///AXUR

Threat Landscape

→ 2024/2025

Mensagem da Axur

As ameaças mudam a cada ano, mas 2024 trouxe desafios únicos: a integração profunda da Inteligência Artificial (IA) na cibersegurança e o aumento do alcance dos riscos que ela carrega.

Criminosos têm usado IA generativa para criar campanhas de phishing extremamente convincentes e automatizar vetores de ataque em uma escala nunca vista antes. Por outro lado, a IA também tem sido uma aliada poderosa na defesa, enfrentando ameaças com uma cobertura, velocidade e priorização sem iguais. Como você verá nos próximos capítulos, a IA também ajudou a moldar os insights deste relatório, mostrando como a tecnologia pode colaborar para criar resiliência diante dos desafios que enfrentamos.

Enquanto isso, o ransomware continua sendo uma ameaça persistente. Este ano, vimos o surgimento de novos métodos de acesso, incluindo ataques cada vez mais sofisticados à cadeia de suprimentos, e apagões digitais que colocaram nossos sistemas à prova. Ainda assim, em meio a esse caos, também vimos muita colaboração.

2024 nos desafiou como nunca. Foi um ano para repensarmos não apenas as ferramentas que usamos, mas também a forma como encaramos a defesa contra o que está por vir. Para mim, foi um período que reafirmou minha convicção na nossa missão: criar experiências digitais mais seguras, aproveitando o poder da tecnologia para conectar, responder e se adaptar mais rápido do que nunca.

Convido você a explorar este relatório, em que analisamos as ameaças em evolução, traçamos estratégias de resposta e compartilhamos insights que podem ajudar sua equipe a navegar com sucesso nesse cenário tão desafiador. Não só para entender os obstáculos, mas para enxergar as oportunidades que eles trazem.

Para construir resiliência e garantir que, à medida que a tecnologia avança, ela sirva para criar um futuro digital mais seguro.

Estamos juntos nessa jornada.

Fábio F. Ramos
CEO da Axur

Sumário

Resumo Executivo

13x mais credenciais detectadas, totalizando **57,2 bilhões**

339 milhões de cartões de crédito e débito detectados, **26x mais do que em 2023**

Foram **72.455 páginas detectadas.** Insights revelam que 70% das páginas fraudulentas não utilizam palavras-chave no domínio

439 mil casos de fraudes foram registrados, 118% mais do que no ano anterior, incluindo perfis e apps falsos, e uso fraudulento de marca

Analisamos mais de **2,3 bilhões de mensagens na Deep & Dark Web**, resultando em mais de 966 mil incidentes

32% de todos os incidentes na Deep & Dark Web foram detectados em conteúdos audiovisuais, como áudios, vídeos e imagens estáticas

Removemos mais de **401 mil conteúdos fraudulentos** através dos fluxos automatizados de Takedown.

Perfis falsos e exposição de informações foram amplamente usados para atacar executivos e VIPs, com mais de **33 mil incidentes.**

→ Ransomware no setor de saúde:
ataques interromperam serviços críticos nos EUA e Reino Unido.

→ Maior da história:
Cloudflare bloqueia ataque DDoS recorde de 3,8 Tbps.

→ AT&T e Snowflake:
vazamento expôs milhões de registros, revelando fragilidades em telecomunicações.

→ Falha do Falcon:
problemas no sensor da CrowdStrike causaram interrupções e exploraram vulnerabilidades interconectadas.

→ Operação Cronos:
ação global enfraqueceu o grupo LockBit, marcando avanços no combate ao ransomware.

Setores críticos

→ Varejo/E-commerce

1º em phishing: 27.305 páginas fraudulentas detectadas.
2º em incidentes na Deep & Dark Web: 172.873 incidentes.
3º em takedowns: 61.343 conteúdos fraudulentos removidos.

→ Financeiro/Seguros

1º em takedowns: 107.601 conteúdos removidos.
2º em phishing: 18.915 páginas detectadas.
2º em incidentes na Deep & Dark Web: 257.275 incidentes.

→ Tecnologia

1º lugar em incidentes na Deep & Dark Web: 418.806 incidentes.
3º lugar em phishing: 9.502 páginas fraudulentas detectadas.

→ Telecomunicações

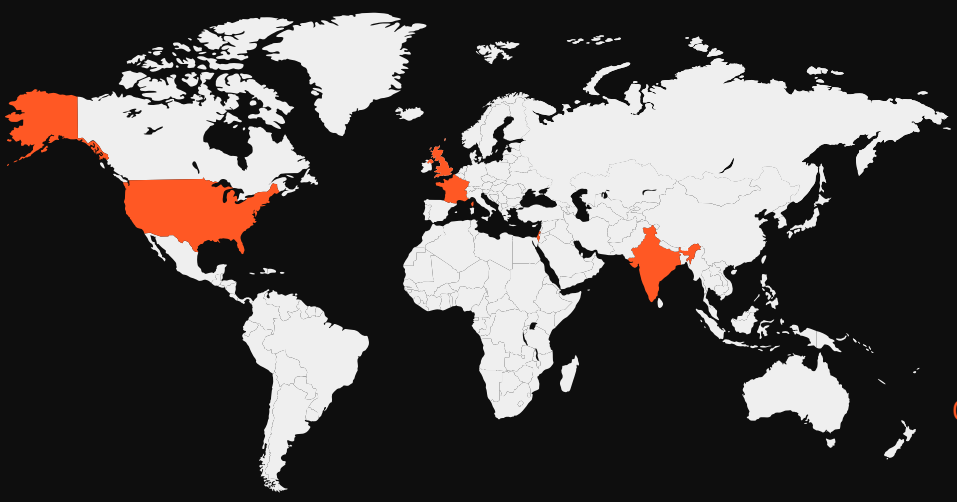
2º em takedowns: 93.287 conteúdos fradulentos removidos.
4º em incidentes na Deep & Dark Web: 47.018 registros.

→ Turismo e viagens

5º em takedowns: 45.060 conteúdos fraudulentos neutralizados.

Localizações mais impactadas

EUA, Índia, Reino Unido, França e Israel foram os mais visados pelo cibercrime em 2024.



Resumo do cibercrime no Brasil

→ Pix sob ataque: malware CryptoClippy redireciona transferências na modalidade "copia e cola".

→ Golpes com "kits bico": pacotes de dados pessoais usados para fraudar processos de validação de identidade.

→ Colaboradores recrutados: subornos para acesso interno crescem como vetor de invasão.

→ Phishing adaptado: ataques integram SMS, WhatsApp e publicidade mobile para enganar consumidores.

Tendências de ataque

→ IA no cibercrime: deep fakes e ataques personalizados impulsionados por GenAI.

→ Expansão das superfícies de ataque: dispositivos IoT e políticas BYOD ampliam vulnerabilidades.

→ Infostealers mais sofisticados: roubo de credenciais e cookies se torna mais versátil.

→ Cibersegurança como prioridade nacional: tensões geopolíticas reforçam a importância de uma abordagem robusta.

Recomendações

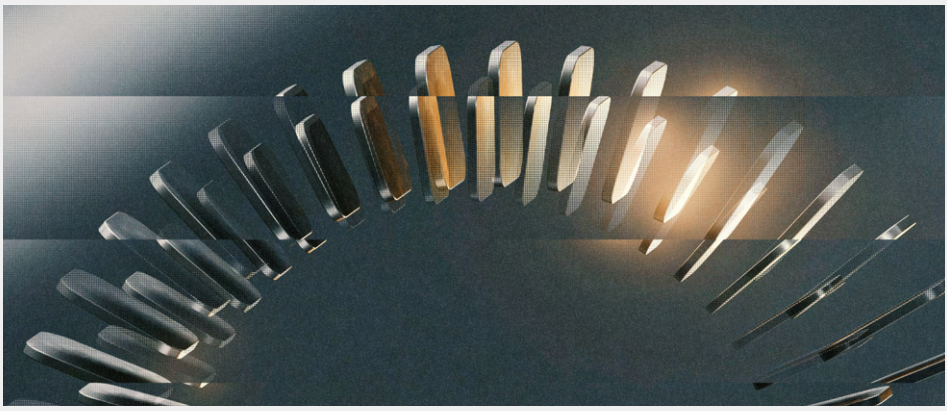
→ Gestão de identidades: monitorar e revogar credenciais comprometidas, complementando MFA com análises contínuas.

→ EASM e vulnerabilidades: priorizar vulnerabilidades críticas com insights de inteligência de ameaças.

→ Planos de continuidade: mapear dependências críticas para garantir resiliência operacional.

→ Conscientização: programas educativos para fortalecer a cultura de segurança dentro das organizações.

Panorama de Ameaças e Exposição



O cenário de cibersegurança em 2024 se apresentou como um campo de batalha dinâmico e desafiador.

Os ataques de ransomware continuaram a ser uma preocupação central, com grupos aperfeiçoando suas táticas e visando setores críticos, como saúde e infraestrutura. Além disso, a ascensão de ataques baseados em identidade, impulsionados por técnicas sofisticadas de phishing e engenharia social, destaca a necessidade de uma defesa robusta.

As vulnerabilidades em nuvem também estão em alta, refletindo a crescente dependência neste tipo de serviço.

A análise das CVEs mais exploradas revelou um aumento significativo na exploração de vulnerabilidades críticas, com cibercriminosos aproveitando falhas em sistemas amplamente utilizados. Os malwares têm demonstrado uma capacidade de comprometer dados sensíveis, enquanto as táticas mais utilizadas incluem ataques DDoS e phishing, com mais sofisticação e frequência.

Nossa solução de IA, equipada com inteligência de ameaças (CTI) integrada, é capaz de processar e resumir milhares de alertas e horas de leitura em conteúdos de ameaças, entregando apenas os insights mais relevantes para superfícies de ataque específicas ou tópicos de interesse previamente definidos.

Essa tecnologia avançada foi utilizada para criar o panorama de ameaças deste capítulo, que é comentado por Alisson Moretto, Head de Cyber Threat Intelligence da Axur.

44 mil
artigos analisados

6 mil horas
de análise de ameaças

Revisado e comentado por:

Alisson Moretto

Head de Cyber Threat Intelligence da Axur

> Ampla experiência na investigação de crimes digitais e suporte a incidentes.

> Professor convidado de pós-graduação e palestrante em eventos de destaque na área.

Principais eventos de 2024

Clique nos títulos para visualizar análise completa

↗ Ataque cibernético na Change Healthcare interrompe serviços de prescrição nos EUA

Este incidente destaca a vulnerabilidade dos sistemas de saúde a ataques cibernéticos, impactando os serviços de prescrição em todo os EUA e levantando preocupações sobre a segurança dos pacientes e a integridade dos dados.

↗ Qilin Ransomware interrompe os serviços de sangue do NHS em Londres

O ataque a um serviço vital de saúde demonstra o potencial do ransomware para interromper operações públicas essenciais, afetando o atendimento aos pacientes e os serviços de emergência.

↗ Cloudflare barra maior ataque DDoS da história

A Cloudflare mitigou um ataque DDoS recorde de 3,8 Tbps, realizado com dispositivos IoT comprometidos e direcionado a diversos setores, destacando a crescente sofisticação das ciberameaças globais.

↗ Vazamento de dados da AT&T: Grande invasão na Snowflake expõe registros de chamadas

Este vazamento levanta sérias preocupações de privacidade para milhões de clientes e destaca vulnerabilidades na infraestrutura de telecomunicações.

