AXUR

EBOOK

Ataques em autenticação multifator

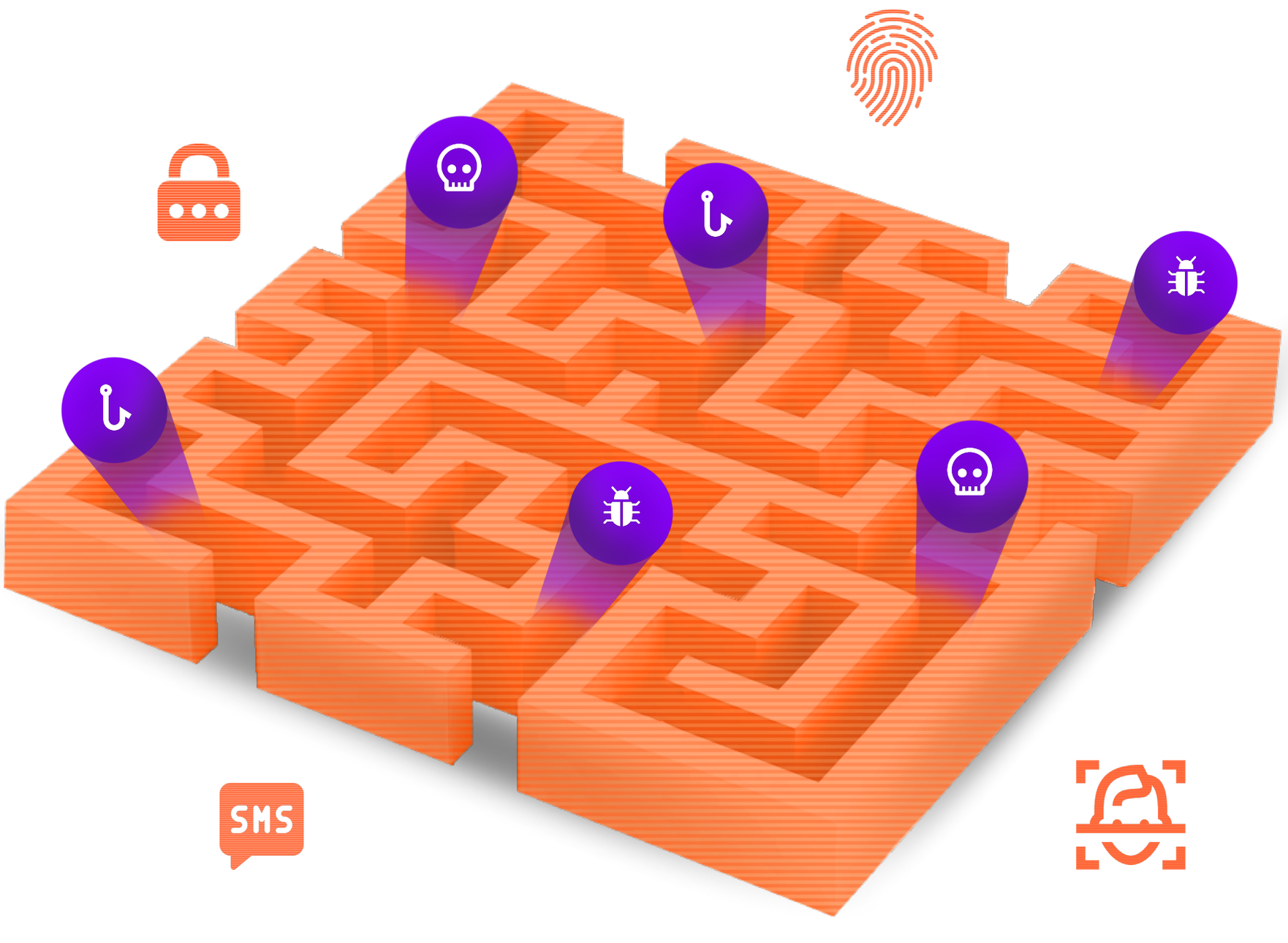
O cibercrime evolui em táticas e lança novos mecanismos burladores de sistemas de proteção. Saiba como os ataques funcionam e como se proteger.

O que você vai encontrar neste ebook

Definição de MFA

MFA	**Multi-factor authentication**: é a **autenticação multifator**. É um processo de autenticação em que a concessão do acesso depende do fornecimento de mais **de um fator ou evidência**. Em uma tentativa de preservar as iniciais do termo em inglês, algumas definições em português usam o termo "múltiplo fator de autenticação"
2FA	Quando apenas dois fatores são usados, é comum o uso da sigla 2FA (two-factor authentication)

Resumo executivo



A gestão de identidades é um dos grandes desafios da segurança da informação. Diante das fragilidades do processo tradicional de autorização com login e senha, muitas empresas e serviços vêm migrando sistemas para uma autenticação mais robusta e com múltiplos fatores.

Os primeiros resultados da autenticação multifator surpreenderam, bloqueando diversas técnicas de invasão. Ainda hoje, ataques menos sofisticados continuam sendo barrados pela mera existência de um segundo fator de autenticação.

Por outro lado, não podemos deixar que esse aparente sucesso se torne uma armadilha e nos impeça de enxergar os ataques que já estão derrotando a autenticação multifator.

Mecanismos de autenticação antes tidos como robustos (como o envio de SMS) já são considerados insuficientes e, segundo a Agência de Cibersegurança e Infraestrutura dos Estados Unidos (CISA), não integram mais o "padrão ouro" da autenticação mutifator. Quem depende exclusivamente de mecanismos mais frágeis está exposto a um risco maior do que talvez imagine.

O phishing foi reinventado para funcionar contra a MFA, e criminosos desenvolveram novas categorias de malware dedicadas a roubar sessões autorizadas e explorar brechas nas implementações da autenticação. Dois fornecedores de soluções de MFA foram invadidos em 2022, violando a segurança das contas protegidas, e brechas foram expostas nas redes de telecomunicação que entregam códigos de uso único.

