



H2 HC

Diego Piffaretti

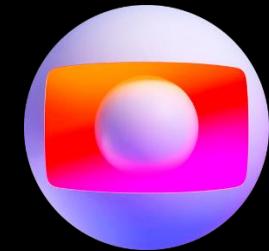
AiTM phishing modern attacks:
I still can bypass your MFA!



Diego Piffaretti (Piffa ou Piffaretti ☺)



- Tech Manager de Cybersegurança na Globo
- Experiência em Red Team (Atualmente lidero o Red Team da Globo)
- Experiência em Cyber Inteligência e CSIRT
- Mestre em Sistemas e Computação pelo IME



 [linkedin.com/in/diegopiffaretti](https://www.linkedin.com/in/diegopiffaretti)

 Mundotecnologico.net

H2
HC



Objetivo

Authentication Bypass and MFA Evasion
AiTM (Adversary-in-the-Middle)

Microsoft 365

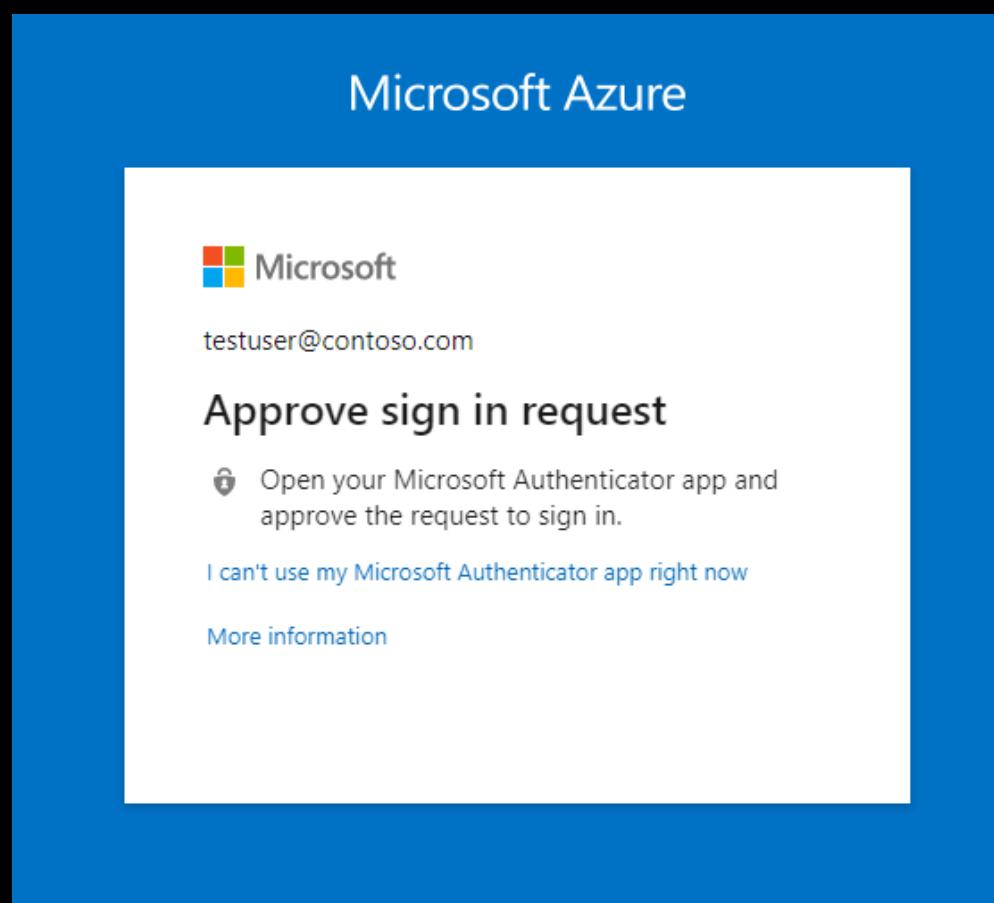
Sign in

Email *

Password * Show

Keep me signed in on this device

Sign In





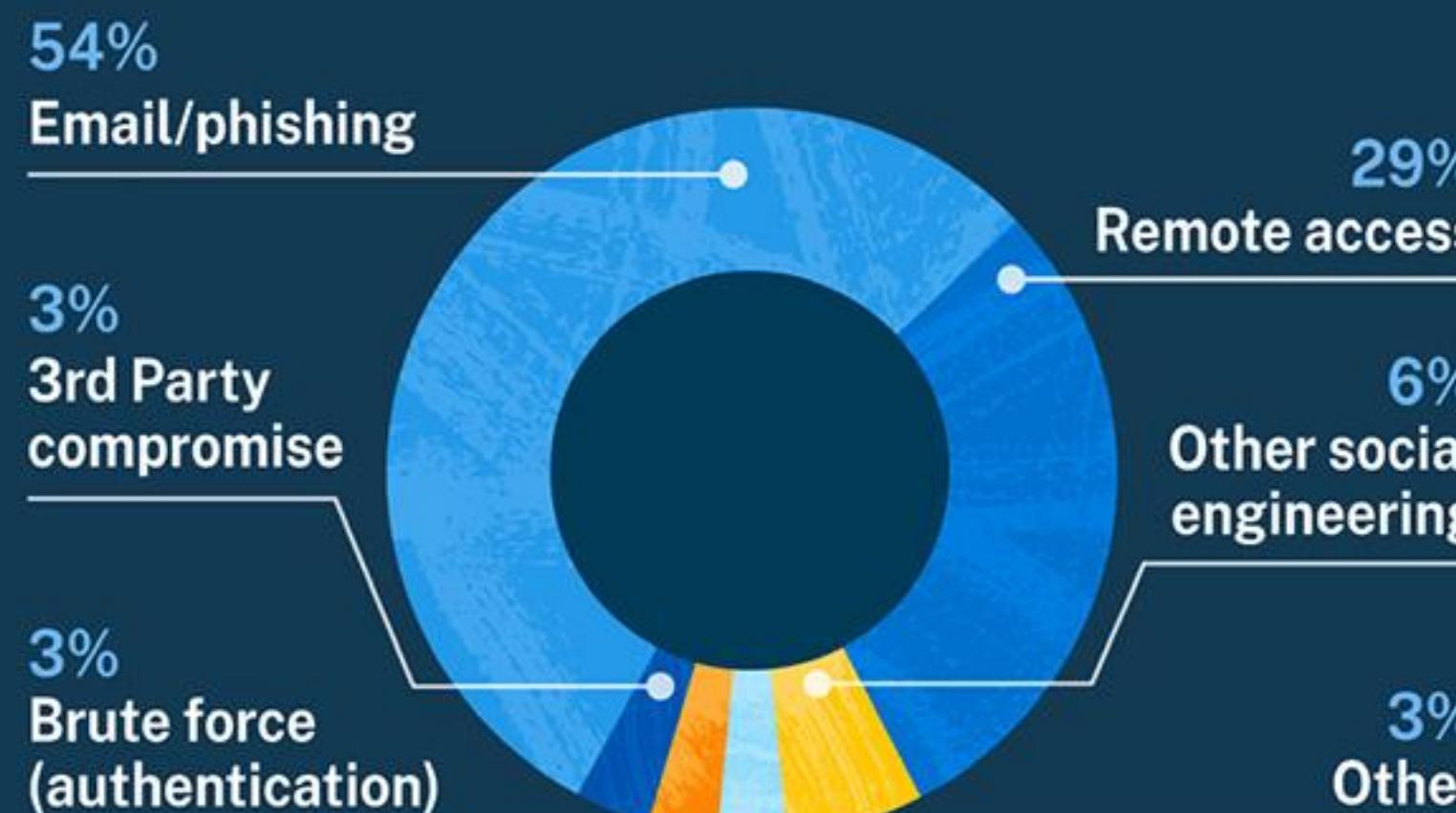
Aplicabilidade

- Campanhas de Red Team Externa
- Campanhas de Engenharia Social



Motivador

Percentage of claims by attack technique



The most common delivery methods and cybersecurity vulnerabilities causing ransomware infections worldwide*



secureframe

*According to MSPs: Source: Statista

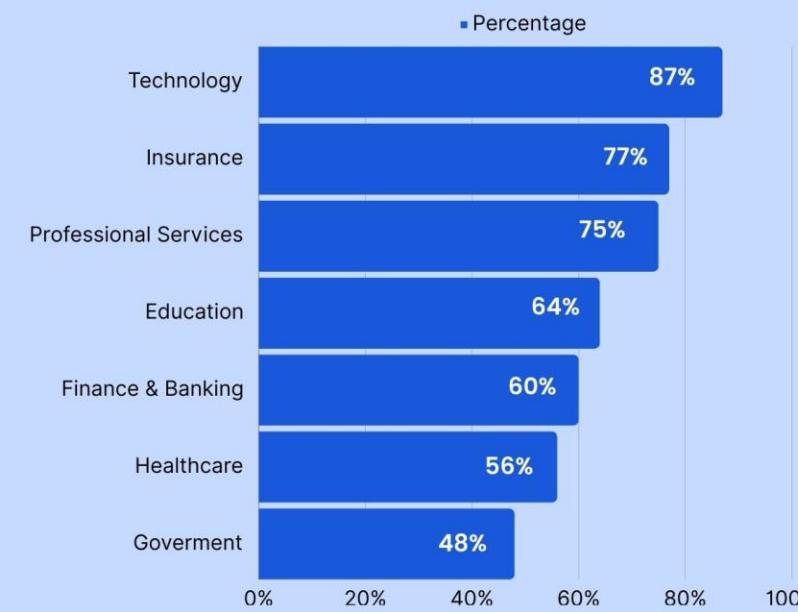


Motivador

MFA Adoption by Industry

Source: Okta

87% of the tech industry has adopted MFA

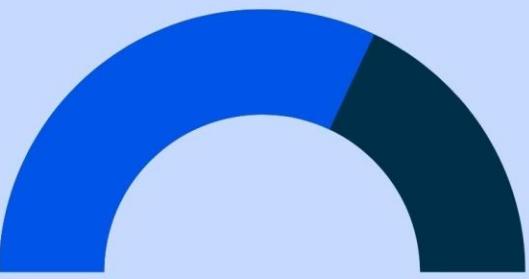


the use of multi-factor authentication

94% of administrators use MFA.



