
THREAT LANDSCAPE
2025 → 2026
AXUR

Sumário

Mensagem da Axur

Em 2025, a cibersegurança viveu um paradoxo claro. Temos mais dados, mais visibilidade e mais ferramentas do que nunca, e, ainda assim, nunca estivemos tão sobrecarregados de alertas. O desafio não está mais em saber o que está acontecendo, mas em transformar informação em ação.

O cenário mudou. Os ataques à cadeia de fornecedores se tornaram frequentes, mirando a base: repositórios, bibliotecas e soluções que sustentam ecossistemas inteiros. E, cada vez mais, grupos de ameaça têm explorado os insiders, o vetor interno usado por atores maliciosos para comprometer ambientes com precisão e discrição.

É nesse contexto que a Axur vem fortalecendo sua missão de entregar dados estruturados, enriquecidos e priorizados. O lançamento do Axur Command representa um passo além, levando as automações para o próximo nível e permitindo que políticas de validação sejam executadas de forma autônoma.

Para 2026, nossa visão é clara. A consolidação dos dados e a capacidade de agir de forma integrada serão os grandes diferenciais. A Axur quer ser, para a superfície de ataque, o que as plataformas de observabilidade são para a engenharia: um sistema nervoso central. Um ponto único onde tudo se conecta, se prioriza e se resolve.

Este relatório apresenta nossa leitura do cenário de ameaças de 2025, com tendências, dados e perspectivas práticas para o ano que vem. Esperamos que ele ajude os times de segurança a priorizar melhor, agir mais rápido e, acima de tudo, antecipar riscos antes que se tornem incidentes.

A tecnologia segue avançando, e com ela vêm novas possibilidades. O nosso papel é garantir que esse avanço aconteça com segurança, confiança e responsabilidade.

Conte conosco nessa jornada.

Fábio Ramos
CEO, Axur.

Sumário executivo

Principais números

- +6 bilhões de credenciais novas e únicas detectadas
- Casos de phishing somam 71.399 páginas detectadas
- Casos de uso fraudulento de marca crescem, com 454 mil incidentes
- Removemos mais de 343 mil conteúdos fraudulentos através dos fluxos automatizados de takedown
- 395 milhões de cartões de crédito e débito detectados
- Phishing cresce 65% para o setor financeiro
- Registro de domínios semelhantes cresce +1000%
- Perfis falsos e exposição de informações continuam sendo usados para atacar executivos e VIPs, com mais de 19 mil incidentes.

Boletins em destaque

Crítico

Ataque cibernético massivo explora vulnerabilidade de C&M, com R$1 bilhão roubado

Saiba mais ↗

Alto

Ataque cibernético de Azael interrompe a infraestrutura do governo brasileiro

Saiba mais ↗

Crítico

Vazamento de Dados em massa expõe 16 bilhões de credenciais: Google, Apple e Facebook em risco

Saiba mais ↗

Alto

Fog Ransomware explora ferramentas de Pentesting para espionagem financeira

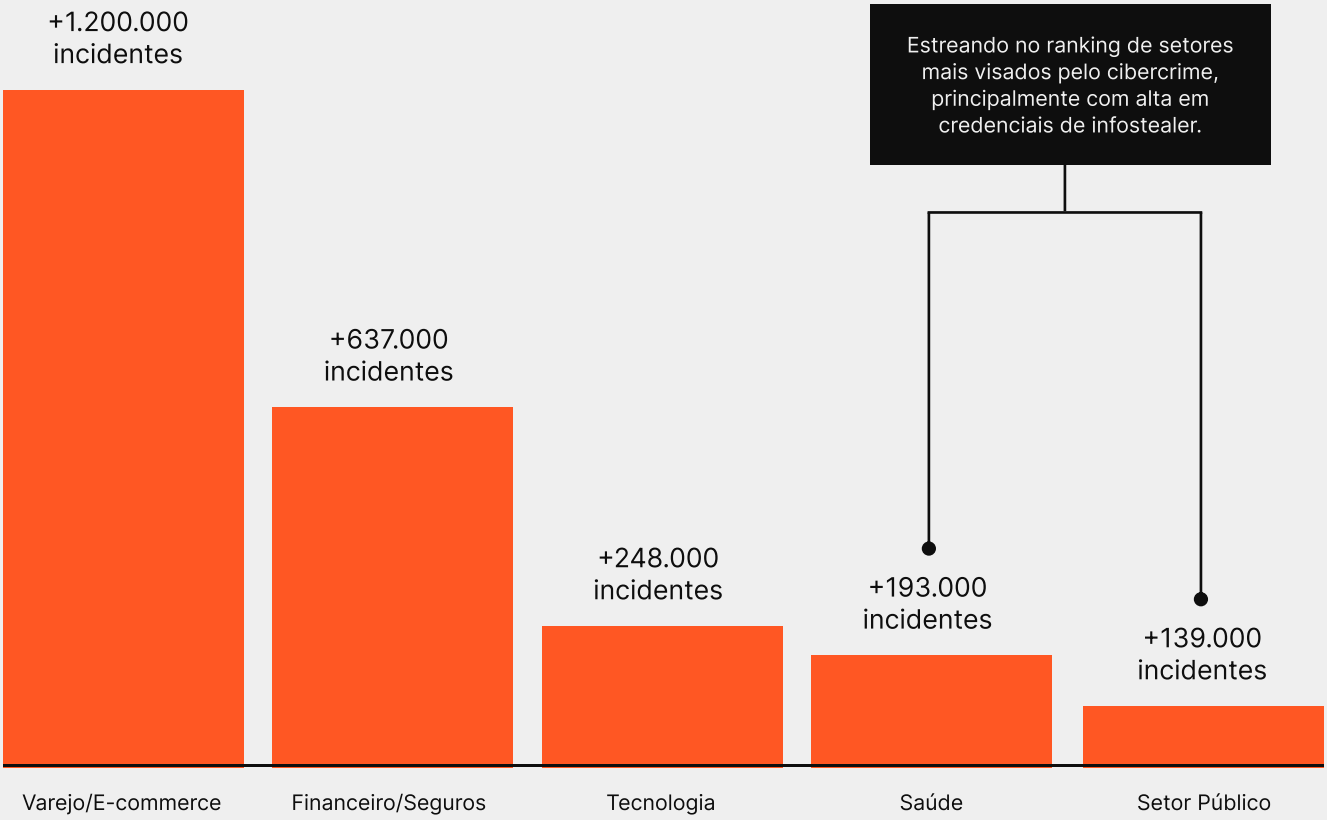
Saiba mais ↗

Crítico

A atualização do kernel do Red Hat RHEL 9 atenua vulnerabilidades críticas

Saiba mais ↗

Ranking de setores por incidentes



Setores mais visados por phishing

Financeiro/Seguros +65%
24.959 páginas detectadas

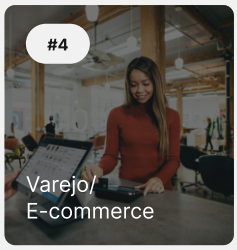
Varejo/E-commerce
21.558 páginas detectadas

Tecnologia
7.572 páginas detectadas

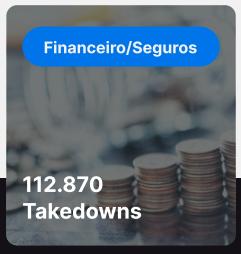
Alimentação/Bebidas
5.431 páginas detectadas

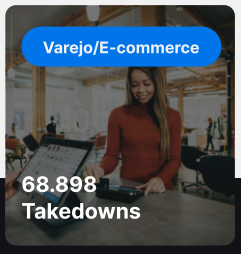
Transporte/Logística
3.594 páginas detectadas

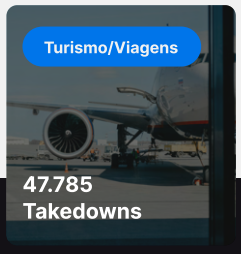
Setores mais visados na deep & dark web

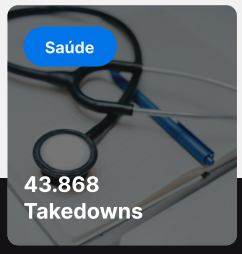


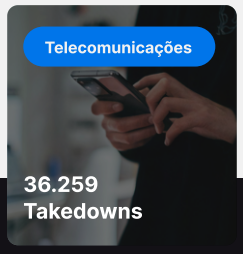
Ranking de takedowns



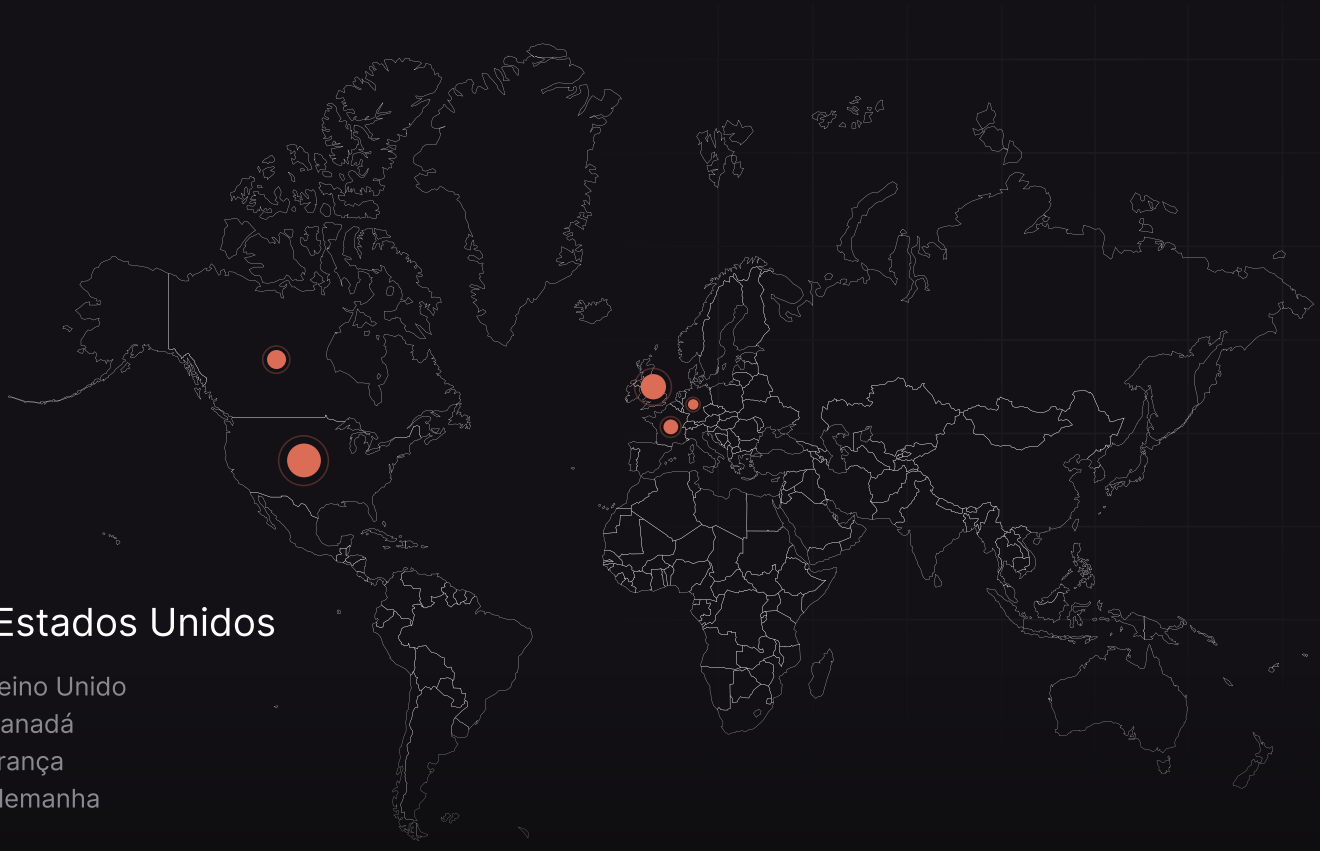








Localizações mais impactadas



1º Estados Unidos

2º Reino Unido
3º Canadá
4º França
5º Alemanha

Perfil do cibercrime no Brasil

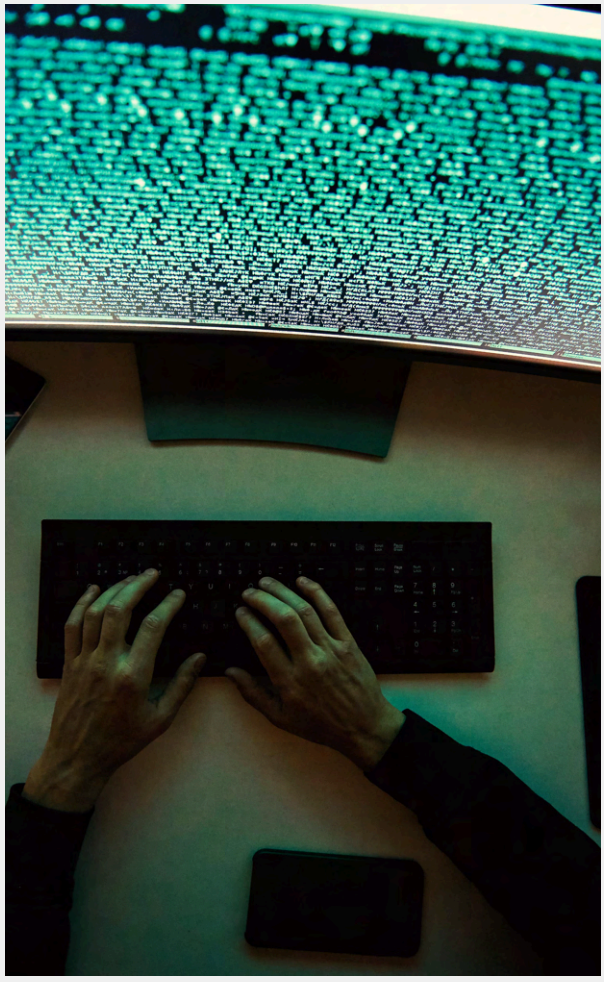
Ataques direcionados a fornecedores do sistema financeiro, como C&M Software e Sinqia/Evertec, resultaram em fraudes superiores a R$ 1 bilhão via Pix, explorando vulnerabilidades em integrações e autenticações entre instituições.

Observa-se a expansão de campanhas de vishing com URAs falsas que induzem o usuário a instalar ferramentas de acesso remoto (RATs), permitindo controle total do dispositivo e movimentações financeiras não autorizadas.

Fraudes no ecossistema de e-commerce evoluem com o uso de dados logísticos reais (rastreamentos e confirmações de entrega) para spoofing de comunicações via WhatsApp, ampliando a taxa de sucesso das campanhas.

O malware PhantomCard, recentemente identificado, utiliza NFC como vetor de ataque, clonando dados de cartões de crédito próximos ao dispositivo comprometido.

Novo malware propagado via WhatsApp Web é capaz de roubar credenciais bancárias, reencaminhar mensagens maliciosas e manter persistência por meio da sincronização da sessão entre dispositivos.



Tendências para 2026

Agentes de IA ganham autonomia

Ferramentas que hoje atuam como assistentes passarão a tomar decisões operacionais, escalando respostas, priorizando investigações e acionando remediações automatizadas. Isso acelera a defesa, mas também cria pontos de decisão que exigem governança estrita: quem autoriza o que a IA pode executar?

Criminosos consolidam o uso de IA

A mesma capacidade de orquestrar e aprender em tempo real foi incorporada a ataques, com a geração automática de campanhas de phishing hiper-personalizadas, fuzzing guiado por modelos e variação massiva de payloads para burlar detecções.

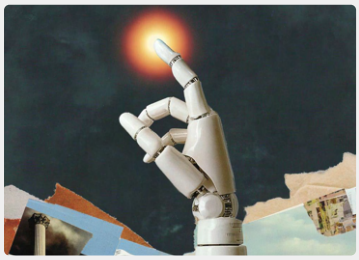
A corrida pela soberania digital

Regulações e políticas nacionais vão fragmentar fluxos de dados e exigir arquiteturas locais ou híbridas, o que redesenha cadeias de confiança, aumenta a complexidade de compliance e cria novos vetores operacionais para quem não se adaptar.

Ameaças esquecidas voltam à ativa

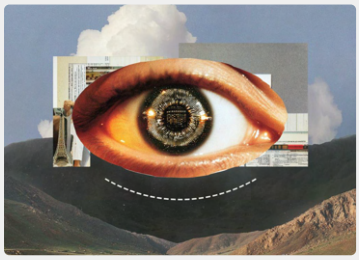
Hardware legados em IoT/OT, mal mantidos ou expostos, estão sendo reativados como recurso em botnets e campanhas persistentes.

Recomendações para os próximos desafios



Prepare-se para a era dos agentes

Agentes autônomos estão assumindo tarefas críticas de resposta e investigação. Antes de delegar ações, estabeleça políticas de autonomia, limites operacionais e mecanismos de auditoria. Defina quem autoriza execuções automatizadas e como revogar instruções em caso de comportamento anômalo.



Olhe para fora do perímetro

A maior parte das exposições começa fora dos ativos internos. Monitorar credenciais vazadas, artefatos de build e menções de marca em fontes externas é essencial para antecipar incidentes. A detecção precoce em ambientes externos reduz significativamente o tempo médio de exposição (MTTD).

Proteja ativos internos críticos

Desenvolvedores e equipes de suporte seguem entre os principais alvos de phishing e credential stuffing. Implemente MFA resistente a push bombing, segregação de funções e monitoramento de uso de ferramentas de acesso remoto. Ataques bem-sucedidos nesses perfis têm efeito multiplicador sobre toda a infraestrutura.

Mapeie a superfície de terceiros

O alerta da CISA sobre o comprometimento em larga escala do ecossistema npm evidenciou o risco crescente nas cadeias de software. Dependências, APIs e pipelines de parceiros ampliam a superfície de ataque e exigem validação contínua de integridade e permissões, já que um único fornecedor comprometido pode propagar código malicioso a todo o ambiente.

Panorama de cibersegurança

É difícil resumir o cenário de cibersegurança em algumas poucas ameaças ou desafios. De certa maneira, o desafio está justamente na diversidade de ameaças e no volume de questões que necessitam de atenção.

Nos últimos anos, a cibersegurança está mais sensível às necessidades de cada negócio, o que contribui com a gestão de riscos e a priorização de projetos. Nesse sentido, não podemos deixar de mencionar que o ambiente de negócios também está desafiante, com incertezas regulatórias e comerciais em escala global que reverberam até nas pequenas e médias empresas.

O ambiente tecnológico também está mudado. Algumas empresas vêm reduzindo a parcela de colaboradores com atuação remota, mas nem o fim do trabalho remoto acabaria como o "dado remoto" armazenado na nuvem, em parceiros e terceiros. Mas, como isso nem sempre é tão evidente, há um risco de que a segurança do acesso remoto seja negligenciada.

Ao mesmo tempo, há uma demanda crescente por serviços interativos e inteligentes, seja no comércio eletrônico ou na prestação de serviços. Novas modalidades de engajamento também abrem oportunidades para os criminosos.

> Tudo isso vem acontecendo sem que haja uma trégua na exploração de vulnerabilidades ou nos incidentes de ransomware.

Pelo contrário: as vulnerabilidades em dispositivos de rede estão cada vez mais preocupantes, e agora são citadas em ataques de ransomware e vazamentos de dados. Enquanto isso, os golpes de engenharia social se deslocam parcialmente dos usuários finais para os profissionais de TI, atingindo um público novo de formas inesperadas.

Dispositivos de borda se tornam alvo prioritário

Os ataques a dispositivos de borda (principalmente VPNs e firewalls) se destacaram em 2024 e se consolidaram em 2025.

A exploração de vulnerabilidades foi um ponto preocupante nesses ataques, mas não o único. Hackers também conseguiram realizar invasões usando credenciais roubadas e até ataques de força bruta. Alguns desses ataques chamaram a atenção por contornarem a autenticação em duas etapas, seja por meio do uso de vulnerabilidades ou talvez graças a um vazamento das chaves de geração de códigos únicos.

O Catálogo de Vulnerabilidades da Agência de Cibersegurança dos Estados Unidos (CISA) indica que dispositivos e softwares de diversos fabricantes tiveram suas vulnerabilidades exploradas ao longo do ano. Broadcom, Cisco, Fortinet, Ivanti, Juniper, Palo Alto Networks e SonicWall são algumas das marcas na lista de 2025.

> O objetivo da exploração desses dispositivos foi bastante variado.

Parte dos ataques teve o objetivo de invadir redes corporativas para instalar ransomware e realizar a já conhecida fraude de extorsão em que os hackers cobram um resgate para recuperar os arquivos cifrados ou para não divulgar as informações exfiltradas dos sistemas comprometidos.

Outro conjunto de ataques foi atribuído a atores vinculados a governos. Nestes ataques, os alvos eram normalmente empresas operadoras de infraestrutura crítica, como empresas de telecomunicação, energia ou entidades governamentais.

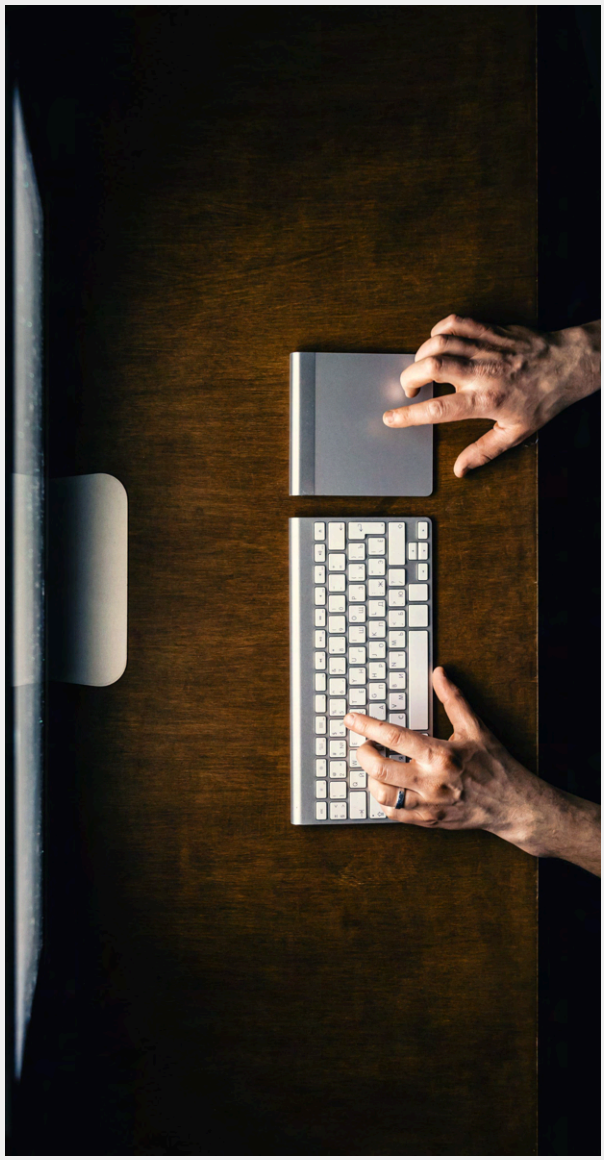
No caso dos ataques contra roteadores domésticos, os invasores normalmente instalam um malware para conectar o equipamento comprometido a uma rede zumbi. Os dispositivos podem então ser usados em ataques de DDoS ou para atuar como proxy dos criminosos, ocultando a origem de outras atividades. Ao menos alguns dos códigos usados são baseados no Mirai, um malware de IoT detectado pela primeira vez em 2016.