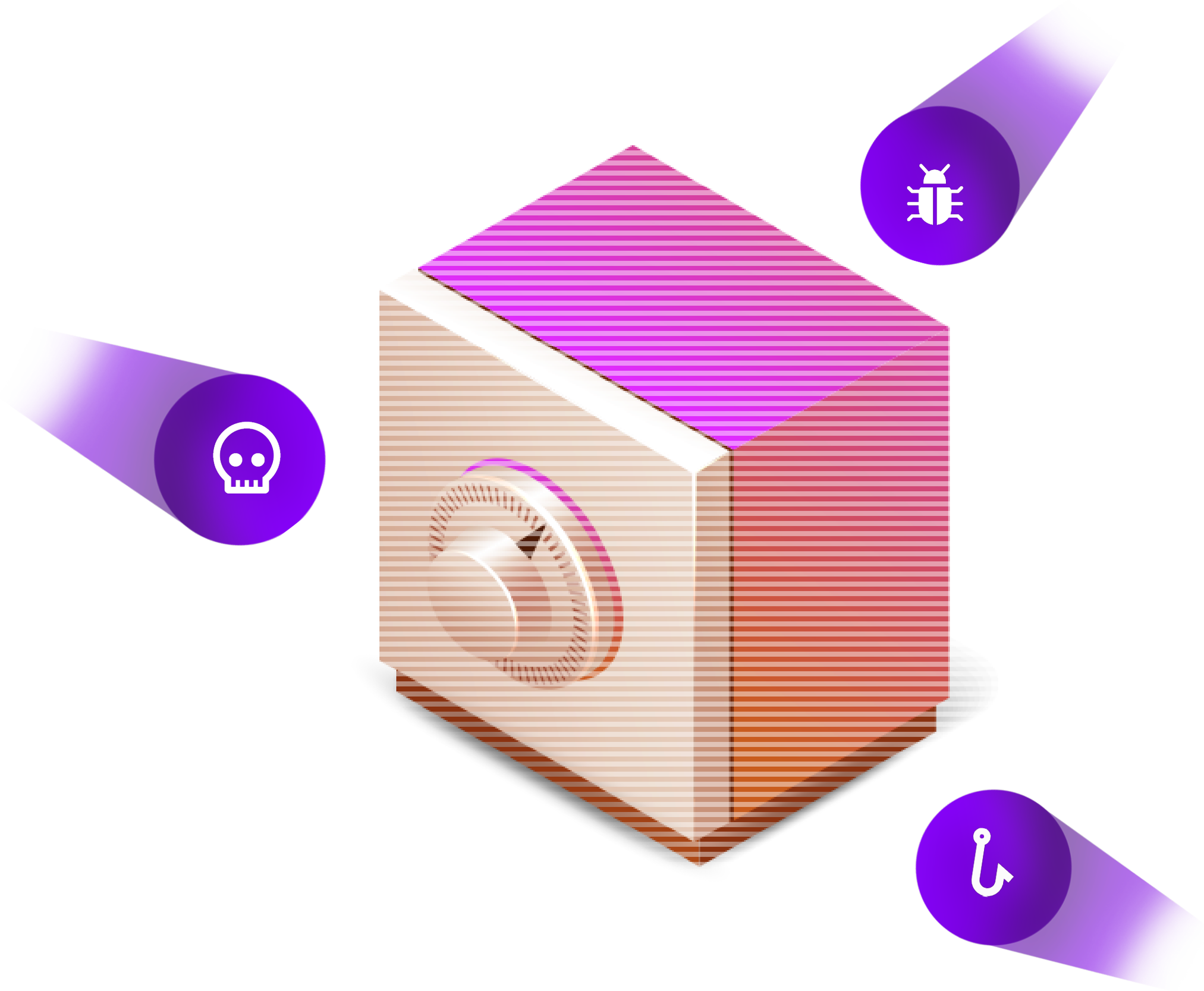
Prestadores de serviços digitais, que oferecem a autenticação multifator a seus usuários, enfrentam ainda mais obstáculos. Não há nenhuma visibilidade sobre as práticas de segurança do usuário, e raramente é viável apostar na conscientização. Deixar de oferecer mecanismos de autenticação cômodos, como o SMS, pode fazer com que o usuário abandone por completo a MFA, o que fragilizaria ainda mais a segurança da conta.

Este documento mostra como estes ataques funcionam, cita exemplos de seu uso e sugere o uso de monitoramento de credenciais vazadas como uma forma descomplicada de melhorar a confiabilidade do processo de autenticação – por não depender de nenhuma mudança no processo de autenticação existente, é fácil de ser integrado ao ecossistema.

O monitoramento também não depende da visibilidade sobre as práticas do usuário, evitando diversos percalços. Além disso, o acesso a dados vazados fornece meios para que uma organização detecte vazamentos e bloqueie acessos indevidos, protegendo inclusive contas de e-mail que são usadas como mecanismos de recuperação em sistemas de MFA.

Ao entender esse cenário, fica claro que o monitoramento pode ajudar a mitigar as vulnerabilidades do MFA e interromper invasões que podem resultar em ações de ransomware, vazamentos de dados e prejuízos financeiros para a empresa.

A importância das credenciais e da MFA



Antes de abordar as aplicações e limitações da autenticação multifator, convém relembrar os motivos para se preocupar com a segurança do processo de autenticação. Os agentes maliciosos podem usar credenciais para acessar os sistemas corporativos, é claro, mas duas questões tornam essa ameaça preocupante: as fragilidades da própria credencial e a ligação indireta e ampla que cada credencial pode ter com todo o ecossistema da empresa.

No caso do sistema de login e senha tradicional, sem fatores adicionais, a proteção depende totalmente da senha. Esse cenário apresenta vários riscos:

- **A escolha da senha depende do usuário**. Nem sempre a credencial escolhida é forte o bastante e, mesmo que o sistema imponha certas regras quanto ao tamanho da senha e os tipos de caracteres necessários, as checagens são insuficientes. O usuário ainda pode escolher senhas de cunho especial (que contenham alguma data, nome de familiares, de animais de estimação, entre outros), ou então repetir senhas usadas em outros sistemas (inclusive contas de serviços pessoais) que foram previamente atacadas pelo agente malicioso.