64% of users implement MFA





Motivador

AiT M as a Service: Mamba 2FA

The Rise of Mamba 2FA: A New Threat in Phishing Attacks



US\$ 250 por 30 dias, os clientes recebem acesso a um bot do Telegram que permite que eles gerem links de phishing e anexos HTML sob demanda.

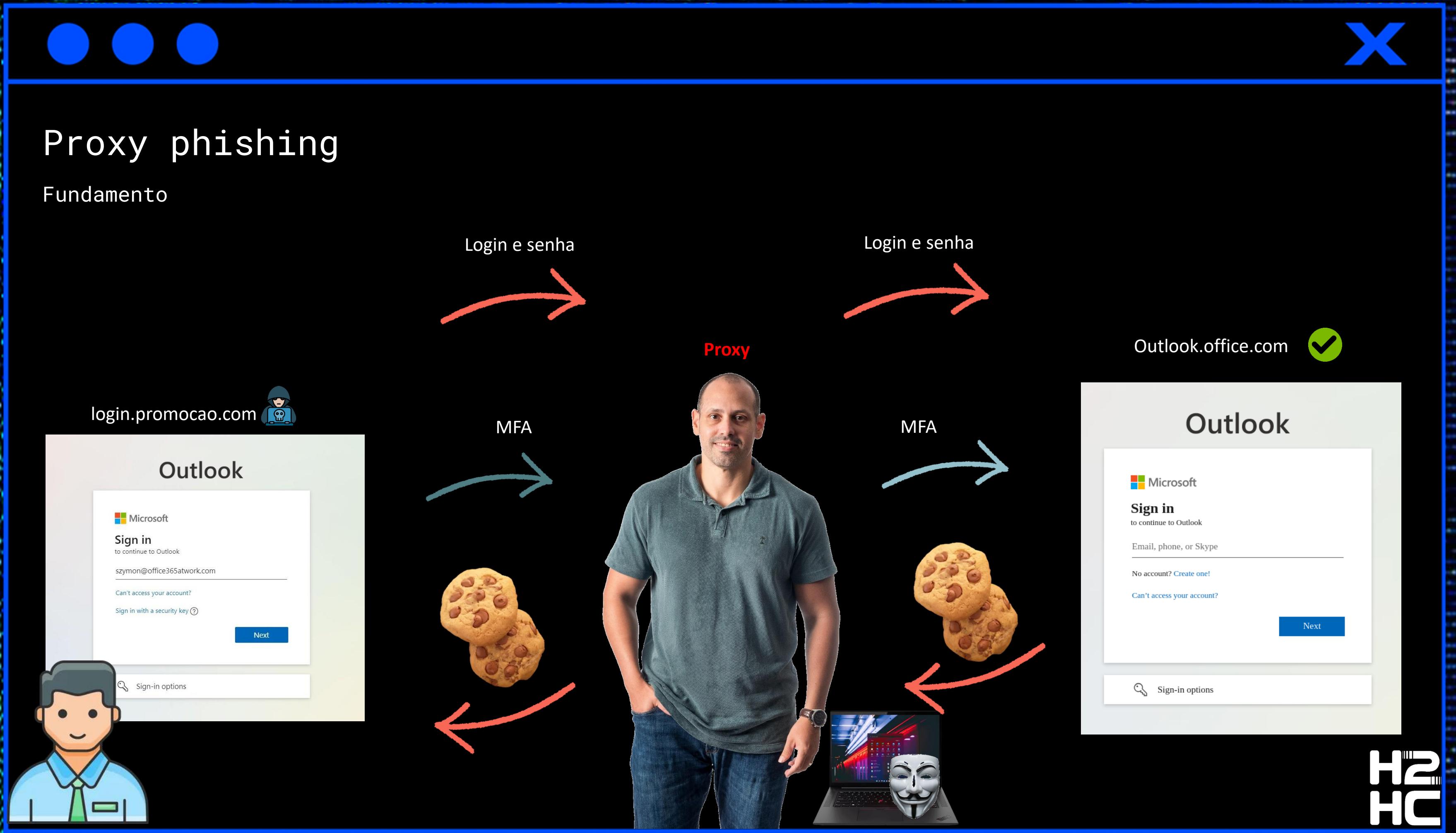


Motivador



Passando aperto na
prática!

H2
HC





Estrutura dos Cookies

- AADSSOTILES - Relacionado ao Azure Active Directory (AAD) Single Sign-On (SSO)
- ai_session - Faz parte do Application Insights, um serviço de monitoramento da Microsoft
- Brcap - Informações sobre o navegador
- Buid - Browser Unique ID
- CCState - Armazena informações relacionadas à configuração regional ou de país do usuário.
- Esctx - Armazena o estado de autenticação
- ESTSAUTH - Relacionado à autenticação no serviço de tokens de segurança da Microsoft (Enterprise Security Token Service - ESTS).
- ESTSAUTHLIGHT - Versão simplificada do cookie ESTSAUTH
- ESTSAUTHPERSISTENT - Também associado ao ESTAUTH, mas com persistência no armazenamento
- Fpc - Federation Proxy Cookie
- MicrosoftApplicationsTelemetryDeviceId - Identificador exclusivo de dispositivo usado para fins de telemetria.
- MSFPC - Cookie de rastreamento da Microsoft
- SignInStateCookie - Relacionado ao estado de login do usuário
- Stsservicecookie - Relacionado ao Security Token Service (STS)
- Wlidperf - Relacionado ao rastreamento de desempenho da conta da Microsoft (Windows Live ID).
- x-ms-gateway-slice - Indica a configuração ou instância do gateway utilizada



Esquenta



LIESA 37 anos

Fundada em 24 de julho de 1984, a Liga Independente das Escolas de Samba do Rio de Janeiro foi criada para defender os interesses das Escolas de Samba do Grupo Especial e coleciona uma série de conquistas ao longo de seus 35 anos, tornando-se modelo nacional.

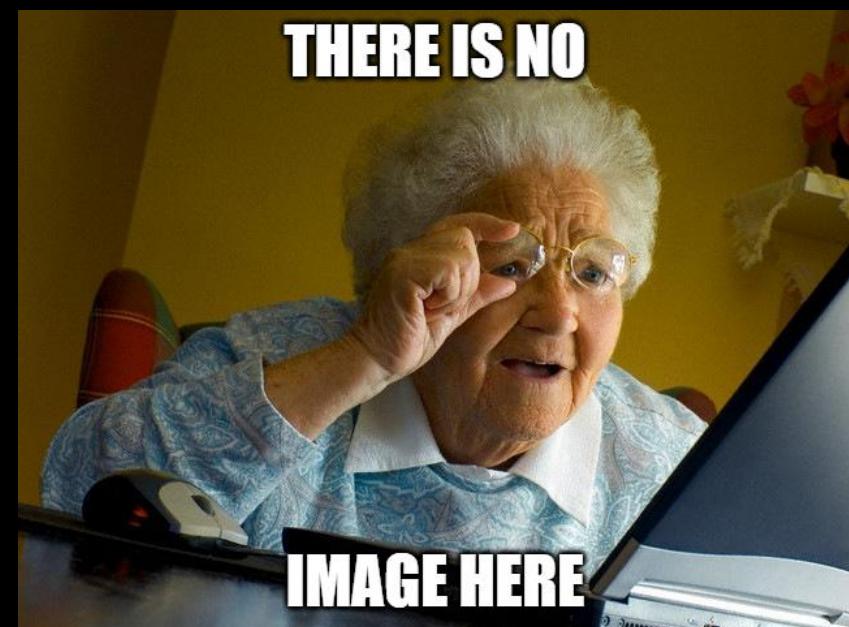
A Liesa em parceria com a Globo irá disponibilizar alguns ingressos para camarotes, boxes especiais e frisas para colaboradores e mais 2 acompanhantes sorteados. Para participar do sorteio, basta preencher uma planilha compartilhada no Sharepoint da Globo com seus dados.

A planilha pode ser acessada [CLICANDO AQUI](#)

- Não é permitida a entrada de crianças com menos de 05 anos de idade
- Proibido levar isopores, garrafas de vidro, sacolas, armas, objetos cortantes, sinalizadores e fogos de artifício.
- É permitido levar até dois vasilhames plásticos de 500 ml com bebida (água, suco, refrigerante ou cerveja) e até dois itens de alimentação (fruta, salgado ou sanduíche).

Elementos :

- Texto
- Hyperlink
- Imagem



H2
HC



LET THE GAMES BEGIN



quickmeme.com

Vamos por partes!