Ataques de engenharia social miram equipes de suporte e recrutamento

Já tem alguns anos que a atuação do grupo Scattered Spider vem demonstrando a efetividade de abordagens inovadoras em ataques cibernéticos, principalmente com o uso de engenharia social. Isso aconteceu novamente em 2025, com invasões que

> começaram a partir de chamadas telefônicas ilegítimas pedindo ajuda para redefinir senhas.

Essa estratégia de contato com equipes de suporte de TI se diferencia do que é mais comum na engenharia social, que são os ataques diretos contra usuários. Nesses novos casos, os fraudadores se passam por usuários pedindo ajuda com suas credenciais e, com isso, conseguem obter uma credencial válida para acessar a rede da empresa ou alguma plataforma.



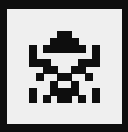
Os ataques mais notórios com essa abordagem aconteceram no Reino Unido, onde redes de varejo foram impactadas e anunciaram prejuízos significativos decorrentes das invasões.

As táticas de engenharia social associadas a emprego e recrutamento também merecem atenção. Esse golpe pode ser realizado tanto contra empresas quanto contra os candidatos. No caso da fraude contra os recrutadores, ela ocorre especialmente nas etapas em que o candidato tem abertura para enviar algum material à empresa.

Quando o recrutador abre o arquivo recebido, ele pode acabar comprometendo o seu sistema e, possivelmente, a rede da empresa.

As fraudes contra os candidatos acontecem de forma semelhante. Os golpistas enviam propostas de emprego falsas, sugerindo que o profissional participe do processo seletivo. O material de apoio para participar do processo estará contaminado com malware, e as consequências podem chegar inclusive à rede corporativa, caso o profissional esteja atualmente empregado.

Curiosamente, essas fraudes frequentemente envolvem vagas e profissionais de TI. É bastante provável que os alvos sejam escolhidos a dedo para atingir empresas ou projetos específicos. Projetos associados ao mercado de criptomoeda, por exemplo, tendem a ser bastante visados pelos criminosos.



Scattered Spider

Coletivo cibercriminoso com motivação financeira ativo desde 2022 (EUA e Reino Unido).

Principais táticas

Engenharia social (spear phishing, smishing, vishing), troca de SIM, fadiga de MFA e uso de ferramentas legítimas de acesso remoto (SupremoControl, AnyDesk, ConnectWise, Splashtop).

Malwares usados

BlackCat, Qilin, Akira, DragonForce; stealers como Racoon e Meduza.

Alvos notórios

MGM Resorts, Caesars Entertainment, Snowflake e grandes instituições financeiras.

Objetivo

roubo e extorsão de dados para ganhos financeiros.

Comentário do especialista

Pedro Moura

Pesquisador do
Axur Research Team

Embora o Scattered Spider tenha se notabilizado como afiliado de grupos como BlackCat/ALPHV e, mais tarde, DragonForce, o coletivo evoluiu em 2025 para desenvolver seu próprio ransomware, abandonando o papel de intermediário. A CISA confirmou essa transição em um alerta recente, destacando o aumento da sofisticação operacional do grupo.

O suposto “encerramento das operações” e o banner de apreensão exibido em seus domínios onion são amplamente interpretados como ações de PsyOps, projetadas para confundir a comunidade de segurança e mascarar uma possível reestruturação.

Extorsão tripla torna ransomware mais difícil de conter

Os ataques de ransomware continuam representando uma ameaça significativa para as empresas, e quase todas as atividades maliciosas registradas acabam tendo algum envolvimento com esses ataques.

O modelo de RaaS (ransomware as a service – ransomware como serviço) estabelece uma estrutura em que diversos "afiliados" se encarregam de encontrar maneiras de instalar o malware dentro das redes corporativas. Desse modo, um mesmo ransomware pode estar associado a várias estratégias de ataque.

Phishing, ataques de supply chain, abuso de credenciais, recrutamento de colaboradores internos, vulnerabilidades – todas essas táticas são usadas para invadir a infraestrutura de TI e iniciar o golpe do ransomware.

Um ponto de atenção no contexto do ransomware diz respeito às modalidades de extorsão no desfecho do incidente. Tradicionalmente, o ransomware cifra os arquivos dos sistemas para paralisar as atividades do negócio e então cobra pela chave capaz de restaurar os dados e recuperar os sistemas.

Diante da frequência desses ataques, muitas empresas adotaram processos de recuperação robustos para restaurar os sistemas a partir de backups protegidos, o que reduziu o poder de coação dos criminosos. Os golpistas então responderam com as táticas de extorsão dupla e tripla, em que a empresa é ameaçada também com a exposição de dados corporativos e ataques de DDoS – situações para as quais a empresa pode não estar preparada ou nem pode evitar.

> Mais recentemente, os criminosos também têm apostado em tentativas de extorsão amparadas exclusivamente pela ameaça de exposição de dados corporativos.

Ainda que os criminosos dispensem o bloqueio de sistemas e arquivos por meio da criptografia, todas as demais características do golpe seguem o padrão do ransomware.

Comentário do especialista

A extorsão dupla já é consolidada e aparece quase como mandatória no cenário atual. Além disso, existem extorsões crescentes exclusivamente relacionadas ao vazamento de dados sem necessariamente ter a criptografia.

Alisson Moretto

Head de Threat Hunting na Axur

Dispensando a criptografia dos dados, os criminosos podem realizar a tentativa de extorsão inclusive quando não foi viável obter acesso de escrita a determinados sistemas, ou quando eles sabem que arquivos podem ser recuperados com facilidade (como no caso do armazenamento em nuvem).

Os argumentos durante a "negociação" com as empresas também vêm evoluindo na mesma direção. As gangues exploram o receio de repercussões legais e danos à reputação decorrentes do vazamento de dados para convencer a vítima a realizar o pagamento, inclusive com o emprego de supostos "advogados" que estariam oferecendo aconselhamento jurídico.

Ataques à cadeia de fornecedores se tornam recorrentes

Ataques contra a cadeia de fornecedores (supply chain) se consolidaram como um vetor robusto para ataques cibernéticos. Os incidentes históricos mais conhecidos são possivelmente o da varejista Target, que sofreu um vazamento de dados a partir do acesso de um prestador de serviços de climatização em 2013, e o da SolarWinds, que teve seu software adulterado por um invasor para implantar backdoors em vários clientes.

Nos últimos anos, a noção de riscos de supply chain vem sendo ampliada em certos aspectos. O uso de plataformas padronizadas e de soluções de software como serviço (SaaS) viabilizou uma nova categoria de ataques em massa, com ou sem o uso de vulnerabilidades específicas.

Os casos do MOVEit Transfer (2023) e da Cleo (2024) são exemplos de incidentes em massa envolvendo alguma vulnerabilidade em um software. Já os ataques de roubo de dados que exploraram os serviços da Snowflake (2024) e Salesforce (2025) utilizaram credenciais roubadas e engenharia social, respectivamente.

Essas campanhas recorrentes mostram que a estratégia de atacar fornecedores e terceiros se consolidou entre os atacantes. Ataques contra terceiros sempre foram possíveis, é claro, mas agora eles são intencionais e estratégicos, inclusive para obter informações privilegiadas (como credenciais) ou ter acesso a um caminho mais fácil para invadir a rede do alvo final.

Software supply chain vira vetor de contaminação

Um subgrupo dos ataques de supply chain são os ataques à infraestrutura de desenvolvimento software, o que normalmente se resume ao "software supply chain". Essa definição pode incluir casos como o da SolarWinds e outras situações em que softwares são adulterados diretamente, mas há uma parcela ainda mais específica de ataques situada exclusivamente nos processos de desenvolvimento de software.

Nesses ataques, os criminosos criam ou modificam pacotes em repositórios como npm e PyPI, que são usados por engenheiros em outros softwares. Com isso, o comportamento malicioso se alastra para outros projetos, atingindo soluções corporativas que usam esses códigos.

É bastante comum que pequenos aplicativos improvisados para atividades administrativas de TI utilizem esses repositórios, então não se pode descartar a existência de risco direto apenas porque a empresa não atua formalmente no desenvolvimento de software.

Além disso, há um risco indireto considerável, caso a empresa utilize outros softwares que dependam de pacotes nessas bibliotecas ou em serviços de apoio ao desenvolvimento de software que venham a ser comprometidos.

Ao longo de 2025, foram observados vários pacotes maliciosos no npm e no PyPI. Hackers criaram diversos pacotes falsos e adulteram pacotes legítimos, o que foi possível após o roubo das credenciais dos mantenedores.

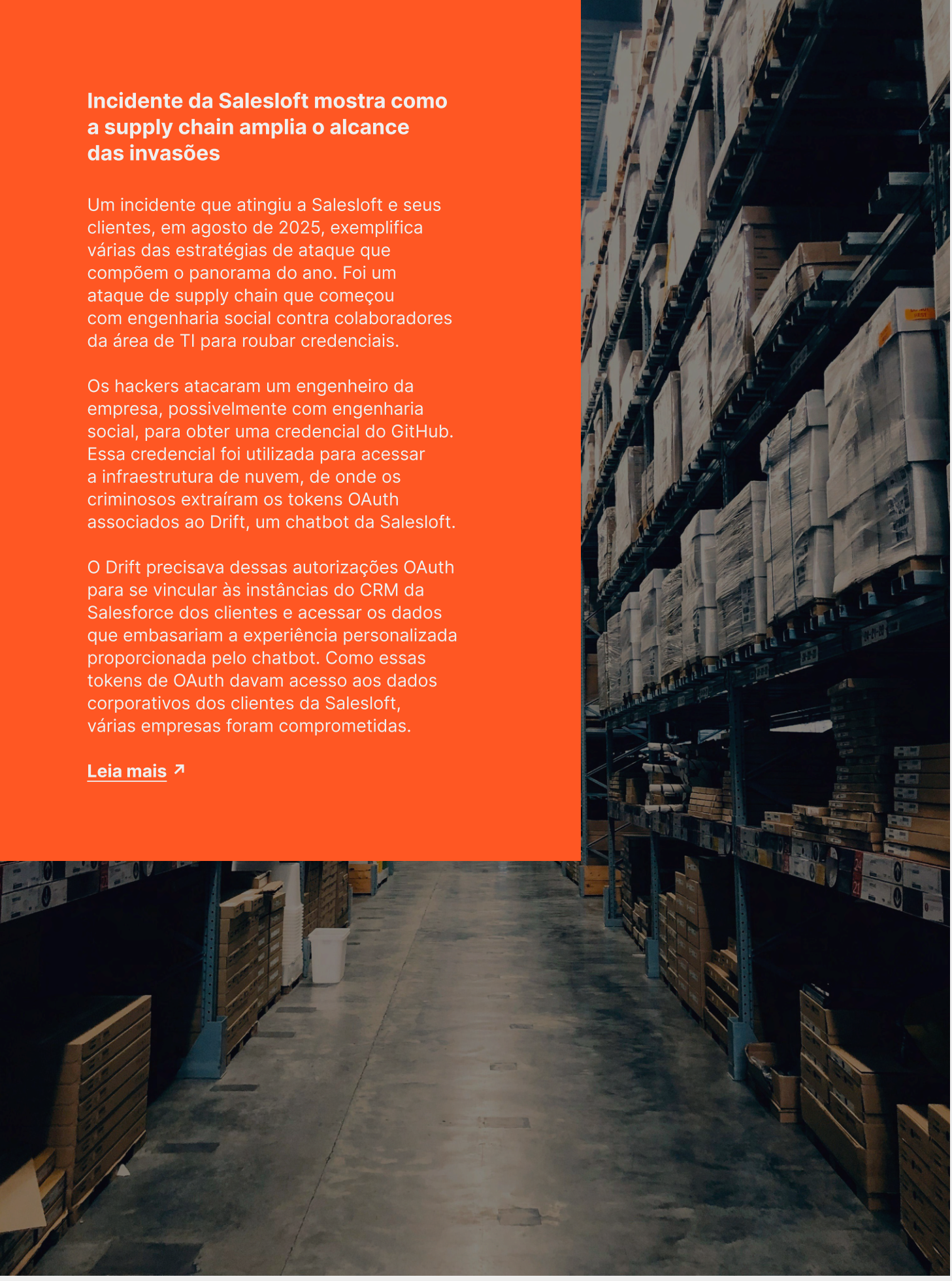
Incidente da Salesloft mostra como a supply chain amplia o alcance das invasões

Um incidente que atingiu a Salesloft e seus clientes, em agosto de 2025, exemplifica várias das estratégias de ataque que compõem o panorama do ano. Foi um ataque de supply chain que começou com engenharia social contra colaboradores da área de TI para roubar credenciais.

Os hackers atacaram um engenheiro da empresa, possivelmente com engenharia social, para obter uma credencial do GitHub. Essa credencial foi utilizada para acessar a infraestrutura de nuvem, de onde os criminosos extraíram os tokens OAuth associados ao Drift, um chatbot da Salesloft.

O Drift precisava dessas autorizações OAuth para se vincular às instâncias do CRM da Salesforce dos clientes e acessar os dados que embasariam a experiência personalizada proporcionada pelo chatbot. Como essas tokens de OAuth davam acesso aos dados corporativos dos clientes da Salesloft, várias empresas foram comprometidas.

Leia mais ↗



2025 em números

Credenciais

A plataforma da Axur detectou 6 bilhões de novas credenciais únicas em 2025.
É importante destacar que, até o ano passado, nosso relatório trazia o número total de credenciais detectadas. A mudança se deu através de processos implementados para trazer uma verificação acurada de dados coletados, na linha do que comentamos sobre menos ruído e mais alertas relevantes.

Com o aumento de grandes recompilados de dados sendo divulgados como se fossem um vazamento novo, é mais importante que nunca oferecer às equipes de segurança alertas curados que evitem o retrabalho de verificar credenciais frequentemente recompartilhadas em grupos e fóruns cibernéticos. Sendo assim, uma credencial única conta como um conjunto de login e senha compartilhado apenas uma vez.

Esse número mostra que ainda há muitas atividades maliciosas com o intuito de roubar credenciais. Essas credenciais comprometidas circulam nos espaços do submundo do crime, alimentando diversas ameaças e golpes.

> Um ponto de atenção é que a maioria das novas credenciais (52,2%) está atrelada a sistemas corporativos.

É possível que essas credenciais concedam acesso a sistemas que guardam informações comerciais ou pessoais cuja exposição prejudicaria as atividades da empresa ou a reputação dela. Em vários países, o vazamento de dados pessoais também gera consequências jurídicas.

Um exemplo recorrente em 2025 foram os ataques que usaram credenciais de VPNs e outros dispositivos de borda de rede (edge devices).

Embora a adoção de MFA reduza os riscos decorrentes de credenciais vazadas, criminosos têm conseguido combinar essas credenciais com golpes de phishing, convencendo um analista de suporte a desativar ou reconfigurar a MFA. Como a senha já está na mão dos criminosos, isso é suficiente para comprometer a conta.
O vazamento de credenciais também aumenta o risco associado a vulnerabilidades que permitam burlar a MFA.

Por estas razões, o monitoramento de credenciais vazadas é um mecanismo importante para aumentar a resiliência dos processos de autenticação em todos os sistemas corporativos, mesmo que uma solução de MFA esteja em uso.

Phishing

> A Axur detectou 71.399 páginas de phishing em 2025.

O phishing é uma das fraudes cibernéticas mais conhecidas e constantes. Na Axur, contabilizamos as páginas web onde o phishing ocorre, não importa qual for o canal utilizado para levar essas páginas às vítimas. Assim, além dos links para sites falsos divulgados em e-mails, as páginas de Smishing (phishing por SMS) e sites promovidos por anúncios pagos também são contabilizados.

Após uma alta significativa na detecção de páginas de phishing no ano anterior, o volume total de páginas se manteve estável em 2025.

A detecção de phishing pode ser aliada ao processo de takedown para retirar a fraude do ar, diminuindo o impacto sobre a marca e os consumidores. Com o uso do Clair (Cyber Lens for Anomaly and Impersonation Recognition), o nosso modelo de inteligência artificial, é possível identificar páginas de phishing de forma confiável e automatizada.

Além disso, os atributos identificados pelo Clair viram filtros que permitem a detecção além das palavras-chaves.

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

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

Casos de phishing que usam as cores da marca, por exemplo, são encontradas pelo monitoramento automatizado e passíveis de takedown automático. Além disso, é possível usar o Threat Hunting para buscar URLs com atributos variados.

Algumas buscas possíveis:

→ Imitação de marca por elementos visuais:
identifica sites que imitam marcas conhecidas ou exibem logotipos específicos. Por exemplo, detecte níveis variados de imitação de "NomeDaMarca" ou encontre sites que exibam o "LogoDaMarca".

→ Tipo de conteúdo e solicitações de dados sensíveis:
sites de phishing por tipo de conteúdo, como páginas de login, páginas de erro ou sites de e-commerce. Também é possível identificar aqueles que solicitam informações sensíveis, como senhas ou dados de pagamento.

→ Análise de domínio e ciclo de vida:
domínios com base nas datas de criação ou expiração, ou com filtro por resultados por datas de detecção recentes para encontrar novas ameaças.

→ Referências e atributos de URL:
examina URLs ou referências específicas e filtra por atributos de domínio, subdomínio ou domínio de topo (TLD) para refinar as buscas.

→ Conteúdo HTML:
busca termos específicos presentes no código das páginas detectadas, como e-mails, números de telefone e mais.

→ Ameaças específicas de idioma e região:
investigações em determinados idiomas ou regiões identificam campanhas de phishing mais localizadas.

Divisão por setor

Analisando o volume de páginas de phishing por setor da marca utilizada no golpe, observamos um aumento na proporção de ataques voltados a bancos e financeiras. No ano anterior, o varejo tinha uma margem confortável no topo da lista, mas este não foi o caso em 2025.

Vale lembrar que golpes que utilizam marcas do varejo podem facilmente adotar narrativas para roubar cartões de crédito e outros dados financeiros. Portanto, uma diferença no tipo de marca utilizada não caracteriza por si só uma mudança nos interesses dos criminosos.

Os dados de 2025 indicam uma mudança relevante no foco das campanhas de phishing no Brasil. O setor Financeiro/Seguros registrou um aumento de 65% nas detecções, superando o Varejo/E-Commerce. Essa movimentação sugere que os agentes de ameaça estão redirecionando esforços para instituições financeiras, atraídos pelo potencial de ganho direto.

O setor de Transporte também apresentou crescimento, em linha com o avanço das fraudes logísticas identificadas no capítulo perfil do cibercrime brasileiro, algumas páginas à frente. Essas fraudes exploram o ecossistema de rastreamento de entregas e o uso de páginas falsas de transportadoras, ampliando a superfície de ataque contra consumidores e empresas do setor.

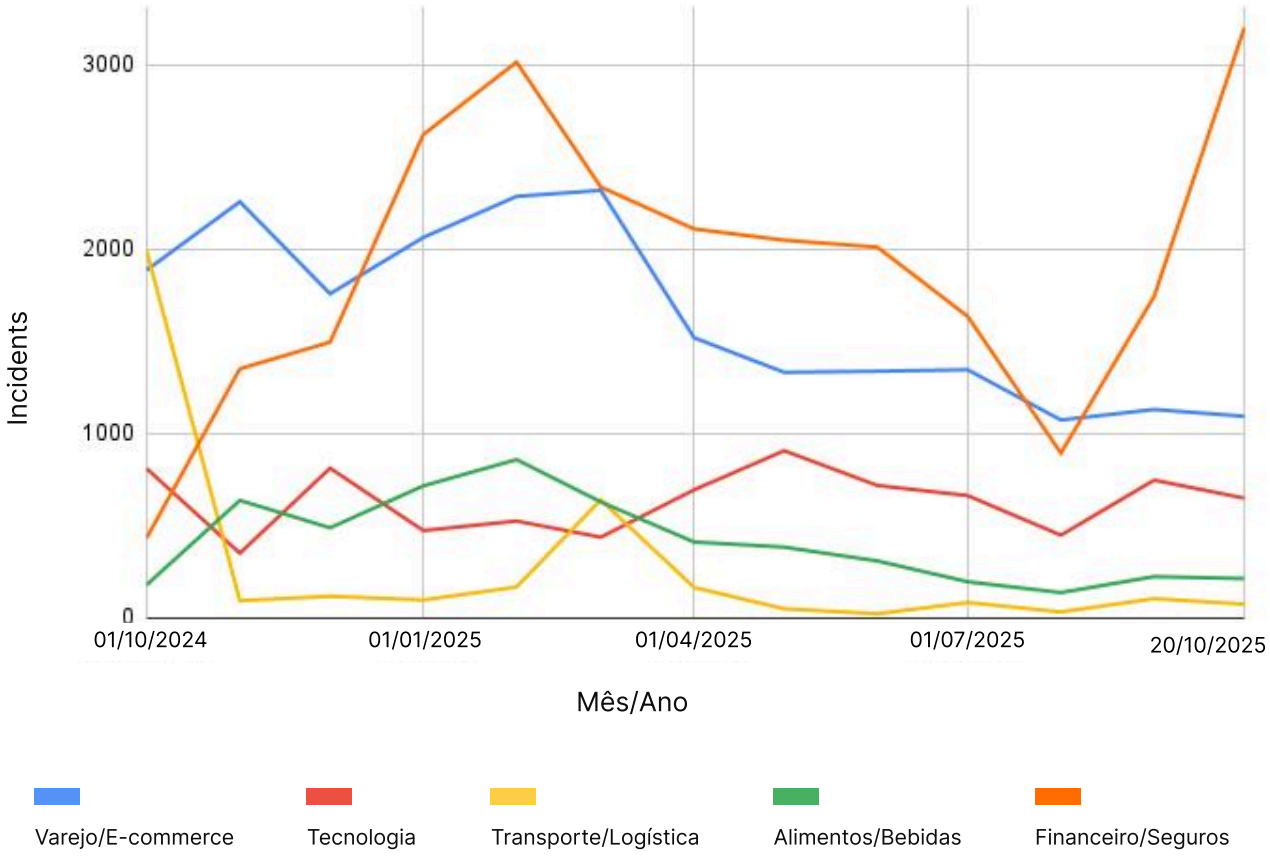
Evolução dos setores mais visados por phishing entre 2024 e 2025

	2024	2025	
Varejo/E-Commerce	27.305	21.558	↓ -21%
Bancos/Financeiras	18.915	24.959	↑ +65%
Tecnologia	9.502	7.752	↓ -18%
Alimentos	3.462	5.431	↑ +56%
Transporte	3.330	3.359	↑ +0,87%

Tendências em phishing: evolução por setor

No recorte por setor, observa-se uma mudança relevante na distribuição dos incidentes de phishing. O segmento financeiro/seguros assumiu a liderança em volume de ataques, superando o varejo e e-commerce, que havia ocupado a primeira posição no ano anterior. Essa inversão pode estar relacionada ao aumento da exploração de credenciais corporativas e ao uso de integrações SaaS como vetor de acesso inicial. Os setores de transporte e logística apresentaram oscilações pontuais, enquanto alimentos e bebidas mantiveram estabilidade relativa, com volumes menores.

