k van Duijn & Wesley Neelen
Ethical Hackers @ ZOLDER

ZOLDER

AITM & TOKEN REPLAY

WHOAREWE

Wesley Neelen

- Ethical hacker
- OSCP / OSEP / ..
- 10+ years of experience

Rik van Duijn

- Ethical hacker
- OSCP- / OSCE
- 10+ years of experience

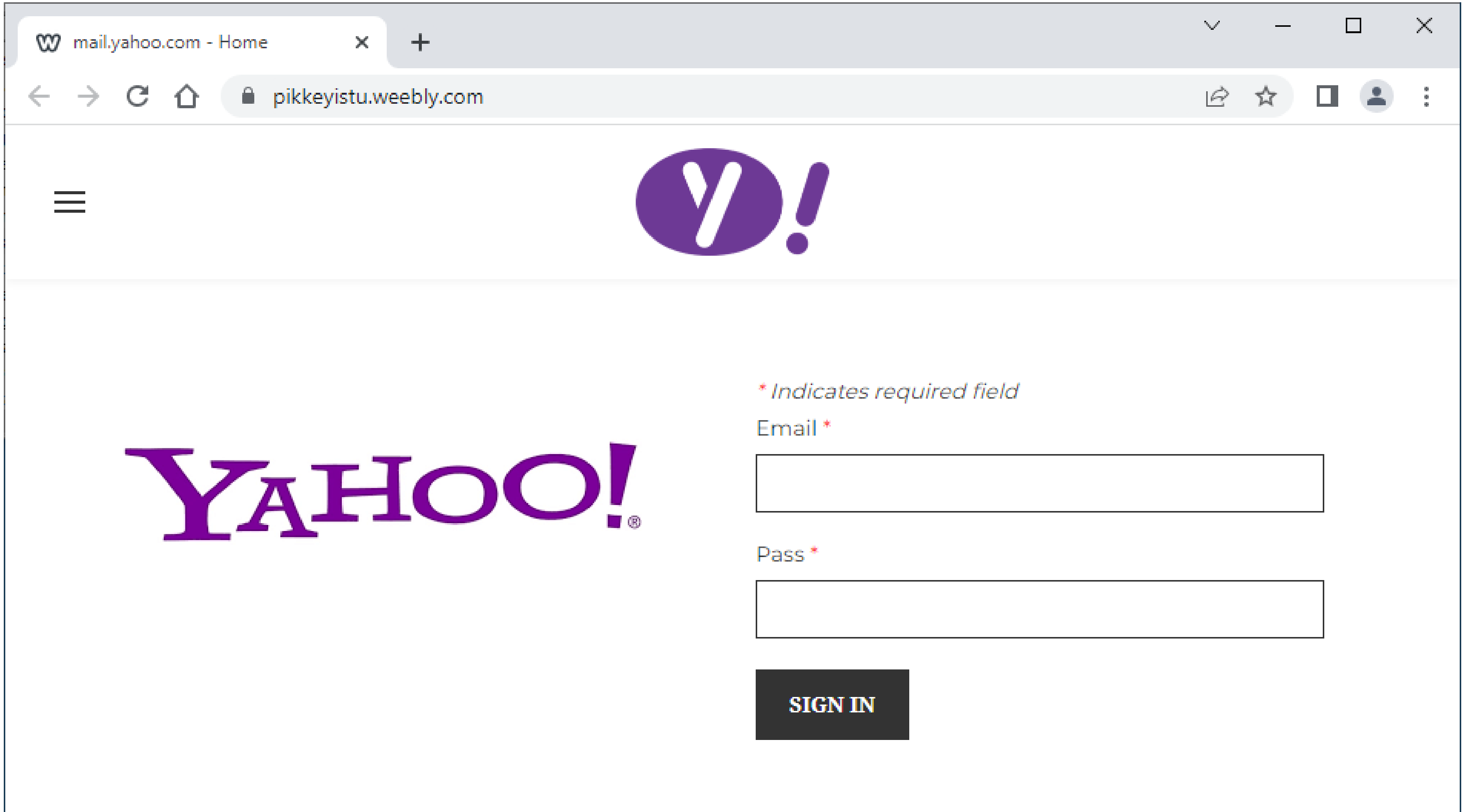
OUR GOAL

Improve IT-security for the largest group of companies possible. No nation-state ironclad enterprise grade security but a small improvement each and every day.

THE PROBLEM

Theres been an increase in phishing attempts against Microsoft 365 accounts.

SOME HISTORY



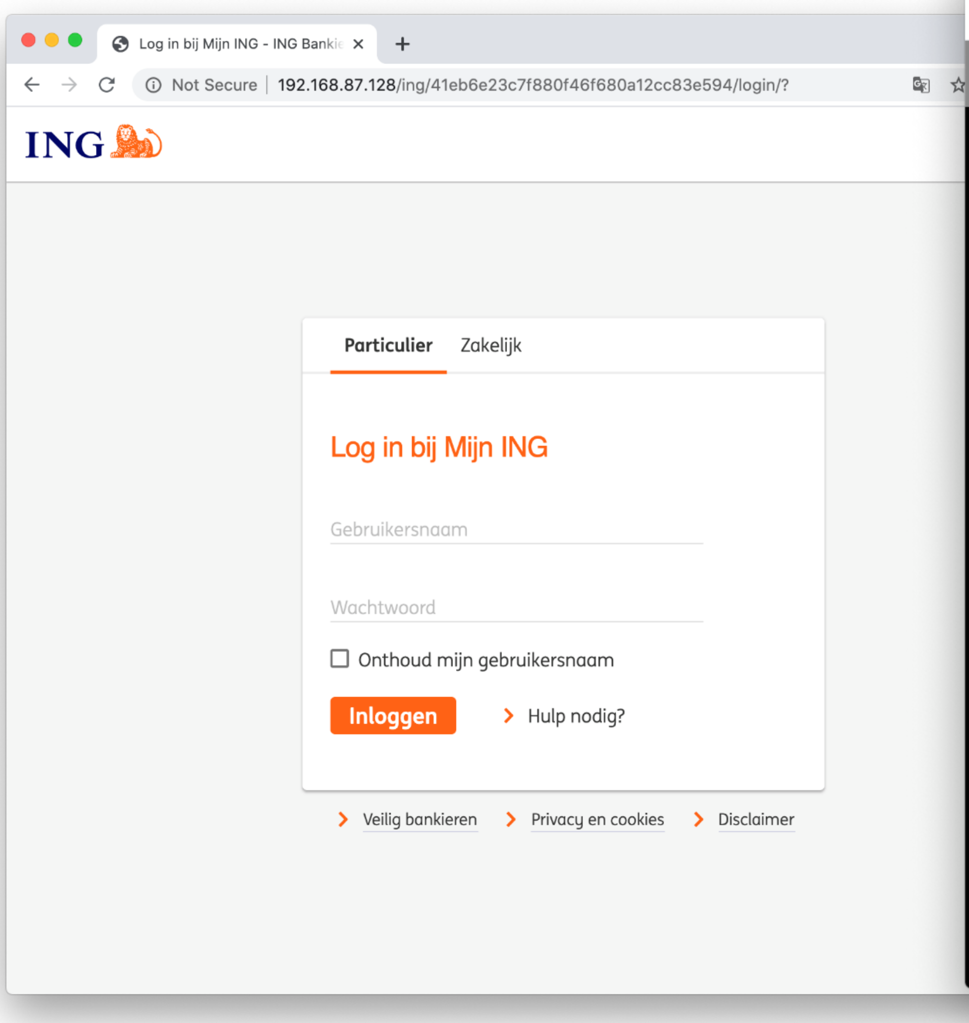
* Indicates required field

Email *

Pass *

SIGN IN

SOME HISTORY



Log in bij Mijn ING - ING Banki

Not Secure | 192.168.87.128/ing/41eb6e23c7f880f46f680a12cc83e594/login/?

ING

Particulier Zakelijk

Log in bij Mijn ING

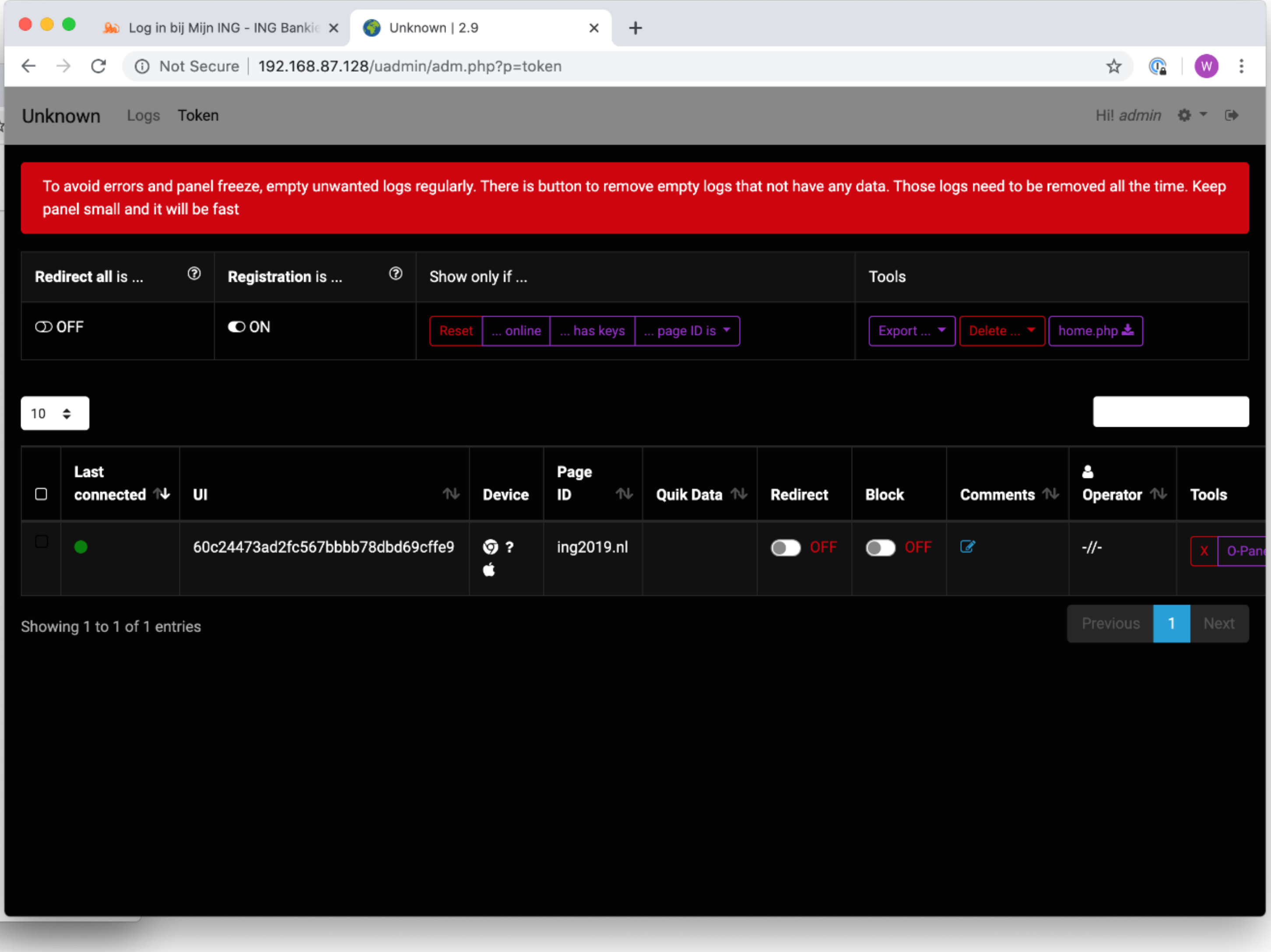
Gebruikersnaam

Wachtwoord

☐ Onthoud mijn gebruikersnaam

Inloggen > Hulp nodig?

> Veilig bankieren > Privacy en cookies > Disclaimer



Log in bij Mijn ING - ING Banki | Unknown | 2.9

Not Secure | 192.168.87.128/uadmin/adm.php?p=token

Unknown Logs Token Hi! *admin*

To avoid errors and panel freeze, empty unwanted logs regularly. There is button to remove empty logs that not have any data. Those logs need to be removed all the time. Keep panel small and it will be fast

Redirect all is ...	Registration is ...	Show only if ...	Tools
OFF	ON	Reset · ... online · ... has keys · ... page ID is	Export ... · Delete ... · home.php

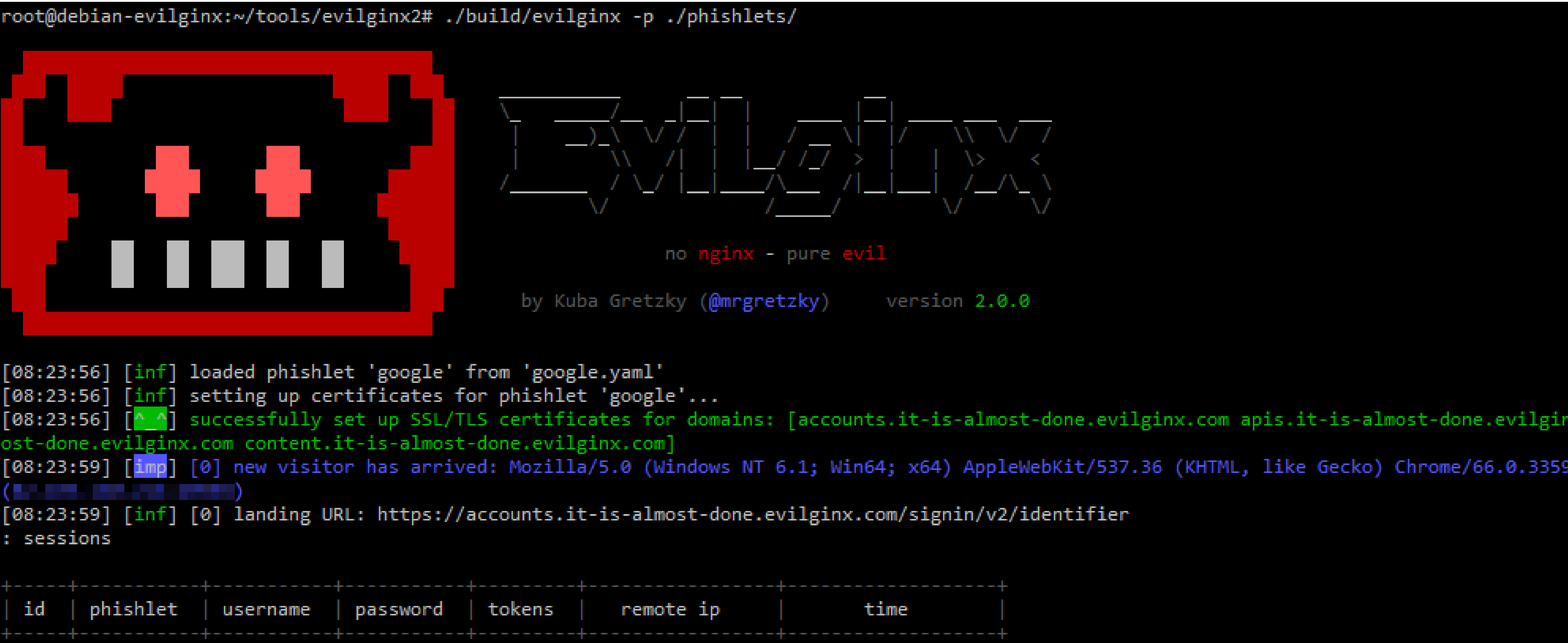
10

☐	Last connected	UI	Device	Page ID	Quik Data	Redirect	Block	Comments	Operator	Tools
☐	●	60c24473ad2fc567bbbb78dbd69cffe9	?	ing2019.nl		OFF	OFF		-//-	X O-Pan

Showing 1 to 1 of 1 entries

Previous 1 Next

SOME HISTORY



```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

                          no nginx - pure evil

                by Kuba Gretzky (@mrgretzky)     version 2.0.0

[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilgin
ost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359
([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

+------+------------+------------+------------+----------+-----------------+--------------------+
| id   | phishlet   | username   | password   | tokens   |   remote ip     |        time        |
+------+------------+------------+------------+----------+-----------------+--------------------+
```

WHY NOW?

