
What is o365-attack-toolkit

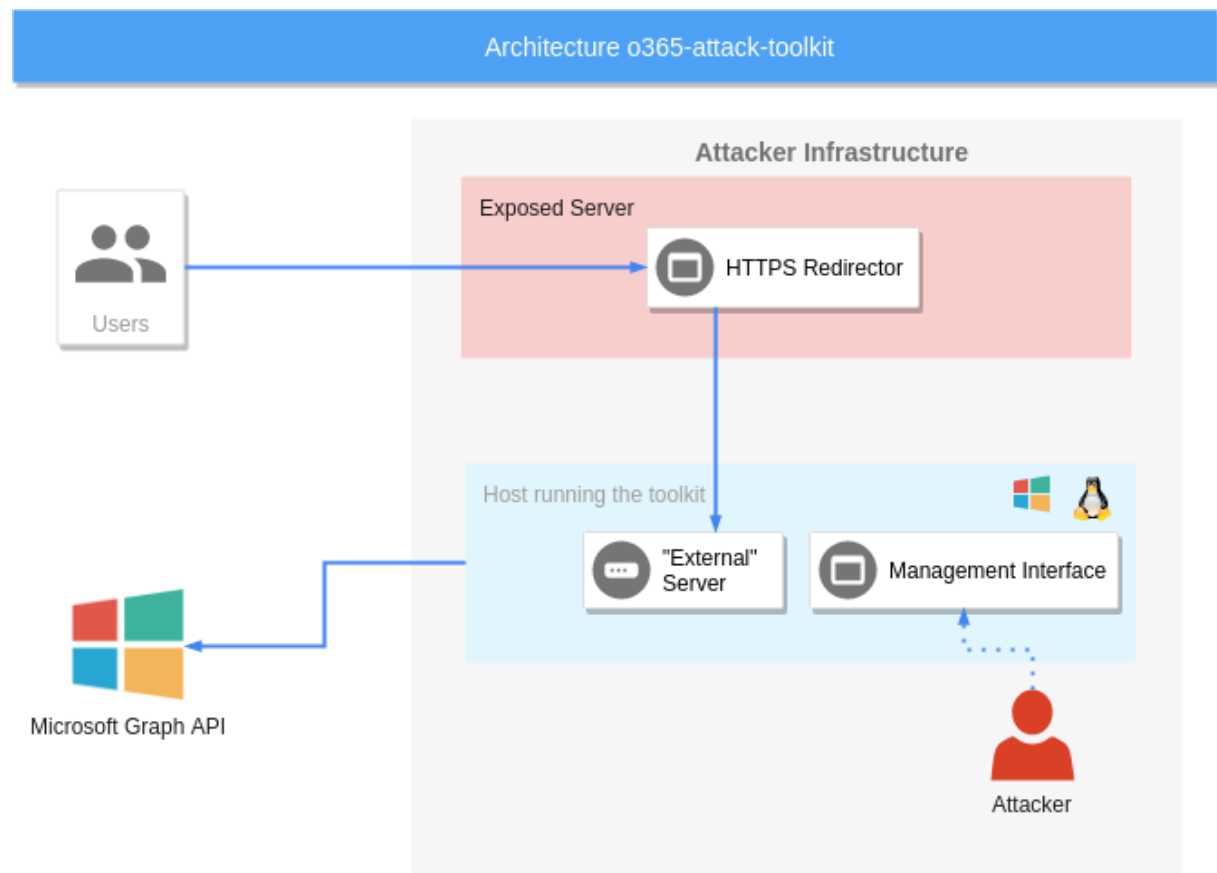
o365-attack-toolkit allows operators to perform oauth phishing attacks.

We decided to move from the old model of static definitions to fully “interactive” with the account in real-time.

Some of the changes

- Interactive E-mail Search - Allows you to search for user e-mails like you would having full access to it.
- Send e-mails - Allows you to send HTML/TEXT e-mails with attachments from the user mailbox.
- Interactive File Search and Download - Allows you to search for files using specific keywords and download them offline.
- File Replacement - Implemented as a replacement for the macro backdooring functionality.