Distribuição dos incidentes de phishing por setor econômico entre 2024 e 2025



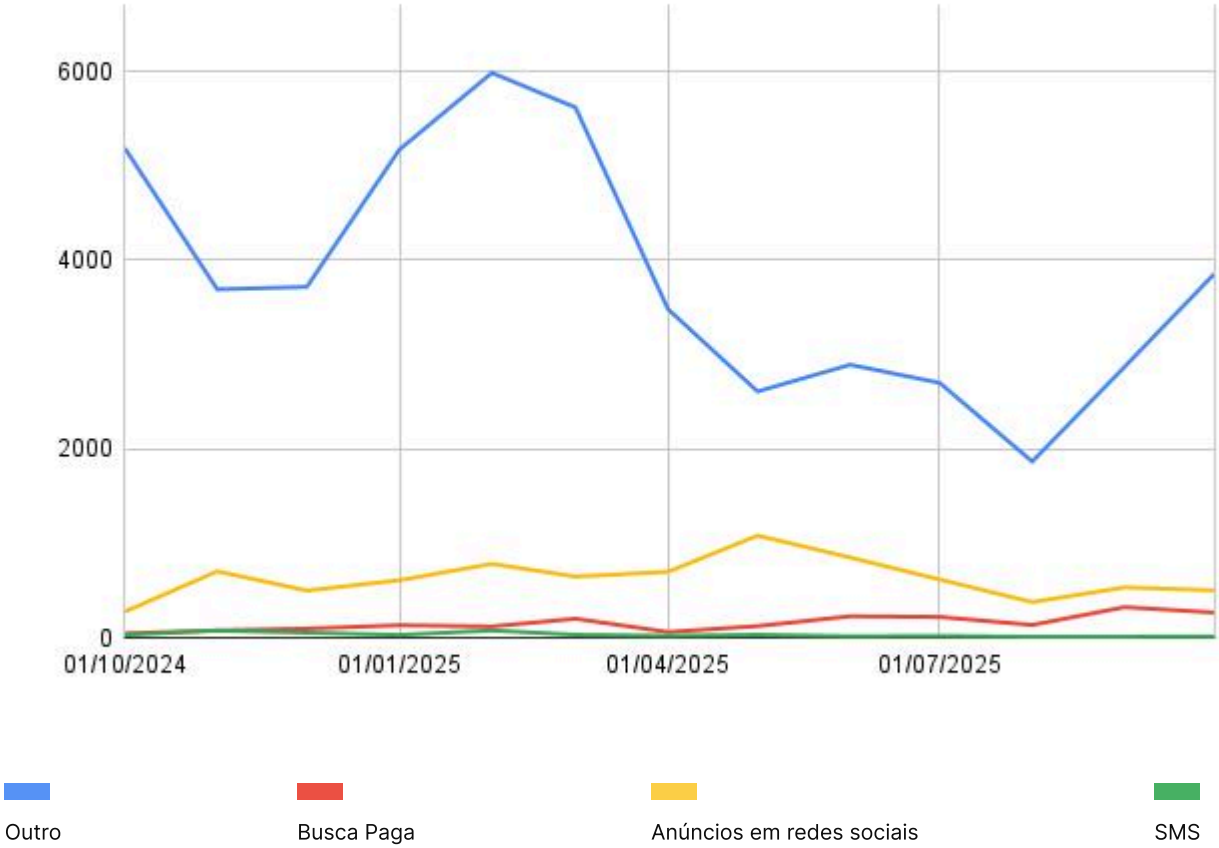
Tendências em phishing: evolução por vetor de ataque

Já os vetores de ataque mantiveram variação considerável ao longo do ano. As campanhas mais tradicionais, reunidas na categoria Outro, que inclui páginas falsas e sites clonados, continuaram predominantes, mas com comportamento irregular e picos concentrados no primeiro trimestre. Entre os canais específicos, anúncios em redes sociais sustentaram uma presença constante, enquanto o uso de busca paga apresentou crescimento gradual. Os ataques via SMS permaneceram em patamar reduzido, embora sigam sendo empregados em campanhas de curto alcance, voltadas a públicos específicos.

A diversificação dos alvos e a ampliação dos canais de fraude sugerem que os atacantes vêm distribuindo esforços entre setores e plataformas para maximizar o impacto das campanhas.

O cenário reforça a necessidade de abordagens mais amplas de monitoramento e correlação de ameaças, capazes de contemplar o ecossistema de exposição digital como um todo.

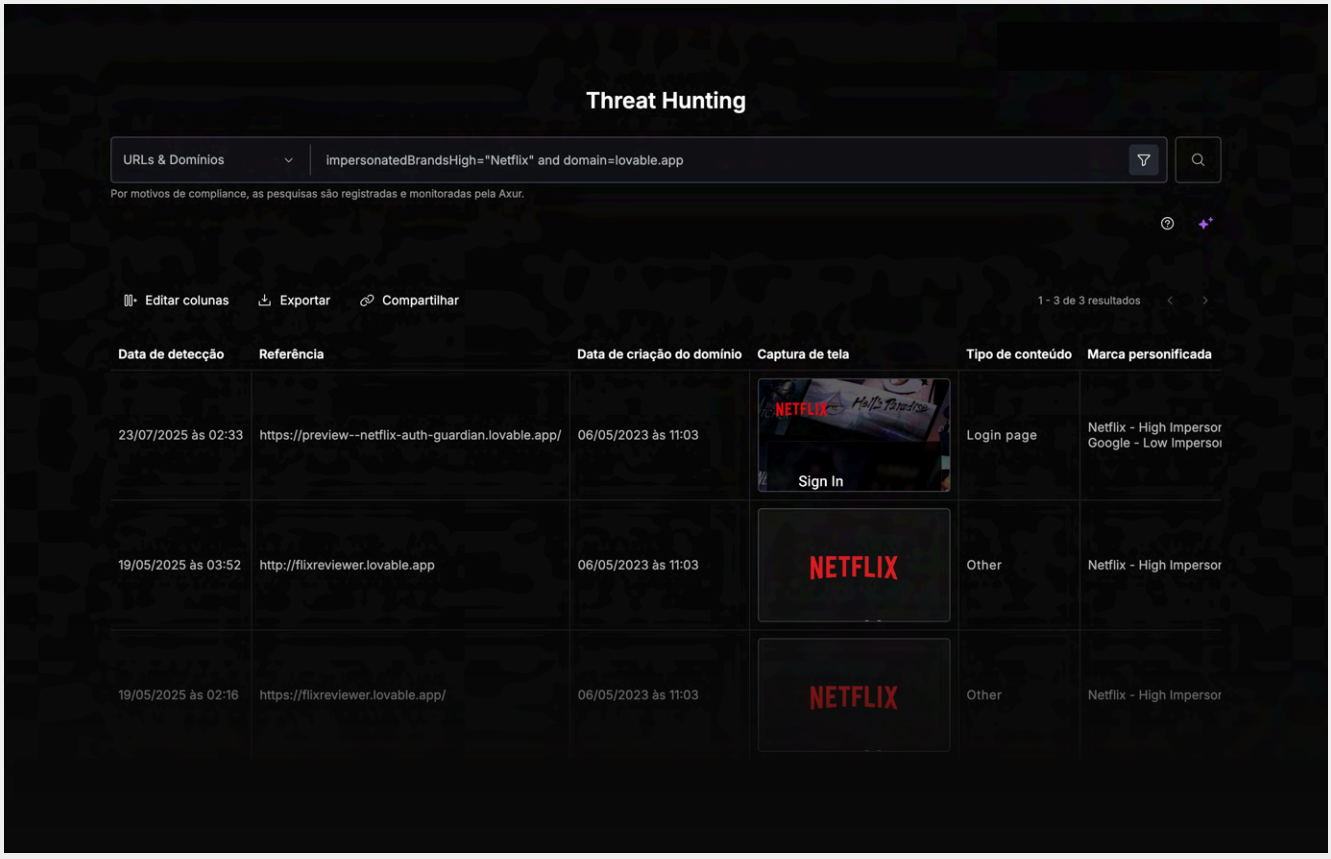
Evolução mensal dos principais vetores de ataque observados entre o fim de 2024 e 2025.



IA acelera o phishing: páginas falsas criadas em minutos com ferramentas como Lovable

Os grupos de fraude digital têm incorporado ferramentas de geração assistida por IA, como o Lovable, para automatizar a criação de páginas de phishing com alta fidelidade visual. Esses construtores permitem replicar interfaces legítimas, bancos, provedores de e-commerce, serviços de autenticação, em questão de minutos, sem exigir conhecimento técnico avançado.

O uso de modelos generativos para clonar fluxos de login, ajustar textos persuasivos e adaptar o idioma ao alvo acelera a produção e personalização de campanhas, reduzindo o tempo entre concepção e execução. Essa tendência consolida o phishing como um vetor de ataque altamente escalável e difícil de detectar, sobretudo quando combinado a kits hospedados em infraestruturas legítimas e domínios recém-registrados.



Captura de tela do Threat Hunting da Axur mostra casos de phishing criados com a ferramenta Lovable.

Uso de domínios de primeiro nível

A lista dos domínios de primeiro nível (DPNs) mais utilizados pelos criminosos se manteve muito parecida com a do ano anterior. The rising share of .app clearly shows how AI-powered website builders have become a go-to resource for criminals creating fraudulent pages. **Netlify, Vercel, and Lovable account for 75% of phishing cases using the .app TLD.**

Top domínios (TLDs) mais usados entre 2024 e 2025

	2024	2025	
.com	26.612	20.921	↓ -21,4%
.online	9.147	4.861	↓ -46,9%
.site	5.062	6.392	↑ +26,3%
.shop	5.196	6.358	↑ +22,4%
.com.br	3.644	4.275	↑ +17,3%
.store	1.721	1.607	↓ -6,6%
.net	1.489	922	↓ -38,1%
.org	1.254	861	↓ -31,3%
.ru	1.017	552	↓ -45,7%
.de	928	895	↓ -3,6%
.xyz	997	494	↓ -50,5%
.app	-	1619	Novo
.top	-	952	Novo

Os 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.

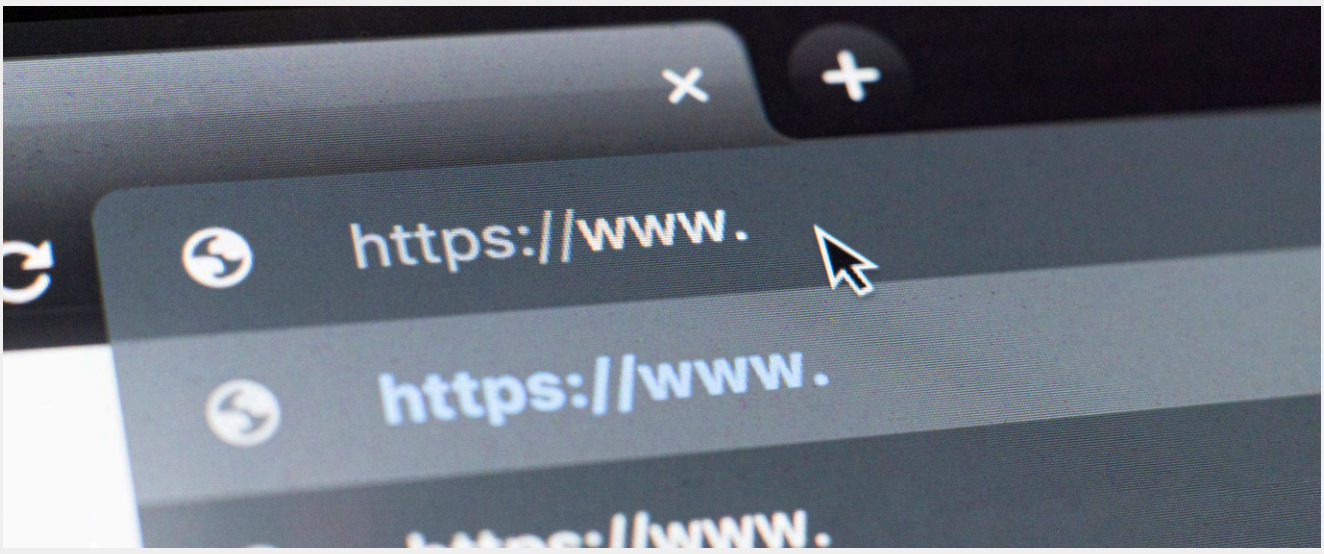
Para fazer esta escolha, o golpista normalmente considera alguns elementos:

→ 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. Esse é um dos fatores que pode explicar o aumento no uso do DPNs ".app", por exemplo.

→ 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.



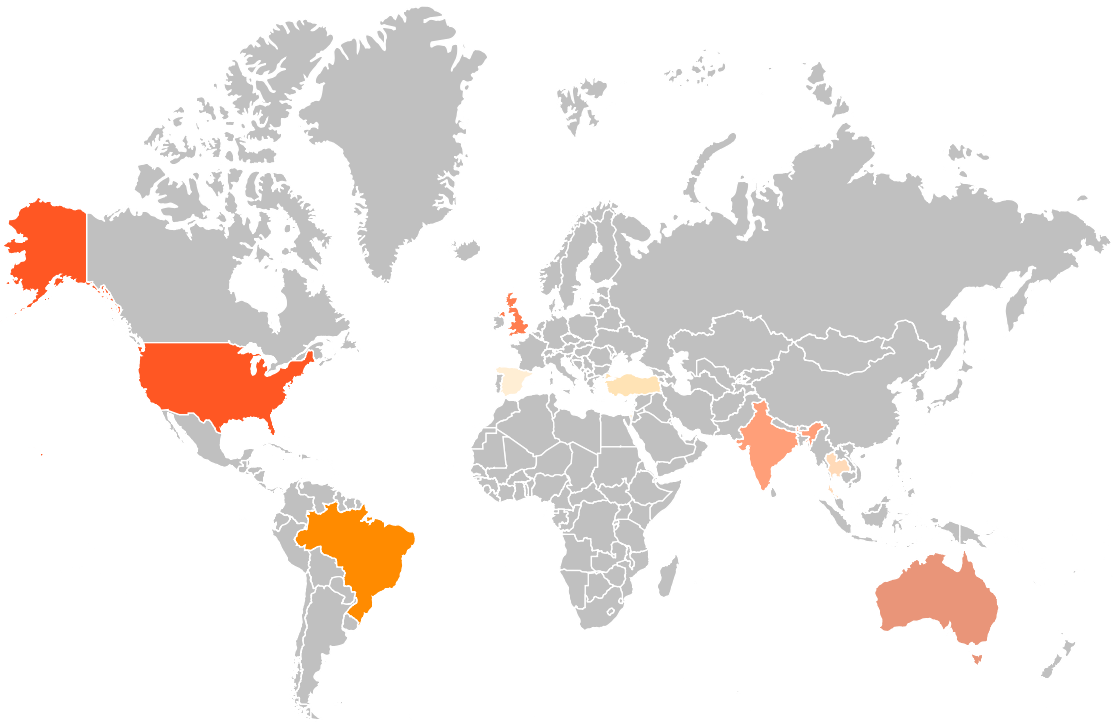
Cartões

> A Plataforma Axur detectou o vazamento de dados de 395 milhões de cartões de crédito e débito.

O número de detecções de cartões vazados em 2025 se manteve estável em relação ao período do relatório anterior. Infelizmente, o número de cartões vazados ainda é expressivo e preocupante.

Graças ao BIN (Bank Identification Number), é possível identificar a origem de cada cartão.

Ranking global de países com cartões válidos expostos em 2025



Estados Unidos: **56,16%** | Brasil: **5,36%** | Reino Unido: **2,24%** | Austrália: **1,73%** | Índia: **1,67%**
Tailândia: **1,32%** | Turquia: **0,74%** | Espanha: **0,71%** | Israel: **0,68%** | Outros: **6,49%**

Em 2025, a liderança global de cartões vazados continua sendo dos Estados Unidos, seguido por Brasil e Reino Unido.

O roubo de cartões representa um risco significativo para as instituições financeiras e para o comércio eletrônico. Após o cartão ser usado de forma indevida, o consumidor normalmente inicia um processo de chargeback, obrigando a loja a devolver o valor cobrado. Como a mercadoria nem sempre pode ser recuperada, a loja terá um prejuízo com essa operação.

Com os dados da Axur, varejistas podem detectar o uso de cartões vazados e bloquear a compra ou realizar as validações necessárias para garantir sua legitimidade.

A verificação também é especialmente importante para instituições de pagamento. As exposições de cartões impactam diretamente instituições financeiras e processadores que precisam validar transações com rapidez e precisão para reduzir perdas e manter a confiança das bandeiras.

Caso de uso real

150%
menos tempo na validação de cartões

Em 2025, a fintech **Zoop**, que fornece infraestrutura tecnológica para o setor financeiro, integrou a base de cartões expostos da Axur a seu processo de validação.

A verificação ocorre em milissegundos e bloqueia preventivamente cerca de 30% das tentativas de transação com cartões comprometidos, reduzindo o tempo de resposta operacional em 150% e fortalecendo a segurança das operações de pagamento.

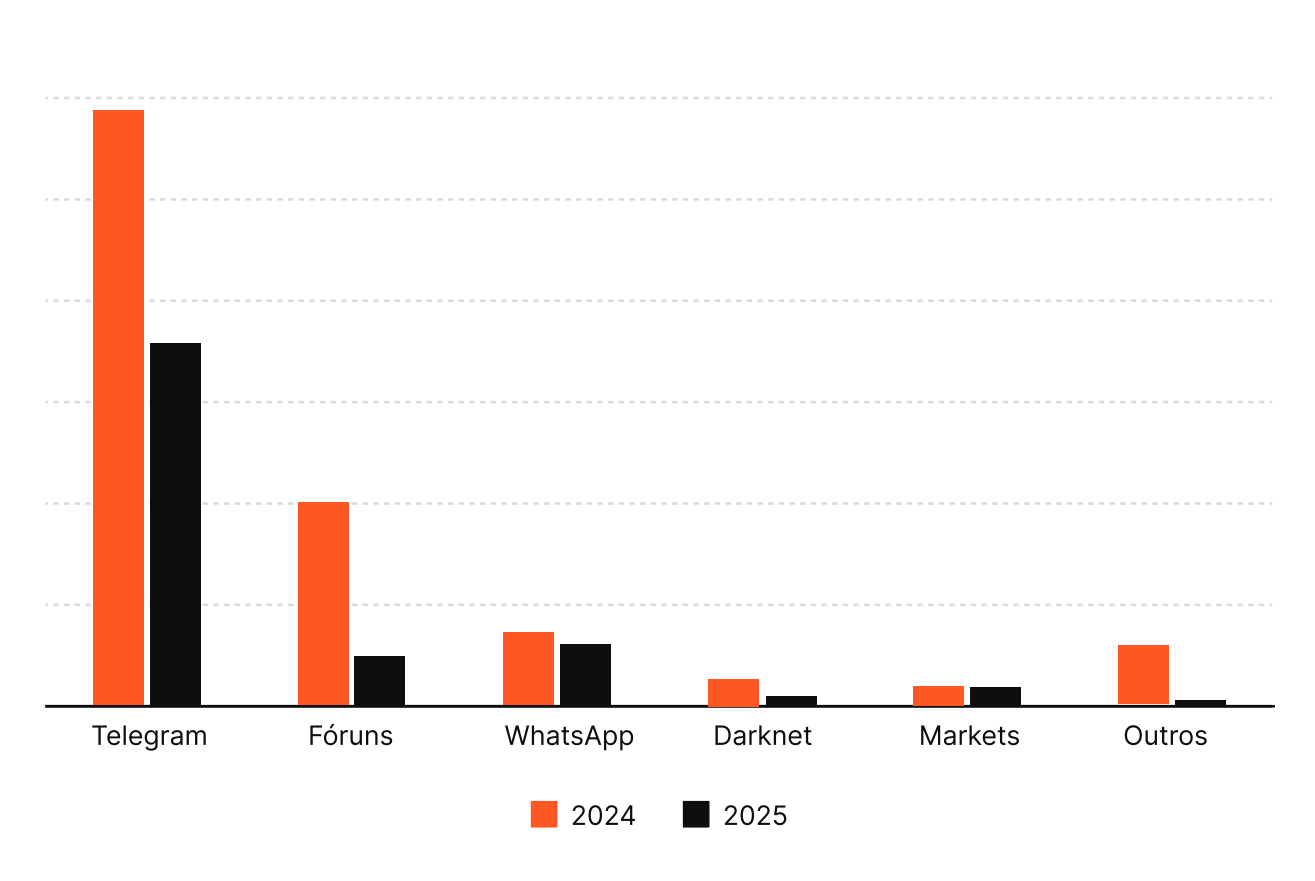
LEIA O CASE

Deep & Dark Web

> Em 2025, encontramos 496.403 comunicações suspeitas na Deep & Dark Web que foram convertidas em incidentes para investigação e coleta de inteligência.