- **A senha pode ter sido armazenada em local inseguro**. Seja uma anotação em papel, um e-mail deixado em contas pessoais ou até uma foto guardada no celular, raramente é possível garantir que não houve alguma violação da política de segurança que fragilize a senha do usuário.
- **É possível roubar a senha com malware, phishing e vários outros ataques**. Mesmo que a senha seja forte e não esteja armazenada em local inseguro, o usuário ainda pode ser atacado diretamente.
- **Acesso global**. A adoção de plataformas de software como serviço e a migração para a computação em nuvem permitem que colaboradores trabalhem de qualquer lugar. Da mesma maneira, as senhas vazadas podem ser usadas por invasores de qualquer lugar do mundo. Além de dificultar a atuação das autoridades policiais, o acesso global eleva a importância da credencial como mecanismo de acesso, pois dispensa a defesa tradicionalmente oferecida pelo perímetro físico da empresa.

Embora a senha seja frágil, ainda são diversos os ataques, ameaças e prejuízos que podem se materializar para toda a empresa a partir do vazamento de uma senha. Alguns exemplos:

- **Ransomware**. Muitas invasões que resultam em sequestro de dados e na paralisação das empresas começam com uma credencial corporativa: acesso a e-mail, rede privada virtual (VPN) e sistemas em nuvem. Sempre que necessário, o invasor emprega técnicas de movimento lateral para aprofundar o acesso inicial obtido, aumentando o escopo do ataque.
- **Vazamento de dados**. Toda informação acessível para o colaborador que teve sua senha comprometida também estará comprometida.
- Prejuízos financeiros. O acesso a sistemas de gestão financeira, compra e contratos pode gerar prejuízos financeiros diretos para a empresa.
- **Business Email Compromise (BEC)**. Ao se passar por executivos e diretores da empresa usando uma senha vazada, o criminoso pode forjar ordens de pagamento e solicitações de dados indevidas.
- **Outros prejuízos e custos**. Vazamentos de dados, ransomware e outras ações de invasores podem acarretar danos à marca e à confiança dos parceiros e clientes, além de justificar a aplicação de multas e outras ações de entidades regulatórias ligadas à proteção da privacidade e do consumidor.

Conforme sistemas são interligados ao ecossistema de TI da organização – incluindo as plataformas de software como serviço e outros sistemas de terceiros, como recrutamento, marketing, redes sociais e outros –, fica evidente a necessidade de aumentar a robustez do processo de autenticação.

É nesse cenário que surgem conceitos como a autenticação multifator, a autenticação step-up (também chamada de contexto de autenticação ou autenticação por etapa), o just-in-time access, entre outros, bem como a evolução das noções de privilégio mínimo (como no Zero Trust).

Sendo assim, o assunto da proteção das credenciais está em constante evolução, com inovações e aprimoramentos sendo propostos a todo instante. A MFA é uma dessas evoluções, mas os riscos e a complexidade do tema mostram que não há uma única solução definitiva para todos os contextos.

Nos capítulos seguintes, abordaremos as limitações mais associadas à MFA tradicional, na qual o login completo exige ao menos dois fatores de autenticação.

Limitações da MFA

Sendo a confidencialidade um dos pilares da segurança da informação, é necessário que algum mecanismo reconheça quem possui autorização para acessar um determinado recurso. A autenticação por meio da senha, embora seja uma solução tradicional, é vulnerável a diversos ataques: a senha pode ser roubada, adivinhada ou repetida pelo usuário, por exemplo.

Nesse contexto, um dos ataques mais simples é o phishing. Desde que seja possível enviar uma comunicação ao usuário (um e-mail, normalmente), um invasor pode tentar convencer a vítima a revelar sua senha em uma tela falsa e capturar a credencial de acesso.

O objetivo mais evidente da autenticação multifator é inviabilizar ataques de baixa sofisticação como o phishing tradicional, reforçando a autenticação simples com etapas adicionais.

Contudo, a adição de etapas adicionais não ocorre sem um aumento da complexidade. Além disso, a MFA muitas vezes é implementada sem uma visão adequada sobre a superfície de ataque e o papel que ela deve desempenhar. É nesse sentido que aparecem algumas limitações e percalços:

- **A ameaça de malware está fora do escopo da MFA**. Ainda que muitos códigos maliciosos sejam criados para roubar credenciais, a MFA não fornece uma proteção eficaz contra a ação desses malwares. Quando o malware atua diretamente a partir do endpoint do usuário (ou seja, o invasor controla o dispositivo durante o acesso do usuário), o invasor se aproveita de uma sessão autenticada em andamento. A não ser que a MFA tenha sido pensado para ações específicas, ela não vai atuar nesse cenário.
- **A autorização em si pode ser atacada.** A MFA melhora o processo de obtenção da autorização, mas não reforça o mecanismo de autorização em si. Em implementações mais simples da MFA, esse ponto é esquecido e a autorização é idêntica à de uma conta com fator único.
- **A MFA pode exigir um novo processo de recuperação de conta.** Se a recuperação de uma conta protegida por MFA ocorrer da mesma forma que a de uma conta sem MFA, o elo mais fraco da corrente é transferido da credencial ao processo de recuperação. Porém, mesmo uma implementação correta da recuperação de conta não elimina ataques contra esse processo.

- **Os fatores adicionais da MFA também podem ser atacados.** Em isolamento, cada fator é vulnerável a ataques específicos. Como a senha é um alvo antigo e comum, os ataques existentes contra os demais fatores muitas vezes passam despercebidos.

Veremos a seguir como essas limitações e dificuldades se manifestam nas implementações práticas da MFA no mundo real.

MFA ou 2FA?

