



H2  
HC

Autor: Piffaretti

Autor: Piffaretti

Diego Piffaretti

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

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti



## 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

Autor: Piffaretti



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

[www.Mundotecnologico.net](http://Mundotecnologico.net)

H2  
HC

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

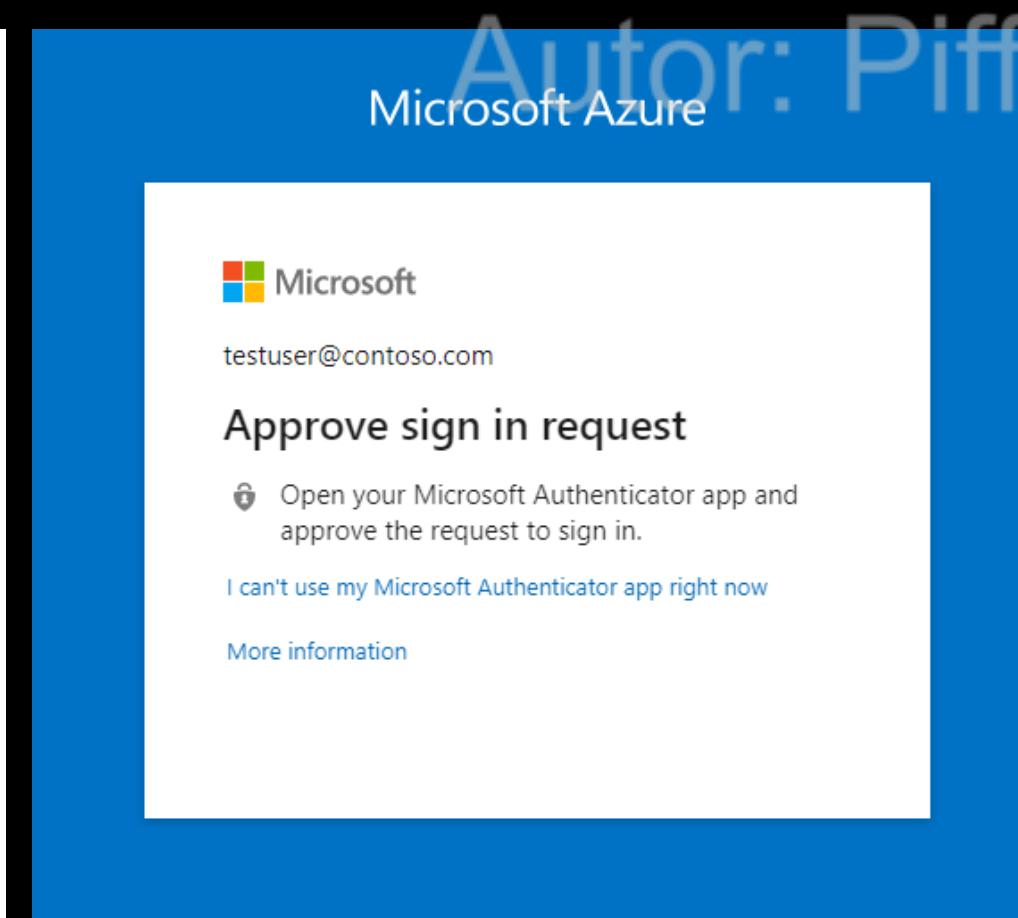
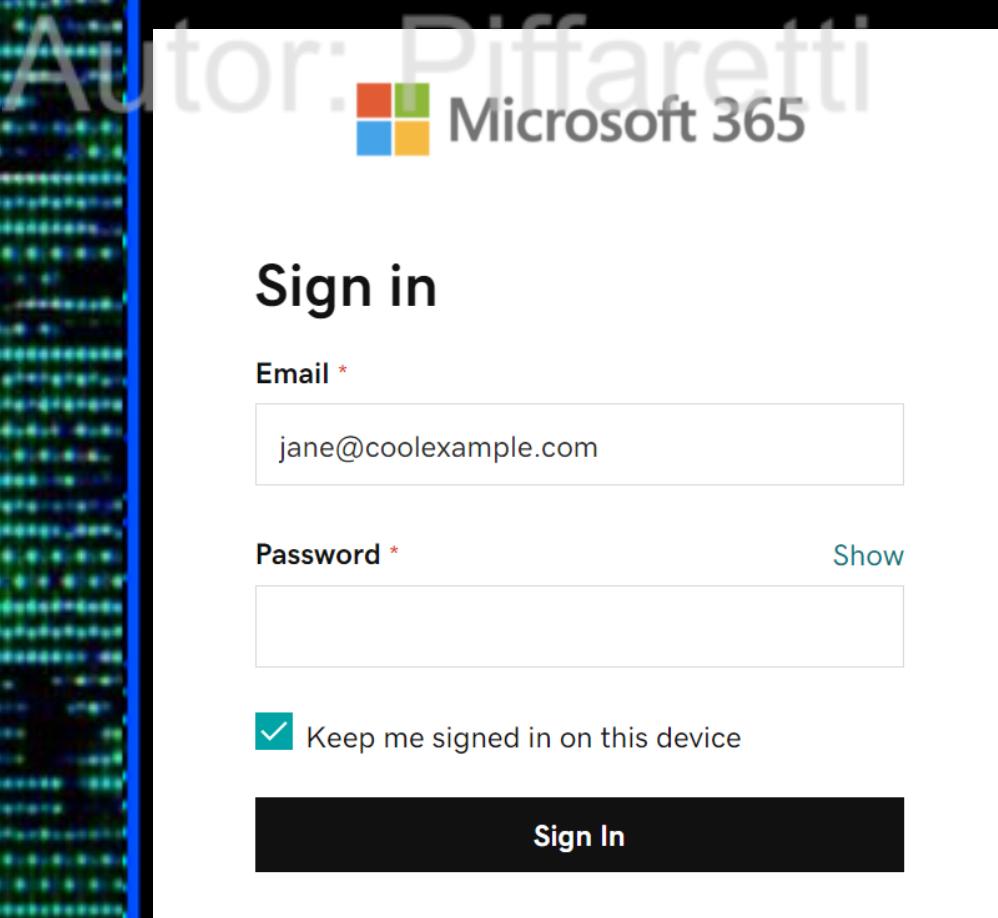
Autor: Piffaretti

