EBOOK

Tokens para Rastreamento de Banco de Dados

O tratamento de dados se tornou essencial e, até, determinante para o sucesso de muitos negócios. Embora a proteção dessas informações seja um desafio, adotar tecnologias que auxiliem no controle patrimonial das bases de dados ajuda a mitigar os riscos inerentes à atividade e ampara a empresa diante de clientes e obrigações legais.

O que são tokens em bancos de dados?

Os tokens em bancos de dados são informações aparentemente legítimas registradas pelo controlador da base para fins de auditoria e rastreamento. Na prática, é um registro ou cadastro exclusivo que deve distinguir uma base de dados de todas as demais.

Para entender a utilidade do token, é preciso conhecer um pouco sobre a natureza dos vazamentos de dados que costumam ocorrer na web.

Quando um banco de dados é vazado na web, a procedência da informação nem sempre é informada. O site “Have I Been Pwned”, que registra vazamentos, contabiliza mais de 114 mil “pastes” – arquivos expostos sem origem clara, mas que possuem dados pessoais. A Axur, apenas no último ano, contabilizou 3,5 milhões de credenciais vazadas nesse formato.

Um vazamento não identificado só não é pior do que aquele em que a origem dos dados é falsificada com o intuito de despistar os analistas de segurança e os encarregados da base. Nas redes sociais e até na imprensa profissional, essas atribuições indevidas induzem jornalistas e consumidores ao erro. Muitas vezes, a negativa da empresa não é suficiente para assegurar a confiança do consumidor.

Também é comum que uma determinada informação (como o cadastro de um cliente) exista de forma idêntica nas bases de muitas empresas. Afinal, é bastante provável

que um cliente preencha os mesmos dados sempre que solicita um produto ou serviço. Sendo assim, a verificação dos registros expostos em um vazamento pode não ser suficiente para comprovar a origem.

A existência de um registro exclusivo na base de dados, como o token, permite sanar essas dúvidas. Como o token não deve existir em nenhum outro local, a presença do token em um vazamento funciona como uma etiqueta de controle patrimonial, atuando como um indício da procedência dos demais dados expostos.

Além disso, o token é capaz de cumprir o papel de chave de pesquisa para localizar uma base divulgada sem autorização. Um token deve ser inserido apenas em um banco de dados particular e específico, ele jamais deve aparecer na web. A mera publicação deste dado é um indício de que pode ter ocorrido um acesso indevido ou uma violação da política de uso de dados da empresa, podendo motivar o início de um processo de tratamento de incidente.

Os tokens para bancos de dados são às vezes chamados de “honey tokens” em referência aos “honeypots” – sistemas vulneráveis que monitoram tentativas de invasão para coletar informações sobre ataques antes que eles atinjam sistemas legítimos. Os tokens em bancos de dados, porém, não são expostos intencionalmente como isca – eles são apenas um “carimbo” digital.

Seja como for, os bancos de dados já estão na mira dos invasores. De acordo com um relatório publicado pelo

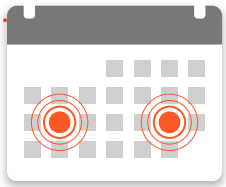
Identity Theft Resource Center (ITRC), uma ONG norte-americana que acompanha assuntos ligados à privacidade e proteção de dados, o ano de 2021 bateu o recorde de vazamentos, com 1.862 incidentes. Os números da Axur refletem esta tendência: foram identificados 2,8 bilhões de registros nos vazamentos que mapeamos em 2021.

Para garantir todos os benefícios do token, vinculados ou não ao monitoramento da web, ele deve ser aplicado de maneira compatível com as características e necessidades da base. O tamanho da base, os métodos de acesso e o compartilhamento das informações são alguns dos critérios que devem ser levados em consideração.

As várias utilidades do token

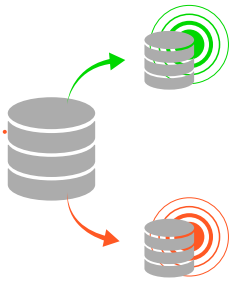
Temporal

Token que indica um **período de tempo determinado**. A presença dele indica o momento em que o acesso à base ocorreu.



Custódia

Token registrado unicamente em versões da base enviadas a terceiros, **diferenciando** cada uma.