O conceito da MFA abrange qualquer situação em que o usuário de uma aplicação precisa combinar mais de um tipo de evidência ou autorização para obter acesso ao ambiente. A implementação correta deste método exige que os "fatores" usados sejam de natureza distinta: algo que se "sabe" (uma senha), algo que se "é" (biometria) ou algo que se possui (chave, cartão, celular, entre outros).

Mais recentemente, a localização do usuário também tem se mostrado um fator viável. No Brasil, ela já aparece como complemento em sistemas que controlam os turnos de trabalho, condicionando a autorização do início do ponto à uma localização predeterminada.

Embora a teoria não esteja limitada a implementações específicas, o uso da MFA é acompanhado de complexidades. De fato, é bastante raro que o processo de autenticação exija mais de dois fatores e, por essa razão, a MFA é mais conhecida pelo nome de 2FA, ou "verificação em duas etapas".

Embora as línguas latinas sofram com inconsistências de tradução – que se somam às inconsistências no uso da terminologia em inglês –, muitas vezes é uma variação do termo "2FA" que aparece nas opções de segurança dos aplicativos. No WhatsApp, por exemplo, ela se chama "confirmação em duas etapas".

No âmbito corporativo, acrescentar mais de um fator pode ser ainda mais difícil, tanto pela necessidade de dar suporte a mais de um produto ou plataforma como pelos custos envolvidos na aquisição de hardware especializado ou serviços de apoio.

Em resumo, embora a MFA contemple mais de dois fatores de autenticação, usar três ou mais fatores não é uma prática comum. Um terceiro fator de autenticação muitas vezes não traz um ganho proporcional de segurança, ainda que aumente a complexidade e a inconveniência ao usuário. Por essa razão, esses fatores adicionais costumam ficar restritos a aplicações e sistemas de alto risco.

Ainda que seja importante observar que o invasor terá de burlar dois fatores de autenticação – e não três ou quatro –, alguns dos ataques contra a MFA continuariam funcionando mesmo que fossem adicionados mais fatores de autenticação. Isso acontece porque, como observado, a segurança nem sempre é proporcional ao número de fatores.

Como o termo "MFA" também inclui o 2FA e muitos ataques têm potencial para funcionar em ambos, normalmente não há uma separação ou diferenciação entre eles. Ou seja, um ataque contra 2FA é um ataque contra MFA e vice-versa.

Os fatores de autenticação

Os mecanismos de autenticação são divididos em três fatores: algo que se sabe, algo que se possui e algo que se é (características inerentes ao usuário). Cada fator é uma categoria; um sistema que exige duas senhas não utiliza dois fatores de fato, pois as duas requisições se enquadram em um mesmo fator.

Quando um processo de autenticação exige uma senha gerada em tempo real em um aplicativo no celular, o objetivo da senha de uso único é comprovar a posse do dispositivo – do celular ou a chave capaz de gerar a senha, contemplando o fator "algo que o usuário possui".

Embora a senha de uso único (one-time password) gerada por aplicativo ou recebida por SMS seja uma "senha", ela não deve ser confundida com a senha em si, pois esta última verifica algo que o usuário sabe e está encaixada em outro fator.

Não existe um único mecanismo para cada fator, o que leva a uma grande variação nas formas e tipos de MFA existentes no mercado. Como não é incomum que uma mesma pessoa tenha contato com várias formas de MFA, **a sobrecarga de fatores de autenticação** acaba contribuindo com os invasores, já que os usuários podem facilmente confundir um método com outro.

Mecanismos usados como fatores de autenticação

Fator	Mecanismos
Conhecimento o usuário “sabe”	Senha PIN Desenho de padrão
Posse o usuário “possui”	**Smartphone** Chave geradora de senha temporária (OTP) Linha telefônica (SMS) Acesso prévio (notificação PUSH, aplicativo autenticado) **Dispositivos em geral** Chave privada salva no dispositivo **Outros** E-mail Chave criptográfica USB (U2F/FIDO) Smartcard (PKI) Token gerador de senha
Natural/Próprio o usuário “é”	Voz Íris Face Digital

A utilização de múltiplos fatores de autenticação causa inconveniências ao usuário e, por esta razão, não é incomum que o mecanismo seja flexibilizado. Nesse cenário, o usuário escolhe se quer utilizar um código gerado por aplicativo, uma autorização no celular ou uma chave criptográfica USB – todos funcionam, mas apenas um é obrigatório para cumprir a exigência do fator. Para o usuário, essa redundância pode ser útil no caso de algum problema nos mecanismos configurados (defeito no celular, ausência de sinal para receber SMS, entre outros).

Infelizmente, esta prática acaba reduzindo a segurança do utilizador, já que o invasor só precisa comprometer um único mecanismo para acessar à conta. Por exemplo: se um usuário pode usar códigos recebidos por SMS ou aplicativo, o invasor pode acessar a conta por meio da rede móvel, do chip, do aparelho ou da chave. Retirando a opção de SMS, o invasor é obrigado a recorrer às duas últimas opções, pois o serviço de telecomunicação deixa de estar envolvido.

Por esta razão, é preciso ter ciência de que o uso de mais de um mecanismo de autenticação dentro do mesmo fator contribui com a conveniência e com a disponibilidade da conta, não com a confidencialidade.

Os ataques contra a MFA

Este capítulo vai abordar ataques concretos capazes de burlar a autenticação multifator. Os ataques podem ser divididos em duas grandes categorias: aqueles que funcionam independentemente do mecanismo adotado, e aqueles que são voltados para atingir mecanismos específicos.

Ataques contra qualquer mecanismo

Malware

- **Em 2022, a Axur extraiu 435,98 milhões de credenciais roubadas a partir da análise de 7,4 TB de arquivos gerados por credential stealers e compartilhados no submundo do crime.**

O uso de fatores adicionais na autenticação não tem efeito na atuação de um malware. Um código malicioso instalado no dispositivo da vítima pode até permitir o controle remoto do sistema, dando ao invasor o mesmo nível de acesso delegado ao usuário após o login.