Autor: Piffaretti

# Objetivo

# Authentication Bypass and MFA Evasion

# AiT M (Adversary-in-the-Middle)



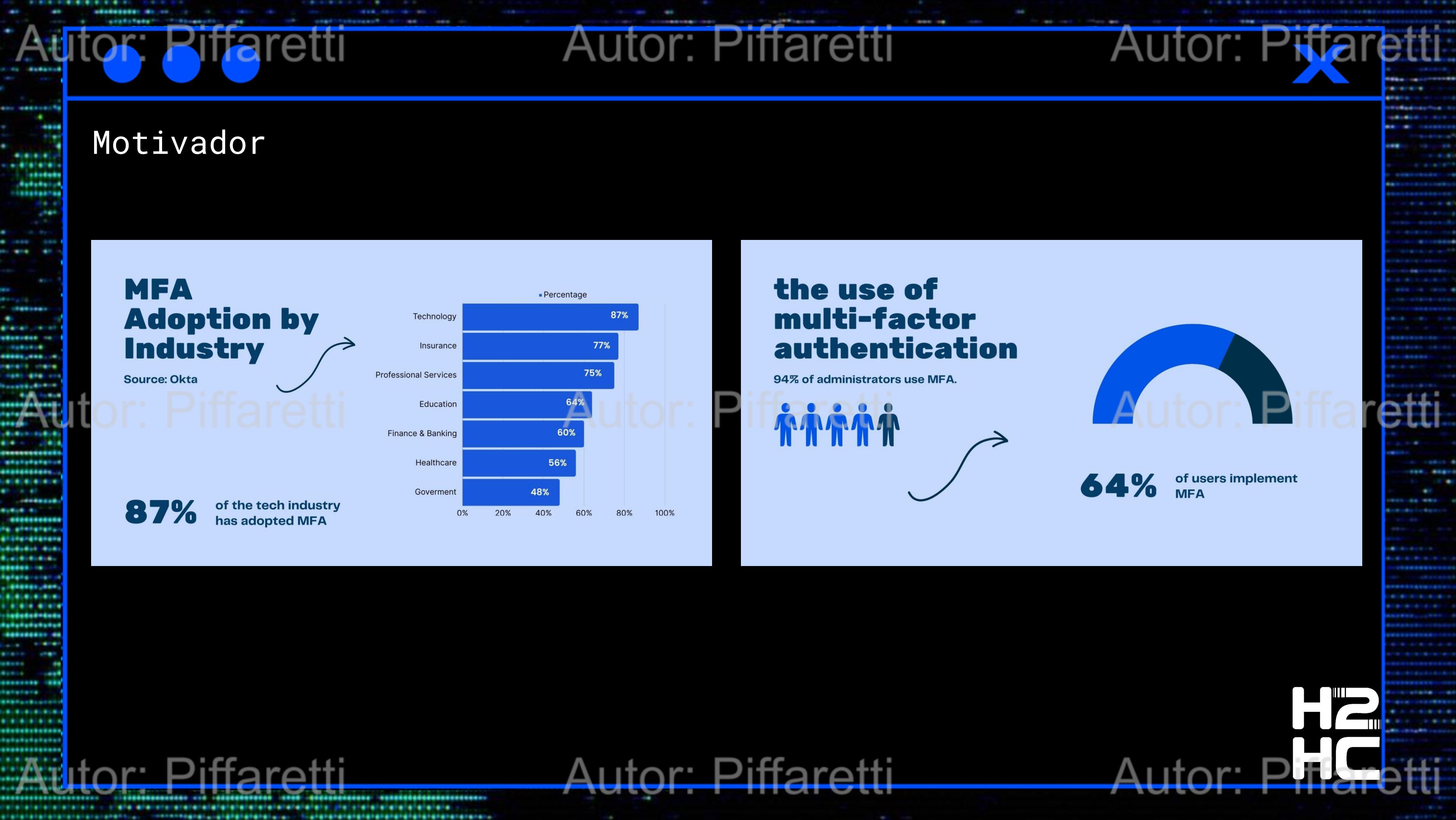
Autor: Piffaretti

Autor: Piffaretti

Autor: Pifaretti







Autor: Piffaretti



Autor: Piffaretti



## Motivador

AiT M as a Service: Mamba 2FA

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.

Autor: Piffaretti

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



Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti



Autor: Piffaretti

H2  
HC

Autor: Piffaretti

Autor: Piffaretti



Autor: Piffaretti



Motivador



Autor: Piffaretti

Passando aperto na  
prática!

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

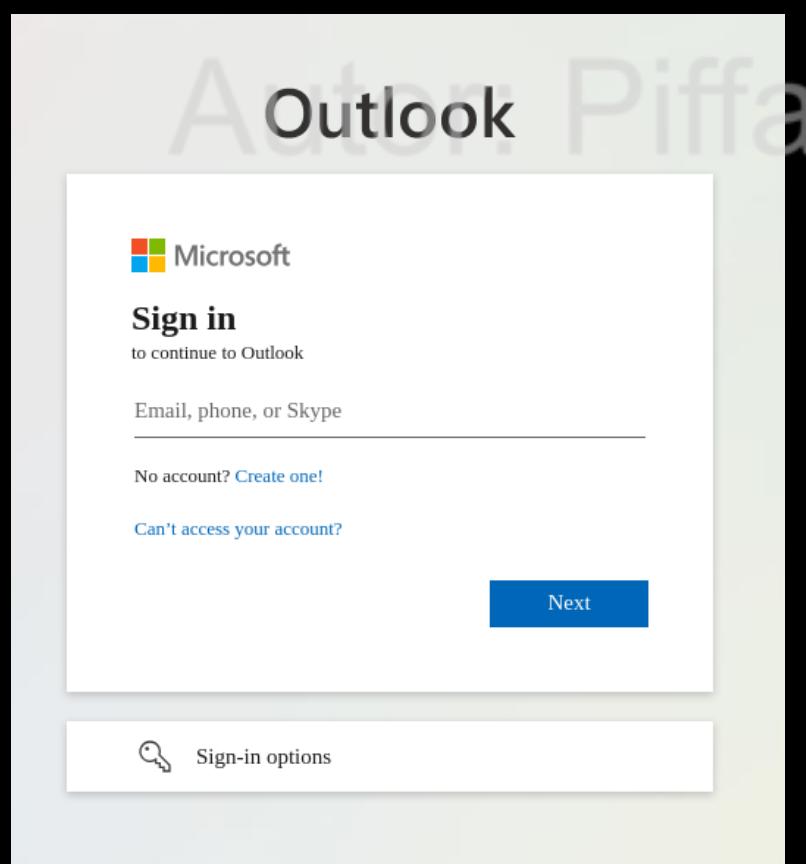
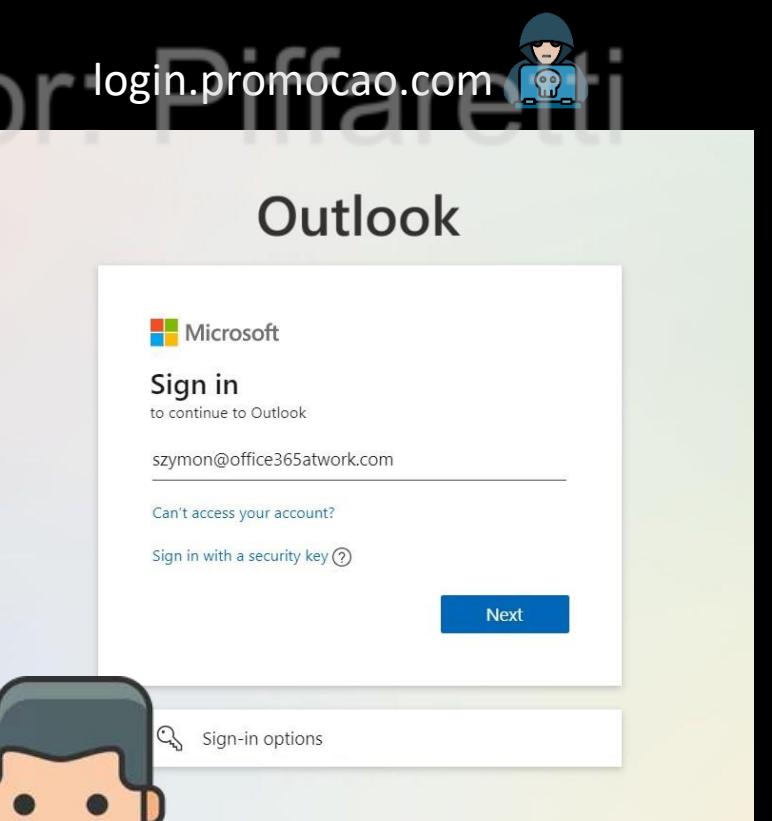
Autor: Piffaretti