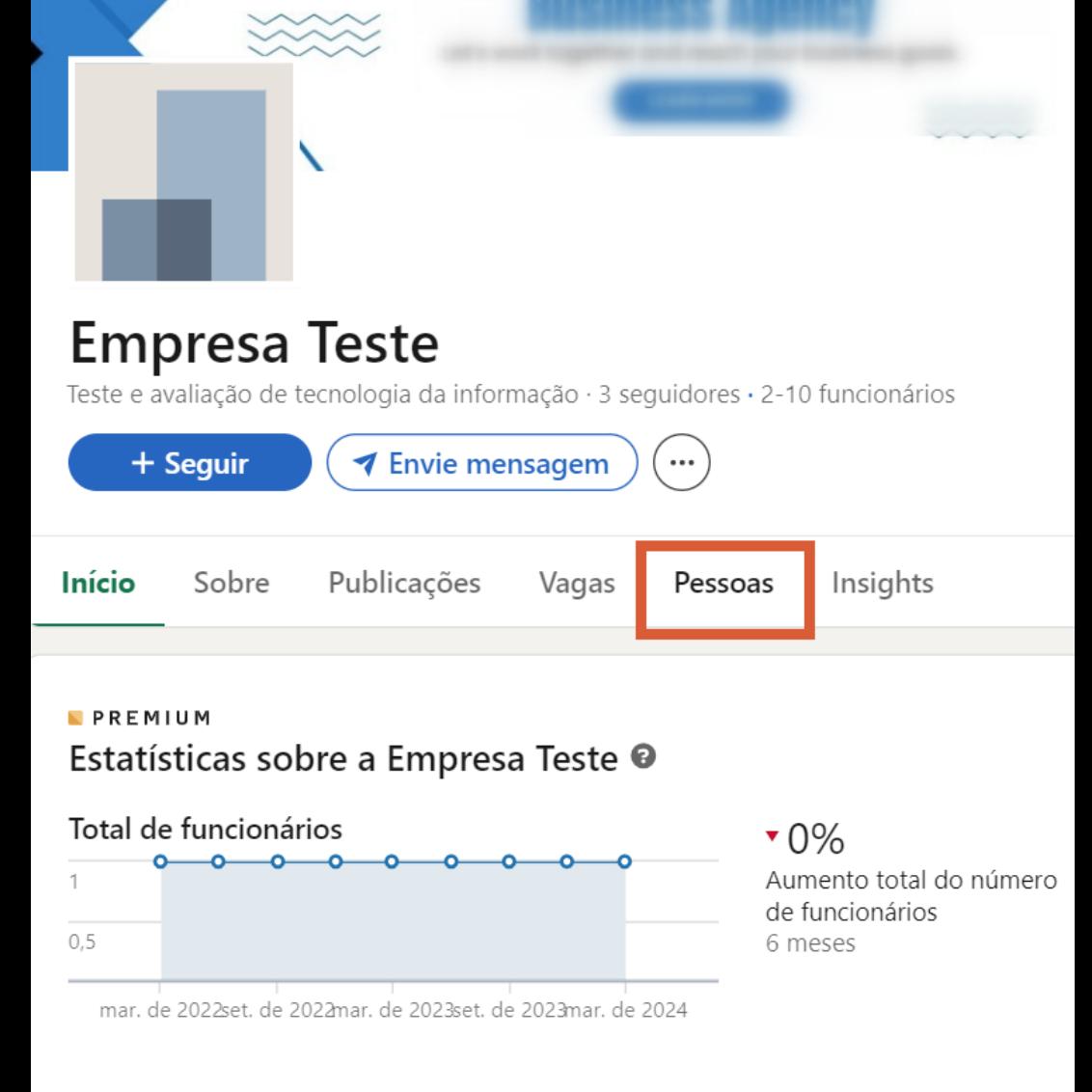
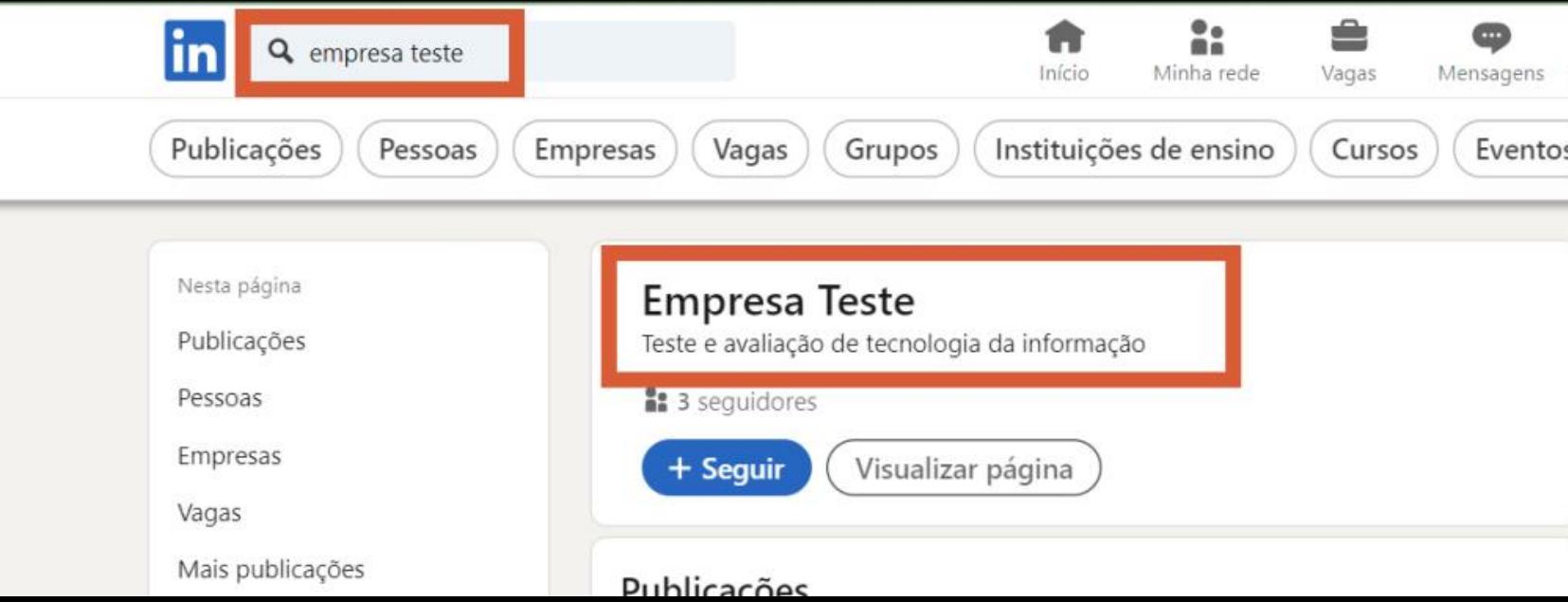
Quais etapas vem antes de
bypassar um MFA?

H2
HC



Enumeração de e-mails

Linkedin Scraping



empresa teste

Início Minha rede Vagas Mensagens

Publicações Pessoas Empresas Vagas Grupos Instituições de ensino Cursos Eventos

Nesta página

Publicações

Pessoas

Empresas

Vagas

Mais publicações

Publicações

Empresa Teste
Teste e avaliação de tecnologia da informação

3 seguidores

+ Seguir Visualizar página

EMPRESA TESTE
Teste e avaliação de tecnologia da informação · 3 seguidores · 2-10 funcionários

+ Seguir Envie mensagem ...

Início Sobre Publicações Vagas Pessoas Insights

PREMIUM

Estatísticas sobre a Empresa Teste

Total de funcionários

1 0,5

mar. de 2022 set. de 2022 mar. de 2023 set. de 2023 mar. de 2024

0%
Aumento total do número de funcionários
6 meses



Enumeração de e-mails

Ferramentas

<https://phonebook.cz>

Phonebook.cz

[Logout](#)

Phonebook lists all domains, email addresses, or URLs for the given input domain. You are searching 165 billion records.

Try: [cia.gov](#), [cnn.com](#), [netflix.com](#), [kremlin.ru](#), [ftx.com](#), [solarwinds.com](#)

Domains
 Email Addresses
 URLs

[atendimento@empresateste.com.br](#)
[contato@empresateste.com.br](#)
[admin@empresateste.com.br](#)
[empresateste@empresateste.com.br](#)
[teste@empresateste.com.br](#)

No more results.

<https://hunter.io>

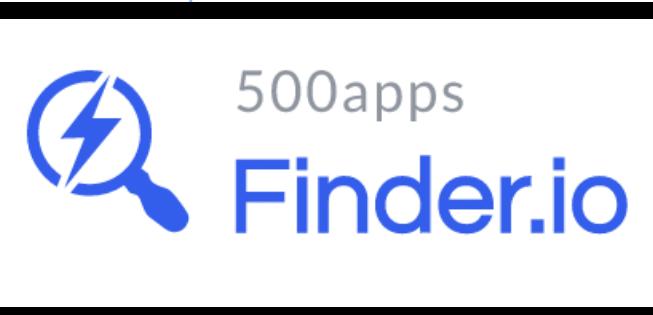
Domain Search [?](#)

