



#GlobalAzure

#GABMUGPeru

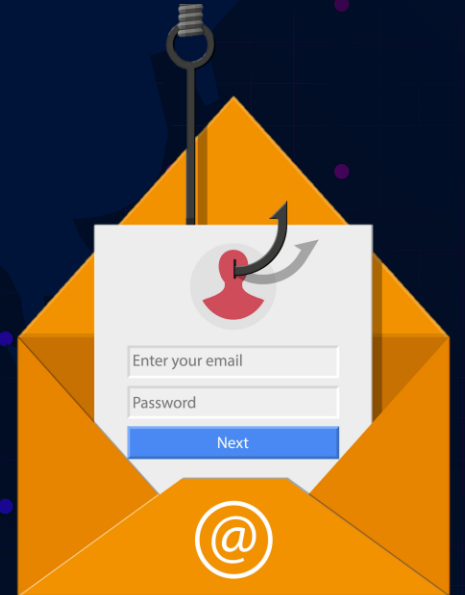
#GABMUGPeru

El futuro de los ataques de identidad

Jorge Castañeda



Microsoft MVP Security



#GlobalAzure

Ataques basados en la identidad - ¿históricos y actuales?

1. Sin MFA.
2. Sin identidad en la nube.
3. Sólo cuentas internas/VPN.
4. Password Spray attacks.
5. Fuerza bruta.
6. Phishing.
7. Robo de credenciales (sitio Pastebin)

= Fácil de vulnerar

Ataques basados en la identidad - ¿ahora y en el futuro?

1. Protección MFA.
2. Identidad en la nube / Identidad híbrida.
3. Basado en el riesgo/Riesgo de usuario e inicio de sesión/Inteligencia de amenazas/UEBA.
4. Políticas basadas en el inicio de sesión.
5. Password Spray attacks.
6. Fuerza bruta.
7. Phishing (Credenciales).

= Más difícil de vulnerar

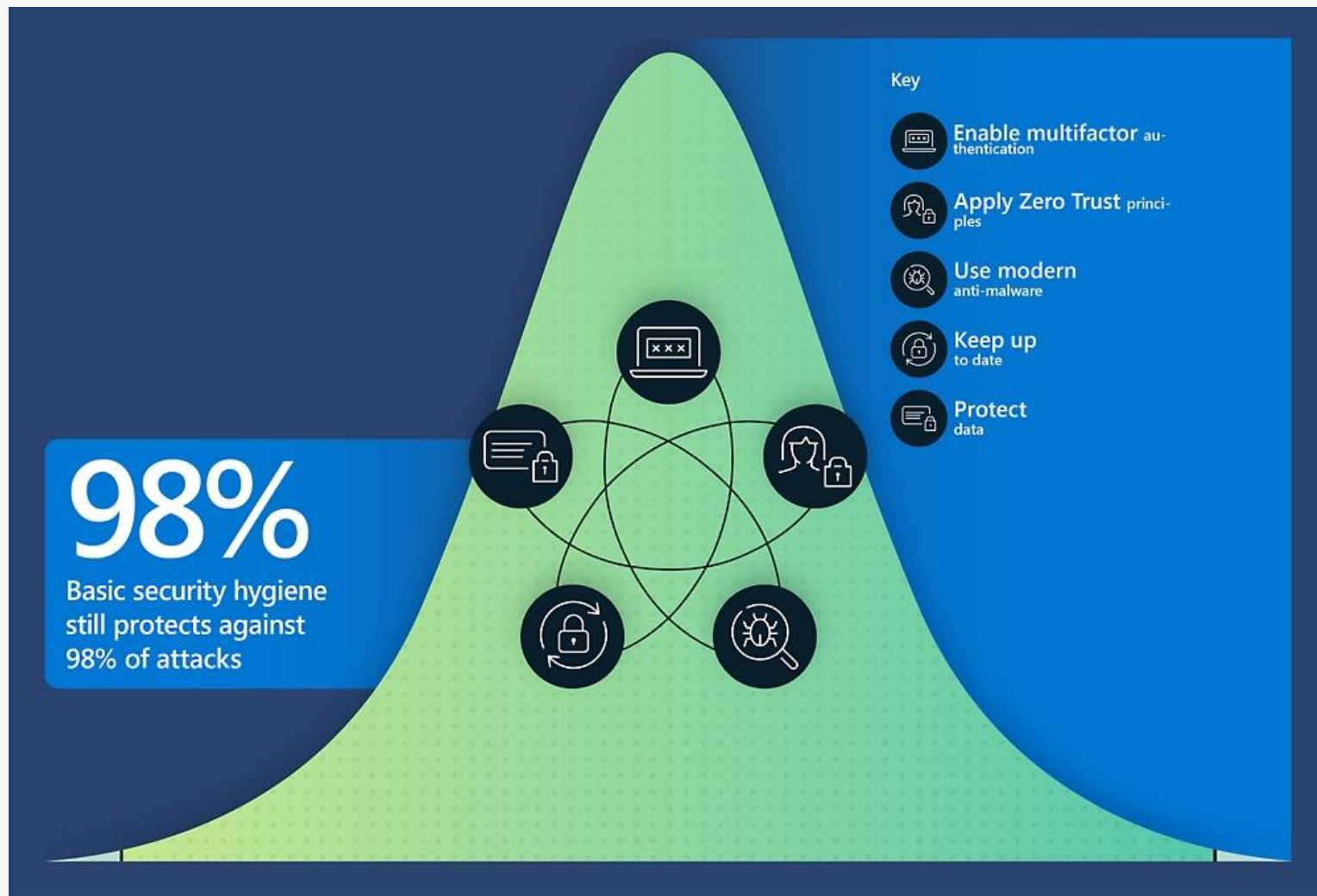
Ataques basados en la identidad - moderno/futuro

