H2HC

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

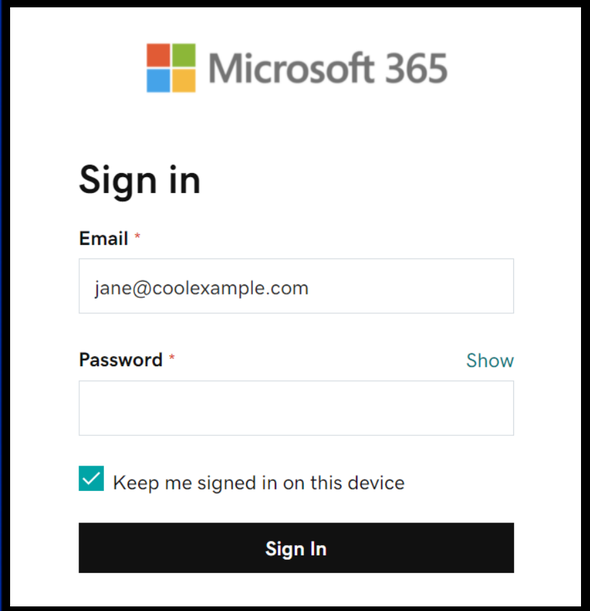
linkedin.com/in/diegopiffaretti

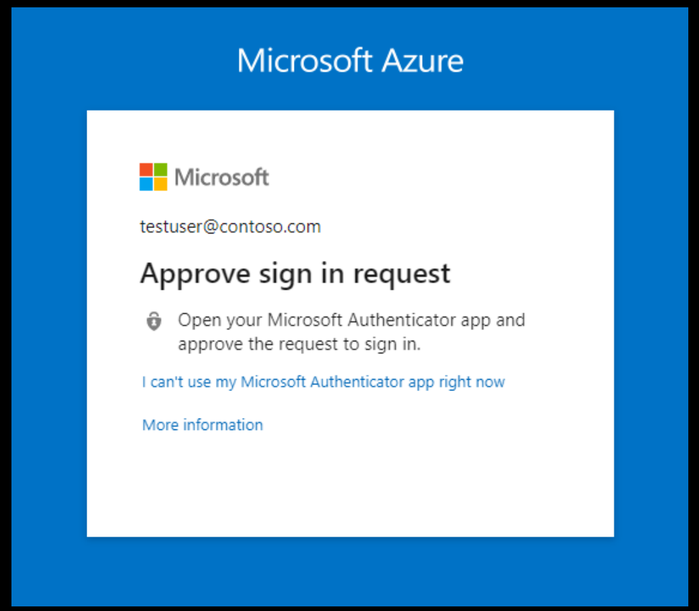
Mundotecnologico.net

Objetivo

Authentication Bypass and MFA Evasion

AiTM (Adversary-in-the-Middle)

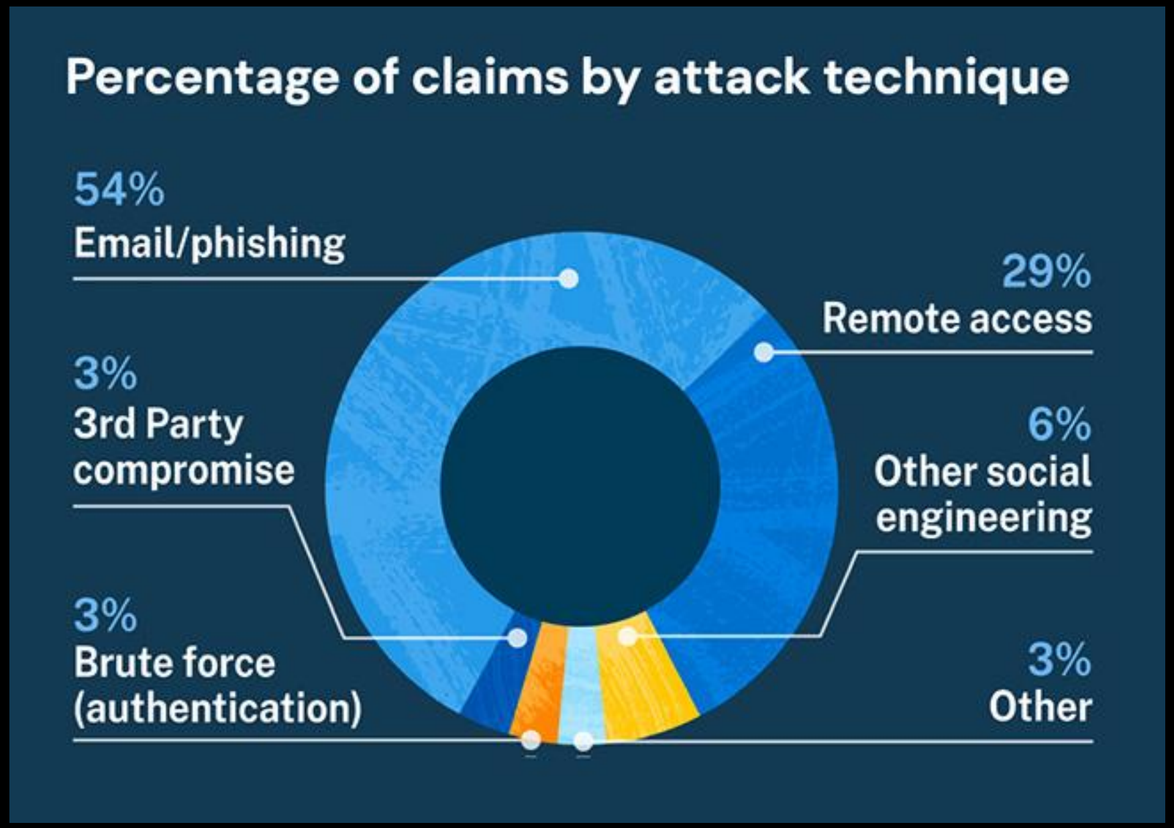


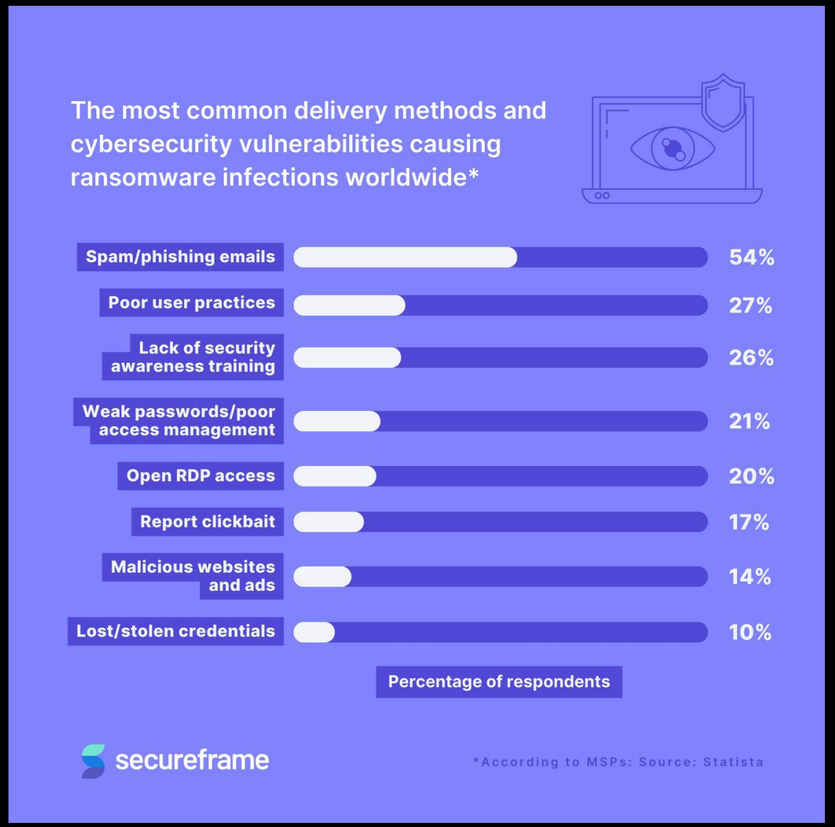


Aplicabilidade

- Campanhas de Red Team Externa
- Campanhas de Engenharia Social

Motivador

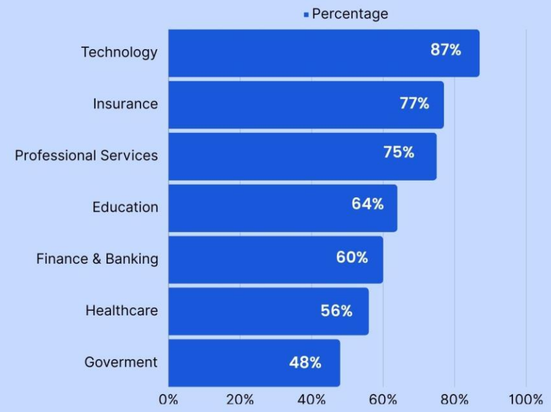

Percentage of claims by attack technique
54%
Email/phishing
29%
Remote access
3%
3rd Party compromise
6%
Other social engineering
3%
Brute force (authentication)
3%
Other


The most common delivery methods and cybersecurity vulnerabilities causing ransomware infections worldwide*
Spam/phishing emails 54%
Poor user practices 27%
Lack of security awareness training 26%
Weak passwords/poor access management 21%
Open RDP access 20%
Report clickbait 17%
Malicious websites and ads 14%
Lost/stolen credentials 10%
Percentage of respondents
secureframe
*According to MSPs; Source: Statista

Motivador

MFA Adoption by Industry

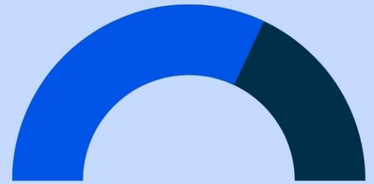
Source: Okta



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

AiTM 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.

Motivador

Passando aperto na prática!

Proxy phishing

Fundamento

Login e senha

Login e senha

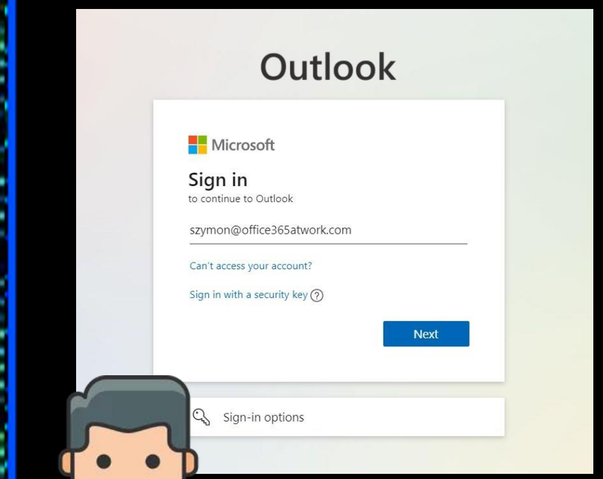
Proxy

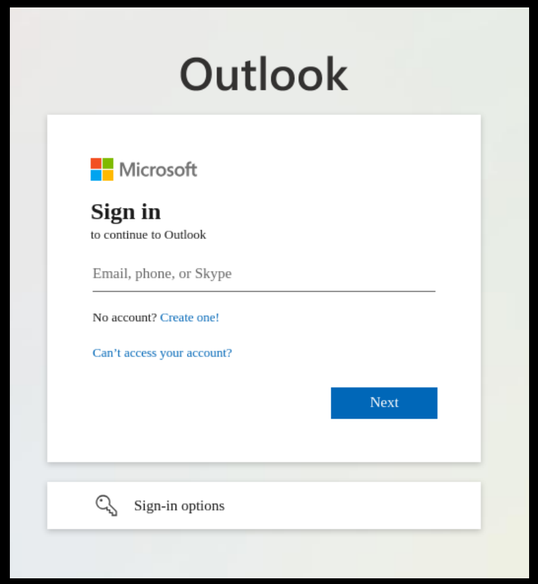
login.promocao.com

Outlook.office.com

MFA

MFA





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.