Type Department Show only results with

2 results for your search

empresateste@empresateste.c...
74% Verify email
1 source

comercial@empresateste.com.br
10% Verify email
2 sources





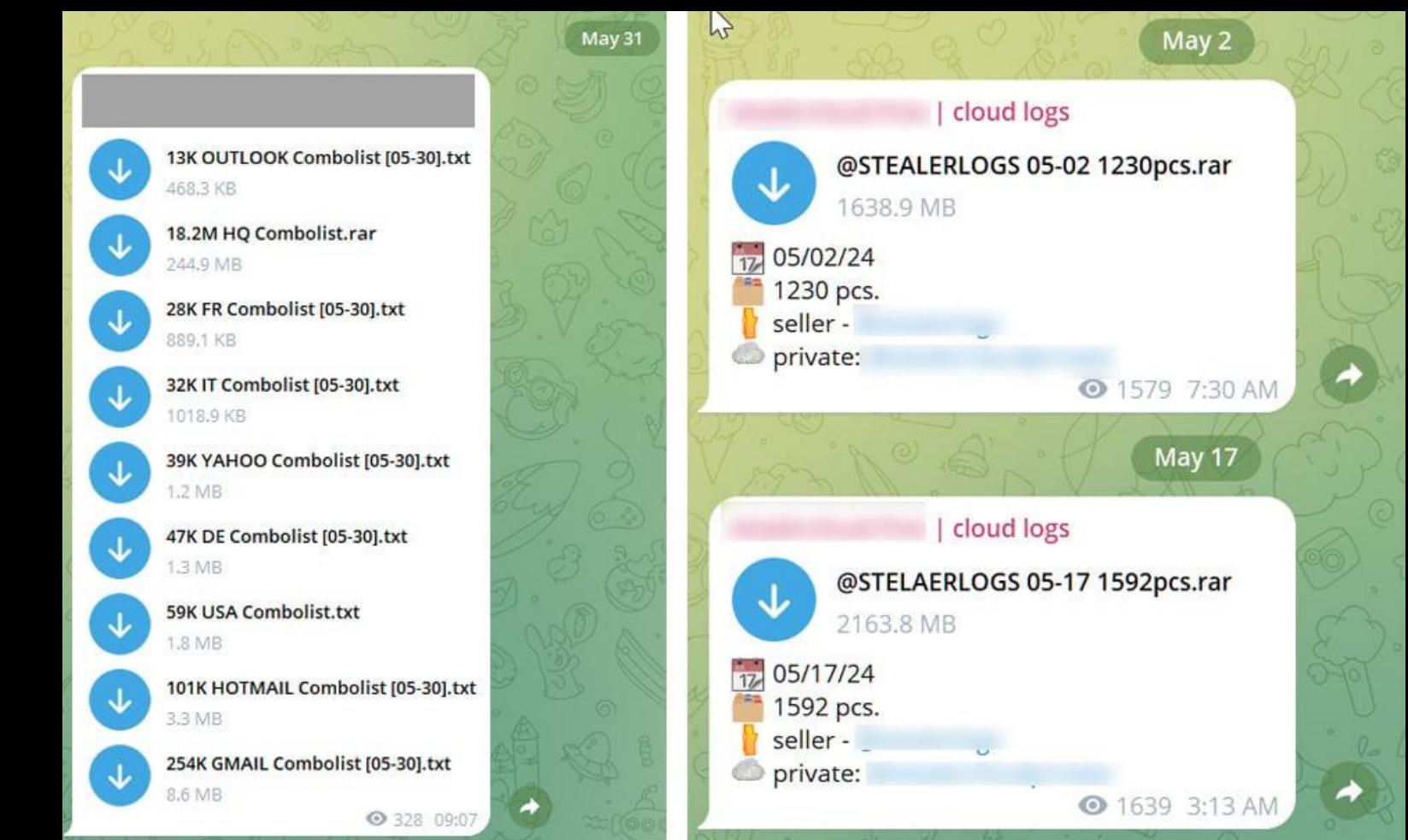
Enumeração de e-mails e credenciais

Ferramentas



BF

Breach Forum



Stealer

H2
HC



Validação de e-mails

Office 365

https://<tenantname>-my.sharepoint.com/personal/<your_user_name>/_layouts/15/onedrive.aspx

Alvo: maria.flores@emprestateste.com.br

Convertendo: maria_flores_empresateste_com_br

Requisição: curl -I https://empresateste-
my.sharepoint.com/personal/maria_flores_empresateste_com_br/_layouts_15_onedrive.aspx



Tool: https://github.com/piffaretti/o365_EmailValidator

Google

pepsi site:sharepoint.com

Todas Imagens Shopping Notícias Vídeos Mais Ferramentas

sharepoint.com
<https://pepsico.sharepoint.com> · Traduzir esta página

<https://pepsico.sharepoint.com/>

Não há nenhuma informação disponível para esta página.
Saiba o motivo



PHISHING

Dominio





DEPOIS DE INSTALAR O KALI



E CRIAR UM E-MAIL FALSO

MR. ROBOT

BYPASS NO ANTISPAM



DO OFFICE 365

E agora?

**H2
HC**



PHISHING

Dominio

- Registrar o domínio o quanto antes (domínios muito recentes geram alertas)
- Anonimizar os seus dados no registro
- Criar entrada SPF (verifica se o servidor de e-mail está autorizado)
- Criar entrada DKIM (confirma a integridade do conteúdo do e-mail)
- Criar entrada DMARC (orienta o que fazer com e-mails que falham)
- Necessário bypass na “Proteção contra usurpação de identidade do domínio”
- Necessário bypass contra “Inteligência contra falsificação”
- Homografia vem sendo detectado

X

Dates	108 days old Created on 2024-02-25 Expires on 2025-02-25 Updated on 2024-03-01
Name Servers	
IP Address	
IP Location	BR - Sao Paulo - Sao Paulo
ASN	BR International Limited, CY (registered Apr 04, 2011)
IP History	4 changes on 4 unique IP addresses over 0 years
Hosting History	3 changes on 3 unique name servers over 0 year

