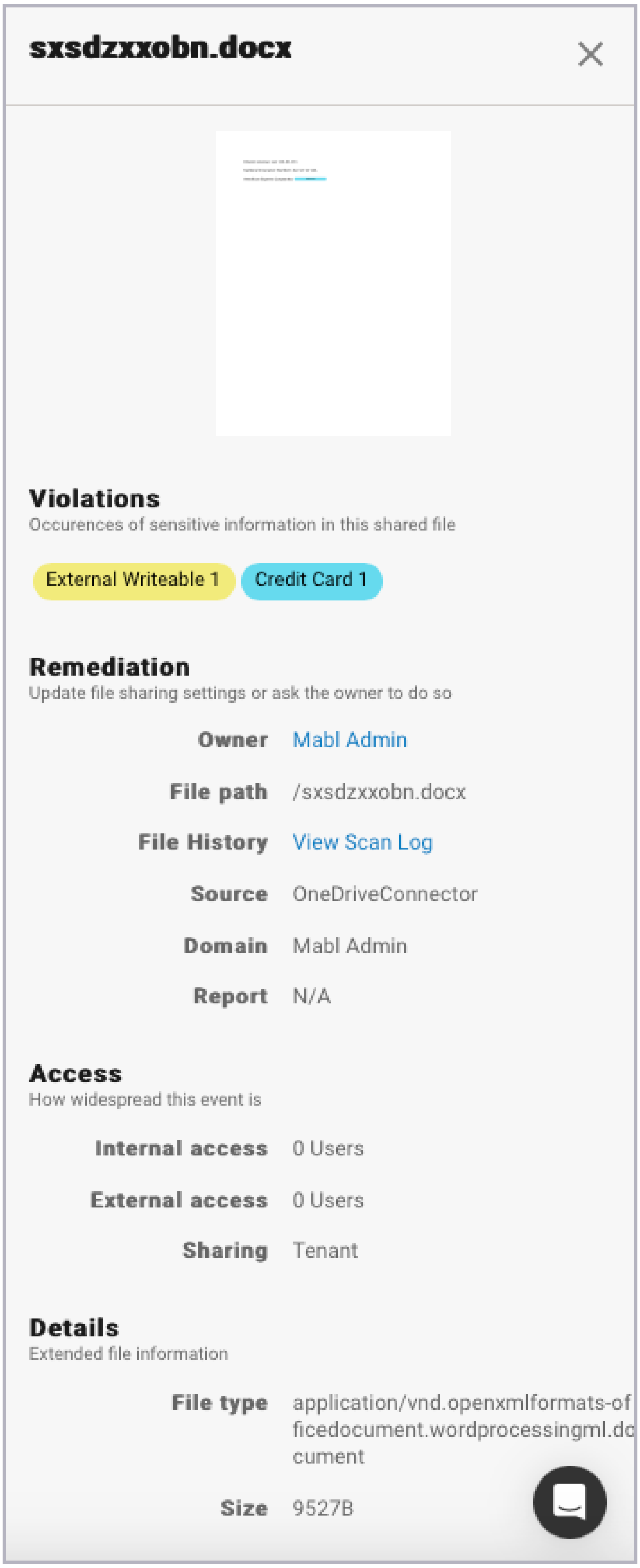
File Details

https://campus.barracuda.com/doc/98225629/

From the Detections page, click on one of the table rows to see information about that file. The details pane opens on the right.



sxsdzxxobn.docx

Violations

Occurences of sensitive information in this shared file

External Writeable 1 | Credit Card 1

Remediation

Update file sharing settings or ask the owner to do so

Owner	Mabl Admin
File path	/sxsdzxxobn.docx
File History	View Scan Log
Source	OneDriveConnector
Domain	Mabl Admin
Report	N/A

Access

How widespread this event is

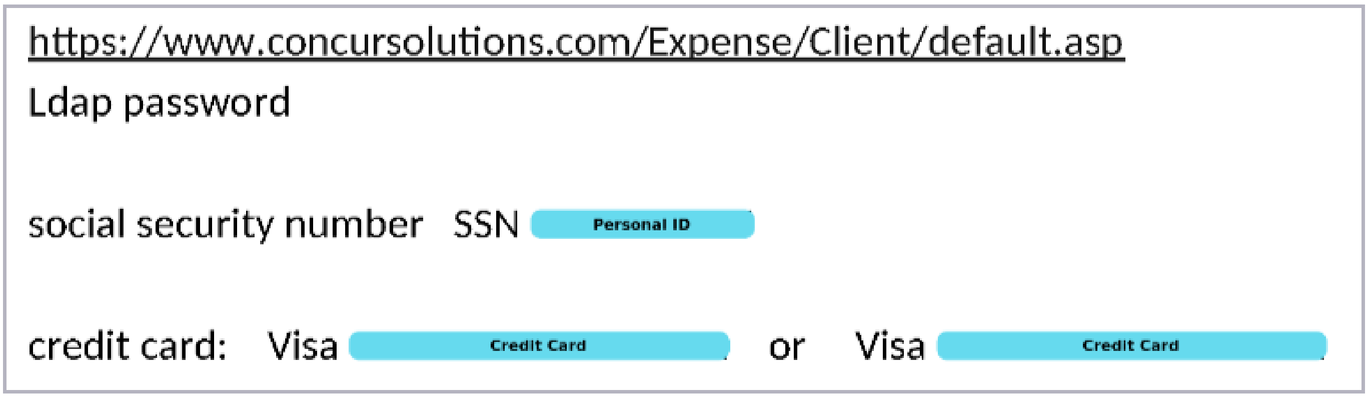
Internal access	0 Users
External access	0 Users
Sharing	Tenant