O malware também pode servir de acessório para outras modalidades de ataque à MFA, como o roubo de cookies de sessão, spear phishing e MFA fatigue.

Uma das principais vantagens do malware é a possibilidade de disseminá-lo usando iscas sem ligação direta com o sistema de autenticação. A vítima pode instalar um malware enquanto busca o download de um programa comum e, sem suspeitar, terá suas informações roubadas após conceder as permissões indevidas ao malware que supostamente seria um programa de confiança.

Esse cenário tem sido bastante comum, inclusive para pessoas que não adotam comportamentos inseguros em sua navegação. Golpistas fazem uso de perfis em redes sociais, anúncios on-line e outros mecanismos para divulgar links que levam ao download de softwares adulterados. A prevalência dos malwares em anúncios levou o FBI a recomendar o uso de um bloqueador de anúncios na web como medida de prevenção.

O malware também pode atuar nos dispositivos pessoais do colaborador de uma empresa, roubando as credenciais por um caminho com visibilidade reduzida para os departamentos de segurança e de tecnologia.

Embora a solução tradicional contra a atuação dos malwares seja a utilização de um antivírus, essa medida por si só tem se mostrado ineficaz. Os malwares do tipo credential stealer podem ser reconfigurados, adaptados e reciclados constantemente, e a atualização do antivírus pode acabar chegando só depois que as credenciais já foram roubadas.

Phishing, spear phishing e VISHING

- **Em 2022, a Axur detectou 34 mil páginas de phishing**

Embora a autenticação multifator seja muito citada como uma medida de prevenção contra as consequências do phishing, este ataque pode ser adaptado para funcionar em um cenário com MFA. O spear phishing (mensagem redigida para um alvo específico) pode ser especialmente eficaz para casos em que o invasor já possui alguma informação sobre a vítima.

Entre as possibilidades estão:

- **Roubo de códigos de recuperação**. A maioria dos sistemas de MFA permitem o uso de códigos de recuperação gerados previamente. O objetivo é garantir que o usuário mantenha o acesso à conta em situações imprevistas, como a perda do celular, da chave USB ou da linha telefônica. Em vez de roubar a senha, o phishing pode ser empregado para roubar o código de recuperação que, por ser fixo, continuará válido para um uso posterior.
- **Etapa inicial de outros ataques**. A mensagem de phishing pode conter links usados para disseminar malware, roubar cookies ou realizar ataques de interceptação.

A rede social Reddit anunciou no início de 2023 que um funcionário foi vítima de um spear-phishing que clonou o visual do ambiente interno da empresa para enganar o usuário.

No caso do vishing (voice phishing, ou phishing por ligação telefônica), o golpista pode tentar telefonar para a vítima e confundi-la solicitando o código recebido por SMS ou a confirmação de outro mecanismo para uma finalidade diferente (uma promoção ou checagem de segurança, por exemplo). Após a vítima realizar a ação solicitada ou informar o código, o invasor terá todas as informações necessárias para realizar o acesso naquele exato instante.

A fornecedora de equipamentos de rede Cisco foi alvo de vishing em 2022. Segundo o relatório da empresa, o invasor derrotou a MFA da conta Google de um funcionário que havia armazenado e sincronizado a senha da rede corporativa em seu navegador Chrome, permitindo que o atacante obtivesse as senhas sincronizadas após acessar a conta Google da vítima.

Esses ataques podem ser mais efetivos depois que a credencial básica (usuário e senha) já tiver sido obtida por outro meio (malware, por exemplo). Senhas repetidas também são um risco neste caso, pois muitos sistemas de login validam a senha (que pode ter vazado de outro serviço) antes de solicitar o segundo fator.

Depois de validar a senha, o atacante pode iniciar as tentativas de phishing do segundo fator tendo a certeza de que está com a senha correta para derrotar o primeiro fator.

Roubo de sessão e cookies (pass-the-cookie)

A MFA exige várias evidências para conceder a autorização de login. Contudo, a autorização em si normalmente é armazenada em um cookie no navegador web ou no aplicativo. A cada visita do usuário, é realizada uma conferência dos parâmetros desse cookie e, constada a existência de uma autorização válida, o usuário continua navegando ou usando a aplicação.

Obtendo esse código de autorização, é possível utilizá-lo para entrar diretamente na conta, sem passar pelo processo de login. Alguns serviços e plataformas adotam checagens visando impedir que o cookie entregue a um navegador funcione em outro, mas a efetividade dessa proteção pode variar de um caso para outro. Esse tipo de ataque é chamado de pass-the-cookie.

Os malwares credential stealers rotineiramente incluem os cookies de sessões autorizadas no pacote de informações roubadas dos computadores contaminados. O conjunto de dados é vendido a outros interessados no submundo do crime, que podem avaliar a melhor forma de utilizar a sessão capturada.

A engenharia social aliada ao phishing também pode ser empregada para roubar a sessão. Nesse caso, o usuário é convencido a colar um código em seu navegador web para roubar os cookies que sejam de interesse do atacante.

O risco ainda é mais elevado em serviços sem criptografia. Nesse caso, o roubo de sessão pode ser realizado por qualquer agente malicioso na mesma rede. Em 2010, um aplicativo chamado Firesheep demonstrou como esse ataque poderia ser realizado com facilidade em redes Wi-Fi públicas, por exemplo.

A maioria das grandes plataformas e aplicações hoje utilizam criptografia, como a TLS (Transport Layer Security). Contudo, aplicações corporativas que fazem uso da MFA precisam utilizar criptografia adequada para evitar o roubo de sessão em redes compartilhadas.

Interceptação e intermediação (AiTM)

O ataque de "homem no meio", que hoje vem sendo chamado de "adversário no meio", é caracterizado por um cenário em que o agente malicioso conseguiu se posicionar "entre" o usuário e o serviço que será acessado.

