

ZOLDER

AIM & 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.



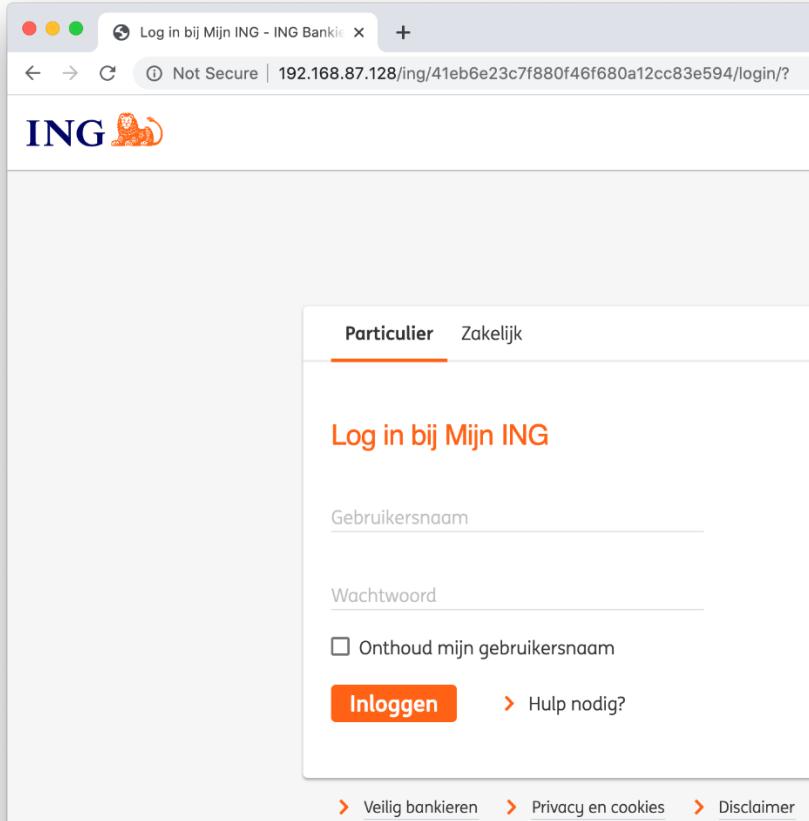


SOME HISTORY

The screenshot shows a web browser window with the following details:

- Title Bar:** mail.yahoo.com - Home
- Address Bar:** pikkeyistu.weebly.com
- Content Area:** A large purple "Y!" logo is centered at the top. Below it, the word "YAHOO!" is written in a large, bold, purple font.
- Form Fields:** There are two input fields:
 - An "Email" field with a placeholder and a red asterisk indicating it is required.
 - A "Pass" field with a placeholder and a red asterisk indicating it is required.
- Buttons:** A "SIGN IN" button at the bottom of the form area.
- Annotations:** A small note above the first input field states: "* Indicates required field".

