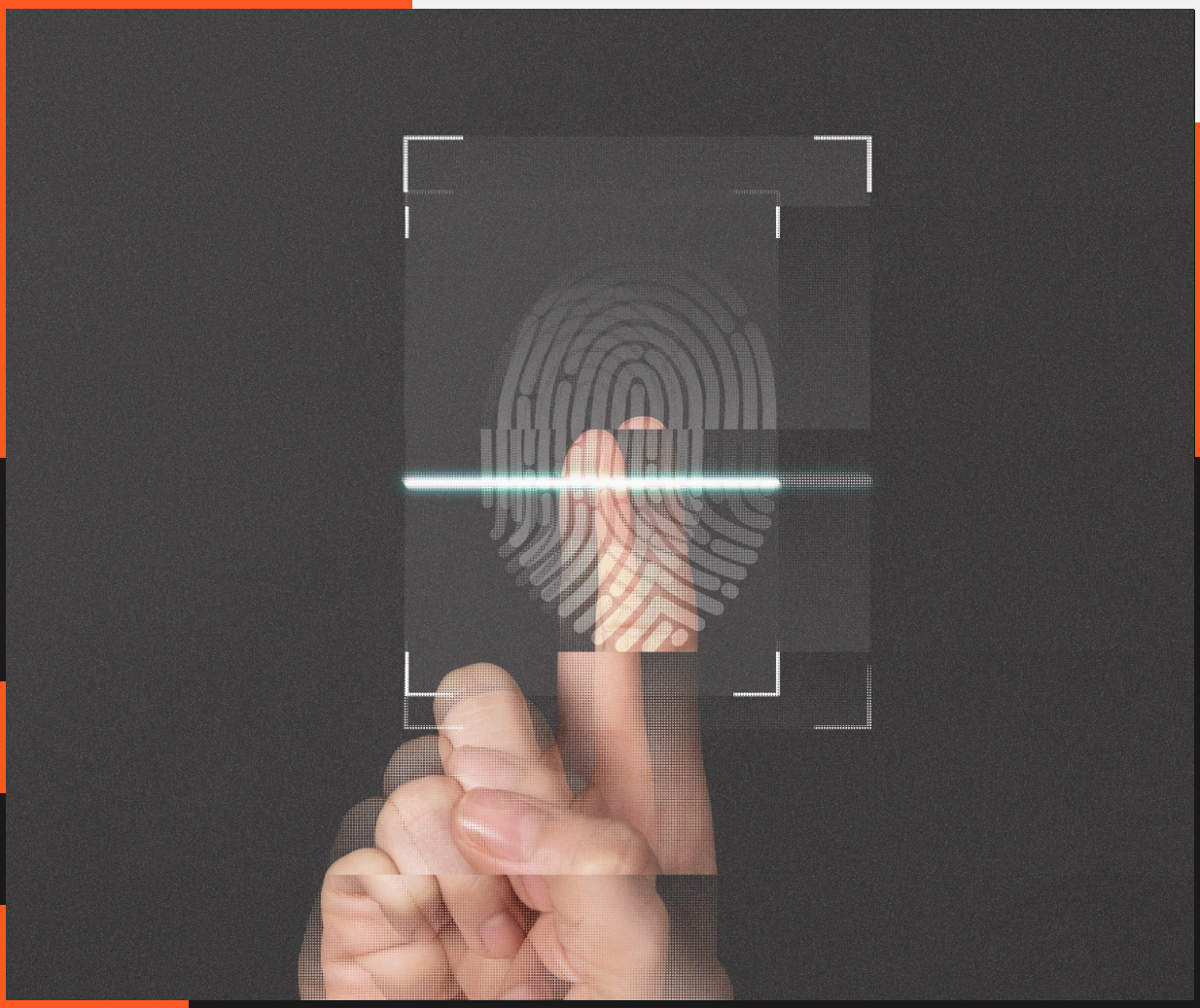


Credenciais em jogo

O que há de novo nos mais recentes vazamentos: reflexões e aprendizados

AXUR

Sumário executivo

Vazamentos de credenciais volumosos podem assustar as pessoas e ganhar manchetes na imprensa de tempos em tempos. O caso de um criminoso prometendo um pacote com 16 bilhões de credenciais é o exemplo mais recente, mas não é inédito nem especialmente relevante. Esses grandes pacotes já se transformaram em uma ocorrência regular, ainda que esporádica.

Não há motivo, ao menos no momento, para crer que esses dados são originais. É inegável que a disponibilização de um grande compilado de credenciais antigas pode representar um novo risco para empresas e indivíduos, uma vez que mais criminosos terão acesso a esses dados. Mas este não deve ser o maior foco de atenção.