Canais de acesso

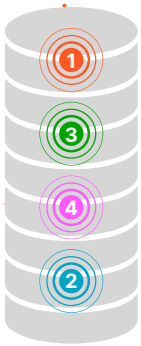
Tokens vinculados a **chamadas de API ou sistemas de uso interno**. Registra a cópia indevida de informações no canal contemplado pelo token.

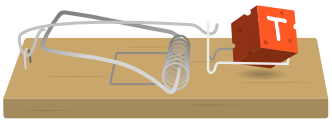
Dimensão

Bases maiores devem conter **tokens adicionais**. Permite a identificação da base mesmo que apenas um trecho seja exposto.

Posição

Tokens **não devem ser registrados em forma sequencial**. Isso aumenta a chance de inclusão do token em vazamentos parciais.





Honey tokens

Tokens **propositalmente expostos** como isca. São formas de criar sistemas vulneráveis que coletam informações sobre ataques antes que eles atinjam sistemas legítimos.

Como usar tokens

Quando utilizado de forma estratégica, o token identificado em um vazamento pode eliminar algumas variáveis ou dúvidas, revelando quando e como um banco de dados pode ter sido vazado.

Controle temporal

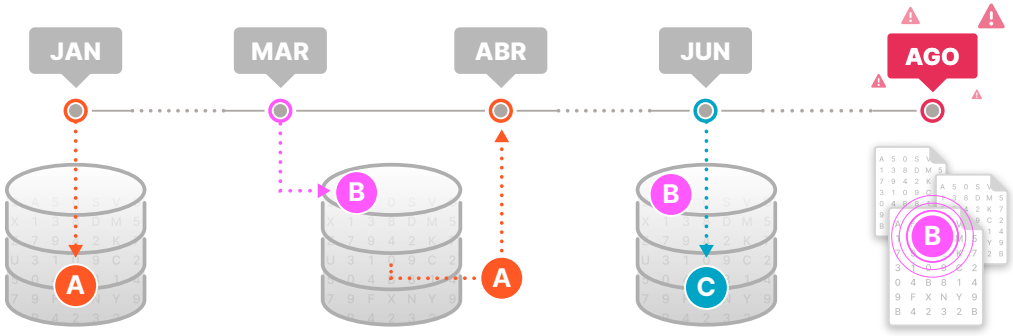
No processo de resposta e tratamento de incidentes de cibersegurança, há um grande valor em apurar quando o acesso indevido começou e por quanto tempo o invasor manteve sua presença. A partir deste marco temporal, é possível concentrar os esforços dos analistas e iniciar a construção da linha do tempo do incidente.

Os tokens podem ser um aliado nesse cenário. Com a adição e remoção de tokens em certos intervalos de tempo (mensal ou trimestral, por exemplo), a data do acesso ao banco de dados poderá ser estimada a partir da presença do token referente ao período.

Dependendo da quantidade de informações disponíveis sobre o vazamento e da estratégia utilizada para a inserção dos tokens, pode ser possível saber até se o acesso indevido ainda está em curso.

Exemplo de controle temporal

Tokens gravados em intervalos específicos podem identificar o período em que uma base foi copiada sem que seja necessário analisar a base inteira.

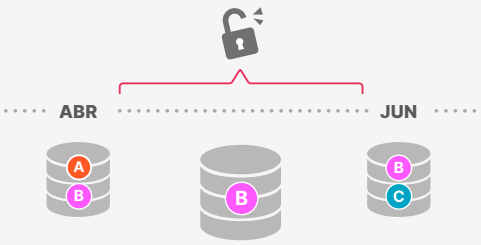


Token A é gerado e incluído no banco de dados.

Em março, o **Token B** é incluído à base de dados. Em abril, o **Token A** é removido.

Token C é adicionado em junho.

Um vazamento é identificado na web, em agosto, através do rastreamento do **Token B**.



Análise

A análise mostra que o banco vazado não possui os tokens **A** e **C**.

É possível estimar que o acesso indevido ocorreu entre abril e junho, quando apenas o **Token B** estava na base.

Controle de procedência e governança de dados

Um token funciona como um carimbo ou marca d'água que identifica um conjunto de dados. Dito de outro modo, ele garante que haja pelo menos um registro exclusivo e inconfundível na base, que pode ser usado para auditar um vazamento e comprovar a procedência da informação.