Architecture



The toolkit consists of several components

Phishing endpoint

The phishing endpoint is responsible for serving the HTML file that performs the OAuth token phishing. ### Backend services Afterward, the token will be used by the backend services to perform the defined attacks. ### Management interface The management interface can be utilized to inspect the extracted information from the Microsoft Graph API.

Features

Interactive E-mail Search

User e-mails can be accessed by searching for specific keywords using the management interface. The old feature of downloading keyworded e-mails has been discontinued.

Send E-mails

The new version of this tool allows you to send HTML/TXT e-mails, including attachments to a specific e-mail address from the compromised user. This feature is extremely useful as sending a spear-phishing e-mail from the user is more believable.

File Search

Microsoft Graph API can be used to access files across OneDrive, OneDrive for Business and SharePoint document libraries. User files can be searched and downloaded interactively using the management interface. The old feature of downloading keyworded files has been discontinued.

Document Replacing

Users document hosted on OneDrive/Sharepoint can be modified by using the Graph API. In the initial version of this toolkit, the last 10 files would be backdoored with a pre-defined macro. This was risky during Red Team operations hence the limited usage. For this reason, we implemented a manual file replacement feature to have more control over the attack.

How to set up

Compile

```
1 cd %GOPATH%
2 git clone https://github.com/mdsecactivebreach/o365-attack-toolkit
3 cd o365-attack-toolkit
4 dep ensure
5 go build
```

Configuration

An example configuration as below :

```
1 [server]
2 host = 127.0.0.1
3 externalport = 30662
4 internalport = 8080
5
6
7 [oauth]
8 clientid = [REDACTED]
9 clientsecret = [REDACTED]
10 scope = "offline_access contacts.read user.read mail.read mail.send
11         files.readWrite.all files.read files.read.all openid profile"
12 redirecturi = "http://localhost:30662/gettoken"
```

Deployment

Before start using this toolkit you need to create an Application on the Azure Portal. Go to Azure Active Directory -> App Registrations -> Register an application.

[Home](#) > [App registrations](#) >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Application - Test ✓

Application Name

Supported account types

Who can use this application or access this API?

- ☐ Accounts in this organizational directory only (Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☒ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

Select the Supported Account Types

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web http://localhost:30662 ✓

Phishing URL

After creating the application, copy the Application ID in the configuration file.

You need to create a client secret which can be done as shown on the following image:

[Home](#) > [App registrations](#) > [Application - Test](#)

Application - Test | Certificates & secrets

Search (Cmd+/)

Got feedback?

- Overview
- Quickstart
- Integration assistant | Preview

Manage

- Branding
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators | Preview
- Manifest

1. Select Certificates & secrets

Add a client secret

2. Create a new client secret

Description

secret

Expires

- ☒ In 1 year
- ☐ In 2 years
- ☐ Never

Add

Cancel

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Update the client secret on the configuration file.

Management Interface

The management interface allows the operator to interact with the compromised users.

Users View

The screenshot shows a web browser window with the address bar at localhost:8080. The page title is "o365-attack-toolkit" and the navigation bar includes "Home", "About", and a "Get URL" button. The main content area is titled "Users" and displays a table with the following columns: #, Name, E-mail, E-mails, and Files. The first row shows a user with ID 0, a redacted name, a redacted email, and buttons for "Search E-mails", "Send E-mail", "Search Files", and "View Files".

#	Name	E-mail	E-mails	Files
0	[Redacted]	[Redacted]	Search E-mails Send E-mail	Search Files View Files

Search User E-mails

The screenshot shows a search results page for the keyword "Weekly". The page title is "Search result for : Weekly" and the navigation bar includes "Home", "About", and a "Get URL" button. The search bar contains the text "Search" and a green "Search" button. The results are displayed in a table with the following columns: Sender, Recipient, Subject, and Body Preview. The first result is from "Microsoft 365 Message Center" with a subject of "Weekly digest: Microsoft service updates" and a body preview of "Message center announcements, October 26-November 1, 2020 Major updates Theme and Fluent icon updates in Teams on the web MC225329 | October 30 - Updated October 30, 2020: We have updated the rollout timeline below. Thank you for your pat". The second result is from "MyAnalytics" with a subject of "Welcome to MyAnalytics" and a body preview of "MyAnalytics Discover your habits. Work smarter. For your eyes only Learn more > Welcome, [Redacted]! Your Office 365 account now includes MyAnalytics, a way to discover how you work MyAnalytics helps improve your... Foc".