É preciso ter ciência de que os riscos dos vazamentos de credenciais não estão limitados a estes episódios. Na verdade, o roubo e o uso indevido de credenciais é uma ameaça constante que leva ao vazamento de milhões de novas credenciais todos os meses.

Os atacantes têm muito interesse nesses dados. Como mostra o Data Breach Investigations Report (DBIR) da Verizon, o uso indevido de credenciais é o vetor inicial de ataque em 22% das invasões.

Embora menos chamativos, esses vazamentos recorrentes são talvez até mais graves que os grandes pacotes que ganham manchetes.

Enquanto essas compilações com bilhões de credenciais trazem dados antigos e repetidos, com muitas senhas obsoletas e inválidas, os arquivos de credenciais divulgados diariamente por grupos criminosos trazem credenciais que acabaram de ser roubadas de um computador que pode estar em uso naquele exato instante.

Essas compilações de credenciais são a manifestação de um ecossistema criminoso que incentiva financeiramente a comercialização de credenciais roubadas e que produz softwares maliciosos para roubos de senha, os infostealers, para alimentar esse ecossistema diariamente.

É considerando este contexto que devemos olhar para esse tipo de notícia. Em nossas organizações, temos que nos atentar para as características mais perigosas da ameaça (como é o caso dos infostealers e a capacidade desses malwares de derrotar a autenticação multifator).

Neste material, vamos relembrar a história dos grandes vazamentos credenciais, exemplificando a fonte desses materiais, e por qual motivo os criminosos criam essas compilações. Ao fim, trazemos recomendações para que organizações aprimorem sua gestão de identidades e credenciais com vários tipos de medidas que podem prevenir e mitigar o impacto de ataques.

Um histórico dos grandes vazamentos de credenciais

Grandes vazamentos de credenciais não são uma novidade no mundo do crime. Em 2012, sites como LinkedIn, eHarmony e Last.fm sofreram ataques cibernéticos em que hackers conseguiram roubar milhões de senhas. O pacote roubado do Linkedin, com 6,5 milhões de credenciais, parecia especialmente expressivo. No entanto, este mesmo pacote ressurgiu quatro anos depois, em 2016, com 165 milhões de contas e 117 milhões de senhas.

Este novo pacote do LinkedIn estava sendo vendido pelo criminoso a qualquer interessado, o que se tornou uma prática recorrente. Contudo, é comum que os criminosos deixem parte das credenciais disponíveis como uma "amostra grátis" para tentar ganhar credibilidade e aumentar as vendas do pacote comercial.

Isto foi visto em 2019 no pacote conhecido como Coleção nº 1 ("Collection #1"), que, como o nome sugere, era o primeiro arquivo de uma série de 5 – quatro dos quais estavam sendo vendidos, enquanto o nº 1 foi disponibilizado para divulgar a oferta.

No total, os cinco arquivos continham 2,2 bilhões de credenciais. Era o maior pacote já visto até então.

A possibilidade de ganhar dinheiro vendendo grandes pacotes de credenciais se tornou um incentivo para que hackers começassem a montar coleções cada vez maiores. Além disso, criou uma motivação financeira para que hackers se especializassem na tarefa de encontrar ou roubar credenciais.

Uma das práticas envolvidas nisso é o credential stuffing, uma técnica que pode ser compreendida como revalidação de senhas. Utilizando as credenciais já vazadas para outros serviços, os criminosos utilizam ferramentas para automatizar tentativas de login com as mesmas senhas em outros serviços.

Isso mitiga as perdas dos criminosos, já que os sites atacados normalmente invalidam as senhas usadas antes do ataque. Quando as senhas do LinkedIn vazaram em 2012, a rede social logo obrigou os usuários afetados a trocarem as senhas, o que significa que os hackers tiveram dificuldade para utilizar as senhas roubadas com o intuito de atacar os próprios usuários do LinkedIn.

No entanto, por meio do credential stuffing, os hackers descobrem outros serviços em que a mesma combinação de usuário e senha foi utilizada. Como estes serviços não foram atacados diretamente, o usuário não foi obrigado a trocar as senhas nestes serviços como ocorreu no próprio LinkedIn. Como nem todos os usuários lembram de trocar a senha em todos os serviços em que foi utilizada, a revalidação pode se mostrar mais útil do que o vazamento original.

O credential stuffing também permite que hackers ofereçam a venda de senhas "novas" que, na verdade, são credenciais antigas "recicladas" em novos serviços. Os efeitos da reutilização de senhas e o credential stuffing já eram visíveis na Coleção nº 1. O pacote tinha apenas 21 milhões de senhas únicas, mas 1,1 bilhão de combinações de usuário e senhas. Ou seja, muitas das senhas apareciam diversas vezes, seja porque os usuários usavam as mesmas senhas ou porque uma mesma senha havia sido revalidada em outro contexto.