WHY NOW

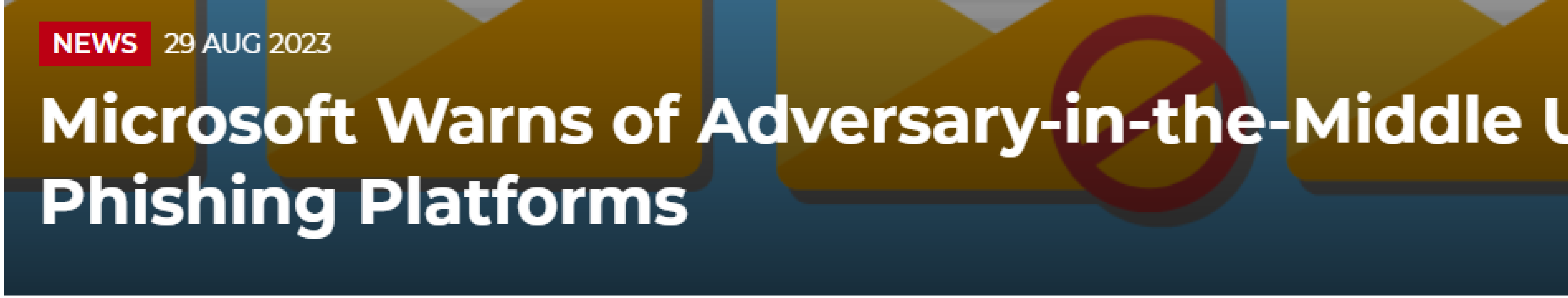
1. SaaS
2. More and more mfa, jay ☺
3. It works (on scale)

IT AINT MUCH
BUT ITS DISHONEST WORK
mgflip.com

CURRENT THREATS

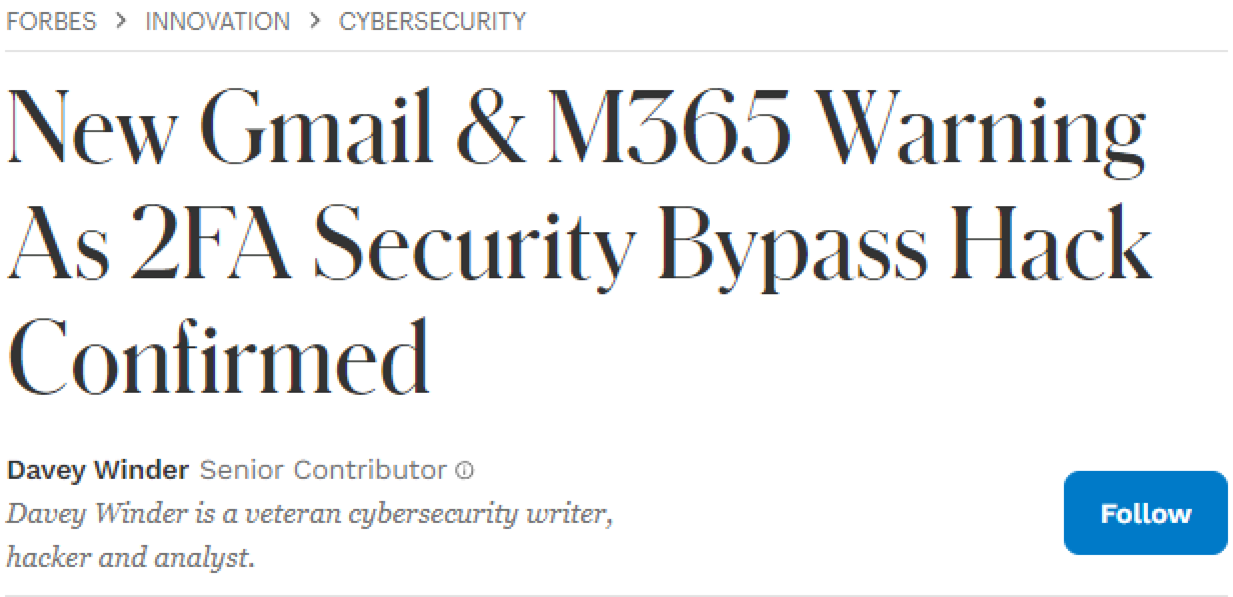
AtticSecurity.com
by ZOLDER

M365 ATTACKS



NEWS 29 AUG 2023

Microsoft Warns of Adversary-in-the-Middle
Phishing Platforms



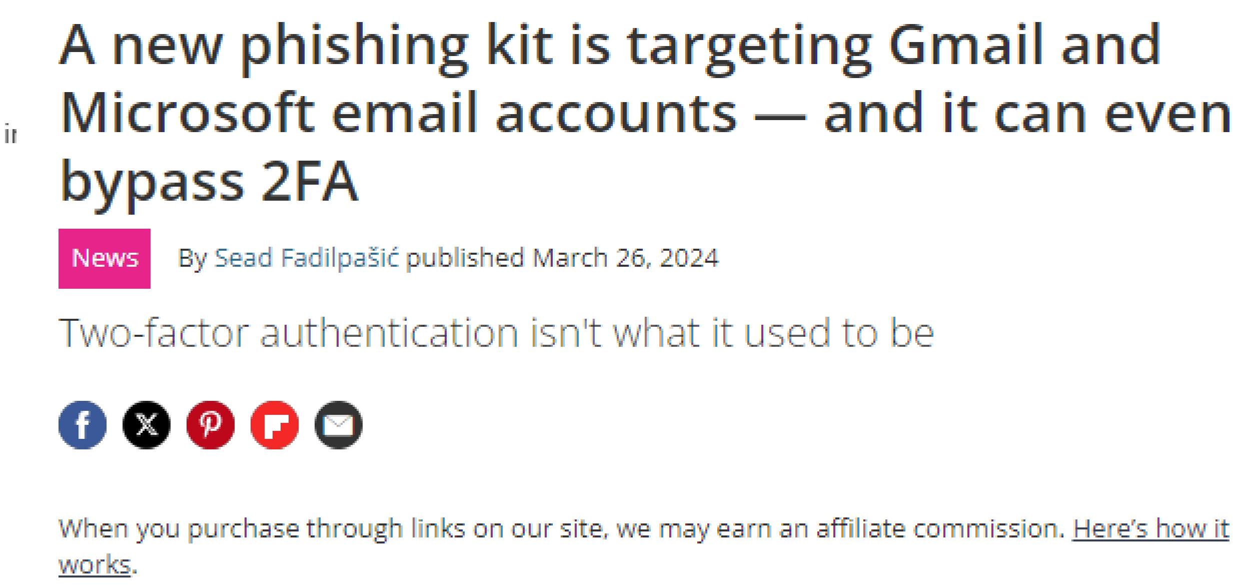
FORBES > INNOVATION > CYBERSECURITY

New Gmail & M365 Warning As 2FA Security Bypass Hack Confirmed

Davey Winder Senior Contributor ⓘ

Davey Winder is a veteran cybersecurity writer, hacker and analyst.

Follow

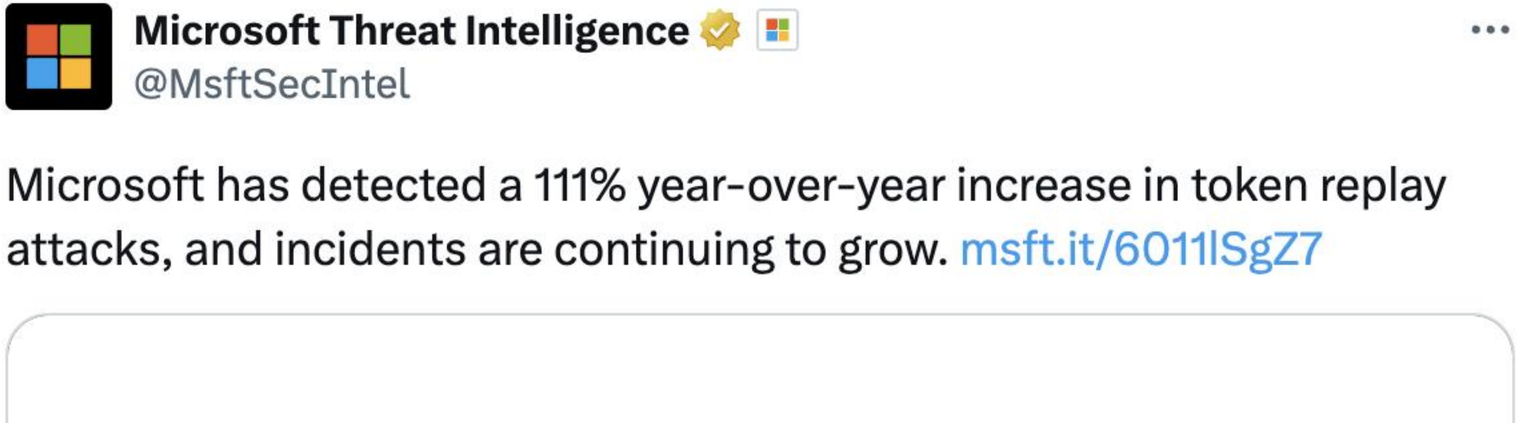


A new phishing kit is targeting Gmail and Microsoft email accounts — and it can even bypass 2FA

News By Sead Fadilpašić published March 26, 2024

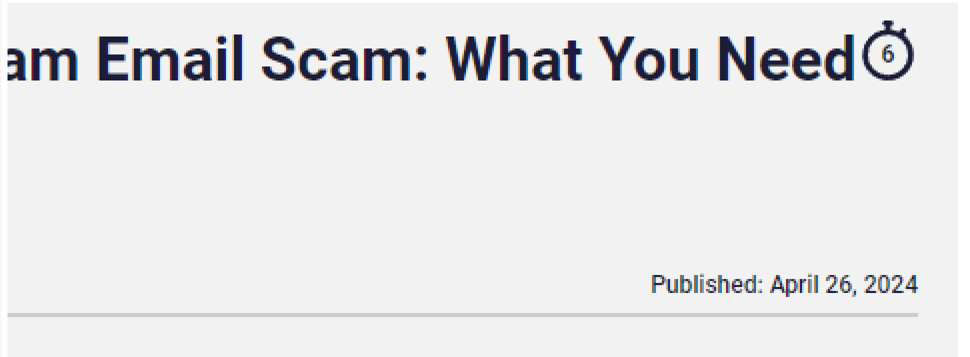
Two-factor authentication isn't what it used to be

When you purchase through links on our site, we may earn an affiliate commission. Here's how it works.



Microsoft Threat Intelligence
@MsftSecIntel

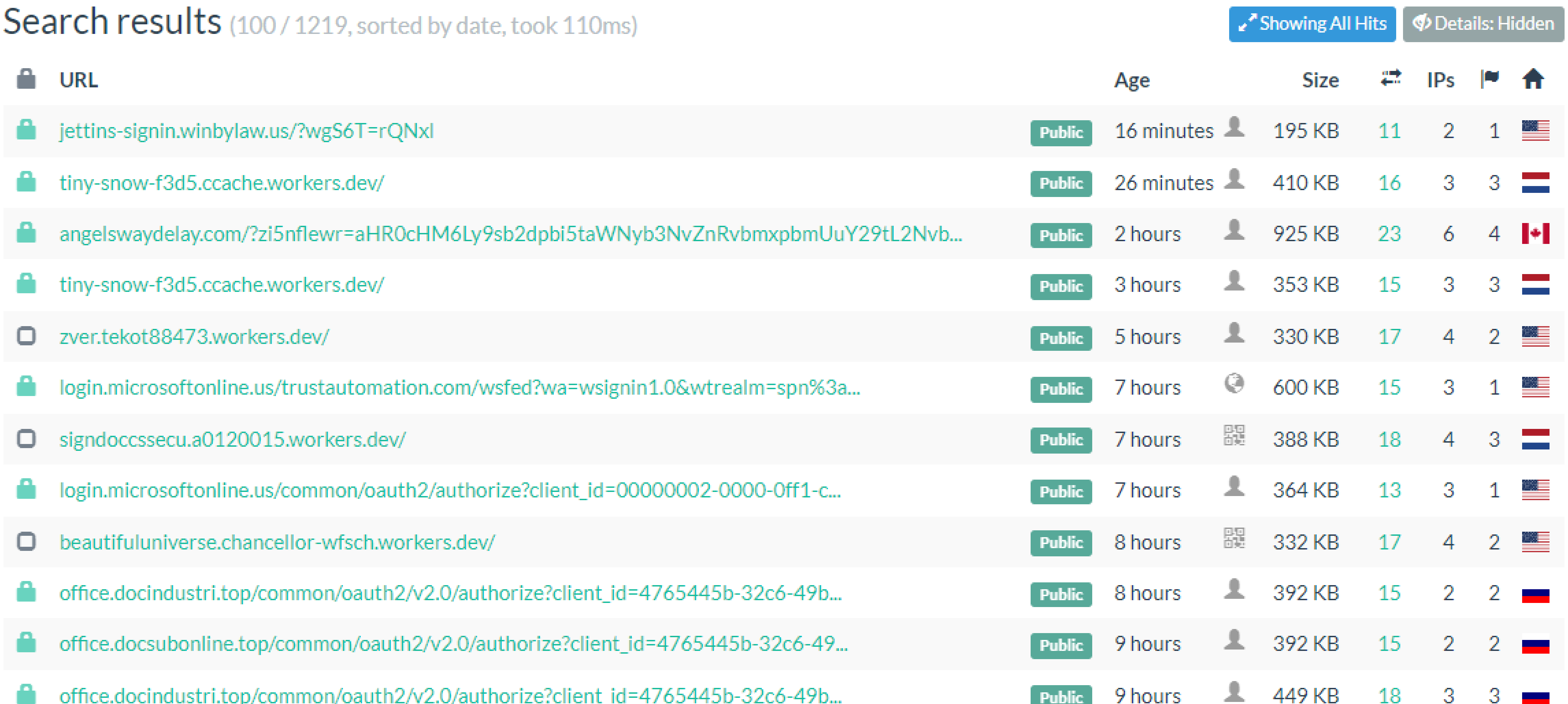
Microsoft has detected a 111% year-over-year increase in token replay attacks, and incidents are continuing to grow. msft.it/6011lSgZ7



am Email Scam: What You Need

Published: April 26, 2024

M365 ATTACKS

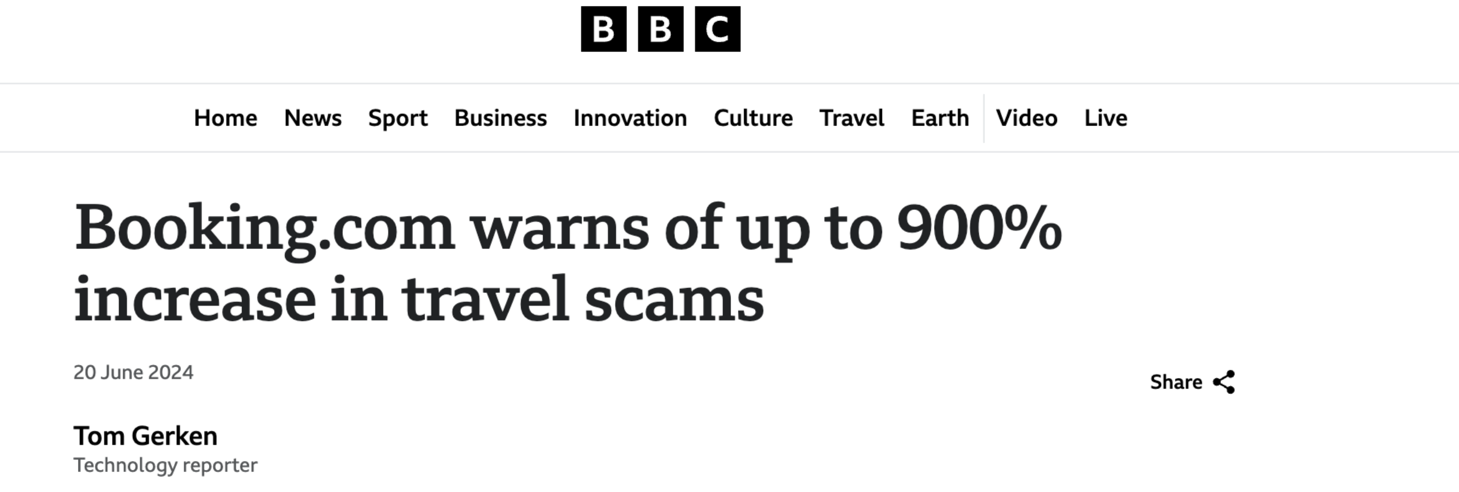


Search results (100 / 1219, sorted by date, took 110ms)

🔒	URL		Age		Size	⇄	IPs	⚑	⌂
🔒	jettins-signin.winbylaw.us/?wgS6T=rQNxl	Public	16 minutes	👤	195 KB	11	2	1	🇺🇸
🔒	tiny-snow-f3d5.ccache.workers.dev/	Public	26 minutes	👤	410 KB	16	3	3	🇳🇱
🔒	angelswaydelay.com/?zi5nflewr=aHR0cHM6Ly9sb2dpbi5taWNyb3NvZnRvbmxpbmUuY29tL2Nvb...	Public	2 hours	👤	925 KB	23	6	4	🇨🇦
🔒	tiny-snow-f3d5.ccache.workers.dev/	Public	3 hours	👤	353 KB	15	3	3	🇳🇱
□	zver.tekot88473.workers.dev/	Public	5 hours	👤	330 KB	17	4	2	🇺🇸
🔒	login.microsoftonline.us/trustautomation.com/wsfed?wa=wsignin1.0&wtrealm=spn%3a...	Public	7 hours	🌐	600 KB	15	3	1	🇺🇸
□	signdoccssecu.a0120015.workers.dev/	Public	7 hours	▦	388 KB	18	4	3	🇳🇱
🔒	login.microsoftonline.us/common/oauth2/authorize?client_id=00000002-0000-0ff1-c...	Public	7 hours	👤	364 KB	13	3	1	🇺🇸
□	beautifuluniverse.chancellor-wfsch.workers.dev/	Public	8 hours	▦	332 KB	17	4	2	🇺🇸
🔒	office.docindustri.top/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b...	Public	8 hours	👤	392 KB	15	2	2	🇷🇺
🔒	office.docsubonline.top/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49...	Public	9 hours	👤	392 KB	15	2	2	🇷🇺
🔒	office.docindustri.top/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b...	Public	9 hours	👤	449 KB	18	3	3	🇷🇺