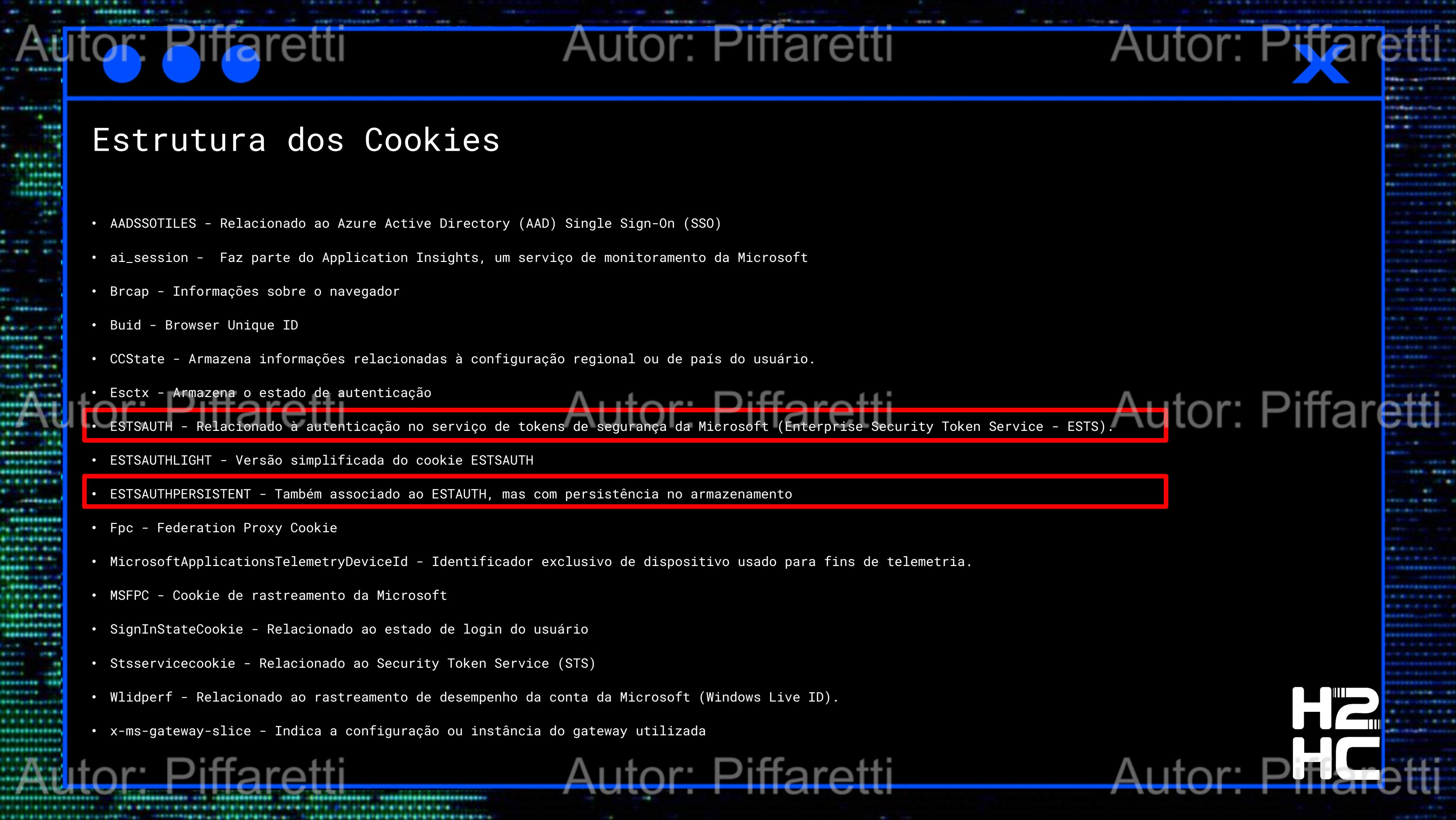


Autor: Piffaretti

# Proxy phishing

Fundamento





## 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.

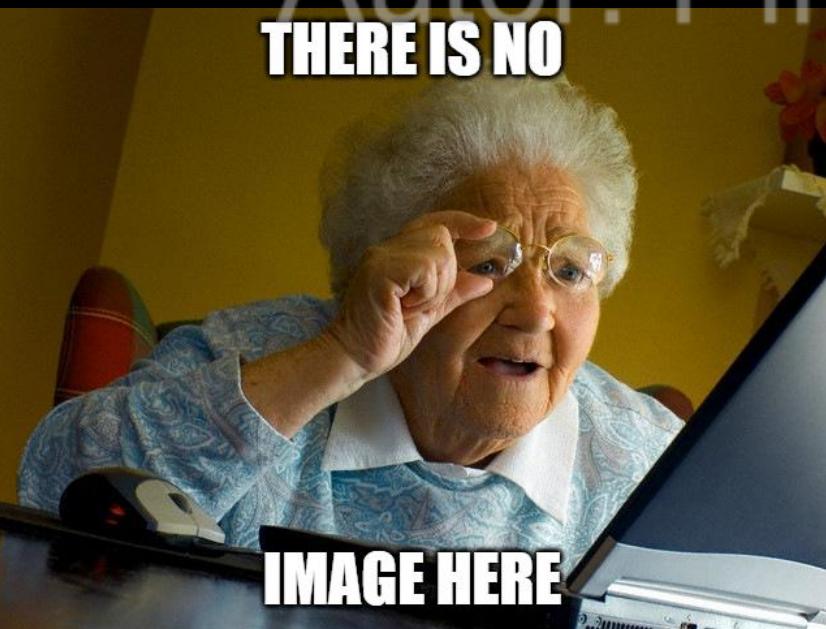
A Liesa em parceria com a Globo irá disponibilizar alguns ingressos para camarotes, boxes especiais e frisas para colaboradores e mais 2 acompanhantes sorteados. Para participar do sorteio, basta preencher uma planilha compartilhada no Sharepoint da Globo com seus dados.

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

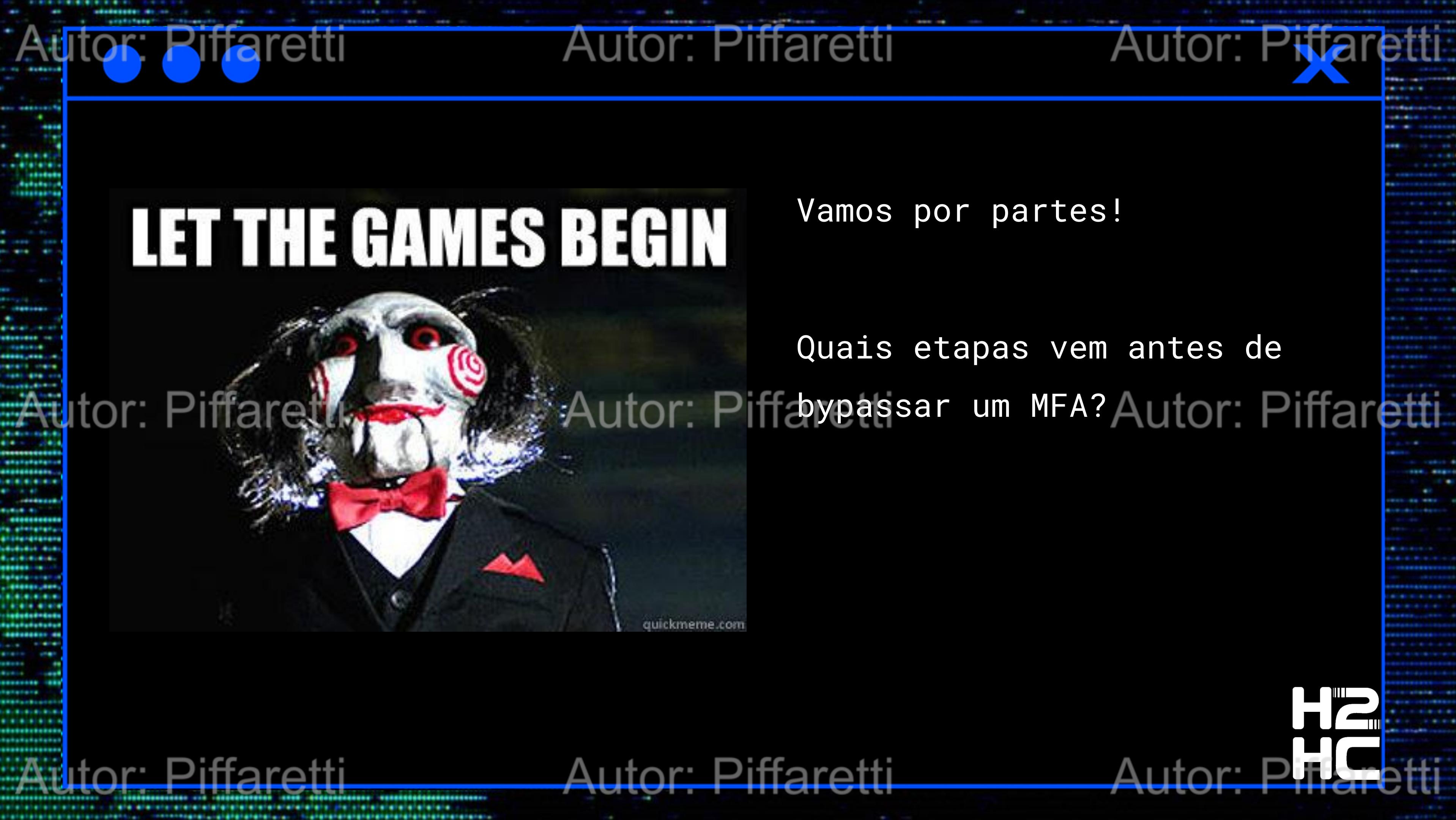
- Não é permitida a entrada de crianças com menos de 05 anos de idade
- Proibido levar isopores, garrafas de vidro, sacolas, armas, objetos cortantes, sinalizadores e fogos de artifício.
- É permitido levar até dois vasilhames plásticos de 500 ml com bebida (água, suco, refrigerante ou cerveja) e até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