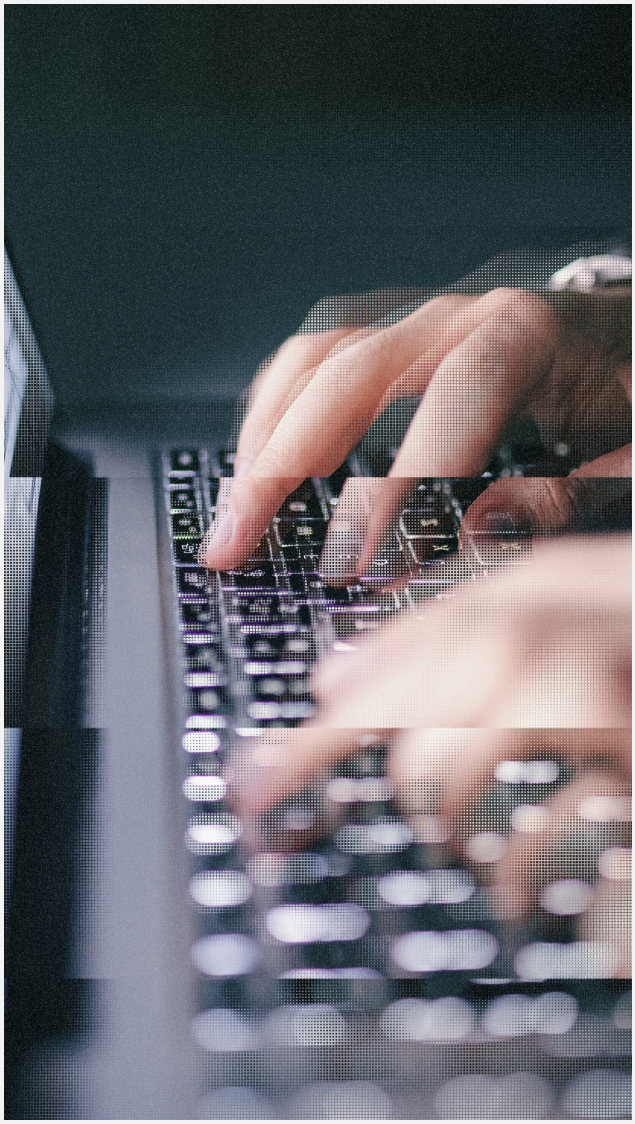
Além do credential stuffing, também crescia o uso de malwares para roubo de senhas, chamados de infostealers. Quadrilhas se especializam no desenvolvimento ou operação desses softwares maliciosos com o intuito de roubar o maior número de credenciais, sem alvo específico, para que essas credenciais fossem comercializadas em lote através de pacotes ou assinaturas recorrentes.

Nesse cenário, não demorou para que os números das Coleções fossem superados, o que ocorreu em 2021 com a publicação do pacote "RockYou2021". O nome do arquivo era uma alusão a um ataque cibernético ocorrido em 2009 contra a RockYou, uma empresa que desenvolvia ferramentas para redes sociais como MySpace e Facebook. Na época do ataque, o vazamento expôs dados de 32 milhões de usuários da RockYou.

O RockYou2021 não se limitava aos dados desta invasão antiga. Com 8,4 bilhões de registros, era uma nova coleção de credenciais montada a partir de muitos outros vazamentos que já tinham ocorrido até então, bem como revalidações, invasões de botnets, phishing, infostealers e, possivelmente, dados inventados.

O pacote foi atualizado e republicado em 2024 (com o nome de "RockYou2024"), chegando a 9,94 bilhões de credenciais.

Em 2025, vimos uma publicação de mais um grande pacote de credenciais – desta vez oferecendo 16 bilhões de registros.



16 bilhões de credenciais vazadas: riscos e contexto

Embora tenha sido divulgado como um "novo" vazamento em alguns veículos de imprensa, o pacote que supostamente traz 16 bilhões tende a seguir o padrão visto em seus antecessores: um misto de vazamentos antigos, senhas revalidadas através de credential stuffing e, possivelmente, muitos registros duplicados e inválidos. Poucas dessas credenciais tendem a ser inéditas e, mesmo assim, nem todas são necessariamente verdadeiras.

Uma análise preliminar da Axur apontou que o material provavelmente tem baixa relevância, considerando os seguintes pontos:

O pacote foi publicado no dia 23 de maio por uma conta recente, não por um ator de reputação conhecida.

Ao contrário dos casos anteriores, não foi disponibilizada uma amostra para comprovar a qualidade do material.

O pacote aparentemente não despertou tanto interesse nos próprios criminosos.

Como o objetivo do criminoso é comercializar esse pacote para outros criminosos, não há qualquer garantia quanto à veracidade do material ou das promessas de venda. Como o autor do pacote não tem um histórico ou reputação conhecida, suas promessas e afirmações devem ser avaliadas com cautela.