AtticSecurity.com
by ZOLDER

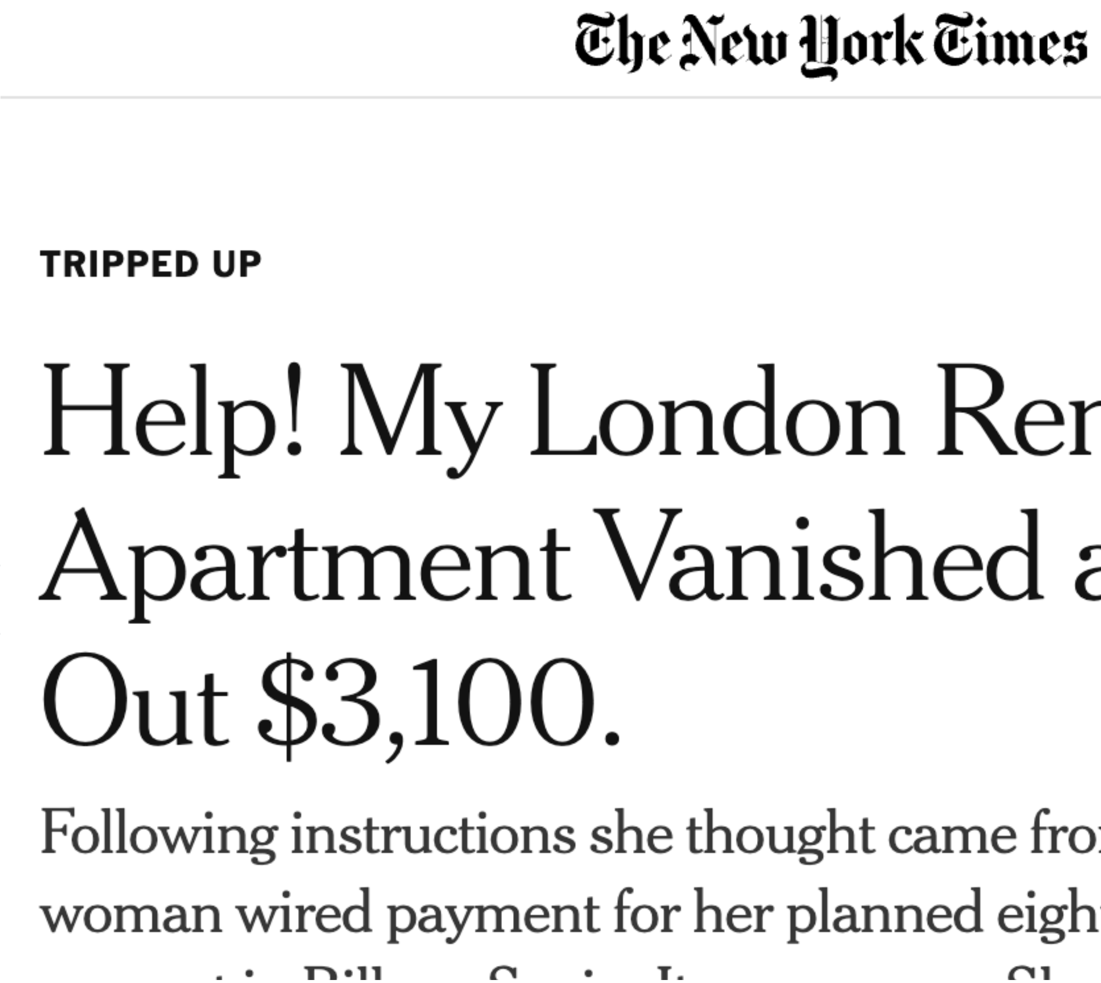
BOOKING.COM



Booking.com warns of up to 900% increase in travel scams

20 June 2024

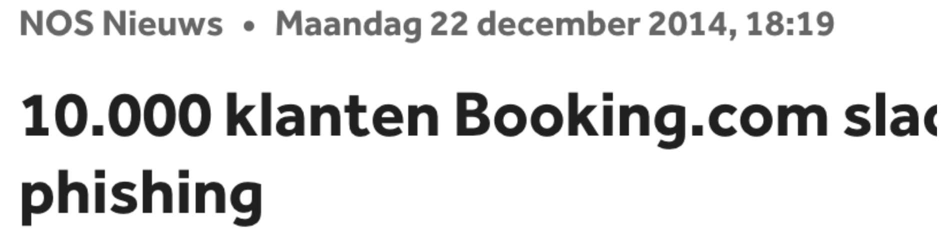
Tom Gerken
Technology reporter



TRIPPED UP

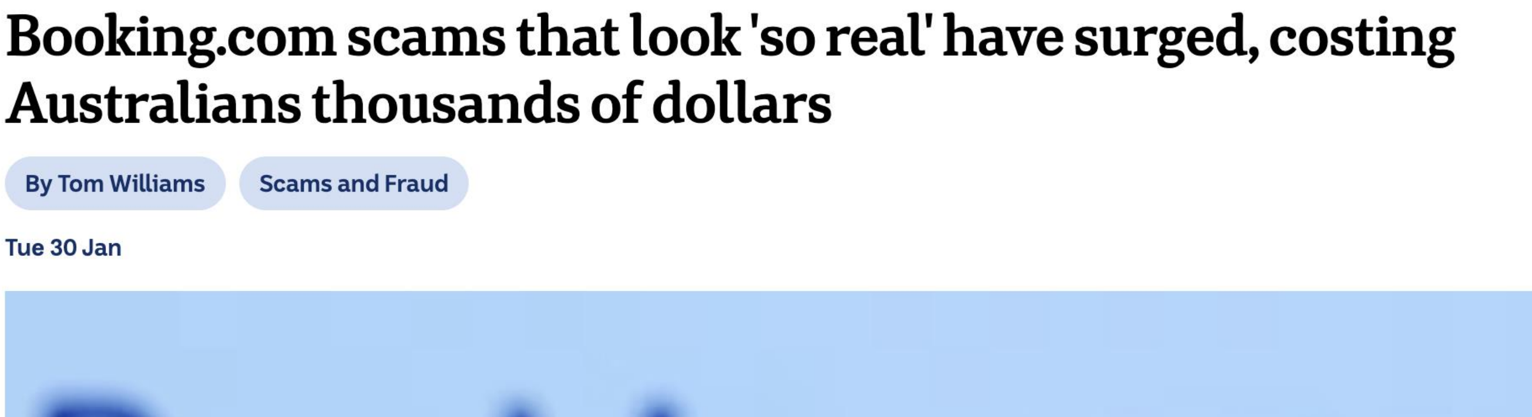
Help! My London Ren Apartment Vanished a Out $3,100.

Following instructions she thought came fro woman wired payment for her planned eigh



NOS Nieuws • Maandag 22 december 2014, 18:19

10.000 klanten Booking.com slac phishing



Booking.com scams that look 'so real' have surged, costing Australians thousands of dollars

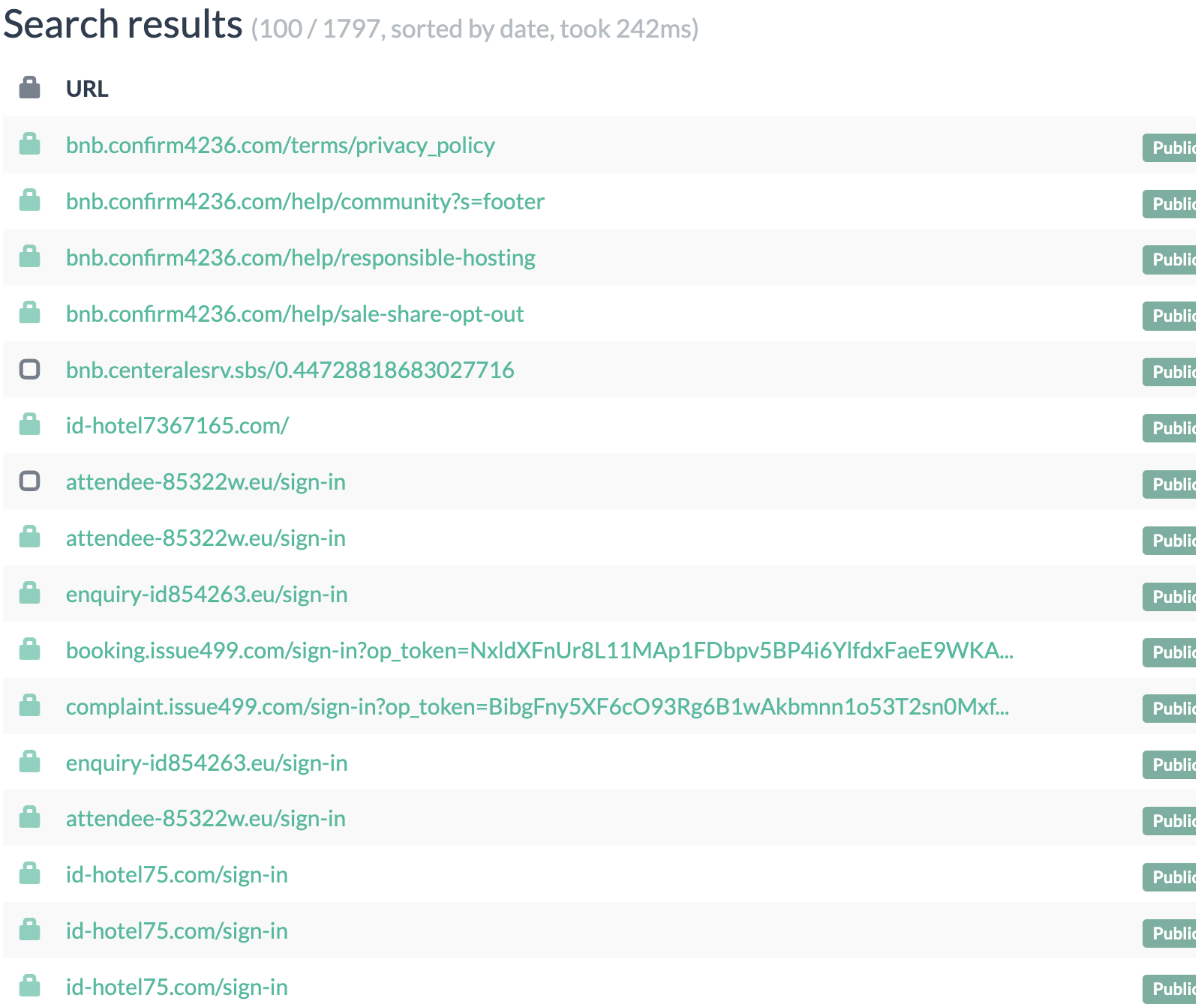
By Tom Williams

Scams and Fraud

Tue 30 Jan

AtticSecurity.com
by ZOLDER

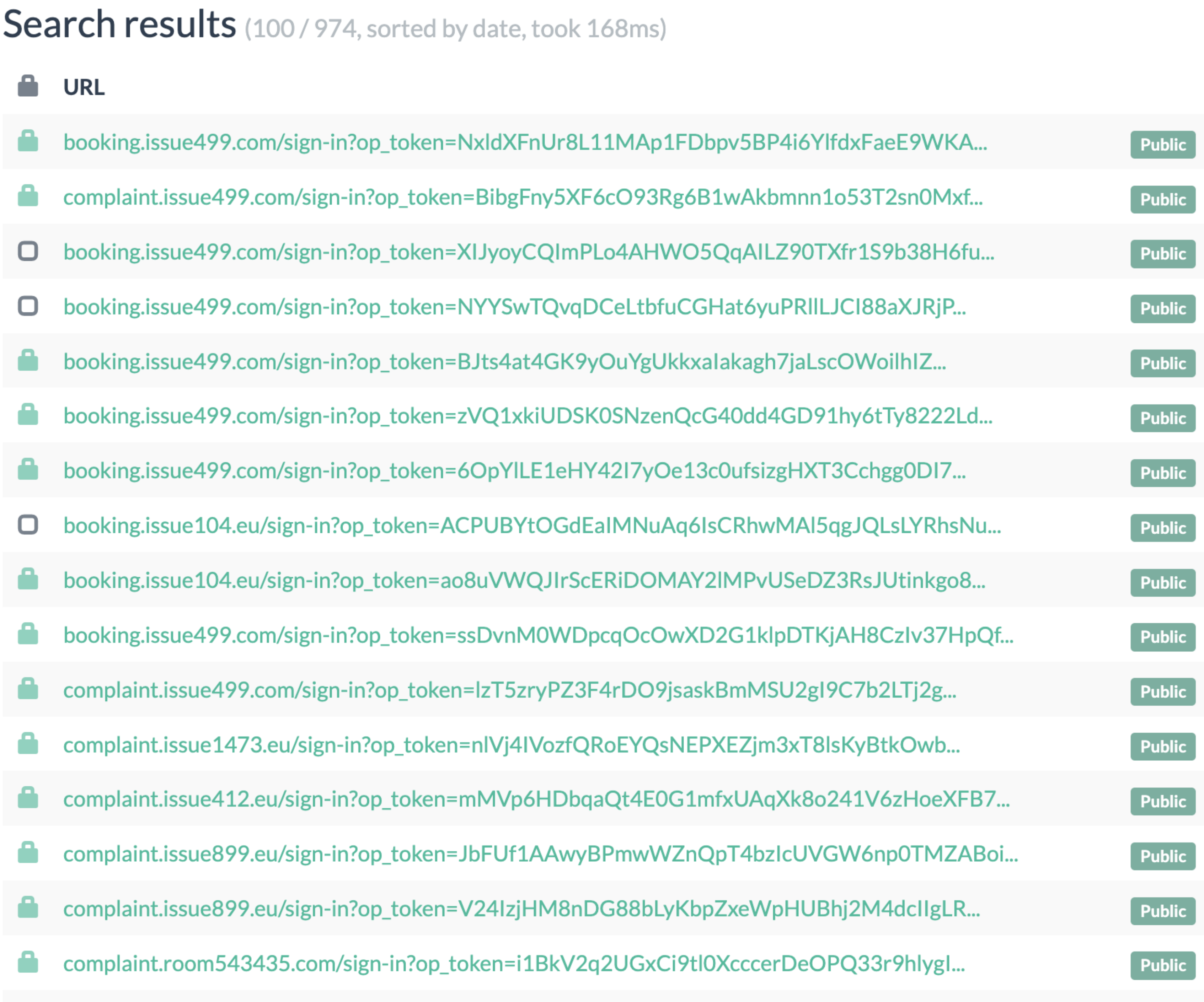
BOOKING.COM ATTACKS



Search results (100 / 1797, sorted by date, took 242ms)

🔒	URL	
🔒	bnb.confirm4236.com/terms/privacy_policy	Publi
🔒	bnb.confirm4236.com/help/community?s=footer	Publi
🔒	bnb.confirm4236.com/help/responsible-hosting	Publi
🔒	bnb.confirm4236.com/help/sale-share-opt-out	Publi
□	bnb.centeralesrv.sbs/0.44728818683027716	Publi
🔒	id-hotel7367165.com/	Publi
□	attendee-85322w.eu/sign-in	Publi
🔒	attendee-85322w.eu/sign-in	Publi
🔒	enquiry-id854263.eu/sign-in	Publi
🔒	booking.issue499.com/sign-in?op_token=NxldXFnUr8L11MAp1FDbpv5BP4i6YlfdxFaeE9WKA...	Publi
🔒	complaint.issue499.com/sign-in?op_token=BibgFny5XF6cO93Rg6B1wAkbmnn1o53T2sn0Mxf...	Publi
🔒	enquiry-id854263.eu/sign-in	Publi
🔒	attendee-85322w.eu/sign-in	Publi
🔒	id-hotel75.com/sign-in	Publi
🔒	id-hotel75.com/sign-in	Publi
🔒	id-hotel75.com/sign-in	Publi

BOOKING.COM ATTACKS

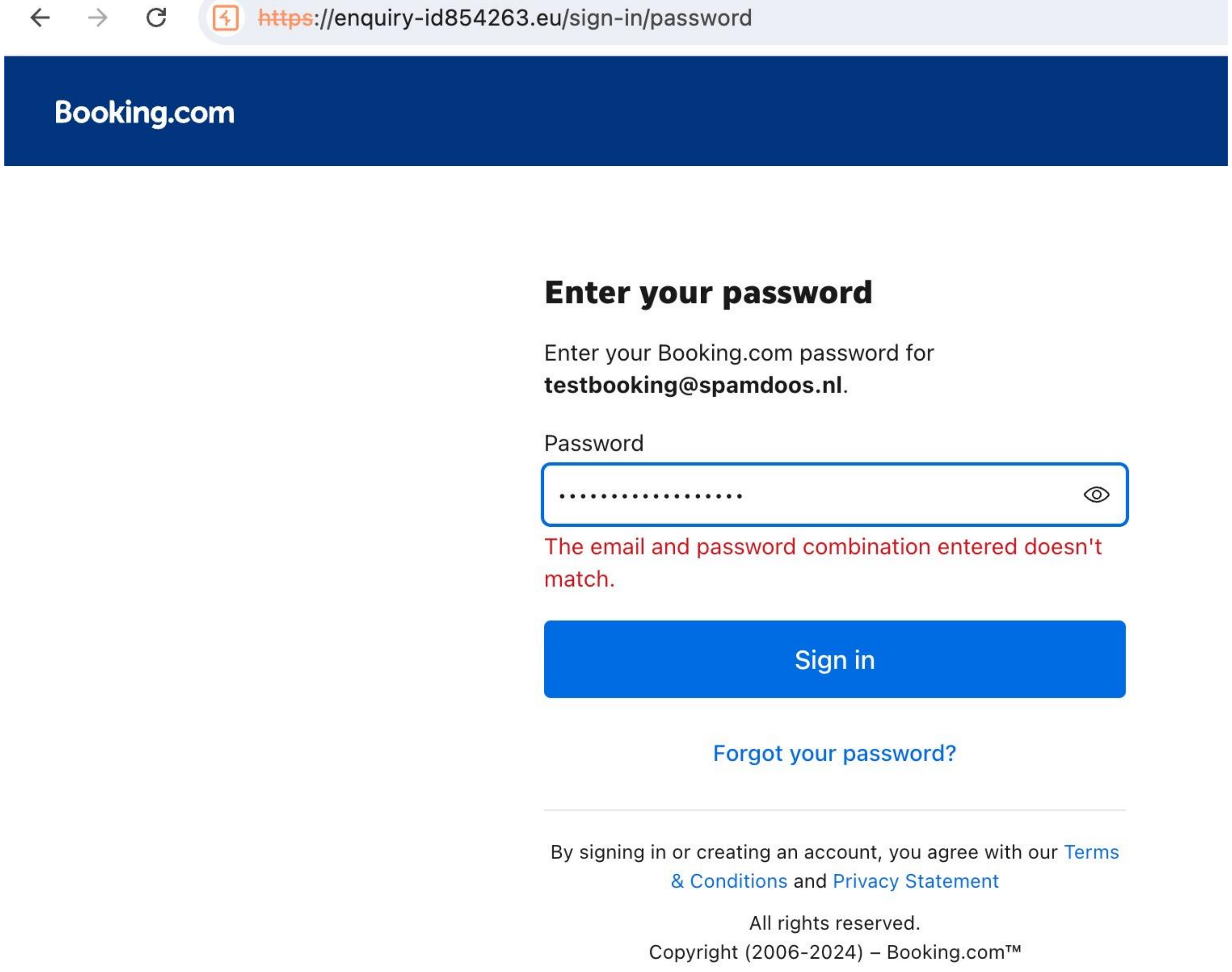


Search results (100 / 974, sorted by date, took 168ms)

🔒	URL	
🔒	booking.issue499.com/sign-in?op_token=NxldXFnUr8L11MAp1FDbpv5BP4i6YlfdxFaeE9WKA...	Public
🔒	complaint.issue499.com/sign-in?op_token=BibgFny5XF6cO93Rg6B1wAkbmnn1o53T2sn0Mxf...	Public
□	booking.issue499.com/sign-in?op_token=XIJyoyCQImPLo4AHWO5QqAILZ90TXfr1S9b38H6fu...	Public
□	booking.issue499.com/sign-in?op_token=NYYSwTQvqDCeLtbfuCGHat6yuPRIlLJCI88aXJRjP...	Public
🔒	booking.issue499.com/sign-in?op_token=BJts4at4GK9yOuYgUkkxalakagh7jaLscOWoilhIZ...	Public
🔒	booking.issue499.com/sign-in?op_token=zVQ1xkiUDSK0SNzenQcG40dd4GD91hy6tTy8222Ld...	Public
🔒	booking.issue499.com/sign-in?op_token=6OpYlLE1eHY42I7yOe13c0ufsizgHXT3Cchgg0DI7...	Public
□	booking.issue104.eu/sign-in?op_token=ACPUBYtOGdEaIMNuAq6IsCRhwMAl5qgJQLsLYRhsNu...	Public
🔒	booking.issue104.eu/sign-in?op_token=ao8uVWQJIrScERiDOMAY2IMPvUSeDZ3RsJUtinkgo8...	Public
🔒	booking.issue499.com/sign-in?op_token=ssDvnM0WDpcqOcOwXD2G1klpDTKjAH8CzIv37HpQf...	Public
🔒	complaint.issue499.com/sign-in?op_token=lzT5zryPZ3F4rDO9jsaskBmMSU2gI9C7b2LTj2g...	Public
🔒	complaint.issue1473.eu/sign-in?op_token=nlVj4IVozfQRoEYQsNEPXEZjm3xT8lsKyBtkOwb...	Public
🔒	complaint.issue412.eu/sign-in?op_token=mMVp6HDbqaQt4E0G1mfxUAqXk8o241V6zHoeXFB7...	Public
🔒	complaint.issue899.eu/sign-in?op_token=JbFUf1AAwyBPmwWZnQpT4bzIcUVGW6np0TMZABoi...	Public
🔒	complaint.issue899.eu/sign-in?op_token=V24IzjHM8nDG88bLyKbpZxeWpHUBhj2M4dcIlgLR...	Public
🔒	complaint.room543435.com/sign-in?op_token=i1BkV2q2UGxCi9tl0XcccerDeOPQ33r9hlygl...	Public

AtticSecurity.com
by ZOLDER

BOOKING.COM ATTACKS



~~https~~://enquiry-id854263.eu/sign-in/password

Booking.com

Enter your password

Enter your Booking.com password for **testbooking@spamdoos.nl**.