Elementos :

- Texto
- Hyperlink
- Imagem



H2  
HC

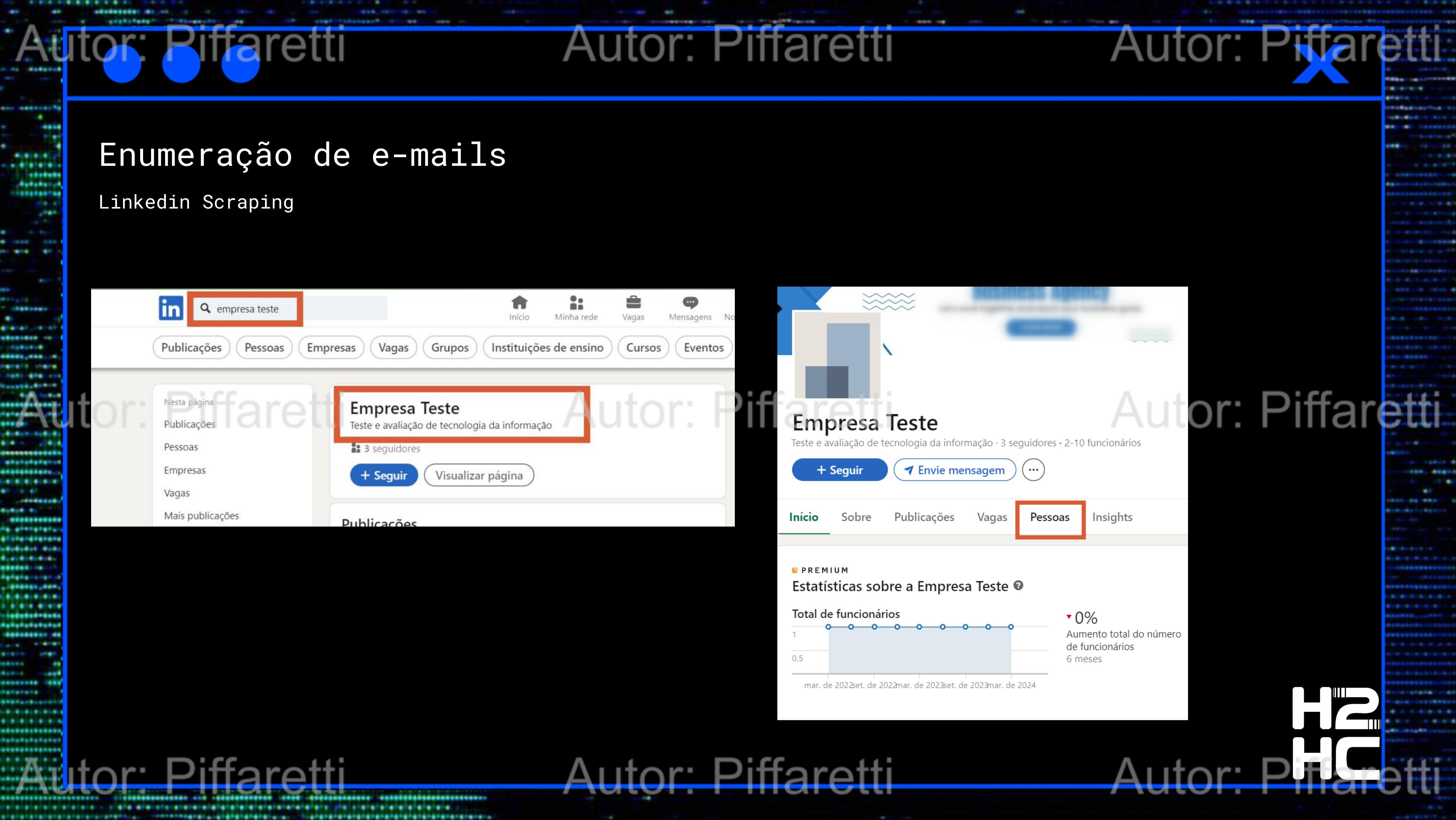


Autor: Piffaretti

Vamos por partes!

Quais etapas vem antes de  
bypassar um MFA?

H2  
HC



# Autor: Piffaretti

# Autor: Piffaretti

# Autor: Piffaretti

## Enumeração de e-mails

### Ferramentas

<https://phonebook.cz>

The screenshot shows the Phonebook.cz homepage with a search bar containing 'empresateste.com.br'. Below the search bar are three radio buttons: 'Domains' (unchecked), 'Email Addresses' (checked), and 'URLs' (unchecked). A list of email addresses is displayed, including: [atendimento@empresateste.com.br](mailto:atendimento@empresateste.com.br), [contato@empresateste.com.br](mailto:contato@empresateste.com.br), [admin@empresateste.com.br](mailto:admin@empresateste.com.br), [empresateste@empresateste.com.br](mailto:empresateste@empresateste.com.br), and [teste@empresateste.com.br](mailto:teste@empresateste.com.br). A link 'No more results.' is at the bottom.

<https://hunter.io>

The screenshot shows the Hunter.io 'Domain Search' interface with the domain 'empresateste.com.br' entered in the search bar. Below the search bar are dropdown menus for 'Type' and 'Department' and a button 'Show only results with'. The results section displays two entries: 'empresateste@empresateste.c...' with a confidence level of 74% and 'comercial@empresateste.com.br' with a confidence level of 10%. Each result has a 'Verify email' button and buttons for 'Save as lead' and 'Add to a campaign'.