Na prática, isso significa que há uma possibilidade considerável de o pacote conter registros de baixa qualidade, incluindo:

→ Credenciais já vazadas anteriormente, com pouca ou nenhuma novidade;

→ Dados preparados para revalidação que não foram checados, que na prática são credenciais inventadas ou inválidas;

→ Credenciais muito antigas, em que há uma chance considerável de que as senhas já foram trocadas e não estão mais em uso;

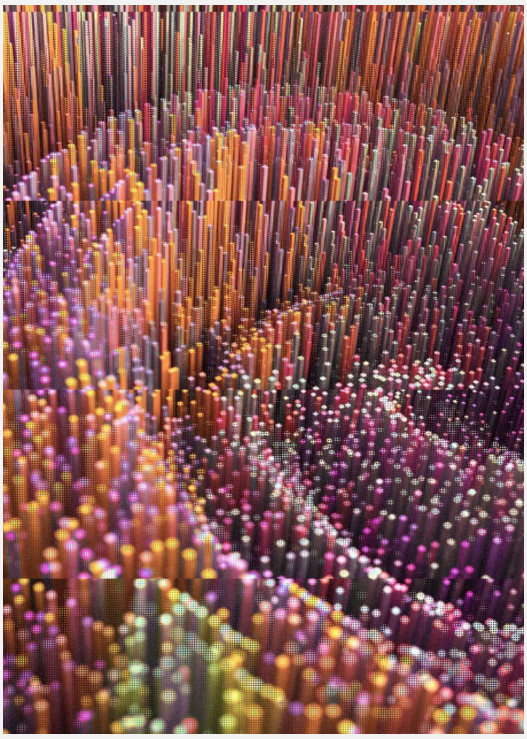
→ Dados inventados ou falsos, que o criminoso incluiu para inflar os números do pacote e que dificilmente serão checados, tendo em vista o volume total;

→ Credenciais duplicadas, resultante da mistura de pacotes anteriores.

A republicação de credenciais já vazadas é uma prática muito recorrente nos espaços criminosos. Em 2024, os sistemas da Axur detectaram 56 bilhões de credenciais vazadas. No entanto, após o processamento e refinamento desses dados, para reduzir falsos positivos e priorizar exposições que representam riscos reais, constatou-se que menos de 1/5 delas podiam ser consideradas inéditas e únicas.

Do ponto de vista dos criminosos, é quase impossível diferenciar uma credencial antiga já invalidada de uma credencial inventada ou falsa. Muitos sistemas modernos seguem a boa prática de evitar informar a um atacante quando uma conta existe, com mensagens de erro que não deixam explícito quando uma senha está incorreta ou quando uma conta não existe.

Por conta disso, os golpistas que decidem ganhar dinheiro vendendo pacotes de credenciais têm um incentivo para manipular os dados e somar informações de pouco valor para impressionar com o volume oferecido. Isso é especialmente verdade quando a oferta parte de um ator sem reputação estabelecida, como é o caso deste novo pacote que supostamente traz 16 bilhões de credenciais.



Quais os riscos?

Mesmo que o pacote de credenciais tenha poucas informações inéditas e válidas, a propagação desses dados em um pacote unificado tende a difundir essas credenciais no mundo do crime, assim como ocorreu com a Coleção nº 1 e o RockYou.

Quem já tratou corretamente um incidente com uma credencial vazada que foi incluída distribuída neste arquivo provavelmente não será atacado outra vez com a mesma credencial. No entanto, há um risco para empresas e indivíduos que ainda não foram atacados com essas credenciais.

Grupos criminosos procuram credenciais valiosas que não tinham sido exploradas ainda, dando início a campanhas de impacto considerável. Em 2024, isso aconteceu com empresas que utilizavam o serviço de armazenamento Snowflake.

De acordo com o Verizon Data Breach Investigations Report de 2025, 22% das invasões começam a partir de uma credencial roubada.

No entanto, a ausência de credenciais novas e válidas neste pacote não significa que o vazamento de credenciais não representa uma ameaça para o negócio.