O ecossistema do cibercrime conta com uma série de canais que normalmente ficam de fora da web visível para a maioria das pessoas, pois não aparecem em pesquisas simples nos motores de busca, e a entrada nesses canais, grupos ou fóruns é muitas vezes restrita.

No entanto, esses espaços de Deep & Dark Web utilizados pelos criminosos podem ser monitorados para gerar inteligência sobre as ameaças cibernéticas que são discutidas nesses locais.



Fontes de incidentes na deep e dark web em 2025.

Setores mais afetados na deep & dark web

O setor financeiro assumiu a liderança, passando de 26,1% para 48,6% das ocorrências, enquanto o varejo caiu de 45% para 18,1%. Essa inversão reflete o crescimento das fraudes direcionadas ao ecossistema bancário e de meios de pagamento, em especial as campanhas envolvendo ataques ao Pix e prestadores de serviços de tecnologia financeira (PSTIs).

O aumento também sugere uma sofisticação maior nas estratégias dos grupos criminosos, que estão explorando com mais força as vulnerabilidades mais estruturais, como integrações de sistemas e credenciais de acesso em instituições financeiras.

O avanço do setor de tecnologia, de 16,8% para 22,5%, também reforça esse movimento: provedores de infraestrutura, fintechs e plataformas SaaS passaram a ocupar papel central na cadeia de risco. Já telecomunicações manteve estabilidade, com leve redução, o que pode indicar maior maturidade dos controles e resposta mais ágil a incidentes.

Em conjunto, os dados confirmam uma tendência de migração das campanhas de fraude para alvos de maior impacto sistêmico, onde a exploração de credenciais, APIs e integrações pode gerar efeitos em cascata sobre múltiplos serviços financeiros.

	2024	2025	
Varejo	45%	18,1%	↓ -59%
Financeiro	26,1%	48,6%	↑ +86%
Tecnologia	16,8%	22,5%	↑ +33%
Telecomunicações	4,8%	4,7%	↓ -2%

A Axur tem visibilidade sobre diversos desses canais e realiza um monitoramento que transforma os sinais coletados em incidentes que podem ser investigados. Em algumas situações, esses sinais permitem até bloquear uma ação antes que ela de fato ocorra.

Caso de uso real

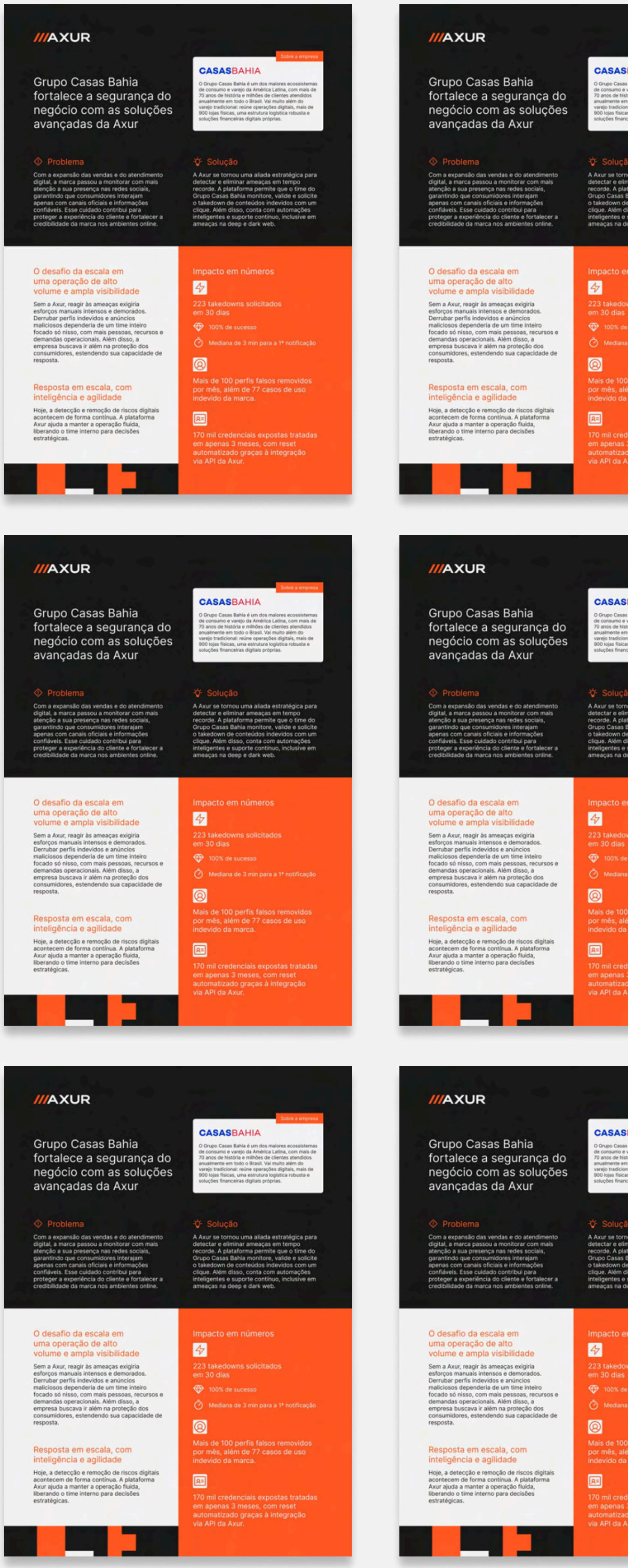
Detecção de insiders a partir de indícios na dark web

Em 2025, o Grupo Casas Bahia utilizou o monitoramento de deep & dark web da Axur para investigar indícios de vazamento de informações corporativas identificados em fóruns restritos.

A partir desses sinais, o Axur Research Team conduziu uma análise aprofundada que revelou a atuação de insiders envolvidos na extração e comercialização de dados internos.

A investigação permitiu mapear a origem do vazamento, conter o grupo responsável e implementar controles preventivos para evitar recorrências e mitigar qualquer impacto reputacional.

LEIA O CASE



Perfis falsos, aplicativos ilegítimos e uso fraudulento de marca

Nenhuma fraude chega às vítimas se identificando como fraude. Em vez disso, elas utilizam marcas e pessoas conhecidas, preferencialmente em cenários plausíveis, para que as vítimas acreditem na narrativa do golpe.

O monitoramento da Axur varre a web para detectar situações em que uma marca é utilizada de forma indevida para promover conteúdo e ofertas ilegítimas, aplicativos maliciosos, perfis fraudulentos e uso não autorizado da marca em links patrocinados de busca.

Em 2025, as ocorrências de uso indevido de marcas registraram alta, com indícios de que práticas relacionadas ao typosquatting, cybersquatting ou registro de domínios semelhantes, (+1000%), e ao uso de marcas em anúncios pagos contribuíram para esse movimento.

O uso fraudulento da marca ainda é o incidente mais comum, seguido dos perfis falsos em redes sociais e os aplicativos falsos.

Os perfis falsos em redes sociais podem ser usados para enganar os consumidores, com ofertas ou serviços que não existem.

O consumidor pode acreditar que está falando com um representante verdadeiro da empresa e adquirir produtos ou serviços que jamais serão entregues, criando uma situação indesejada para a empresa, que perdeu um cliente, e o próprio consumidor, que perdeu seu dinheiro.

O uso de marca em busca paga também aumentou, de 1.282 para 5.499 registros, o que corrobora a tendência observada pelos pesquisadores da Axur de que os golpistas têm buscado cada vez mais usar a publicidade online para conferir aparência de legitimidade a fraudes.

Os aplicativos falsos para dispositivos mobile são uma ameaça grave especialmente para empresas do setor financeiro, uma vez que esses aplicativos podem usar a marca de bancos e financeiras para solicitar os dados e as credenciais das vítimas.

Em 2025, os aplicativos móveis falsos parecem apresentar uma queda significativa. Porém, como mostramos na análise de TLDs, este movimento pode estar relacionado a uma migração tática dos agentes de ameaça, que passaram a explorar com mais intensidade URLs hospedadas em domínios .app.

	2024	2025	
Uso fraudulento de marca	204.060	262.302	↑ +28,5%
Perfil falso em rede social	126.432	132.349	↑ +4,7%
App mobile falso	17.621	11.561	↓ -34,4%
Nome de domínio similar	248	2.954	↑ +1.091,1%
Uso de marca em busca paga	1.282	5.499	↑ +328,9%

Executivos e VIPs

> Detectamos mais de 19 mil incidentes envolvendo a imagem e as informações de Executivos & VIPs.

Criminosos podem se aproveitar da imagem e das informações de executivos e outras personalidades conhecidas em diversos cenários.

Os dados dos executivos podem alimentar golpes de Business Email Compromise (BEC), em que o golpista envia e-mails falsos para outros colaboradores da empresa ou parceiros comerciais. Se os destinatários acreditarem na mensagem, eles podem seguir orientações perigosas e até realizar movimentações financeiras indevidas.

Essas informações pessoais também podem ser usadas para elaborar fraudes contra os próprios executivos, criando um risco para a organização e seus sistemas internos.

> Detectamos cerca de 2 mil incidentes envolvendo a exposição de credenciais de executivos ou da alta direção das empresas.

Já a imagem dos executivos em perfis e no conteúdo falso das redes sociais pode ser usada para aumentar a credibilidade de algum produto ou serviço. Nessa questão, temos observado uma regionalização das fraudes que envolvem o endosso de oportunidades de investimentos, com a utilização da imagem de executivos conhecidos no país, como o apresentador Luciano Huck. Antes, esse tipo de golpe utilizava quase que exclusivamente a imagem de figuras internacionais, como Elon Musk.

O aprimoramento das ferramentas de inteligência artificial facilitou a criação de deep fakes convincentes, seja em imagens estáticas ou em vídeos. Com isso, muitas pessoas podem ter dificuldade para identificar que o conteúdo é falso. Em certos incidentes, o conteúdo falso pode estar apenas na legenda da foto, distorcendo o contexto da imagem para induzir a vítima ao erro.

Ameaças a executivos	Quantidade
Perfil falso em rede social	8.759
Exposição de informação pessoal	8.572
Exposição de credencial	2.460
Exposição de cartões	27
Total	19.818

Takedown agêntico: uma nova etapa na automação de resposta

> Até outubro de 2025, 343 mil casos de conteúdo fraudulento já tinham sido removidos graças às notificações automatizadas da Axur.

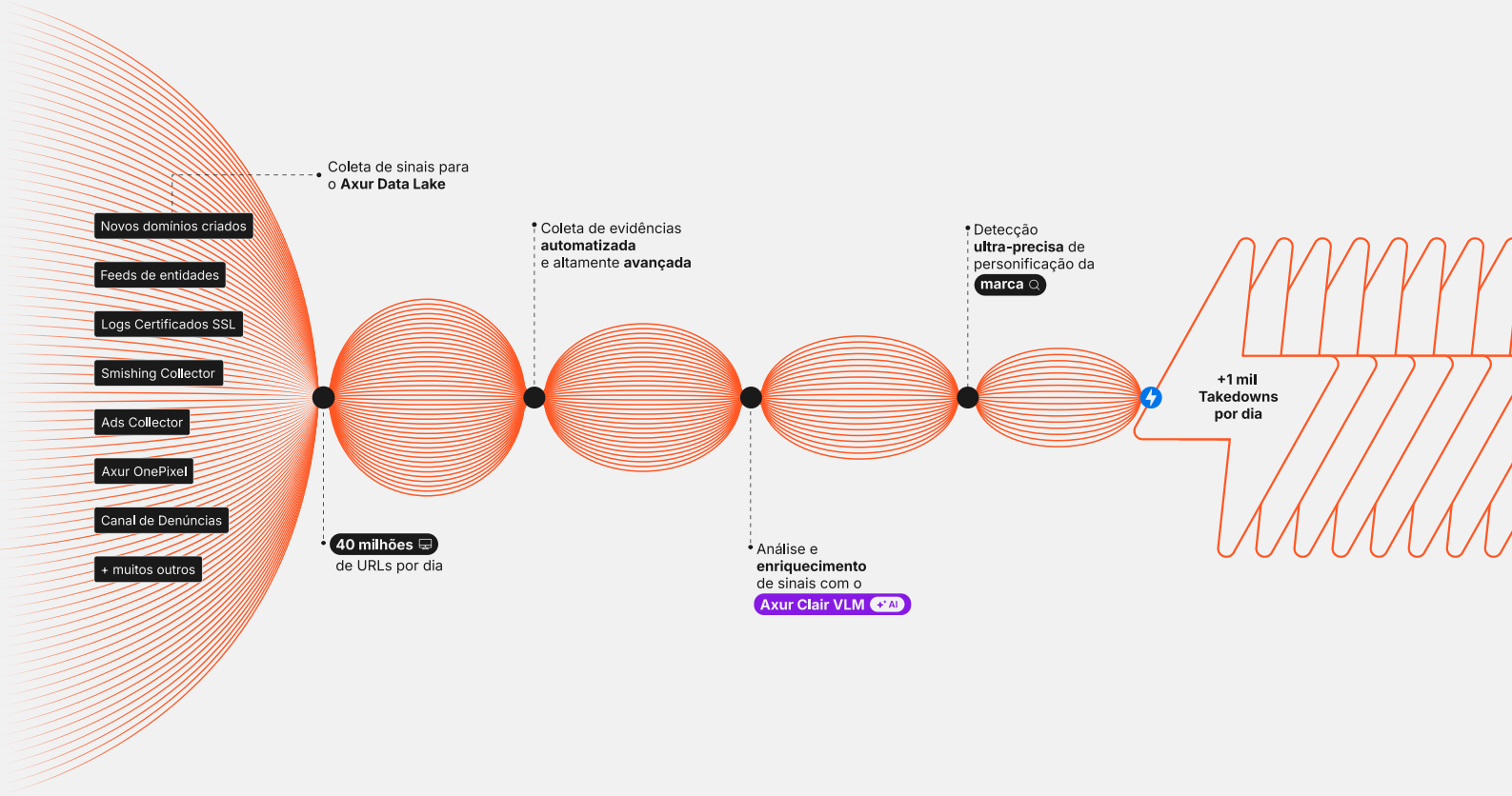
O volume, sustentado por fluxos baseados em IA e validação de evidências, consolidou a maturidade de um processo que hoje evolui para um novo paradigma: o takedown agêntico.

Diferentemente da automação tradicional, que executa tarefas pré-programadas com base em regras fixas, o takedown agêntico introduz capacidade de decisão autônoma. O modelo Clair, Cyber Lens for Anomaly and Impersonation Recognition, baseado em arquitetura Vision Language Model (VLM), interpreta tanto o conteúdo textual quanto os elementos visuais de cada página, identificando padrões de fraude, indícios de personificação e sinais de phishing mesmo quando a marca não é mencionada explicitamente.

A partir dessa análise contextual, o sistema é capaz de definir a ação cabível, notificar o provedor responsável e acompanhar as respostas, operando de forma contínua e com mínima intervenção humana. Trata-se de um modelo agêntico, no qual a IA não apenas detecta e reporta, mas decide e executa.

O diferencial está na integração entre análise multimodal e tomada de decisão automatizada, permitindo que o Clair conduza o ciclo completo de resposta, da identificação da ameaça à execução do takedown, com rastreabilidade e consistência.

É uma evolução que aproxima a segurança digital de um modelo verdadeiramente de mitigação de risco, tornando os processos mais rápidos, precisos e sustentáveis ao longo do tempo.

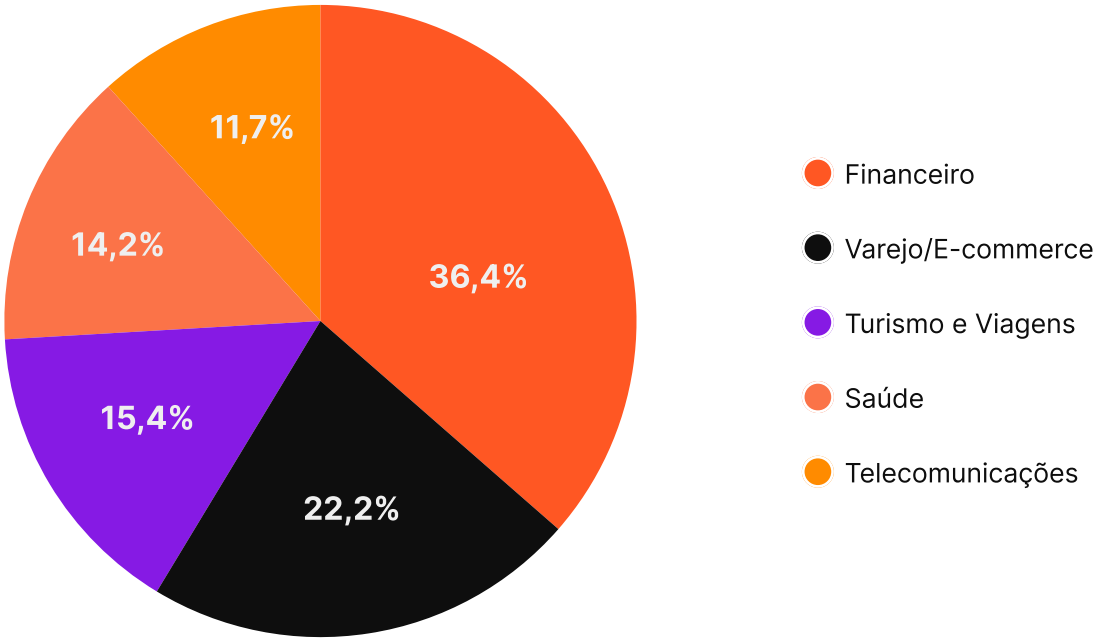


Takedowns por setor

A distribuição dos takedowns por setor mostra que o setor financeiro responde por 36,4% das remoções, mantendo-se como o principal alvo, um resultado em linha com o aumento das fraudes observadas no segmento ao longo do período. Em seguida aparecem varejo e e-commerce (22,2%), turismo e viagens (15,4%), saúde (14,2%) e telecomunicações (11,7%).

A predominância do setor financeiro reflete tanto a alta atratividade econômica das fraudes bancárias quanto a maior capacidade de detecção e resposta das instituições, o que se traduz em mais ações de takedown conduzidas no período.

Distribuição dos takedowns por setor entre outubro de 2024 e outubro de 2025



Plataformas mais notificadas

Em 2025, removemos mais de 70 mil perfis falsos através das notificações para a Meta, responsável pelas redes Facebook, Instagram, WhatsApp e Threads.

Tempo para a primeira notificação

O tempo para a primeira notificação é um dos indicadores mais críticos no ciclo de resposta a incidentes, pois determina a rapidez com que uma ameaça identificada chega à etapa de mitigação.

Os dados da plataforma Axur mostram que, em média, a primeira notificação é emitida entre três e cinco minutos após a solicitação de takedown. O tempo mais curto foi observado nos casos de nome de domínio similar (3,05 minutos) e distribuição não autorizada (3,02 minutos).

Reduzir o intervalo entre a detecção e a primeira notificação significa diminuir a janela de exposição, o período em que a ameaça permanece ativa e potencialmente acessível a vítimas.

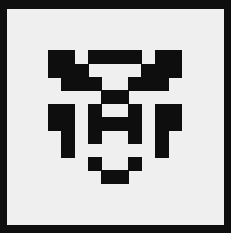
Em escala, essa diferença de poucos minutos pode representar milhares de acessos evitados a páginas falsas ou perfis fraudulentos, reforçando a importância do monitoramento automatizado e da priorização inteligente de alertas.

Tipo	1ª Notificação
Phishing	5,07 minutos
Perfil falso	3,22 minutos
Nome de domínio similar	3,05 minutos
Distribuição não autorizada	3,02 minutos
Venda não autorizada	3,78 minutos

Cyber Threat Intelligence com Inteligência Artificial

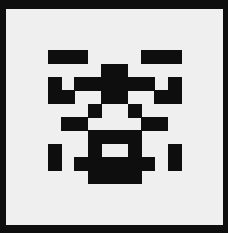
Por meio do módulo de Cyber Threat Intelligence da Axur, é possível acompanhar as ameaças mais relevantes e entender o panorama de ameaças de um período específico, como o recorte de 2025.

Atores maliciosos



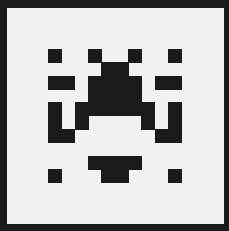
Scattered Spider

O Scattered Spider é um grupo ocidental que ganhou muita atenção em 2025 após diversos ataques bem-sucedidos contra empresas no Reino Unido. O grupo é conhecido por utilizar credenciais expostas e ataques de phishing (principalmente com voz) para obter essas credenciais ou fragilizar a autenticação multifator. Após formar uma suposta uma aliança com o ShinyHunters e LAPSUS$, o grupo também realizou uma campanha bem-sucedida de ataque a ambientes Salesforce, combinando phishing e a exploração de integrações com terceiros.



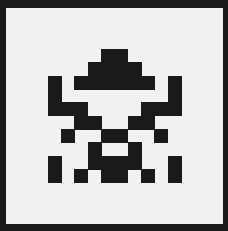
Qilin

O Qilin é uma quadrilha que opera na modalidade de ransomware como serviço (RaaS). Cada afiliado pode escolher seu próprio método para obter o acesso inicial aos alvos, o que significa que há uma diversidade considerável nas técnicas utilizadas. O grupo aparentemente concentrou atividades que antes eram de outros grupos, tornando-o possivelmente o nome mais ativo na categoria de ransomware no final de 2025.



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. O grupo reduziu suas atividades em abril.



Salt Typhoon

Muitos especialistas consideram que o Salt Typhoon está associado ao governo chinês. Ele se destacou em 2025 devido a uma série de ataques que começaram ainda em 2024, quando a imprensa noticiou que várias empresas de telecomunicação nos Estados Unidos teriam sido invadidas pelo Salt Typhoon. Este grupo é notório por atacar alvos de infraestrutura crítica (como telecomunicações e energia) e órgãos governamentais, geralmente com a finalidade de obter informações sobre terceiros.

Grupo em destaque no cenário brasileiro

Plump Spider

Em 2025, a Axur também acompanhou as movimentações do Plump Spider, grupo brasileiro sendo referenciado nos ataques às instituições financeiras.

Leia mais sobre as análises do grupo e seu modus operandi.

LEIA MAIS

CVEs em destaque

As principais vulnerabilidades de 2025 praticamente contam uma história: são falhas que começam em dispositivos de borda de rede e migram para o endpoints, onde o invasor então obtém o acesso administrativo para consolidar sua presença na rede corporativa.