[Whois Record](#) (last updated on 2024-06-13)

```
Domain Name: [REDACTED]
Registry Domain ID: [REDACTED]
Registrar WHOIS Server: [REDACTED]
Registrar URL: [REDACTED]
Updated Date: 2024-03-01T14:14:06.0Z
Creation Date: 2024-02-25T14:10:51.0Z
Registry Expiry Date: 2025-02-25T23:59:59.0Z
Registrar: [REDACTED] operations, UAB
Registrar IANA ID: [REDACTED]
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org)
Registrant State/Province: MA
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: [REDACTED]
Name Server: [REDACTED]
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@[REDACTED]
Registrar Abuse Contact Phone: [REDACTED]
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```



PHISHING

E-mail

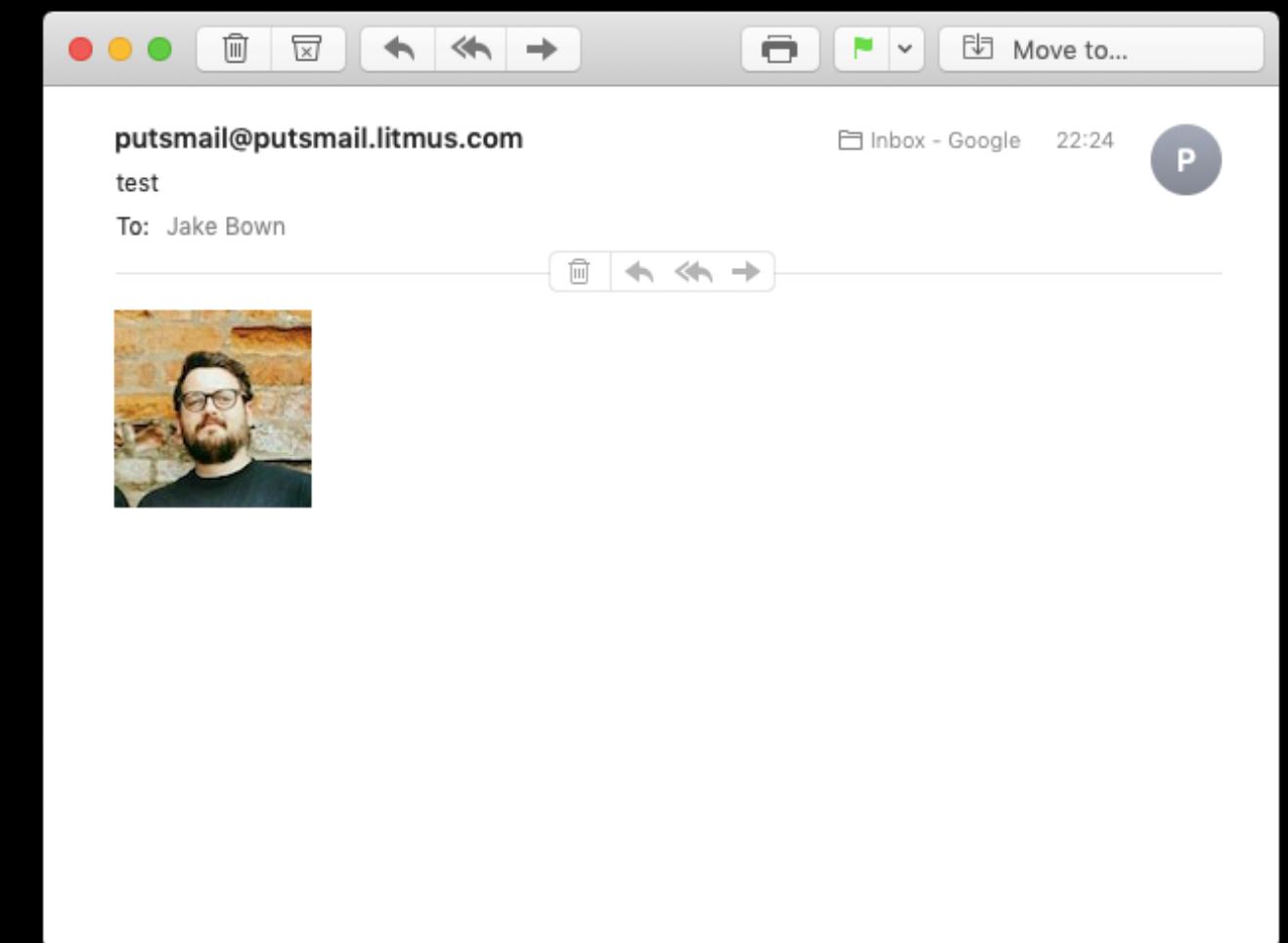
- Necessário bypass na “Proteção contra usurpação de identidade do usuário”
- Necessário bypass contra “Inteligência contra falsificação”
- Necessário bypass conta “Detonation analysis (File and URL)”
- Não usar caracteres incomuns
- Evitar usar técnica de Backscatter (spoof)
- Evitar formulário HTML
- Não usar Javascript ou VBScript
- Evitar idiomas diferentes de PT-BR (Se o alvo for BR) e EN-US
- Não usar hyperlink com final .biz ou .info
- Não enviar e-mail com NDR (notificação de falha na entrega)



PHISHING

E-mail

- Evitar o uso de imagens no e-mail, office 365 bloqueia o carregamento de imagem externa
- Enviar de preferência de 500 em 500 e-mails
- Enviar de remetente gmail.com costuma passar tranquilo
- Se for usar domínio customizado, utilize Mailchimp para disparo ou faça um google workspace trial
- Não enviar anexo
- Se tiver que realmente utilizar imagem, use a técnica de converter imagem em tabela HTML (<https://github.com/jakerb/ImageTable>)





PHISHING

E-mail

- Não usar redirects ou encurtadores comuns como hyperlink (não adianta!). Não usar de maneira alguma bit.ly
- Não passar a URL do phishing pura por e-mail ou teams antes da campanha
- Usar encurtador com ação de usuário para completar redirect (Ex:clique para continuar) ou usar encurtador com bloqueio de região/IP (bloquear IPs da Microsoft e/ou EUA) - short.io ou curtlink.com
- Crie seu próprio redirect, com captcha por exemplo ou “clique aqui” para continuar

HORA DE SUBIR NOSSO

PROXY PHISHING

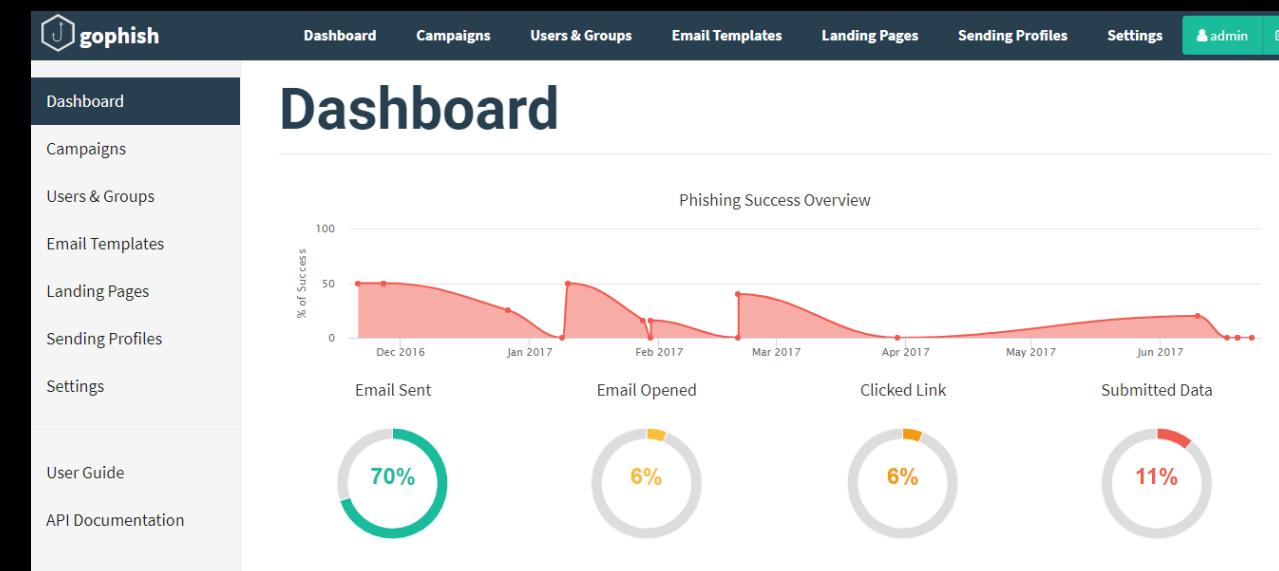


Proxy phishing

Evilginx 3.3



- Repositório oficial: <https://github.com/kgretzky/evilginx2>
- Tem integração com GoPhish



Phishlets (templates): <https://github.com/simplerhacking/Evilginx3-Phishlets>

Documentação bacana que ajuda a instalar: <https://help.evilginx.com/docs/getting-started/building>



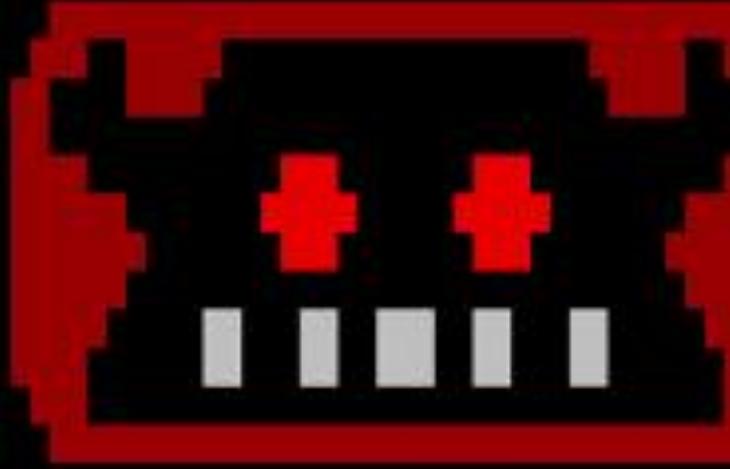
Evilginx

Dicas

- Depois de instalar, editar o arquivo do Linux *resolved.conf* e setar a config: DNSStubListener=no e setar um DNS (8.8.8.8)
- Evilginx está na versão 3 mas o repositório se chama *evilginx2*. 
- Os phishlets (templates de página web falsa) da versão 3 são poucos e não estão funcionando muito bem
- Os phishlets da versão 2 tem muitas opções, mas não funcionam na versão 3, é necessário fazer adaptações para funcionar
- Necessário tirar o header do evilginx para evitar ser pego.
- Bloquear os IPs da Microsoft no evilginx, salve o seguinte arquivo na pasta `~/.evilginx/`:
https://github.com/aalex954/MSFT-IP-Tracker/releases/latest/download/msft_asn_ip_ranges.txt

Documetançao: <https://github.com/An0nUD4Y/Evilginx2-Phishlets>

Evilginx

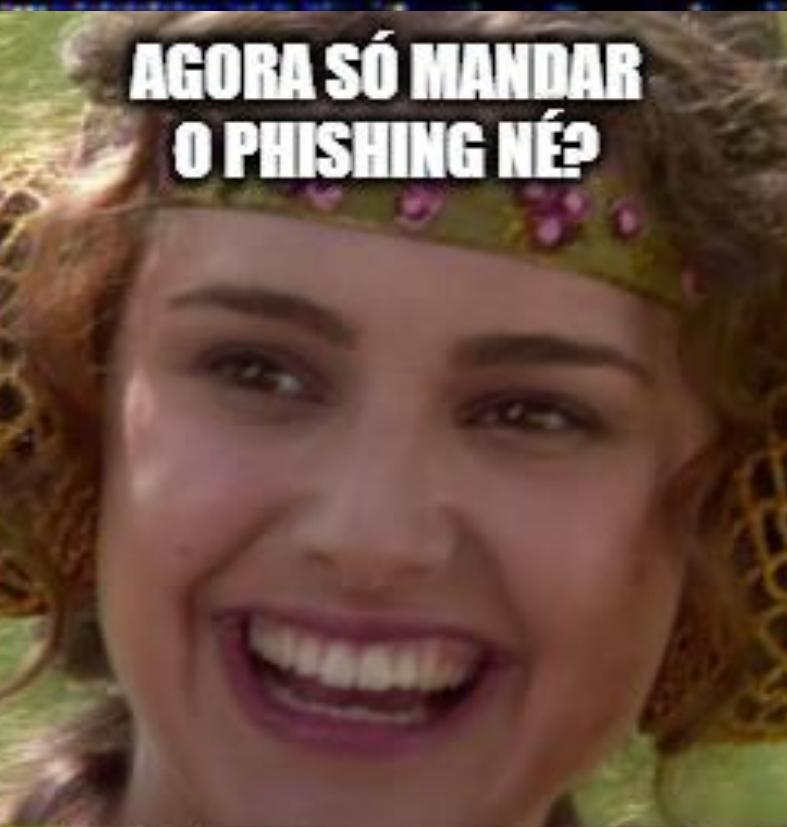


no nginx - pure evil
by Kuba Gretzky (@mrgretzky) version 2.3.3

```
[16:18:50] [inf] debug output enabled
[16:18:50] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[16:18:50] [inf] loading configuration from: /root/.evilginx
[16:18:50] [war] server domain not set! type: config domain <domain>
[16:18:50] [war] server ip not set! type: config ip <ip_address>

+-----+
| phishlet | author | active | status | hostname |
+-----+
| amazon   | @customsync | disabled | available |
| instagram | @prrrrinnee | disabled | available |
| outlook   | @mrgretzky | disabled | available |
| reddit    | @customsync | disabled | available |
| twitter-mobile | @white_fi | disabled | available |
| facebook  | @mrgretzky | disabled | available |
| o365      | @jamescullum | disabled | available |
| okta     | @mikesiegel | disabled | available |
| protonmail | @jamescullum | disabled | available |
| twitter   | @white_fi | disabled | available |
| linkedin  | @mrgretzky | disabled | available |
| wordpress.org | @meitar | disabled | available |
| citrix    | @424f424f | disabled | available |
| github    | @audibleblink | disabled | available |

