The art of defense evasion -part — 3 Bypass Multi Factor Authentication (MFA)

osamaellahi.medium.com/the-art-of-defense-evasion-part-3-bypass-multi-factor-authentication-mfa-26d3a87dea0f

Osama Ellahi

April 7, 2022

Let’s evade the security solutions. Part 2 Endpoint Evasion & Part 1 Sandbox Evasion.

Osama Ellahi

--

Attackers are bypassing MFA for almost 4 years, when evilginx2 was released. There were a lot of limitations but list benefits and use cases handed by evilginx2 are greater. Evilginx2 actually use reverse proxy server which sits in between your victim and original server and after successfully tokens communicated, it also saved them.

After studying the code of old tools, we tried to come up with some new bypass techniques. These techniques were also used by some threat actors. And it also requires so much hard work.

There are tools (Selenium, Playwright, etc.) available in the market which performs web automation, the purpose of these tools is to test the website’s performance. So **we use this automation against MFA.**

OFFODE

To give POC (Proof of concept) of our idea, we build a tool {{OFFODE}} which performs bypass of outlook and gets whole control of office.com.

This tool can be deployed on window's machine, window's server and Linux server as well. Since it is developed in node js and playwright, it is compatible with every device.

It is recommended to use it UI Operating system (Not CLI based). Because cookies saving part is still in progress. And if you are using UI operating system you can perform actions from logged in browser.

At the end it will give you logged in outlook account (of victim) in the browser which can be used as intention. It will be more clear if you watch this picture.

How this tool works ?

Once **user** opens the link he/she will see the login page of outlook, enter email and press enter.

Server will automatically opens a new browser on server side (using playwright) and enter same email which user gave and press enter. If the email exist server will show the user password screen, otherwise give response email is nor correct.

User will enter password (maybe correct, maybe not) and press enter.

Server will give this password to already opened browser and press enter and wait for response, if password is incorrect, server will show user incorrect password screen with error from original server. If password is correct server will watch is there is any MFA enable in this account. If no MFA is enabled server will get the session, try to intercept the cookies(in progress) and save them in public directory with filename of user's email. If there is MFA enable, server will check which MFA is it and show user same page.

If **user** set up authentication app OTP in MFA, he/she will be asked for OTP which is in the Microsoft auth app just like original server asks. User will enter those digits from authentication app and press enter.

Server will automatically enter those digits on the original server and perform actions accordingly. Same is the case with mobile number OTP case.

Installation

At first install node js in your system and then download the project from this link. After that use following commands to install all dependencies of project

```
npm install
```

Once all dependencies are installed, try installing playwright with following command.

```
npm install playwright
```

After installation of playwright start your project with this command.

```
npm start
```

By default it will start with 8888 port. To test you can use it with ngrok also.

Use Cases

Since this is just a POC of new technology so we try to cover all the use cases but this tool will always need management.

> Automation on server side and showing users saved pages with dynamic changing can widely be used on other platforms and websites.

We cover following use cases.

Case 1: Basic Email & Password

This is simple case where server checks for the user’s email validation, password validation and saves tokens. Person on server side can open outlook.com and office.com of user.

Case 2: Authentication OTP

Server will watch if user has enabled the Microsoft authentication app OTP. Then server will perform action according to the situations.

Case3: Phone Number OTP

Server checks if user have set phone number OTP. It will ask user the same thing that original server is asking to node server.

— —

We are regularly watching this tool for better performance and further changing. And we would love to see your suggestions and comments.