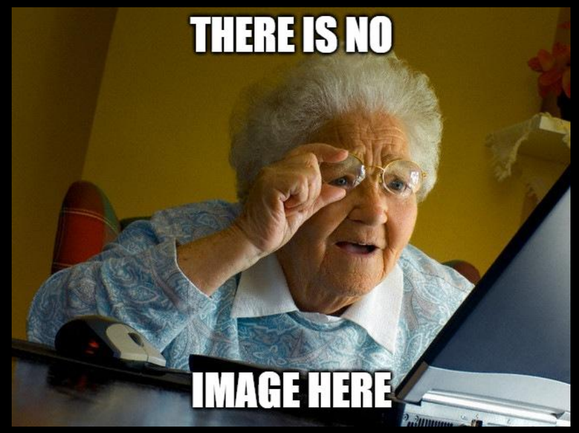
A Liesa em parceria com a Globo irá disponibilizar alguns ingressos para camarotes, boxes especiais e frisas para colaboradores e mais 2 acompanhantes sorteados. Para participar do sorteio, basta preencher uma planilha compartilhada no Sharepoint da Globo com seus dados.

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

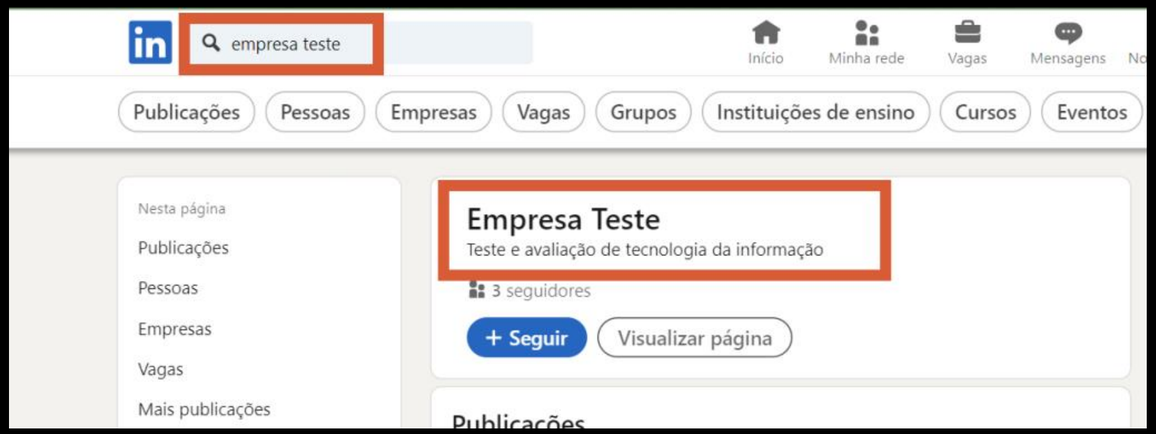


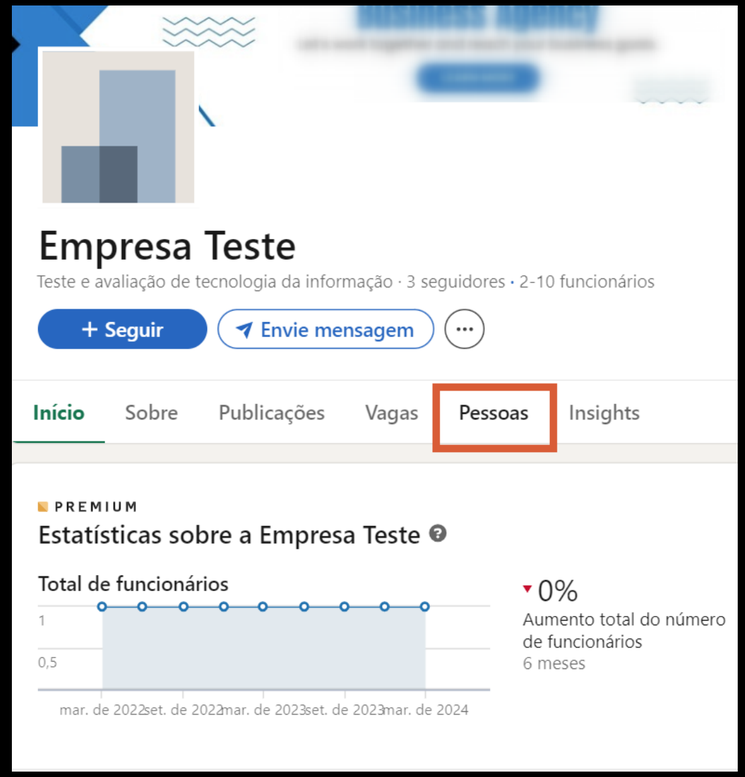
Vamos por partes!

Quais etapas vem antes de bypassar um MFA?

Enumeração de e-mails

Linkedin Scraping

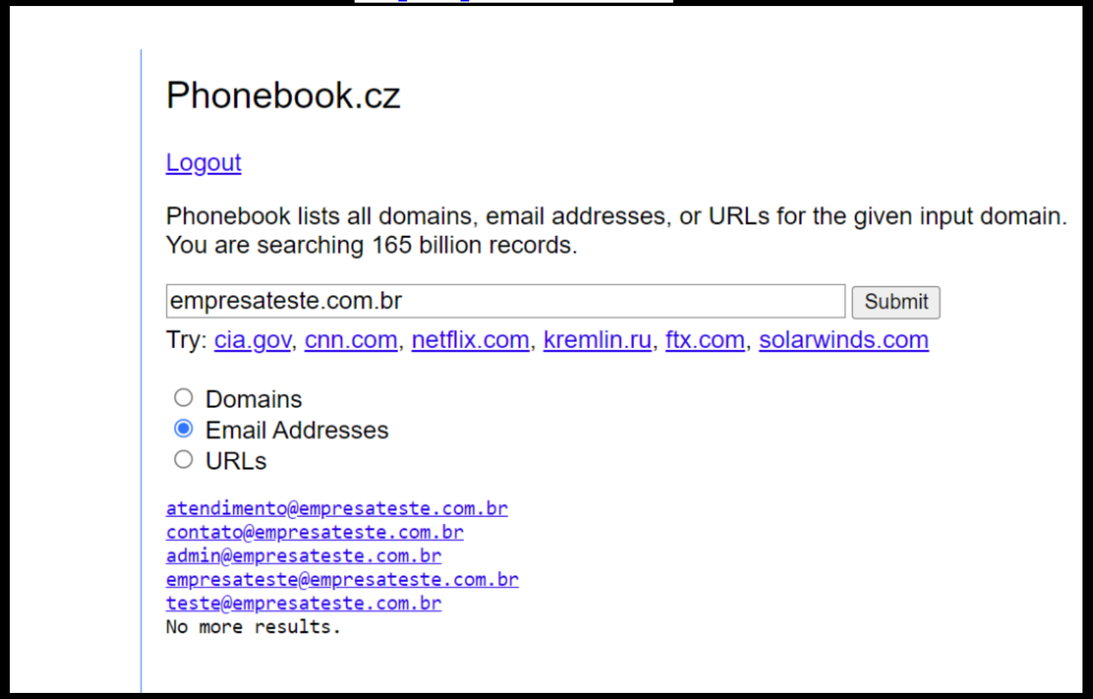




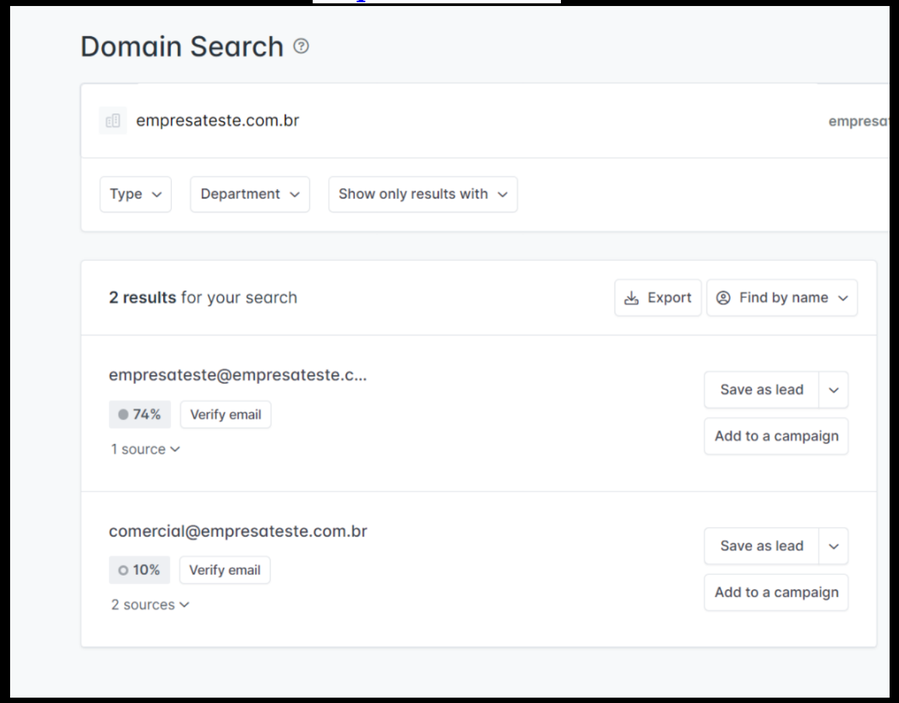
Enumeração de e-mails

Ferramentas

https://phonebook.cz



https://hunter.io



500apps Finder.io

RocketReach

MALTEGO

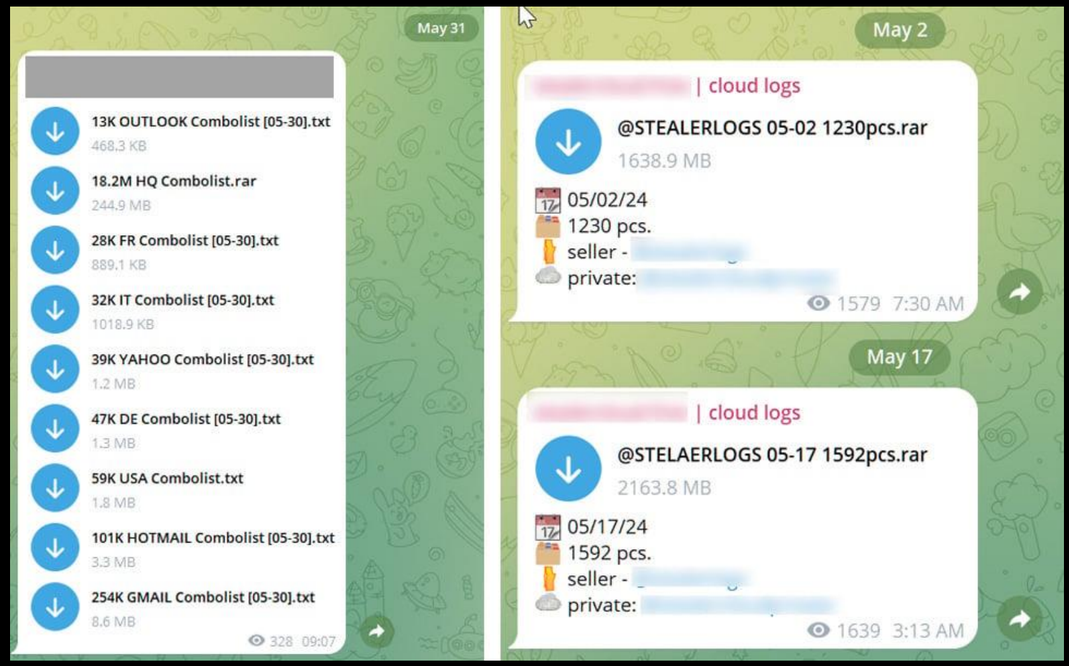
https://mundotecnologico.net/2024/04/04/tecnicas-de-enumeracao-de-e-mails/