Esse cenário pode ser facilmente construído por meio de um link enviado em um phishing. Em algumas situações mais específicas, pode ser possível redirecionar o acesso do usuário para uma página falsa e, caso a vítima não esteja atenta à barra de endereços e outras indicações do navegador, o redirecionamento pode passar despercebido.

Ao contrário do phishing tradicional, em que a página falsa apenas captura a credencial informada, esse ataque faz uso de intermediação (ou "proxy") de acesso: todas as informações e interações feitas pelo usuário são remetidas à página verdadeira. Se a senha digitada for incorreta, o usuário verá um erro; se houver mais de um fator de autenticação, ele será perfeitamente replicado.

As diferenças começam quando o usuário finaliza o processo de login. Nesse momento, em vez de enviar o cookie de sessão e outras informações de autorização ao navegador do usuário, os dados são enviados ao atacante para que ele possa acessar a conta.

Sendo assim, a concretização do ataque pode depender do emprego de uma tática de pass-the-cookie ou pela automatização das ações maliciosas que o invasor pretende realizar.

Embora pareça sofisticado, esse ataque pode ser facilmente orquestrado com ferramentas prontas e gratuitas como Evilginx2, Modlishka e Muraena. O atacante só precisa configurar um domínio e um servidor web para criar o site falso com uma dessas soluções.

Ataques deste tipo já foram registrados pela Microsoft contra vários de seus clientes. Em julho de 2022, a empresa revelou que mais de 10 mil organizações que usam a nuvem Azure ou Microsoft 365 tinham sido alvo de ataques desse tipo.

Autorização de aplicações (OAuth)

Uma das vantagens de muitas plataformas de software como serviço (SaaS) é a possibilidade de integrar aplicações externas. Para que as aplicações sejam compatíveis com a MFA, elas precisam ser vinculadas ao acesso do usuário por meio de uma chave de autenticação (OAuth) com canal de API (application programming interface).

Em resumo, trata-se de um canal de acesso dedicado a aplicativos conectados, o que gera prós e contras para o invasor. O acesso é mais limitado do que o login real, mas o invasor terá mais facilidade para automatizar a coleta de dados usando a API. Seja como for, o acesso não passa pela MFA depois de ser concedido pelo dono da conta.

Como as capacidades desse canal de acesso e o funcionamento dele nem sempre estão claros para todos os usuários, invasores já se aproveitaram disso para tentar convencer as vítimas a autorizar aplicativos nas contas delas. Outra possibilidade é o uso de aplicativos autorizados por OAuth com a finalidade de construir um acesso persistente após um login bem-sucedido.

Outra variação desse conceito pode envolver tokens de single sign-on (SSO), embora isso normalmente dependa da implementação ou até de vulnerabilidades técnicas no serviço de login.

Seja como for, a obtenção de um token OAuth autorizado permite burlar o processo de autenticação.

Uma vez concedida, essa permissão às vezes é separada das sessões do usuário. Ou seja, o acesso não é removido quando o utilizador encerra todas as sessões abertas. Se a token da API ou OAuth não puder ser facilmente revogada, é possível inclusive que ela permaneça válida após a troca da senha da conta.

O risco representado por essas autorizações indevidas fez com que muitos serviços restringissem o uso de suas APIs. No caso de sistemas corporativos e OAuth, pode ser necessário conferir as permissões e configurações do ambiente para verificar se os usuários podem ou não delegar esse acesso a terceiros.

Ataques a mecanismos específicos

MFA Fatigue

- **Mecanismo atacado**: notificação push / acesso prévio

Também chamado de "push bombing", o MFA Fatigue é usado para burlar sistemas de MFA por notificação push. Esse é o mecanismo de MFA em que o usuário recebe um aviso no smartphone solicitando a confirmação de um acesso iniciado em outro dispositivo.

Além de aplicativos dedicados ao recebimento das notificações push para confirmação, outra abordagem semelhante prevê o uso de um dispositivo previamente autorizado para confirmar o acesso de uma nova sessão.

Para realizar esse ataque, o invasor faz diversas tentativas de login usando a credencial da vítima para que cada uma gere uma solicitação de confirmação de acesso. Nessa situação, a vítima pode acabar confirmando o acesso do invasor por se cansar das mensagens de aviso, por um toque acidental na tela ou até por ter confundido uma tentativa própria de acesso com a do invasor.

Em setembro de 2022, o Uber revelou que o grupo criminoso Lapsus$ conseguiu burlar sua autenticação multifator usando o MFA Fatigue.

SIM Swap, Spoofing E SS7

- **Mecanismo atacado**: código por SMS

Um atacante pode interferir no encaminhamento de códigos por SMS de duas maneiras: alterando o chip que receberá o código ("SIM swap") ou interferindo no protocolo de comunicação entre as operadoras de telefonia, o Signalling System 7 (SS7).

Os ataques ao SS7 são mais raros e são mais efetivos quando há algum erro de implementação ou vulnerabilidade. Mesmo assim, a operadora de telefonia O2, da Alemanha, confirmou em 2017 que clientes bancários tiveram suas contas roubadas porque criminosos conseguiram redirecionar SMSs para confirmação de transferências para números controlados pelos ladrões.

Vale lembrar que invasores também conseguiram utilizar o serviço de caixa postal dos celulares para gravar códigos de autorização recebidos por chamada telefônica. Contudo, esses ataques não aconteceram por interferência direta no protocolo SS7 – os invasores se aproveitaram do Caller ID spoofing (falsificação de origem da chamada) oferecido por provedores de VoIP para acessar as caixas postais de forma irregular.

Ataques de SIM Swap, porém, são mais comuns. Eles ocorrem quando os invasores conseguem transferir a titularidade de uma linha móvel para outro chip, muitas vezes graças à atuação de cúmplices da quadrilha criminosa dentro das empresas de telecomunicação.

Nos Estados Unidos, as autoridades acusaram vários indivíduos de realizar crimes envolvendo SIM Swap, em especial para roubar criptoativos. Vários deles eram ex-colaboradores de operadoras de telefonia como AT&T e Verizon. Isso motivou a criação de novos procedimentos de segurança para dificultar a transferência da linha para outro chip.