SOME HISTORY



Log in bij Mijn ING

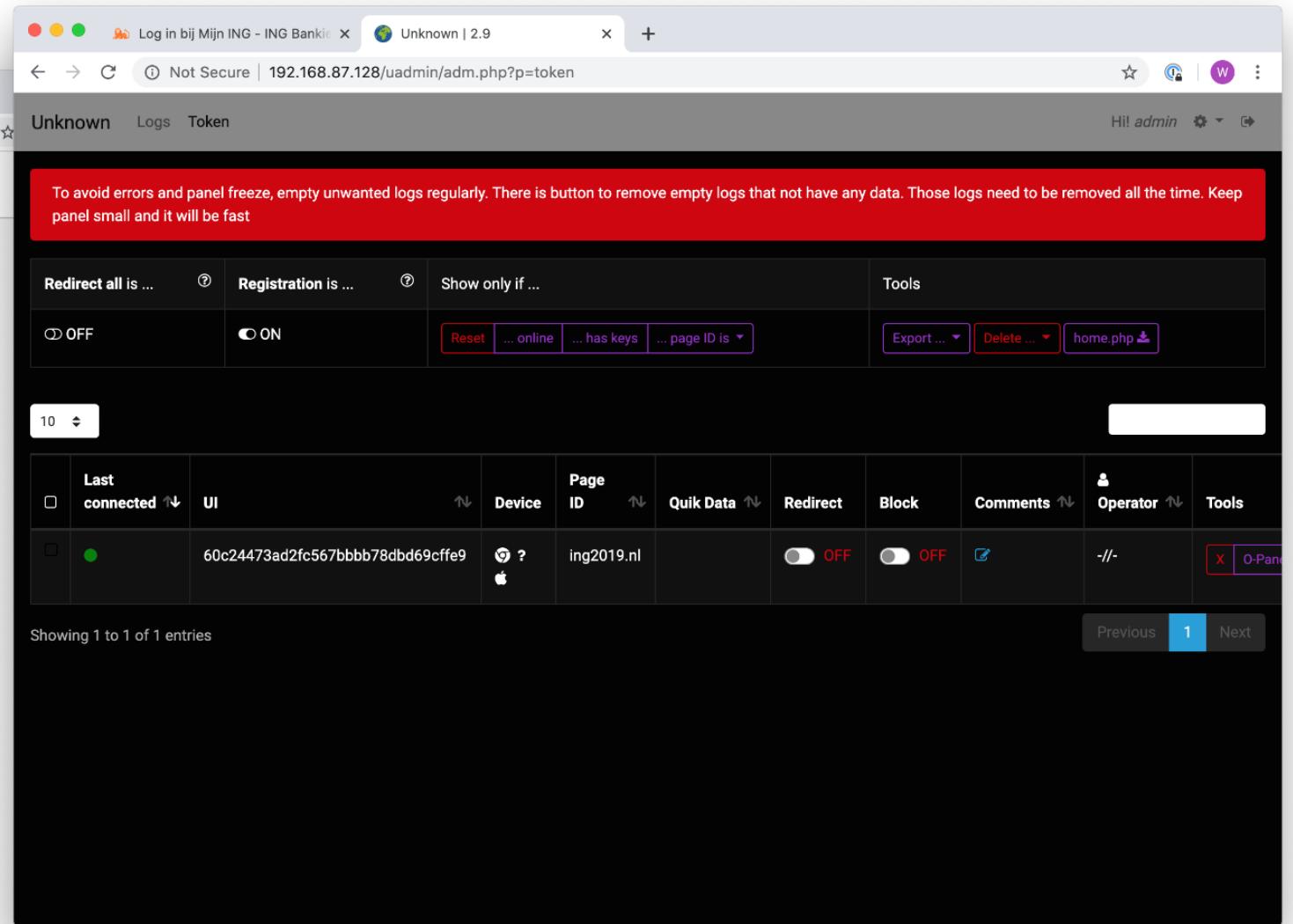
Gebruikersnaam

Wachtwoord

Onthoud mijn gebruikersnaam

Inloggen ➤ Hulp nodig?

➤ Veilig bankieren ➤ Privacy en cookies ➤ Disclaimer



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 |
|---------------------------|-------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| <input type="radio"/> OFF | <input checked="" type="radio"/> ON | Reset ... online ... has keys ... page ID is ... | Export ... Delete ... home.php ↻ |

| Last connected | UI | Device | Page ID | Quik Data | Redirect | Block | Comments | Operator | Tools |
|---------------------------------|------------|--------|---------|-----------|----------|-------|----------|----------|-------|
| 60c24473ad2fc567bbbb78dbd69cff9 | ing2019.nl | OFF | OFF | -//- | X O-Pan | | | | |

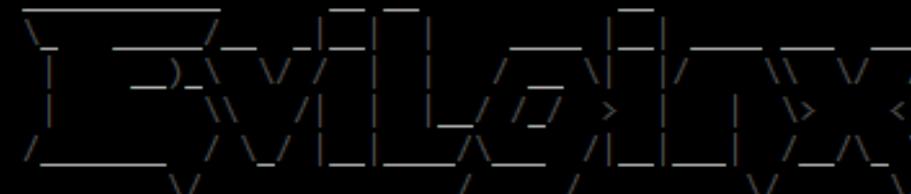
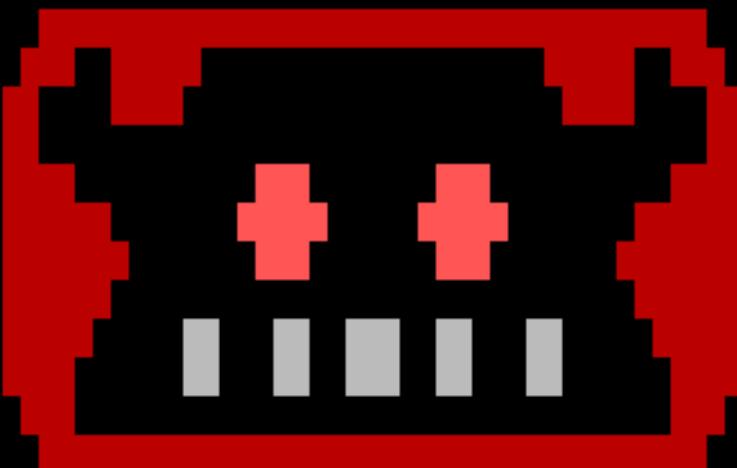
Showing 1 to 1 of 1 entries