Enumeração de e-mails e credenciais

Ferramentas

Breach Forum

BF



Stealer

Validação de e-mails

Office 365

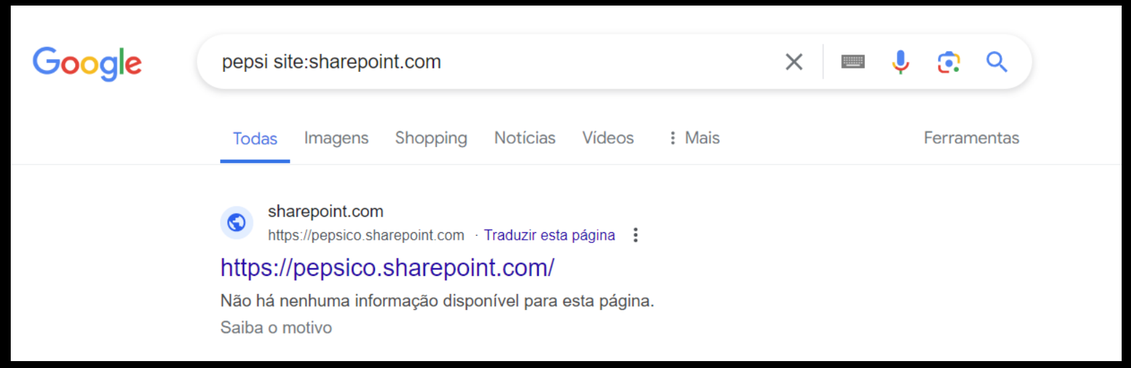
https://<tenantname>-my.sharepoint.com/personal/<your_user_name>/_layouts/15/onedrive.aspx

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



https://<tenant>-my.sharepoint.com/personal/<your_username>/_layouts/15/onedrive.aspx

PHISHING

Dominio


DEPOIS DE INSTALAR O KALI
E CRIAR UM E-MAIL FALSO
MR. ROBOT

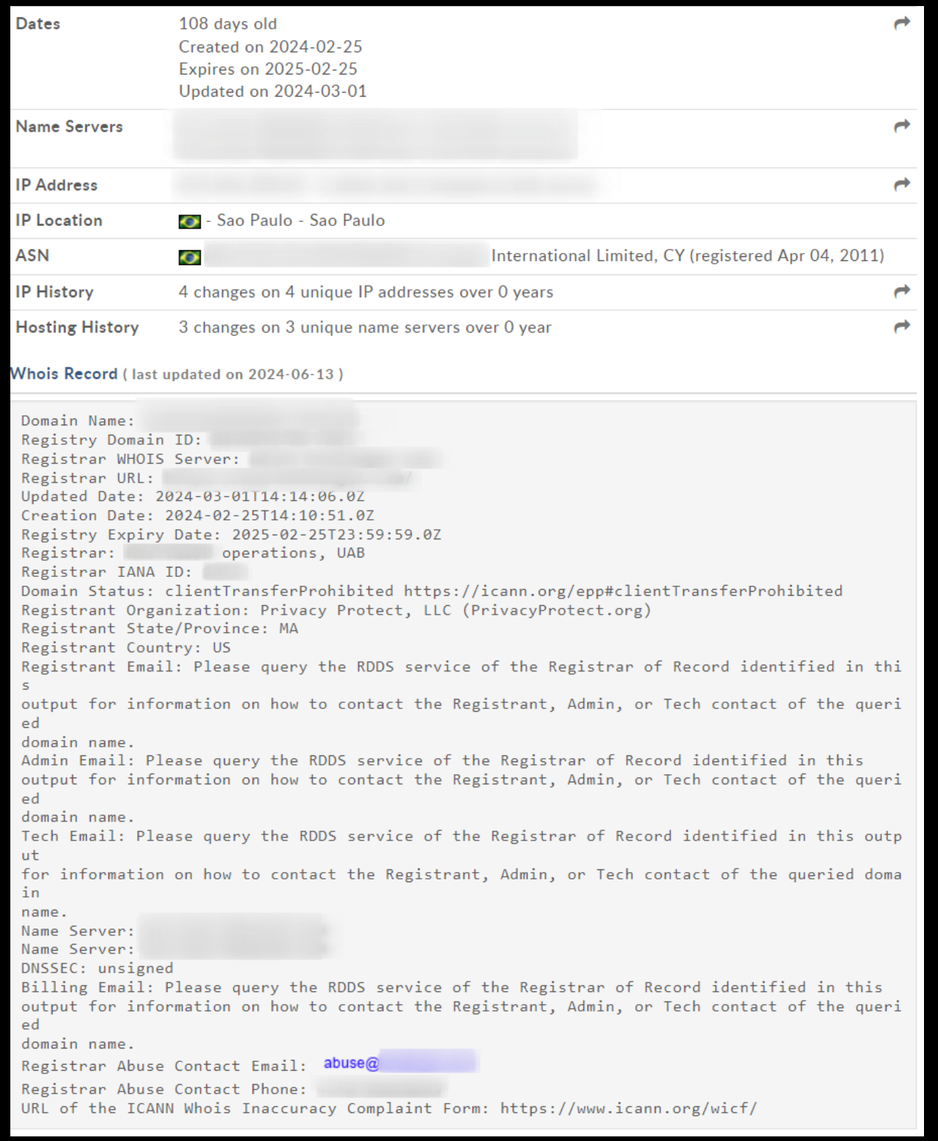

BYPASS NO ANTISPAM
DO OFFICE 365

E agora?