Ao mesmo tempo, o token pode ser usado para rotular bases compartilhadas com parceiros e fornecedores. Ou seja, podem ser colocados tokens diferentes na base original e naquela que foi compartilhada com um fornecedor específico.

Caso seja exposto aquele token que foi compartilhado e não o da base original, há um indício claro de que o vazamento partiu de terceiros.

A mesma linha de raciocínio pode ser aplicada a diferentes filiais de uma empresa ou linhas de negócio. Criando tokens exclusivos para cada ponto de compartilhamento ou acesso, as bases podem ser diferenciadas das demais, mesmo que os outros registros precisem ser idênticos por uma necessidade do negócio.

Outra vantagem do token está na sinalização da exposição acidental das informações. Se a exposição ocorrer na própria infraestrutura da empresa, o monitoramento do token pode desencadear uma reação imediata, prevenindo o acesso indevido de atores maliciosos.

Inclusive, criminosos estão sempre buscando bases desprotegidas ou sistemas com erros de configuração

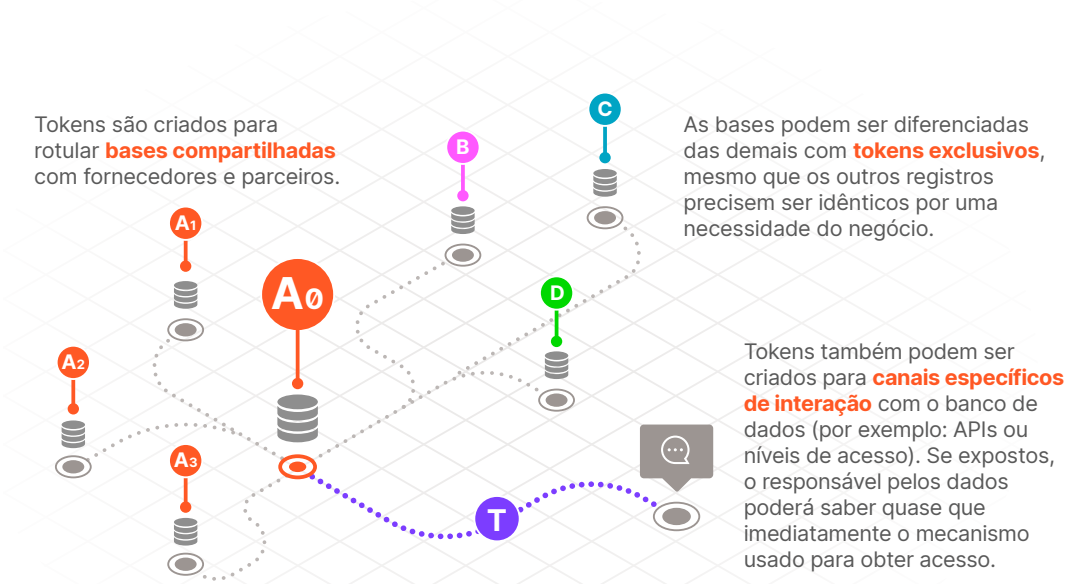
que resultam em exposição de dados. O monitoramento robusto munido da precisão do token (que só você conhece) é capaz de acelerar o tratamento desses incidentes, e o tempo de resposta pode ser a chave para mitigar o impacto de confidencialidade e evitar um vazamento de grandes proporções.

Vale lembrar que a Lei Geral de Proteção de Dados (LGPD) trata de dois tipos de agentes de tratamento – o controlador e o operador. Segundo a legislação, cabe ao controlador verificar que o operador está observando as normas e instruções estipuladas. Sendo assim, a existência de mecanismos que permitam isolar a fonte ou causa de um vazamento (como o token) pode ser de grande valia para a adequação das práticas de governança de dados.

Em outro cenário mais técnico, podem ser criados tokens para canais específicos de interação com o banco de dados (por exemplo, em determinadas APIs ou para alguns tipos de níveis de acesso – como gestores). Caso seja exposto unicamente o token exclusivo daquele canal, o controlador ou operador dos dados poderá saber quase que imediatamente o mecanismo usado para obter acesso aos dados.