Sender	Recipient	Subject	Body Preview
Microsoft 365 Message Center	[Redacted]	Weekly digest: Microsoft service updates	Message center announcements, October 26-November 1, 2020 Major updates Theme and Fluent icon updates in Teams on the web MC225329 October 30 - Updated October 30, 2020: We have updated the rollout timeline below. Thank you for your pat
MyAnalytics	[Redacted]	Welcome to MyAnalytics	MyAnalytics Discover your habits. Work smarter. For your eyes only Learn more > Welcome, [Redacted]! Your Office 365 account now includes MyAnalytics, a way to discover how you work MyAnalytics helps improve your... Foc

View E-mail

o365-attack-toolkit

Home About Get URL

Search

Sender

Microsoft 365 Message Center

MyAnalytics

Microsoft 365 Message Center

Microsoft 365 Message Center

Microsoft 365 Message Center

Weekly digest: Microsoft service updates 2020-10-19 07:22:25 +0000 UTC

Microsoft

Message center announcements, October 12-18, 2020

HR MAGAZINE

Major updates

Update channel name changes for iOS, Mac and Android Microsoft 365 apps

MC224273 | October 15 - In June 2020, we changed the update channel names for Microsoft 365 Apps running on Windows (MC212678, May 2020). We are now updating iOS, Mac and Android applications to bring consistency across the platforms Office is available on. Key points Microsoft 365 Roadmap ID 68703 Timing: November 10, 2020 Roll-out: tenant level Action: review and assess

[View more](#)

(Updated) Using Microsoft Authentication Library (MSAL) with Yammer Groups API

MC221062 | October 14 - Updated October 13, 2020: Thank you for your feedback. Based on your input, at this time we will not be moving forward with the retirement of Yammer Groups API endpoints support of Yammer OAuth tokens. We will announce our new plan via Message center when we are ready to proceed. Your feedback is greatly appreciated. Updated blog: Using MSAL with Yammer Groups API Yammer Groups API endpoints will only support the usage of Azure Active Directory (AAD) tokens. Yammer Groups API endpoints will no...

[View more](#)

Search

View e-mail

View e-mail

View e-mail

View e-mail

View e-mail

Send E-mail

Email address

Target

Content Type:

text/html ▼

Subject

Subject

Message Details

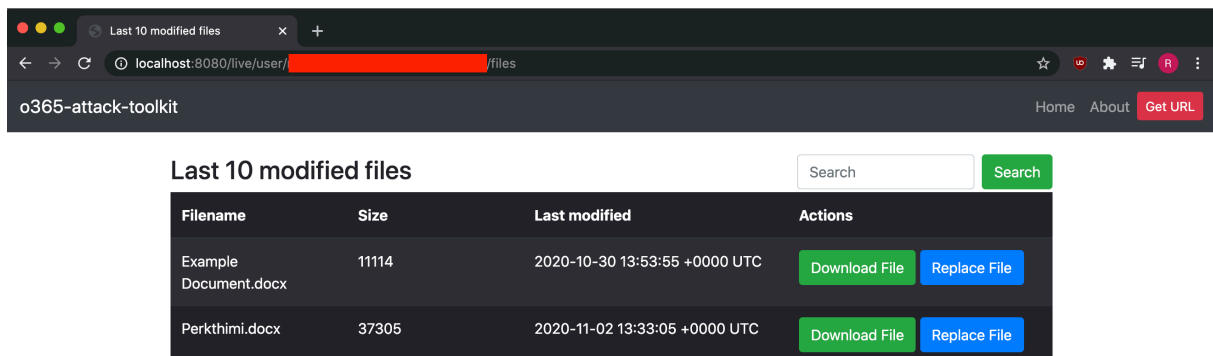
Attachment

Choose file

No file chosen

Send

Search Files



Replace File