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



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

Whois Record (last updated on 2024-06-13)

```
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 thi
s
output for information on how to contact the Registrant, Admin, or Tech contact of the queri
ed
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 queri
ed
domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this outp
ut
for information on how to contact the Registrant, Admin, or Tech contact of the queried doma
in
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 queri
ed
domain name.
Registrar Abuse Contact Email: abuse@
Registrar Abuse Contact Phone:
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

PHISHING

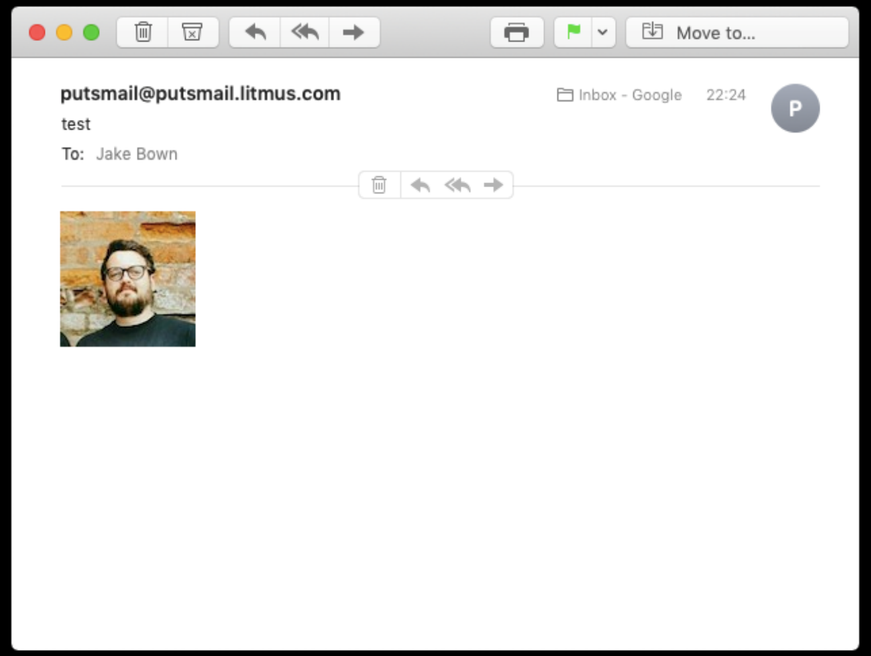
E-mail

- 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

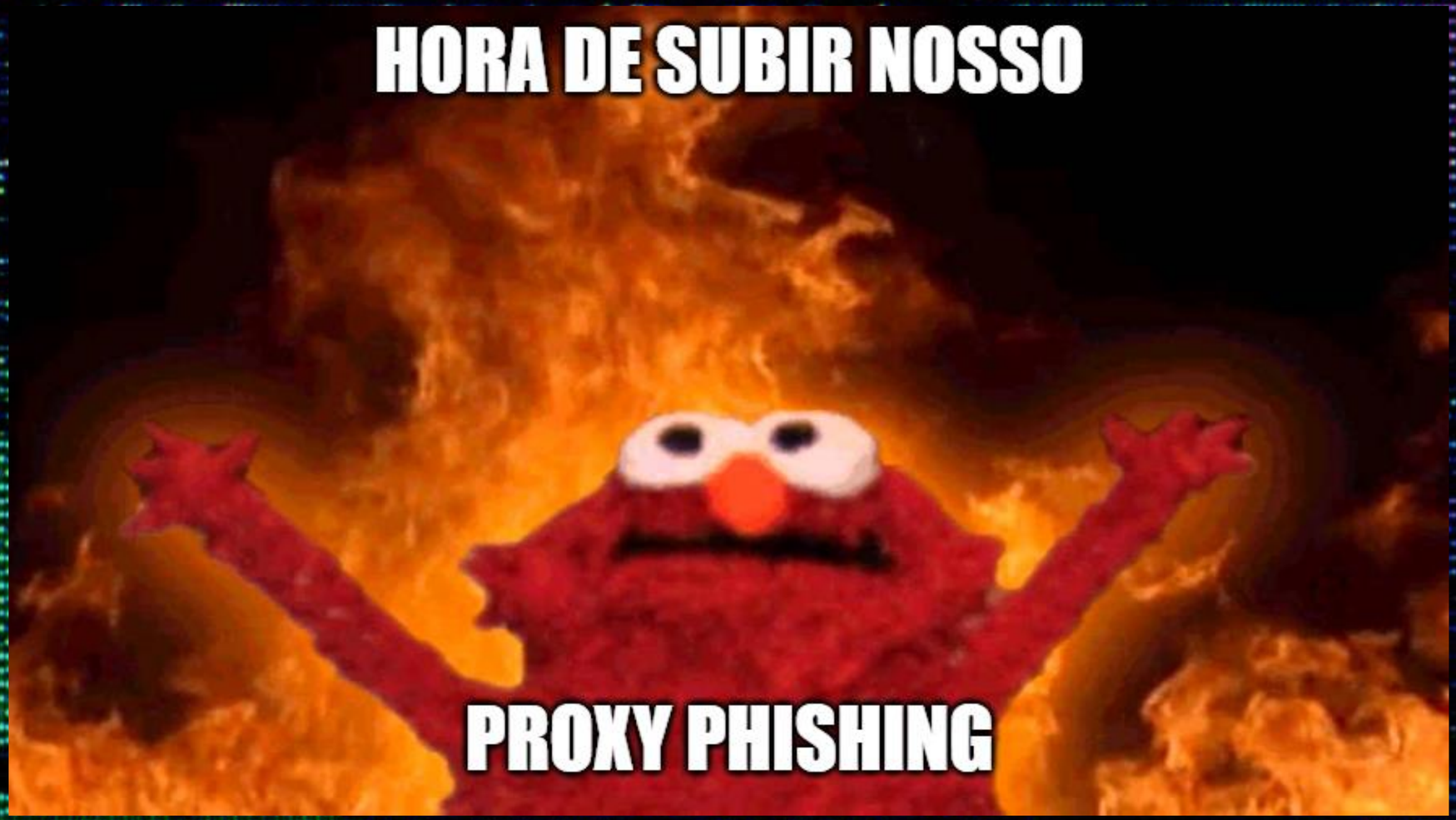
- Evitar o uso de imagens no e-mail, office 365 bloqueia o carregamento de imagem externa
- Enviar de preferência de 500 em 500 e-mails
- Enviar de remetente gmail.com costuma passar tranquilo
- Se for usar domínio customizado, utilize Mailchimp para disparo ou faça um google workspace trial
- Não enviar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



PHISHING

E-mail

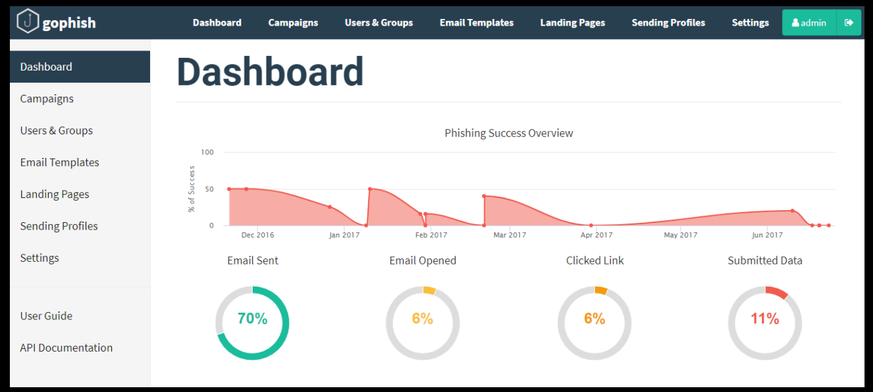
