Deloitte.

Reduce cyber-security risks in documents

Deloitte's tool "Access Key Discovery" scans documents to detect stored passwords.

The Need

Passwords and API-keys are generally required to securely access a service or file locations. While increasing cyber-security incidents have created a general awareness of what constitutes a safe password, the fact that the incidents persist bears evidence to the continued risk of their inappropriate handling.

Even passwords that respect commonly accepted security criteria (minimum length, uppercase and lowercase letters as well as special characters) are not secure if they are written directly into emails, documents or code, rather than being stored exclusively in secure locations such as password managers.

Multiple copies of such documents are scattered across hard drives and stored in the cloud, proliferated by sharing across teams and – worse – even outside the organization in collaboration with clients. Exposed passwords are a goldmine for hackers and pose a significant security risk to organizations. Breaches can be costly – in terms of reputational damage (stolen customer information), time-consuming clean-up, and even regulatory fines. Prevention requires vigilance and dedicated effort – sifting through countless documents to ensure they are safe. Faced with competing priorities and scarce resources, organizations struggle to manage password security proactively and find themselves lacking the appropriate controls.

❯

Our Solution: Formalyzer

Deloitte's approach with Access Key Discovery addresses these issues by enabling users to easily search documents for all kinds of stored passwords. It supports 26 different file formats, and lets you customize your search according to a variety of parameters.

Once a file has been uploaded to Access Key Discovery, users can choose between (or combine) three different detection methods: Algorithms, Model with Public Dataset and Word-Match Index. All three methods may be used in parallel and assigned a weight for their relative contribution. The Algorithms method can be fine-tuned with additional filters, such as regular expressions or hashes. The Public Dataset model uses multiclass classification to predict password strength, customizable via thresholds values between classes. The Word-Match Index method analyzes content based on common password characteristics.

Detailed results of the password scan may be filtered by 20 feature tags that reveal a password's location, features and type. Summary results may be viewed by means of several interactive graphs, such as distribution of passwords by metrics or top files by embedded passwords.

Advantages/Benefits of Formalyzer

· Reduced cyber-security risks

· Saved time on searching for stored passwords

· Highly customizable search parameters

· Search across a wide variety of file formats

· Search within a single document or multiple files at once (via ZIP file)

· Automatic analysis of search results

Example Use Cases

· Users can search their own code for passwords or private keys before publishing or sending to customers.

· Companies can improve system security by scanning folders on shared drives to find passwords or private keys in places where they should not be stored.

· Companies can assess security level of passwords within dedicated password files on their servers, analyze existing passwords, and search for common patterns or weaknesses.

Contact

David Thogmartin

Director | Risk Advisory
AI & Data Analytics | aiStudio
dthogmartin@deloitte.de

Video demonstration

Interested in seeing Deloitte's Access Key Discovery for yourself?

Click here to watch a demonstration.

Deloitte.

Issue 12/2023