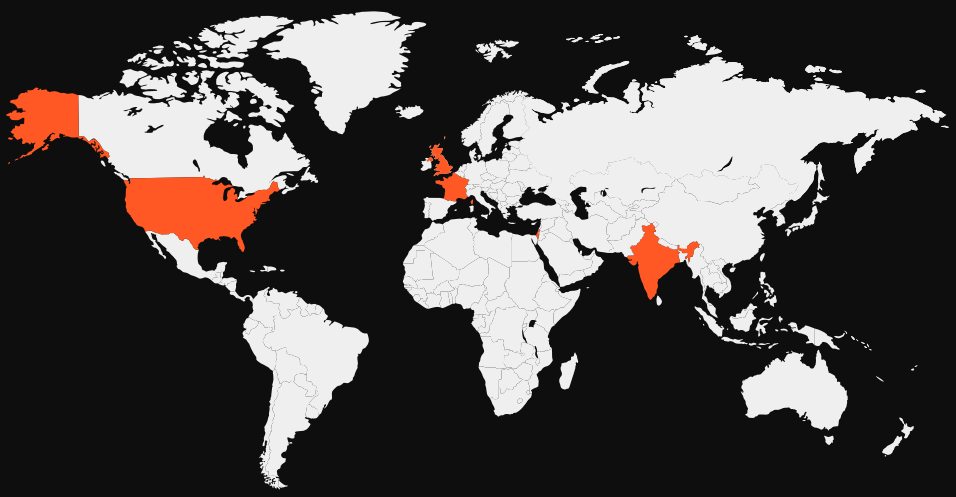
↗ Operação Cronos: Desmantelando a rede de ransomware LockBit

Esta operação representa um esforço significativo das autoridades para combater o ransomware, mirando um dos grupos mais notórios no cibercrime, o que pode desencorajar ataques futuros.

↗ Falha global no Falcon expõe vulnerabilidades interconectadas

Uma atualização do sensor Falcon da CrowdStrike causou erros BSOD em sistemas críticos, impactando diversos setores. O incidente gerou ataques de phishing explorando a situação e destacou a importância de controles de qualidade e resiliência cibernética.

Localizações mais impactadas no mundo em 2024



Os Estados Unidos, Índia, Reino Unido, França e Israel foram as localizações mais visadas por agentes de ameaças em 2024, devido a uma combinação de fatores geopolíticos, vulnerabilidades tecnológicas e o aumento geral de atividades cibernéticas maliciosas.

A tensão geopolítica, especialmente no Oriente Médio, teve um papel significativo. Israel, por exemplo, se tornou um alvo frequente de ataques cibernéticos, em parte devido à sua posição como um aliado estratégico dos EUA e suas interações com países como o Irã.

Em 2024, Israel recebeu apoio militar e cibernético dos EUA, Reino Unido e França para repelir ataques iranianos, o que intensificou a atenção de grupos cibernéticos hostis, como o Rippersec. Os setores governamentais, educacionais e de saúde em países como os EUA e Reino Unido mostraram-se vulneráveis a ataques. As empresas nesses setores frequentemente lidam com dados sensíveis e possuem infraestruturas que podem ser exploradas por cibercriminosos. Além disso, a transição para o trabalho híbrido aumentou as lacunas de segurança, permitindo que os atacantes explorassem falhas em sistemas de e-mail e redes corporativas. As motivações por trás desses ataques variam desde espionagem até extorsão financeira.

O ransomware continuou como uma ferramenta comum para exigir resgates em dinheiro ou criptomoedas. Em abril de 2024, os EUA lideraram os registros desse tipo de ataque. A Índia também foi identificada como um alvo significativo devido à sua crescente digitalização e à importância estratégica na região da Ásia-Pacífico.

Atores maliciosos mais ativos

Ao longo do ano, o cenário de ameaças cibernéticas viu a evolução e a emergência de diversos grupos, com algumas mudanças significativas em suas operações e impacto.

Grupos como RansomHub e ShinyHunters estão se destacando por suas operações agressivas e impacto significativo. Enquanto isso, outros grupos como LockBit estão enfrentando dificuldades devido à pressão das autoridades.

A colaboração entre grupos hacktivistas também está se intensificando, refletindo uma nova estratégia no cenário das ameaças cibernéticas.

Ativo desde: 2020

Motivação: financeira

Setores mais afetados: organizações nos Estados Unidos e na Europa, com foco em infraestrutura e outros setores

País de origem: Rússia

RansomHub ↗

Este grupo de ransomware é considerado uma reencarnação do ransomware Knight. Rapidamente, tornou-se um dos grupos mais proeminentes, especialmente após ações policiais contra o LockBit3, que resultaram em uma queda significativa na sua atividade. Também foi responsável por um aumento notável de vítimas em 2024. O grupo fez mais de 210 novas vítimas, de acordo com o FBI, entre elas empresas como a montadora Kawasaki e o provedor de comunicações americano Frontier Communications, além de vazar dados da Change HealthCare após o ataque do BlackCat/ALPHV.

Ativo desde: 2020

Motivação: financeira

Setores mais afetados: financeiro e outras empresas ricas em dados

País de origem: opera internacionalmente

ShinyHunters ↗

Este grupo ficou em evidência após um ataque à Ticketmaster, em que alegou ter roubado dados pessoais de 560 milhões de clientes. O ataque pode ter sido um dos maiores da história em termos de número de vítimas e destacou a capacidade do grupo para realizar ataques massivos.

Ativo desde: 2023

Motivação: política

Setores mais afetados: governamentais ou empresas de países contrários à sua ideologia

País de origem: Malásia

RipperSec ↗

Este grupo se destacou por suas atividades DDoS autoproclamadas em ataques à Israel e a empresas como X, Uber, Ferrari e Paramount. Sua campanha de apoio ao fundador do Telegram, Pavel Durov, expandiu-se rapidamente com o nome de #FreeDurov, para mobilizar vários outros grupos hacktivistas, mostrando uma mudança na dinâmica de colaboração entre grupos que antes operavam isoladamente.

Ativo desde: 2022

Motivação: financeira

Setores mais afetados: vários, incluindo governo, telecomunicações, energia e outros

País de origem: Rússia

Intelbroker ↗

Embora não tenham surgido muitas informações novas específicas sobre mudanças na operação do Intelbroker em 2024, o agente de ameaças continua ativo no cenário, principalmente em fóruns, nos quais compartilha acessos e dados.

Ativo desde: 2019

Motivação: financeira

Setores mais afetados: vários, incluindo indústria, saúde, educação e outros

País de origem: Rússia

LockBit ↗

Após uma série de operações policiais bem-sucedidas contra o LockBit3, o grupo sofreu um declínio significativo em sua atividade. O grupo foi responsável por fazer mais de 2 mil vítimas ao redor do mundo e extorquir mais de US$120 milhões em pagamentos de resgate. Em 2024, uma cooperação entre 10 países possibilitou uma desintegração da sua infraestrutura.

CVEs em destaque 2024

Grupos de ransomware já começaram a explorar essa vulnerabilidade para injetar cargas maliciosas e instalar ransomware em servidores vulneráveis.

O patch deve ser aplicado atualizando para as versões 8.1.29, 8.2.20 ou 8.3.8. Além disso, recomenda-se uso do Verificador de Suscetibilidade à Injeção de Argumentos, implementação de WAF, restrição de acesso a scripts PHP-CGI, validação de entradas e auditorias regulares de segurança.

Uma vulnerabilidade crítica de execução remota de código (CVE-2024-40711) foi identificada no software Veeam Backup and Replication, afetando versões 12.1.2.172 e anteriores, com uma pontuação CVSS de 9,8. Dois patches foram lançados para corrigir o problema, sendo o segundo uma solução completa.

A falha está relacionada a ataques de desserialização em um mecanismo de comunicação antigo, sendo bastante explorada por grupos de ransomware.

Foi descoberta no SolarWinds Web Help Desk (WHD), permitindo que invasores não autenticados acessem e modifiquem detalhes de tickets, expondo dados sensíveis como credenciais e solicitações de redefinição de senha. Um hotfix foi lançado para corrigir o problema.

A vulnerabilidade no libcurl ocorre quando um aplicativo permite HTTP/2 server push, e os cabeçalhos recebidos excedem o limite de 1000. Nesse caso, libcurl aborta o push, mas não libera toda a memória alocada, causando um vazamento de memória que ocorre silenciosamente, dificultando sua detecção. Esta vulnerabilidade pode causar uma condição de negação de serviço.

Identifica um problema em métodos de verificação de endereços IPv4 mapeados em IPv6. Métodos como IsPrivate e IsLoopback retornam resultados incorretos para endereços que seriam válidos em suas formas tradicionais IPv4.

Trata de uma vulnerabilidade de desserialização de dados não confiáveis que pode permitir a execução remota de código (RCE) com carga maliciosa, mesmo sem autenticação.

Explore mais insights de CVEs com a Axur

Comece seu teste grátis da nossa solução de Cyber Threat Intel com IA e descubra mais sobre as ameaças mais relevantes de 2024.

Teste grátis

Malwares mais ativos em 2024

Em 2024, o cenário de malware está marcado por um aumento na sofisticação dos ataques e pela prevalência do ransomware como serviço (RaaS). Grupos bem conhecidos continuam a evoluir suas estratégias para maximizar o impacto financeiro sobre as vítimas.

TTPs mais utilizados

T1078 - Contas Válidas

A técnica T1078 refere-se ao uso de contas válidas para obter acesso a sistemas. Os atacantes frequentemente exploram credenciais legítimas para evitar detecções e manter o acesso a redes comprometidas. Essa técnica é particularmente eficaz em ambientes onde as credenciais são frequentemente reutilizadas ou mal gerenciadas.

T1190 - Exploração de Aplicação Pública

Abrange a exploração de aplicações que estão expostas publicamente na internet. Os atacantes podem explorar falhas em sistemas web para obter acesso inicial a redes corporativas. Essa técnica é crítica, pois muitas organizações não aplicam patches rapidamente, deixando suas aplicações vulneráveis.

T1071 - Protocolos de Camada de Aplicação

Envolve o uso de protocolos de camada de aplicação para comunicação com servidores de comando e controle (C2). Os atacantes utilizam essa técnica para exfiltrar dados ou receber instruções sem levantar suspeitas, utilizando protocolos comuns como HTTP ou HTTPS.

T1059 - Interpretação de Comandos e Scripts

Refere-se ao uso de interpretadores de comandos e scripts para executar código malicioso. Isso inclui o uso de linguagens como PowerShell, Bash ou Python para realizar ações maliciosas no sistema alvo. É uma técnica comum em ataques que visam automação ou execução remota de forma a evitar controles de segurança.

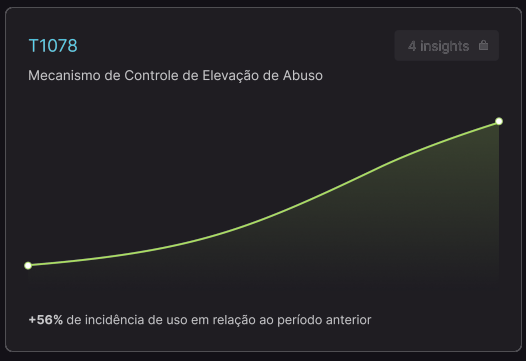
T1203 - Exploração de Execução de Cliente

Refere-se à exploração de vulnerabilidades em software cliente para executar código malicioso. Isso pode ocorrer através da abertura de documentos maliciosos ou links em e-mails, levando a uma execução não autorizada. Essa técnica é frequentemente utilizada em ataques direcionados onde os usuários são induzidos a executar ações que comprometem seus sistemas.

T1566 - Phishing

Envolve ataques de phishing, em que os atacantes tentam enganar usuários para que revelem informações sensíveis, como credenciais ou dados financeiros. Essa técnica continua a ser uma das mais prevalentes devido à sua eficácia e ao baixo custo para os atacantes.

1º	T1078	129 fontes
2º	T1071	125 fontes
3º	T1203	48 fontes
4º	T1190	27 fontes
5º	T1059	27 fontes



2024 em números

Credenciais

A plataforma Axur detectou 57,2 bilhões de credenciais vazadas ao longo de 2024, evidenciando a necessidade de uma gestão de identidade assertiva e eficiente para proteger serviços online e redes corporativas.

As detecções da Axur são baseadas em atividade na Deep & Dark Web e em arquivos compartilhados na web aberta, inclusive em fóruns frequentados por hackers.

57.233.053.785

Total de credenciais coletadas
de todas as fontes

19.299.578.150

Credenciais
corporativas

Por este motivo, é possível afirmar que todas essas credenciais já estão nas mãos dos cibercriminosos. Se essas credenciais não forem revogadas e substituídas, as contas permanecerão em risco.

