminuir.

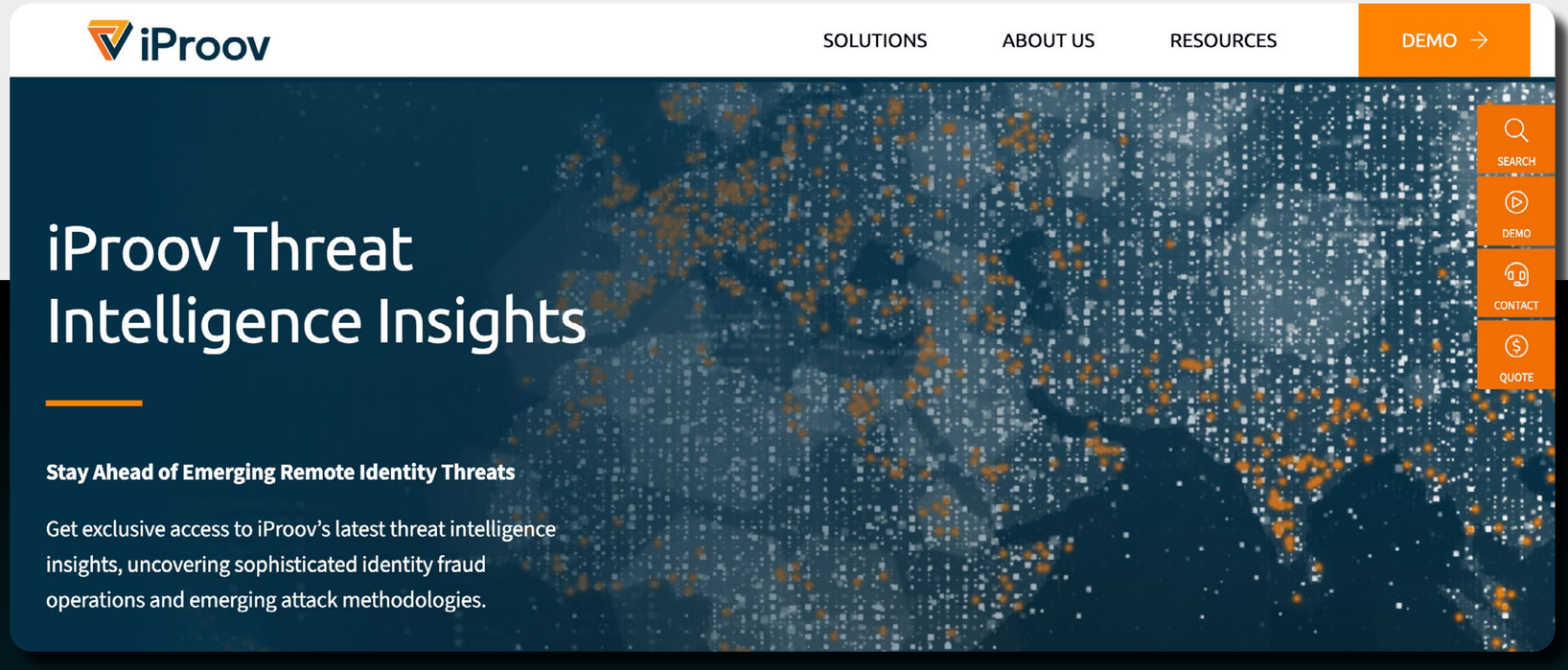
O fator de detecção humano continua sendo uma vulnerabilidade crítica: Nossa pesquisa de deepfake mostra que apenas 0,1% das pessoas conseguem identificar mídias sintéticas com segurança. Essa suscetibilidade generalizada, combinada à qualidade crescente do conteúdo sintético, cria riscos sem precedentes para os sistemas de verificação de identidade remotos.

01 **Proteção em tempo real:** ir além das atualizações periódicas para recursos de monitoramento contínuo e resposta instantânea

02 **Defesa dinâmica:** implementar medidas de segurança que evoluem ao lado de ameaças emergentes

03 **Colaboração humano-máquina:** combinando sistemas de detecção automatizados com análise de especialistas biométricos e caça a ameaças

O futuro da segurança de identidade não está em nenhuma tecnologia ou abordagem única, mas na integração de várias camadas defensivas alimentadas por informações sobre ameaças em tempo real e guiadas por um profundo conhecimento científico. À medida que enfrentamos um cenário de ameaças crescente e cada vez mais complexo, a questão não é mais se as organizações enfrentarão ataques de identidade sofisticados, e sim quão bem elas estão preparadas para detectá-los e evitá-los. O sucesso neste novo ambiente requer um compromisso com a evolução contínua da segurança, apoiada por informações sobre ameaças, recursos de MDR em tempo real e tecnologia de verificação remota que vai além da detecção de vivacidade para validar a presença humana genuína.



Sua organização precisa de informações mais frequentes sobre o cenário de ameaças remotas do IDV?

Registre seu interesse

Relatório de assinatura mensal de inteligência de ameaças