CVE-2024-21762

EPSS 0.9291 | Actively exploited | NVD

9.8

Este CVE se refere a uma das diversas vulnerabilidades exploradas em dispositivos de borda ao longo de 2025. Esta falha estava presente em algumas versões do FortiOS e permite a execução de comandos a partir de solicitações específicas.

CVE-2024-55591

EPSS 0.94152 | Actively exploited | NVD

9.8

Este CVE se refere a mais uma vulnerabilidade no FortiOS. Quando realizado com sucesso, o ataque burla o processo de autenticação concede permissões administrativas ao invasor.

CVE-2025-53770

EPSS 0.87044 | Actively exploited | NVD

9.8

Informações técnica a respeito de uma vulnerabilidade no SharePoint vazaram para alguns atacantes que exploraram a brecha na modalidade de dia zero, ou seja, antes da correção ser distribuída pela Microsoft. Diversas empresas foram atacadas por grupos de hackers associados à China.

CVE-2025-29824

EPSS 0.00696 | Actively exploited | NVD

7.8

Este CVE trata de uma vulnerabilidade no Windows com impacto de elevação de privilégio. Pode ser utilizada por invasores para facilitar a movimentação lateral dentro de uma rede corporativa após a invasão e para instalar softwares maliciosos mais difíceis de detectar e remover.

CVE-2023-46805

EPSS 0.94377 | Actively exploited | NVD

8.2

Outra vulnerabilidade que burla o processo de autenticação em dispositivos de borda. O sistema afetado é o Ivanti Connect Secure (ICS), uma solução para acesso remoto (VPN). Essa vulnerabilidade pode concede um acesso inicial à rede corporativa.

CVE-2024-21887

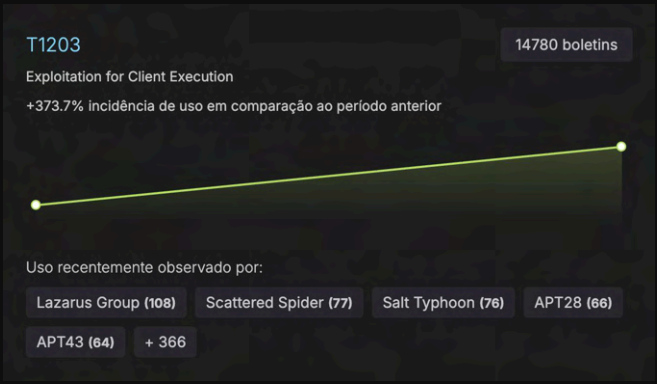
EPSS 0.9442 | Actively exploited | NVD

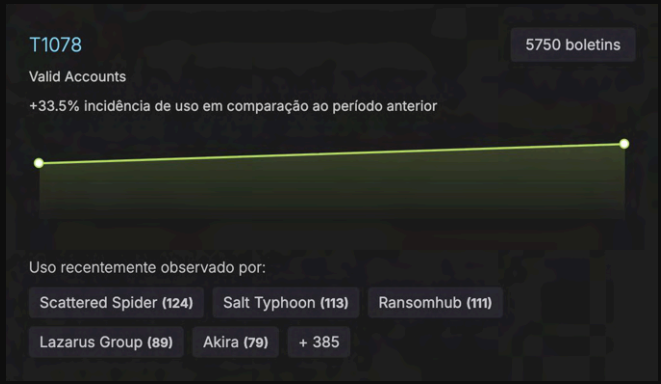
9.1

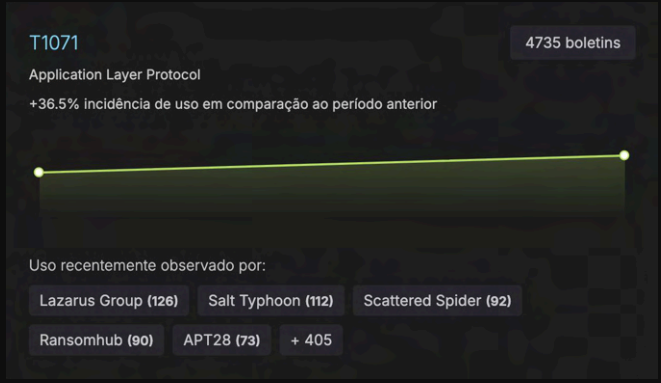
Mais uma vulnerabilidade no Ivanti Connect Secure. Neste caso, a falha está no processamento de solicitações específicas, permitindo que o invasor execute códigos arbitrários no sistema.

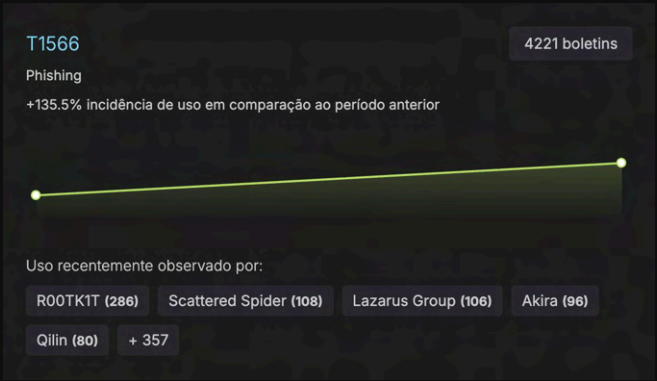
TTPs em destaque

As técnicas mais recorrentes em 2025 refletem a sofisticação crescente dos ataques: exploram vulnerabilidades em aplicações expostas ou de cliente para obter execução de código e acesso inicial (T1190, T1203), avançam com o uso de credenciais válidas (T1078) para manter persistência e escalar privilégios, e se consolidam com comunicações disfarçadas (T1071) e campanhas de phishing direcionadas (T1566) que garantem controle e movimentação lateral dentro da rede corporativa.









Malware em destaque

Os grupos de ransomware mais ativos de 2025 reforçam a consolidação do modelo “as a service”. Akira e LockBit mantêm alto volume de ataques com extorsão dupla, explorando credenciais válidas para acesso inicial, enquanto Ransomhub surge como sucessor de operações anteriores, ampliando o foco em vazamento de dados de alto valor.

Qilin se destaca pela sofisticação e customização do código, dificultando a análise defensiva, e Lumma Stealer, operando sob o modelo MaaS, concentra-se no roubo e revenda de credenciais, alimentando o ecossistema de acesso inicial.

Insight da plataforma Axur

Cyber Threat Intelligence

A complexidade atual da cibersegurança exige que as equipes filtrem, correlacionem e priorizem informações em meio a volumes massivos de dados. O CTI da Axur foi desenvolvido justamente para resolver esse desafio, combinando algoritmos de IA e um modelo de linguagem treinado em ameaças cibernéticas para transformar dados fragmentados em alertas curados e contextuais.

Diariamente, o sistema analisa centenas de fontes, como relatórios, feeds, grupos especializados e notícias, e identifica o que realmente é relevante para cada ambiente, mapeando ameaças e vulnerabilidades conforme a superfície de ataque de cada cliente.

Cenário geopolítico

Visão geral do cenário geopolítico

Acordos e parcerias internacionais foram fragilizados em 2025 por uma somatória de dificuldades.

De um lado, temos as barreiras regulatórias: tarifas comerciais, restrições em exportações, sanções financeiras, realinhamento de prioridades e novas legislações que entraram em vigor.

Do outro, temos os desafios concretos que motivaram essas medidas: os ataques cibernéticos contra a infraestrutura crítica, receios quanto ao domínio da China como fornecedora de peças, equipamentos e produtos em setores estratégicos, a disputa sobre a liderança tecnológica em inteligência artificial, a guerra entre a Rússia e a Ucrânia e a escalada de conflitos e incertezas no Oriente Médio.

Esses fatores contribuíram para a visão de que não basta proteger empresas ou setores específicos, uma vez que eles dependem de toda uma cadeia de fornecedores. Diversidade e redundância não seriam soluções viáveis, uma vez que todos se veem interligados por um número limitado de desenvolvedores de softwares e plataformas de TI.

Essa perspectiva despertou o debate sobre soberania digital, dando forma a uma nova onda de ideias e investimentos em infraestrutura de TI.

Embora as consequências sejam mais tangíveis no setor governamental e terceiros que trabalham com infraestrutura crítica, é possível que efeitos se espalhem para outros setores da economia.

A política e as tensões globais sempre impactaram os negócios, sobretudo nas empresas cuja atuação não se limita às fronteiras de um único país. Com a internet e os serviços digitais, temos um cenário em que quase todos dependem de softwares, de equipamentos e de serviços de tecnologia viabilizados por uma complexa teia de fornecedores globais.

Nessas circunstâncias, a relação entre as tensões geopolíticas e os desafios na área de cibersegurança tende a se ampliar.

> Uma evidência disso apareceu em uma pesquisa do Fórum Econômico Mundial publicada no início de 2025 em que 60% das empresas disseram acreditar que tensões geopolíticas impactaram sua estratégia de cibersegurança.

A relevância dessas tensões varia para cada empresa. Por isso, convém elencar os temas ligados à cibersegurança que se destacaram ao longo do ano e analisar quais consequências eles trouxeram para os diferentes setores da economia.

Ataques a infraestrutura crítica

A preocupação com a resiliência cibernética em elementos críticos de infraestrutura (energia, telecomunicações, água e logística) não é nova, mas os métodos utilizados para avaliar a maturidade do setor e as propostas de aprimoramento têm avançado de forma significativa.

Em 2024, o governo Biden deu início a uma revisão dos guindastes usados em portos americanos com o objetivo de substituir os modelos fabricados na China. Reguladores posteriormente citaram a presença de componentes eletrônicos não documentados com conectividade externa como uma das justificativas para essa medida.

Em paralelo, agentes de segurança do governo indicaram que invasores chineses estavam infiltrados nos sistemas de TI de várias empresas em setores críticos, sem dar exemplos específicos.

Em setembro de 2024, a imprensa, inicialmente através do Wall Street Journal, divulgou que hackers chineses vinculados Salt Typhoon obtiveram acesso a várias operadoras de telecomunicação. Apesar da gravidade do incidente, o que marcou esse ataque foi o interesse dos invasores: os clientes das operadoras.

Em 2025, testemunhamos os desdobramentos dessa campanha. Outros países começaram a publicar notas e boletins alertando sobre a atividade do Salt Typhoon nas operadoras de telecomunicação em seu território, muitas vezes explorando falhas nos chamados dispositivos de borda (edge devices) de marcas como Cisco, Ivanti e Palo Alto Networks.

> Em agosto, o FBI alertou que mais de 80 países foram atacados pelo Salt Typhoon.

No mesmo mês, o órgão alertou sobre atividade de outro grupo de hackers, desta vez associado à Rússia, que também estaria focado em operadores de infraestrutura crítica.

Tanto a China quanto a Rússia negam envolvimento com os ataques. Estejam os países diretamente envolvidos ou não, as invasões geram tensões e receios com consequências claras para as empresas envolvidas. Um exemplo se deu após uma reportagem do site ProPublica denunciar o envolvimento de engenheiros chineses em contratos do Departamento de Defesa, obrigando a Microsoft a prometer que não mais utilizaria essas equipes.

A ideia de "nacionalizar" serviços em prol da segurança nacional acabou chegando também em propostas ao legislativo norte-americano. Congressistas se debruçaram sobre regras para a compra de equipamentos e até para call centers, todas com potencial de impor barreiras à terceirização.

Ao mesmo tempo, órgãos de governo em vários países vêm estruturando avaliações de cibersegurança. Em dezembro de 2024, a Agência de Cibersegurança da União Europeia (ENISA) lançou seu primeiro relatório sobre o "estado da cibersegurança" no bloco.

O foco dessas medidas tende a ser a infraestrutura crítica e alguns órgãos governamentais. No entanto, elas já estão sendo estendidas às empresas que prestam serviços aos setores protegidos.

Comentário do especialista

Sérgio Costa

Pesquisador do
Axur Research Team.

Ao analisar os grupos hacktivistas, no contexto do conflito envolvendo Israel, Hamas e Irã, os grupos estão cada vez mais unidos por uma causa comum e possivelmente realizando ações coordenadas, com uma tendência crescente a visar infraestruturas críticas.

Apesar disso, ataques DDoS clássicos ainda são prevalentes. Alguns grupos estão citando o desenvolvimento de ransomwares, que podem servir como fonte de suporte financeiro para suas ações. A linha entre hacktivismo e atividades patrocinadas por estados-nação está se tornando cada vez mais tênue, levantando dúvidas sobre as verdadeiras motivações de certos grupos.

Conflitos regionais

A guerra entre a Rússia e a Ucrânia cria uma situação singular para os ataques cibernéticos. Ações bem-sucedidas são até comemoradas pelos canais que distribuem notícias do conflito, eliminando boa parte da dúvida sobre sua origem.

Ataques notórios foram realizados contra operadoras de telecomunicação da Ucrânia (Kyivstar) e da Rússia (Nodex, Lovit, Beeline, Rostelecom). Muitos dos incidentes envolvem DDoS e são realizados por hackers ditos "voluntários".

Outro cenário específico é o do Oriente Médio, com tensões envolvendo principalmente Israel, o Hamas e o Irã.

O Ministro de Inteligência do Irã chegou a anunciar que agentes do país tinham se infiltrado no programa nuclear israelense. De maneira geral, admissões dessa natureza são raras, e a dúvida não está mais na origem do ataque (como ocorre nas operações de espionagem que não são reconhecidas), mas sim na veracidade dos fatos narrados pelo atacante.

Houve também uma escalada nas tensões entre a Índia e o Paquistão, com quatro dias de conflito armado em maio. Nesse período, o Paquistão anunciou uma campanha de ataques cibernéticos contra a Índia para derrubar serviços e destruir arquivos. As hostilidades terminaram com um acordo de cessar-fogo.

Desafios de supply chain

Ataques ligados a tensões geopolíticas nem sempre são os únicos que utilizam uma determinada estratégia, mas é comum que eles adotem essas estratégias conhecidas com uma finalidade diferente ou com mais sofisticação.

Isso não é diferente para os ataques a cadeias de fornecedores (supply chain). Enquanto as campanhas de ataques a terceiros realizados por criminosos buscam por dados corporativos e procuram por uma chance de extorquir as vítimas, os ataques a operadoras de telecomunicação têm a finalidade de coletar informações sobre alvos de interesse geopolítico.

Além dos ataques a operadoras de telecomunicação em dezenas de países, há relatos de que provedores de internet em Moscou também teriam sido atacados para facilitar a espionagem das embaixadas instaladas na capital russa.

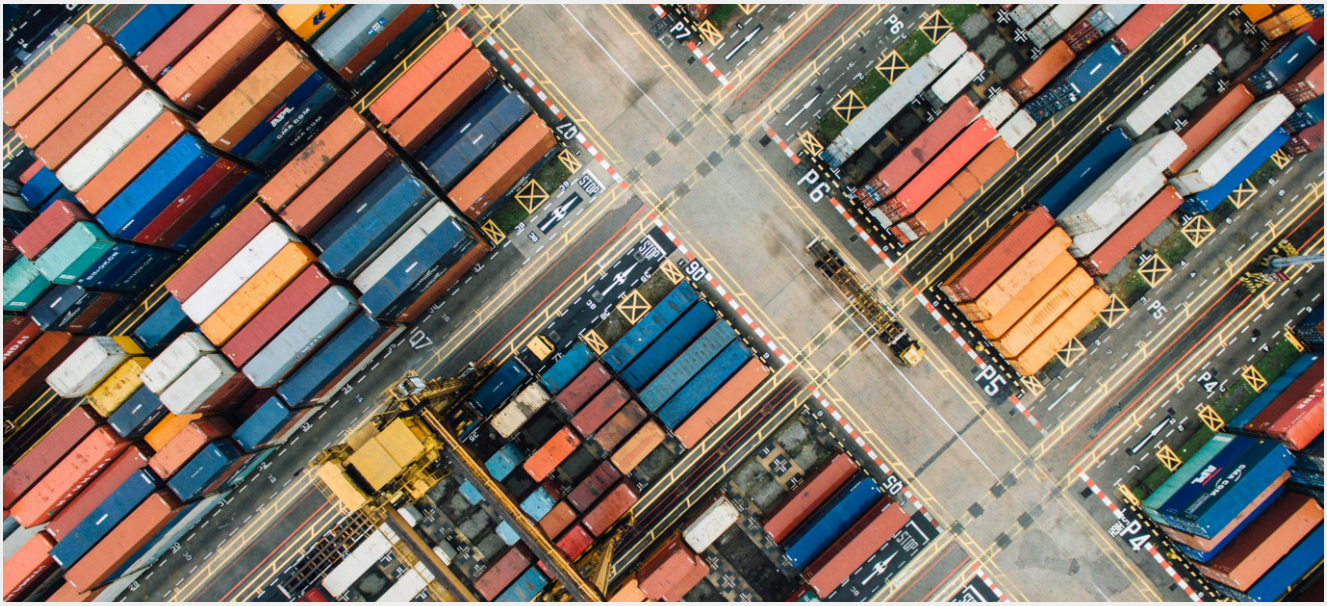
Ao contrário dos criminosos, que buscam os alvos mais rentáveis e vulneráveis, ataques para fins de espionagem patrocinados por governos podem estudar com mais calma um alvo e encontrar brechas menos expostas.

Operadores de infraestrutura crítica são um alvo valioso e atuam como um "fornecedor" para uma grande parcela das empresas e indivíduos, o que ajuda a explicar essas ações. Contudo, vale lembrar que o incidente da SolarWinds também foi atribuído a um grupo patrocinado por um governo (a Rússia).

> Por isso, é justo concluir que qualquer empresa particular que preste serviço para alvos de interesse geopolítico pode se tornar alvo desses ataques.

A ideia é evitar um cenário em que as autoridades desses países decidam distribuir softwares comprometidos ou hardware sabotado. A operação dos pagers explosivos do Oriente Médio já havia demonstrado esse risco em 2024.

Mais recentemente, temos visto casos como os impedimentos a engenheiros chineses em contratos governamentais dos Estados Unidos e a decisão da Microsoft de reduzir o acesso chinês a informações do Microsoft Active Protections Program (MAPP), uma plataforma que traz informações prévias sobre vulnerabilidades que logo serão corrigidas.



A decisão da Microsoft de limitar o acesso chinês ocorreu após uma vulnerabilidade do SharePoint compartilhada através do MAPP ser explorada antes da distribuição do patch. Com a falha sem correção, hackers (que seriam chineses, segundo as análises dos incidentes) conseguiram acesso fácil a centenas de empresas.

A China é o principal alvo dessas medidas, mas o país asiático também trabalha para não depender mais de software e hardware americano. O governo chinês inclusive recomendou que empresas de tecnologia locais não adquirissem os chips H20 da Nvidia, que foram desenvolvidos para contornar as restrições de exportações de hardware de IA.

Há, no entanto, uma série de medidas mais neutras visando aumentar a resiliência cibernética, como a adoção de Software Bill of Materials (SBOMs) e outras metodologias de gestão de risco de terceiros.

Ao mesmo tempo, ações na Justiça vêm tentando derrubar a ideia de que é possível terceirizar o risco, responsabilizando o contratante por não fiscalizar o trabalho realizado em seu nome. Essas medidas visam a criação de um cenário em que as próprias empresas demandam uma preocupação maior de segurança por parte de seus fornecedores, o que contribui para resiliência cibernética de setores inteiros da economia.

O roubo de US$ 1,5 bilhão

Muitos dos ataques patrocinados por governos são realizados para fins de espionagem. No entanto, os hackers da Coreia do Norte divergem desse padrão, atuando principalmente para obter recursos e financiar o regime.

Em março, a corretora de criptomoedas ByBit sofreu um ataque cibernético do Lazarus, um notório grupo norte-coreano. A ação, que foi considerada o maior roubo da história, resultou no desvio de US$ 1,5 bilhão de fundos da corretora.

O ataque foi possível porque os invasores comprometeram um fornecedor da ByBit, a Safe {Wallet}. O primeiro alvo do ataque foi um engenheiro da Safe que, segundo algumas evidências, pode ter sido vítima de phishing. Com acesso ao sistema desse engenheiro, os invasores então obtiveram uma chave do armazenamento em nuvem da Safe para adulterar um código JavaScript em sua plataforma. O código comprometeu uma carteira da ByBit.

Esse incidente ilustra as complexidades técnicas dos ataques de supply chain, a persistência dos hackers patrocinados por governos e a forma como os riscos de terceirização muitas vezes extrapolam os limites imaginados pelas metodologias de gestão de risco.

Soberania digital e resiliência

O conceito de "soberania digital" não é exatamente novo, mas não foi por mera coincidência que investimentos em datacenters nacionais e soberanos foram anunciados no mesmo ano em que o governo dos Estados Unidos decidiu adquirir parte da Intel.

Essencialmente, a ideia de soberania digital defende que um país tenha independência para cuidar de suas necessidades de TI, tanto em termos de infraestrutura como na gestão e regulamentação.

Países que têm alguma capacidade de fabricação de semicondutores de ponta estão tomando medidas para fortalecer a cadeia produtiva do setor ou atrair novos investimentos. Nos Estados Unidos, isso começou ainda em 2023 com a lei CHIPS. Já em 2025, a fabricante de memórias japonesa Kioxia anunciou que desligaria terceiros que não conseguissem uma pontuação satisfatória em uma avaliação de segurança, possivelmente refletindo novas demandas de clientes e reguladores.

Enquanto isso, os Estados Unidos assumiram o controle de 10% da fabricante de processadores Intel – uma rara intervenção direta do governo norte-americano que ajudou a estabilizar o valor de mercado da empresa.

Mas, tendo em vista a complexidade da fabricação de semicondutores, muitos países não têm condições de replicar a cadeia de produção da infraestrutura de TI, mesmo contando com aliados estratégicos. Sendo assim, uma alternativa é garantir a presença de ativos em território nacional e a capacidade de gestão e regulamentação.

Com a aprovação do CLOUD Act em 2018, críticos questionaram a independência dos provedores norte-americanos, apontando que eles seriam obrigados a cumprir ordens e entregar informações em desacordo com a legislação local. Com a migração para a nuvem, a influência norte-americana deixou de se limitar a serviços pontuais como e-mail ou chat e colocou toda a infraestrutura de TI sob uma jurisdição externa.

Durante a pandemia do coronavírus, a nuvem foi o caminho natural para que as empresas pudessem continuar funcionando com trabalho remoto e evitassem a aquisição de hardware, que estava com preço elevado em decorrência da suspensão do funcionamento das fábricas e a demanda por equipamentos.

Essa consolidação reforçou as preocupações associadas ao CLOUD Act. No entanto, o avanço da inteligência artificial, com seus elevados requisitos computacionais, trouxe um elemento ainda mais urgente ao tema.