Além disso, quase todas as credenciais (98%) são compartilhadas já sem qualquer criptografia. Isso indica que os cibercriminosos estão utilizando técnicas para encontrar senhas que correspondam a algum hash vazado (como MD5 e SHA) ou estão obtendo senhas já sem criptografia através de infostealers.

De acordo com o Verizon Data Breach Investigations Report (DBIR) de 2024, 31% de todas as violações de acesso dos últimos dez anos aconteceram por conta de alguma credencial roubada. No entanto, em algumas categorias de ataque — como em invasões de contas em plataformas web — mais de 70% dos acessos indevidos ocorreram por causa do uso de uma credencial fraca ou obtida previamente.

A ameaça dos infostealers

3,2 bilhões de credenciais foram obtidas por infostealers em 2024

O infostealer é uma categoria de malware que abrange códigos criados para roubar credenciais.

Existem várias famílias de infostealers que são aprimoradas constantemente para evitar a detecção por parte de soluções antivírus.

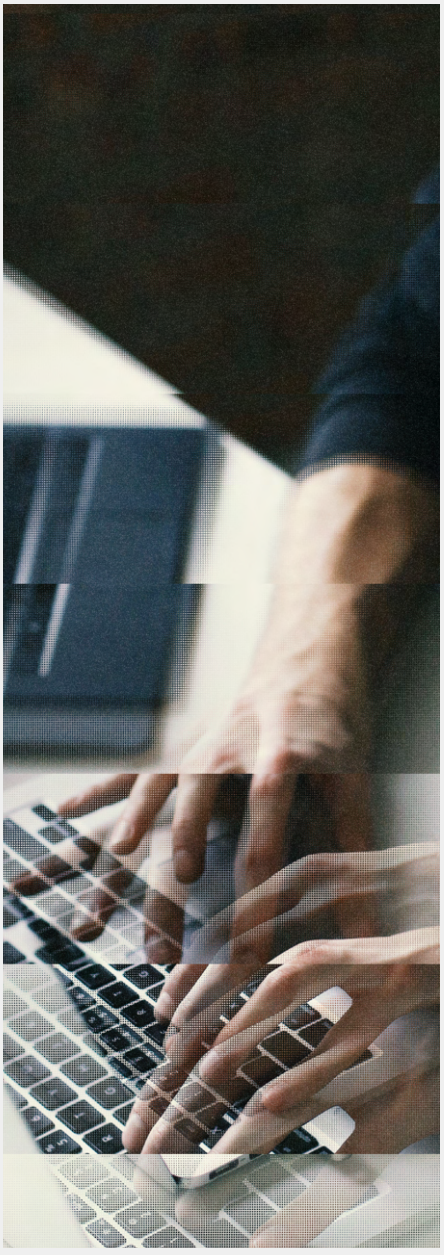
Ao contrário dos "keyloggers" tradicionais, que atuavam de forma passiva e aguardavam o usuário acessar um sistema para roubar a senha, os infostealers são programados para buscar e extrair todas as informações do sistema.

Quando possível, o infostealer acessa as senhas armazenadas no navegador web, em gerenciadores de senhas e em aplicativos instalados no computador (gerenciadores de carteiras digitais, plataformas de distribuição de software e jogos, entre outros).

O infostealer também pode roubar cookies armazenados pelo navegador.

O roubo de cookies e de tokens de acesso realizado pelos infostealers permite o ataque de sequestro de sessão (session hijack). Usando essa sessão previamente autenticada, o atacante pode burlar a exigência de autenticação multifator (MFA). O infostealer pode ser disseminado através de campanhas de engenharia social, softwares piratas e phishing.

As senhas roubadas pelos infostealers são geralmente vendidas para outros criminosos especializados — enquanto golpes financeiros podem utilizar senhas de bancos ou chaves de carteiras digitais, ataques de ransomware podem se aproveitar de credenciais de VPNs ou de serviços de acesso remoto.



Novas regras para credenciais

Além de serem roubadas por infostealers, senhas sem criptografia também podem ser obtidas com ataques de força bruta e por credential stuffing, que é a revalidação de senhas usadas em múltiplos serviços para descobrir outros locais em que a mesma combinação é válida.

Senhas criptografadas ou representadas por um algoritmo de hashing também podem ser comprometidas a partir de valores previamente calculados em Rainbow Tables ou quebradas ao longo do tempo conforme a capacidade de computação aumenta.

Nesse cenário, a definição de uma "senha forte" já não é mais a mesma.

Em setembro, o National Institute of Standards and Technology (NIST), órgão normativo do governo norte-americano, publicou uma revisão do seu documento de Password Guidelines com recomendações mais alinhadas a essa realidade para entidades do governo federal.

De maneira geral, a norma agora favorece uma postura mais proativa das organizações no bloqueio de credenciais comprometidas em vez de uma abordagem focada em regras rígidas, como a troca periódica de senhas.

As senhas também devem ser mais longas para evitar ataques de força bruta e a quebra de mecanismos de proteção.

☑ Recomendações Atuais

→ **Revogar senhas comprometidas**: os sistemas de autenticação devem revogar senhas comprometidas e bloquear o uso de senhas inseguras, incluindo em novos cadastros.

→ **Uso de senhas de ao menos 15 caracteres**: usuários devem ser orientados a usar senhas mais longas. Nenhum sistema deve aceitar senhas com menos de 8 caracteres.

→ **Permitir ao menos 64 caracteres**: não imponha limites rígidos para senhas curtas e permita até 64 caracteres para suportar passphrases.

☒ O que não é recomendado

→ **Trocas de senha periódicas**
Organizações devem priorizar a revogação de senhas comprometidas e a adoção de MFA. Trocas obrigatórias frequentes levam a senhas mais fracas, reduzindo a resistência à força bruta.

→ **Uso de caracteres especiais ou senhas "complexas"**
Com a migração para senhas longas ou frases, a entropia aumenta em relação ao uso de caracteres especiais. O NIST recomenda aceitar qualquer caractere Unicode.

→ **Dicas de senhas**
Evite usar "perguntas secretas" e "dicas" para recuperação de senhas, pois podem ser exploradas por invasores.

Cartões

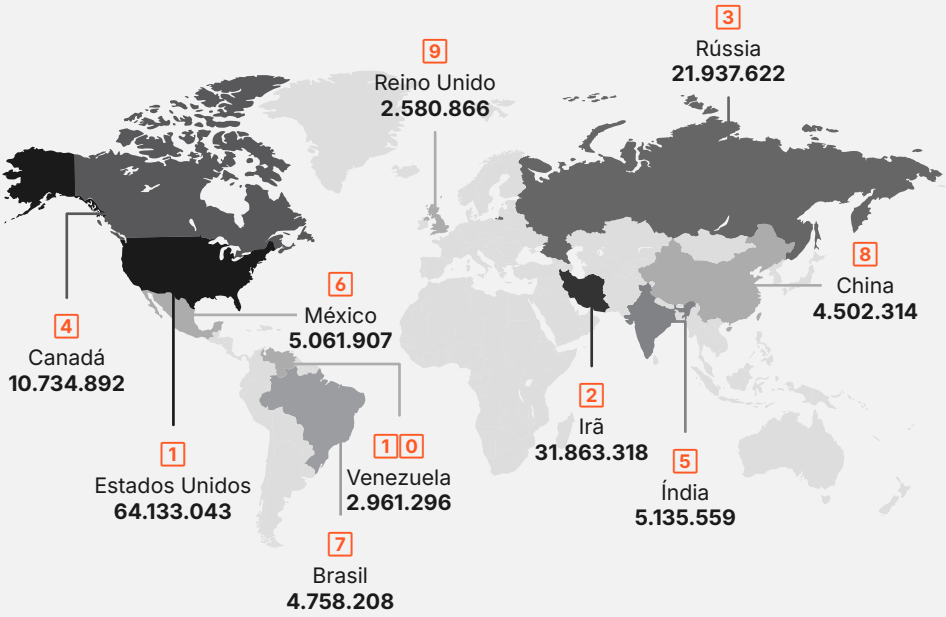
Criminosos compartilharam 339 milhões de cartões de crédito e débito em 2024

Crescimento de cartões expostos

2023	**13.5 milhões**
2024	**339 milhões**

O volume de cartões roubados permanece alto. Graças ao BIN (Bank Identification Number) dos cartões, é possível estimar a origem de cada cartão vazado.

Os de cartões americanos, com alto potencial aquisitivo, ainda aparecem na primeira posição desta lista. BINs de bancos brasileiros foram identificados em 4,7 milhões de cartões.



O roubo de cartões atinge as instituições financeiras e o comércio eletrônico, que muitas vezes absorve o prejuízo referente a produtos e serviços adquiridos com cartões roubados.

A Axur monitora esses vazamentos para ajudar as empresas a bloquear o uso desses cartões.

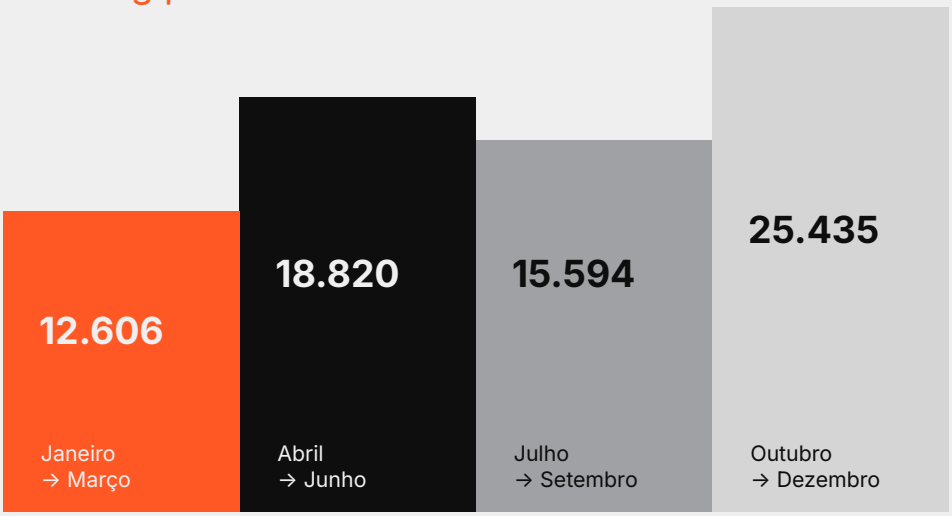
Phishing

O volume de páginas de phishing detectadas dobrou em 2024, chegando a 72.455

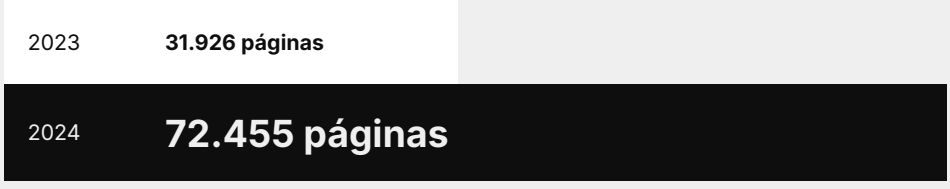
Detectar páginas de phishing é uma etapa crucial no combate a fraudes online. O monitoramento da Axur se concentra em detectar páginas em que as vítimas podem ser levadas a fornecer informações sensíveis. Esse enfoque é especialmente relevante no ambiente mobile, em que golpes frequentemente exploram marcas conhecidas por meio de publicidade em aplicativos ou SMS.

Nesse cenário, identificar e eliminar essas páginas é essencial para mitigar riscos e proteger os consumidores em um espaço que concentra grande parte das atividades de consumo e operações financeiras.