500apps  
**Finder.io**

RocketReach

MALTEGO

<https://mundotecnologico.net/2024/04/04/tecnicas-de-enumeracao-de-e-mails/>

# H2 HC



Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

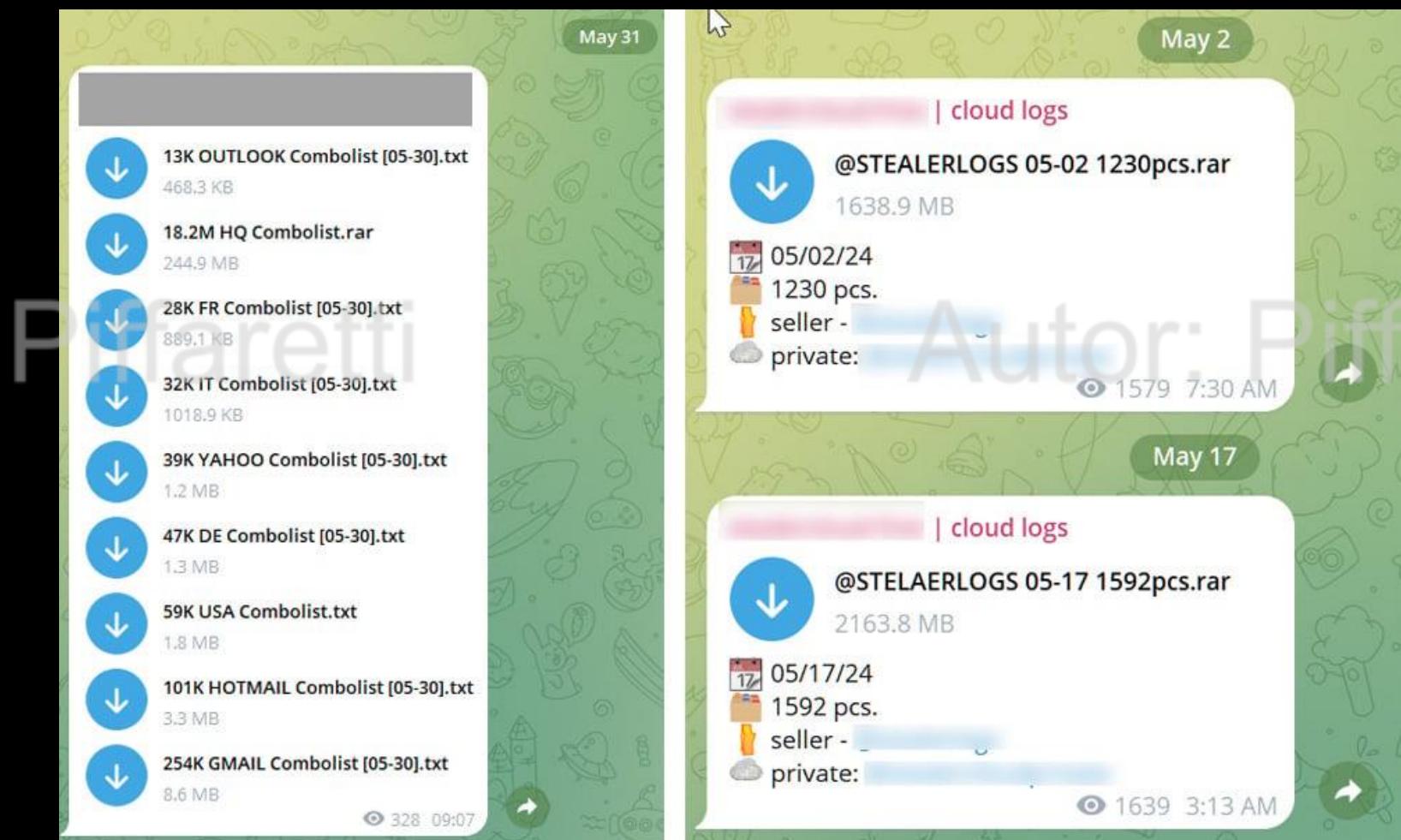
Enumeração de e-mails e credenciais

Ferramentas



BF

Breach Forum



Stealer

H2  
HC

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti X

## Validação de e-mails

Office 365

[https://<tenantname>-my.sharepoint.com/personal/<your\\_user\\_name>/\\_layouts/15/onedrive.aspx](https://<tenantname>-my.sharepoint.com/personal/<your_user_name>/_layouts/15/onedrive.aspx)

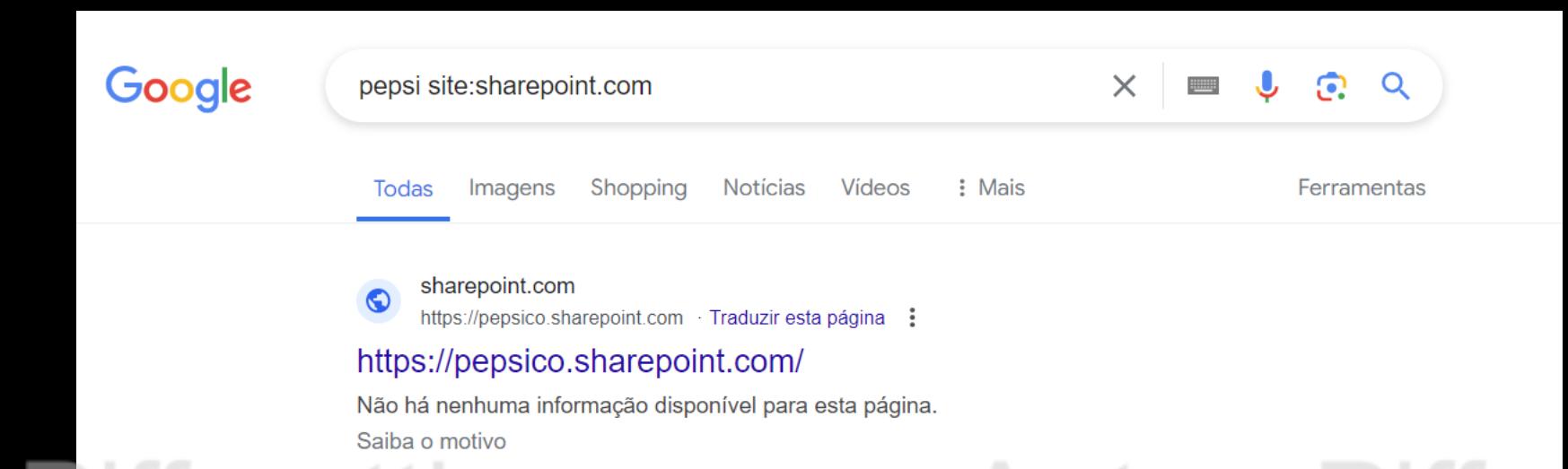
Alvo: maria.flores@emprestateste.com.br

Convertendo: maria\_flores\_empresateste\_com\_br

Requisição: curl -I https://emprestateste-  
my.sharepoint.com/personal/maria\_flores\_empresateste\_com\_br/\_layouts\_15\_onedrive.aspx



Tool: [https://github.com/piffaretti/o365\\_EmailValidator](https://github.com/piffaretti/o365_EmailValidator)



Google

pepsi site:sharepoint.com

Todas Imagens Shopping Notícias Vídeos Mais Ferramentas

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

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

Autor: Piffaretti



## PHISHING

Dominio



Autor: Piffaretti



Autor: Piffaretti



Autor: Piffaretti



Autor: Piffaretti



Autor: Piffaretti

Autor: Piffaretti



Autor: Piffaretti



Autor: Piffaretti



Autor: Piffaretti

H2  
HC

**Autor: Piffaretti**

# 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

**Autor: Piffaretti**

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	- Sao Paulo - Sao Paulo
ASN	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
<a href="#">Whois Record</a> ( last updated on 2024-06-13 )	
<p>Domain Name:            Registry Domain ID:            Registrar WHOIS Server:            Registrar URL:            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: operations, UAB            Registrar IANA ID:            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:            Name Server:            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@            Registrar Abuse Contact Phone:            URL of the ICANN Whois Inaccuracy Complaint Form: <a href="https://www.icann.org/wicf/">https://www.icann.org/wicf/</a></p>	