Details

Extended file information

File type	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size	9527B

The file name is at the top.
Directly below that is a visualization of the file. Any text or data determined to be sensitive will be redacted in this preview. Click on the image to see a larger representation. Here is an example of redacted content in a file preview:



https://www.concursolutions.com/Expense/Client/default.asp

Ldap password

social security number SSN Personal ID

credit card: Visa Credit Card or Visa Credit Card

Note: "Preview not available" will be displayed here for malicious files. Processing stops once a file is determined to be malicious.

Violations

The label chips in this section display the categories of sensitive data found within the file along with the number of instances of each.

- Supported categories include credentials, credit card, license number, malicious content, passport, personal ID, personal medical ID, suspicious content, and tax ID.
- The color of the classification label indicates the type of information detected.
  - **Blue labels** – Indicate the file contains sensitive information such as a license number or tax ID.
  - **Yellow labels** – Indicate sharing violations.
  - **Red labels** – Indicate that the file is malicious.
  - **Gray labels** – Indicate the file contains information from keyword classifiers that have been set in the Classifiers page.

Remediation

This section contains information about the file as it relates to your organization and remediation history.

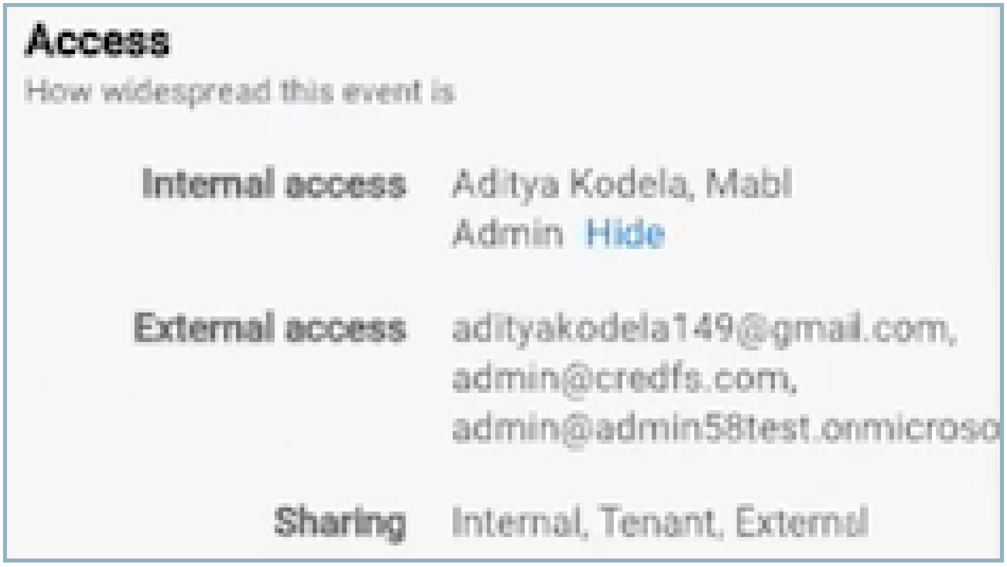
- **Owner** – User/entity that owns the file. Click this link to see all file detections for this owner.

- **File Path** – Location of file within the file tree. Click this link to see all file detections in the same path location.
- **File History** – Click to see the detection and remediation history of the file.
- **Source** – The platform endpoint used to detect the file.
- **Domain** – Administrative authority of the file.
- **Report** – Security report of scan findings for the file. This will only be available if the file was tagged by Barracuda Advanced Threat Protection and determined to be malicious.

Access

How widespread is the accessibility to this file.

- **Internal Access** – Number of users/entities on the same platform (i.e. Sharepoint) that have access to the file.
    - Clicking on the number of Internal users will show a list of those users.
- **External Access** – Number of users/entities outside of the organization that have access to the file.
    - Depending on the platform and configuration, the number of External users will be a link. Clicking it will show a list of those users.



Access

How widespread this event is

Internal access: Aditya Kodela, Mabl Admin Hide

External access: adityakodela149@gmail.com, admin@credfs.com, admin@admin58test.onmicroso

Sharing: Internal, Tenant, External

- **Sharing** – File access permissions. Files can multiple permissions.
    - **Private** – Only accessible to the owner. If Private, then **Internal Access** and **External Access** will both be 0.
    - **Internal** – Shared with others within the organization.
    - **External** – Shared outside the organization.
    - **Tenant** – Shared with the tenant.
    - **Protected** – Publicly shared, but with restrictions (i.e. not anonymous).
    - **Public** – There are no restrictions to file access. Open to anyone.

Details

Specific file details.

- **File Type** – The kind of file/file format.
- **Size** – The size of the file in bytes.
- **Last Detected** – The time and date of the last time Barracuda Data Inspector found the file to be malicious or contain sensitive information.
- **Last Modified User** – The user that last modified the file.
- **Last Modified** – The time and date the file was last modified.
- **Created** – The time and date the file was created.

Figures