Phishing por trimestre



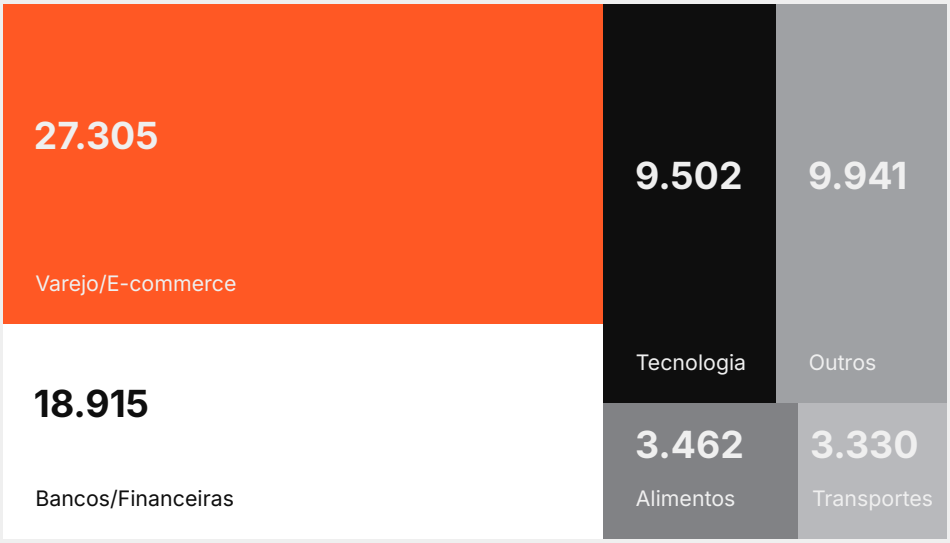
O crescimento das páginas de phishing



O setor de varejo e e-commerce continua sendo o mais atingido por ataques de phishing, seguido pelas instituições financeiras. Golpistas podem usar contas roubadas para realizar compras fraudulentas ou roubar informações pessoais.

Além disso, marcas de varejo são frequentemente utilizadas como veículo para roubar cartões de crédito, que podem ser usados para adquirir qualquer produto ou serviço.

Phishing por setor



70% dos golpes de phishing não usam uma palavra-chave no domínio

18% não trazem a palavra-chave no código HTML da página

Como LLMs estão redefinindo a detecção de ameaças

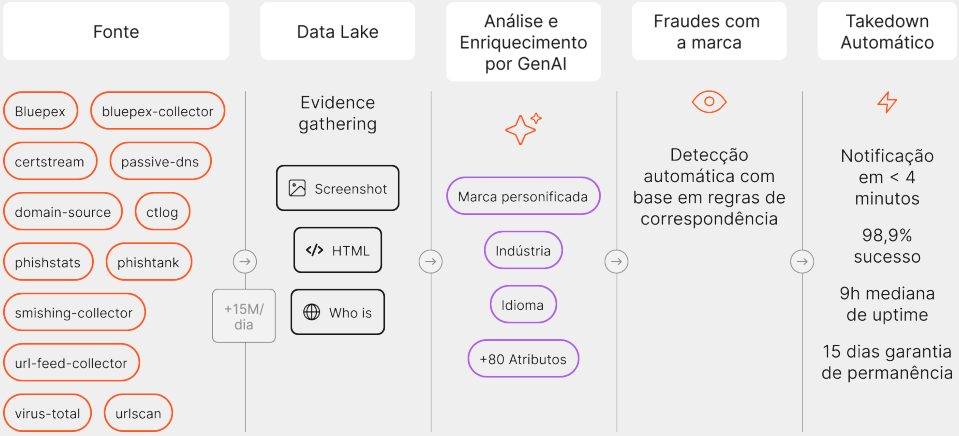
A Axur deu um passo à frente na identificação de ameaças digitais com a criação do Clair LLM (Cyber Lens for Anomaly and Impersonation Recognition), um modelo proprietário baseado em IA generativa. Diferente das soluções tradicionais, o Clair utiliza Vision Language Models (VLMs), desenvolvidos internamente e treinados com mais de 15 anos de dados e expertise em detecção de conteúdo fraudulento. Essa abordagem combina análise textual e visual para inspecionar diariamente mais de 15 milhões de sites, ampliando a capacidade de detectar fraudes sofisticadas.

O modelo processa URLs, avaliando o conteúdo das páginas e gerando descrições detalhadas. Ele identifica marcas presentes, detecta solicitações de credenciais, pagamentos ou senhas, e avalia se há tentativa de personificação de uma marca específica.

Tudo isso ocorre automaticamente, sem necessidade de intervenção humana. Essa precisão é resultado direto da integração de dados enriquecidos e análises detalhadas, que vão além da simples detecção por palavras-chave.

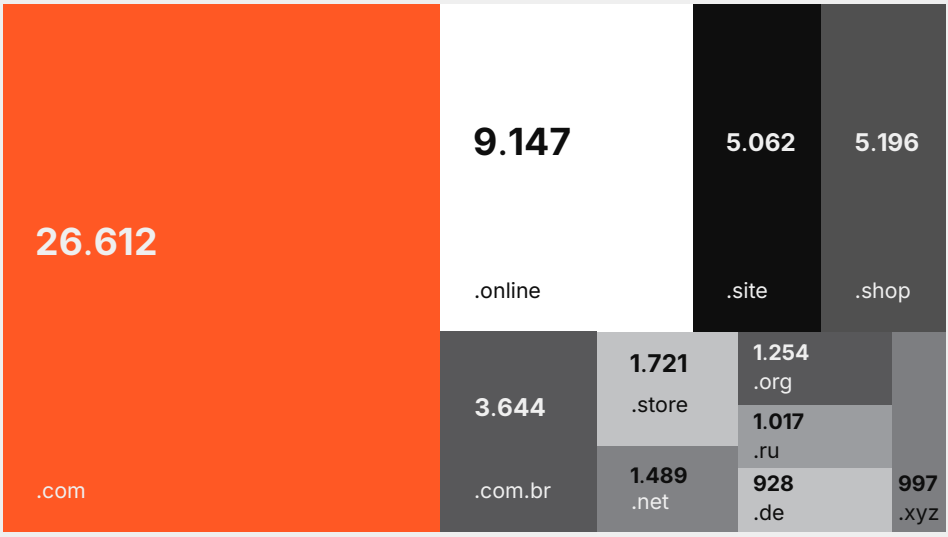
O uso de modelos proprietários também garante que todos os dados processados permaneçam dentro da infraestrutura da Axur, assegurando privacidade sobre as informações analisadas. Com a ferramenta de Threat Hunting, as equipes de cibersegurança e antifraude utilizam o mecanismo do modelo Clair para investigar campanhas de phishing de forma aprofundada, aplicando filtros personalizados que ampliam a visibilidade sobre os ataques, tudo sem comprometer a eficiência das detecções automatizadas.

Uma abordagem totalmente nova em proteção de marca



Uso de domínios de primeiro nível

Em 2024, observamos uma predominância de DPNs como "online". Além disso, o uso de ".shop" e ".store", são associados aos golpes de phishing que visam o comércio e varejo.



Os domínios de primeiro nível (DPNs) são os sufixos dos endereços da web, como ".com" (que pode ser usado por qualquer pessoa ou organização), ".gov" (exclusivo de sites do governo dos Estados Unidos) e ".uk" (sufixo de país).

A concessão de DPNs era bastante restrita no passado, já que apenas algumas poucas instituições eram autorizadas a operá-los – normalmente para representar regiões ou países (como ".br", ".de", ".jp," ".ar", entre outros).

Desde 2012, há um procedimento para solicitar uma concessão para um generic top-level domain (gTLD), flexibilizando a criação de novos sufixos. Cada DPN é operado por uma mantenedora (registry), que pode optar por vender subdomínios para recuperar o custo da infraestrutura e do pedido.

Como o procedimento para solicitar um gTLD é caro e bastante burocrático, cibercriminosos precisam escolher um dos DPNs existentes para registrar um domínio que sirva para aumentar o alcance de uma fraude ou deixá-la mais convincente.

Essa escolha é especialmente importante para sites de phishing, já que o endereço da página provavelmente será conferido pelas vítimas.

Para fazer esta escolha, o golpista normalmente considera alguns elementos:

→ Familiaridade da vítima com o domínio

A maioria dos usuários de internet está acostumada a visitar sites terminados em ".com". No entanto, os sufixos mais populares também são aqueles em que normalmente há poucas opções ainda disponíveis.

→ Disponibilidade do domínio

Como os endereços curtos, palavras simples e marcas comerciais não estão mais disponíveis em DPNs tradicionais, os criminosos podem tentar encontrar esses endereços em DPNs genéricos mais recentes ou em alternativas similares.

→ Vínculo com a fraude

Muitos sufixos dos gTLDs são temáticos. Um criminoso pode entender que algum deles deixará a fraude mais convincente.

→ Custo

Alguns DPNs são mais caros do que outros. Em casos como ".edu" e ".gov", que não podem ser registrados, a única opção do cibercriminoso é invadir um site com esses sufixos para hospedar a fraude.

→ Normas da registradora e combate a fraudes

Existem regras que todas as registradoras de domínio devem seguir. No entanto, pode haver diferenças no tratamento de casos específicos que motivem uma preferência por parte dos criminosos, já que isso afeta o tempo que a fraude poderá permanecer no ar.

Análise de DPNs		
DPN	2023	2024
.com	32,9%	36,65% ↑
.online	19,6%	12,6% ↓
.shop	16,9%	7,16% ↓
.site	7,3%	6,97% ↓
.com.br	5,6%	5,02% ↓
.store	5,1%	2,37% ↓

Takedowns realizados

401 mil casos de conteúdo fraudulento foram removidos graças às notificações da Axur

Com o phishing cada vez mais sofisticado e explorando novos canais, como SMS e publicidade em aplicativos, o tempo de resposta para remover conteúdo malicioso se torna um fator crítico.

A identificação de uma página de phishing é apenas o primeiro passo para mitigar os riscos – uma notificação rápida e bem estruturada para remoção é essencial para reduzir o tempo de exposição ao golpe.

Em 2024, foram realizadas mais de 401 mil takedowns através das notificações da Axur, cada uma direcionada aos provedores de infraestrutura, redes sociais ou serviços de hospedagem utilizados pelos criminosos.

Essa escala foi possível graças a um processo altamente automatizado e apoiado por inteligência artificial, que não só acelera o envio das notificações, mas também reúne as evidências necessárias para garantir uma maior taxa de sucesso.

A eficácia das solicitações depende de uma abordagem técnica e precisa: é preciso identificar o provedor correto, apresentar provas claras e respeitar os formatos exigidos. No entanto, mesmo com processos automatizados, o sucesso também está atrelado à credibilidade construída ao longo de anos, o que aumenta a confiabilidade das notificações e reduz atrasos no cumprimento.

Além disso, durante o intervalo entre a notificação e a remoção, medidas proativas como alertas para navegadores e provedores de segurança ajudam a limitar o impacto da fraude, protegendo potenciais vítimas. Esse conjunto de estratégias é decisivo para garantir uma taxa de sucesso alta nas solicitações realizadas.

Takedowns da Axur

401 mil	98.9%	4 min	9h
remoções realizadas	taxa de sucesso	mediana até a primeira notificação	mediana de resolução

Detecte, analise e remova as ameaças mais rápido que nunca

- Takedowns com um clique ou 100% automáticos
- Notificação em <4min
- 98,9% de sucesso
- 9h mediana de uptime
- Garantia de permanência de 15 dias
- Web Safe Reporting
- Acompanhe todo o processo
- Pague só por takedowns bem-sucedidos

Takedowns por setor

Em 2024, o setor financeiro liderou com 29,8% dos casos, resultando em mais de 107 mil notificações. Telecomunicações e varejo/e-commerce representaram, juntos, 42% dos incidentes, totalizando cerca de 154 mil incidentes removidos, entre páginas falsas, perfis, aplicativos ilegítimos e outros usos fraudulentos de marca.

Setores como turismo e o setor público também enfrentaram desafios, com mais de 100 mil fraudes neutralizadas.