Password

••••••••••••••••••

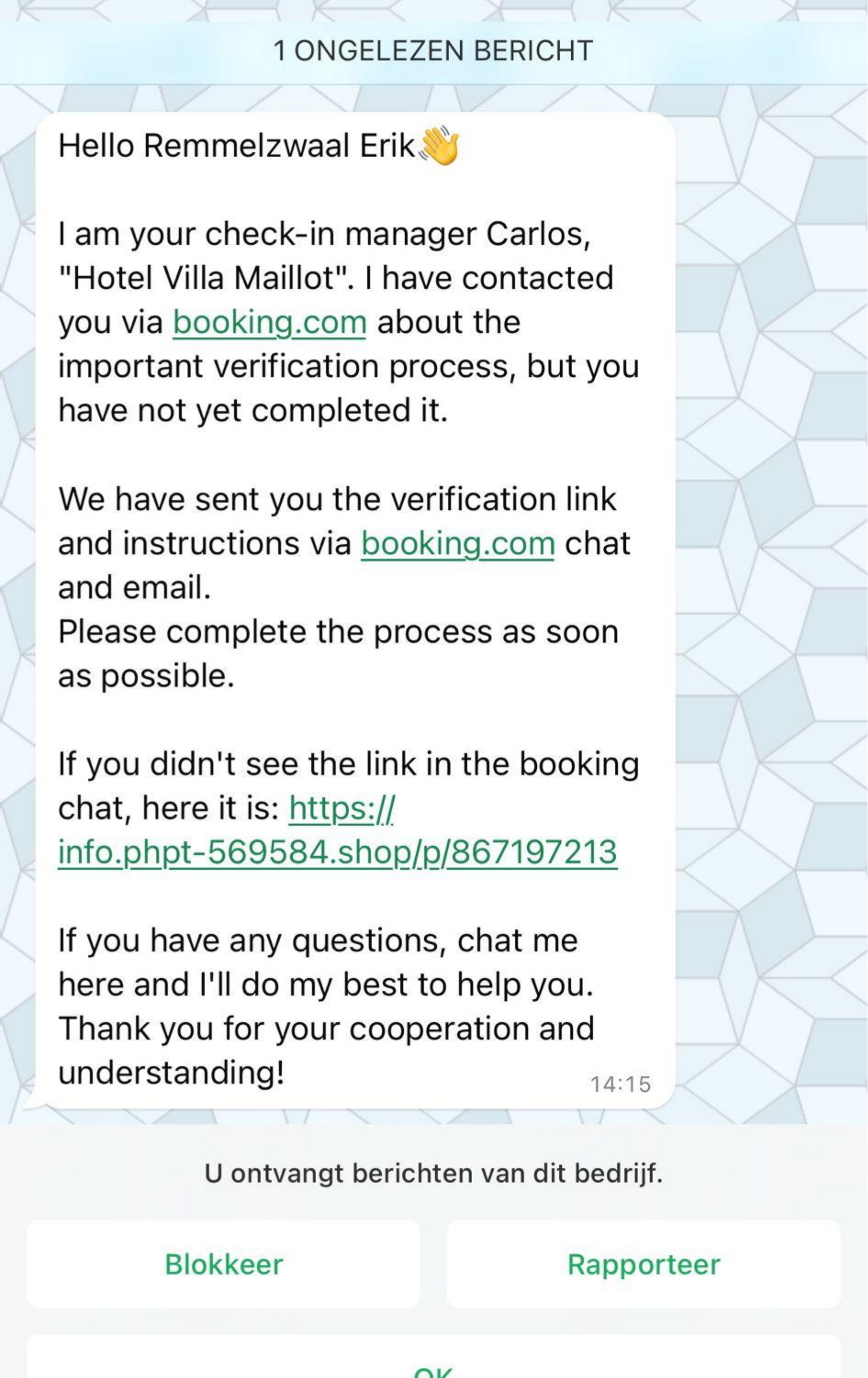
The email and password combination entered doesn't match.

Sign in

Forgot your password?

By signing in or creating an account, you agree with our Terms & Conditions and Privacy Statement

All rights reserved.
Copyright (2006-2024) – Booking.com™



1 ONGELEZEN BERICHT

Hello Remmelzwaal Erik👋

I am your check-in manager Carlos, "Hotel Villa Maillot". I have contacted you via booking.com about the important verification process, but you have not yet completed it.

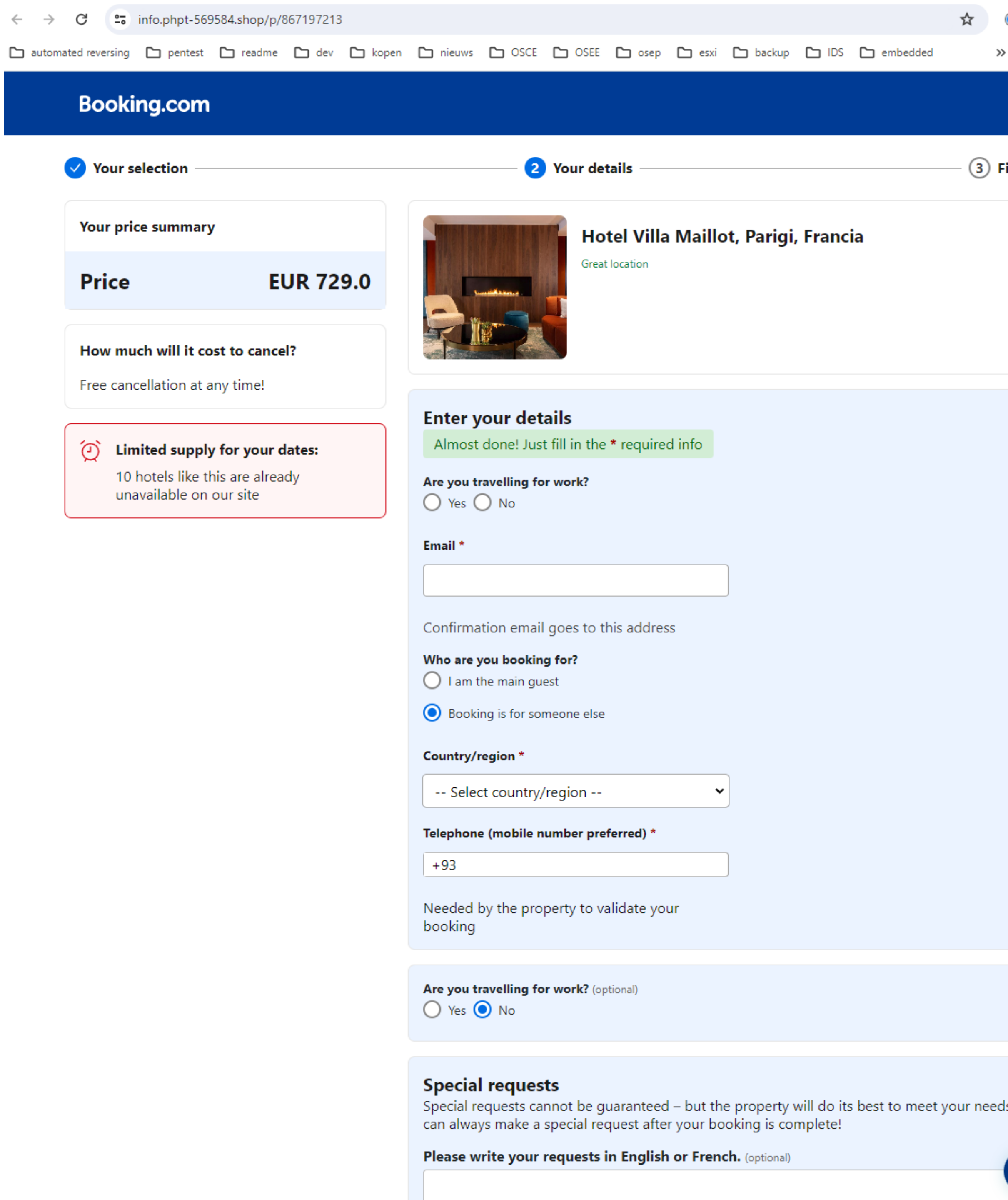
We have sent you the verification link and instructions via booking.com chat and email.
Please complete the process as soon as possible.

If you didn't see the link in the booking chat, here it is: https://info.phpt-569584.shop/p/867197213

If you have any questions, chat me here and I'll do my best to help you.
Thank you for your cooperation and understanding!

14:15

U ontvangt berichten van dit bedrijf.



Your price summary

Price EUR 729.0

How much will it cost to cancel?

Free cancellation at any time!

Limited supply for your dates:
10 hotels like this are already unavailable on our site

Hotel Villa Maillot, Parigi, Francia

Great location

Enter your details

Almost done! Just fill in the * required info

Are you travelling for work?
○ Yes ○ No

Email *

Confirmation email goes to this address

Who are you booking for?
○ I am the main guest
● Booking is for someone else

Country/region *
-- Select country/region --

Telephone (mobile number preferred) *
+93

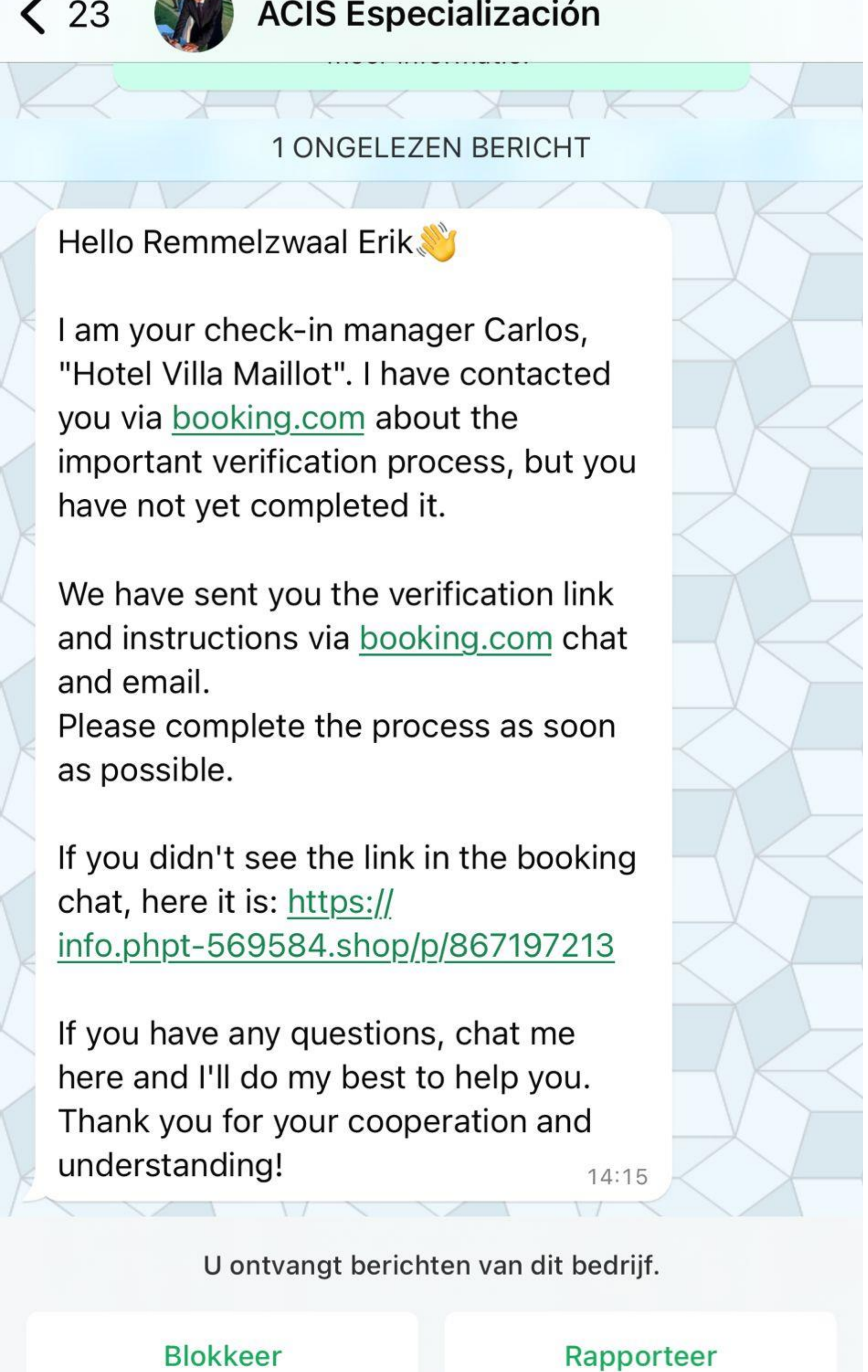
Needed by the property to validate your booking

Are you travelling for work? (optional)
○ Yes ● No

Special requests

Special requests cannot be guaranteed – but the property will do its best to meet your need
can always make a special request after your booking is complete!

Please write your requests in English or French. (optional)



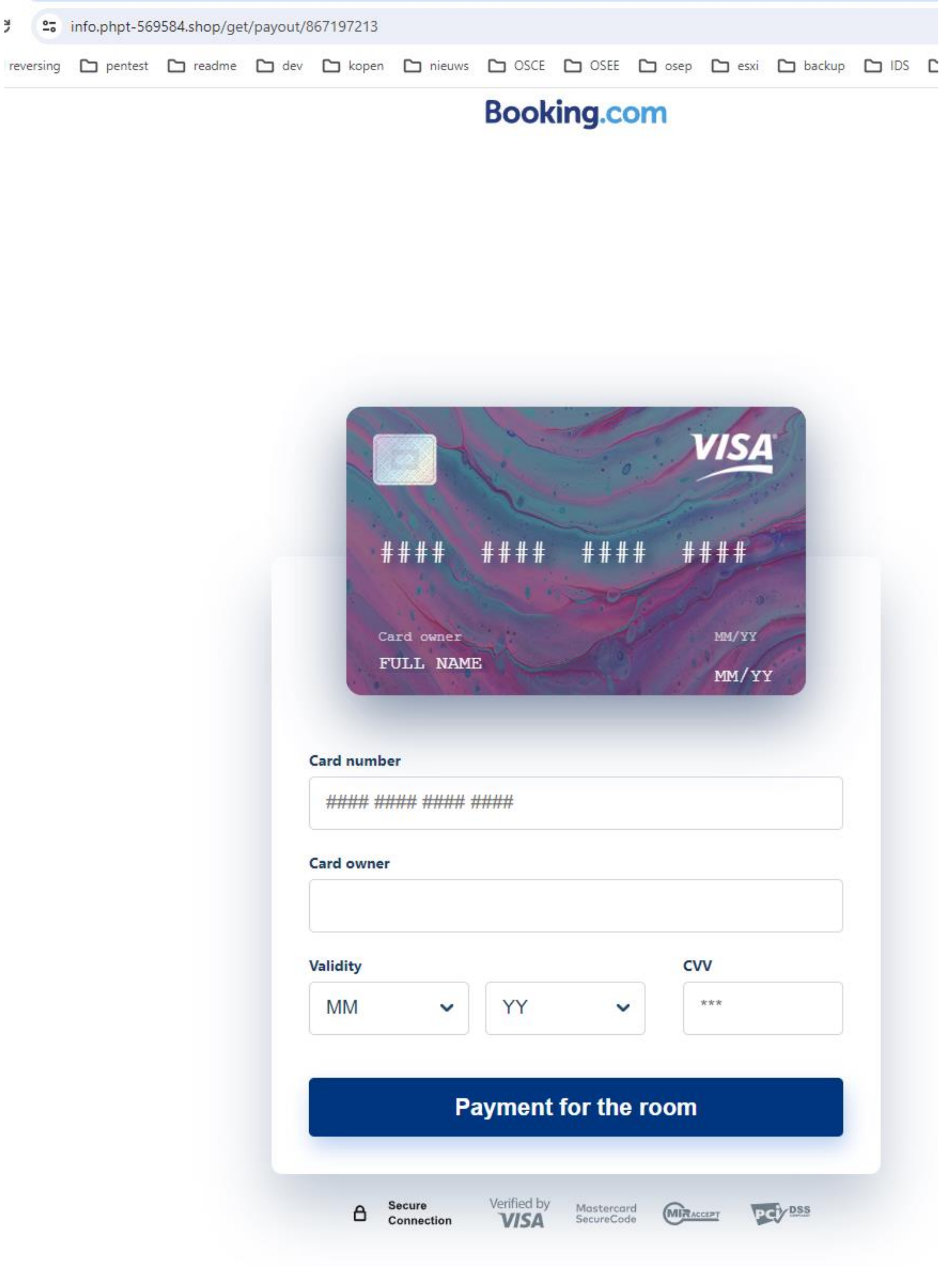
Hello Remmelzwaal Erik👋

I am your check-in manager Carlos, "Hotel Villa Maillot". I have contacted you via booking.com about the important verification process, but you have not yet completed it.

We have sent you the verification link and instructions via booking.com chat and email.
Please complete the process as soon as possible.