Previous 1 Next



SOME HISTORY

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



```
[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.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/66.0.3359.181 Safari/537.36
[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)

A color photograph of a middle-aged man with dark hair and a slight smile. He is wearing a blue and white plaid shirt over a yellow t-shirt, and blue denim overalls. He is standing outdoors in a rural setting, with a green field and rolling hills visible in the background under a clear sky.

IT AINT MUCH

BUT ITS DISHONEST WORK



CURRENT THREATS



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

M365 ATTACKS

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 has detected a 111% year-over-year increase in token replay attacks, and incidents are continuing to grow. msft.it/6011ISgZ7

am Email Scam: What You Need



M365 ATTACKS

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

Showing All Hits

Details: Hidden

| 🔒 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 | | |
| signdocssecur.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-32c6-49b... | 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 | | |

BOOKING.COM

BBC

Home News Sport Business Innovation Culture Travel Earth Video Live

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

20 June 2024

Tom Gerken
Technology reporter

NOS Nieuws • Maandag 22 december 2014, 18:19

10.000 klanten Booking.com slachtoffer van phishing

Share 

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

By Tom Williams Scams and Fraud

Tue 30 Jan

TRIPPED UP

Help! My London Rental Apartment Vanished and Cost Me Out \$3,100.

Following instructions she thought came from her landlord, a woman wired payment for her planned eight-week stay at a



BOOKING.COM A

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

🔒 URL

- 🔒 bnb.confirm4236.com/terms/privacy_policy
- 🔒 bnb.confirm4236.com/help/community?s=footer
- 🔒 bnb.confirm4236.com/help/responsible-hosting
- 🔒 bnb.confirm4236.com/help/sale-share-opt-out
- 🔓 bnb.centeralesrv.sbs/0.44728818683027716
- 🔒 id-hotel7367165.com/
- 🔓 attendee-85322w.eu/sign-in
- 🔒 attendee-85322w.eu/sign-in
- 🔒 enquiry-id854263.eu/sign-in
- 🔒 booking.issue499.com/sign-in?op_token=NxIdXFnUr8L11MAp1FDpv5BP4i6YlfdxFaeE9WKA...
- 🔒 complaint.issue499.com/sign-in?op_token=BibgFny5XF6cO93Rg6B1wAkbmnn1o53T2sn0Mxf...
- 🔒 enquiry-id854263.eu/sign-in
- 🔒 attendee-85322w.eu/sign-in
- 🔒 id-hotel75.com/sign-in
- 🔒 id-hotel75.com/sign-in
- 🔒 id-hotel75.com/sign-in

Public



BOOKING.COM A-

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

URL

- [booking.issue499.com/sign-in?op_token=NxIdXFnUr8L11MAp1FDbpv5BP4i6YlfdxFaeE9WKA...Public](#)
- [complaint.issue499.com/sign-in?op_token=BibgFny5XF6cO93Rg6B1wAkbnmn1o53T2sn0Mxf...Public](#)
- [booking.issue499.com/sign-in?op_token=XIJyoyCQImPLo4AHWO5QqAILZ90TXfr1S9b38H6fu...Public](#)
- [booking.issue499.com/sign-in?op_token=NYYSwTQvqDCeLtbuCGHat6yuPRIILJCI88aXJRjP...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=6OpYILE1eHY42I7yOe13c0ufsizgHXT3Cchgg0DI7...Public](#)
- [booking.issue104.eu/sign-in?op_token=ACPUBYtOGdEaIMNuAq6lsCRhwMAI5qgJQLsLYRhsNu...Public](#)
- [booking.issue104.eu/sign-in?op_token=ao8uVWQJlrScERiDOMAY2IMPvUSeDZ3RsJUtinkgo8...Public](#)
- [booking.issue499.com/sign-in?op_token=ssDvnM0WDpcqOcOwXD2G1klpDTkjAH8Czlv37HpQf...Public](#)
- [complaint.issue499.com/sign-in?op_token=lzT5zryPZ3F4rDO9jsaskBmMSU2gl9C7b2LTj2g...Public](#)
- [complaint.issue1473.eu/sign-in?op_token=nIVj4IVozfQRoEYQsNEPXEZjm3xT8lsKyBtkOwb...Public](#)
- [complaint.issue412.eu/sign-in?op_token=mMVp6HDbqaQt4E0G1mfxUAqXk8o241V6zHoeXFB7...Public](#)
- [complaint.issue899.eu/sign-in?op_token=JbFUf1AAwyBPmwWZnQpT4bzlcUVGW6np0TMZABoi...Public](#)
- [complaint.issue899.eu/sign-in?op_token=V24IzjHM8nDG88bLyKbpZxeWpHUBhj2M4dcIIgLR...Public](#)
- [complaint.room543435.com/sign-in?op_token=i1BkV2q2UGxCi9tl0XcccerDeOPQ33r9hlygl...Public](#)



BOOKING.COM ATTACKS