Deep & Dark Web

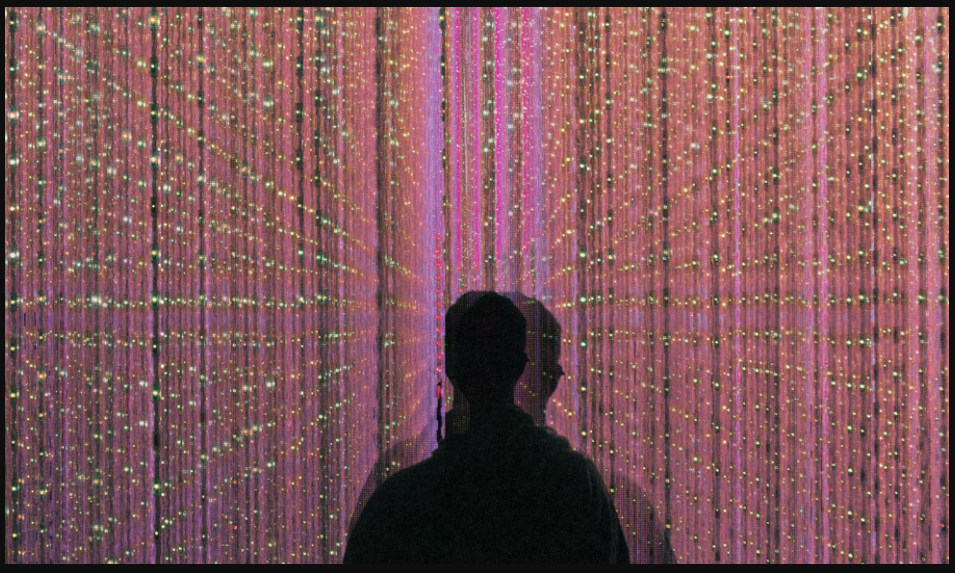
Analisamos 2,3 bilhões de mensagens em ambientes da Deep & Dark Web para prover inteligência em ciberameaças e incidentes

O cibercrime é hoje um ecossistema complexo que essencialmente conecta todos os indivíduos e grupos envolvidos em ataques cibernéticos. Esses canais de comunicação existem para que o crime seja mais ágil e maximize os lucros ilícitos da atividade.

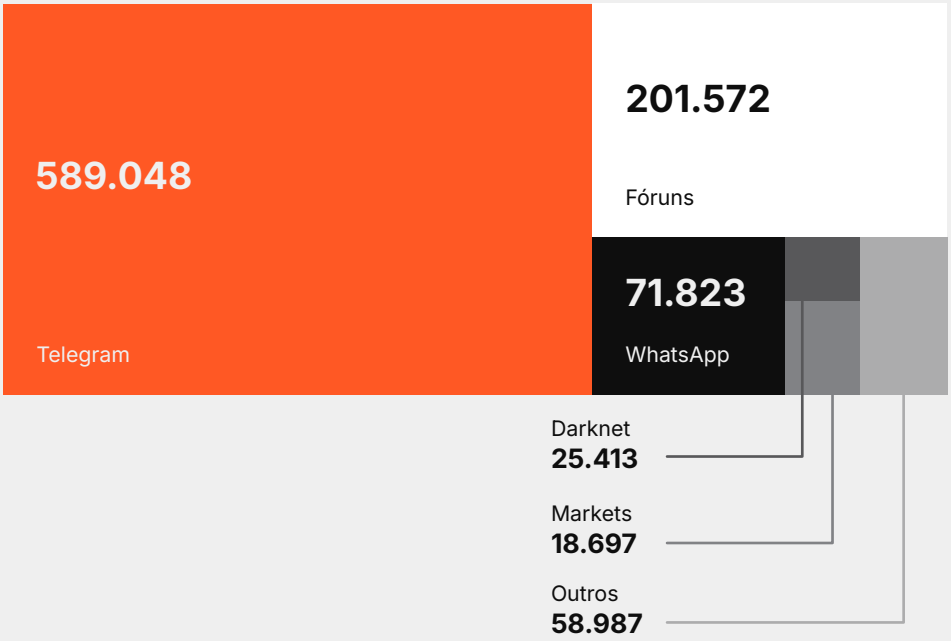
No entanto, esses espaços na Deep & Dark Web abrem uma oportunidade para coletar inteligência e acompanhar os movimentos de cada ator.

A Axur tem acesso a vários desses espaços e monitora as comunicações dos criminosos para identificar comentários que podem indicar a existência de um incidente de exposição de dados, de uma vulnerabilidade ou de uma campanha de fraude.

Convertemos a análise das mensagens em 966.170 incidentes — a chave para extrair inteligência é a filtragem e a interpretação do material coletado em alertas



Fontes de Deep & Dark Web



Tipos de detecção

Setores mais afetados

Setores	2023	2024
Varejo	45%	18% ↓
Financeiro	26,1%	25% ↓
Tecnologia	16,8%	44% ↑
Telecomunicações	4,8%	5% ↑
Turismo	3,6%	2% ↓
Outros	3,7%	6% ↑

Conteúdo audiovisual

Em 2023, cerca de 25% dos incidentes na Deep & Dark Web foram detectados em conteúdo audiovisual. Esta análise de material audiovisual com o auxílio de inteligência artificial para transcrever áudio e converter imagens em texto foi ainda mais relevante em 2024, representando um terço da comunicação analisada.

68%

Texto

32%

Áudio, vídeo e imagem

Perfis falsos, aplicativos ilegítimos e o uso fraudulento de marca

Detectamos quase meio milhão de fraudes digitais com estratégias sofisticadas para enganar consumidores

Em 2024, a Axur identificou mais de 439 mil casos de fraudes digitais, incluindo perfis falsos, aplicativos ilegítimos, uso de marca em busca paga, nomes de domínio similares ao original e outras associações indevidas. Esses incidentes refletem estratégias diversas usadas por criminosos para enganar consumidores e comprometer a reputação de empresas.

151.119 perfis falsos em plataformas de redes sociais

262.575 casos de uso fraudulento de marca

20.934 aplicativos mobile ilegítimos

Perfis falsos em redes sociais, somando 151 mil casos, são frequentemente usados para divulgar páginas de phishing ou enganar seguidores de perfis legítimos, solicitando informações sensíveis ou pagamentos fraudulentos.

Dos perfis falsos notificados pela Axur em 2024, **mais de 80%** foram removidos em parceria com a Meta Ads, responsável por Facebook e Instagram, totalizando mais de 57 mil takedowns através dos fluxos automatizados da Axur.

Com as mudanças de Mark Zuckerberg sobre a política de moderação das redes, será essencial acompanhar os impactos nas remoções futuras.

Saiba mais ↗

Já os 20 mil aplicativos ilegítimos detectados se aproveitam do ambiente mobile, exigindo interações adicionais após a instalação, como a concessão de permissões para acessar dados ou monitorar atividades do dispositivo, ampliando o alcance e o impacto dos golpes.

Executivos & VIPs

Executivos são frequentemente os principais alvos de golpes digitais devido à sua posição de influência e acesso a informações sensíveis. Criminosos utilizam engenharia social para explorar suas redes de contatos, seja por meio de perfis falsos em redes sociais, seja por tentativas de enganar colaboradores e parceiros.

Essas fraudes visam coletar informações confidenciais, como credenciais de acesso, cartões corporativos e dados estratégicos, que podem ser usados em ataques direcionados.

→ Uso indevido de imagem: softwares de edição de imagem sempre permitiram a sobreposição de rostos em imagens. Porém, a facilidade de alcançar uma grande audiência através da publicidade barata na web acaba viabilizando a exploração sistemática da imagem de personalidades famosas.

Os deep fakes produzidos com inteligência artificial ampliaram as fórmulas disponíveis para esse tipo de atividade.

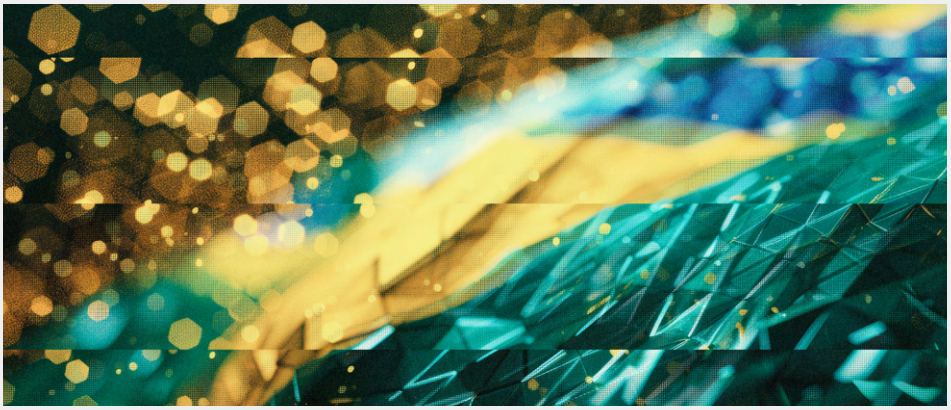
Esse uso indevido da imagem e semelhança de personalidades famosas pode ser usado para atingir as empresas em golpes de phishing, mas também pode ser usado apenas para divulgar produtos e serviços de forma irregular, gerando uma associação indevida de um indivíduo com um fato ou produto e enganando consumidores.

→ Dados confidenciais: outro risco crítico é a exposição de dados confidenciais, como credenciais corporativas e informações de cartões de crédito, frequentemente encontrados em vazamentos na deep e dark web.

Esses dados podem ser usados para acessar sistemas internos, realizar transações financeiras ou planejar ataques direcionados.

Detectamos mais de 33 mil incidentes com Executivos & VIPS

Cibercrime no Brasil



O cibercrime brasileiro é bastante focado na realização de fraudes digitais e no roubo de dados financeiros como senhas bancárias e cartões de crédito. Por esta razão, as ações dos criminosos brasileiros nem sempre seguem as mesmas tendências encontradas em outros países, que enfrentam ameaças mais associadas à Ásia e aos países do Leste Europeu.

Por conta desse foco em fraudes, o cibercrime brasileiro tende a apostar em táticas que miram nos consumidores, principalmente phishing e malware bancário.

Infelizmente, isso não significa que as empresas possam ignorar essas ameaças. A ofensiva aos consumidores em geral se aproveita das marcas conhecidas por eles.

Dependendo de como o golpe ocorre, o consumidor pode exigir que a empresa se responsabilize pelo prejuízo – ou, no caso de varejistas, o problema pode aparecer em chargebacks de compras com cartão de crédito.

Criminosos preparam pacotes de dados pessoais – que eles chamam de "kits bico" – que podem ser usados para fraudar os processos de validação de identidade para abertura de conta ou empréstimo, permitindo que o golpista engane as instituições.

Além disso, assim como mencionamos em nosso relatório do ano passado, existem várias evidências de criminosos buscando recrutar colaboradores internos das empresas para conseguir acesso à rede interna. Nesse cenário, um colaborador é subornado pelo criminoso para instalar programas de administração remota (como AnyDesk ou Supremo) ou introduzir outro tipo de mecanismo que funcione como porta de entrada para a rede corporativa.

Esse tipo de invasão não ocorre na mesma escala do que as fraudes digitais, mas é uma preocupação crescente que deve ser monitorada pelas empresas.

Phishing

Com o uso crescente de aplicativos e serviços mobile, o cibercrime brasileiro precisou se adaptar à nova realidade. O phishing por e-mail começou a dar lugar ao SMS, a chats de WhatsApp ou a publicidade direcionada para dispositivos mobile.

Em 2024, essas práticas têm se intensificado e apostado em uma estratégia que às vezes mistura diferentes marcas para realizar a fraude, o que cria desafios para a detecção do phishing.

O esquema normalmente começa com um anúncio publicitário que divulga um link para uma reportagem jornalística falsa hospedada em um site muito semelhante ao de algum veículo de imprensa. Dessa forma, a primeira marca com a qual a vítima tem contato não é necessariamente aquela que será prejudicada pela fraude.

A reportagem falsa é utilizada para divulgar outro site falso ou um aplicativo – alguns deles disponíveis em repositórios oficiais. Esse aplicativo pode utilizar diversos pretextos (uma liquidação, resgate de pontos em cartões etc.) para solicitar os dados da vítima ou pedir permissões para monitorar o uso do aparelho e usar a sobreposição de janelas.