Um fato notável em 2025 foi a suspensão temporária do endereço de e-mail de um procurador do Tribunal Penal Internacional em resposta a uma sanção do governo dos Estados Unidos. Como o e-mail era um serviço de nuvem da Microsoft, o episódio levantou questões sobre a privacidade e sobre como provedores de nuvem estrangeiros respeitariam as leis europeias.

Os provedores norte-americanos reagiram e se comprometeram com uma infraestrutura soberana, mas não puderam negar que estavam sujeitos às decisões do governo e dos tribunais dos Estados Unidos. Isso significa que eles teriam, sim, de entregar dados às cortes americanas, mesmo que os dados estivessem armazenados em território europeu.

Com esse recado, algumas empresas anunciaram novos investimentos em infraestrutura soberana na Europa, de olho no mercado governamental e na demanda por mais segurança jurídica.

Esse movimento não se restringe à Europa. A China tem iniciativas semelhantes para reduzir a dependência em hardware e software norte-americano, enquanto o Brasil está investindo em uma Nuvem de Governo, em infraestrutura de computação para inteligência artificial e em pesquisas na área de semicondutores.

Consequências para a cibersegurança

Visto de forma isolada, a soberania digital parece ser uma questão política e abstrata. Contudo, esse tema está ligado a questões de governança, segurança nacional e resiliência cibernética.

Do ponto de vista de resiliência, a consolidação da infraestrutura de TI em apenas alguns provedores traz riscos significativos, já que todos os serviços atrelados a esses provedores podem sofrer interrupções ou violações simultaneamente. A gestão de risco também é dificultada, uma vez que os mecanismos para compensar esse risco sistêmico serão mais complexos. Dependendo das prioridades e dos métodos, a mitigação dos riscos de um apagão cibernético generalizado pode ser mais cara do que o custeio de uma infraestrutura distribuída.

O tema de risco sistêmico está vinculado a outro assunto mais próximo do dia a dia das empresas: a cadeia de fornecedores e terceiros (supply chain).

Além de computadores e softwares, datacenters precisam de fornecedores para serviços de resfriamento, energia e conectividade – e tudo isso deve entrar na conta para uma infraestrutura confiável. Nesse sentido, incidentes de supply chain podem acalorar a discussão de soberania digital na mesma medida em que a regulamentação desse tema pode trazer impacto para a gestão de riscos atrelados a fornecedores.

Infelizmente, não há como prever o futuro, especialmente diante da instabilidade geopolítica atual. É possível, por exemplo, que o tema de soberania digital siga por um rumo mais político, com acordos multilaterais e mecanismos de colaboração internacional para proteger a jurisdição de cada país.

Por outro lado, também é possível que ela se desdobre em ações com impacto direto nos negócios e na estratégia de cibersegurança. Um exemplo é a criação de incentivos para adoção de software, hardware e infraestrutura dedicados ao aprimoramento da governança cibernética.

Perfil do cibercrime brasileiro

O cibercrime brasileiro é marcado pela predominância de fraudes diretas contra consumidores. Diversas abordagens de engenharia social são utilizadas para manipular as vítimas e obter informações sensíveis ou distribuir diversos tipos de malware.

Ainda que os golpes raramente impressionem do ponto de vista técnico, não se pode ignorar a tenacidade dos criminosos e a multiplicidade de narrativas na elaboração de golpes de phishing. Igualmente notável é a capacidade das quadrilhas de utilizar técnicas simples de modo eficaz e de conduzir os elementos offline do crime, como o saque dos recursos e lavagem de dinheiro.

De todo modo, essa concepção vem se mostrando incompleta para descrever o cibercrime brasileiro nos últimos anos. Dando continuidade a essa tendência, várias ações criminosas em 2025 demonstraram um nível considerável de sofisticação técnica.

> Além disso, os golpes de engenharia social estão atingindo cada vez mais as empresas, não apenas os consumidores. Essa transformação não se resume a uma mudança na categoria dos alvos.

É claro que pessoas jurídicas podem sofrer as mesmas fraudes financeiras que consumidores, mas empresas também se ligam a outras empresas e aos próprios consumidores, o que abre um grande leque de possibilidades para fraudes. Os ataques de supply chain (cadeia de fornecedores) são uma tendência global que também apareceu no cenário brasileiro.

Ações que marcaram 2025

Invasão de prestadores de serviços de instituições financeiras para atacar a infraestrutura do Pix

Malware mobile para fraudes com cartão de crédito através de NFC

Ataques de engenharia social contra empresas para a instalação de softwares de acesso remoto

WhatsApp: malware capaz de se propagar e fraudes com dados de comércio eletrônico

Ataques a PSTIs do sistema bancário

Hackers conseguiram acesso a provedores de serviços de tecnologia da informação (PSTIs) autorizados pelo Banco Central para desviar recursos das contas especiais mantidas pelas instituições financeiras.

O valor total movimentado nas duas principais ações supera R$ 1 bilhão, mas parte dos recursos foi bloqueada ou recuperada antes de sair do sistema financeiro nacional. Como os ataques atingiram empresas que prestam serviços às instituições financeiras, não houve uma só vítima em cada incidente.

No primeiro incidente, que atingiu a C&M Software, os hackers subornaram um funcionário da empresa para obter uma credencial de acesso e informações sobre a operação do sistema. A tática de subornar colaboradores já era recorrente no Brasil, mas foi a primeira vez que um ataque desse tipo conseguiu atingir vários bancos e movimentar quantias tão significativas.

No segundo incidente, os invasores acessaram os sistemas da Sinqia/Evertec. A empresa informou que o acesso não autorizado ocorreu por meio da credencial de um terceiro, demonstrando mais uma vez o risco de ataques a fornecedores.

Essas ações demonstram que os criminosos brasileiros não estão mais se limitando a ações em pequena escala contra consumidores. É possível que as lições aprendidas com esses ataques viabilizem ações ainda mais arrojadas no futuro, destoando do perfil tradicional do cibercrime brasileiro.

Requisitos do Banco Central

Após os incidentes que atingiram Provedores de Serviços de Tecnologia da Informação (PSTIs) e as instituições financeiras conectadas através deles, o Banco Central publicou a Instrução Normativa n° 664 e a Resolução n° 498 para aprimorar os requisitos mínimos exigidos dessas instituições.

Entre as exigências, o Banco Central lista o monitoramento de informações relevantes na Deep & Dark Web e em "grupos privados de comunicação". Esses dados de Cyber Threat Intelligence ajudam as empresas a detectar, prevenir e investigar incidentes.

Varreduras periódicas do ambiente de TI e a gestão de certificados digitais também constam na lista do Bacen. A gestão da superfície externa (External Attack Surface Management – EASM) deve ser considerada para essa finalidade no contexto dos ativos expostos à internet.

Com esses e outros requisitos, o Bacen trouxe algumas das práticas recomendadas de segurança da informação para aprimorar a resiliência do sistema financeiro nacional.

Engenharia social

Os golpes por e-mail permanecem relevantes no cibercrime brasileiro, mas cabe apontar alguns fatos interessantes que demonstram a exploração de outros canais.

Um deles é a apreensão de mais um "carro do SMS". A polícia já havia encontrado um veículo equipado com sistemas para transmitir mensagens na rede celular em 2024, e isso aconteceu novamente em 2025. Como o nome sugere, esses veículos difundem mensagens com números de telefone ou endereços fraudulentos para roubar informações das vítimas.

Comentário do especialista

Nesse contexto, cabe destacar também os golpes com Unidades de Resposta Audível (URAs) falsas e chamadas em massa. Esses golpes não são novos, mas estão muito frequentes, e algumas pessoas podem receber várias ligações ou mensagens se passando por instituições e indivíduos confiáveis.

Laís Clesar

Gerente do Axur Research Team

Outra campanha notória são os ataques de vishing (phishing por voz, com chamadas telefônicas) em que os criminosos convencem as vítimas a instalarem um programa de administração remota como SoftEther VPN, Ammyy Admin, DWAgent, HopToDesk, RustDesk, Supremo ou TeamViewer.

Esses ataques também atingem empresas, embora não seja possível descartar que os colaboradores tenham sido aliciados pelos criminosos e tenham ciência do que estão fazendo.

Outro golpe relevante do ano foram as fraudes por WhatsApp que utilizaram dados de logística do comércio eletrônico. Nesse golpe, a vítima recebe um aviso de que é preciso resolver uma pendência (normalmente com um pagamento) para receber uma encomenda.

Fraudes envolvendo pendências falsas em pacotes e encomendas não são novas, mas esse golpe se destacou pelo uso de dados legítimos. O nome do comprador, o código de rastreamento e o endereço de entrega estavam presentes na mensagem enviada às vítimas.

Além disso, os criminosos usavam a transportadora responsável pela entrega como remetente da mensagem enviada por WhatsApp, o que significa que eles também sabiam o número de telefone do consumidor. Como a fraude não se limitou a nenhuma transportadora ou loja específica, é seguro supor que os hackers conseguiram acessar dados em algum sistema intermediário onde essas informações são armazenadas.

Malware: NFC e WhatsApp

Os criminosos brasileiros têm atualizado sua estratégia de empregar cavalos de Troia para roubar credenciais de contas bancárias ou mesmo realizar transferências a partir dos sistemas das vítimas. Com a migração dos correntistas para os dispositivos, os códigos maliciosos migraram também.

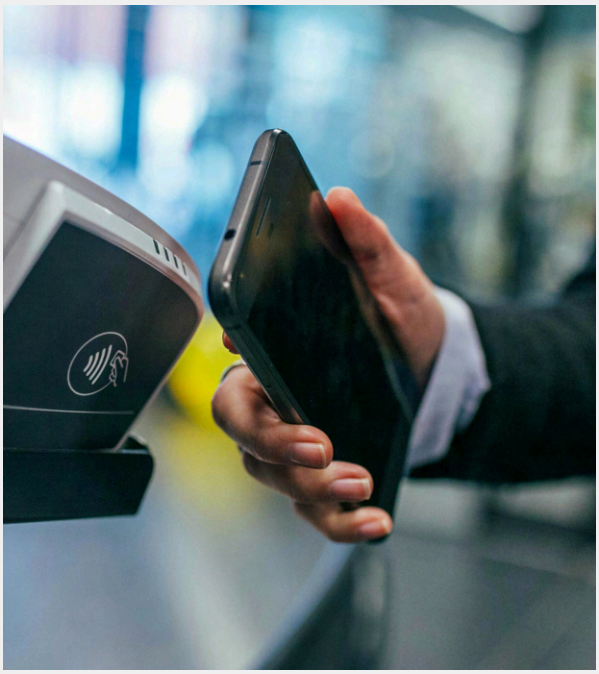
Alguns dos programas maliciosos para Android utilizam os recursos de acessibilidade do sistema para ganhar acesso ao conteúdo da tela e simular gestos e a digitação, assumindo o controle do aparelho e exibindo telas falsas para roubar informações da vítima. Já outros buscam obter credenciais, redirecionar usuários para sites de phishing, entre outros objetivos.

No entanto, um tipo de fraude diferente apareceu no Brasil em 2025: um malware que atua como um proxy de NFC, lendo o cartão de crédito da vítima e transferindo dados para um terminal de pagamento.

> O malware foi chamado de PhantomCard.

Para convencer a vítima a aproximar o cartão do aparelho, o malware conta com uma narrativa de engenharia social, informando que o aplicativo vai "proteger" o cartão de alguma forma. Essa é uma das roupagens do ataque que usa o malware, mas pode ter diversas variações a depender do ator malicioso que estiver operando a campanha. Esse pretexto para ler o cartão pode ser modificado, mas será sempre necessário convencer a vítima a tomar essa ação.

Esse golpe já havia sido aplicado em 2024 em outras regiões. O surgimento dele no Brasil aponta que pode estar ocorrendo uma "importação" das táticas para dentro do território brasileiro, ou que os criminosos nacionais estão recebendo apoio técnico de quadrilhas estrangeiras.



Por fim, mais um malware diferenciado em 2025: um código capaz de se propagar pelo WhatsApp, enviando uma mensagem aos contatos das vítimas contaminadas. Esse malware realiza o envio das mensagens pelo WhatsApp Web em sistemas Windows.

Algumas amostras não funcionam em dispositivos móveis. Para contornar essa limitação, a mensagem maliciosa diz à vítima que o anexo só pode ser aberto no computador – uma alegação falsa, pois o anexo pode ser aberto no celular, onde é inofensivo. No entanto, essa afirmação da mensagem pode ser convincente para os usuários, uma vez que o próprio WhatsApp exibe avisos sobre conteúdos que só podem ser visualizadas no celular (mensagens de visualização única são um exemplo).

Quando aberto no Windows, o malware inicia uma sequência de instalação que resultará na instalação de um malware que monitora a navegação do usuário para roubar credenciais bancárias. O código também sequestra a sessão do WhatsApp para reenviar a mensagem maliciosa aos contatos da vítima.

Tendências

Agentes de IA

A visão de que a inteligência artificial poderia realizar ações por conta própria sempre esteve presente. No entanto, os primeiros produtos com esse conceito tinham um caráter um tanto experimental, tanto pela utilidade limitada como pelos riscos de deixar a IA encarregada de tomar ações críticas.

Os agentes de IA amadureceram ao longo de 2025 com a disponibilização e o aprimoramento de produtos dinâmicos voltados a todos os segmentos do mercado. Alguns dos avanços mais rápidos foram observados em tarefas de desenvolvimento de software, em que IAs começaram a encontrar bugs e vulnerabilidades juntamente com os respectivos relatórios para comunicá-los aos desenvolvedores.

> A popularização do termo "vibe coding" é um reflexo dessa tendência.

Como era de se esperar, inovações semelhantes surgiram nas técnicas de ataque. Pesquisadores têm demonstrado formas de explorar a interpretação da IA que aliam injeções de prompts maliciosos e APIs para produzir resultados indesejados.

Os riscos incluem vulnerabilidades mapeadas logo após o lançamento de browsers como o Perplexity Comet e o ChatGPT Atlas, da OpenAI.

Um dos ataques divulgados ao Comet usava esteganografia, texto invisível embutido em páginas da web, que é lido pelo mecanismo de OCR do navegador e enviado diretamente ao sistema de IA sem validação. Isso possibilita que invasores executem ações não autorizadas, como roubo de dados, acesso a contas e comprometimento de sistemas corporativos.

Já o navegador da OpenAI estava vulnerável à injeção persistente de comandos maliciosos na memória do assistente, possibilitando execução arbitrária de código e escalonamento de privilégios. Os dois casos mostram que os agentes também se tornam uma superfície de ataque crítica às empresas.

> Devido ao potencial dos agentes de IA, muitas empresas podem começar a procurar maneiras de integrá-los em seus fluxos, trazendo toda a discussão técnica sobre esses agentes para dentro do ambiente corporativo e, portanto, criando desafios para proteger esses sistemas.

A adoção de agentic AI dentro das organizações não se resume à experimentação; representa uma mudança de paradigma operacional. Ao evoluírem de copilotos para sistemas autônomos com capacidade de decisão e execução, esses agentes passam a integrar diretamente o ciclo de resposta: detectar, decidir e agir.

Essa autonomia exige uma arquitetura de governança sólida, baseada em restrições, aprovações, isolamento e trilhas de auditoria que assegurem rastreabilidade e reversibilidade das ações.

Empresas que pretendem incorporar agentes autônomos precisam alinhar identidades de máquina, políticas de privilégio mínimo e mecanismos de supervisão humana para evitar execuções indevidas ou escalonamentos não autorizados. O risco não está apenas nas alucinações dos modelos, mas na execução de comandos válidos em contextos errados, o que demanda métricas de observabilidade e auditoria em tempo real.

Além disso, a disseminação de agentes fora do controle corporativo, impulsionada pelo shadow IT, amplia a superfície de exposição. Mesmo sem integração oficial, esses agentes podem interagir com sistemas críticos ou dados sensíveis, tornando indispensável

> uso de controles de identidade dinâmicos, isolamento de ambientes e monitoramento contínuo das interações entre agentes e APIs corporativas.

Em 2026, a maturidade em segurança será definida pela capacidade de equilibrar autonomia e controle, permitindo que a IA atue com agilidade, mas dentro de limites verificáveis, auditáveis e reversíveis.

Os times de cibersegurança precisarão ficar atentos a esses movimentos para prestar o apoio necessário, visando um uso consciente e seguro desses agentes para fortalecer o negócio.

Uso por atores maliciosos

Se temos o "vibe coding", temos também o "vibe hacking". Modelos de IA podem detectar vulnerabilidades para deixar softwares mais robustos, mas criminosos podem se valer da mesma ideia para encontrar novas vulnerabilidades com o intuito de explorá-las.

Da mesma forma, criminosos podem usar IAs para facilitar o desenvolvimento e a adaptação de códigos maliciosos, ou para reestruturar artefatos com o intuito de evitar a detecção por ferramentas de segurança, como EDR, XDR, filtros de spam e IDS.

Agentes de IA e suas identidades também podem ser explorados por criminosos que obtiveram acesso à rede corporativa, criando um canal para a movimentação lateral que não estará necessariamente limitado pela segmentação de rede tradicional.

Conforme o uso da IA cresce entre os invasores e dentro das empresas, a necessidade de adotar a IA como aliada na cibersegurança vai ficando cada vez mais clara.

> Existem muitas tarefas de cibersegurança que hoje não recebem a devida atenção, principalmente pela dificuldade de priorizar alertas e a auditoria de eventos.

Isso faz com que muitos alertas sejam ignorados ou analisados apenas superficialmente, inclusive em ambientes de SOC.

Somente 9% das organizações monitoram 100% da sua superfície de ataque (IBM) e 28% dos profissionais de cibersegurança usam IA para reduzir os falsos positivos.

(ISC2 2024 Cybersecurity Workforce Study).

Por essa razão, é provável que muitos comecem a explorar agentes de IA como forma de melhorar o entendimento dos eventos em sua infraestrutura para agilizar a detecção e a resposta a incidentes.

A capacidade da IA de vincular alertas internos a bases de dados enriquecidas com inteligência em ameaças tem potencial para ampliar significativamente a qualidade dos alertas que chegam às equipes de cibersegurança.

Adotar agentes de IA na cibersegurança também é uma oportunidade para entender os requisitos dessa tecnologia e as soluções para integrá-la com segurança à infraestrutura de TI. Esse aprendizado pode ser compartilhado com as demais áreas do negócio e guiar a adoção de IA nos mais variados processos.

Insight da plataforma:
Axur Command

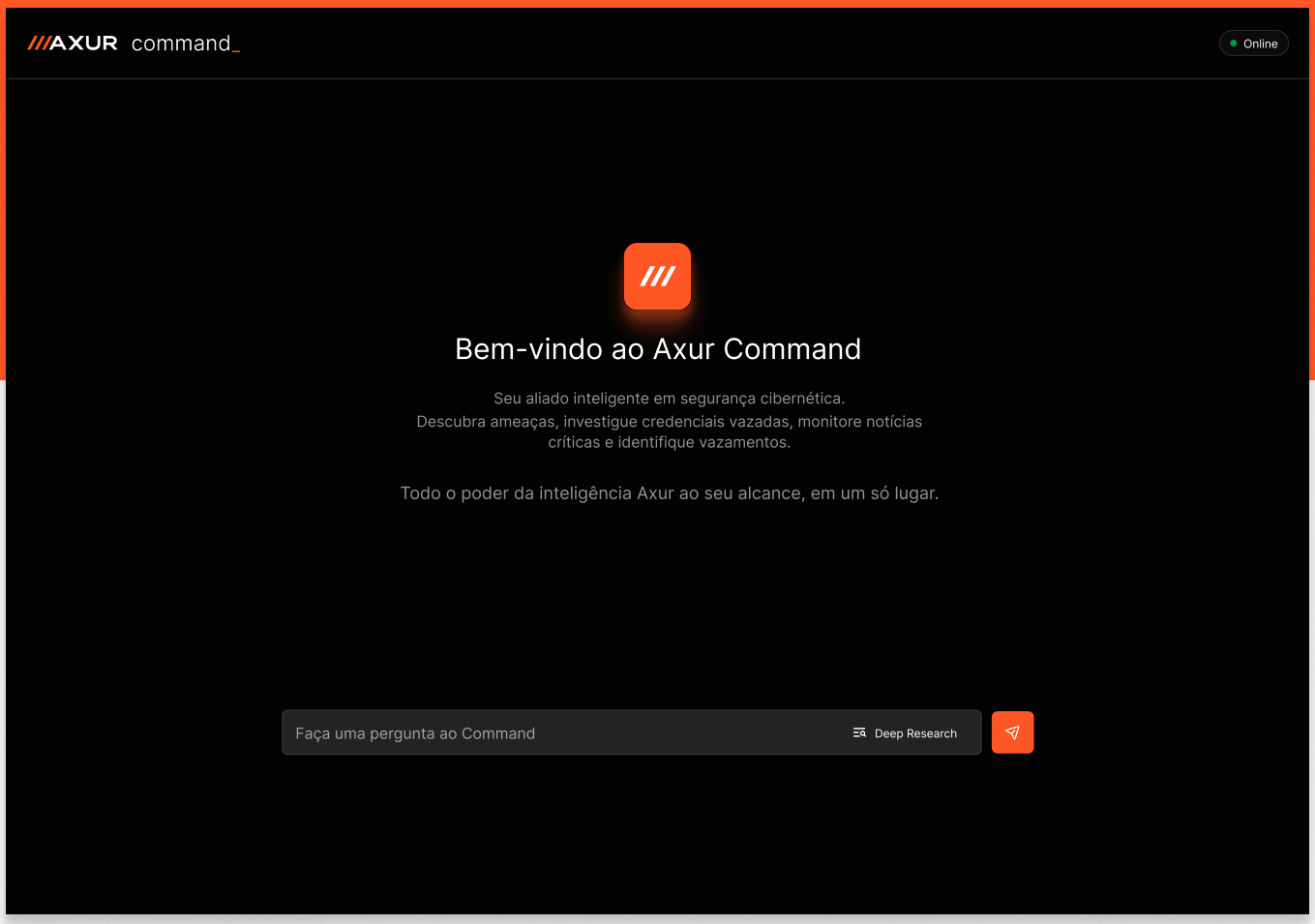
O Axur Command introduz um novo paradigma de automação em cibersegurança: um centro de comando que orquestra agentes de IA especializados para correlacionar alertas, eliminar falsos positivos e executar respostas coordenadas em tempo real.

A solução conecta diferentes fontes — como SIEM, EDR, CTI e EASM — em um fluxo único de detecção e resposta, reduzindo o tempo de análise e a sobrecarga das equipes de segurança.