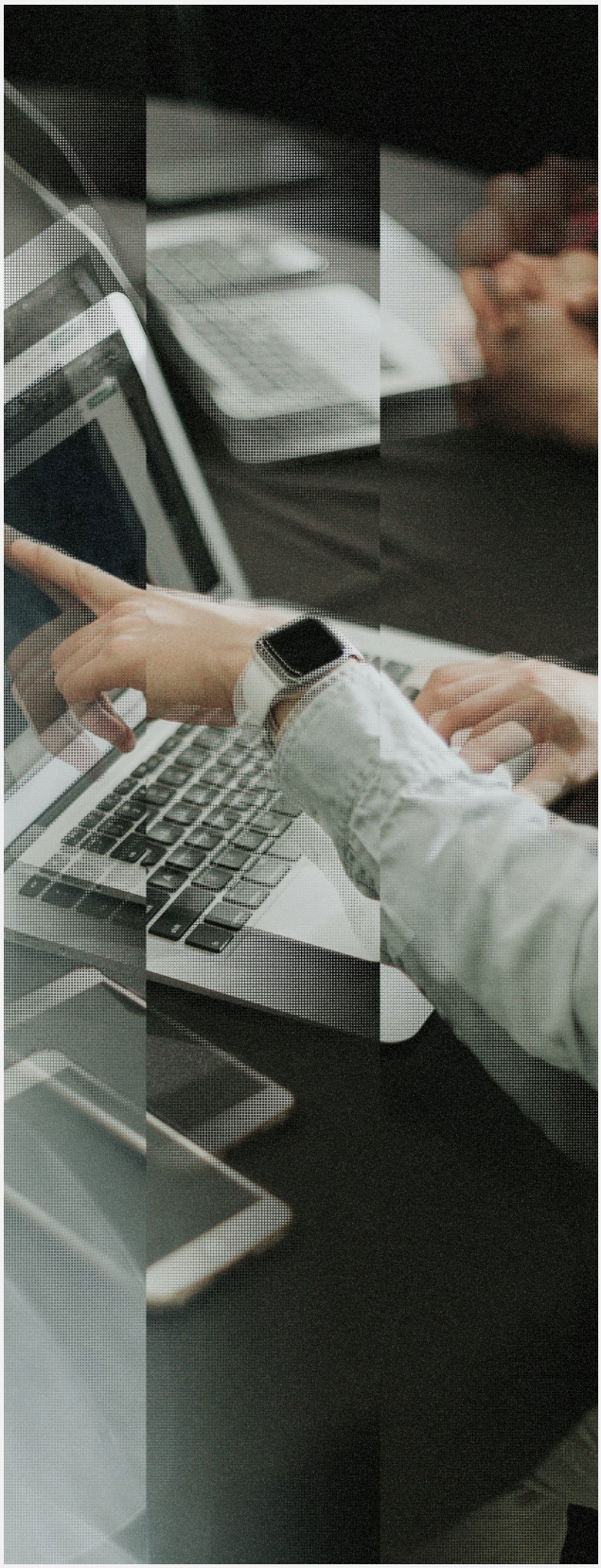
Além de serem mais recorrentes, os vazamentos menores costumam ter mais credenciais recentes e válidas, o que pode representar um risco maior do que os grandes pacotes de vazamentos.
Um vazamento de credenciais não representa um risco pelo seu volume, mas sim pela possibilidade de que traga alguma credencial válida para um sistema sensível ou corporativo.

Muitas credenciais corporativas são usadas em sistemas abertos na internet, como plataformas de SaaS (software como serviço) e acessos remotos via VPN. Os criminosos se interessam por essas credenciais, já que elas podem ser utilizadas em ataques cibernéticos contra essas empresas.

A principal fonte dessas credenciais valiosas e recentes são os infostealers. Os colaboradores das empresas podem ser atacados por infostealers que roubam todas as credenciais armazenadas no sistema e, por conta de políticas de Bring Your Own Device (BYOD), os operadores desses infostealers podem utilizar uma gama variada de iscas para distribuir esse tipo de malware – inclusive iscas referentes ao uso pessoal do equipamento, como em redes sociais.

Com isso, infostealers podem roubar credenciais corporativas de equipamentos pessoais, criando um desafio para a empresa em termos de visibilidade e mitigação desses riscos.

Grandes pacotes de credenciais são organizados e distribuídos esporadicamente, mas são apenas um sintoma de uma ameaça maior e recorrente envolvendo os roubos diários de credenciais por infostealers e outros meios.



Estratégias de mitigação além do MFA

A autenticação multifatorial (MFA) pode evitar que credenciais simples (como usuários e senhas) sejam utilizadas com sucesso para comprometer um sistema. No entanto, dados de acesso válidos ainda podem ser utilizados por criminosos para iniciar ataques contra a MFA.

O tipo de ataque viável contra a MFA varia de acordo com o método específico implementado.

Os ataques contra os diferentes métodos de MFA

Método de MFA	Ameaças
Autorização por aplicativo	Erro de usuário (que pode ser motivado com push bombing/ MFA Fatigue)
Código por SMS/Voz	Phishing, SIM Swap, ataques a rede (SS7)
OTP (One-time password, com chave física ou app gerador)	Phishing

No caso de grandes vazamentos de senhas, que tendem a trazer apenas credenciais simples e antigas, a MFA pode ter um papel importante na mitigação do ataque.