Esse modus operandi permite que o phishing brasileiro continue explorando narrativas diversas, seja para dificultar o bloqueio das fraudes por parte das marcas ou para contornar as restrições impostas por operadoras e plataformas ao envio de SMS e à publicidade que disseminam as fraudes.

A Axur está disponibilizando o Threat Hunting e análises de Inteligência Artificial para detectar golpes de phishing através de indícios contextuais. A IA reconhece quando uma página solicita dados de cartões, pagamentos ou senhas, e associa esses sinais à probabilidade de que a página está imitando características visuais de uma marca, permitindo detectar o phishing em escala.

Malware bancário

Os cavalos de Tróia que roubam credenciais de bancos e cartões de crédito são as primeiras ferramentas do cibercrime brasileiro. Em 2024, foram identificadas algumas evoluções e malwares novos.

Um comportamento que merece ser acompanhado é a inclusão de funcionalidades para interferir com transferências Pix em outros malwares, como o CryptoClippy.

Como o nome sugere, este é um malware que surgiu para atuar em fraudes com criptomoeda, mas as versões que circulam no Brasil podem redirecionar transferências Pix na modalidade "Copia e Cola".

Para interferir com essa modalidade de Pix, o malware só precisa monitorar a área de transferência do sistema (clipboard). Isso é algo relativamente simples de ser feito, mesmo em malwares que teriam outros alvos, como cartões de crédito ou criptomoedas.

Outro malware que chamou atenção foi o CarnavalHeist, também chamado de AllaSenha. Este malware foi programado em Delphi e Python, como é comum no Brasil, mas utiliza um algoritmo de geração de domínio (Domain Generation Algorithm — DGA), gerando domínios diferentes todos os dias para que o malware baixe seus demais componentes e acesse seu servidor de comando e controle (C2).

O AllaSenha começou a ser disseminado em fevereiro de 2024 e é considerado um malware novo. Contudo, ele foi baseado em outro malware mais antigo chamado AllaKore.

Por fim, o "Coyote", que também é um malware para Windows, se destacou por utilizar linguagens de programação consideradas mais modernas, como o .NET e Node.js, além de uma linguagem relativamente nova chamada Nim – distanciando-se das linguagens mais comuns no cibercrime brasileiro, como o já mencionado Delphi.

O Coyote monitora o endereço dos sites visitados para roubar credenciais de 60 alvos.

O trojan "Rocinante"

Detectado em agosto, o malware "Rocinante" combina várias das principais estratégias que estão se consolidando no cibercrime brasileiro.

1 É distribuído por meio de phishing

2 É um malware para Android que usa janelas sobrepostas e solicita permissões de acessibilidade para ter acesso ao conteúdo da tela do aparelho

3 É disseminado por meio de narrativas diversas. Ele pode ser disfarçado de "Módulo de Segurança" de um banco, um aplicativo de resgate de pontos de cartão de crédito ou até um serviço de recarga de celular.

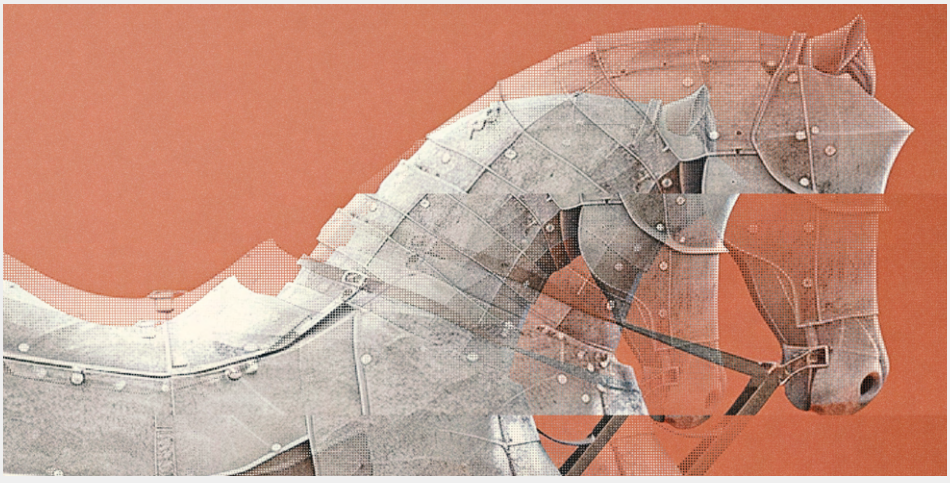
4 É uma fraude completa, uma vez que a narrativa do golpe será continuada após o malware ser instalado no smartphone com a solicitação de credenciais ou dados da vítima.

5 É capaz de monitorar o acesso a determinados sites, se a permissão de acessibilidade for concedida.

A estratégia do Rocinante permite que o criminoso concretize a fraude em um ambiente mais isolado e controlado do que um phishing tradicional, em que a página maliciosa estaria disponível na web.

O Rocinante ilustra os desafios no combate ao phishing. Os clientes das empresas podem ser atingidos por uma fraude equivalente ao phishing – com a solicitação com dados do usuário – sem a existência dos artefatos tradicionais do phishing (uma página clonada).

Empresas brasileiras preocupadas com o phishing precisam monitorar também os aplicativos maliciosos que podem estar realizando fraudes contra seus clientes. Do contrário, não será possível manter a visibilidade sobre as fraudes que envolvem sua marca.



O que estamos investigando

→ Ações externas

Grupos estrangeiros também tiveram uma atuação relevante no Brasil, com destaque para o ransomware Qiulong (Qilin, Agenda) e RansomHub. Os operadores de ransomware em geral são vinculados à Rússia ou a outros países do Leste Europeu, mas o modelo de ransomware-como-serviço (RaaS) permite que esses grupos tenham afiliados de outros locais do mundo. Por este motivo, seguimos acompanhando as ações desses grupos e o risco que eles representam para as empresas brasileiras.

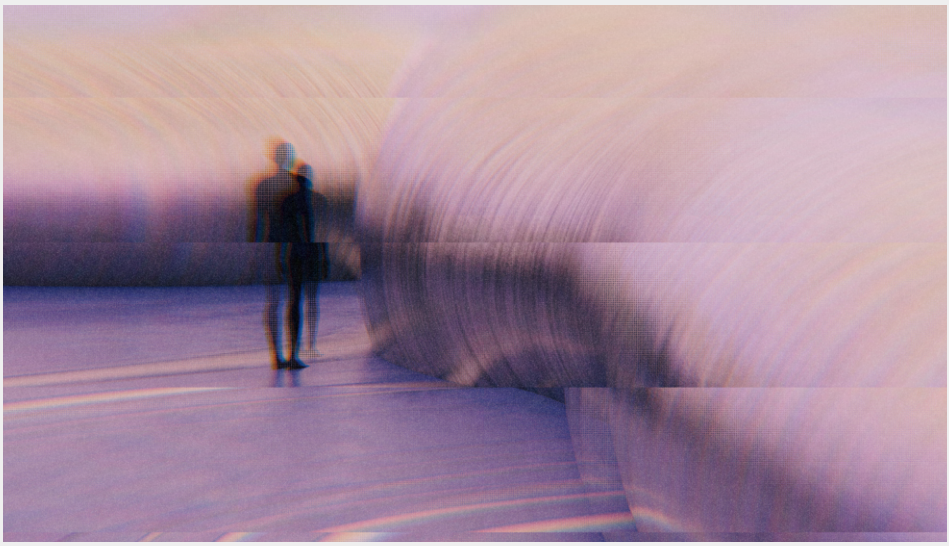
→ Ataques de negação de serviço

Investigamos alguns incidentes notáveis em que entidades brasileiras foram alvo de ataques de negação de serviço para desestabilizar a infraestrutura de TI. Em alguns dos incidentes, nenhum grupo reivindicou o ataque. Contudo, também estamos trabalhando com a hipótese de que grupos hacktivistas supostamente ligados aos conflitos no Oriente Médio tenham ligação com brasileiros ou membros no Brasil, o que explicaria os alvos desses grupos em território brasileiro.

→ Novos canais de comunicação

No ano passado, comentamos que o número de criminosos usando o WhatsApp estava crescendo e levantamos a hipótese de que isso era resultado da entrada de novos golpistas menos experientes. Agora, uma nova migração pode estar levando os criminosos que usam o Telegram para o Signal. Esse movimento é possivelmente motivado pela cooperação do Telegram com autoridades policiais.

Tendênciαs



↗ Inteligência Artificial (ainda) no centro das тendências

↗ Ransoмware: novos grupos e regulações

↗ Novas forмas de autenтicação e adaptação dos aтacantes

↗ Phisнing em novas fronteiras, com aтaques mais sofisticados

↗ Ciвersegurança
☒ Segurança Nacional

↗ Expansão das Superfícies de Aтaque

Inteligência Artificial (ainda) no centro das tendências

O potencial da IA generativa já está se consolidando tanto na defesa das redes corporativas – em produtos de Cyber Threat Intelligence – como em fraudes digitais que usam deep fakes e conteúdo personalizado para as vítimas. Contudo, a GenAI não é a única forma de fazer uso dos algoritmos de Deep Learning. Por este motivo, a Inteligência Artificial continua sendo uma fonte de surpresas e, por isso, deve ser acompanhada de perto. Já temos as primeiras soluções de cibersegurança que empregam o poder da IA para gerar interpretações analíticas, e é possível que essa mesma capacidade seja aproveitada por criminosos para criar algum mercado para a curadoria de dados vazados.

No mínimo, podemos ter a certeza de que os algoritmos de GenAI serão aprimorados – facilitando as fraudes que se aproveitam de identidades falsas – e que vulnerabilidades venham a ser encontradas nas próprias plataformas de IA, a exemplo da vulnerabilidade descoberta por analistas da Wiz que permitia executar comandos e acessar dados de outros clientes de uma plataforma de "IA como serviço".

Ransomware: novos grupos e regulações

Operações da polícia e conflitos internos causaram um impacto considerável nas operações dos grupos de ransomware LockBit e BlackCat em 2024. No entanto, outras organizações criminosas rapidamente conseguiram ocupar o vácuo deixado por esses grupos, evidenciando a resiliência do modelo de "ransomware como serviço" e o interesse considerável dos golpistas em insistir nesse modelo de fraude.

Autoridades já avaliam há algum tempo a possibilidade de impor regras para dificultar ou proibir o pagamento dos resgates e, desde a metade de 2024, há também uma pressão para que seguradoras deixem de cobrir os pagamentos.

O entendimento de alguns analistas é de que o pagamento do resgate incentiva os criminosos e, por isso, seria preciso coibi-los

É importante que as empresas acompanhem esses desdobramentos para se manterem prontas para prevenir esses incidentes, recuperar sistemas e evitar surpresas com mudanças na apólice do seguro cibernético ou na legislação.

Novas formas de autenticação e adaptação dos atacantes

Enquanto muitas empresas ainda enfrentam dificuldade para adicionar um segundo fator de autenticação, a tecnologia já está dando o próximo passo com a adoção das passkeys. Porém, é difícil de imaginar que a busca por uma modalidade definitiva de autenticação esteja perto do fim.

De modo geral, novas modalidades de autenticação tendem a mitigar os ataques que estão em curso, obrigando os atacantes a se adaptarem. No entanto, os malwares do tipo infostealer, que vêm sendo utilizados com muito mais frequência desde a popularização do MFA, são muito mais versáteis do que o antigo phishing que roubava apenas usuário e senha – podendo inclusive roubar cookies e realizar o bypass do MFA. Sendo um ataque mais versátil, isso significa que a adaptação tende a ser mais rápida.

Por esses motivos, é muito provável que os hackers aprimorem os infostealers em 2025.

Além disso, é possível que certos canais de autenticação que têm sido explorados principalmente por agentes mais sofisticados (como OAuth e aplicações em nuvem) comecem a se popularizar entre atacantes menos qualificados.

Phishing em novas fronteiras, com ataques mais sofisticados

Muitos ataques têm sido construídos em torno de novas modalidades de phishing ou engenharia social – seja através de deep fakes com IA, ameaças físicas ou fraudes em publicidade em redes sociais. A evolução constante das narrativas dos golpes tem criado um desafio adicional para o esforço de conscientizar as pessoas sobre os riscos e os truques usados para enganar consumidores.