Entre suas principais capacidades estão:

Automação de tarefas de Tier-1, com agentes que triagem alertas e priorizam incidentes.

Correlação em tempo real entre múltiplas origens de dados, revelando o contexto completo das ameaças.



Regulamentação

Quando algo tem impactos sociais significativos, é natural que diversas forças da sociedade civil se movimentem para estabelecer regras. Esse regramento pode vir em uma lei, em iniciativas voluntárias ou em órgãos de autorregulamentação estabelecidos pelos interessados.

Essa dinâmica também vale para a tecnologia, é claro. A evolução veloz da inteligência artificial furou a bolha do mundo da tecnologia para atrair também a atenção do mundo político. Diversas leis já foram aprovadas ou estão em discussão, e não é fácil prever quais novas discussões poderão surgir em 2026. Apesar do protagonismo da IA, não é só ela que está sendo examinada por reguladores.

A presença crescente das seguradoras no mercado de cibersegurança vem promovendo uma discussão maior sobre a responsabilidade pelos danos decorrentes dos incidentes de segurança. Pagar o resgate em ataques de ransomware pode ficar mais complicado. A mudança de regras dentro do próprio setor também é algo esperado para 2026. Um exemplo disso é o plano do Google para limitar o sideloading de aplicativos de Android com um cadastro obrigatório para todos os desenvolvedores. O Brasil deve ser um dos primeiros países a ser submetido à nova regra, que tem o objetivo de reduzir o volume de ataques com aplicativos falsos.

Qualquer mudança abrangente na forma como usamos a tecnologia tem o potencial para transformar também as ameaças.

Soberania digital e de dados

A temática da soberania digital ganhou bastante relevância ao longo de 2025, uma vez que o clima geopolítico vem deixando muitos países preocupados com a independência da sua infraestrutura tecnológica e a capacidade de manter o controle sobre dados armazenados em nuvens de escala global.

> Os objetivos da soberania digital podem impactar a infraestrutura de TI e criar desafios de governança e conformidade. Essas mudanças têm impacto certo na cibersegurança, que precisará estar envolvida em todo o processo.

Ao menos em parte, essa discussão pode ser compreendida como um desdobramento do abalo que a logística internacional e o comércio mundial sofreram a partir da pandemia da Covid-19. Ao fim da pandemia, observamos neste relatório que o trabalho remoto e a pressão sobre os fornecedores de semicondutores levaram as cadeias de fornecimento dos equipamentos de TI ao limite, aumentando a demanda pela nuvem e diminuindo o controle que as empresas tinham sobre seu próprio hardware.

A soberania digital reúne debates sobre o mercado, o acesso à tecnologia e a segurança nacional. As consequências para as empresas aparecem no desenho da infraestrutura de TI, que possivelmente terá de ser segregada para clientes de diferentes países, dependendo de como as conversas a respeito da soberania avançarem.

Por outro lado, os investimentos em infraestrutura que começaram já em 2025 devem começar a mostrar resultados em 2026, criando oportunidades para as empresas que estiverem prontas e seguras para esse desafio.

Internet das coisas e tecnologia operacional (OT/IoT)

A Internet das Coisas (IoT) e a Tecnologia Operacional (OT) criam desafios constantes para as equipes de cibersegurança. Esses equipamentos nem sempre têm um software robusto, e às vezes são abandonados pelos fabricantes muitos anos antes de serem substituídos.

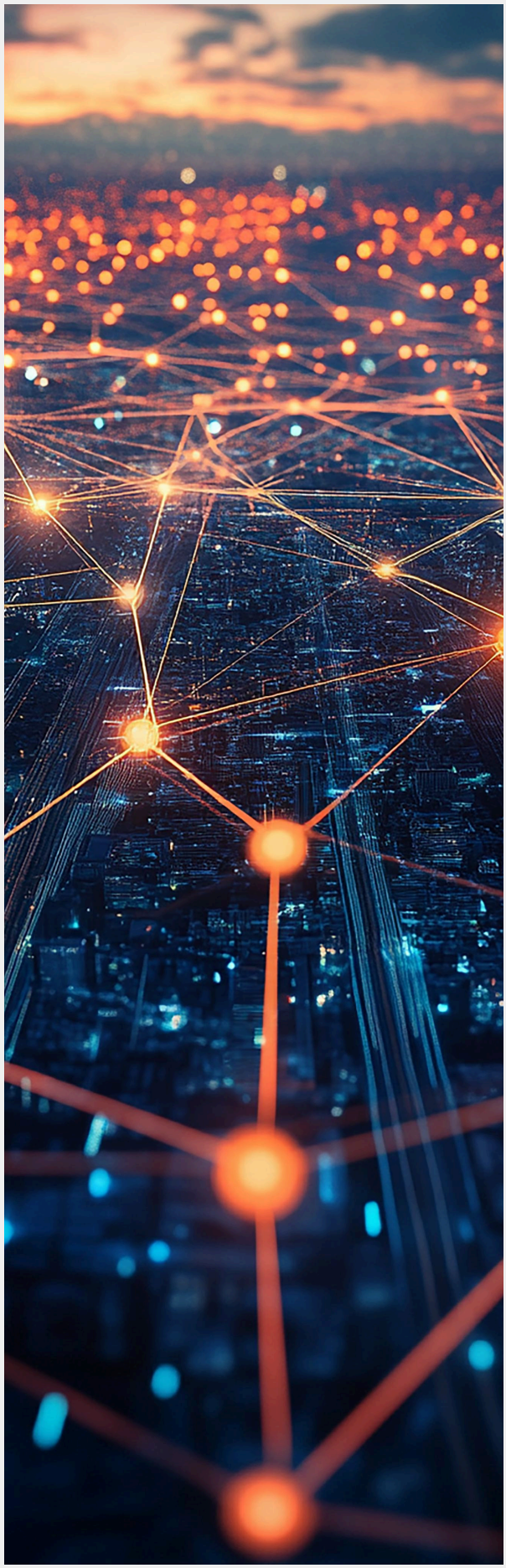
> Infelizmente, esse legado vem piorando, uma vez que os equipamentos estão envelhecendo.

Ainda que os fabricantes tenham assumido um compromisso muito maior com a segurança dos produtos nos últimos anos, vai demorar um tempo até que todos os equipamentos sejam substituídos.

> Em 2025, botnets antigas foram ressuscitadas com novas vulnerabilidades em equipamentos de rede

Os setores de telecomunicação, energia e saúde são especialmente vulneráveis a falhas nessa categoria de ativos, mas eles também estão presentes no varejo e em hotéis. Algumas linhas de produtos, como câmeras de segurança, são utilizadas por negócios de todos os setores.

Além da aplicação de patches de segurança, a principal recomendação para a proteção desses dispositivos é o uso de firewalls ou configurações de rede que impeçam qualquer tipo de acesso externo. Uma boa solução de External Attack Surface Management (EASM) pode ser utilizada para detectar dispositivos acessíveis externamente e vulnerabilidades na infraestrutura exposta.



Insight da plataforma:
External Attack Surface Management (EASM)

O EASM da Axur foi projetado para mapear, monitorar e proteger essa superfície de ataque externa, oferecendo uma visão completa de todos os ativos acessíveis e das vulnerabilidades associadas a eles.

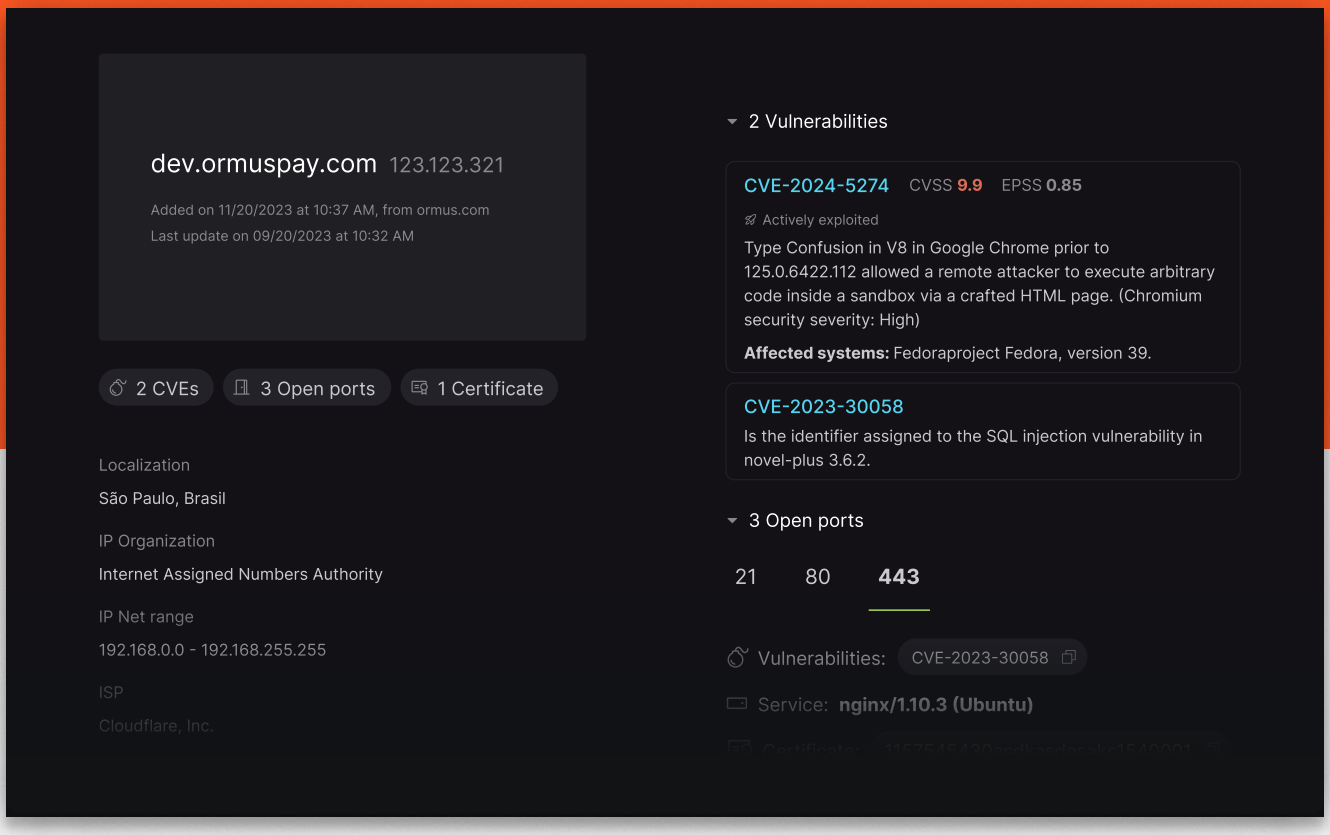
A solução identifica domínios, subdomínios, IPs e serviços em execução, correlacionando esses dados com bancos de vulnerabilidades conhecidos (CVEs) e verificando certificados digitais, portas abertas e protocolos em uso.

Essa análise contínua permite que as equipes:

Descubram ativos desconhecidos ou esquecidos, reduzindo riscos de shadow IT e exposição acidental.

Antecipem riscos emergentes por meio da integração direta com o módulo de Cyber Threat Intelligence (CTI) da Axur.

Classifiquem vulnerabilidades críticas com base em contexto, gravidade e potencial de exploração.



Desenvolvedores na mira do phishing e dos stealers

Os alvos tradicionais do phishing são os consumidores e usuários de serviços de tecnologia. Os ataques de ransomware levaram o phishing a diversos departamentos das empresas, que agora podem receber mensagens altamente contextualizadas e relevantes para suas respectivas funções.

> Agora, porém, estamos observando o crescimento de um novo tipo de phishing direcionado aos desenvolvedores de software.

O ambiente de desenvolvimento de software endossou grandes repositórios de bibliotecas e componentes, como npm (Node.js) e PyPI (Python), e automações de várias tarefas, muitas vezes com base em códigos de terceiros (por meio do GitHub Actions). Esses pontos que conectam vários projetos de software se tornaram alvos intermediários de hackers interessados em atingir as empresas e usuários que os utilizam.

Em 2025, foram observados ataques de typosquatting envolvendo os sites desses repositórios, bem como pacotes individuais que podem comprometer os desenvolvedores que os utilizem. Credenciais roubadas foram utilizadas para alterar pacotes oficiais e populares, e o incidente do tj-actions no GitHub conseguiu propagar um código malicioso para vários projetos.

Integrações com ferramentas de IA podem criar situações indesejadas por causa de falhas de injeção de prompt, como já mencionamos. Mas não podemos esquecer que, além das vulnerabilidades técnicas, todos esses processos envolvem pessoas que são suscetíveis à engenharia social.

Uma tática frequentemente usada contra programadores em 2025 foi a do emprego falso, em que a vítima é abordada por um suposto recrutador para realizar uma entrevista. O recrutador solicita que a vítima instale programas ou rode um código específico para participar do suposto processo do seletivo. Caso a vítima siga as instruções, o sistema será contaminado com um malware.

Ataques de malware contra programadores são preocupantes, uma vez que os infostealers podem roubar tokens com permissões de acesso a repositórios. É um tanto surpreendente que não haja registro de mais casos envolvendo o uso indevido de chaves de API, mas talvez isso mude em 2026.

Insight da plataforma Axur:
Monitoramento de dados expostos

O Monitoramento de dados expostos da Axur identifica credenciais, chaves de API, tokens de acesso e trechos de código sensíveis publicados em ambientes públicos como o GitHub.

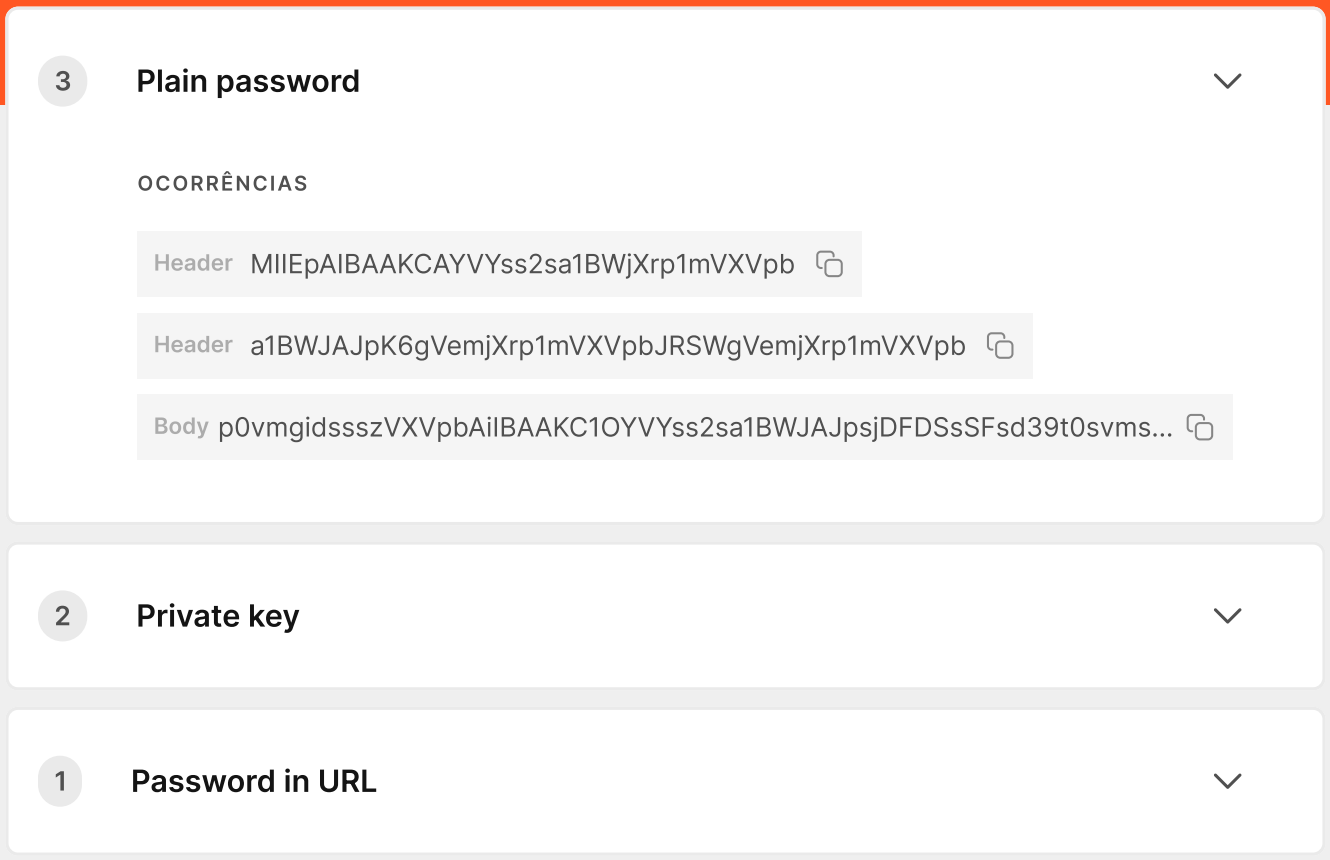
A solução prioriza os alertas conforme o risco e a relevância para cada organização, ajudando as equipes a agir antes que uma exposição se torne incidente.

Entre as principais aplicações estão:

Localização de credenciais e segredos embutidos em códigos e pipelines de automação (como GitHub Actions).

Identificação de chaves reutilizadas ou ativas, reduzindo a probabilidade de uso indevido.

Segredos expostos



Ações de cibersegurança para 2026

Criar políticas para a adoção de IA

Em síntese:

- As permissões de agentes de IA devem se valer da granularidade viabilizada pela gestão de acesso nas APIs e outras integrações.
- Agentes de IA podem automatizar vários processos de análise, detecção e resposta em cibersegurança.
- Se o negócio demandar o uso de agentes, as equipes de segurança terão de estar prontas para validar seu uso, com políticas e tecnologias para implementação e auditoria.

A criação de políticas para adoção de agentes de IA deve ser estruturada sobre frameworks graduais de autonomia, em que cada estágio define a latitude operacional do agente, desde a mera observação até a execução com políticas e auditoria integrada. Para cada nível, a organização deve determinar regras explícitas de escopo, reversão e observabilidade, garantindo que ações automatizadas sejam sempre rastreáveis e reversíveis.

O modelo RAIL (Restrições, Aprovações, Isolamento e Logs auditáveis) fornece o alicerce técnico dessas políticas, alinhando-se a práticas como o NIST CSF 2.0 e o CTEM (Continuous Threat Exposure Management). Isso implica definir identidade digital própria para cada agente, permissões baseadas no princípio do menor privilégio e validação humana obrigatória em ações críticas.

A implementação também deve incorporar métricas de confiança operacional, medindo a precisão, reversibilidade e tempo médio de resposta dos agentes, e prever sandboxing e auditoria contínua, para que a autonomia venha acompanhada de governança verificável. Essa abordagem posiciona as políticas de adoção de IA não apenas como diretrizes éticas, mas como arquitetura de segurança aplicada, fundamental para sustentar a defesa autônoma de forma segura e escalável.

Equipes de cibersegurança que se mantiverem como pioneiras na adoção de agentes para automatizar suas próprias funções devem ter mais facilidade para identificar ameaças emergentes.

Estabelecer governança efetiva e alinhada ao negócio

Em síntese:

- A conformidade não deve ser uma etapa formal e isolada do processo de cibersegurança.
- Sempre que possível, novas soluções de cibersegurança devem contribuir com as metas de governança estabelecidas.
- Avaliar como medidas técnicas de perícia, Threat Hunting e Cyber Threat Intelligence podem aprimorar processos de conformidade.

O conceito de governança ganha uma nova dimensão quando incorporado à lógica do Continuous Threat Exposure Management (CTEM). Em vez de tratar conformidade e segurança como ciclos isolados, o CTEM propõe uma visão contínua e orientada por contexto, onde a governança é sustentada por visibilidade técnica e alinhamento estratégico. Cada etapa, da definição de escopo à mobilização, se torna um mecanismo de governança em si, conectando dados de risco, priorização e resposta a decisões de negócio.

Essa abordagem complementa a função GOVERN do NIST CSF 2.0 ao introduzir um modelo operacional que mantém o controle em tempo real sobre a exposição, não apenas sobre políticas estáticas. Em vez de apenas identificar vulnerabilidades, as equipes de segurança passam a definir prioridades com base no valor do ativo, impacto operacional e contexto de ameaça, aproximando a gestão de risco da gestão corporativa.

O CTEM também reforça que a governança precisa ser observável e mensurável: métricas como cobertura de escopo, tempo médio de validação e proporção entre exposições detectadas e resolvidas tornam-se indicadores de maturidade.

Na prática, tem-se um reforço da ideia de que a cibersegurança é responsável pela capacidade de gestão dos ativos de TI, bem como suas políticas e processos que garantem sua conformidade.

Infelizmente, o trabalho de conformidade muitas vezes se resume a processos formais e morosos, com pouco impacto na resiliência do negócio. Isso não é sustentável nem é o interesse real dos bons reguladores, especialmente à luz das preocupações com segurança nacional que têm motivado as reformas regulatórias na área de tecnologia. Transformar a capacidade de governança em ganhos reais de resiliência será uma vantagem competitiva para as empresas. Isso fica mais fácil quando a cibersegurança se alinha ao negócio, enxergando as necessidades da empresa também em suas necessidades no mercado, no combate à fraude, proteção de marca e reputação.

Afinal, combater as fraudes contra os consumidores e proteger a reputação da empresa também são formas de evitar os desgastes que decorrem de ações judiciais e da associação indevida com a atividade ilícita que explora a marca da empresa.

A capacidade de investigar incidentes por meio de Threat Hunting e boas fontes de Cyber Threat Intelligence também é determinante para atingir objetivos reais de conformidade.

Idealmente, todas as medidas de segurança que recomendamos, como a automação por IA, o monitoramento de credenciais e vazamento e a visibilidade sobre o supply chain, devem ser pensadas também pela ótica da conformidade, fazendo dela uma parte do processo de segurança e não uma etapa formal desvinculada das medidas técnicas. Quanto mais robustos forem os controles existentes para fins de governança, mais fácil também será a adoção de agentes de IA.

É importante lembrar que pode ser difícil prever de que forma regulações ou necessidades do mercado podem impactar o negócio. Flexibilidade e capacidade de reação serão bons valores em 2026.