If you didn't see the link in the booking chat, here it is: https://info.phpt-569584.shop/p/867197213

If you have any questions, chat me here and I'll do my best to help you. Thank you for your cooperation and understanding! 14:15



Card number
####

Card owner

Validity
MM
YY

CVV
***

Payment for the room

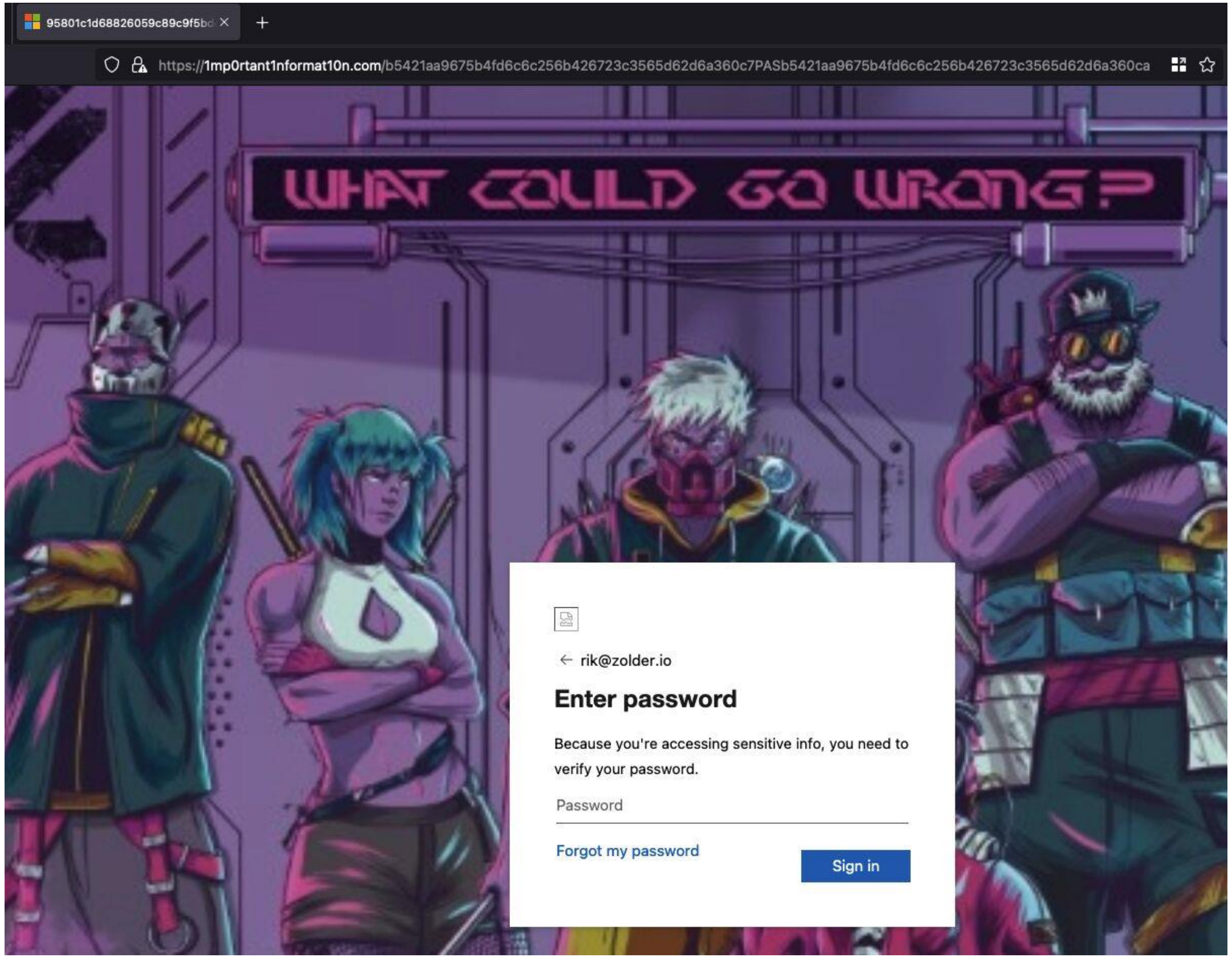
IMPLEMENTATIONS

IMPLEMENTATION

- Evilginx
- VNC in the browser
- Evilpuppet -> https://github.com/nexon33/EvilPuppetJS
- MSPHP panel -> https://github.com/Josexv1/wso-webshell/blob/master/wso.5.1.4.php
- Cloudflare Workers -> https://zolder.io/aitm-attacks-using-cloudflare-workers/

SOME HALF IMPLEMENTATIONS

- No CSS
- They only load logo and background



95801c1d68826059c89c9f5bd
https://1mp0rtant1nformat10n.com/b5421aa9675b4fd6c6c256b426723c3565d62d6a360c7PASb5421aa9675b4fd6c6c256b426723c3565d62d6a360ca
WHAT COULD GO WRONG?

← rik@zolder.io

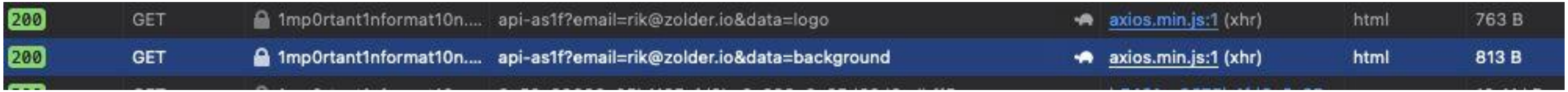
Enter password

Because you're accessing sensitive info, you need to verify your password.

Password

Forgot my password

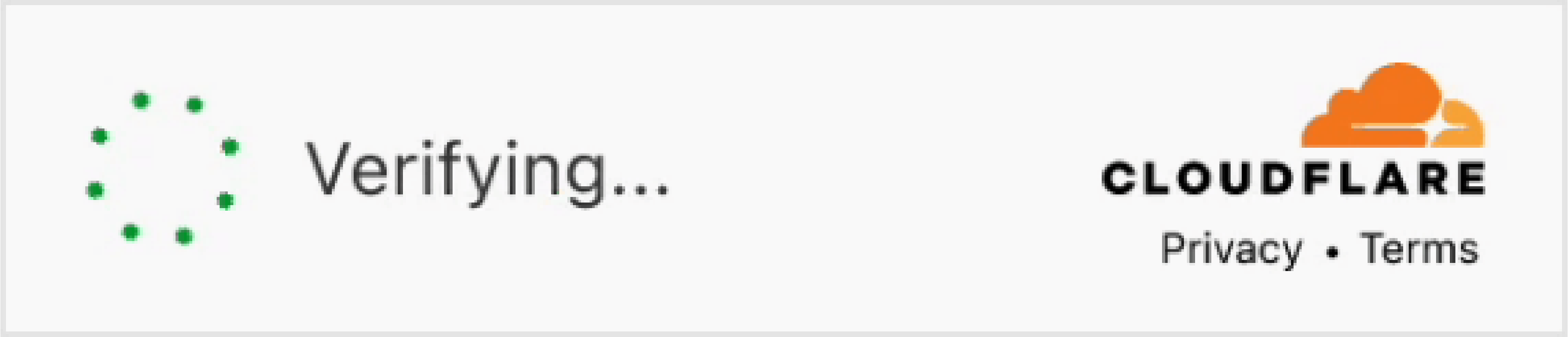
Sign in



```
200  GET  1mp0rtant1nformat10n....  api-as1f?email=rik@zolder.io&data=logo        axios.min.js:1 (xhr)  html  763 B
200  GET  1mp0rtant1nformat10n....  api-as1f?email=rik@zolder.io&data=background  axios.min.js:1 (xhr)  html  813 B
```

PREVENT DETECTION

When you see this, its almost always a problem



Verifying...

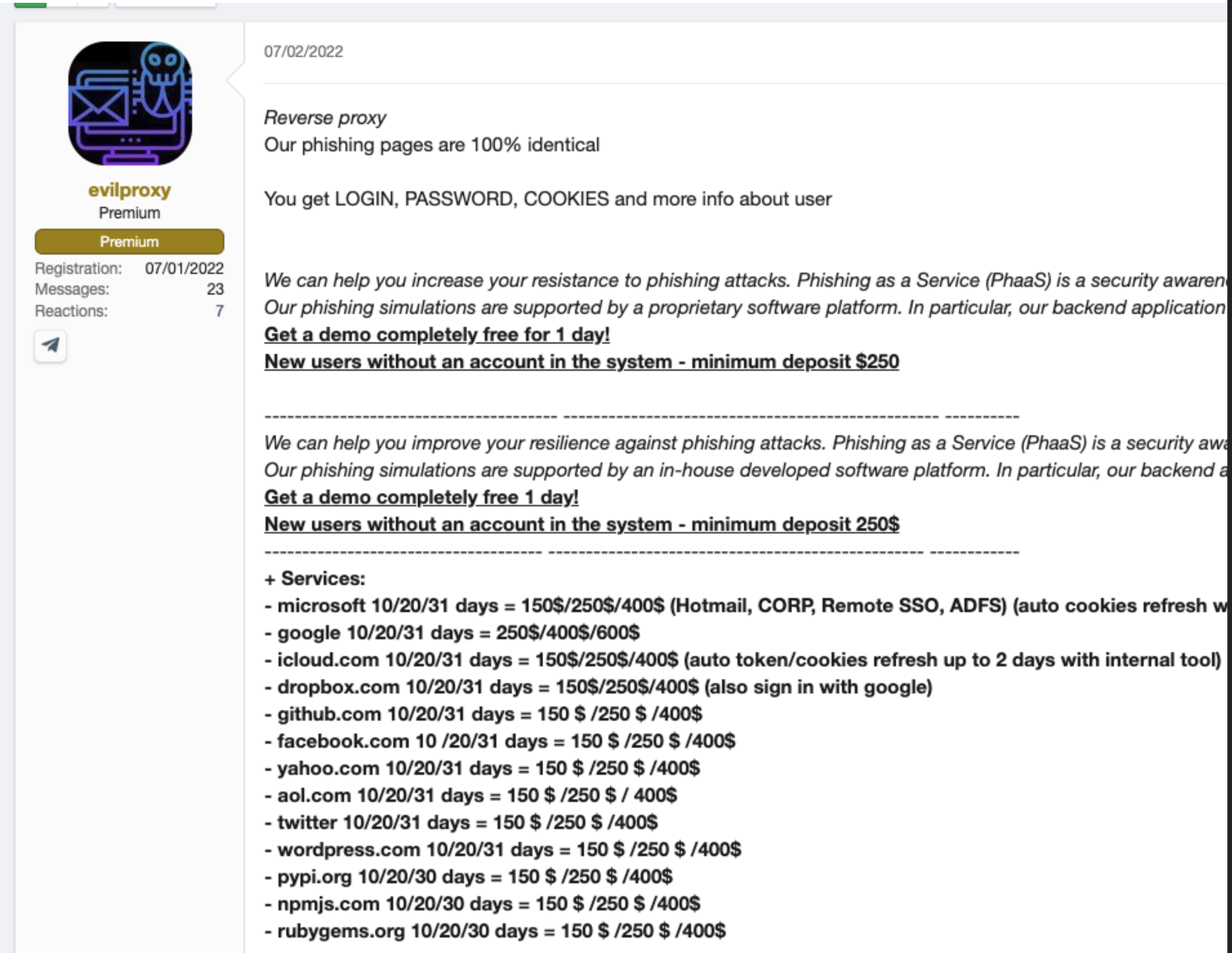
ACTORS

DIFFERENT ACTORS

- DaDSec
- EvilProxy
- Tycoon
- Greatness
- FishXProxy

- Change is coming, more and more non-saas but old-school panel providers are popping up.

EVILPROXY



evilproxy
Premium

Premium

Registration:	07/01/2022
Messages:	23
Reactions:	7

07/02/2022

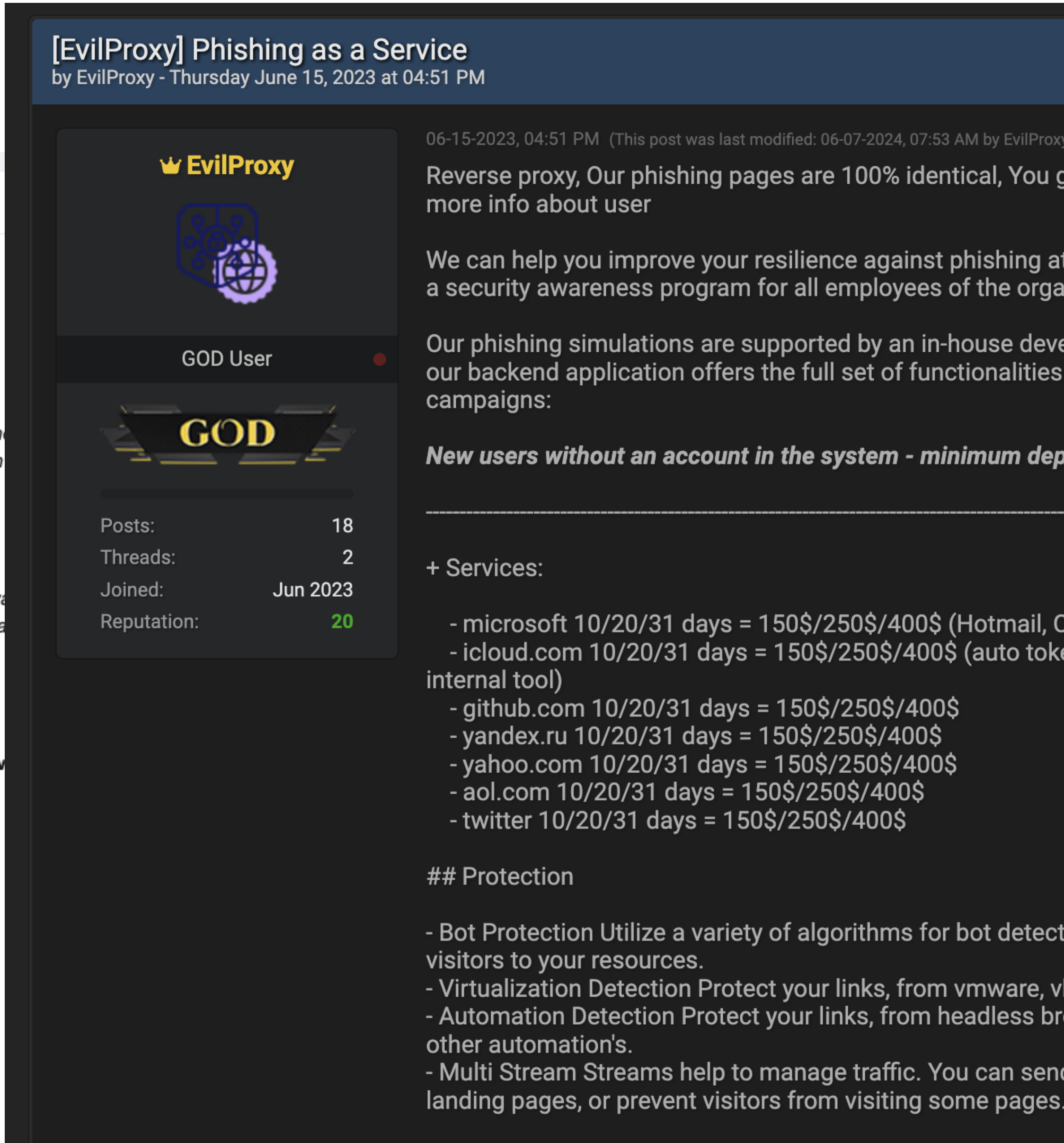
Reverse proxy
Our phishing pages are 100% identical

You get LOGIN, PASSWORD, COOKIES and more info about user

We can help you increase your resistance to phishing attacks. Phishing as a Service (PhaaS) is a security awaren
Our phishing simulations are supported by a proprietary software platform. In particular, our backend application
Get a demo completely free for 1 day!
New users without an account in the system - minimum deposit $250

-- -- ----------
We can help you improve your resilience against phishing attacks. Phishing as a Service (PhaaS) is a security awa
Our phishing simulations are supported by an in-house developed software platform. In particular, our backend a
Get a demo completely free 1 day!
New users without an account in the system - minimum deposit 250$
------------------------------------- -- ------------

+ Services:
- microsoft 10/20/31 days = 150$/250$/400$ (Hotmail, CORP, Remote SSO, ADFS) (auto cookies refresh w
- google 10/20/31 days = 250$/400$/600$
- icloud.com 10/20/31 days = 150$/250$/400$ (auto token/cookies refresh up to 2 days with internal tool)
- dropbox.com 10/20/31 days = 150$/250$/400$ (also sign in with google)
- github.com 10/20/31 days = 150 $ /250 $ /400$
- facebook.com 10 /20/31 days = 150 $ /250 $ /400$
- yahoo.com 10/20/31 days = 150 $ /250 $ /400$
- aol.com 10/20/31 days = 150 $ /250 $ / 400$
- twitter 10/20/31 days = 150 $ /250 $ /400$
- wordpress.com 10/20/31 days = 150 $ /250 $ /400$
- pypi.org 10/20/30 days = 150 $ /250 $ /400$
- npmjs.com 10/20/30 days = 150 $ /250 $ /400$
- rubygems.org 10/20/30 days = 150 $ /250 $ /400$



[EvilProxy] Phishing as a Service
by EvilProxy - Thursday June 15, 2023 at 04:51 PM

EvilProxy

GOD User

GOD

Posts:	18
Threads:	2
Joined:	Jun 2023
Reputation:	20

06-15-2023, 04:51 PM (This post was last modified: 06-07-2024, 07:53 AM by EvilProxy

Reverse proxy, Our phishing pages are 100% identical, You g
more info about user

We can help you improve your resilience against phishing at
a security awareness program for all employees of the orga

Our phishing simulations are supported by an in-house deve
our backend application offers the full set of functionalities
campaigns:

New users without an account in the system - minimum dep

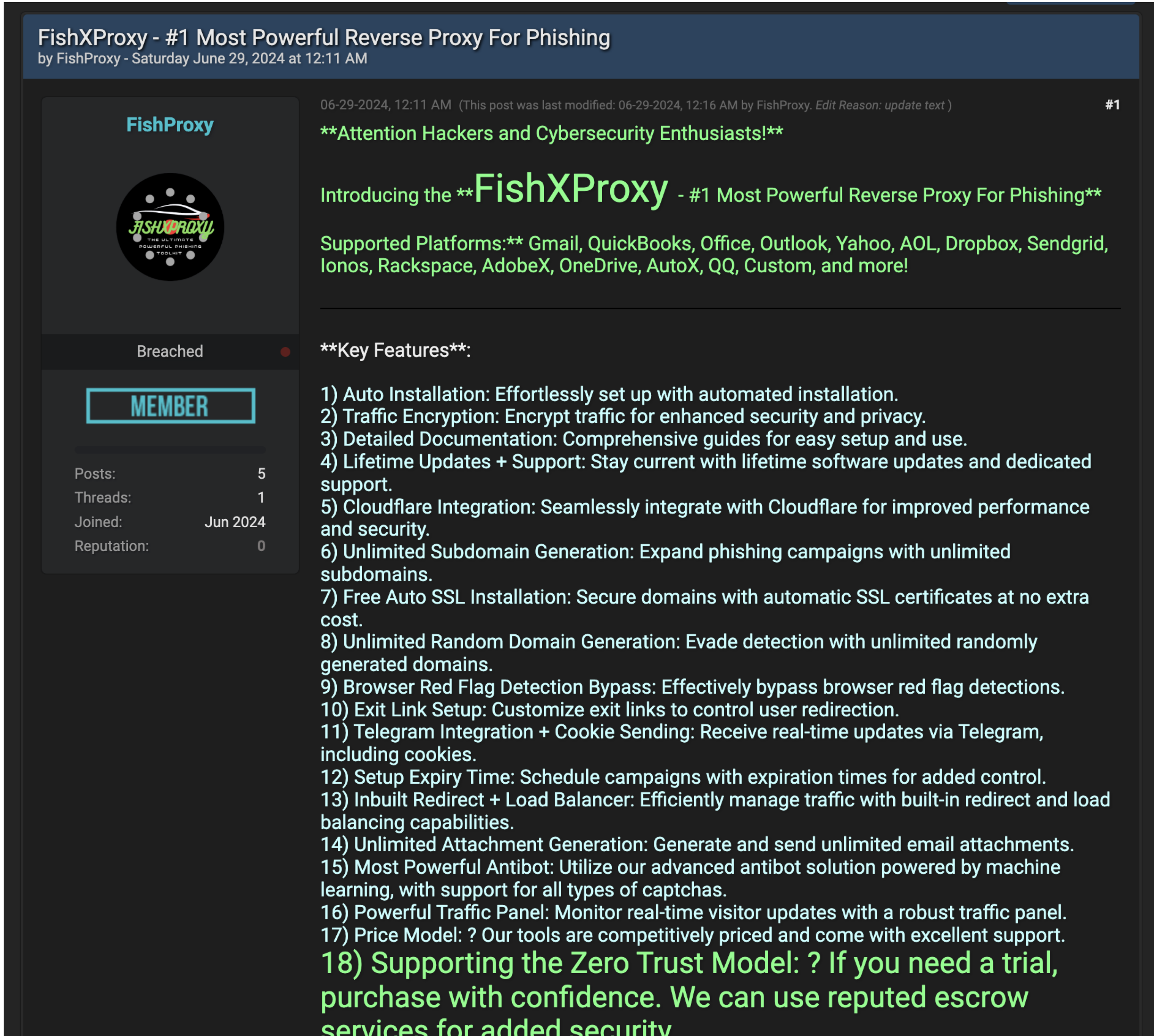
+ Services:

- microsoft 10/20/31 days = 150$/250$/400$ (Hotmail, C
- icloud.com 10/20/31 days = 150$/250$/400$ (auto toke
internal tool)
- github.com 10/20/31 days = 150$/250$/400$
- yandex.ru 10/20/31 days = 150$/250$/400$
- yahoo.com 10/20/31 days = 150$/250$/400$
- aol.com 10/20/31 days = 150$/250$/400$
- twitter 10/20/31 days = 150$/250$/400$

Protection

- Bot Protection Utilize a variety of algorithms for bot detect
visitors to your resources.
- Virtualization Detection Protect your links, from vmware, v
- Automation Detection Protect your links, from headless br
other automation's.
- Multi Stream Streams help to manage traffic. You can sen
landing pages, or prevent visitors from visiting some pages.

FISHXPROXY



FishXProxy - #1 Most Powerful Reverse Proxy For Phishing
by FishProxy - Saturday June 29, 2024 at 12:11 AM

Posts:	5
Threads:	1
Joined:	Jun 2024
Reputation:	0

06-29-2024, 12:11 AM (This post was last modified: 06-29-2024, 12:16 AM by FishProxy. *Edit Reason: update text*) #1

Attention Hackers and Cybersecurity Enthusiasts!

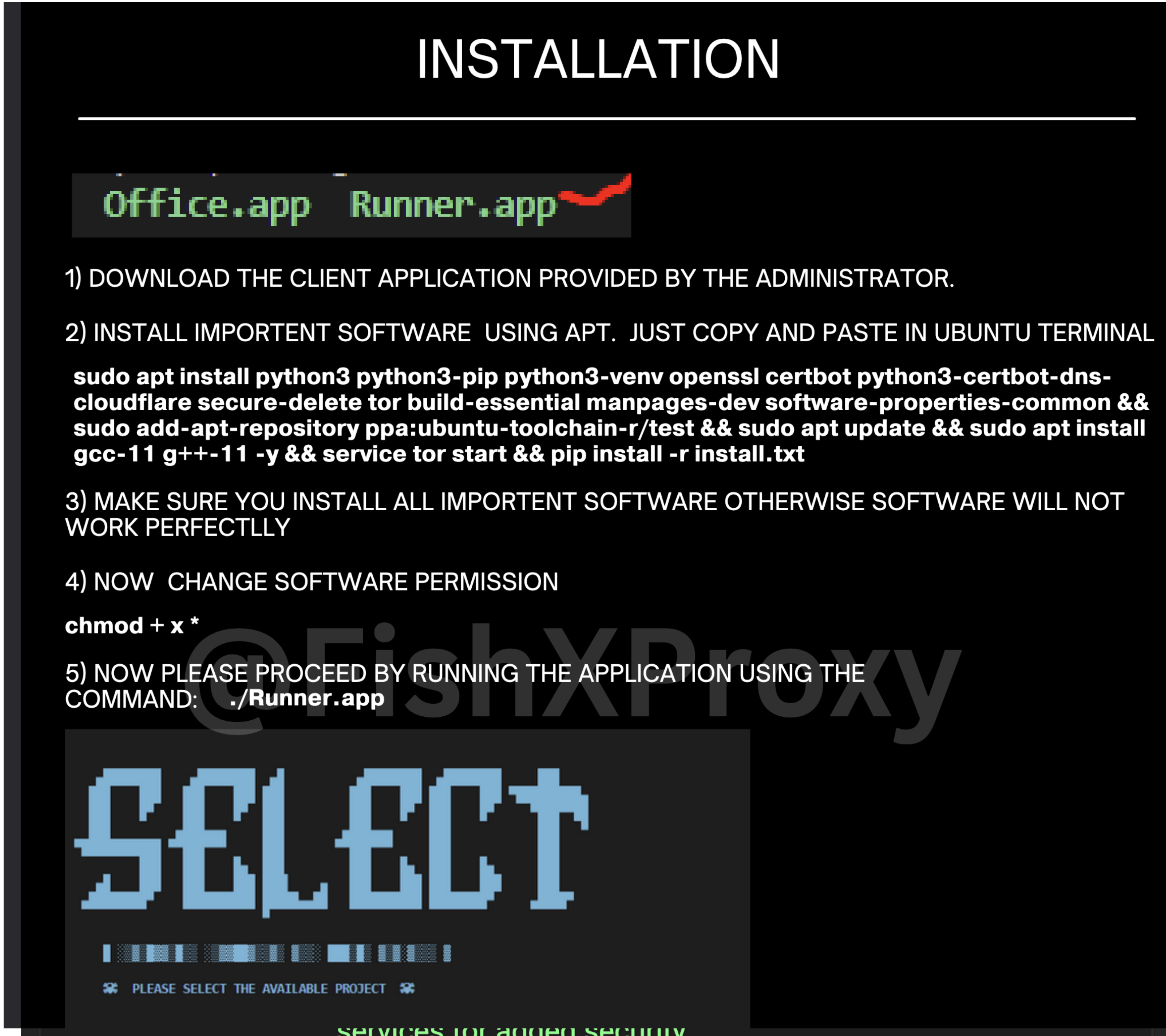
Introducing the **FishXProxy - #1 Most Powerful Reverse Proxy For Phishing**

Supported Platforms:** Gmail, QuickBooks, Office, Outlook, Yahoo, AOL, Dropbox, Sendgrid, Ionos, Rackspace, AdobeX, OneDrive, AutoX, QQ, Custom, and more!

Key Features:

1) Auto Installation: Effortlessly set up with automated installation.
2) Traffic Encryption: Encrypt traffic for enhanced security and privacy.
3) Detailed Documentation: Comprehensive guides for easy setup and use.
4) Lifetime Updates + Support: Stay current with lifetime software updates and dedicated support.
5) Cloudflare Integration: Seamlessly integrate with Cloudflare for improved performance and security.
6) Unlimited Subdomain Generation: Expand phishing campaigns with unlimited subdomains.
7) Free Auto SSL Installation: Secure domains with automatic SSL certificates at no extra cost.
8) Unlimited Random Domain Generation: Evade detection with unlimited randomly generated domains.
9) Browser Red Flag Detection Bypass: Effectively bypass browser red flag detections.
10) Exit Link Setup: Customize exit links to control user redirection.
11) Telegram Integration + Cookie Sending: Receive real-time updates via Telegram, including cookies.
12) Setup Expiry Time: Schedule campaigns with expiration times for added control.
13) Inbuilt Redirect + Load Balancer: Efficiently manage traffic with built-in redirect and load balancing capabilities.
14) Unlimited Attachment Generation: Generate and send unlimited email attachments.
15) Most Powerful Antibot: Utilize our advanced antibot solution powered by machine learning, with support for all types of captchas.
16) Powerful Traffic Panel: Monitor real-time visitor updates with a robust traffic panel.
17) Price Model: ? Our tools are competitively priced and come with excellent support.
18) Supporting the Zero Trust Model: ? If you need a trial, purchase with confidence. We can use reputed escrow services for added security

FISHXPROXY



INSTALLATION

```
Office.app  Runner.app
```

1) DOWNLOAD THE CLIENT APPLICATION PROVIDED BY THE ADMINISTRATOR.

2) INSTALL IMPORTENT SOFTWARE USING APT. JUST COPY AND PASTE IN UBUNTU TERMINAL

```
sudo apt install python3 python3-pip python3-venv openssl certbot python3-certbot-dns-cloudflare secure-delete tor build-essential manpages-dev software-properties-common && sudo add-apt-repository ppa:ubuntu-toolchain-r/test && sudo apt update && sudo apt install gcc-11 g++-11 -y && service tor start && pip install -r install.txt
```

3) MAKE SURE YOU INSTALL ALL IMPORTENT SOFTWARE OTHERWISE SOFTWARE WILL NOT WORK PERFECTLLY

4) NOW CHANGE SOFTWARE PERMISSION

```
chmod + x *
```

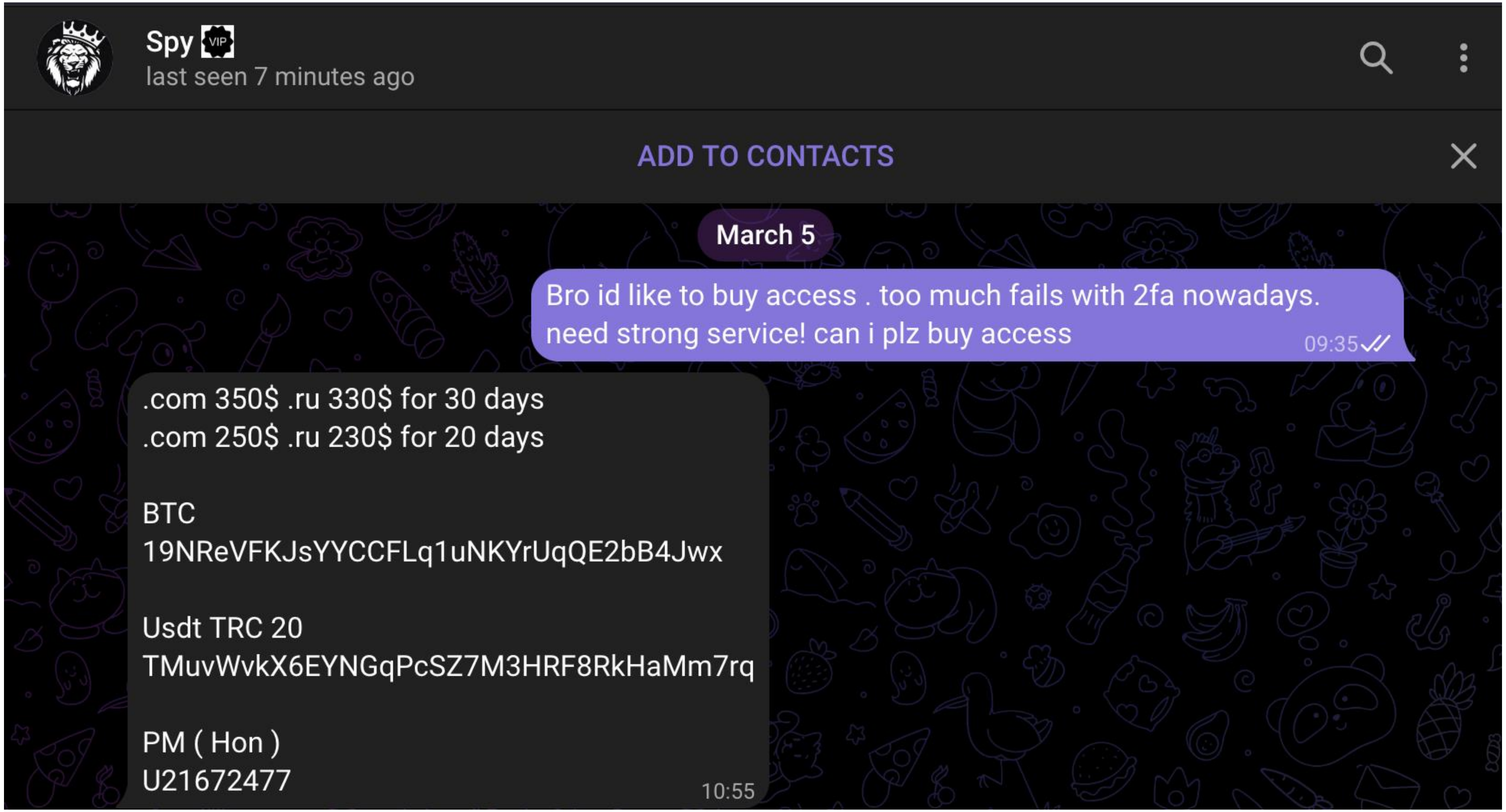
5) NOW PLEASE PROCEED BY RUNNING THE APPLICATION USING THE COMMAND: **./Runner.app**

```
SELECT

  PLEASE SELECT THE AVAILABLE PROJECT
```

services for added security

TYCOON



Bro id like to buy access . too much fails with 2fa nowadays. need strong service! can i plz buy access 09:35

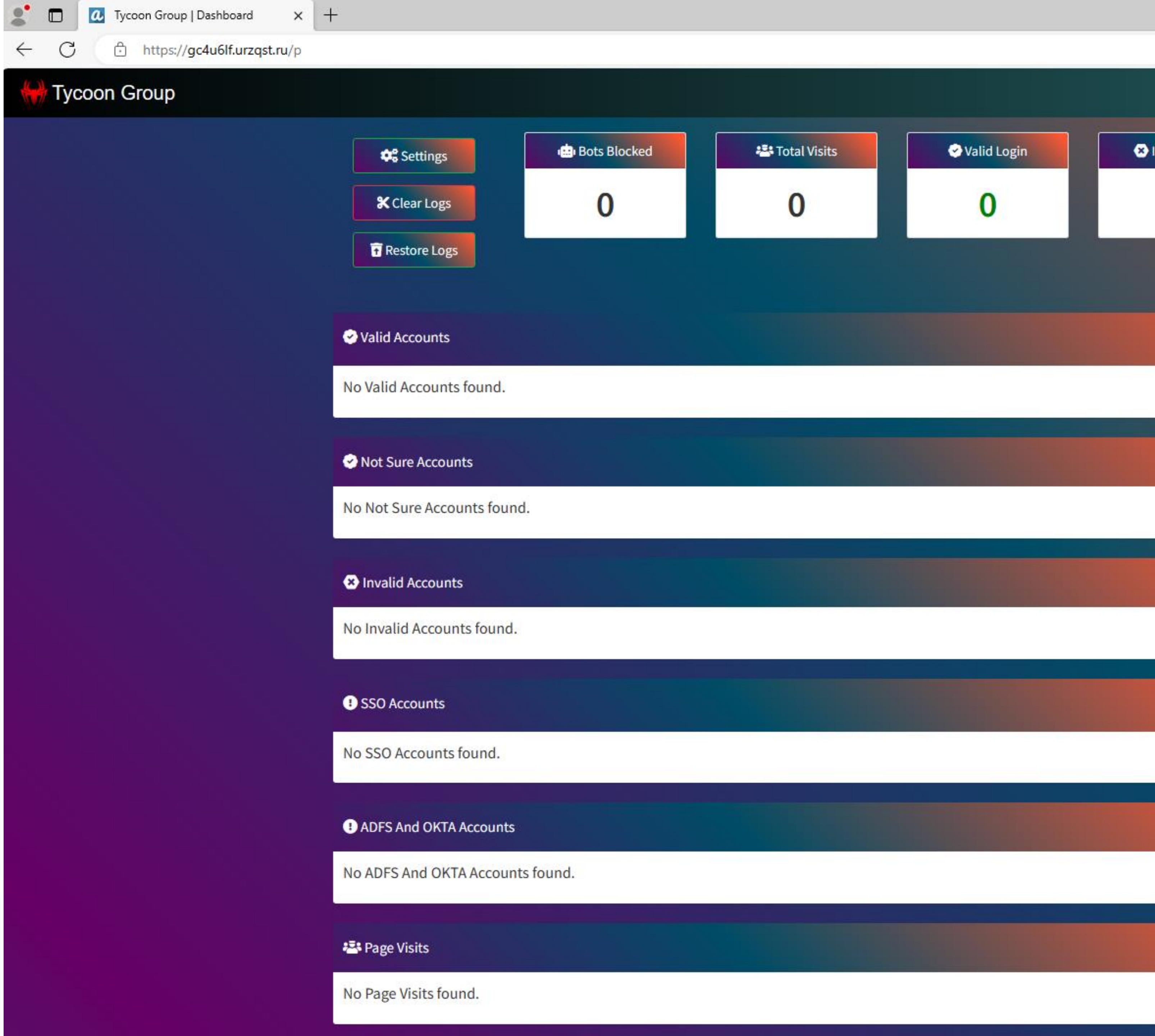
.com 350$ .ru 330$ for 30 days
.com 250$ .ru 230$ for 20 days

BTC
19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx

Usdt TRC 20
TMuvWvkX6EYNGqPcSZ7M3HRF8RkHaMm7rq

PM (Hon)
U21672477 10:55

TYCOON



https://gc4u6lf.urzqst.ru/p

Tycoon Group

Bots Blocked 0

Total Visits 0

Valid Login 0

Valid Accounts

No Valid Accounts found.