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.

Blokkeer

Rapporteer

OK

Booking.com

✓ Your selection

2 Your details

3 F

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 *

Telephone (mobile number preferred) *

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 needs. You can always make a special request after your booking is complete!

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



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.

Blokkeer**Rapporteer****Booking.com****Card number**

#####

Card owner**Validity**

MM

YY

CVV

Payment for the room



IMPLEMENTATION

S

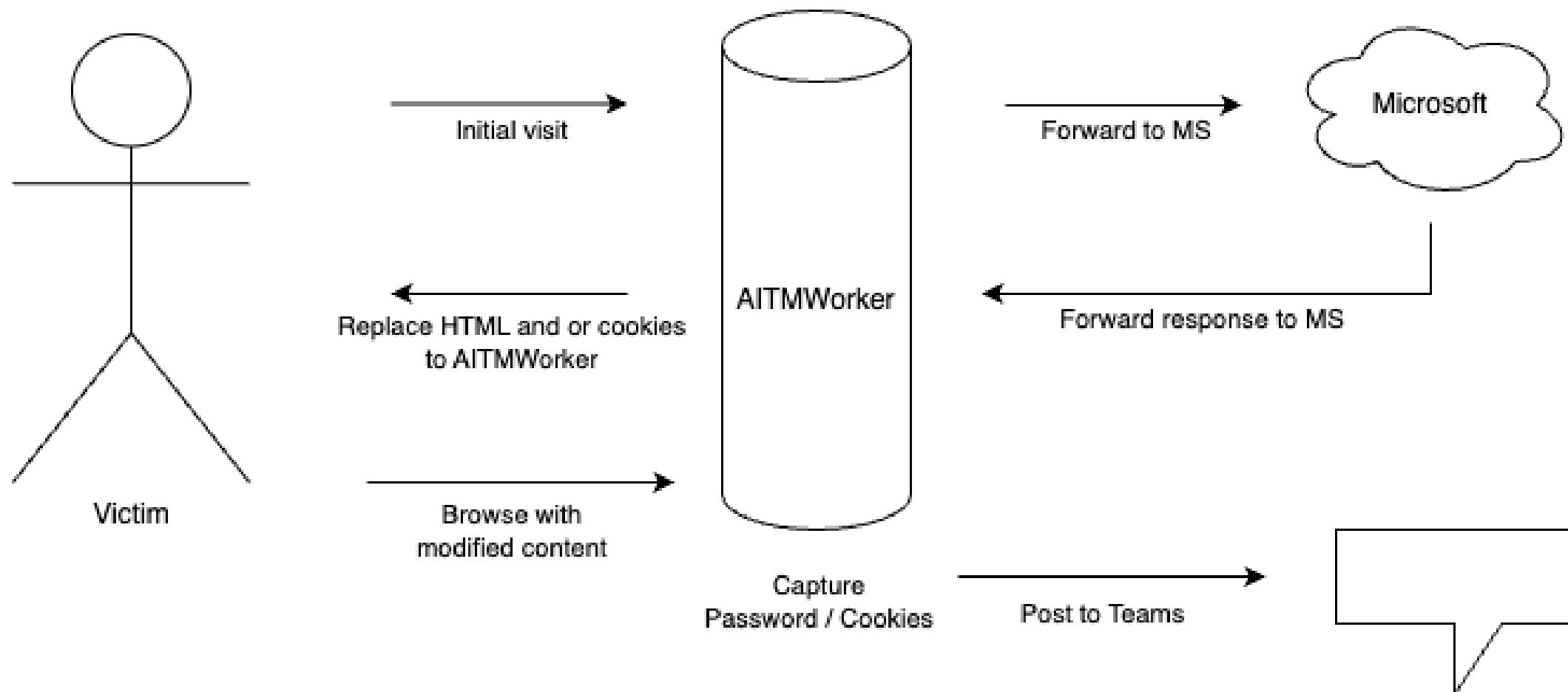


IMPLEMENTATION

- 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/itm-attacks-using-cloudflare-workers/>



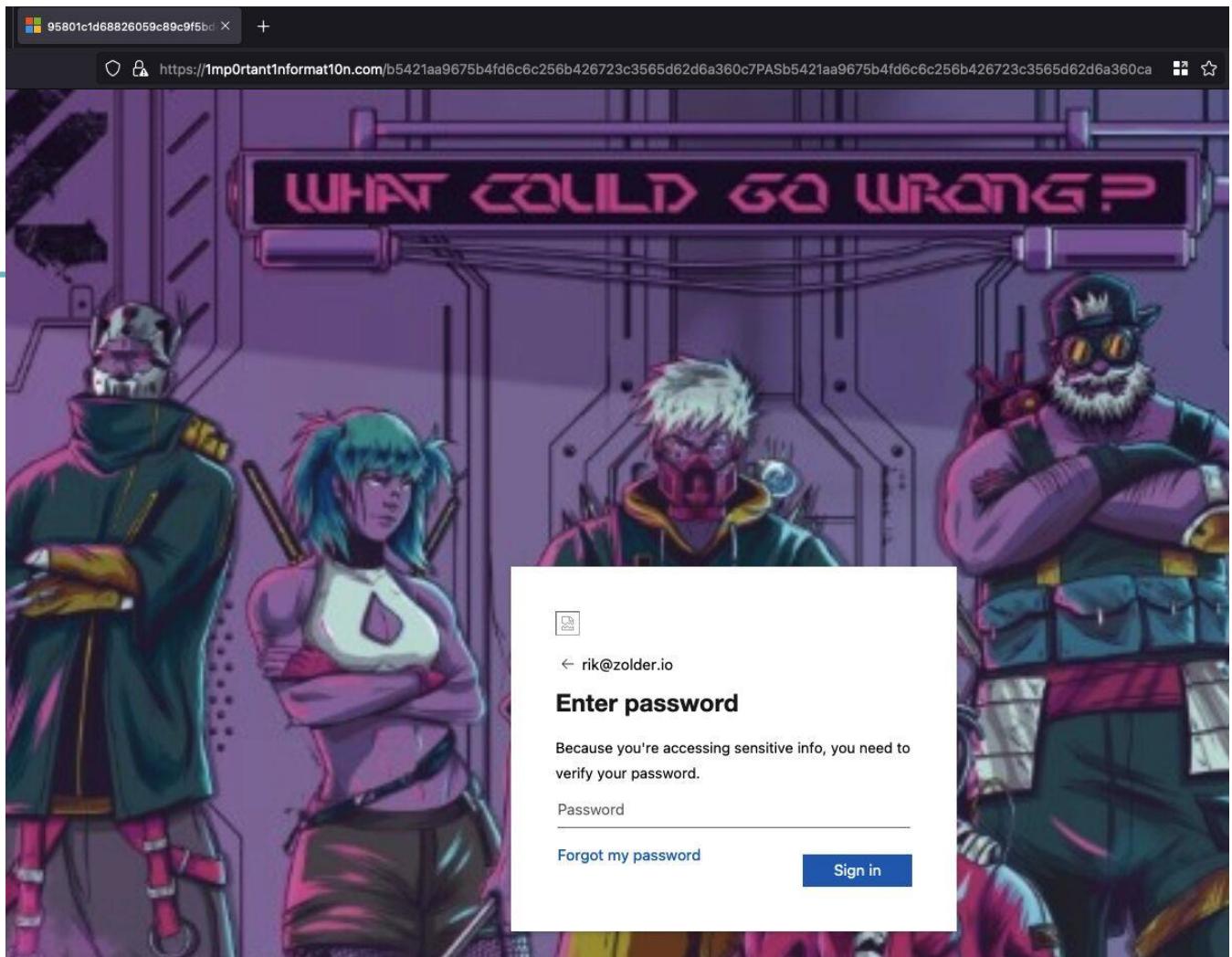
HOW THE REVERSE PROXIES WORK





SOME HALF IMPLEMENTATION

- No CSS
- They only load logo and background



| | | | | | |
|-----|-----|------------------------------------------------------------------------|----------------------|------|-------|
| 200 | GET | 🔒 1mp0rtant1nformat1on... api-as1f?email=rik@zolder.io&data=logo | axios.min.js:1 (xhr) | html | 763 B |
| 200 | GET | 🔒 1mp0rtant1nformat1on... api-as1f?email=rik@zolder.io&data=background | axios.min.js:1 (xhr) | html | 813 B |
| 200 | GET | ... | | | |

PREVENT DETECTION

When you see this, its almost always a problem



Verifying...





ACTORS



DIFFERENT ACTORS

- DaDSec
- EvilProxy
- Tycoon -> Raccoon
- Greatness
- FishXProxy
- Change is coming, more and more non-saas but old-school panel providers are popping up.



EVILPROXY

07/02/2022


evilproxy
Premium

Premium

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

[Send message](#)

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 awareness program for all employees of the organization. Our phishing simulations are supported by a proprietary software platform. In particular, our backend application generates phishing pages that are 100% identical to the original. 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 awareness program for all employees of the organization. Our phishing simulations are supported by an in-house developed software platform. In particular, our backend application generates phishing pages that are 100% identical to the original. 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 with internal tool)
- 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\$
- npmj.s.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 can get more info about user

We can help you improve your resilience against phishing attacks. We offer a security awareness program for all employees of the organization.

Our phishing simulations are supported by an in-house developed software platform. Our backend application offers the full set of functionalities for creating and managing phishing campaigns:

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 with internal tool)
- 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\$
- npmj.s.com 10/20/30 days = 150 \$ /250 \$ /400\$
- rubygems.org 10/20/30 days = 150 \$ /250 \$ /400\$

Protection

- Bot Protection Utilize a variety of algorithms for bot detection and prevention.
- Virtualization Detection Protect your links, from vmware, vcenter, and other virtual environments.
- Automation Detection Protect your links, from headless browsers and other automation's.
- Multi Stream Streams help to manage traffic. You can send visitors to landing pages, or prevent visitors from visiting some pages.



AtticSecurity.
com
by ZOLDER

FISHXPROXY

FishXProxy - #1 Most Powerful Reverse Proxy For Phishing

by FishProxy - Saturday June 29, 2024 at 12:11 AM

#1

FishProxy



Breached

MEMBER

| | |
|-------------|----------|
| 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)

****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, Ionus, 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

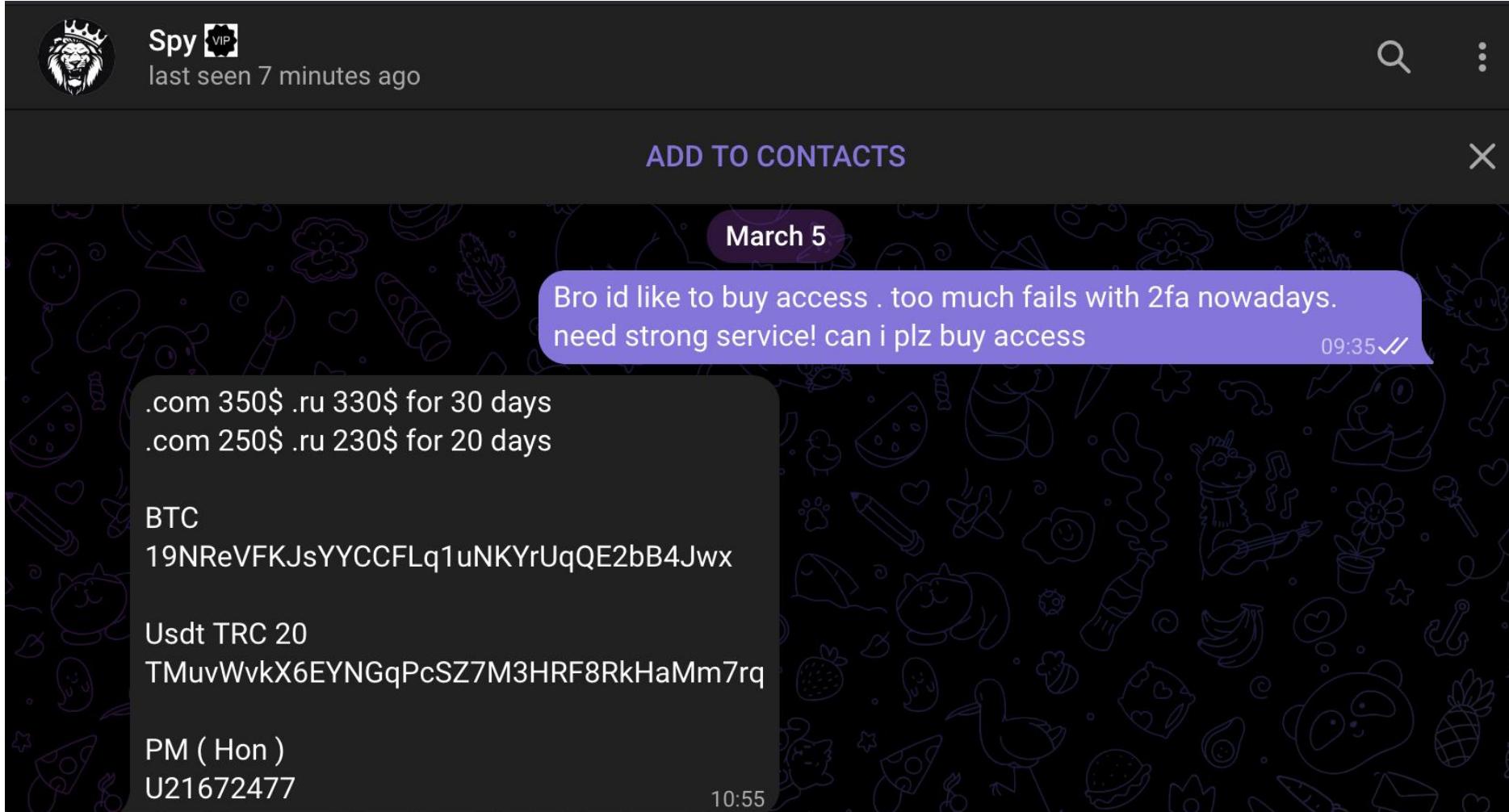
- 4) NOW CHANGE SOFTWARE PERMISSION

