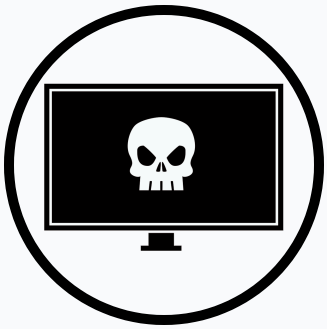
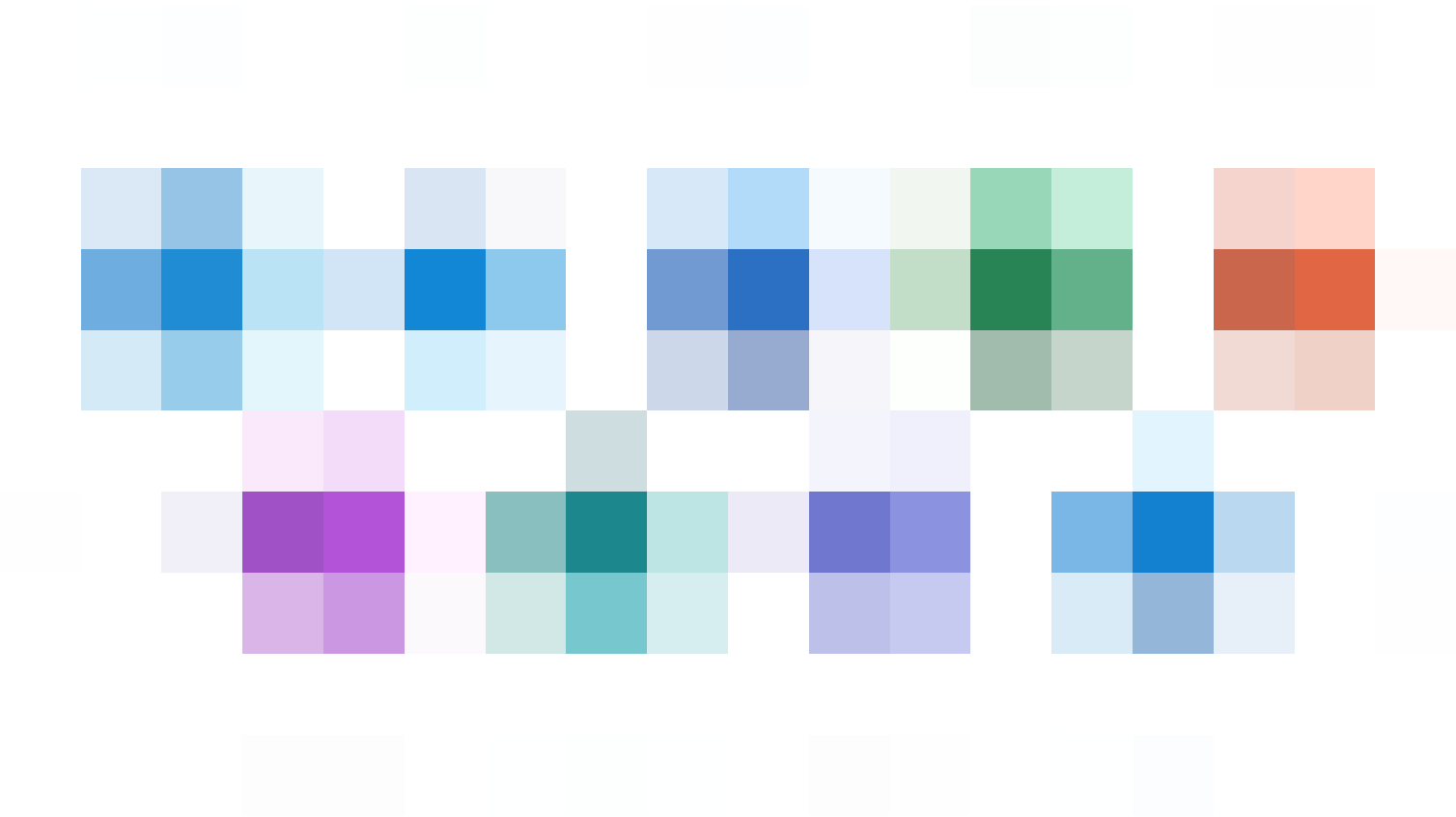


mr.d0x

C:\Users\mr.d0x> whoami_

@mrd0x | MalDev Academy | LOTS Project | MalAPI.io | Filesec.io



Stealing Access Tokens From Office Desktop Applications

September 17, 2022

Dumping tokens from Microsoft Office desktop applications' memory

Update: This only works against Microsoft 365 which is generally what organizations use. It will not work on Microsoft Office Professional Plus.

Update 2: Within a matter of days tools have already been built to dump Office desktop application tokens.

- **OfficeMemScraper.ps1**
- **TokenFinder.py**
- **office_tokens BOF**

Introduction

While I was reading the recent article about how **Microsoft Teams stores access tokens in plaintext**, I asked myself if this issue extended to other Office applications. I knew that this should be somehow possible because Office applications are generally connected to a Microsoft account.

Searching Memory Regions For Access Tokens

I launched Microsoft Word, made sure I was authenticated into my O365 account and began searching the memory regions for specific strings. After understanding what the **token format should look like**, I eventually found what I was looking for.

Searching for strings within memory that contain `eyJ0eX` gave me several results.