**Autor: Piffaretti****Autor: Piffaretti****Autor: Piffaretti****Autor: Piffaretti****Autor: Piffaretti****Autor: Piffaretti**

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti X

## PHISHING

### E-mail

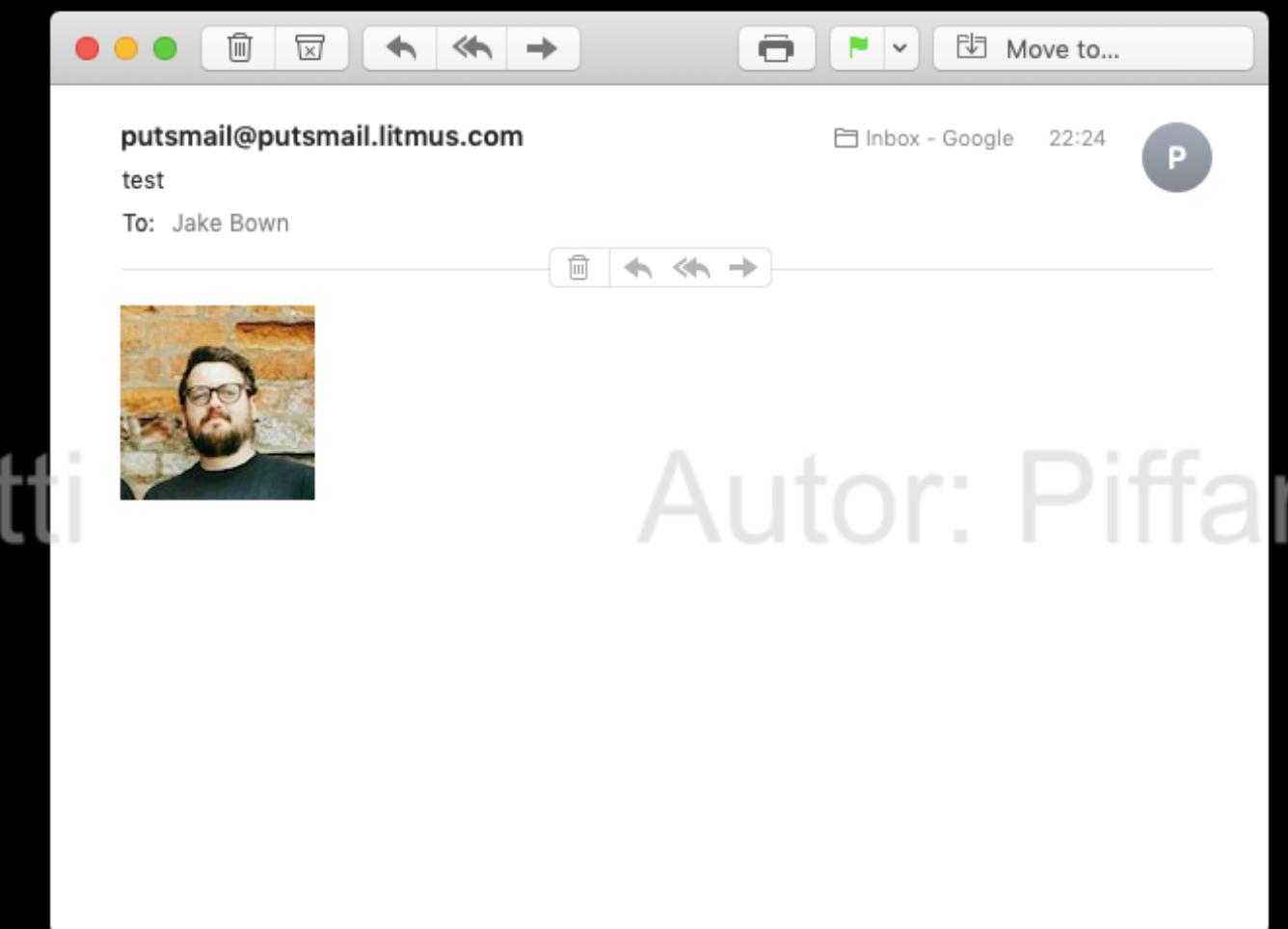
- Necessário bypass na “Proteção contra usurpação de identidade do usuário”
- Necessário bypass contra “Inteligência contra falsificação”
- Necessário bypass conta “Detonation analysis (File and URL)”
- Não usar caracteres incomuns
- Evitar usar técnica de Backscatter (spoof)
- Evitar formulário HTML
- 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)

Autor: Piffaretti

## 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>)



H2  
HC

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti X

## 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

H2  
HC



Autor: Piffaretti



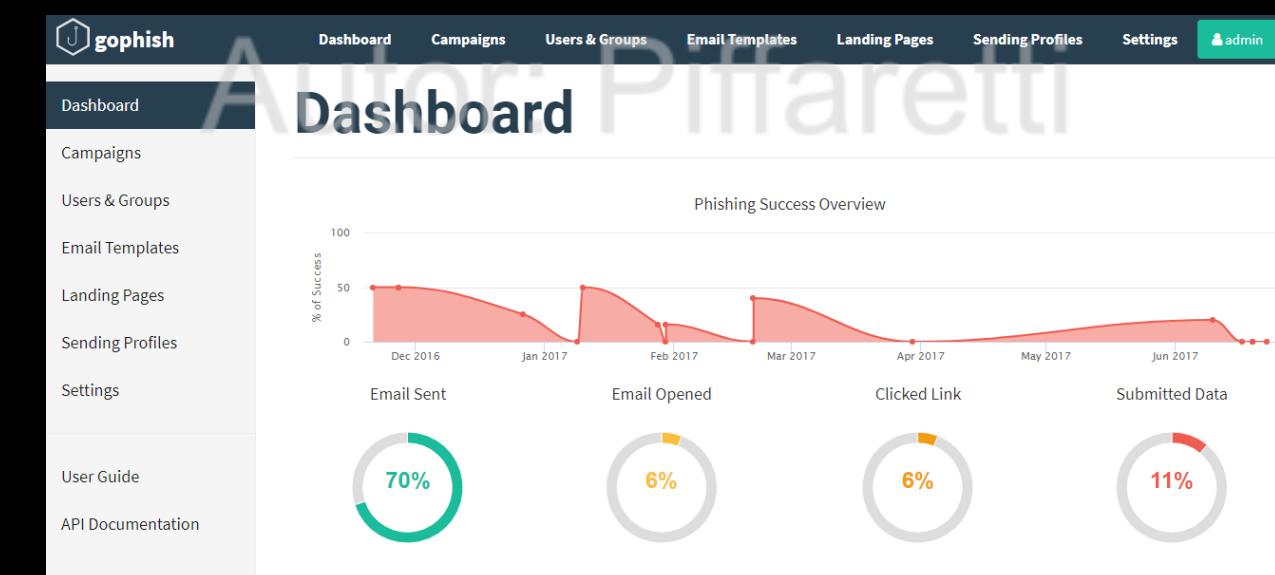
## Proxy phishing

Evilginx 3.3

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



Autor: Piffaretti



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

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

H2  
HC

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

## 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](https://github.com/aalex954/MSFT-IP-Tracker/releases/latest/download/msft_asn_ip_ranges.txt)