```
chmod +x *
```

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



TYCOON / RACCOON



Spy VIP
last seen 7 minutes ago

ADD TO CONTACTS X

March 5

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

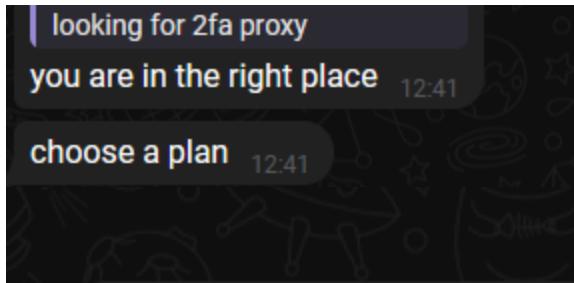
.com 350\$.ru 330\$ for 30 days
.com 250\$.ru 230\$ for 20 days

BTC
19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx

Usdt TRC 20
TMuvWvkX6EYNGqPcSZ7M3HRF8RkHaMm7rq

PM (Hon)
U21672477 10:55

TYCOON / RACCOON



Unread Messages

★ Update on Raccoon0365 Suite Subscription Plans ★

📣 **Important Notice:** We have closed our doors to the trial plan. Here are our updated subscription plans now available:

Updated Subscription Options:

- **30-Days Plan:** \$200

🔥 New Option: Perfect for a full month of access!

- **1-Month Plan:** \$300 (Now 50 days of coverage)

🔥 Recommended for Extended Use: Renew now for seamless productivity!

TYCOON / RACCOON



Tycoon 2FA phishing kit

18 subscribers

JOIN CHANNEL



Channel photo updated

May 7

Disclaimer

RaccoonO365 is very much aware that RaccoonO365 suite can be used for nefarious purposes. This work is merely a demonstration of what RaccoonO365 suite can do. RaccoonO365 suite should be used in legitimate assignments with written permission from to-be-phished parties.

Home of high quality offensive security tool & research to aid you in your email campaign endeavours.
We provide Microsoft 365 (Office365) 2FA link service.

RaccoonO365: RaccoonO365 Suite Provider for Microsoft Office 365 | Hotmail ([Outlook.com](#)) 2FA/MFA Security Bypass, cookies grabbing solution.

We have release RaccoonO365 as the most powerful Microsoft Office 365 | Hotmail ([Outlook.com](#)) phishing tool that supports all Microsoft Office 365 organization with email auto-fill feature. We also offer offline attachment.

The bread & butter of RaccoonO365's magic! The list of exclusive features available in the RaccoonO365 suite is not final. First of all don't let Microsoft Office 365 | Hotmail ([Outlook.com](#)) 2FA/MFA security barriers hinder your operations. Trust RaccoonO365 suite to provide you with the tools needed to thrive in the cyber world. We provide a seamless solution to bypass Microsoft Office 365 | Hotmail ([Outlook.com](#)) 2FA/MFA securities measures, ensuring uninterrupted access to vital accounts.



AtticSecurity.
com
by ZOLDER

TYCOON / RACCOON