Not Sure Accounts

No Not Sure Accounts found.

Invalid Accounts

No Invalid Accounts found.

SSO Accounts

No SSO Accounts found.

ADFS And OKTA Accounts

No ADFS And OKTA Accounts found.

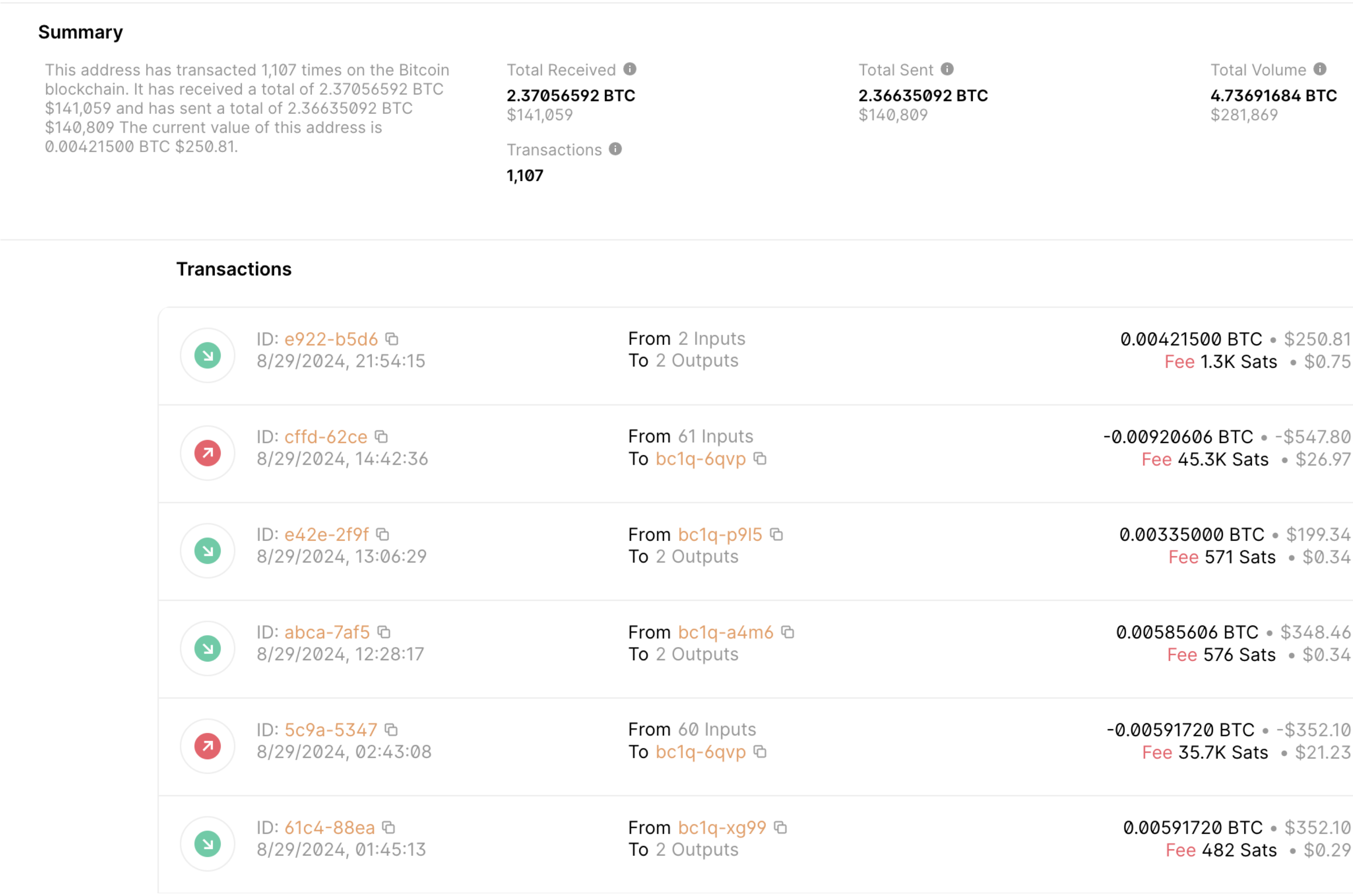
Page Visits

No Page Visits found.

TYCOON

- 1GvdAwPyTRKmRzybyrfHtbYWVJbecCbTNj
- 19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx
- TMuvWvkX6EYNGqPcSZ7M3HRF8RkHaMm7rq

- 660K+ (dependent on BTC price 😂)



Summary

This address has transacted 1,107 times on the Bitcoin blockchain. It has received a total of 2.37056592 BTC $141,059 and has sent a total of 2.36635092 BTC $140,809 The current value of this address is 0.00421500 BTC $250.81.

Total Received	Total Sent	Total Volume
2.37056592 BTC $141,059	2.36635092 BTC $140,809	4.73691684 BTC $281,869

Transactions
1,107

Transactions

↘	ID: e922-b5d6 8/29/2024, 21:54:15	From 2 Inputs To 2 Outputs	0.00421500 BTC • $250.81 Fee 1.3K Sats • $0.75
↗	ID: cffd-62ce 8/29/2024, 14:42:36	From 61 Inputs To bc1q-6qvp	-0.00920606 BTC • -$547.80 Fee 45.3K Sats • $26.97
↘	ID: e42e-2f9f 8/29/2024, 13:06:29	From bc1q-p9l5 To 2 Outputs	0.00335000 BTC • $199.34 Fee 571 Sats • $0.34
↘	ID: abca-7af5 8/29/2024, 12:28:17	From bc1q-a4m6 To 2 Outputs	0.00585606 BTC • $348.46 Fee 576 Sats • $0.34
↗	ID: 5c9a-5347 8/29/2024, 02:43:08	From 60 Inputs To bc1q-6qvp	-0.00591720 BTC • -$352.10 Fee 35.7K Sats • $21.23
↘	ID: 61c4-88ea 8/29/2024, 01:45:13	From bc1q-xg99 To 2 Outputs	0.00591720 BTC • $352.10 Fee 482 Sats • $0.29

PREVENTION AND DETECTION

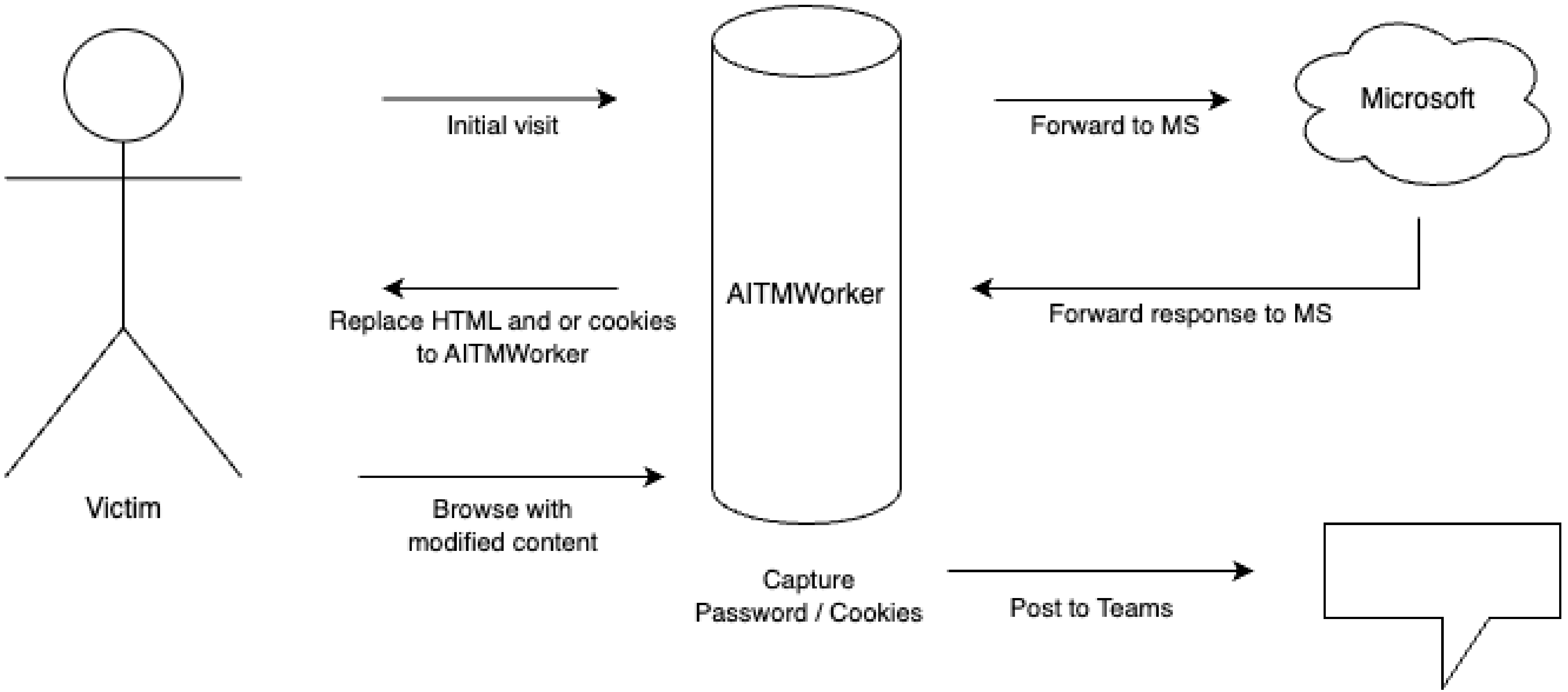
PREVENTION FOR M365 IS *EASY*

- … Compared to other SaaS platforms
- For companies with budget

Options:

- Enforce phishing resistant MFA (requires AAD P1/P2)
- Enforce device compliance (requires AAD P1/P2)

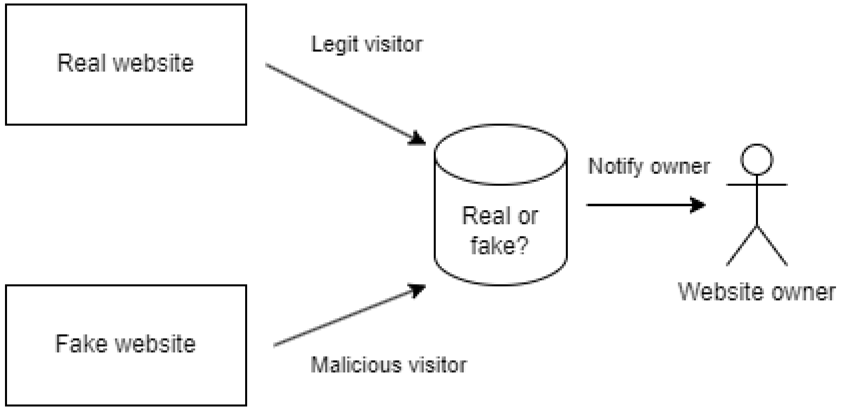
HOW THE REVERSE PROXIES WORK


Initial visit
Forward to MS
Microsoft
AITMWorker
Replace HTML and or cookies to AITMWorker
Forward response to MS
Victim
Browse with modified content
Capture Password / Cookies
Post to Teams

DETECTING ATTACKS

Built detection technique for regular phishing sites (didsomeoneclone.me):

- Inserting a pixel into the real website -> loaded via the real or fake website?

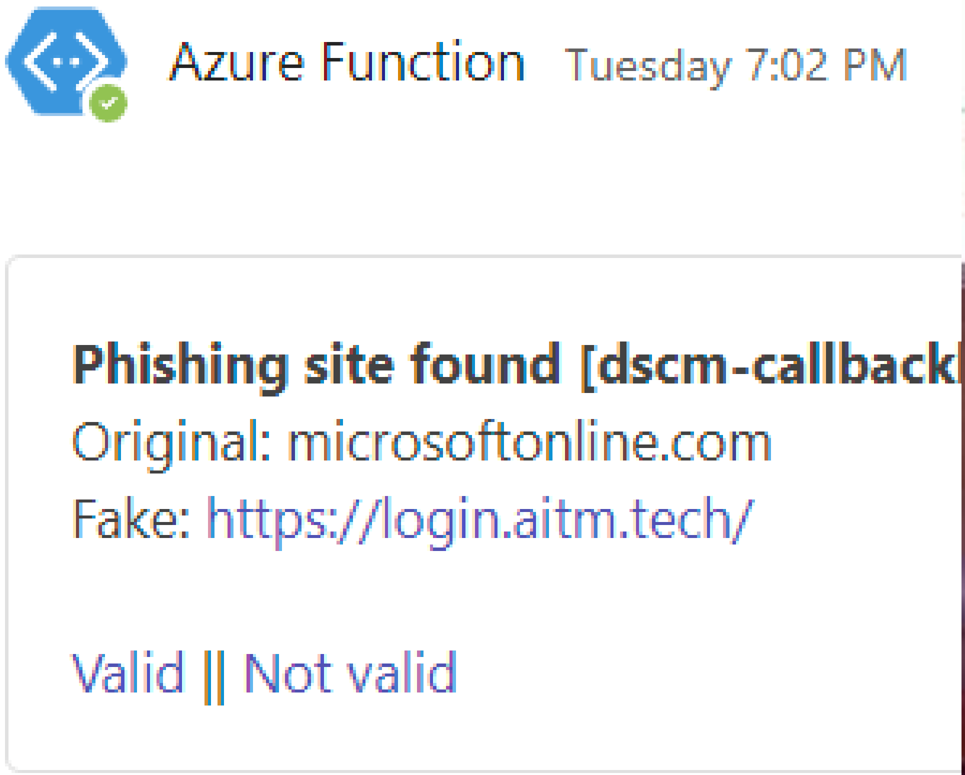


PIXEL + MICROSOFT 365?

- Erik: what about Microsoft Custom Branding CSS setting?

CAN WE GET A PIXEL INTO M365 LOGIN PAGES?

- The answer is: yes



Azure Function Tuesday 7:02 PM

Phishing site found [dscm-callback

Original: microsoftonline.com

Fake: https://login.aitm.tech/

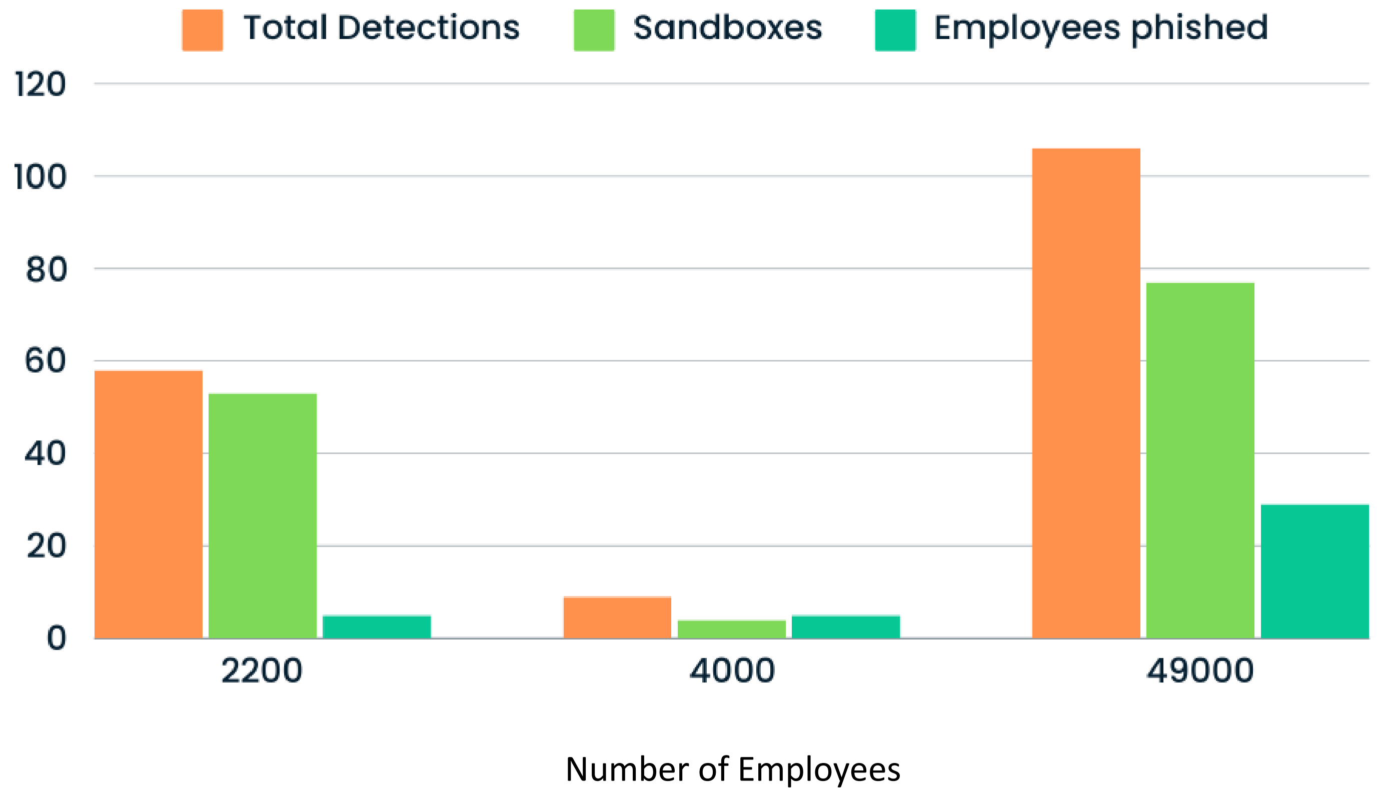
Valid || Not valid

EXPECTATION: IT’S A SMALL GROUP THAT’S TARGETED

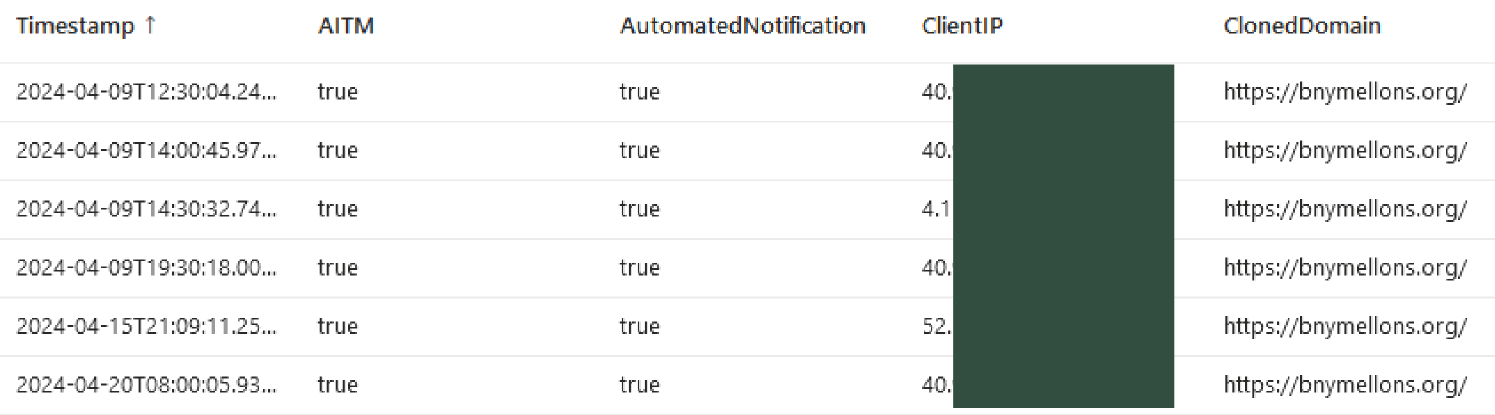
- “It doesn’t happen often”
- Reality:
  - **First month**
  - **100** tenants
  - **162** detections