Implementar o monitoramento de dados e credenciais

Em síntese:

- Os golpes de extorsão que ameaçam expor dados corporativos substituindo o ransomware em alguns casos, exigindo monitoramento externo de vazamentos.
- Monitorar credenciais vazadas ajuda a evitar que criminosos obtenham acesso a dados armazenados em nuvem e plataformas SaaS.
- Monitorar vazamentos de dados facilita a governança e permite que a empresa adote uma postura mais firme junto a seus parceiros.

O ransomware tradicional vem cedendo espaço a ataques cibernéticos de extorsão em que os criminosos ameaçam empresas com a exposição dos dados que roubaram dos ativos aos quais tiveram acesso, incluindo aqueles localizados na nuvem, fora da rede corporativa.

Não existem formas de impedir que os dados sejam expostos caso o resgate não seja pago e, mesmo que a empresa pague o resgate, também não há como ter certeza de que os dados foram descartados. É possível que desavenças entre os golpistas resultem em uma nova ameaça ou que os criminosos decidam comercializar as informações roubadas em algum momento, mesmo que o resgate tenha sido pago.

Há duas atitudes importantes para aumentar a resiliência contra essas ameaças. A primeira é proteger todos os ativos da infraestrutura de TI, inclusive os externos. O monitoramento de credenciais expostas é especialmente relevante, devendo sempre considerar também as credenciais corporativas usadas em plataformas de terceiros.

Todo e qualquer lugar que guarda dados corporativos deve ser monitorado e protegido. Em muitos casos, a credencial de um usuário é a única barreira para impedir que invasores acessem dados armazenados na nuvem ou em soluções de SaaS. Como essas credenciais não são utilizadas nos próprios sistemas da empresa, o monitoramento externo é a melhor alternativa.

A segunda atitude a ser tomada é o monitoramento de vazamentos e dados corporativos. Monitorar a exposição de dados da empresa tem benefícios para governança e para o início rápido de tratativas para a mitigação de incidentes. No caso de dados compartilhados com parceiros ou fornecedores, esse monitoramento também sinaliza a preocupação com a proteção de dados, servindo como ferramenta para detectar indiretamente as violações de segurança em terceiros que resultem em um vazamento.

Buscar visibilidade sobre o supply chain

Em síntese:

- Hackers estão buscando vulnerabilidades em todo o supply chain de um alvo.
- Certas soluções de cibersegurança podem ser utilizadas para ampliar a visibilidade sobre o supply chain.
- A inteligência em ameaças e as integrações de IA podem ser pensadas de maneira cooperativa com os parceiros.

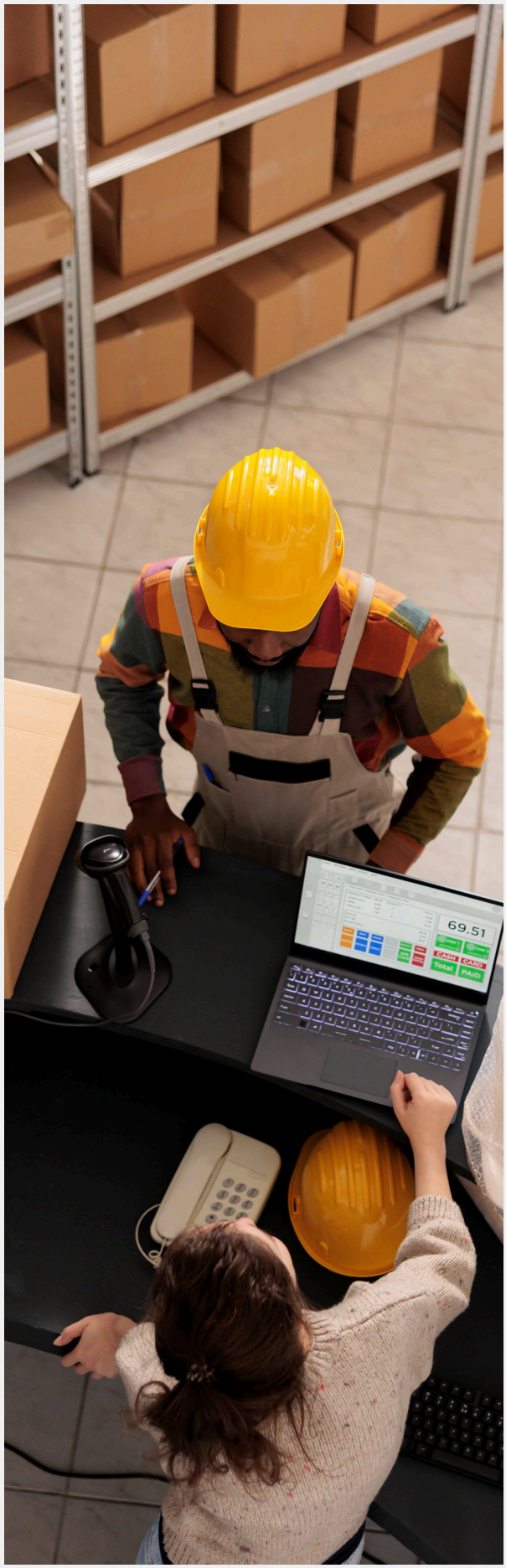
Atores maliciosos vêm demonstrando a capacidade de localizar vulnerabilidades em terceiros para atingir seus alvos. Por isso, é importante buscar meios de ampliar a visibilidade sobre toda a cadeia de fornecedores e terceiros, o supply chain.

Vale mencionar que os alvos podem ser de oportunidade e não previamente desejados, a partir de um fornecedor vulnerável, pode-se entender o que é mais interessante para os atacantes.

Algumas soluções de segurança já existentes podem ser refinadas para incluir a infraestrutura de terceiros. O Cyber Threat Intelligence da Axur pode ser configurado para buscar informações sobre as categorias de ativos usados por terceiros críticos, alertando sobre eventos que podem indicar uma elevação no risco no ambiente dos fornecedores.

Ferramentas como Threat Hunting e os monitoramentos de dados expostos e de credenciais também podem ser utilizados para dar visibilidade sobre o supply chain.

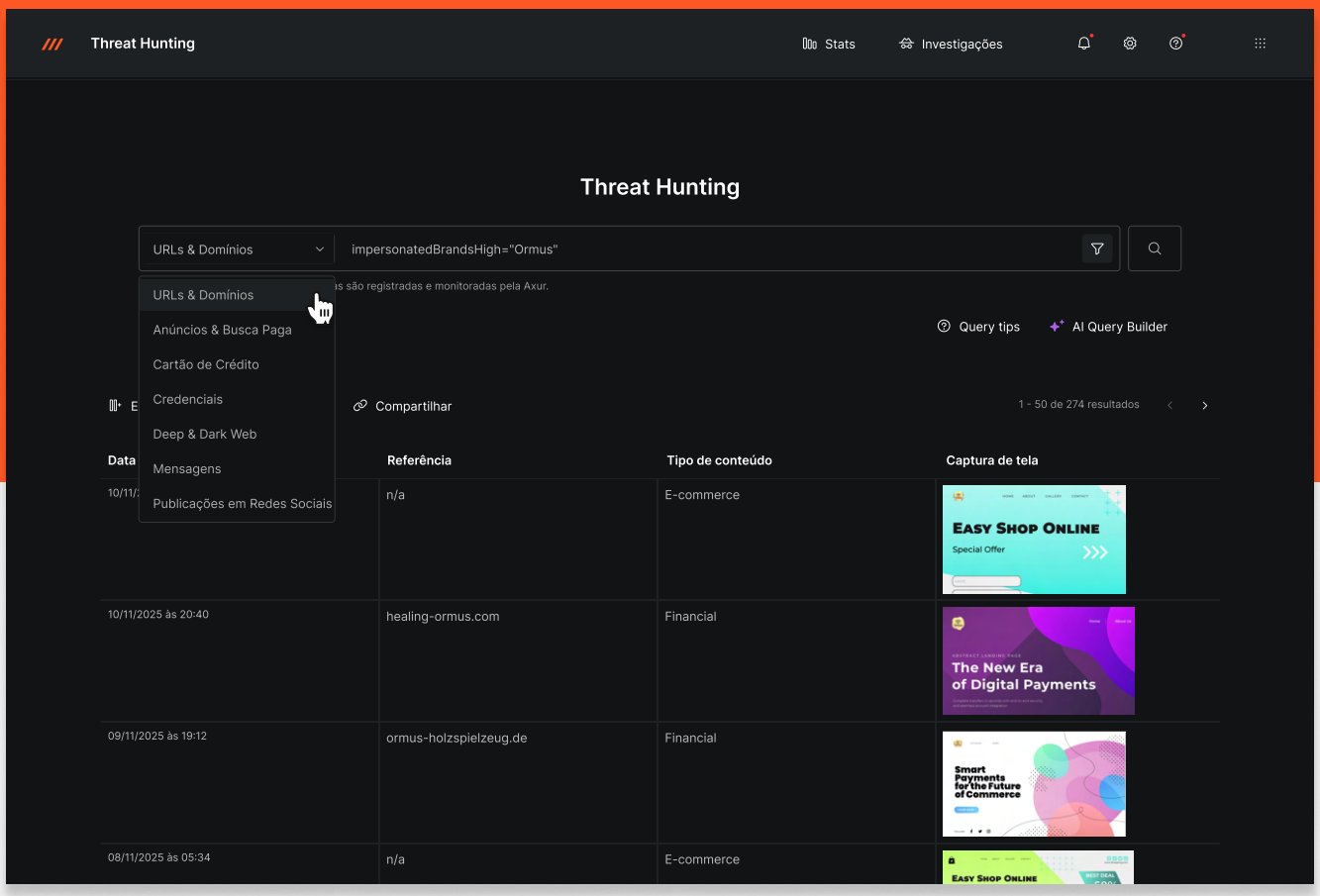
Da mesma forma, agentes e outras ferramentas de IA também podem ser usadas para facilitar a comunicação com terceiros e facilitar o tratamento de incidentes.



Insight da plataforma Axur:
Threat Hunting

O Threat Hunting da Axur permite realizar buscas avançadas na base de ameaças externas para identificar exposições de credenciais, cartões, domínios, mensagens na deep & dark web, e URLs maliciosas e perfis em redes sociais. Além de investigar incidentes internos, a ferramenta possibilita localizar credenciais e ativos comprometidos de fornecedores estratégicos, mapear campanhas de phishing direcionadas a parceiros e antecipar riscos compartilhados no supply chain.

DESCUBRA 101 CASOS DE THREAT HUNTING



Conscientizar usuários e parceiros

Em síntese:

- Ataques de phishing continuam evoluindo, inclusive com novos alvos primários em algumas campanhas.
- Engenheiros de software e equipes de suporte técnico se tornaram alvos frequentes de phishing.
- É preciso apostar em medidas técnicas, conscientização e treinamento.

É compreensível que muitos enxerguem o phishing como um problema majoritariamente centrado nos usuários finais de departamentos sem vínculo com a TI.

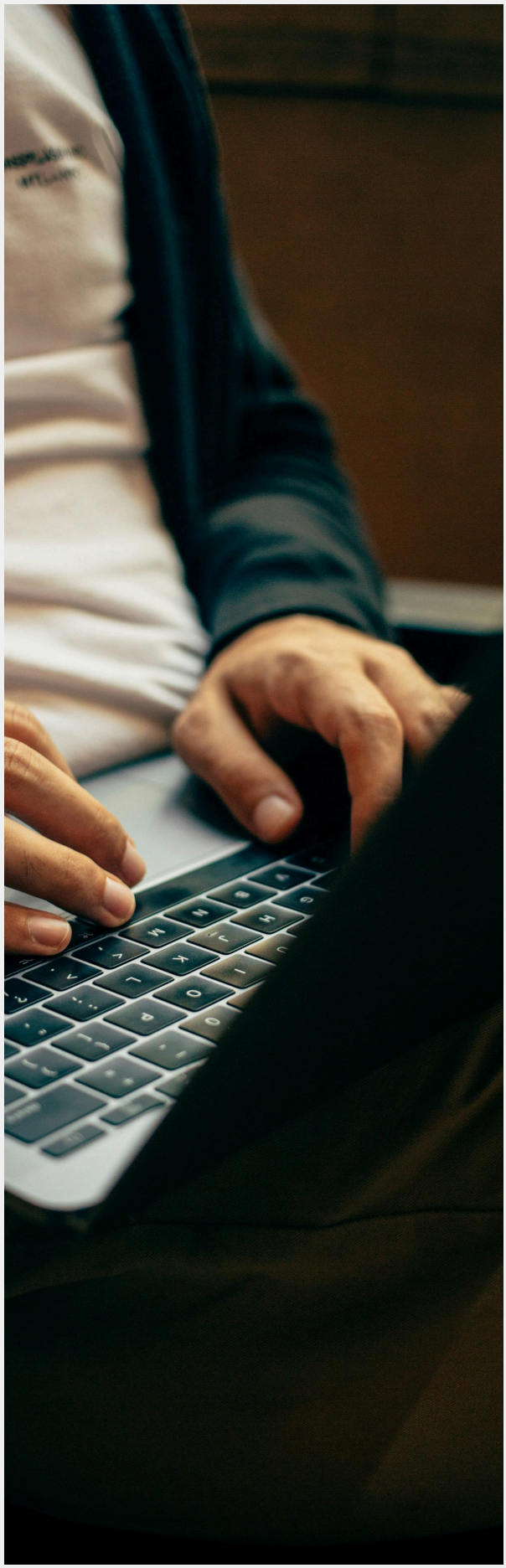
Historicamente, o departamento de Recursos Humanos é um dos mais atingidos, já que criminosos podem se passar por candidatos de emprego para aplicar golpes.

As fraudes em 2025 mudaram esse cenário. Engenheiros de software foram atingidos por meio de typosquatting (exploração de erros de digitação) em pacotes e seus repositórios.

Em outra situação, os criminosos enviam propostas falsas de emprego e distribuem um software malicioso sob a justificativa de que ele seria necessário para realizar o teste técnico durante a seleção.

Caso a vítima acredite na fraude, o resultado é quase sempre a execução de um infostealer, o qual roubará credenciais do desenvolvedor – inclusive credenciais corporativas, se elas estiverem disponíveis.

Esses cenários, somados aos ataques de phishing por telefone que miraram centrais de help desk e suporte técnico, demandam uma possível expansão das campanhas de treinamento e conscientização em segurança.



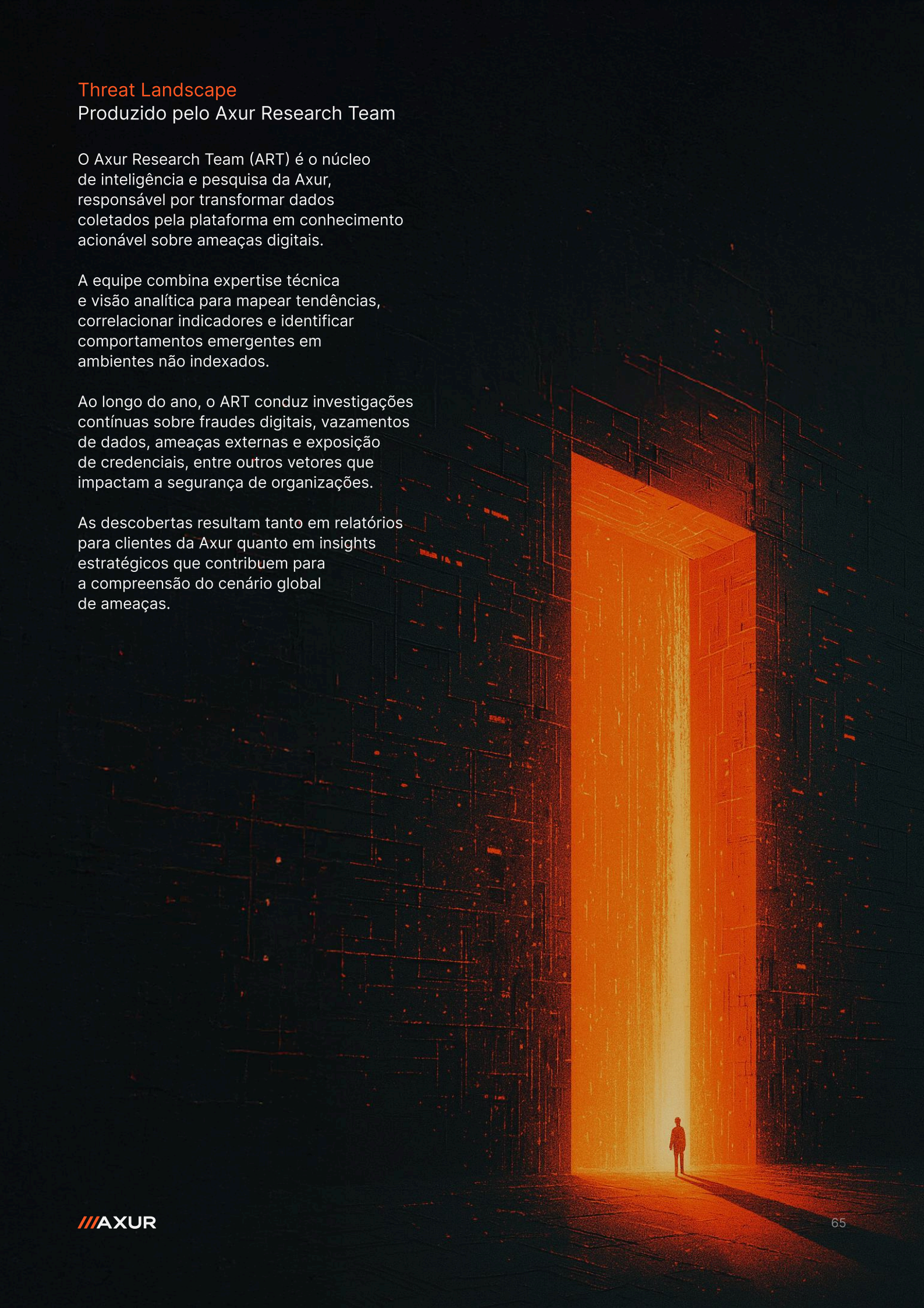
Threat Landscape
Produzido pelo Axur Research Team

O Axur Research Team (ART) é o núcleo de inteligência e pesquisa da Axur, responsável por transformar dados coletados pela plataforma em conhecimento acionável sobre ameaças digitais.

A equipe combina expertise técnica e visão analítica para mapear tendências, correlacionar indicadores e identificar comportamentos emergentes em ambientes não indexados.

Ao longo do ano, o ART conduz investigações contínuas sobre fraudes digitais, vazamentos de dados, ameaças externas e exposição de credenciais, entre outros vetores que impactam a segurança de organizações.

As descobertas resultam tanto em relatórios para clientes da Axur quanto em insights estratégicos que contribuem para a compreensão do cenário global de ameaças.



Sobre a Axur

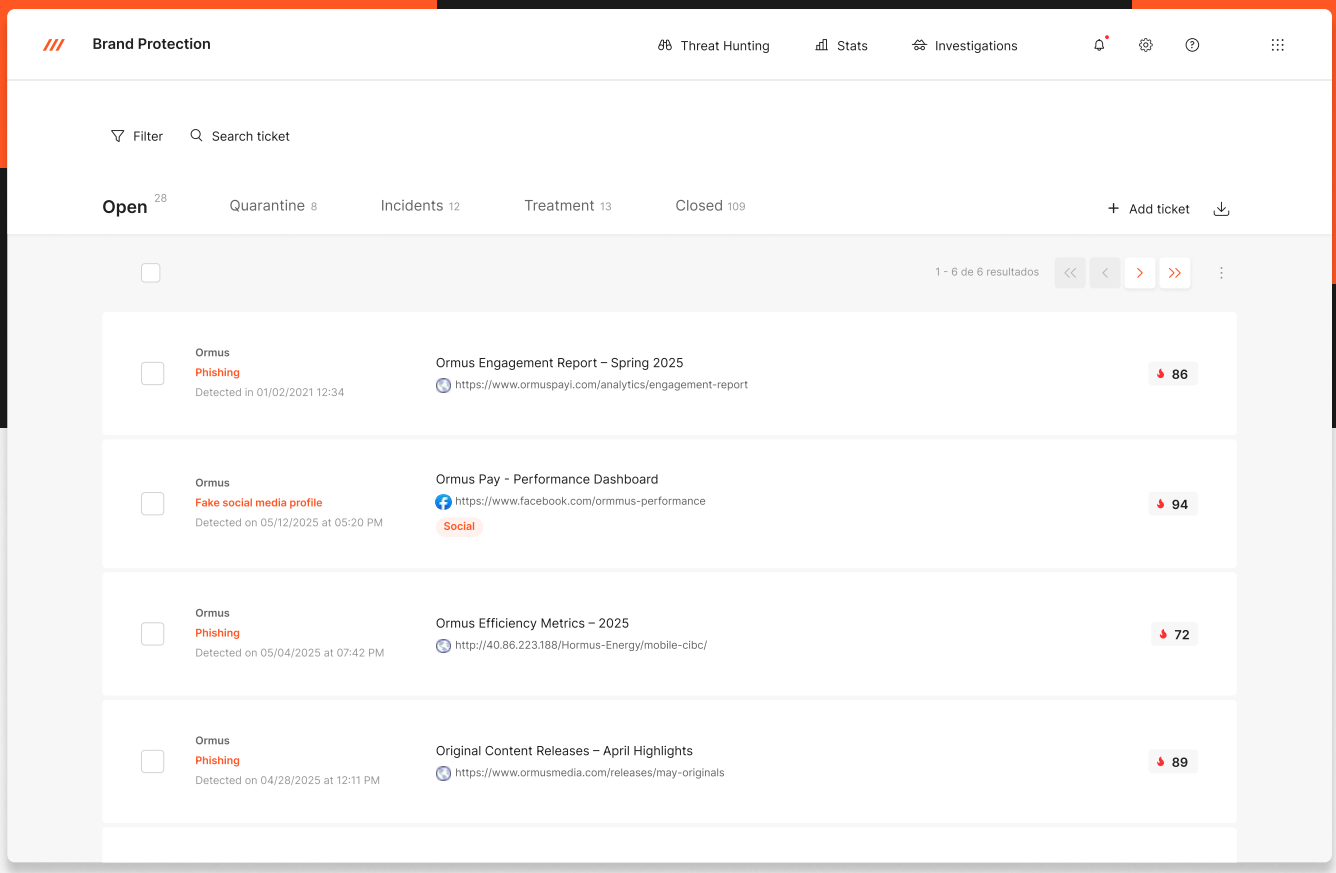
A Axur é uma solução líder em cibersegurança externa que empodera equipes de segurança para tratar ameaças fora do perímetro.

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.

AGENDE UMA DEMO




THREAT LANDSCAPE
2025 → 2026
AXUR