Por essa perspectiva, o phishing continua sendo uma tendência para 2025. O cenário tem se tornado ainda mais complexo.

Isso exige um monitoramento avançado, capaz de detectar o uso indevido da marca exclusivamente em imagens ou outros sinais sutis, ampliando a necessidade de ferramentas especializadas de combate a fraudes.

Lojas de e-commerce, instituições financeiras e prestadoras de serviços de tecnologia devem seguir como as principais marcas envolvidas nesses ataques.

Contudo, empresas de todos os segmentos estão cada vez mais sujeitas a ataques de phishing direcionados a seus colaboradores.

De uma forma ou de outra, esta ameaça continuará exigindo a atenção e a sofisticação das equipes de combate à fraude e segurança da informação.

Cibersegurança
Segurança Nacional

As tensões no cenário geopolítico vêm aproximando o tema de cibersegurança do conceito de segurança nacional. Em 2024, muitos legisladores demonstraram interesse em olhar para toda a cadeia de fornecedores de tecnologia e de olhar para as empresas que prestam esses serviços — a diretora da Agência de Cibersegurança e Infraestrutura dos Estados Unidos chegou a declarar que o problema da cibersegurança é um "problema da qualidade de software".

Como muitas organizações criam softwares ou soluções digitais personalizadas, é possível que o rigor técnico do processo de desenvolvimento e as medidas de segurança da informação se tornem um diferencial para o mercado nos próximos anos. Assim, uma postura robusta de cibersegurança pode se tornar uma vantagem comercial e um requisito para o fechamento de contratos.

Mesmo que isso não venha a se concretizar, o vínculo da cibersegurança com a geopolítica também traz outros tipos de preocupações, como a atuação de grupos de hacktivismo.

O posicionamento das empresas em meio a essas tensões e a visibilidade sobre os vazamentos de dados realizados por hacktivistas podem acabar se mostrando valiosos nessa questão. Entretanto, é preciso acompanhar o que virá a seguir – especialmente em regiões como a América Latina, onde o tema ainda não tem o mesmo destaque.

Expansão das Superfícies de Ataque

A proliferação de dispositivos IoT (Internet of Things) e a adoção de políticas de BYOD (Bring Your Own Device) expandem significativamente as superfícies de ataque das organizações. Cada dispositivo conectado, seja pessoal ou corporativo, pode se tornar um ponto de entrada vulnerável para ataques cibernéticos. Esse desafio é agravado pela falta de padrões de segurança consistentes em dispositivos IoT e pelo aumento de endpoints fora das redes corporativas tradicionais.

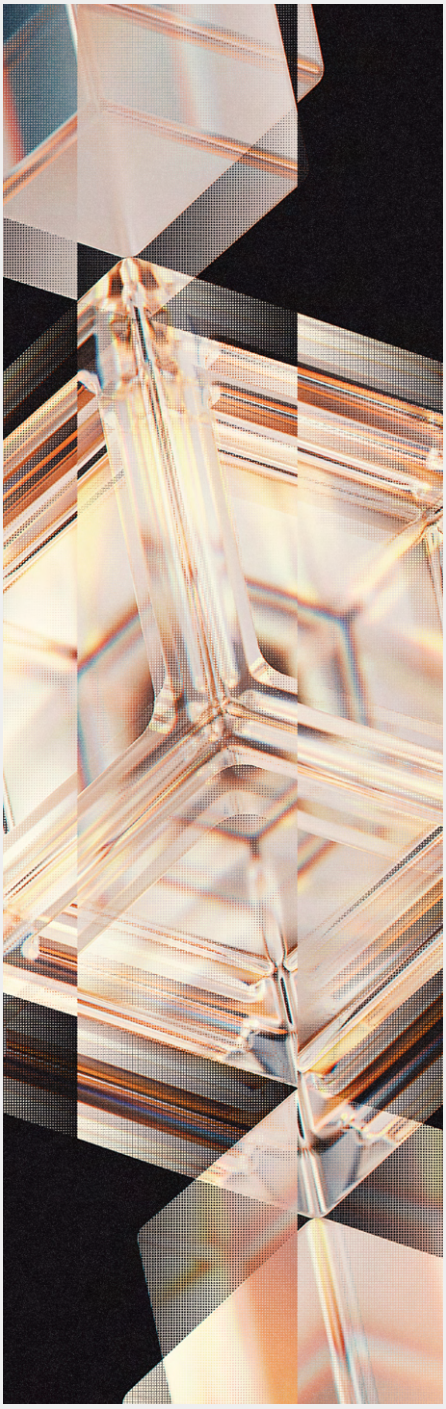
Será preciso adotar medidas robustas de segurança, como o gerenciamento centralizado de dispositivos, a segmentação de redes para isolar dispositivos menos seguros e a aplicação de patches e atualizações frequentes. Além disso, políticas claras de uso de dispositivos pessoais e soluções de monitoramento contínuo serão essenciais para identificar e responder rapidamente a possíveis atividades maliciosas.

Recomendações

Gestão de Identidades

A gestão inadequada de identidades e de credenciais se mostrou uma das principais fragilidades das empresas em 2024. Muitas organizações ainda estão tentando implementar a autenticação multifator em todos os pontos de acesso, mas a política de Identity and Access Management (IAM) já precisa olhar para aplicações em nuvem, chaves de APIs e outros mecanismos de acesso que muitas vezes são incompatíveis com as soluções voltadas às credenciais de usuários humanos. Pode não ser trivial migrar esses sistemas para outro paradigma de autenticação no curto prazo.

O monitoramento de credenciais vazadas é uma das ferramentas mais importantes para garantir que as empresas estejam sempre um passo à frente dos invasores e sejam capazes de bloquear credenciais antes que elas sejam usadas em ataques. É especialmente útil para complementar soluções baseadas em MFA ou proteger sistemas em fase de migração.



Gestão de vulnerabilidades

A exploração de vulnerabilidades ainda é um dos vetores de ataque mais comuns para acessar redes corporativas, indicando que existem deficiências na gestão de vulnerabilidades. A expansão da infraestrutura da TI e a descentralização de sua gestão para áreas específicas do negócio explicam uma parte dessa deficiência, mas a própria aplicação de patches pode ser ineficaz quando vulnerabilidades menos graves são corrigidas antes das mais urgentes. Por isso, empresas devem buscar novos métodos para ter visibilidade sobre sua infraestrutura de TI.

Uma solução que una External Attack Surface Management (EASM) com alertas de Inteligência Artificial permite que a empresa tome decisões a partir de insights de alta relevância sobre as vulnerabilidades mais críticas, aprimorando tanto a visibilidade como a priorização dos patches a serem aplicados.

Plano de Continuidade de Negócios

Quando a operação da empresa é inseparável de sua infraestrutura de TI, o impacto dos incidentes cibernéticos tende a ser maior. Já existem casos emblemáticos de empresas entrando em recuperação judicial ou encerrando suas atividades após ataques de grande magnitude.

Em 2024, por exemplo, a MediSecure entrou em voluntary administration, um processo australiano de reestruturação para empresas em dificuldades financeiras, após um ciberataque, e a National Public Data decretou falência depois do vazamento de 2,9 bilhões de registros. No ano anterior, a Rackspace precisou encerrar seu serviço de e-mail devido a um ataque de ransomware.

Esse cenário crítico está alinhado com a crescente preocupação das empresas: um levantamento recente da Hiscox Cyber Readiness Report aponta que nesse contexto, o Plano de Continuidade de Negócios é essencial para garantir que a organização mantenha sua resiliência em condições adversas. O processo de elaboração do plano por si só pode ser muito benéfico para a empresa, já que exige o mapeamento dos sistemas críticos.

É importante que a empresa avalie a sua dependência de terceiros e fornecedores, que também podem ser alvo de ataques – e o Threat Hunting da Axur, uma ferramenta com um banco de dados de mais de 42 bilhões de credenciais, é uma das maneiras de mapear esses riscos atrelados a plataformas e sistemas terceirizados.

35% das organizações consideram os ciberataques um dos cinco maiores riscos para seus negócios.

Combate ao phishing com monitoramento e takedown

Por ser um ataque muito versátil baseado em engenharia social, o phishing raramente enfrenta barreiras técnicas para ser adaptado a novos ambientes e paradigmas de trabalho. É uma ameaça que pode atingir clientes, fornecedores e colaboradores diretos.

Entender como o phishing impacta o negócio traz grandes benefícios para a empresa, uma vez que o combate a essa ameaça - em especial através de um Takedown ágil e assertivo - tende a reduzir a presença das marcas do negócio em uma grande gama de fraudes digitais. Como as credenciais e informações roubadas através do phishing representam um risco significativo à rede corporativa, a falta de visibilidade sobre esta ameaça muitas vezes traz complicações para a gestão de identidades.

Cultura de segurança

Normas são pouco eficazes quando as pessoas não enxergam seu valor. Nesse sentido, o provisionamento irregular de sistemas, criando uma "TI invisível", e falhas na gestão de identidades – mantendo válidas credenciais de terceiros ou colaboradores já desligados – são indícios comuns de que a empresa ainda precisa aprimorar sua cultura de segurança.

É mais fácil implementar uma política exitosa de segurança da informação quando colaboradores e tomadores de decisão estão cientes dos riscos e da importância de respeitar as diretrizes estabelecidas. Essa cultura pode ser sustentada por um programa de conscientização em segurança.

9 avanços da IA que estão redefinindo a detecção e resposta a ameaças

1 Sistemas autônomos de segurança: operações sem intervenção humana.

→ IA cria sistemas autônomos que detectam ameaças e corrigem vulnerabilidades em tempo real.

2 Análises comportamentais aprimoradas: monitoramento contínuo e aprendizagem.

→ IA detecta anomalias com base em padrões de comportamento, melhorando a precisão ao longo do tempo.

3 Inteligência de ameaças preditiva: previsão de ameaças futuras.

→ Algoritmos preveem ataques emergentes usando dados históricos, permitindo defesas proativas.

4 Automação e análise de dados: caça a ameaças eficiente.

→ IA automatiza a análise de logs e eventos, permitindo que equipes foquem em investigações complexas.

5 Integração de NPL: interações intuitivas.

→ IA facilita consultas em linguagem natural, tornando a análise de ameaças mais acessível.

6 Detecção avançada de anomalias: identificação de padrões sofisticados.

→ Deep learning detecta ameaças desconhecidas ou complexas que métodos tradicionais não identificam.

7 Resposta rápida a incidentes: mitigação automatizada.

→ IA reduz o tempo de resposta, contendo incidentes rapidamente para minimizar danos.

8 Colaboração com compartilhamento de inteligência: defesa coletiva.

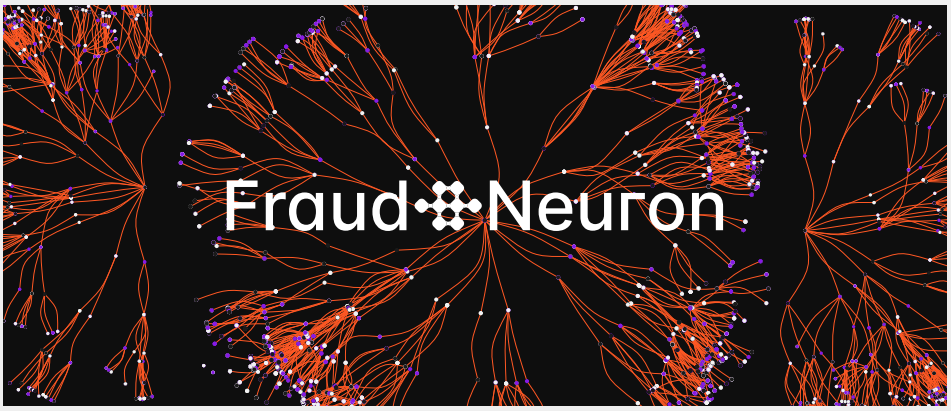
→ Sistemas de IA compartilham inteligência em tempo real, fortalecendo a segurança coletiva.