  - **9 months**
  - **368** tenants
  - **1307** detections

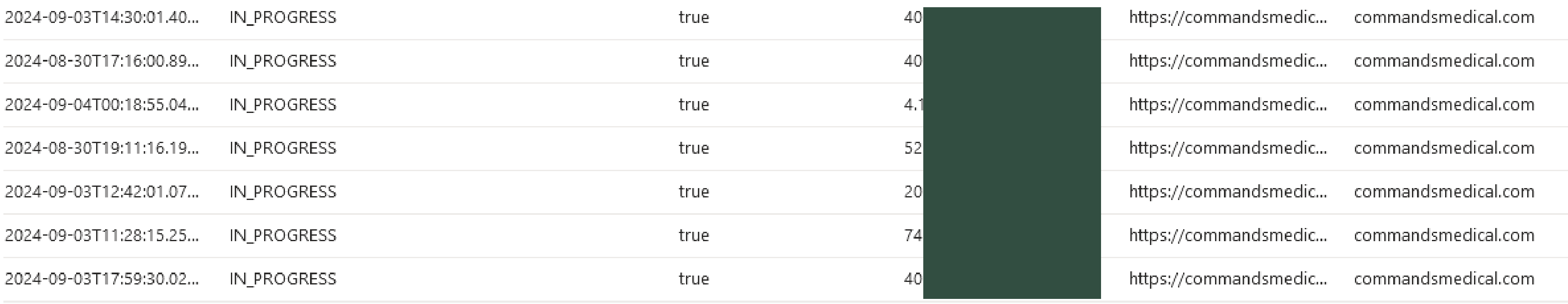
Customer Examples didsomeoneclone.me (two months timeframe)



AT SCALE, DIFFERENT TENANTS SAME DOMAIN



Timestamp ↑	AITM	AutomatedNotification	ClientIP	ClonedDomain
2024-04-09T12:30:04.24...	true	true	40.[redacted]	https://bnymellons.org/
2024-04-09T14:00:45.97...	true	true	40.[redacted]	https://bnymellons.org/
2024-04-09T14:30:32.74...	true	true	4.1[redacted]	https://bnymellons.org/
2024-04-09T19:30:18.00...	true	true	40.[redacted]	https://bnymellons.org/
2024-04-15T21:09:11.25...	true	true	52.[redacted]	https://bnymellons.org/
2024-04-20T08:00:05.93...	true	true	40.[redacted]	https://bnymellons.org/



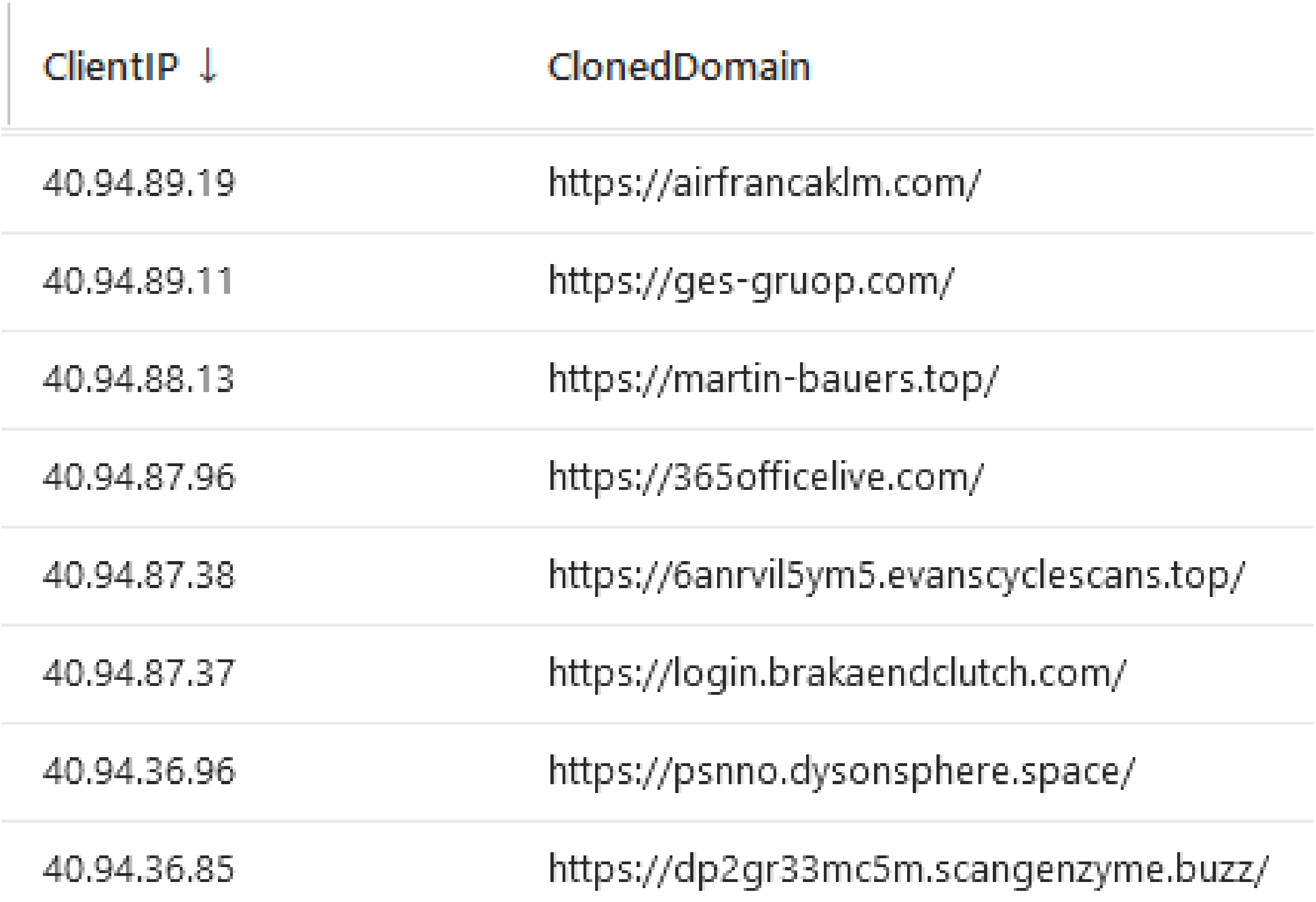
2024-09-03T14:30:01.40...	IN_PROGRESS	true	40[redacted]	https://commandsmedic...	commandsmedical.com
2024-08-30T17:16:00.89...	IN_PROGRESS	true	40[redacted]	https://commandsmedic...	commandsmedical.com
2024-09-04T00:18:55.04...	IN_PROGRESS	true	4.1[redacted]	https://commandsmedic...	commandsmedical.com
2024-08-30T19:11:16.19...	IN_PROGRESS	true	52[redacted]	https://commandsmedic...	commandsmedical.com
2024-09-03T12:42:01.07...	IN_PROGRESS	true	20[redacted]	https://commandsmedic...	commandsmedical.com
2024-09-03T11:28:15.25...	IN_PROGRESS	true	74[redacted]	https://commandsmedic...	commandsmedical.com
2024-09-03T17:59:30.02...	IN_PROGRESS	true	40[redacted]	https://commandsmedic...	commandsmedical.com

FALSE POSITIVES?

- Limited, some examples:
  - login.microsoft.com
  - tasks.office.com
  - autologon.microsoftazuread-sso.com
  - login.windows.net

Very reliable detection, after fine-tuning

MICROSOFT SANDBOXES

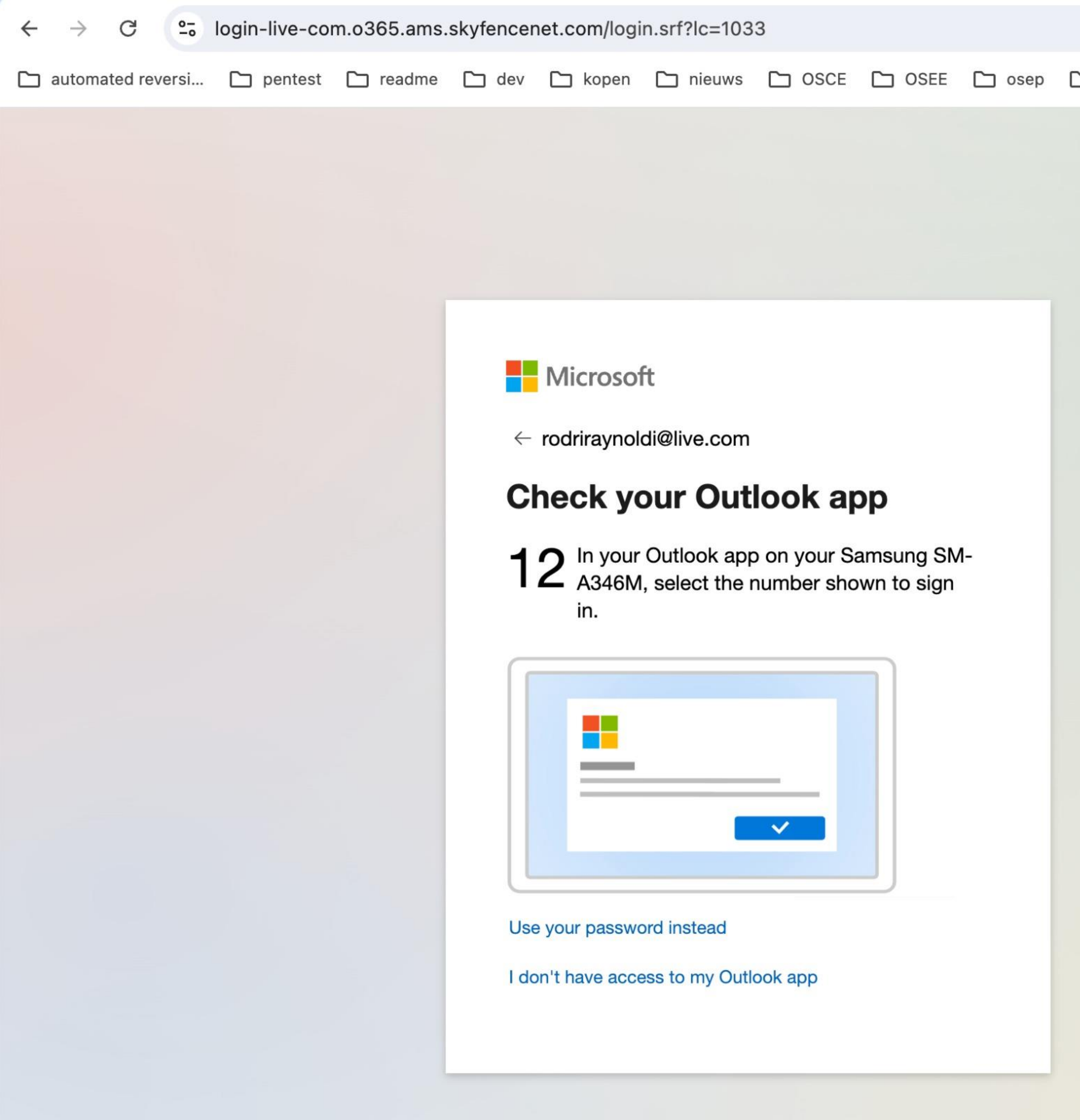


ClientIP ↓	ClonedDomain
40.94.89.19	https://airfrancaklm.com/
40.94.89.11	https://ges-gruop.com/
40.94.88.13	https://martin-bauers.top/
40.94.87.96	https://365officelive.com/
40.94.87.38	https://6anrvil5ym5.evanscyclescans.top/
40.94.87.37	https://login.brakaendclutch.com/
40.94.36.96	https://psnno.dysonsphere.space/
40.94.36.85	https://dp2gr33mc5m.scangenzyme.buzz/

THE FUTURE

FUTURE

- We’ve seen an increase in the offering of reverse proxy phishlets or just complete solutions
- There’s also been a push for generic reverse proxies that don’t need to be modified per website
- Banking phishing would require some extra development but it’s a matter of time



login-live-com.o365.ams.skyfencenet.com/login.srf?lc=1033

Microsoft

rodriraynoldi@live.com

Check your Outlook app

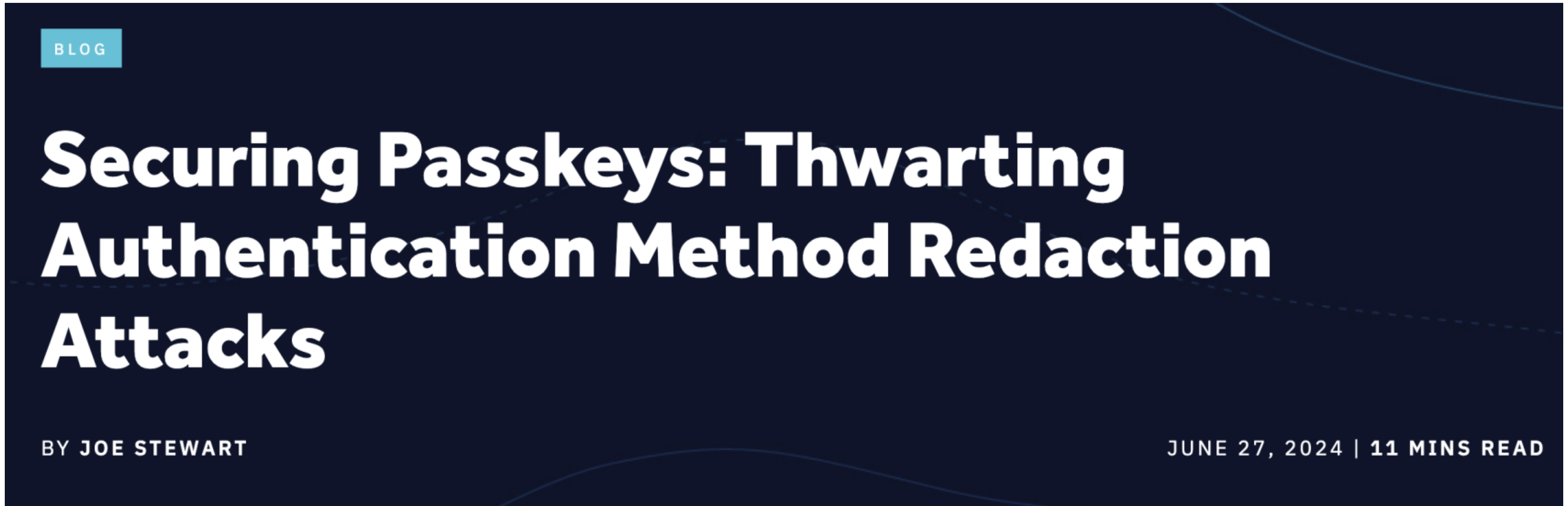
12 In your Outlook app on your Samsung SM-A346M, select the number shown to sign in.

Use your password instead

I don't have access to my Outlook app

CONCLUSION

- Its gonna be shit for a while
  - Increase in AITM attacks against regular users
  - Increase in AITM attacks against generic platforms
  - Companies will need to switch
- Passkeys are great but the UX isnt there yet
- Passkeys are great but not enforcing them once configured leaves you vulnerable



BLOG

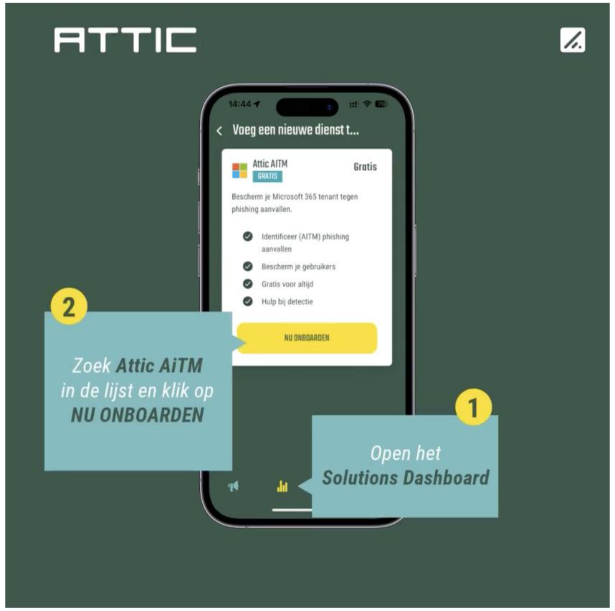
Securing Passkeys: Thwarting Authentication Method Redaction Attacks

BY JOE STEWART

JUNE 27, 2024 | 11 MINS READ

THANK YOU

Want free aitm detection for Microsoft 365? ->



Voeg een nieuwe dienst t...

Attic AITM GRATIS Gratis

Bescherm je Microsoft 365 tenant tegen phishing aanvallen.

- ✓ Identificeer (AITM) phishing aanvallen
- ✓ Bescherm je gebruikers
- ✓ Gratis voor altijd
- ✓ Hulp bij detectie

NU ONBOARDEN

2 Zoek Attic AiTM in de lijst en klik op NU ONBOARDEN

1 Open het Solutions Dashboard

atticsecurity.com/aitmfree