: config domain example.com
[16:18:56] [inf] server domain set to: example.com
[16:18:56] [war] server ip not set! type: config ip <ip_address>
: config ip 1.2.3.4
[16:19:01] [inf] server IP set to: 1.2.3.4
```



AGORA SÓ MANDAR
O PHISHING NÉ?

VAI FUNCIONAR NÉ?





Evilginx

Blue Team detection



- IP Real exposto
- Facilita bots da Microsoft e outros identificarem a fraude
- Facilita ferramentas de defesa do alvo identificarem a fraude
- Facilita o bloqueio da defesa (IP de VPS)



Evilginx

Google Safe Browsing



Deceptive site ahead

Firefox blocked this page because it may trick you into doing something dangerous like installing software or revealing personal information like passwords or credit cards.

Advisory provided by [Google Safe Browsing](#).

[Go back](#)

[See details](#)

[REDACTED] has been [reported as a deceptive site](#). You can [report a detection problem](#) or [ignore the risk](#) and go to this unsafe site.

Learn more about deceptive sites and phishing at [www.antiphishing.org](#). Learn more about Firefox's Phishing and Malware Protection at [support.mozilla.org](#).



Infra AiTM

VPS + VPN



Como fazer gastando pouco?

 Microsoft Azure

FREE:

750 horas de VMs
USD\$200 em crédito

Ponto positivo:

- Fácil de navegar
- Tem IP BR (SP)

Ponto negativo:



 Google Cloud

FREE:

1 instância da VM e2-micro
USD\$200 em crédito

Ponto positivo:

- Mediano de navegar

Ponto negativo:

- Não tem IP BR



 Amazon Lightsail

FREE:

3 meses grátis (750 horas por mês)

Ponto positivo:

- Fácil de navegar
- Dura mais tempo que os demais

Ponto negativo:

- Não tem IP BR
- Cuidado para lembrar de cancelar a subscrição

 ORACLE CLOUD

Ponto positivo:

- Free eternamente
- Tem IP BR
- Terra de ninguém


QUE SATISFAÇÃO
ASPIRA
GER ifunny.co



Evilginx

Google Safe Browsing Bypass

Configure Super Bot Fight Mode

Definitely automated Definitely automated traffic typically consists of bad bots. Select an action for this traffic.	<input type="button" value="Block"/>
Likely automated Likely automated traffic can include bad bots, along with other traffic. Select an action for this traffic.	<input type="button" value="Challenge"/>
Verified bots Verified bots are unique good bot identities validated by Cloudflare. Select an action for verified bots for this traffic.	<input type="button" value="Allow"/>
Static resource protection Enable if static resources on your application need bot protection. <small>Note: Static resource protection can also result in legitimate traffic being blocked.</small>	<input type="button" value="Off"/>
JavaScript Detections Use lightweight, invisible JavaScript detections to improve Bot Management. Learn more.	<input type="button" value="On"/>

Security

Bots

Identify and mitigate automated traffic to protect your domain from bad bots.

[Bots documentation](#)

Bot Fight Mode Challenge requests that match patterns of known bots, before they access your site. This feature includes JavaScript Detections .	<input checked="" type="checkbox"/>
New AI Scrapers and Crawlers Block bots from scraping your content for AI applications like model training.	<input type="checkbox"/>

Then take action...

Choose action

- Managed Challenge
- Managed Challenge
- Block
- JS Challenge
- Skip
- Interactive Challenge



The screenshot shows a browser window with a blue header bar containing three blue dots and a large blue 'X'. The main content area has a black background with white text. At the top left, it says "Evilginx" and "Google Safe Browsing Bypass". Below this, there's a large empty space with three small black dots at the top center. In the middle, the text "Checking your browser before accessing [REDACTED]" is displayed, followed by "This process is automatic. Your browser will redirect to your requested content shortly." and "Please allow up to 5 seconds...". At the bottom, it says "DDoS protection by Cloudflare" and "Ray ID: 552a703fdd91c6fc". To the right of the main content, there's a vertical sidebar with a "Managed (recommended)" section, a "# Light mode" section with a "Verify you are human" checkbox, a "Verifying..." section with a green loading icon, and a "Success!" section with a green checkmark icon.

Evilginx

Google Safe Browsing Bypass

Checking your browser before accessing [REDACTED].

This process is automatic. Your browser will redirect to your requested content shortly.

Please allow up to 5 seconds...

DDoS protection by Cloudflare

Ray ID: 552a703fdd91c6fc

Managed (recommended)

Cloudflare will use information from the visitor to decide if an interactive challenge should be used. If we show an interaction, the user will be prompted to check a box (no images or text to decipher).

Light mode

Verify you are human CLOUDFLARE Privacy • Terms

Verifying... CLOUDFLARE Privacy • Terms

Success! CLOUDFLARE Privacy • Terms

H2
HC



Evilginx

Bypass Other Security measures



CLOUDFLARE®

IP Firewall

Web Application Firewall

Access Rules

Firewall rules based on IP address, IP address range, or two letter country code. (Country codes found [here](#)).

Search Access Rules

Enter an IP, IP range, or two letter country code.

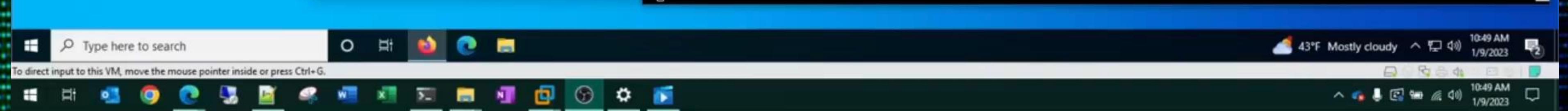
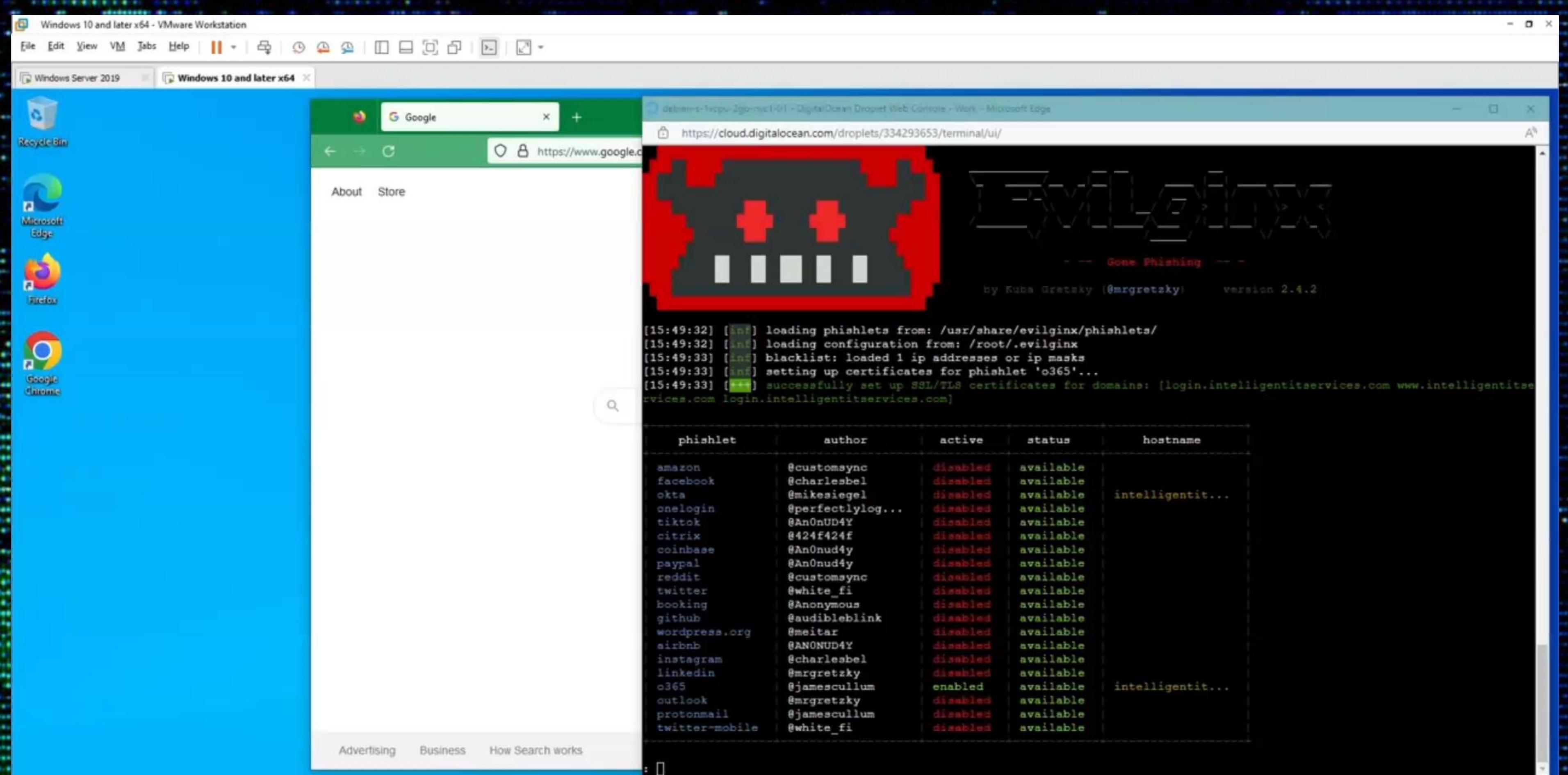
Block

This website

Add a note