- Não usar redirects ou encurtadores comuns como hyperlink (não adianta!). Não usar de maneira alguma bit.ly
- Não passar a URL do phishing pura por e-mail ou teams antes da campanha
- Usar encurtador com ação de usuário para completar redirect (Ex:clique para continuar) ou usar encurtador com bloqueio 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*

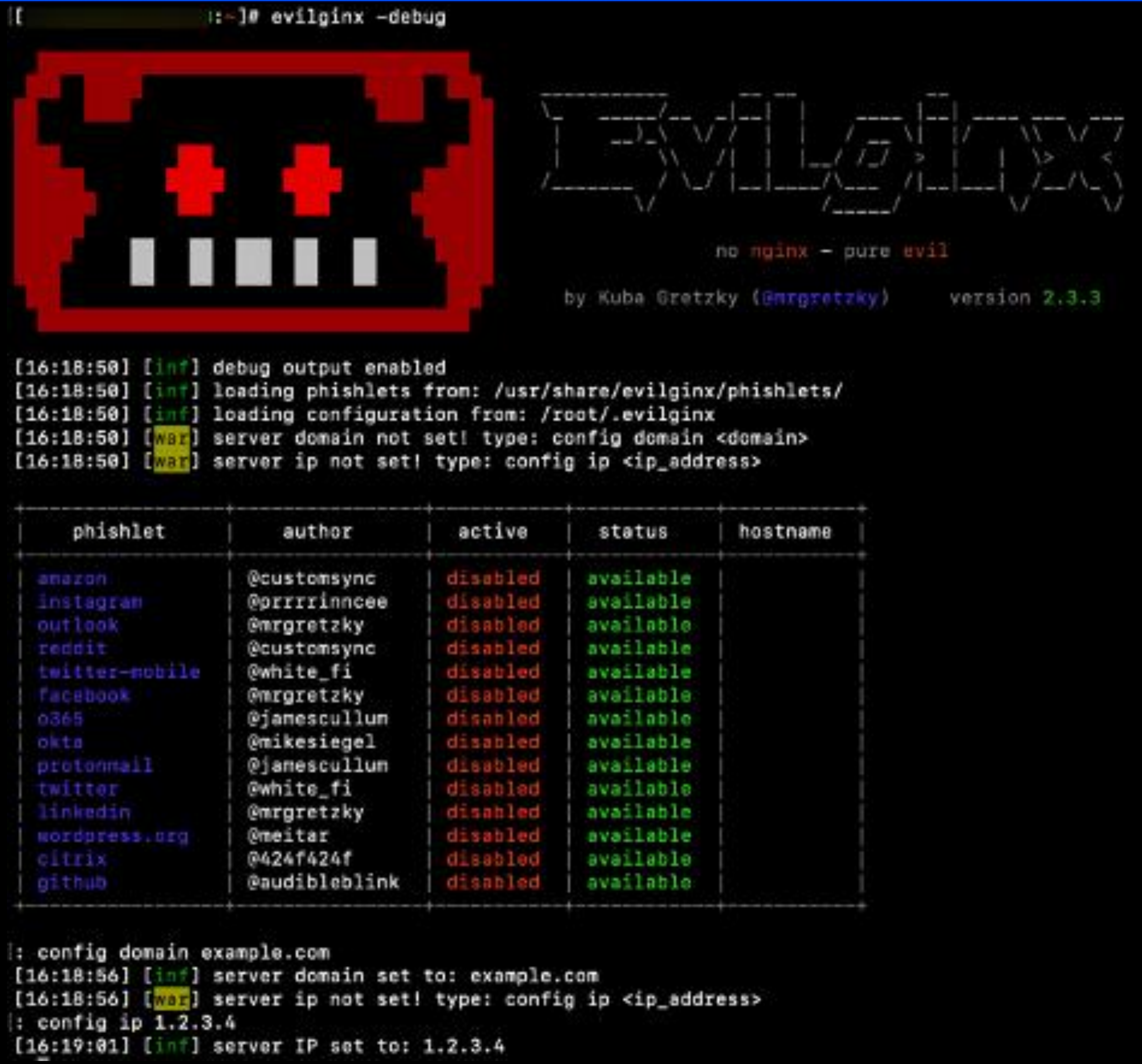
Evilginx

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*

Documetanção: *https://github.com/An0nUD4Y/Evilginx2-Phishlets*

Evilginx


[[redacted]:~]# evilginx -debug
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 | @prrrrinncee | 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?


BBB
CALMA AÍ
CALABRESO

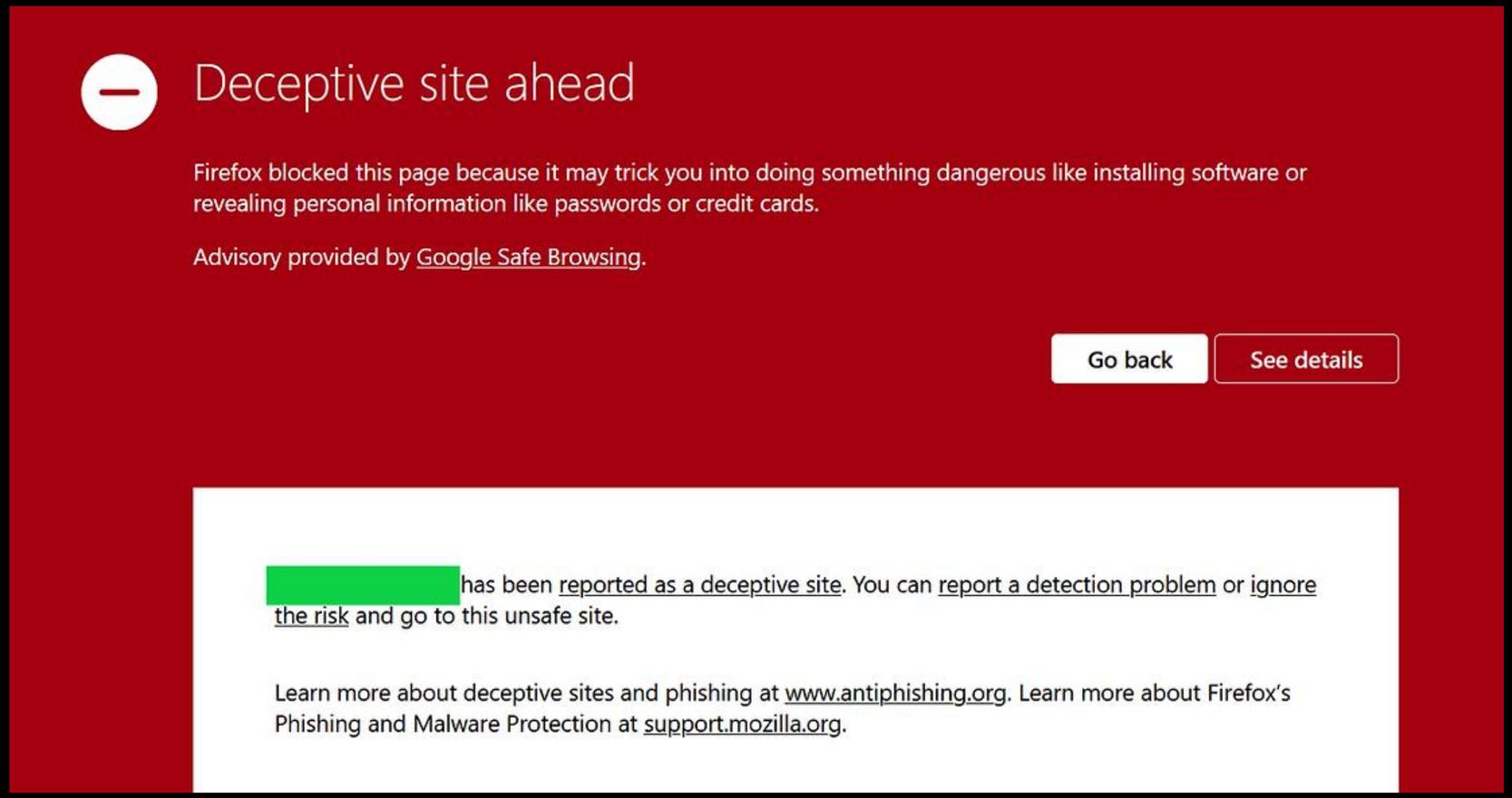
Evilginx

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



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

AmazonLightsail

FREE:

3 meses grátis (750 horas por mês)

Ponto positivo:

- Fácil de navegar
- Dura mais tempo que os demais

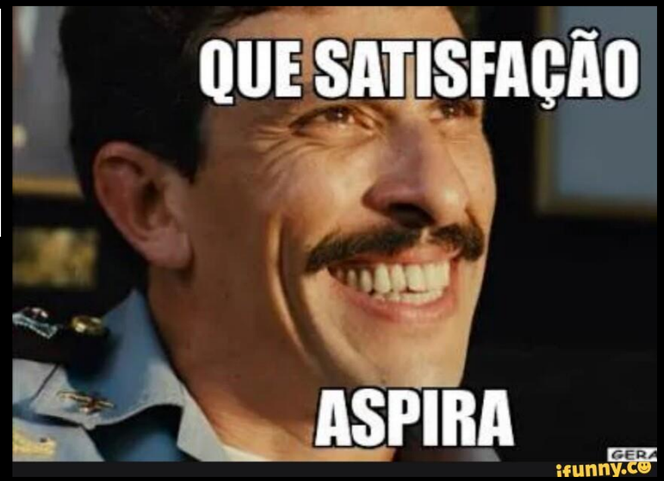
Ponto negativo:

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

ORACLE CLOUD

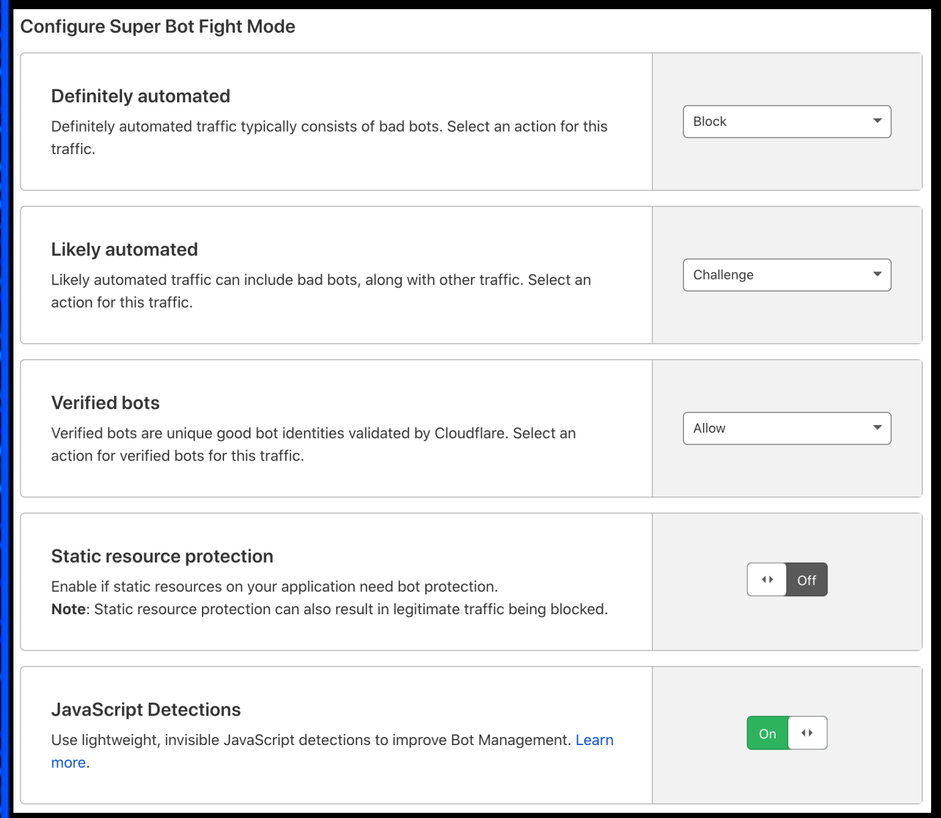
Ponto positivo:

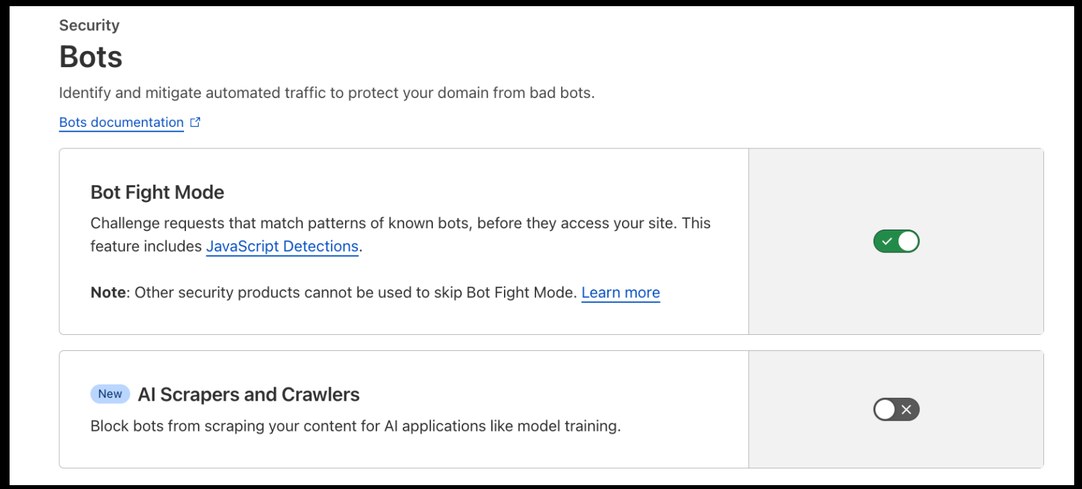
- Free eternamente
- Tem IP BR
- Terra de ninguém