Exemplo de controle de procedência

Bases compartilhadas com tokens únicos
podem ser rastreadas após um vazamento.



Análise

Caso seja exposto aquele token que foi compartilhado (por exemplo, **D** ou **A3**) e não o da base original, há um indício claro de que o vazamento partiu de terceiros.

A Lei Geral de Proteção de Dados (LGPD) define dois tipos de agentes de tratamento – o **controlador** e o **operador**. Cabe ao controlador verificar que o operador está observando as normas e instruções estipuladas.

Escolhendo a quantidade de tokens

A quantidade de tokens a ser incluída em uma base varia de acordo com a finalidade planejada. Utilizar os tokens para demarcar intervalos de tempo ou canais de acesso vai exigir um processo recorrente de inclusão e até remoção dos tokens da base, por exemplo, enquanto o token simples de monitoramento pode ser mantido por prazo indeterminado.

No mesmo sentido, o acréscimo dos tokens a bases compartilhadas com parceiros ou fornecedores, pode exigir o uso de um número maior de tokens. A quantidade dependerá do nível de especificidade desejada e da quantidade de compartilhamentos realizados. Se o mesmo token for utilizado para 5 compartilhamentos, por exemplo, ele não servirá para determinar com precisão qual das bases compartilhadas foi comprometida.

Contudo, é o comportamento daqueles que expõem informações na web que deve ser visto como o fator mais importante para a escolha dos tokens.

Uma característica comum em dados vazados na web é a exposição de registros sequenciais. Porém, as informações vazadas às vezes são apenas uma amostra do conjunto obtido pelos criminosos e não incluem a base inteira. Se o token não estiver na amostra, ele não será reconhecido pelos sensores de monitoramento que estiverem varrendo a web.

Pensando nisso, uma contramedida interessante é o uso de vários tokens espalhados pela base. Com isso, há uma chance maior de que a sequência exposta inclua o token, viabilizando um alerta antecipado sobre a exposição dos dados.

“Nunca se sabe qual trecho vai ser coletado. Por isso é importante distribuí-los ao longo do tempo e da base, preferencialmente até de forma randômica”, recomenda Thiago Bordini, diretor de Cyber Threat Intelligence (CTI) da Axur.

De fato, em bases com 1.000 registros ou mais, a Axur sugere a inclusão de pelo menos três tokens. Se a base for ainda maior ou exposta a muitos riscos, é válido considerar a inclusão de tokens adicionais para aumentar a probabilidade dele aparecer nas amostras que caem na web.

Bordini explica que a inclusão de tokens em intervalos temporais é vantajosa para as abordagens de contrainteligência, nas quais o contato direto com os responsáveis por um vazamento ajuda a delimitar o impacto do incidente. Ele exemplifica: “Se um token A foi inserido no mês anterior e o token B foi inserido no mês corrente, podemos inferir que a detecção do token A e a ausência do token B indica que não foi obtido um acesso completo a toda a base”.

Por que os tokens são aliados da resposta a incidente

O processo de resposta a um incidente de vazamento de dados é repleto de desafios. Veja como os tokens podem contribuir:

Resposta a incidente de vazamento de dados

Desafio	Como o token pode ajudar
Monitoramento	Sendo um registro único e sem dados sensíveis, o token é perfeito como chave de pesquisa para monitorar a exposição do banco de dados.
Determinar se o banco de dados vazado é realmente seu e qual banco foi exposto	Como o token é um registro exclusivo e único, a presença ou ausência do token na base vazada será um indicativo relevante sobre a origem dos dados.
Delimitar o período do acesso indevido	A adoção de um “rodízio” de tokens substituídos periodicamente pode demarcar o intervalo de tempo do acesso indevido.
Averiguar o descumprimento de políticas por parte de terceiros	A adição de tokens exclusivos para bases compartilhadas pode isolar a origem dos dados expostos.

Desafio	Como o token pode ajudar
Evidenciar ameaças internas e descumprimento de políticas por parte de colaboradores	Tokens podem só aparecer em certos níveis de acesso ou em sistemas internos, identificando vazamentos iniciados por esses meios.
Agilizar e diminuir custos do processo de resposta a incidente	Aliado ao monitoramento da web e threat intelligence, o token pode ser o primeiro sinal de um vazamento, antecipando a resposta a incidente para minimizar riscos jurídicos e danos à marca.