Apesar disso, a MFA não é sempre capaz de impedir a atuação dos infostealers e as consequências dos vazamentos diários de credenciais que eles provocam. Infostealers podem roubar credenciais em formato de token armazenadas em cookies dos navegadores web ou por softwares instalados no sistema. Esses tokens permitem a clonagem da sessão autenticada, contornando completamente as etapas de autenticação.

Existem ainda casos em que o usuário desativa a MFA por conta de alguma dificuldade no uso do segundo fator de autenticação.

Criminosos também podem utilizar o acesso obtido por infostealers para autorizar outros tokens de acesso ou até configurar novos mecanismos de MFA na conta da vítima. Se a vítima já utiliza SMS, por exemplo, o invasor pode configurar um aplicativo gerador de OTP para continuar acessando a conta mesmo sem acesso ao número de telefone.

Por estes motivos, o MFA por si só não mitiga todos os cenários envolvendo credenciais.

Felizmente, a circulação das credenciais roubadas no mundo crime permite que elas sejam monitoradas e invalidadas antes que os criminosos tenham a chance de utilizá-las.

O monitoramento de credenciais vazadas ajuda a proteger as identidades de vários desses cenários, criando uma barreira adicional para proteger todos os acessos corporativos, aliando-se à MFA e demais medidas da gestão de acessos privilegiados.

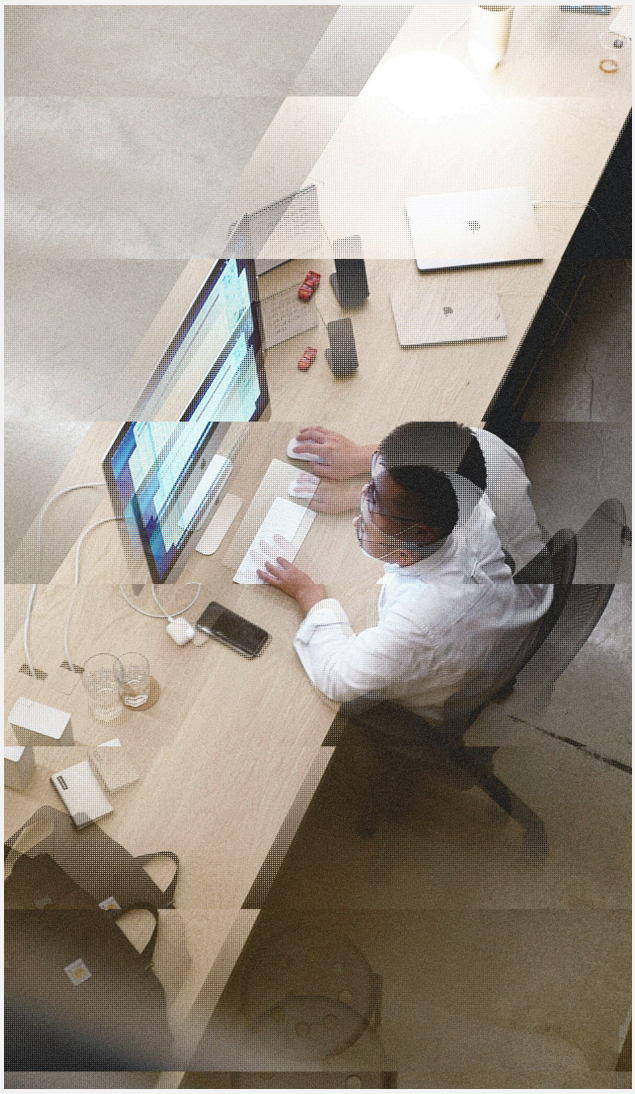
Recomendações para gestão de identidades

Monitorar o vazamento de credenciais

O monitoramento de credenciais vazadas ajuda sua empresa a saber quando alguma credencial corporativa está circulando nas redes criminosas. É um importante sinal de inteligência que pode ser atrelado a ações preventivas e imediatas, como invalidar a senha, investigar a origem do vazamento e aprimorar programas de treinamento interno ou políticas de Bring Your Own Device (BYOD).

No contexto de resiliência ou defesa em profundidade, o monitoramento de credenciais ajuda a prevenir ataques que poderiam ter tomado forma devido a falhas em outros processos que podem ter deixado credenciais antigas expostas. Também tem um papel crítico na proteção de sistemas vulneráveis ao roubo de tokens de acesso ou plataformas em que a adoção de MFA não é viável. É também uma das medidas mais simples de serem implementadas, pois não exige mudanças na rede corporativa para ser implementada.

Converse com um especialista da Axur e descubra como o monitoramento de credenciais protege o seu negócio.



