Data Leakage

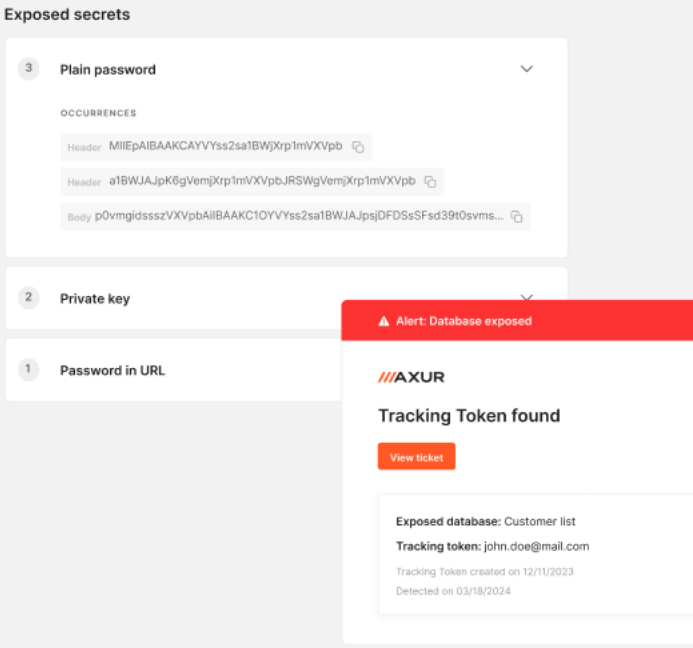
Be Ahead of Confidential Data Exposure and Safeguard Your External Attack Surface

Problem

Threat actors adeptly exploit data breaches, using them as conduits for scams and cyberattacks. Remarkably, over 81% of ransomare attacks originate from exposed corporate credentials. You need help to safeguard your organization's most valuable information and preserve privileged access with a proactive platform that continuously monitors and detects potential breaches and exposures in real-time.

Solution

Axur offers a robust answer to this challenge, making it possible for you to ensure the safety of your sensitive data and also gain a comprehensive overview of your external attack surface. Surface Web, Deep & Dark Web, and Infostealers data are closely monitored, encompassing access credentials, compromised passwords, exposed credit card information, code or file keys, and more sensitive data. Furthermore, our solutions extend their vigilance to encompass proprietary platforms, to respond promptly and manage risk effectively.



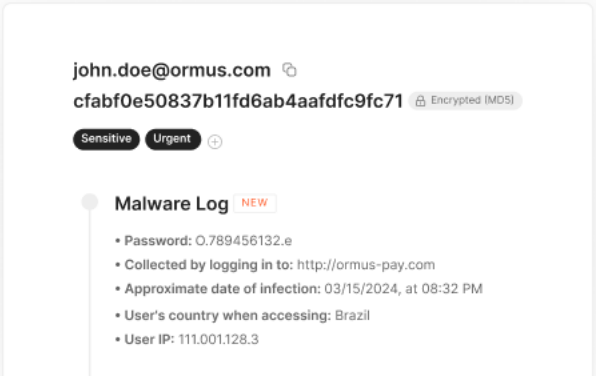
Enhance the response time and mitigate impacts with compliance & data protection laws

- Daily monitoring of domains and credential exposure
- Automatic searches for references to brands, products, services and company classified documents
- Detects data sale on deep & dark web forums and darknet markets
- Regular checking of paste sites, used by cybercriminals to disseminate information that enables attacks
- Big leaks processing

+42 billions credentials

detected in data breaches

1 bi new added monthly



Corporate Credential Exposure

Monitor the exposure of corporate credentials used by your employees in environments and applications. Access a historical record of exposed credentials to make swift decisions, respond quickly, and mitigate risks.

Infostealer Credential

Be aware of customers and employee compromised credentials detected in malwares like infostealers. Axur's targeted monitoring of domains and URLs accurately determine which credentials successfully authenticate on specific sites or applications.

- Identify complex attacks that may bypass MFA
- Contextual detection of all exposed data and information from the infected machine

Customer Credential Exposure

Detect exposed credentials used for logging into your web platform, e-commerce site, or digital environment. Quickly respond by requiring a password reset or restricting transactions and activities.

- Initial Database Cleansing
- Webhooks Alerts

Monitored sources for credentials exposure:

- Deep & Dark Web, including groups, forums and communities on Telegram/WhatsApp/Discord
- Malware logs
- Uncataloged or unindexed sites
- Darknets (such as TOR, Freenet, I2P, Usenet)
- Internet Relay Chat (IRC) channels
- Open and closed forums on the surface web
- Big leaks (Canva, Trello, etc.)

Paste sites, including:

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

Credit Cards Exposure

for applications

Use an API to gain instant access to a vast database of exposed cards. Validate the security of a card before any purchase approval or registration on your platform, minimizing the risk of improper transactions.

- Seamless integration with internal systems and other applications
- A global list of exposed cards for reference
- AI features for automatic identification of exposed cards

Credit Cards Exposure

for issuers

Monitor your credit card BINs for leaks on the Surface and Deep & Dark Web.

- Advanced API and webhook notifications
- Details such as card number, CVV, expiration date, detection date, and the source of the leak

Database Exposure

Insert tokens disguised as real data into your databases and be alerted if they are found in any leak. Tracking Tokens simplify the leak response and audit process to minimize legal consequences.

- Helps to confirm the legitimacy of the database and control access over time
- Isolates the source of exposed data through unique tokens for databases shared with third parties

Code Secret Leak

Identify code keys from your domains such as tokens, passwords, and critical configuration files that may be exposed in public codes or commits on GitHub.

Other Sensitive Data

Identify the exposure of personal, proprietary or sensitive data associated with your brand across multiple platforms and files, such as Scribd, 4Shared, Trello, and S3 Buckets hosted on Amazon AWS, Azure Blobs, and Digital Ocean Spaces.

Safeguard Your Data Now

Discover all our solutions at axur.com

Get a demo

///AXUR