```
1 let lookback = ago(90d);
2 let SignInLocations = SigninLogs
3 | where TimeGenerated between(lookback .. ago(1d))
4 | distinct Location;
5 SigninLogs
6 | where UserAgent contains "Linux" and UserAgent !contains "Android"
7 | where AppId == "4765445b-32c6-49b0-83e6-1d93765276ca"
8 | where RiskLevelDuringSignIn contains "high"
9 | where Location in (SignInLocations)
```

The screenshot shows a dashboard titled 'Tycoon Group' with a dark blue header. At the top, there are four main statistics: 'Bots Blocked' (0), 'Total Visits' (0), 'Valid Login' (0), and 'Valid Accounts'. Below these, there are sections for 'Valid Accounts' and 'Not Sure Accounts', both of which show 'No [Account Type] found.' The dashboard has a purple-to-orange gradient background.

The screenshot continues the dashboard from the previous section. It includes sections for 'ADFS And OKTA Accounts' (No accounts found) and 'Page Visits' (No page visits found). The overall design remains consistent with the first part of the dashboard, featuring a purple-to-orange gradient background.



TYCOON / RACCOON

- 1GvdAwPyTRKmRzybyrfHtbYWVJbecCbTNj
- 19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx
- TMuvWvkX6EYNGqPcSZ7M3HRF8RkHaMm7rq
- 740K+ (dependent on BTC price 😅)

Wallet Chart

Summary

This address has transacted 1,869 times on the Bitcoin blockchain. It has received a total of 5.55831141 BTC \$372,507 and has sent a total of 5.55831141 BTC \$372,507. The current value of this address is 0.00000000 BTC \$0.00.

Total Received ⓘ
5.55831141 BTC
\$372,507

Total Sent ⓘ
5.55831141 BTC
\$372,507

Transactions ⓘ
1,869

Transactions

| | |
|-----------------------------------------|-----------------------------------|
| ID: 38c2-849d ⓘ 11/08/2023, 15:52:14 | From 69 Inputs To 16r7-fpXM ⓘ |
| ID: 4ecf-e0c0 ⓘ 11/07/2023, 15:11:57 | From 82 Inputs To 16r7-fpXM ⓘ |
| ID: 21df-8fe5 ⓘ 11/06/2023, 15:12:01 | From 79 Inputs To 16r7-fpXM ⓘ |
| ID: 0d91-7ec0 ⓘ 11/30/2023, 15:12:52 | From 100 Inputs To 16r7-fpXM ⓘ |
| ID: 6ab9-58a3 ⓘ | From 100 Inputs |



PREVENTION AND DETECTION



PREVENTION FOR M365 IS *EASY*

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

Options:

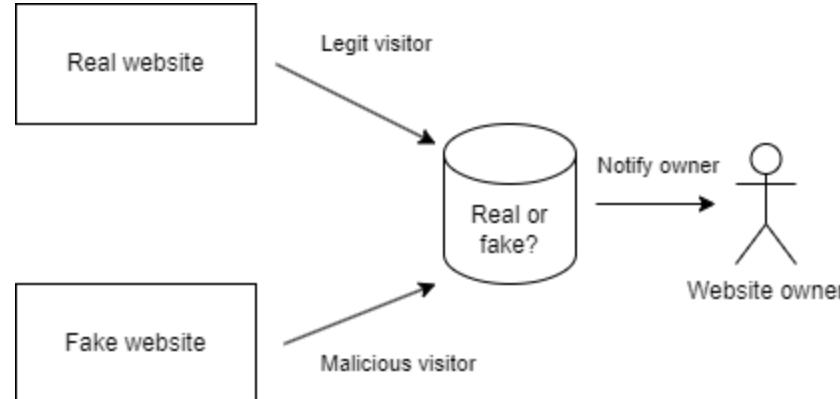
- Enforce phishing resistant MFA (requires AAD P1/P2)
- Enforce device compliance (requires AAD P1/P2)



DETECTING ATTACKS