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

H2  
HC

Autor: Piffaretti

# Evilginx

```
[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>
```

Autor: Piffaretti

phishlet	author	active	status	hostname
amazon	@customsync	disabled	available	
instagram	@rrrrrinnee	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
```

Autor: Piffaretti

# Autor: Piffaret

Autor: Piffaretti

1 server IP set to: 1.2.3.4

# Autor: Piffaretti

Autor: Piffaretti

Autor: Pflaum



Autor: Piffaretti



## Evilginx

Blue Team detection



Autor: Piffaretti



- 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)

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti



Autor: Piffaretti



Autor: Piffaretti



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](#).

Autor: Piffaretti

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](#).

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

H2  
HC

Autor: Piffaretti



Autor: Piffaretti

Autor: Piffaretti



Infra AiTM

VPS + VPN



Como fazer gastando pouco?

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti



<p><b>Autor: Piffaretti</b></p>  <p><b>FREE:</b> 750 horas de VMs USD\$200 em crédito</p> <p>Ponto positivo:</p> <ul style="list-style-type: none"> <li>• Fácil de navegar</li> <li>• Tem IP BR (SP)</li> </ul> <p><b>BANNED</b></p>	<p><b>Autor: Piffaretti</b></p>  <p><b>FREE:</b> 1 instância da VM e2-micro USD\$200 em crédito</p> <p>Ponto positivo:</p> <ul style="list-style-type: none"> <li>• Mediano de navegar</li> </ul> <p><b>BANNED</b></p>	<p><b>Autor: Piffaretti</b></p>  <p><b>FREE:</b> 3 meses grátis (750 horas por mês)</p> <p>Ponto positivo:</p> <ul style="list-style-type: none"> <li>• Fácil de navegar</li> <li>• Dura mais tempo que os demais</li> </ul> <p>Ponto negativo:</p> <ul style="list-style-type: none"> <li>• Não tem IP BR</li> <li>• Cuidado para lembrar de cancelar a subscrição</li> </ul>	<p><b>Autor: Piffaretti</b></p>  <p>Ponto positivo:</p> <ul style="list-style-type: none"> <li>• Free eternamente</li> <li>• Tem IP BR</li> <li>• Terra de ninguém</li> </ul> 
---	---	---	--

Autor: Piffaretti



# 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.

Block

### Likely automated

Likely automated traffic can include bad bots, along with other traffic. Select an action for this traffic.

Challenge

### Verified bots

Verified bots are unique good bot identities validated by Cloudflare. Select an action for verified bots for this traffic.

Allow

### Static resource protection

Enable if static resources on your application need bot protection.  
**Note:** Static resource protection can also result in legitimate traffic being blocked.

Off

### JavaScript Detections

Use lightweight, invisible JavaScript detections to improve Bot Management. [Learn more.](#)

On

Autor: Piffaretti

Autor: Piffaretti



CLOUDFLARE®

## 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](#).



**Note:** Other security products cannot be used to skip Bot Fight Mode. [Learn more](#)

#### New AI Scrapers and Crawlers

Block bots from scraping your content for AI applications like model training.



#### Then take action...

##### Choose action

Managed Challenge

Managed Challenge

Block

JS Challenge

Skip

Interactive Challenge

H2  
HC

Autor: Piffaretti



Evilginx

Google Safe Browsing Bypass

Autor: Piffaretti

Autor: Piffaretti



CLOUDFLARE®

••• Autor: Piffaretti

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

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

H2  
HC

Autor: Piffaretti

Autor: Piffaretti



Evilginx

Bypass Other Security measures

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

Autor: Piffaretti

Autor: Piffaretti



CLOUDFLARE®

Autor: Piffaretti

Autor: Piffaretti

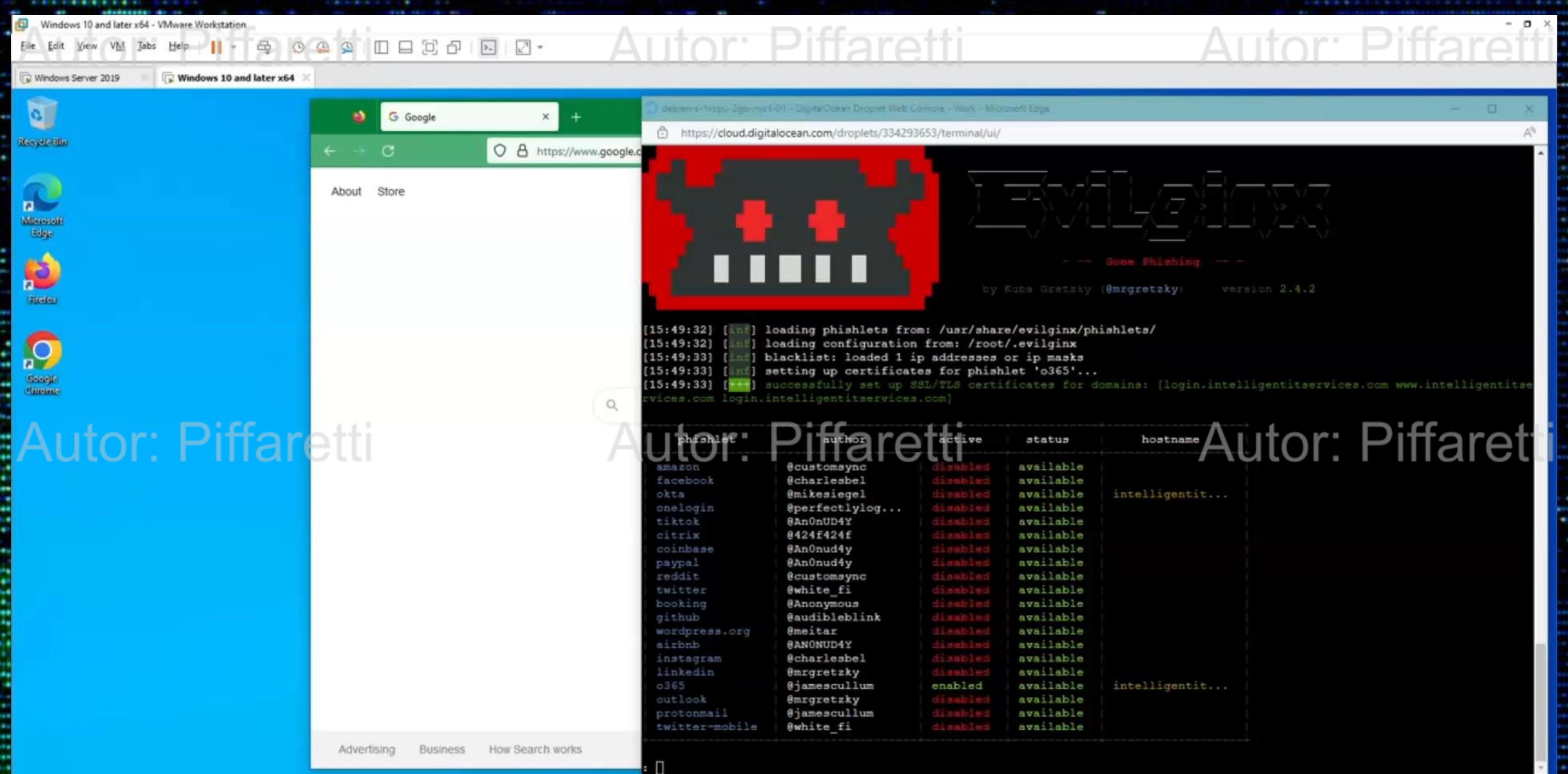
Autor: Piffaretti

H2  
HC

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti





Autor: Piffaretti

DEFESA

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti



## 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



Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti X

# Ao perceber um ataque, o que fazer?

Screenshot of the Microsoft Azure portal showing the user profile page for "Diego Piffaretti". The "Visão geral" tab is selected. A red box highlights the "Revogar sessões" (Revoke sessions) button in the top navigation bar. An orange arrow points from the text "Ao perceber um ataque, o que fazer?" to this button.

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

Informações básicas

Nome UPN ID de objeto Data e hora de criação Tipo de usuário Identidades Meu Feed

Associações de grupo Aplicativos Funções atribuídas Licenças atribuídas

Revogar sessões