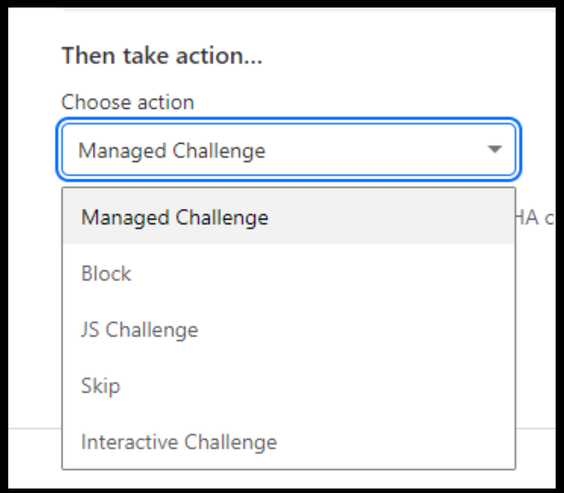


Evilginx

Google Safe Browsing Bypass

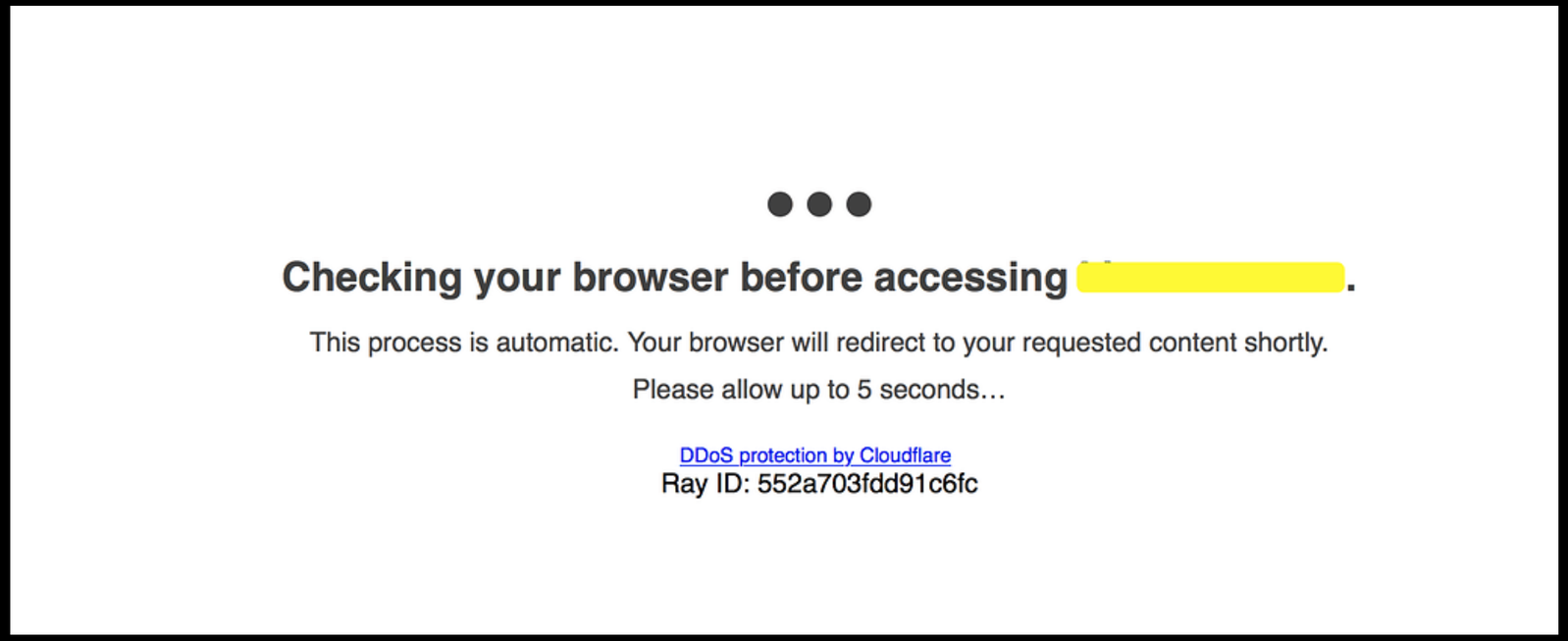


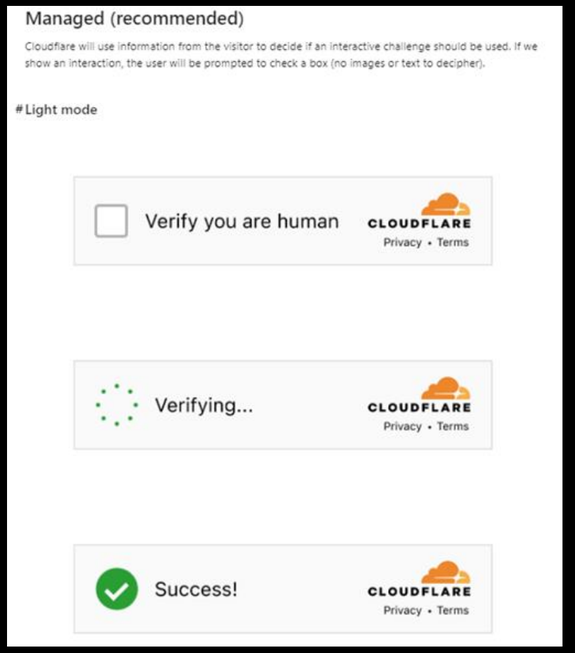




Evilginx

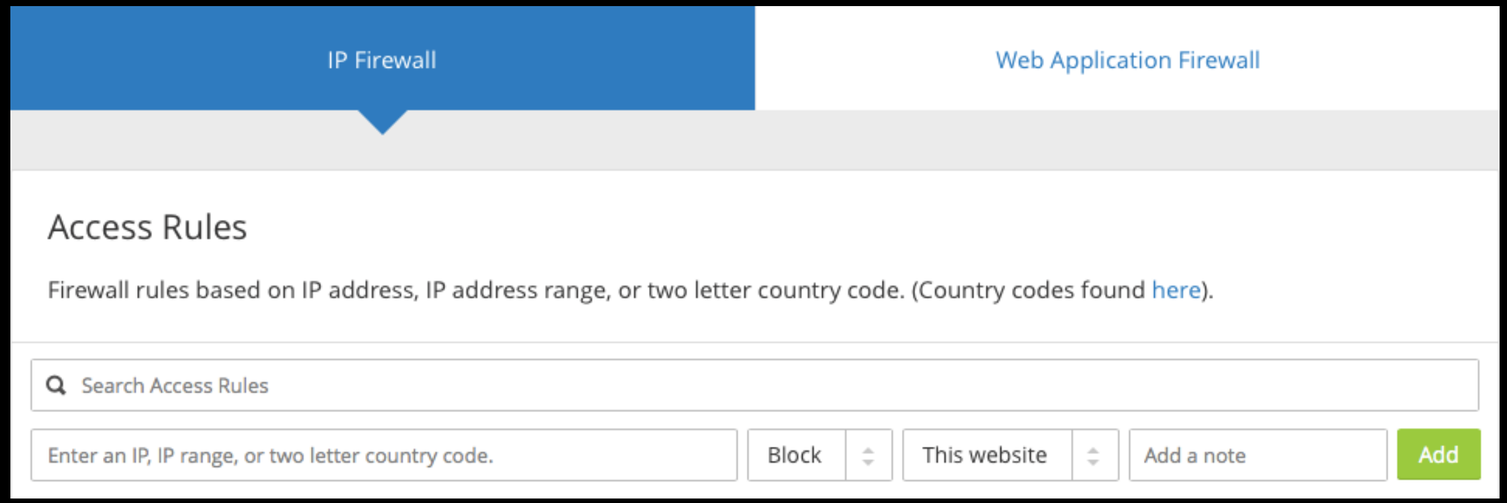
Google Safe Browsing Bypass

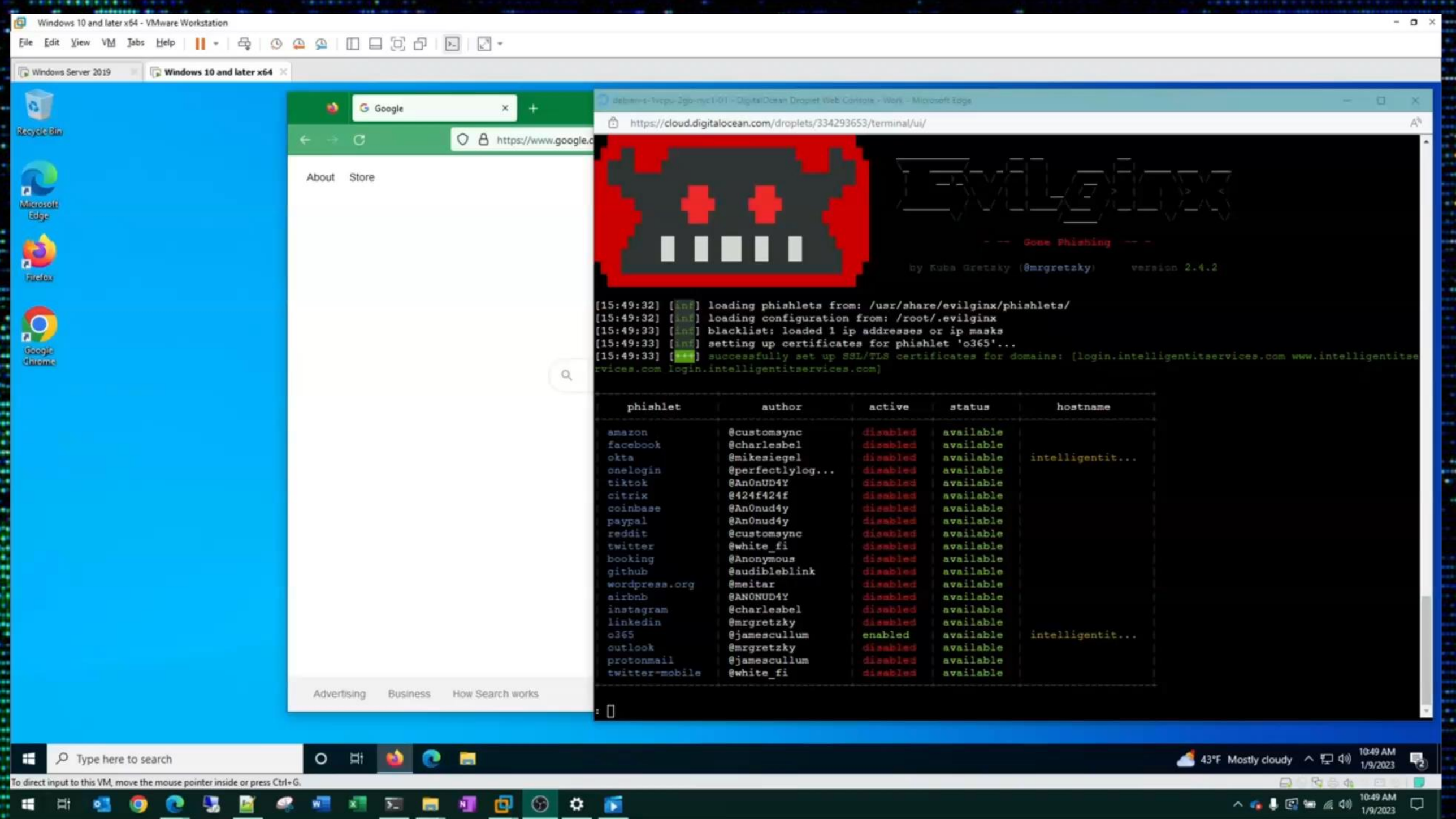




Evilginx

Bypass Other Security measures



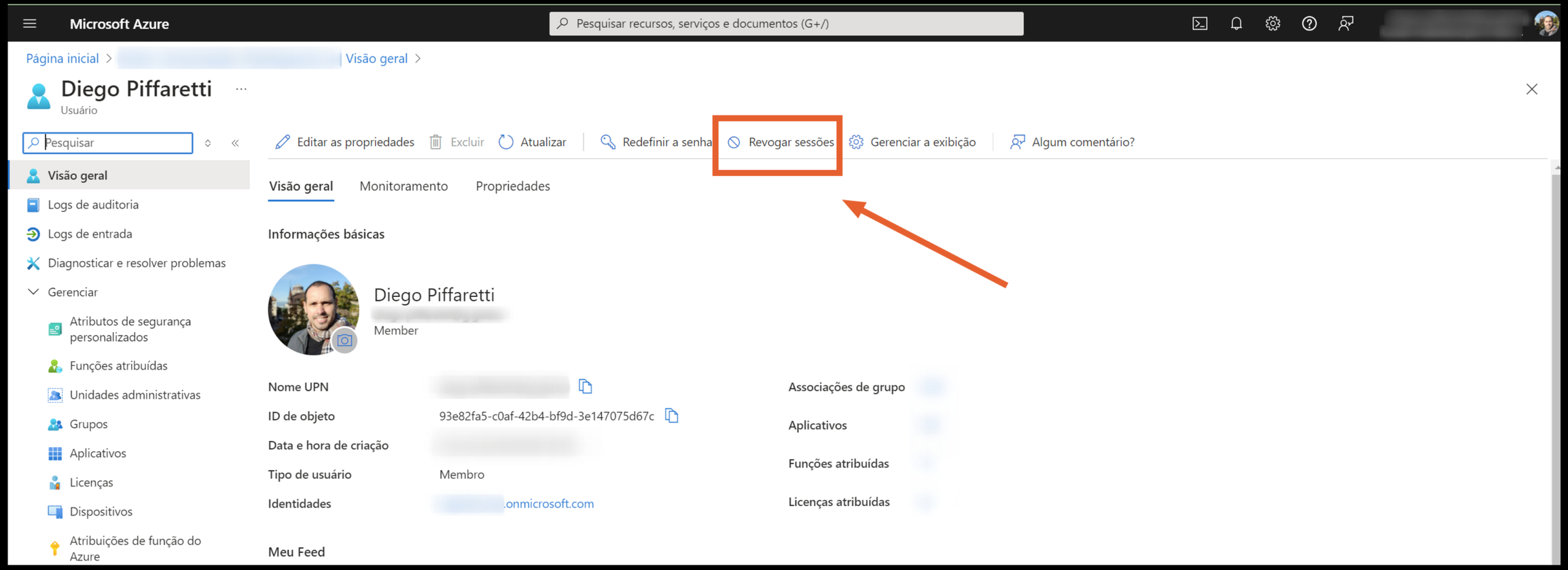

Windows 10 and later x64 - VMware Workstation
File Edit View VM Tabs Help
Windows Server 2019
Windows 10 and later x64
Recycle Bin
Microsoft Edge
Firefox
Google Chrome
Google
https://www.google.c
About Store
Advertising Business How Search works
https://cloud.digitalocean.com/droplets/334293653/terminal/ui/
Gone Phishing
by Kuba Gretzky (@mrgretzky) version 2.4.2
[15:49:32] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[15:49:32] [inf] loading configuration from: /root/.evilginx
[15:49:33] [inf] blacklist: loaded 1 ip addresses or ip masks
[15:49:33] [inf] setting up certificates for phishlet 'o365'...
[15:49:33] [+++] successfully set up SSL/TLS certificates for domains: [login.intelligentitservices.com www.intelligentitservices.com login.intelligentitservices.com]
phishlet author active status hostname
amazon @customsync disabled available
facebook @charlesbel disabled available
okta @mikesiegel disabled available intelligentit...