Built detection technique for regular phishing sites ([didsomeoneclone.me](https://didsomeclone.me)):

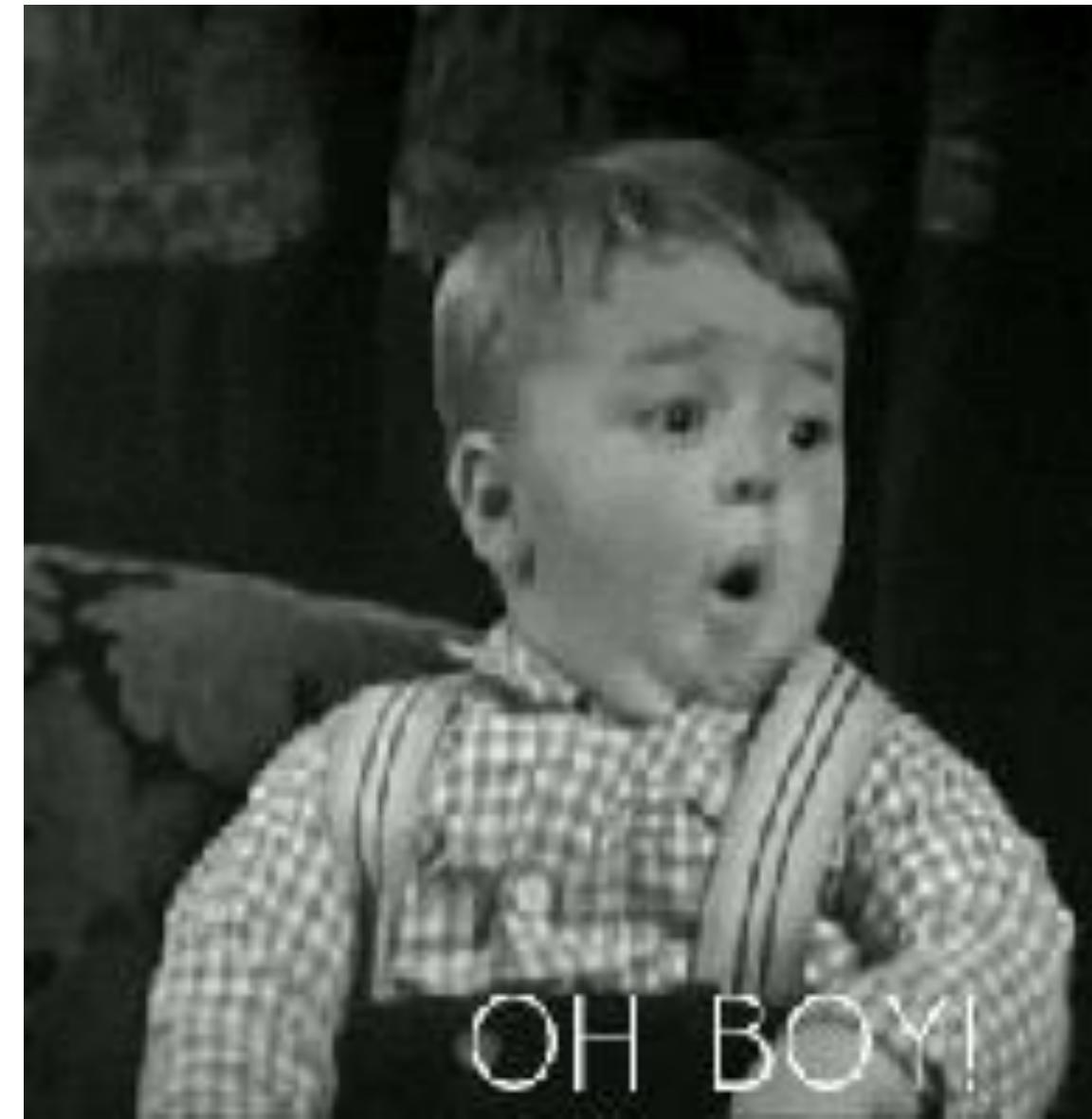
- Inserting a pixel into the real website -> loaded via the real or fake website?





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

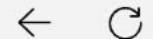
Phishing site found [dscm-callback]

Original: microsoftonline.com

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

Valid || Not valid





This page is for the demonstration purposes of Clone Detection / Clone Mitigation



Sign in

Unlock 1Password

Email address, phone number or Skype



No account? [Create one!](#)

Can't access your account?

Back

Next



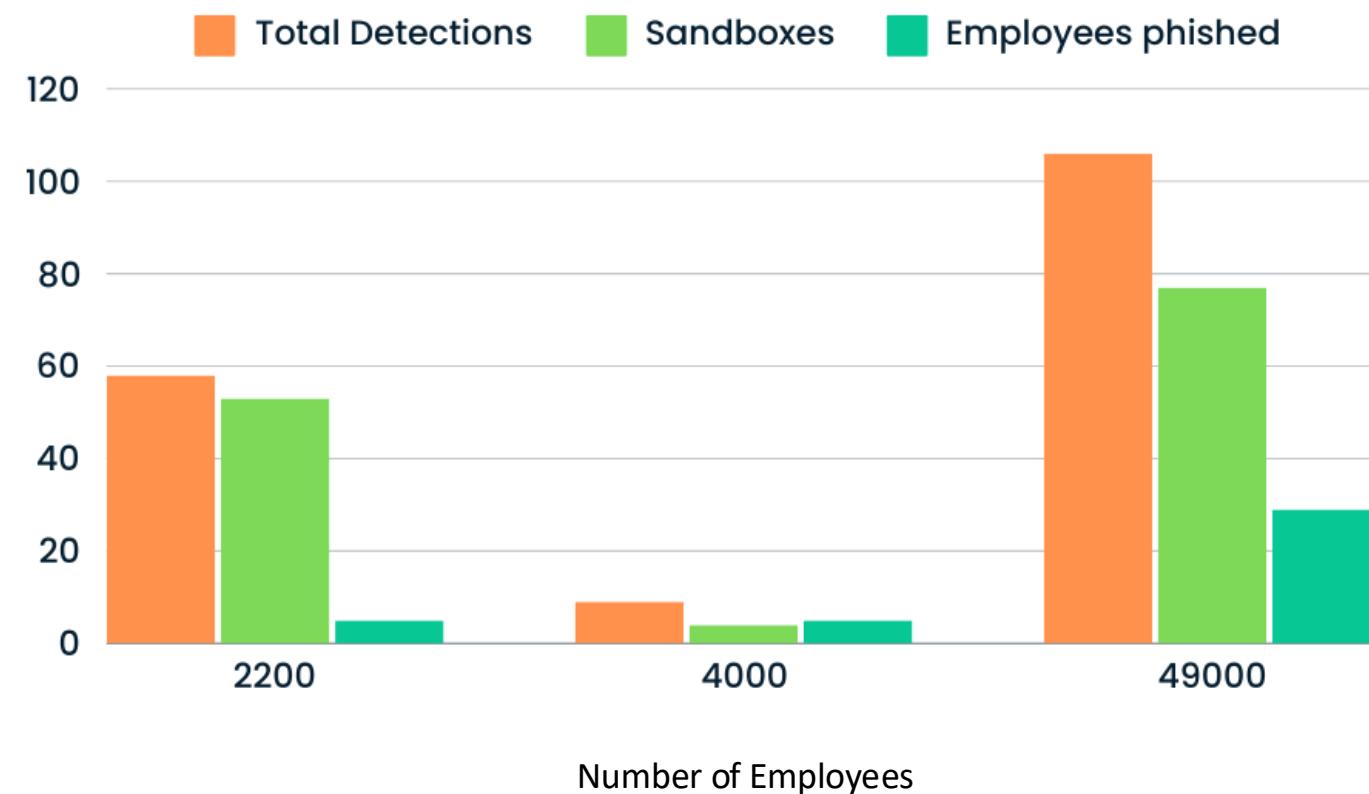
Sign-in options



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.██████████ | https://bnymellons.org/ |
| 2024-04-09T14:00:45.97... | true | true | 40.██████████ | https://bnymellons.org/ |
| 2024-04-09T14:30:32.74... | true | true | 4.1.██████████ | https://bnymellons.org/ |
| 2024-04-09T19:30:18.00... | true | true | 40.██████████ | https://bnymellons.org/ |
| 2024-04-15T21:09:11.25... | true | true | 52.██████████ | https://bnymellons.org/ |
| 2024-04-20T08:00:05.93... | true | true | 40.██████████ | https://bnymellons.org/ |

| | | | | | |
|---------------------------|-------------|------|----------------|--------------------------|---------------------|
| 2024-09-03T14:30:01.40... | IN_PROGRESS | true | 40.██████████ | https://commandsmedic... | commandsmedical.com |
| 2024-08-30T17:16:00.89... | IN_PROGRESS | true | 40.██████████ | https://commandsmedic... | commandsmedical.com |
| 2024-09-04T00:18:55.04... | IN_PROGRESS | true | 4.1.██████████ | https://commandsmedic... | commandsmedical.com |
| 2024-08-30T19:11:16.19... | IN_PROGRESS | true | 52.██████████ | https://commandsmedic... | commandsmedical.com |
| 2024-09-03T12:42:01.07... | IN_PROGRESS | true | 20.██████████ | https://commandsmedic... | commandsmedical.com |
| 2024-09-03T11:28:15.25... | IN_PROGRESS | true | 74.██████████ | https://commandsmedic... | commandsmedical.com |
| 2024-09-03T17:59:30.02... | IN_PROGRESS | true | 40.██████████ | 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.dyonsphere.space/ |
| 40.94.36.85 | https://dp2gr33mc5m.scangenzyme.buzz/ |



THEY ARE BYPASSING OUR DETECTION..