De qualquer forma, todos os mecanismos com base em SMS dependem da segurança do provedor de serviços de telecomunicação.

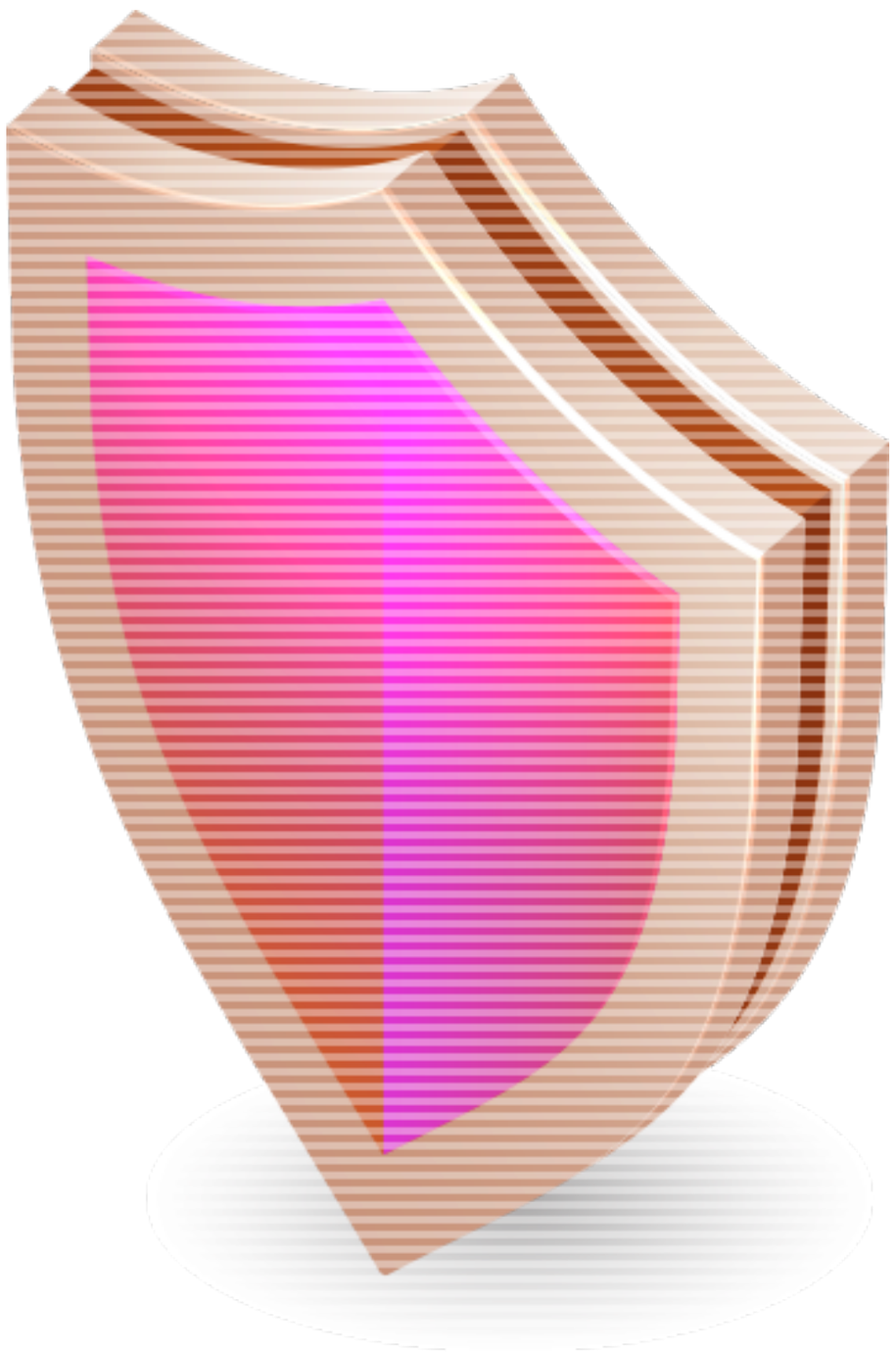
Extravio

- **Mecanismo atacado**: código por SMS, OTP, chave USB, chave embutida em dispositivo

Como a MFA utiliza "algo que o usuário possui" como um fator de autenticação, o invasor pode optar por roubar o dispositivo. A efetividade do roubo pode variar de um caso para outro – por exemplo, cartões SIM com chip e celulares bloqueados podem não ser úteis para o invasor. Já outros mecanismos, como chaves USB, não utilizam nenhuma autenticação adicional para a liberação da chave armazenada.

Para mitigar as consequências, é importante que a vítima informe o extravio o quanto antes, o que nem sempre vai acontecer. A existência de mecanismos adicionais de autenticação pode acabar permitindo que o usuário continue acessando sua conta através de outros mecanismos. Além disso, é possível que a vítima confunda o roubo com algo menos grave (uma simples perda ou esquecimento), o que pode retardar a comunicação do extravio.

Como evoluir na segurança dos acessos



Muitas das técnicas viáveis para violar a autenticação multifator só podem ser empregadas depois que o atacante já obteve a credencial (usuário e senha) da vítima. Por essa razão, há uma oportunidade para melhorar a segurança do processo se pudermos proteger a própria credencial.

Combinados com um processo robusto de resposta a incidentes, dados sobre credenciais vazadas ajudam a detectar e mitigar incidentes de segurança, indicando quais credenciais estão em risco e precisam ser bloqueadas pela empresa.

Da mesma forma, informações provenientes de Cyber Threat Intelligence (CTI) sobre a atuação dos atacantes podem identificar o vazamento de tokens de autenticação ou cookies que caíram nas mãos de criminosos.

Esses dados são obtidos pelo **monitoramento de credenciais da Axu**r por meio do acompanhamento das movimentações dos agentes maliciosos e da identificação de dados vazados na Web (seja na Surface Web, na Dark Web ou na Deep Web).