onelogin @perfectlylog... disabled available
tiktok @An0nUD4Y disabled available
citrix @424f424f disabled available
coinbase @An0nud4y disabled available
paypal @An0nud4y disabled available
reddit @customsync disabled available
twitter @white_fi disabled available
booking @Anonymous disabled available
github @audibleblink disabled available
wordpress.org @meitar disabled available
airbnb @AN0NUD4Y disabled available
instagram @charlesbel disabled available
linkedin @mrgretzky disabled available
o365 @jamescullum enabled available intelligentit...
outlook @mrgretzky disabled available
protonmail @jamescullum disabled available
twitter-mobile @white_fi disabled available
Type here to search
43°F Mostly cloudy
10:49 AM 1/9/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

DEFESA

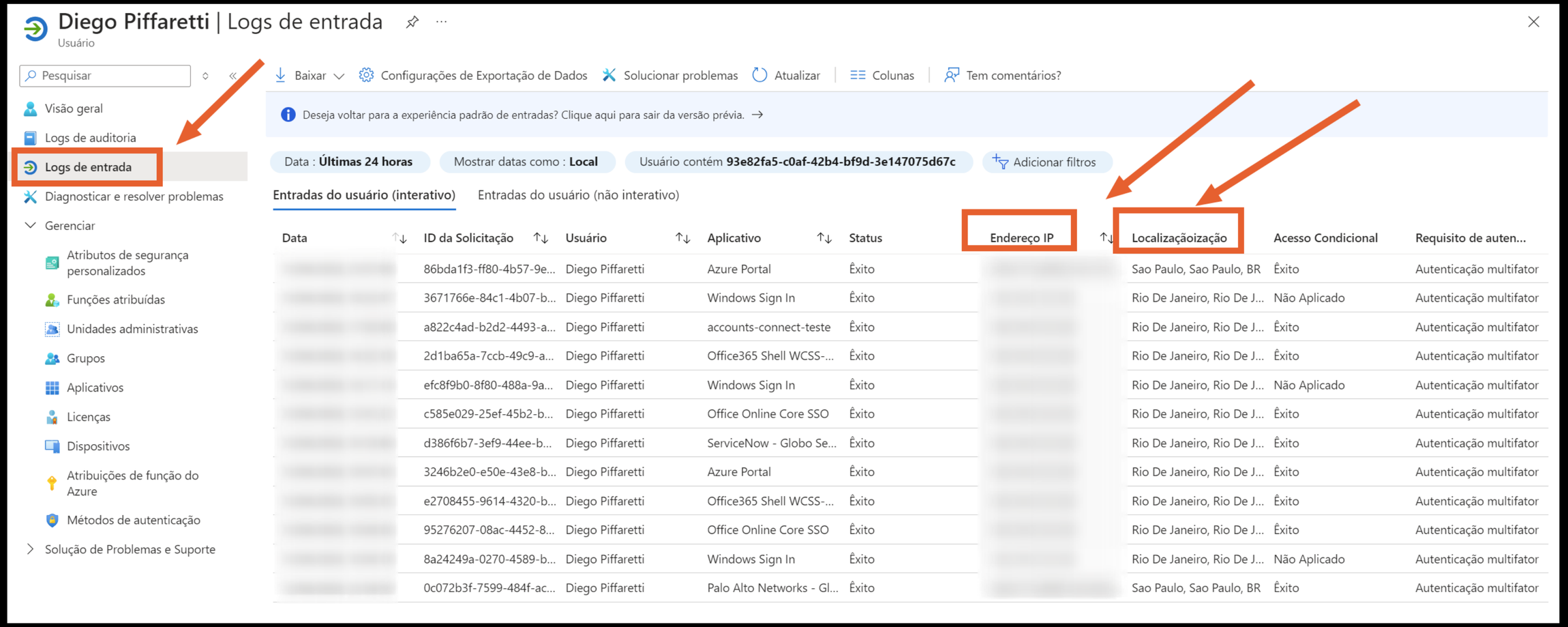
Ao perceber um ataque, o que fazer?

- 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

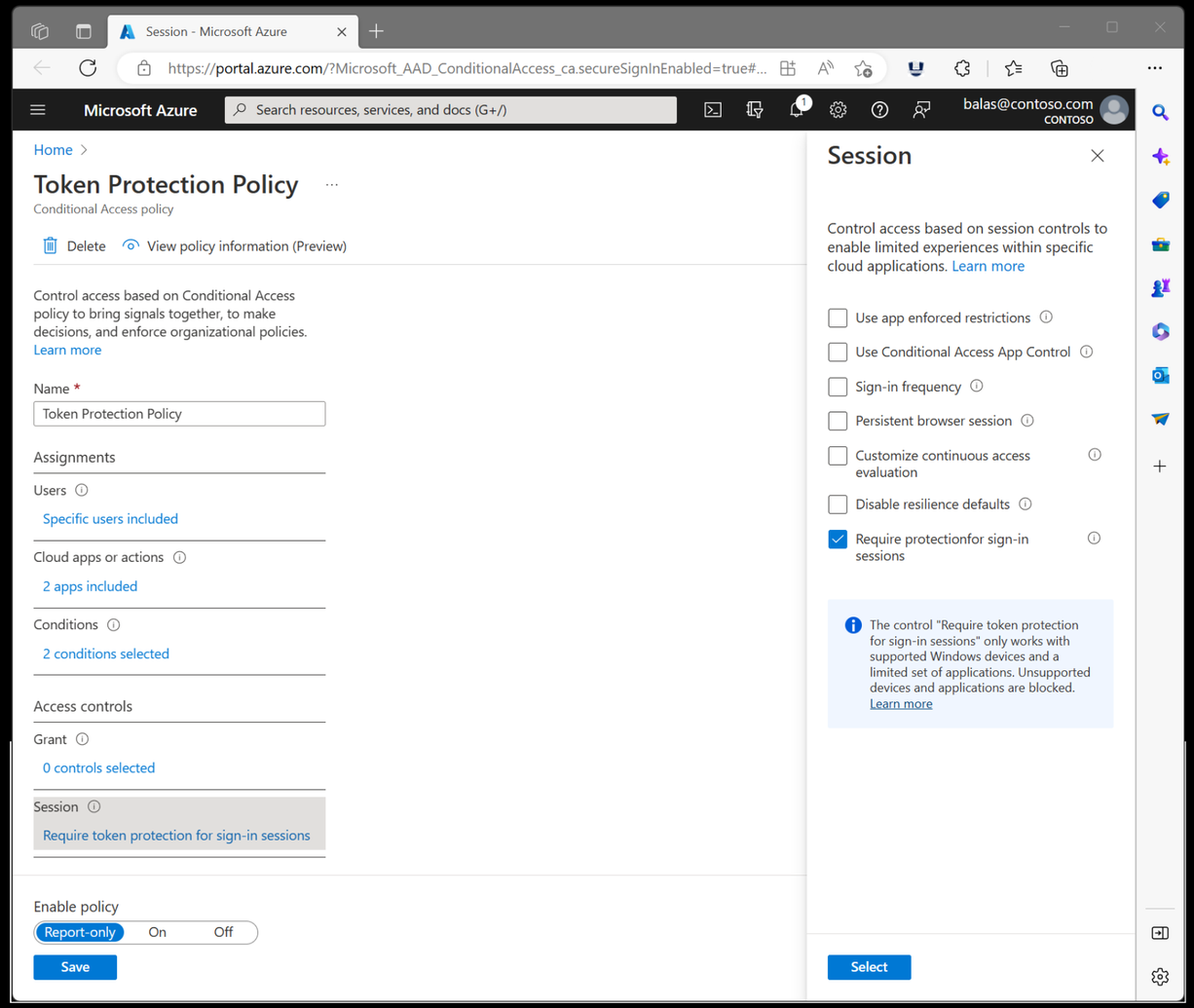
Ao perceber um ataque, o que fazer?

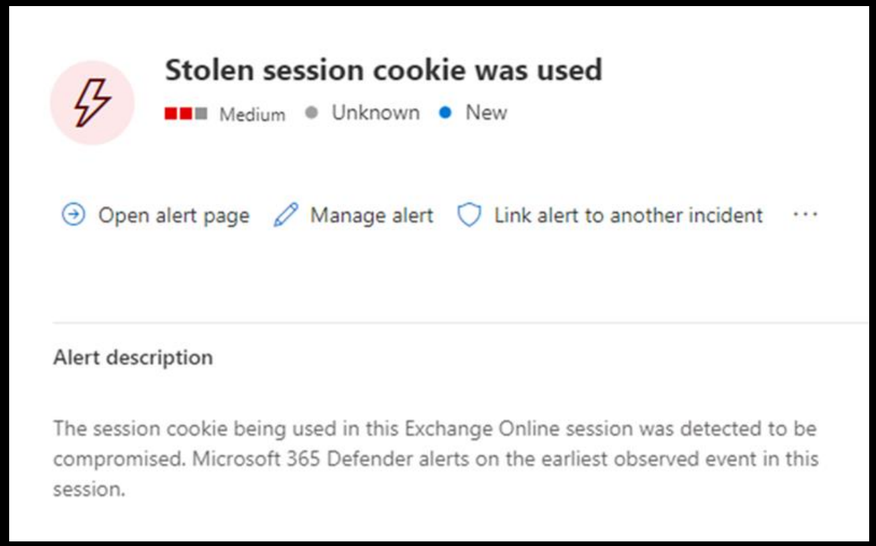


Ao perceber um ataque, o que fazer?

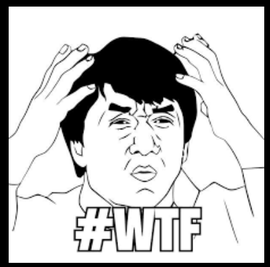


Conditional Access: Token protection (preview)





Desktop applications accessing Exchange Online and SharePoint Online on Windows

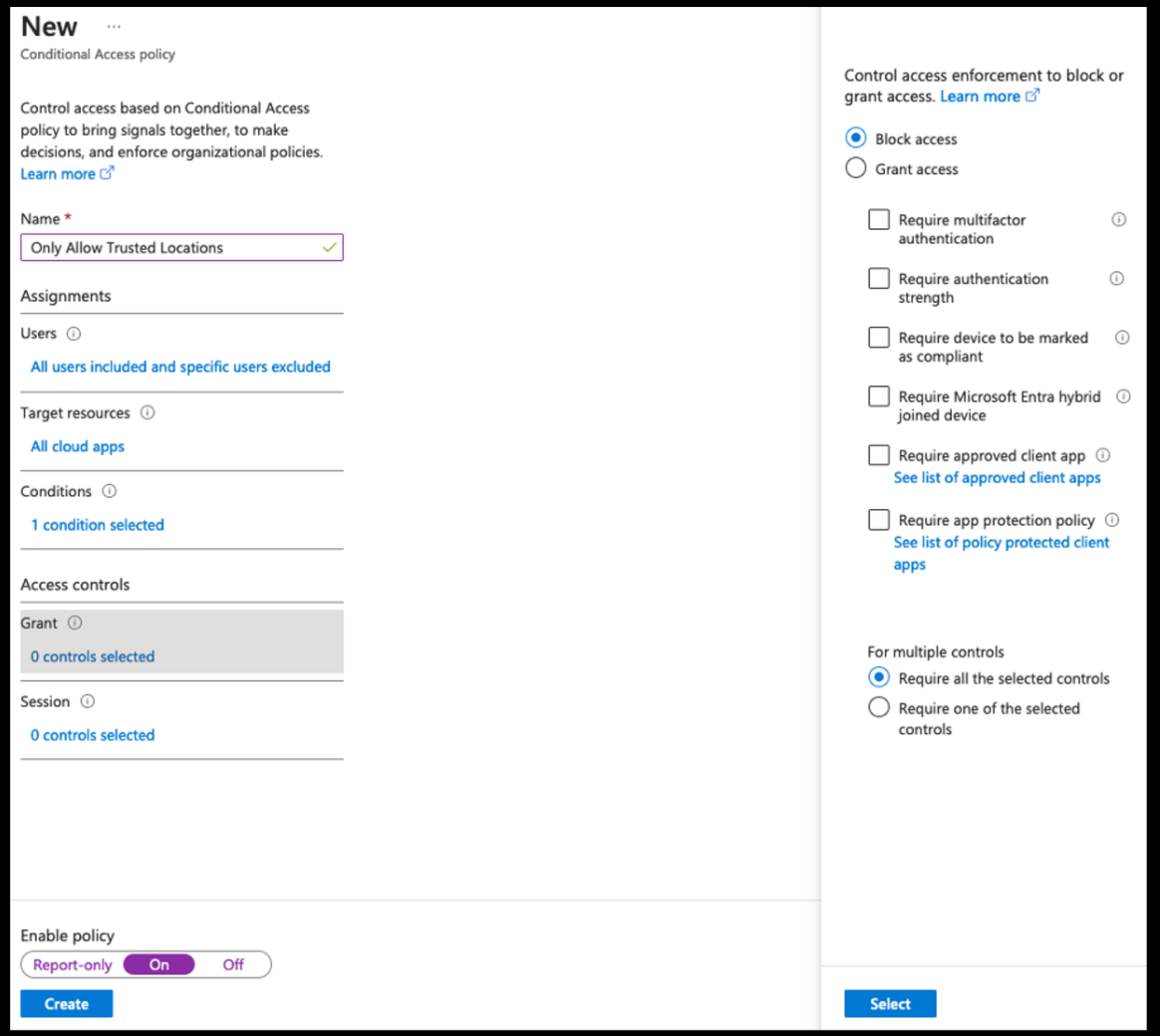