Add

H2
HC



DEFESA





Ao perceber um ataque, o que fazer?

- Revogar sessão
- Resetar senha
- Analisar os logs de entrada na Azure/GCP, identificar IP atacante. Bloquear IP do atacante
- Bloquear URL
- Rastrear quem mais recebeu o phishing. Atuar em outros usuários que tenham acessado
- Deletar mensagem das caixas de e-mail.
- Plano de comunicação
- Na dúvida, revogar sessão e bloquear o usuário até uma melhor investigação



Ao perceber um ataque, o que fazer?

Microsoft Azure

Página inicial > Visão geral >

Diego Piffaretti Usuário

Pesquisar

Visão geral

Logs de auditoria

Logs de entrada

Diagnosticar e resolver problemas

Gerenciar

- Atributos de segurança personalizados
- Funções atribuídas
- Unidades administrativas
- Grupos
- Aplicativos
- Licenças
- Dispositivos
- Atribuições de função do Azure

Visão geral Monitoramento Propriedades

Redefinir a senha Revogar sessões Gerenciar a exibição Algum comentário?

Informações básicas

Nome UPN: Diego Piffaretti

ID de objeto: 93e82fa5-c0af-42b4-bf9d-3e147075d67c

Data e hora de criação:

Tipo de usuário: Membro

Identidades: onmicrosoft.com

Meu Feed

Associações de grupo

Aplicativos

Funções atribuídas

Licenças atribuídas

Revogar sessões

A red arrow points from the text "Ao perceber um ataque, o que fazer?" to the "Revogar sessões" button.

Ao perceber um ataque, o que fazer?

Diego Piffaretti | Logs de entrada

Usuário

Pesquisar

Baixar

Configurações de Exportação de Dados

Solucionar problemas

Atualizar

Colunas

Tem comentários?

Visão geral

Logs de auditoria

Logs de entrada

Diagnosticar e resolver problemas

Gerenciar

- Atributos de segurança personalizados
- Funções atribuídas
- Unidades administrativas
- Grupos
- Aplicativos
- Licenças
- Dispositivos
- Atribuições de função do Azure
- Métodos de autenticação

Solução de Problemas e Suporte

Deseja voltar para a experiência padrão de entradas? Clique aqui para sair da versão prévia.

Data : Últimas 24 horas

Mostrar datas como : Local

Usuário contém 93e82fa5-c0af-42b4-bf9d-3e147075d67c

Adicionar filtros

Entradas do usuário (interativo) Entradas do usuário (não interativo)

Data	ID da Solicitação	Usuário	Aplicativo	Status	Endereço IP	Localização	Acesso Condisional	Requisito de auten...
86bda1f3-ff80-4b57-9e...	Diego Piffaretti	Azure Portal	Êxito	Sao Paulo, Sao Paulo, BR	Éxito	Autenticação multifator		
3671766e-84c1-4b07-b...	Diego Piffaretti	Windows Sign In	Êxito	Rio De Janeiro, Rio De J...	Não Aplicado	Autenticação multifator		
a822c4ad-b2d2-4493-a...	Diego Piffaretti	accounts-connect-teste	Êxito	Rio De Janeiro, Rio De J...	Éxito	Autenticação multifator		
2d1ba65a-7ccb-49c9-a...	Diego Piffaretti	Office365 Shell WCSS...	Êxito	Rio De Janeiro, Rio De J...	Éxito	Autenticação multifator		
efc8f9b0-8f80-488a-9a...	Diego Piffaretti	Windows Sign In	Êxito	Rio De Janeiro, Rio De J...	Não Aplicado	Autenticação multifator		
c585e029-25ef-45b2-b...	Diego Piffaretti	Office Online Core SSO	Êxito	Rio De Janeiro, Rio De J...	Éxito	Autenticação multifator		
d386f6b7-3ef9-44ee-b...	Diego Piffaretti	ServiceNow - Globo Se...	Êxito	Rio De Janeiro, Rio De J...	Éxito	Autenticação multifator		
3246b2e0-e50e-43e8-b...	Diego Piffaretti	Azure Portal	Êxito	Rio De Janeiro, Rio De J...	Éxito	Autenticação multifator		
e2708455-9614-4320-b...	Diego Piffaretti	Office365 Shell WCSS...	Êxito	Rio De Janeiro, Rio De J...	Éxito	Autenticação multifator		
95276207-08ac-4452-8...	Diego Piffaretti	Office Online Core SSO	Êxito	Rio De Janeiro, Rio De J...	Éxito	Autenticação multifator		
8a24249a-0270-4589-b...	Diego Piffaretti	Windows Sign In	Êxito	Rio De Janeiro, Rio De J...	Não Aplicado	Autenticação multifator		
0c072b3f-7599-484f-ac...	Diego Piffaretti	Palo Alto Networks - Gl...	Êxito	Sao Paulo, Sao Paulo, BR	Éxito	Autenticação multifator		

H2
HC



Conditional Access: Token protection (preview)

Screenshot of the Microsoft Azure Conditional Access Token Protection Policy configuration page.

Token Protection Policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *: Token Protection Policy

Assignments

Users: Specific users included

Cloud apps or actions: 2 apps included

Conditions: 2 conditions selected

Access controls

Grant: 0 controls selected

Session

Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

- Use app enforced restrictions ⓘ
- Use Conditional Access App Control ⓘ
- Sign-in frequency ⓘ
- Persistent browser session ⓘ
- Customize continuous access evaluation ⓘ
- Disable resilience defaults ⓘ
- Require protection for sign-in sessions ⓘ

The control "Require token protection for sign-in sessions" only works with supported Windows devices and a limited set of applications. Unsupported devices and applications are blocked. [Learn more](#)

Select

Stolen session cookie was used

Medium • Unknown • New

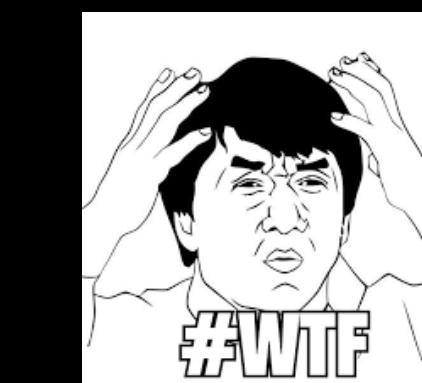
[Open alert page](#) [Manage alert](#) [Link alert to another incident](#) ...

Alert description

The session cookie being used in this Exchange Online session was detected to be compromised. Microsoft 365 Defender alerts on the earliest observed event in this session.



Desktop applications accessing Exchange Online and SharePoint Online on Windows



H2
HC



Conditional Access: Risk-based

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED
High	Offline	Users with leaked credentials ⓘ	44 of 45
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ	76 of 78
Medium	Offline	Impossible travels to atypical locations ⓘ	11 of 14
Medium	Real-time	Sign-in from unfamiliar location ⓘ	0 of 1
Low	Offline	Sign-ins from infected devices ⓘ	76 of 78

Necessário ter uma licença P2 da Microsoft ☺

Three blue circular icons in the top-left corner.

A large blue 'X' icon in the top-right corner.

Conditional Access – Trusted Locations Only

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name * ✓

Assignments

Users ⓘ [All users included and specific users excluded](#)

Target resources ⓘ [All cloud apps](#)

Conditions ⓘ [1 condition selected](#)

Access controls

Grant ⓘ [0 controls selected](#)

Session ⓘ [0 controls selected](#)

Enable policy

Create **Select**

Control access enforcement to block or grant access. [Learn more](#)

Block access
 Grant access

Require multifactor authentication ⓘ
 Require authentication strength ⓘ
 Require device to be marked as compliant ⓘ
 Require Microsoft Entra hybrid joined device ⓘ
 Require approved client app ⓘ [See list of approved client apps](#)
 Require app protection policy ⓘ [See list of policy protected client apps](#)

For multiple controls
 Require all the selected controls
 Require one of the selected controls

H2
HC

...

X

Conditional Access – Intune Device Compliance

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name * ✓

Assignments

Users ⓘ All users included and specific users excluded

Target resources ⓘ All cloud apps

Conditions ⓘ 0 conditions selected

Access controls

Grant ⓘ 0 controls selected

Session ⓘ 0 controls selected

Enable policy

Report-only On Off

[Create](#)

Control access enforcement to block or grant access. [Learn more](#)

Block access Grant access

Require multifactor authentication ⓘ

Require authentication strength ⓘ

Require device to be marked as compliant ⓘ

⚠ Don't lock yourself out! Make sure that your device is compliant. [Learn more](#)

Require Microsoft Entra hybrid joined device ⓘ

Require approved client app ⓘ See list of approved client apps

Require app protection policy ⓘ See list of policy protected client apps

For multiple controls

Require all the selected controls

Require one of the selected controls

[Select](#)

Defender - Impossible Travel

Cloud App Security

Policy	Count	Status	Type
Logon from a risky IP address	10 open alerts	High	Threat detection
Mass download by a single user	18 open alerts	High	Threat detection
Publicly shared confidential files	4 matches	Medium	Compliance
Block PDF	9 open alerts	Medium	DLP
Unusual file share activity (by user)	0 open alerts	Low	Threat detection
Unusual file download (by user)	0 open alerts	Low	Threat detection
Multiple failed login attempts	0 open alerts	Low	Threat detection
Unusual file deletion activity (by user)	0 open alerts	Low	Threat detection
Activity from suspicious IP addresses	0 open alerts	Low	Threat detection
Impossible travel	3 open alerts	Medium	Threat detection
Activity from anonymous IP addresses	8 open alerts	Medium	Threat detection

A red arrow points to the "Impossible travel" policy row, which is highlighted with a red border.

H2
HC



Automated attack disruption

- Identifica ataques AiTM – Baseado na IA do Defender XDR
- Resposta automática (Desativa a conta de usuário no Active Directory e no Azure Active Directory)
- Um cookie de sessão roubado será automaticamente revogado

Automatically disrupt adversary-in-the-middle attacks with XDR





Outras defesas

- Treinamento e campanhas de conscientização
- MFA habilitado em todos os usuários
- Contas de serviço que não podem ter MFA, possuírem restrição de acesso via Acesso Condicional (EX: restringir acesso somente aos IPs da empresa)
- Conditional Access
- Cogitar o uso de Hardware Keys MFA (U2F) – EX: Yubikey



H2
HC



AiT M

Status Proteções

Method	Protected (mitigation) against AiTM
Custom Tenant branding	✗
Azure AD Identity Protection	✗ (only alerting)*
Microsoft Defender for Endpoint	! (only alerting + blocking known AiTM websites)*
Microsoft Defender SmartScreen	! (blocking known AiTM websites)*
Microsoft 365 Defender	! (Attack Disruption capabilities)*
Microsoft Defender for Cloud Apps	✗ (only alerting)*
Microsoft Defender for Office 365	✗ (only removing emails including phishing links)*



AiTM

Status Proteções

Method	Protected (mitigation) against AiTM
Require device to be marked as compliant	<input checked="" type="checkbox"/>
Require device to be marked as Hybrid Azure AD joined device	<input checked="" type="checkbox"/>
Conditional Access Session Controls	<input checked="" type="checkbox"/> ✖ (limit time window when the attacker can use the session cookie)
Conditional Access Trusted Locations	<input checked="" type="checkbox"/>



AiTM

Status Proteções

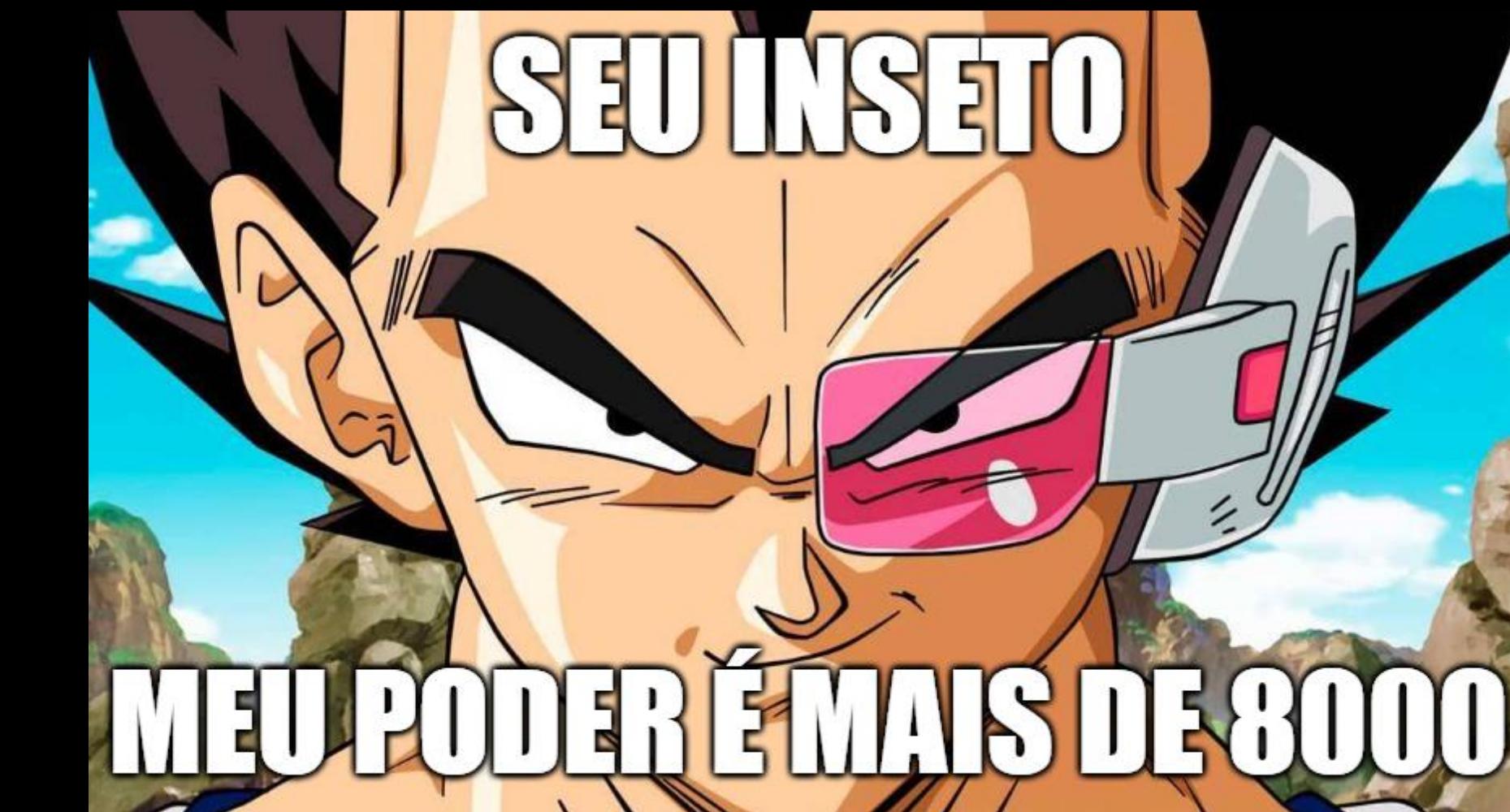
Method	Protected (mitigation) against AiTM
FIDO2 security keys	✓
Windows Hello for Business	✓
Certificate-based authentication	✓
Passwordless phone sign-in	✗
Phone number and SMS	✗
Username and password	✗



Conclusão



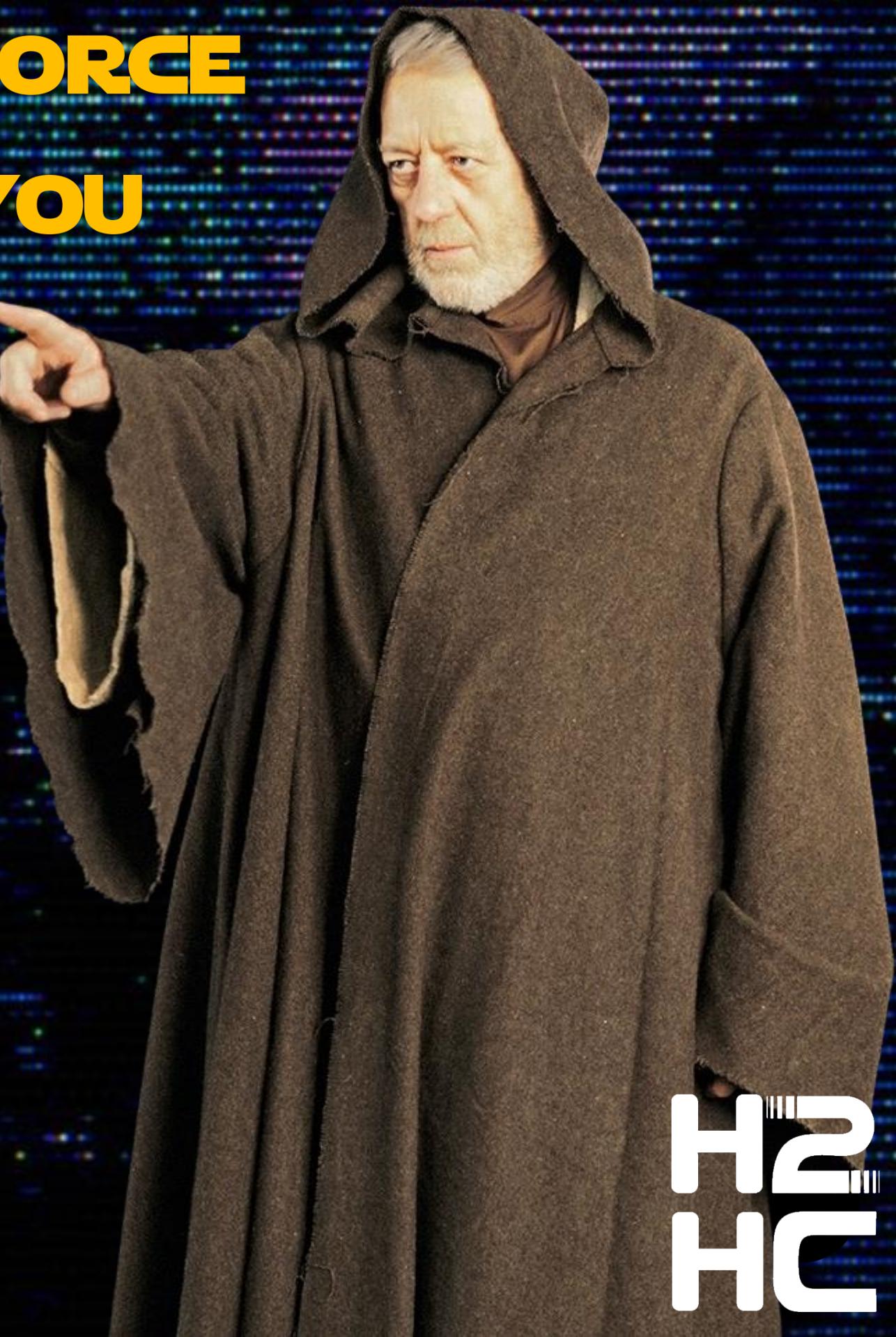
Google



H2
HC

OBRIGADO!

MAY THE FORCE
BE WITH YOU



linkedin.com/in/diegopiffaretti



Mundotecnologico.net

H2
HC