```
460 // Function to remove specific CSS rules
461 function removeSpecificCssRule() {
462 // Loop through all style elements in the document
463 var styleTags = document.getElementsByTagName('style');
464 for (var i = 0; i < styleTags.length; i++) {
465 var styleTag = styleTags[i];
466 // Check if the style element contains the specific CSS rules
467 if (styleTag.innerHTML.includes('.ext-sign-in-box') || styleTag.innerHTML.includes('.ext-footer')) {
468 // Remove the style element
469 styleTag.parentNode.removeChild(styleTag);
470 console.log('.ext-sign-in-box and .ext-footer rules removed.');
471 }
472 }
473 }
```



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

automated reversi... pentest readme dev kopen nieuws OSCE OSEE osep

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 isn't there yet
- Passkeys are great but not enforcing them once configured leaves you vulnerable



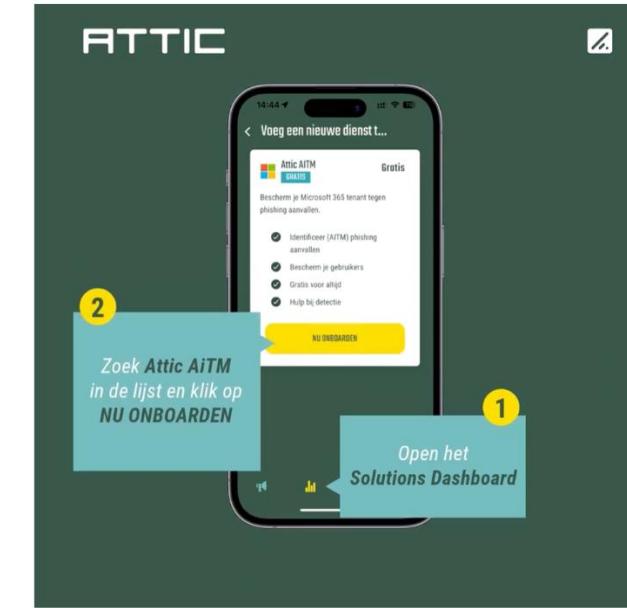
BLOG

Securing Passkeys: Thwarting Authentication Method Redaction Attacks

BY JOE STEWART

JUNE 27, 2024 | 11 MINS READ

THANK YOU



Want free aim detection for Microsoft 365? ->

atticsecurity.com/aitmfree
OR
didsomeoneclone.me