Conditional Access: Risk-based

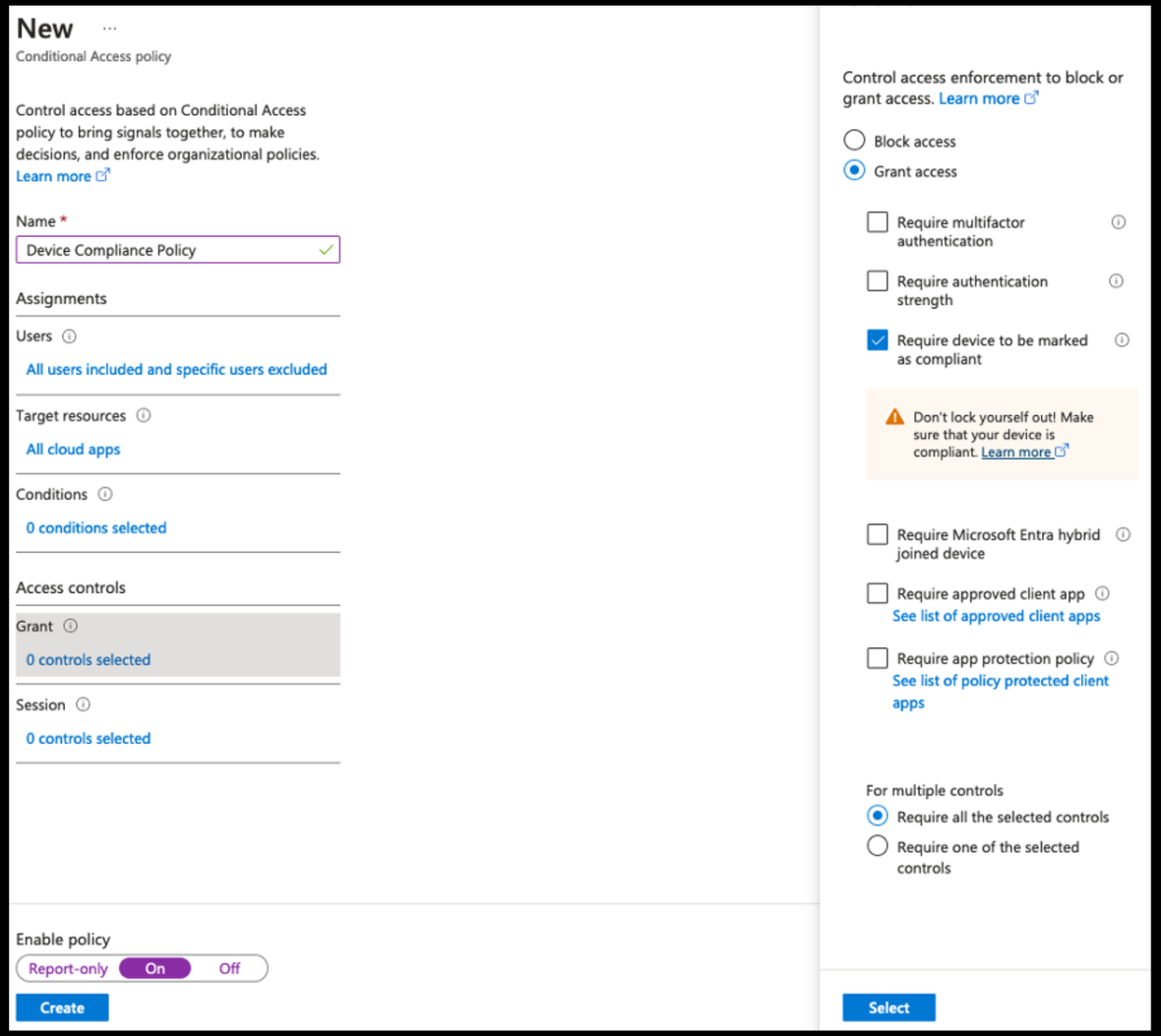
RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED
High	Offline	Users with leaked credentials	44 of 45
Medium	Real-time	Sign-ins from anonymous IP addresses	76 of 78
Medium	Offline	Impossible travels to atypical locations	11 of 14
Medium	Real-time	Sign-in from unfamiliar location	0 of 1
Low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

Necessário ter uma licença P2 da Microsoft ☹

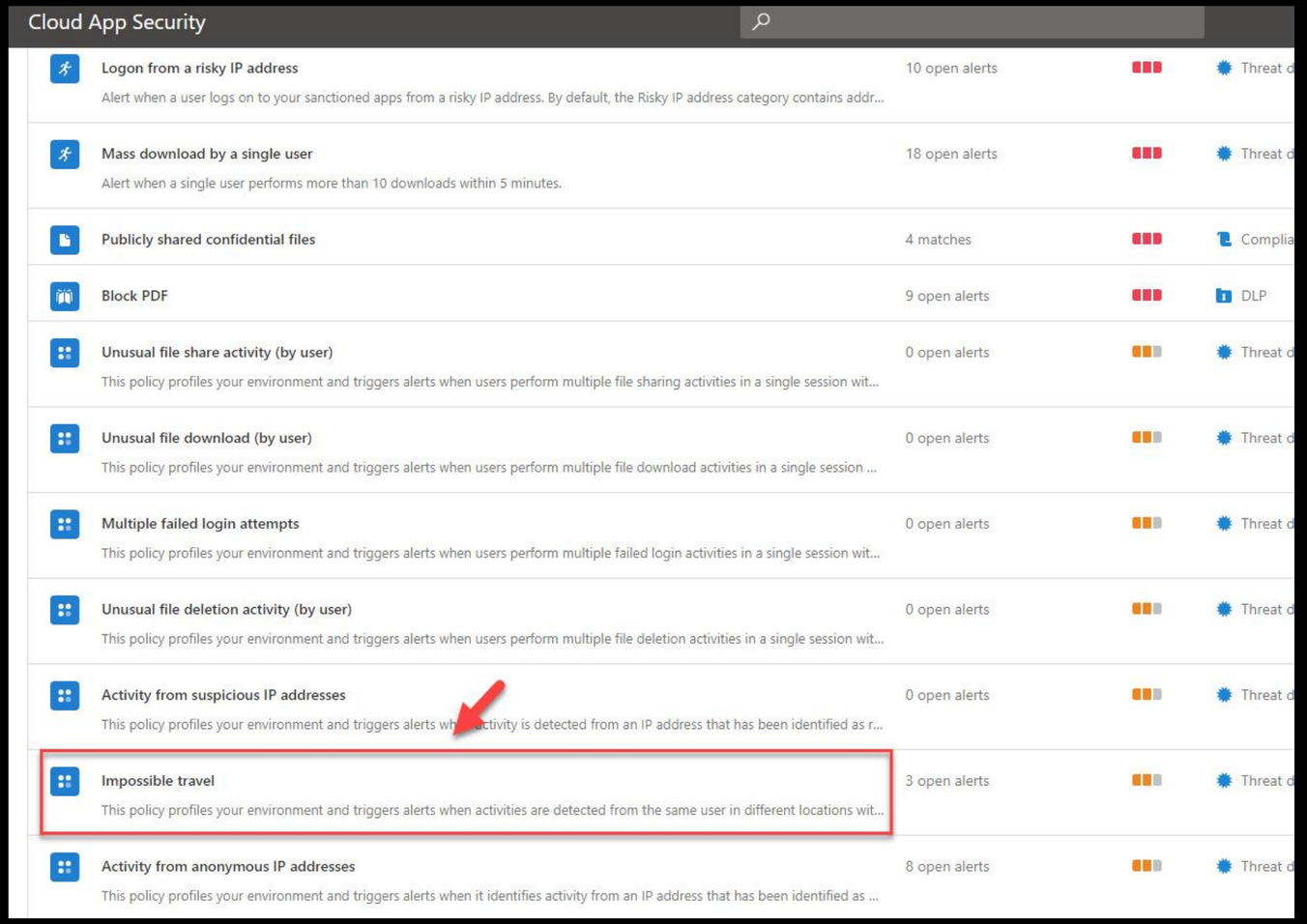
Conditional Access – Trusted Locations Only



Conditional Access – Intune Device Compliance



Defender – Impossible Travel



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

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

AiTM

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	✅
Require device to be marked as Hybrid Azure AD joined device	✅
Conditional Access Session Controls	❌ (limit time window when the attacker can use the session cookie)
Conditional Access Trusted Locations	✅

AiTM

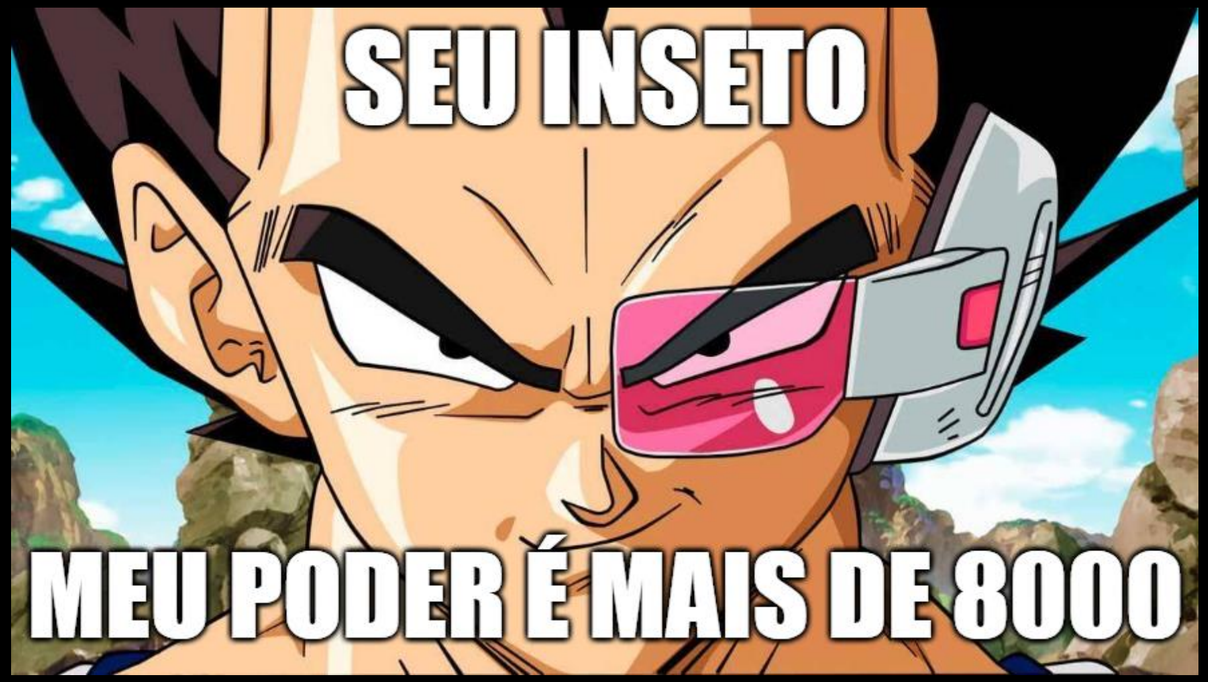
Status Proteções

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

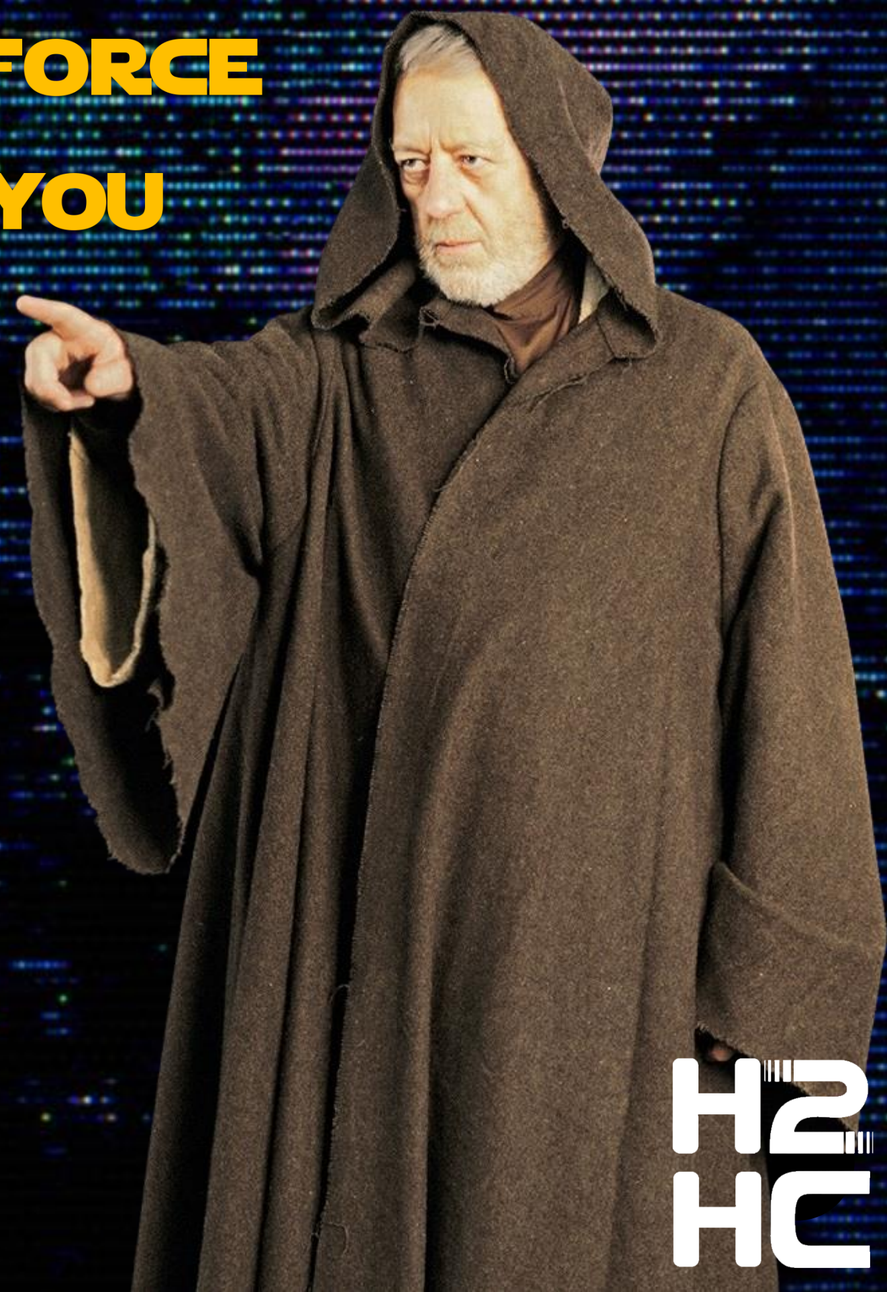
Microsoft

Google



OBRIGADO!

MAY THE FORCE
BE WITH YOU



linkedin.com/in/diegopiffaretti

Mundotecnologico.net

H2HC