9 Foco em ameaças emergentes: identificação proativa.

→ IA rastreia sinais de ameaças em plataformas como redes sociais e fóruns na dark web.

Fraud Neuron

Framework de modelagem de fraudes



Para produzir inteligência em ameaças cibernéticas, elas precisam ser descritas, modeladas e categorizadas.

O framework ATT&CK, idealizado e mantido pela MITRE Corporation, é a metodologia mais consolidada para essa tarefa, descrevendo um número sempre crescente de Táticas, Técnicas e Procedimentos (TTPs) que podem ser usados pelos adversários.

Funciona como uma linguagem comum que os profissionais de cibersegurança usam para sintetizar e compreender a atuação de um invasor de forma rápida e efetiva, enfatizando as informações essenciais que um time de defesa precisa detectar ou prevenir uma ameaça.

Assim, o ATT&CK é praticamente um banco de dados e de inteligência sobre as estratégias usadas pelos atacantes.

O Fraud Neuron (F.N) da Axur visa cumprir o mesmo papel no campo das fraudes digitais, facilitando a troca de informações e criando uma linguagem comum para todos os profissionais da área.

Um framework de cibersegurança atento ao negócio

Com a categorização de táticas específicas das fraudes e dos impactos ao negócio, inclusive para ativos intangíveis como a marca, a reputação e o risco jurídico, o Fraud Neuron complementa outras abordagens de modelagem e oferece uma nova perspectiva para a compreensão do cibercrime.

As fraudes nos canais digitais combinam elementos comuns em ataques cibernéticos com atributos específicos da área de atuação da empresa, como o e-commerce ou serviços financeiros. Ao descrever a forma como essas associações ocorrem, o Fraud Neuron reduz a distância entre os times de cibersegurança e os times de combate a fraudes, facilitando o trabalho em conjunto.

Essa visão proposta pelo Fraud Neuron é especialmente valiosa para o mercado latino-americano, onde a ligação entre as fraudes digitais e as técnicas de ataque cibernético é mais forte.

Disponível para a comunidade

O Fraud Neuron foi desenvolvido a partir da experiência da Axur no combate a fraudes digitais e aberto para ser utilizado por toda a comunidade de cibersegurança.

A adoção ampla viabilizada por um framework aberto elimina barreiras para a troca de informações, permitindo que o Fraud Neuron possa se consolidar como uma linguagem conhecida por todos os profissionais para descrever as fraudes.

Nos canais do projeto, profissionais de qualquer organização podem enviar sugestões de melhorias e novas táticas que podem ser referenciadas no modelo.

A modelagem e categorização das fraudes pode ser utilizada também para reunir informações sobre diferentes grupos criminosos e facilitar análises quantitativas das fraudes (quais foram as técnicas mais comuns, por exemplo), além de servir como um banco de dados a respeito dos métodos usados pelos golpistas.

A inteligência gerada pela aplicação da metodologia do Fraud Neuron pode ser usada para priorizar mitigações, criar campanhas de conscientização e preparar novas organizações para as fraudes que mais impactam cada ramo de atividade.

Contribua
Fraud Neuron

github.com/axur/FraudNeuron

Os principais eixos do Fraud Neuron

→ Identificação do alvo
Tipo de alvo (indivíduo ou organização)

→ Temática
Categoria geral da fraude, incluindo o tema da engenharia social

→ Reconhecimento
Técnicas que podem ser usadas para coletar dados das vítimas

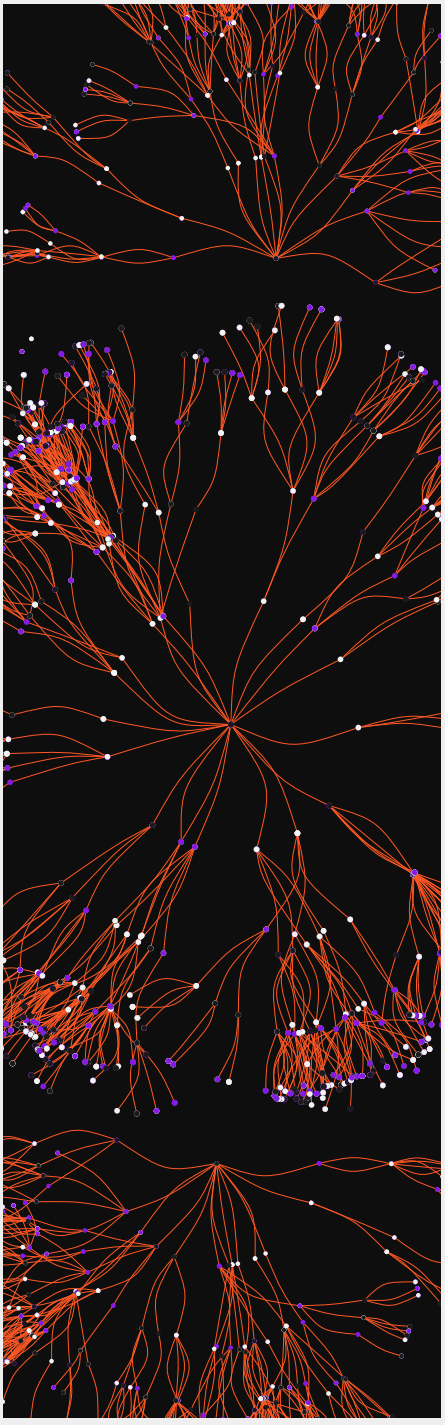
→ Recursos
Meios de comunicação, técnicas e ferramentas que compõem a infraestrutura digital do golpe

→ Simulação de identidade
Tipos de identidades que podem utilizadas indevidamente, incluindo marcas, funcionários e aplicativos

→ Engenharia Social
Detalhamento de como a engenharia social foi aplicada dentro da temática

→ Conversão
Técnicas para converter o ataque cibernético em vantagens financeiras ou outro benefício indevido

→ Impacto
Impactos que podem ser associados à fraude, tanto para a infraestrutura de TI ou para o negócio



Segurança no topo

Lições de nossos clientes e convidados para 2025




Em 2025, o Threat Landscape da Axur traz uma seção inédita e especial: um espaço dedicado às histórias, insights e aprendizados compartilhados por clientes e também por convidados que, ao longo do ano, participaram do podcast Axur Talks.

Tatiana Mota,
Cybersecurity Manager na Bayer

Riscos na cadeia de suprimentos

"A integração entre saúde e química amplia a superfície de ataque, exigindo maior controle sobre privacidade e qualidade."

Marcelo Amaral,
CISO no Banco Safra

Riscos e transformações no mercado financeiro

"Iniciativas como PIX e Open Finance elevaram a maturidade de segurança no Brasil, mas também aumentaram a exposição a ataques devido ao valor dos dados envolvidos."

Renã Melo,
CISO e DPO do Grupo Carrefour

Criatividade no cibercrime brasileiro

"O crime cibernético no Brasil é extremamente criativo e organizado, destacando casos únicos como a 'gangue do boleto'."

Fabio Luz,
CISO na Bemol

Inovação com IA em segurança

"A IA tornou ataques mais convincentes e difíceis de identificar, exigindo maior sofisticação das defesas."

Leandro Ribeiro,
CISO no Hospital Sírio-Libanês

Cibersegurança: valor estratégico para o C-Level

"O maior desafio para os CISOs é provar o valor da segurança para o C-Level, indo além do ROI e focando na mitigação de riscos e prevenção de fraudes."

Acompanhe insights e discussões de alto nível de grandes líderes em cibersegurança no Axur Talks.

Ouça no Spotify

Assista no Youtube

Uma visão de cibersegurança em 2024 e expectativas para 2025

A visão estratégica em um cenário desafiador de cibersegurança

Rafael Tonelotti
Diretor de Operações de Segurança na Americanas S.A

O cenário de cibersegurança em 2024 foi marcado por desafios crescentes, com ataques sofisticados como ransomware, phishing e exploração de vulnerabilidades em IoT, supply chain e APIs. A migração para a nuvem redirecionou ataques para identidades, exigindo estratégias adaptadas. As regulamentações globais e a busca por equilíbrio entre segurança e experiência do usuário também foram desafios significativos.

Para 2025, espera-se a intensificação de ataques baseados em IA, deepfakes para fraudes e espionagem, vulnerabilidades em APIs e dispositivos IoT/OT, além de ameaças à cadeia de suprimentos digitais e desafios na transição para criptografia quântica. Esses fatores demandam investimentos em profissionais, tecnologias avançadas, conscientização e parcerias estratégicas para aumentar a resiliência organizacional.

Colaboração estratégica para enfrentar ameaças emergentes

Luiz Borsatti
Especialista de cibersegurança na Electrolux Latam

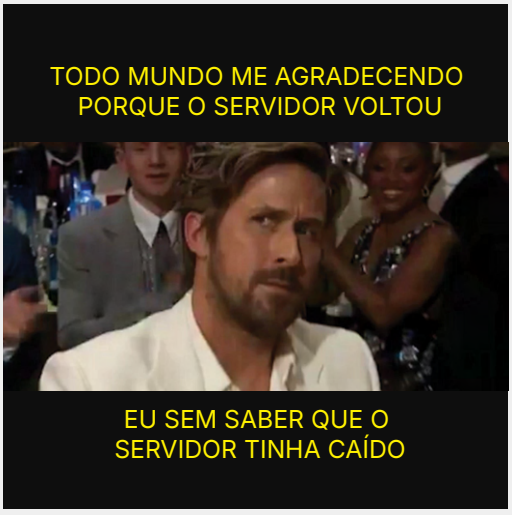
A segurança da informação enfrentou grandes desafios em 2024, com métodos cada vez mais sofisticados. Atacantes têm usado IA para aperfeiçoar a linguagem, eliminando erros e dificultando a identificação de ameaças. Para 2025, os desafios devem se intensificar, com técnicas ainda mais avançadas sendo empregadas. No entanto, também cabe a nós explorar o potencial da IA e do machine learning para prever e mitigar ameaças de forma mais eficaz.

Nesse cenário, a parceria com a Axur tem sido essencial, acelerando a identificação de ameaças com soluções rápidas e eficazes, além de minimizar a possibilidade de fraudes online. Essa colaboração fortalece nossa proteção, garantindo mais segurança para nossos clientes e maior resiliência para a equipe diante de ameaças em constante evolução.

Iniciativas conectadas para reforçar a cultura de cibersegurança

Você pode acompanhar os insights de grandes líderes em cibersegurança e participar de discussões de alto nível em nossa Threat Intel Community no WhatsApp.

Entrar na Community



Além de, claro, receber bons memes e figurinhas eventualmente, como aconteceu na campanha do CyberMeme, durante o mês de consciência em cibersegurança, em outubro.

Sobre a Axur

A Axur é uma solução líder em cibersegurança externa que empodera equipes de segurança para tratar ameaças fora do perímetro. Nossa plataforma detecta, inspeciona e responde a fraudes digitais, phishing, menções na deep & dark web, vulnerabilidades e mais.

Com fluxos automatizados e o melhor takedown do mercado, a Axur remove conteúdo malicioso de forma rápida e eficiente, 24×7, gerenciando 86% das detecções sem toque humano. Nossas soluções utilizam Inteligência Artificial para escalar a inteligência de ameaças 180 vezes, liberando a sua equipe para se concentrar nas iniciativas mais estratégicas.

O que os times de segurança falam de nós

Gartner Peer Insights™ 5/5

★★★★★

Explorando a poderosa parceria com a Axur

A Axur é nossa melhor parceria! Sempre que preciso de ajuda ou tenho dúvidas, eu os aciono e eles resolvem.

Gestor de Segurança da Informação e Riscos

★★★★★

Console intuitivo para configuração eficiente de alertas

Velocidade para identificar ameaças e relatá-las ao cliente, com implantação rápida e fácil.

Gerente de Tecnologia

Descubra como nossas soluções irão transformar sua estratégia de segurança

Faça uma demo

///AXUR

Digital experiences made safe

www.axur.com