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

# 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?

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

Logs de entrada (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		

Logs de auditoria 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

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

Autor: Piffaretti

Autor: Piffaretti

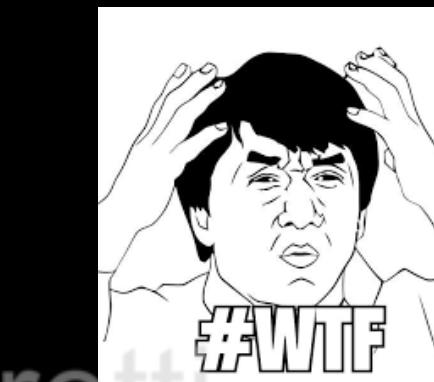
Autor: Piffaretti X

## Conditional Access: Token protection (preview)

The screenshot shows the Microsoft Azure portal interface for creating a Token Protection Policy. The left sidebar lists policy components: Name (Token Protection Policy), Assignments, Users, Cloud apps or actions (2 apps included), Conditions (2 conditions selected), Access controls, Grant (0 controls selected), Session (Require token protection for sign-in sessions selected), and Enable policy (Report-only). The main content area is titled "Session" and describes how to control access based on session controls. It includes several checkboxes: Use app enforced restrictions, Use Conditional Access App Control, Sign-in frequency, Persistent browser session, Customize continuous access evaluation, Disable resilience defaults, and Require protection for sign-in sessions (which is checked). A note below states that the "Require token protection for sign-in sessions" control only works with supported Windows devices and a limited set of applications.

The screenshot shows a Microsoft 365 Defender alert titled "Stolen session cookie was used". The alert is categorized as Medium severity. It includes options to Open alert page, Manage alert, Link alert to another incident, and more. The alert description states: "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

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti X

## 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 ☺

H2  
HC

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

## 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  Report-only  On  Off

Block access  Grant access

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

- 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

[Create](#) [Select](#)

H2  
HC

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti 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

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**

**Create**

**Autor: Piffaretti****Autor: Piffaretti****Autor: Piffaretti**

## Defender - Impossible Travel

**Cloud App Security**

Policy	Count	Status	Category
Logon from a risky IP address	10 open alerts	<span style="color:red;">■■■</span>	Threat detection
Mass download by a single user	18 open alerts	<span style="color:red;">■■■</span>	Threat detection
Publicly shared confidential files	4 matches	<span style="color:red;">■■■</span>	Compliance
Block PDF	9 open alerts	<span style="color:red;">■■■</span>	DLP
Unusual file share activity (by user)	0 open alerts	<span style="color:orange;">■■■■■</span>	Threat detection
Unusual file download (by user)	0 open alerts	<span style="color:orange;">■■■■■</span>	Threat detection
Multiple failed login attempts	0 open alerts	<span style="color:orange;">■■■■■</span>	Threat detection
Unusual file deletion activity (by user)	0 open alerts	<span style="color:orange;">■■■■■</span>	Threat detection
Activity from suspicious IP addresses	0 open alerts	<span style="color:orange;">■■■■■</span>	Threat detection
<b>Impossible travel</b>	3 open alerts	<span style="color:orange;">■■■■■</span>	Threat detection
Activity from anonymous IP addresses	8 open alerts	<span style="color:red;">■■■■■</span>	Threat detection

A red arrow points to the "Impossible travel" policy, 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



Autor: Piffaretti



Autor: Piffaretti



## 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

Autor: Piffaretti



AiTM

Status Proteções

Autor: Piffaretti



Autor: Piffaretti

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)*



Autor: Piffaretti

## 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"/>

H2  
HC

Autor: Piffaretti



Autor: Piffaretti

Autor: Piffaretti



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	✗

H2  
HC

Autor: Piffaretti



Conclusão



Autor: Piffaretti



Autor: Piffaretti

Autor: Piffaretti



Autor: Piffaretti

Autor: Piffaretti



Autor: Piffaretti





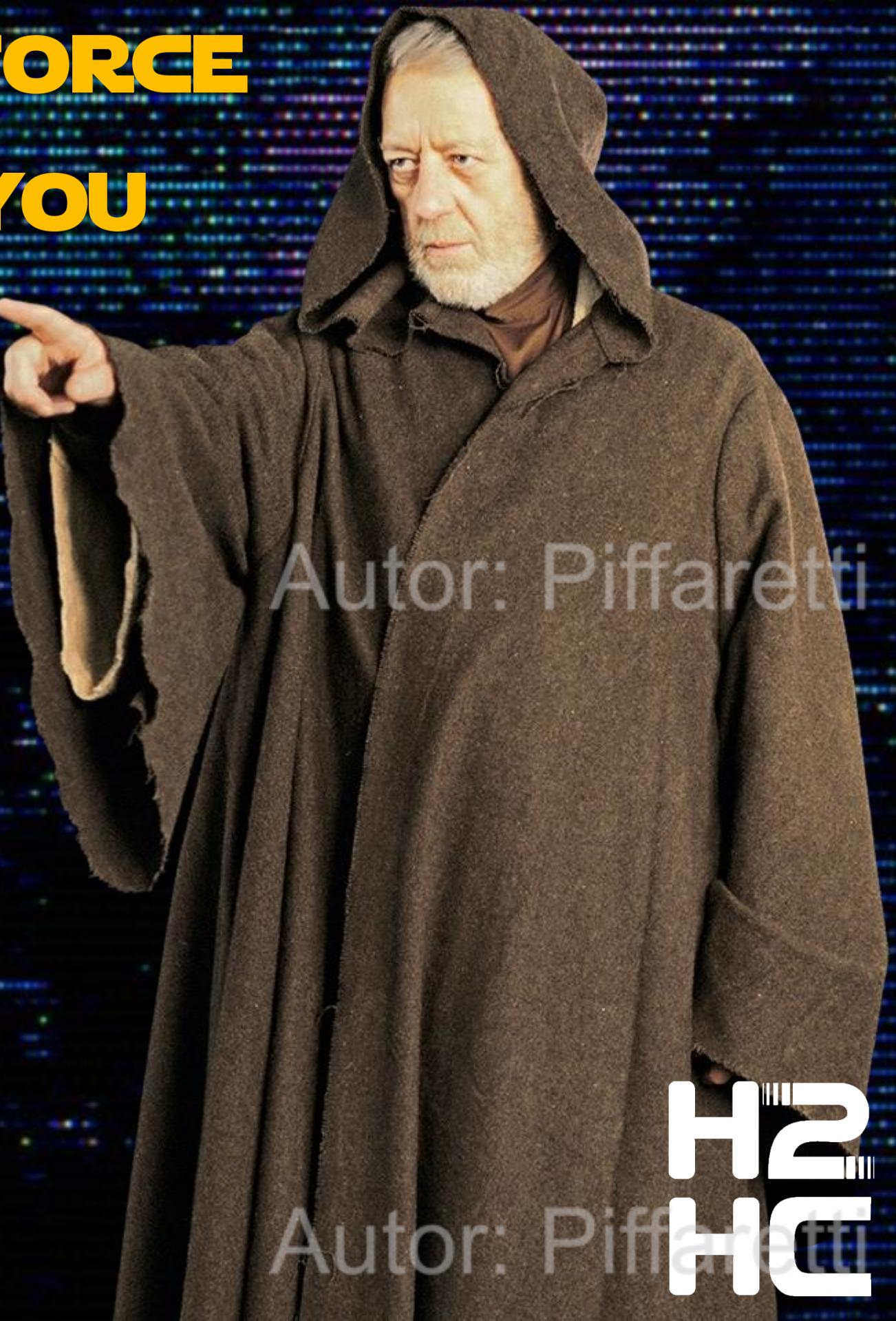
# OBRIGADO!

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

MAY THE FORCE  
BE WITH YOU



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

 [Mundotecnologico.net](http://Mundotecnologico.net)

Autor: Piffaretti

Autor: Piffaretti

Autor: Piffaretti

H2  
HC