Choosing The Correct Access Token

The JWT tokens were not all the same and after decoding several of them I realized that the intended audience (specified by the `aud` payload claim) was different. Some of them were:

- api.office.net
- messaging.engagement.office.com
- substrate.office.com
- **outlook.office365.com**

I don't know enough about these APIs but I do know that there is documentation for the **Outlook REST API**.

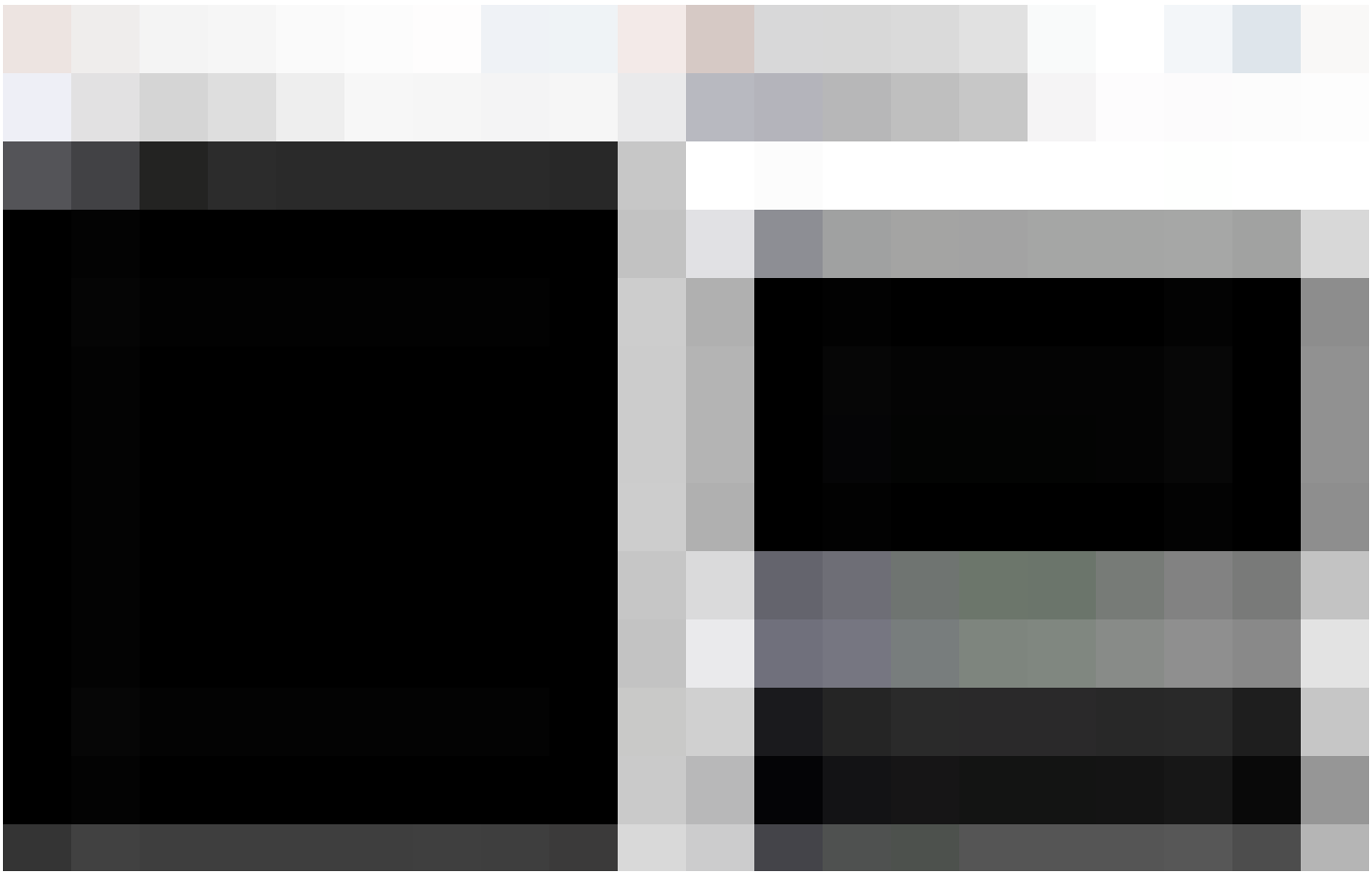
Token Scope

Before trying out the token, I had to view the scope to understand what this token can allow me to do. There were several permissions within scope such as:

- All Mail.ReadWrite
- All Files.ReadWrite
- MailboxSettings.ReadWrite

Using The Token

In the image below, I used the Outlook Mail REST API to extract all the emails successfully. The scope allows you to do much more than just reading emails though.



Extracting Access Tokens From A Memory Dump

Reading the access token directly from memory is not necessary. You can easily make a memory dump of the Office application, take it offline and extract the token.

```
strings64.exe WINWORD.EXE.dmp | findstr /i eyJ0eX
```

The tokens are successfully extracted from the dump file.

Conclusion

There are a couple of things to keep in mind. First, the Outlook REST API will be deprecated in November 2022, so if you're testing this after the deprecation date you should search for the **Microsoft Graph API** token. Next, although this article was only dedicated to Microsoft Office applications I'm sure this can be extended to several other desktop applications from other vendors.

Credits

Thanks to **@NathanMcNulty** for always helping me with Azure related questions.

← ATTACKING WITH WEBVIEW2 APPLICATIONS

PHISHING WITH CHROMIUM'S APPLICATION MODE →