Fuga de Datos

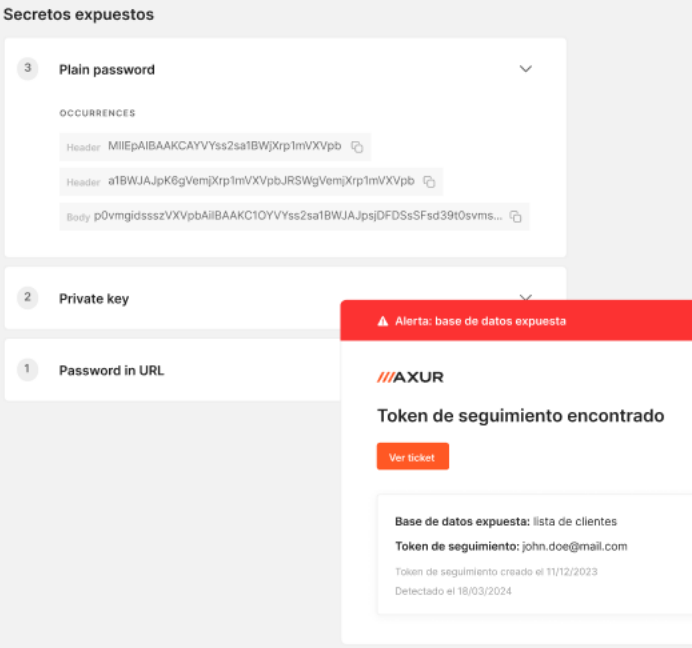
Anticipe la exposición de datos confidenciales y proteja su superficie de ataque externo

Problema

Los actores de amenazas explotan hábilmente las violaciones de datos, utilizándolas como conductos para estafas y ciberataques. Sorprendentemente, más del 81% de los ataques de ransomware tienen su origen en credenciales corporativas expuestas. Actualmente, se necesita ayuda para proteger la información más valiosa de su organización y preservar el acceso privilegiado, con una plataforma proactiva que monitoree y detecte continuamente posibles violaciones y exposiciones en tiempo real.

Solución

Axur ofrece una sólida respuesta a este desafío, permitiéndole garantizar la seguridad de sus datos sensibles y también obtener una visión integral de su superficie de ataque externo. Se monitorean de cerca los datos de la Surface Web, Deep & Dark Web e Infostealers, abarcando credenciales de acceso, contraseñas comprometidas, información de tarjetas de crédito expuestas, claves de código o archivos y datos más sensibles. Además, nuestras soluciones extienden su vigilancia para abarcar plataformas propietarias, para responder de manera rápida y gestionar el riesgo de manera efectiva.



Mejore el tiempo de respuesta y mitigue los impactos con leyes de cumplimiento y protección de datos

- Monitoreo diario de dominios y exposición de credenciales
- Búsquedas automáticas de referencias a marcas, productos, servicios y documentos clasificados de la empresa
- Detección de la venta de datos en foros de la Deep & Dark Web y mercados en la Darknet
- Verificación regular de sitios de paste, utilizados para diseminar información que posibilita ataques
- Procesamiento de grandes filtraciones

+42 mil millones de credenciales

detectadas en violaciones de datos

1 mil millones agregadas mensualmente

Exposición de Credencial Corporativa

Monitoree la exposición de las credenciales corporativas utilizadas por sus empleados en entornos y aplicaciones. Acceda a un registro histórico de credenciales expuestas para tomar decisiones rápidas, responder rápidamente y mitigar riesgos.

Credencial de Infostealer

Esté al tanto de las credenciales comprometidas de clientes y empleados detectadas en malware como infostealers. El monitoreo dirigido de Axur de dominios y URLs determina con precisión qué credenciales autentican con éxito en sitios o aplicaciones específicas.

- Identifique ataques complejos que pueden eludir la MFA;
- Detección contextual de todos los datos e información expuestos de la máquina infectada.

Exposición de Credencial del Cliente

Detecte las credenciales expuestas utilizadas para iniciar sesión en su plataforma web, sitio de comercio electrónico o entorno digital. Responda rápidamente exigiendo un restablecimiento de contraseña o restringiendo transacciones y actividades.

- Limpieza inicial de la Base de Datos
- Alertas Webhooks

Fuentes monitoreadas para exposición de credenciales:

- Deep & Dark Web, incluyendo grupos, foros y comunidades en Telegram/WhatsApp/Discord;
- Registros de malware;
- Sitios no catalogados o no indexados;
- Darknets (como TOR, Freenet, I2P, Usenet);
- Canales de Internet Relay Chat (IRC);
- Foros abiertos y cerrados en la web;
- Grandes filtraciones (Canva, Trello, etc.)

Sitios de pastes, incluyendo:

Pastebin | Ghostbin | Bitbin | Openstack | ControlC
Dpaste | Hastebin | Paste2 | Pasteorg | Zeropaste

Exposición de Tarjetas de Crédito para Aplicaciones

Utilice una API para obtener acceso instantáneo a una amplia base de datos de tarjetas expuestas. Valide la seguridad de una tarjeta antes de cualquier aprobación de compra o registro en su plataforma, minimizando el riesgo de transacciones indebidas.

- Integración perfecta con sistemas internos y otras aplicaciones
- Una lista global de tarjetas expuestas para referencia
- Funciones de IA para identificación automática de tarjetas expuestas.

Exposición de Tarjetas de Crédito para Emisores

Monitoree los BIN de sus tarjetas de crédito en busca de filtraciones en la Surface y Deep & Dark Web.

- API avanzada y notificaciones por webhook;
- Detalles como número de tarjeta, CVV, fecha de vencimiento, fecha de detección y fuente de la filtración.

Exposición de Bases de Datos

Inserte tokens disfrazados como datos reales en sus bases de datos y reciba alertas si se encuentran en alguna filtración. Los Tokens de seguimiento simplifican el proceso de respuesta y auditoría de filtraciones para minimizar las consecuencias legales.

- Ayuda a confirmar la legitimidad de la base de datos y controla el acceso con el tiempo;
- Aísla la fuente de los datos expuestos mediante tokens únicos para bases de datos compartidas con terceros.

Filtración de Claves de Código

Identifique claves de código de sus dominios como tokens, contraseñas y archivos de configuración críticos que pueden estar expuestos en códigos o confirmaciones públicas en GitHub.

Otros Datos Sensibles

Identifique la exposición de datos personales, propietarios o sensibles asociados con su marca en múltiples plataformas y archivos, como Scribd, 4Shared, Trello y S3 Buckets alojados en Amazon AWS, Azure Blobs y Digital Ocean Spaces.

Proteja sus datos ahora

Conozca todas nuestras soluciones: axur.com

Solicite una demostración

///AXUR