Ao ser alertada sobre uma credencial obtida por criminosos, a empresa pode dar início ao processo de resposta a incidente e impedir que ela seja usada em ataques. A possibilidade de **automação** desse processo aumenta ainda mais as chances de mitigar ou até evitar um incidente.

Visão fora do perímetro

Uma das vantagens do monitoramento da Axur é o acesso aos dados obtidos por malwares do tipo credential stealer. As informações capturadas por esses malwares são distribuídas no submundo do crime digital em arquivos de "log", os quais trazem dados do sistema, senhas, cookies e outros dados especificados pelos operadores do código malicioso.

Dessa maneira, o monitoramento é capaz de dar visibilidade para credenciais roubadas em qualquer dispositivo, inclusive em sistemas de colaboradores remotos, clientes ou terceiros, **acrescentando uma camada de proteção tanto para a rede corporativa quanto para serviços digitais prestados a clientes e parceiros**.

Para clientes e parceiros

Para os fornecedores de serviços digitais que exigem credenciais de acesso de cada cliente ou parceiro, não é possível depender da segurança do dispositivo do utilizador. Infelizmente, qualquer violação de segurança decorrente de um ataque de phishing ou malware sofrido pelo usuário vai gerar transtornos também para esse fornecedor – tanto pela atividade indevida na conta como pelo custo do suporte que precisará ser oferecido ao usuário para a recuperação do acesso.

O monitoramento de credenciais pode filtrar serviços ou domínios, detectando todas as credenciais vazadas para um serviço específico. Como prestador de serviços, você pode alertar os usuários sobre a necessidade da troca da senha ou desfazer mudanças na conta geradas por uma invasão.

Para colaboradores e funcionários

Com o trabalho híbrido no home office ou através de políticas de Bring Your Own Device (BYOD), muitas empresas têm permitido a utilização de dispositivos pessoais. A segurança desses dispositivos é um desafio para a equipe de segurança, pois nem sempre é possível registrar toda a atividade deles. Em outras palavras, há uma carência de visibilidade.

Além disso, as atividades pessoais realizadas pelo colaborador podem gerar riscos adicionais que são difíceis de estimar. Mesmo que a política de segurança organização proíba um tipo de uso do dispositivo, o usuário ainda pode violar a política de segurança ou as políticas de uso do dispositivo recebido para o trabalho.

Como o monitoramento enxerga credenciais vazadas independentemente de sua origem, uma atividade de malware ou phishing que atingiu o dispositivo pessoal do usuário também será detectada. É uma visibilidade que a empresa dificilmente teria de outra forma.

Benefício para usuários e para a empresa

Mesmo com a MFA disponível, nem todos os usuários optam por utilizá-la. Também há casos em que a empresa depende de sistemas que não oferecem MFA ou que não podem ser migrados para uma plataforma de single sign-on.

O monitoramento atua em qualquer um destes casos. Como é possível ver no quadro abaixo, a abrangência de detecções do monitoramento garante benefícios para usuários com ou sem MFA, pode alertar usuários sobre dados que podem aparecer em tentativas de spear phishing e ainda podem auxiliar a investigação de violações da política de segurança.

O monitoramento detecta:

- **Senhas roubadas**: para usuários ou sistemas sem MFA, proteger a senha é o mesmo que resguardar a segurança do processo de autenticação. Para usuários com MFA, uma senha roubada pode anteceder um ataque de phishing contra os códigos de recuperação, um golpe telefônico ou uma tentativa de MFA fatigue.
- **Cookies roubados**: os cookies de autenticação podem ser usados para acessar contas com ou sem MFA. Detectando e invalidando os cookies que caíram nas mãos dos criminosos, todos os usuários podem ser beneficiados.
- **Dados que podem ser usados por spear phishing**: o spear phishing caracteriza-se por uma mensagem extremamente personalizada, e o atacante pode utilizar dados pessoais da vítima obtidos para deixar a mensagem mais confiável. Com o monitoramento, usuários de alto privilégio podem ser alertados sobre as informações pessoais que vazaram e que podem ser aproveitadas nesse tipo de ataque.

- **Dados que podem violar sistemas de recuperação**: a MFA exige que organizações e prestadores de serviços adotem mecanismos de recuperação para os casos em que o segundo fator não estiver disponível. As credenciais roubadas podem dar acesso a sistemas de e-mail ou outros dados ligados a esse processo, fragilizando a MFA.
- **Violações da política de segurança**: os logs dos credential stealers quase sempre incluem informações a respeito do sistema do usuário. Essas informações podem ajudar a empresa a determinar se uma conta corporativa foi acessada a partir de dispositivos pessoais ou se o usuário cadastrou o e-mail corporativo em outros serviços.

Quer verificar sua segurança?

Agende uma demonstração gratuita da plataforma Axur e saiba como o monitoramento de ameaças pode ajudar a sua empresa a ficar protegida em toda a superfície externa.

Sobre a Axur

A Axur possibilita a escala e automatização do tratamento de ameaças cibernéticas para apoiar os times de segurança da informação e proporcionar experiências digitais mais seguras. A nossa plataforma de Threat Intelligence tem o tempo de reação mais rápido do mercado, solicitando takedowns automáticos, 24×7.

Isso é possível porque a plataforma Axur atua em quatro camadas: além da detecção, as tecnologias de inspeção, automação e remoção diminuem muito o tempo médio de contenção (MTTC) dos times de segurança. Além disso, nossos especialistas em Inteligência Cibernética expandem a investigação tanto na Surface como na Deep & Dark Web, tornando a Axur a empresa líder em Cyber Threat Intelligence na América Latina.

Detecte e remova ameaças com a plataforma All-in-one nº 1 do mercado

AGENDE UMA DEMO

CONVERSE COM UM ESPECIALISTA

Contato para imprensa:
Letícia Peres
press@axur.com
+55 (11) 9 3209.7588