Tracking Tokens Axur

A Axur oferece uma solução integrada de geração e monitoramento de tokens para bases de dados no formato de e-mail. Ao criar um token na plataforma Axur, diversos espaços da Surface Web (como o Google, o Pastebin e o Github) começam a ser monitorados pela ferramenta para que a possível exposição do token seja identificada no menor tempo possível.

Embora a noção de vazamento seja muito vinculada a redes anônimas (deep & dark web), é preciso considerar o volume real e o risco derivado de exposição ampla garantida por sites maiores e de fácil acesso. Entre todas as 273 milhões de credenciais vazadas em 2021 e identificadas pela Axur, 98,2% delas foram expostas na Surface Web.

Implementar o token preventivamente para facilitar esse monitoramento é simples. Na maioria dos casos, basta que ele seja incluído na base de dados. Dependendo do tamanho da base e da estratégia adotada, é preciso adicionar um número maior de tokens em locais específicos, conforme as recomendações de boas práticas para esse tipo de solução.

Caso o token seja localizado em um dos espaços monitorados, de acordo com os critérios de pesquisa do monitoramento da Axur, um alerta será gerado para que a ocorrência receba o tratamento devido e cabível, inclusive com a possibilidade de um takedown ágil para minimizar a circulação dos dados.

Conforme a estratégia de tokens adotada e as circunstâncias dos dados expostos, o trabalho de resposta a incidentes poderá ser bastante direcionado e facilitado – especialmente quando comparado ao esforço necessário para periciar sistemas sem nenhum ponto de partida definido.

A solução de tokens também contribui para que os times de CTI (Cyber Threat Intelligence) e ART (Axur Research Team) possam identificar se a sua base foi envolvida em um vazamento de dados exposto na Deep Web e Dark Web, complementando e ampliando o valor oferecido por ambos os serviços.

Fortaleça sua operação de segurança da informação com a gestão de riscos digitais da plataforma Axur

Nossa plataforma é um hub de tecnologia e serviços gerenciados, oferecendo visibilidade de riscos digitais para operações que desejam escalar a prevenção e a resposta a incidentes.

400
empresas

600
marcas

+3.700
grupos fechados em redes sociais

+ de 1.7 bilhão
de sinais analisados

Quase 3 milhões
de mensagens com menções de clientes interceptadas em nossa plataforma

Dados do último ano.

Oferecemos monitoramento, detecção, triagem e reação para os principais grupos de riscos encontrados na internet:

- Fraudes Digitais
- Vazamento de Dados
- Pirataria Online
- Deep & Dark Web

A Plataforma Axur oferece o apoio de especialistas para lidar com ataques de grande impacto, direcionando ações táticas e operacionais de defesa cibernética.

Com os times CTI/ART da Axur, você aumenta a superfície de pesquisa, descoberta e investigação de ameaças da sua estrutura de SI e Threat Intel, revelando padrões de fraudes imperceptíveis para estratégias reativas.

AGENDE UMA DEMO

Desenvolvimento:

Altieres Rohr
Redação

Patrick Santos
Design

Sobre a Axur

Líder em proteção contra riscos digitais na América Latina, a Axur ajuda empresas a preservar a valiosa relação de confiança construída com seus clientes e parceiros por meio de experiências digitais mais seguras.

Contamos com uma equipe de Inteligência Cibernética que, unidos à alta tecnologia de Inteligência Artificial, permitem maior visibilidade e reação rápida aos riscos. Tudo isso integrado à nossa plataforma, que monitora todas as camadas da web 24×7, solicitando takedowns automaticamente.

Nossos times de pesquisa (Axur Research Team) e serviços (CTI Team) em Cyber Threat Intelligence estão prontos para oferecer o apoio necessário à resposta contra ameaças de alto impacto.

Contato para a imprensa

press@axur.com

Endereços

EUA
535 Mission Street – 14th floor
San Francisco, CA 94105

Singapura
109 North Bridge Road
Cityhall District, 179097

Brasil
Rua Mostardeiro, 322 – 15º andar
Porto Alegre, RS 90430-000

axurbr Axur AxurBrasil AxurBrasil AxurBrasil Axur