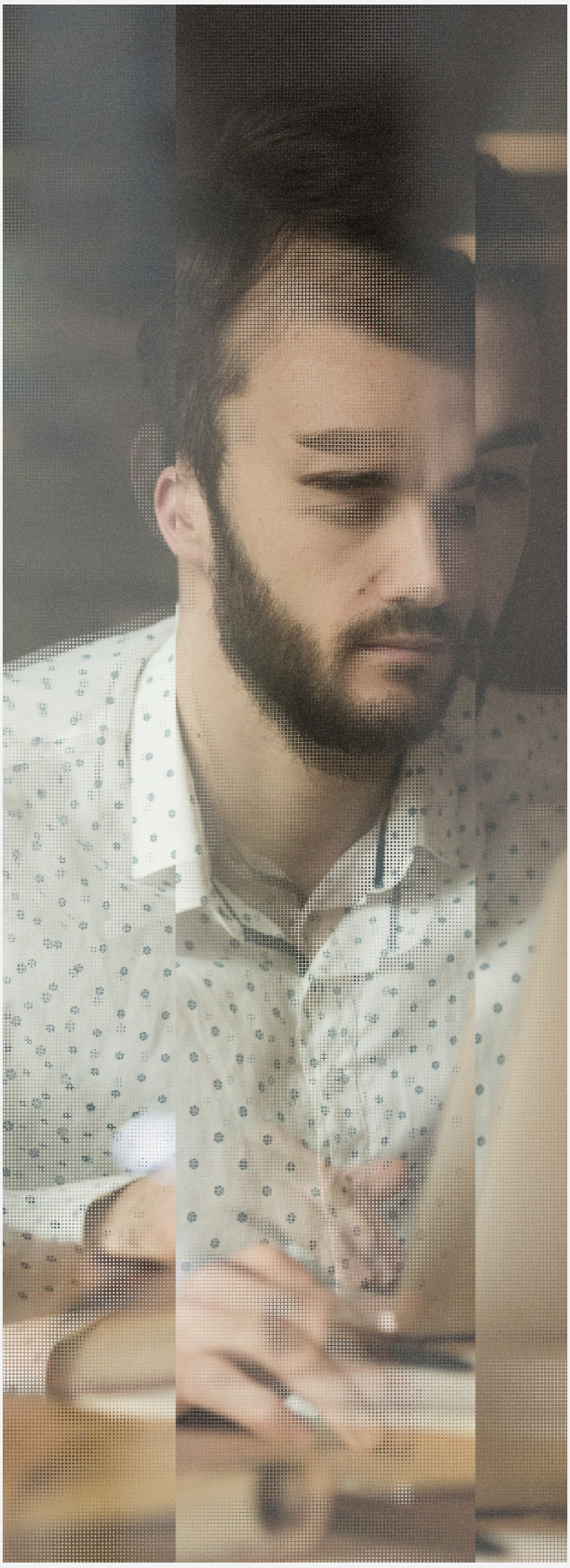
Proteja ativos externos expostos

Sistemas de VPN, dashboards com acesso externo e aplicações web são alvos constantes de ataques com credenciais roubadas por estarem expostos. A Gestão da Superfície de Ataque Externa (External Attack Surface Management – EASM) ajuda manter um inventário atualizado desses ativos, o que pode contribuir simultaneamente com a gestão de identidades e gestão de vulnerabilidades.

Adotar privilégios mínimos e zero trust

A adoção do princípio do privilégio mínimo (least privilege) ajuda a reduzir o impacto de um vazamento de credenciais, uma vez que o invasor terá acesso reduzido aos sistemas corporativos. No entanto, dificilmente é possível realizar atividades de trabalho em que haja algum nível de privilégio, o que significa que essa invasão ainda pode ter consequências indesejáveis.

Quando possível, o privilégio mínimo deve ser expandido com a estratégia de zero trust. Nesse modelo, o usuário precisa ser novamente autenticado antes de realizar tarefas sensíveis, utilizando mecanismos como just-in-time access ou monitoramento de acessos.



Gerenciar o ciclo de vida de identidades

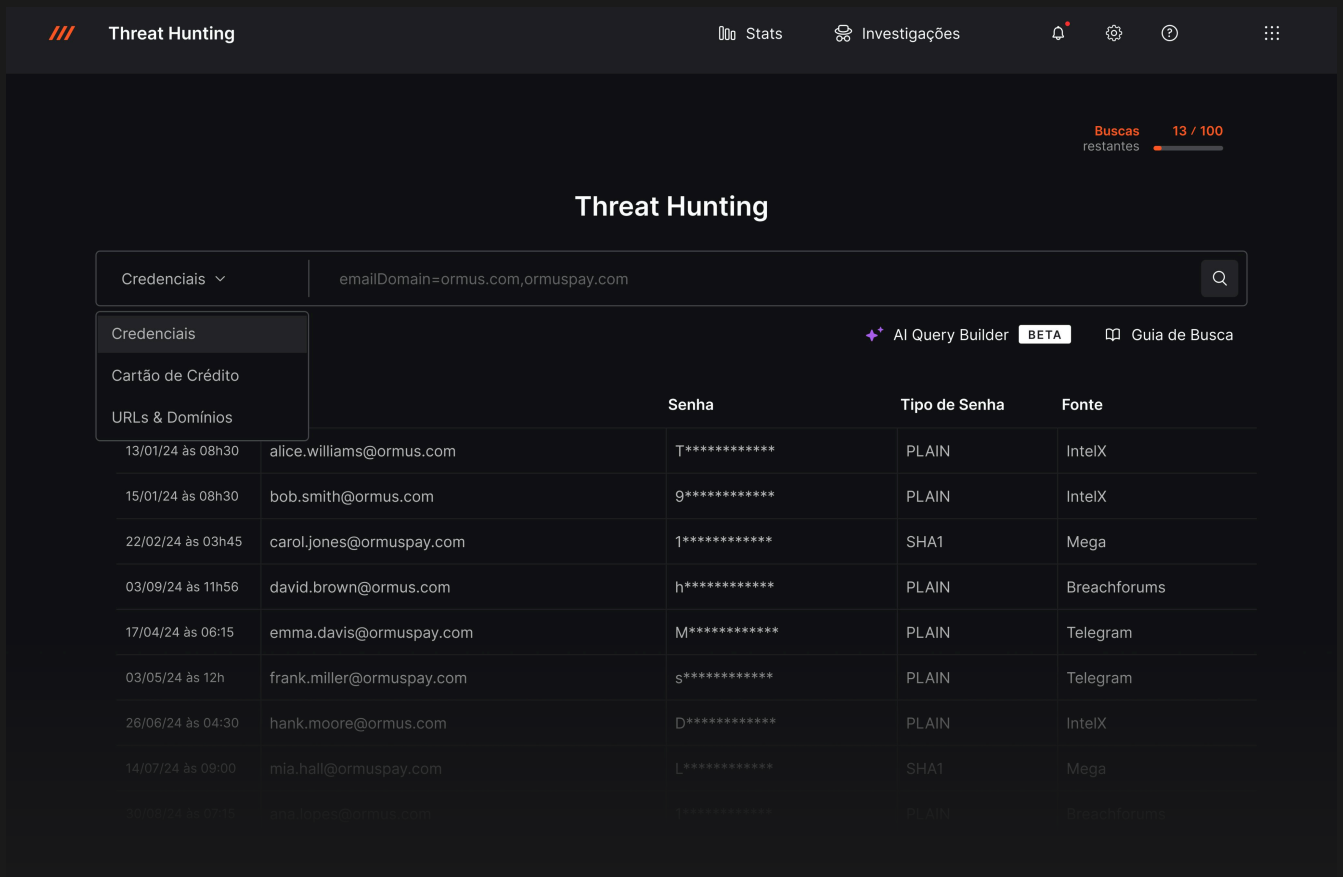
Há situações em que as credenciais mais vulneráveis são aquelas que ficaram de fora do processo de gestão de identidades. Isso acontece com certa frequência quando identidades obsoletas não são invalidadas nem perderam suas permissões. Por serem obsoletas, essas credenciais tendem a permanecer estáticas e válidas durante muito tempo, colocando em risco dados aos quais ela possivelmente nem tinha acesso quando foi criada.

Por esta razão, é importante que as credenciais sejam gerenciadas do início ao fim do seu ciclo de vida. Se necessário, as credenciais corporativas devem ser sanitizadas para eliminar credenciais que não são mais necessárias.

Utilizar MFA resistente a phishing

Apesar dos infostealers serem capazes de derrotar algumas implementações da autenticação multifator, a MFA ainda tem seu papel na proteção de identidades, principalmente em cenários de phishing. Por isso, é ideal que a solução de MFA adotada seja resistente a phishing, o que significa evitar soluções baseadas em one-time password (OTP) criadas por aplicativo ou enviadas por SMS – sendo este último o método menos recomendado. Como essas senhas únicas podem ser informadas pelo usuário ao atacante em um cenário de phishing, elas são consideradas mais vulneráveis.

Embora as chaves FIDO e cartões físicos sejam considerados superiores, há complicações técnicas e custos que podem tornar esses métodos inviáveis. A autenticação por autorização via aplicativo é uma alternativa, mas é importante combiná-la com a conscientização dos colaboradores a respeito de ataques de MFA Fatigue ou push bombing.



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.

Descubra como nossas soluções irão transformar sua estratégia de segurança

AGENDE UMA DEMO

Gartner Peer Insights 4.8

Descubra todas as soluções em **axur.com**

AXUR