1. Consentimiento OAuth ataques de phishing
2. Cargas de trabajo de Azure AD / Principales servicios
3. MFA Spamming
4. Permisos API
5. Token de actualización principal (PRT)
6. Robo de token de dispositivo

= Ataques futuros

Flujo de protección

Protégase contra el 98% de los ataques utilizando antimalware, aplicando el acceso de mínimo privilegio, habilitando la autenticación multifactor y manteniendo las versiones actualizadas y protegiendo los datos. El 2% restante de la curva de campana incluye ataques atípicos.




Flujo de Ataque

Comienza con Reconocimiento.

1. Búsqueda en la web pública para obtener la información disponible.
2. ¿Cuenta habilitada en AzureAD / Office 365 Tenant?
3. Dirígete a usuarios sensibles (LinkedIn, redes sociales o sitios web)
4. Búsquedas de nomenclaturas conocidas.

Búsqueda en la Web pública para obtener la información disponible



Publicaciones

Personas

Empleos

Empresas

🔗 Bootcamp: Azure Administrator

This Github repo will be used for distributing content to participants joining our bootcamp. These files are required to complete the hands-on labs.

These files **do not** contain any copyrighted contents.

For questions please contact me.

- jorgec@itdemos.com

Domain Search ⓘ

itdemos.com

canvia.com 5 results ×

Filters ^

🔍

Type ▾

Department ▾

Show only results with ▾

5 results for your search

📄 Export


🔍 Find by name ▾

canaleticodirectorio@.....		Save as lead	1 source ▾
📌 79%			
contactanos@.....	Support	Save as lead	5 sources ▾
📌 79%			
info@.....	Support	Save as lead	8 sources ▾
📌 79%			
marketing@.....	Marketing	Save as lead	1 source ▾
📌 78%			

Company

^

itdemos.com



Email pattern: {f}{l}ast@ itdemos.com

Accept all: **YES** ⓘ

Industry: Technology

Technologies

▾

OSINT

Open Source Intelligence

1. Maltego
2. Usersearch.org
3. DorkSearch
4. SpiderFoot
5. BuiltWith
6. DarkSearch.io
7. Grep.app
8. Recon-ng
9. Shodan
10. Metagoofil
11. Searchcode
12. Wigle
13. Whatsmyname
14. Dnsdumpster

Automatizar el descubrimiento

```
(xorxe@kali)-[~/crosslinked]
$ python3 crosslinked.py -f '{first}.{last}@[redacted].com' [redacted]

CrossLinked (x) @m8sec v0.2.1

[*] Searching google, bing for valid employee names at "[redacted]"
[*] 100 https://www.google.com/search?q=site:linkedin.com/in+"[redacted]"&num=100
&start=0 (200)
[*] 199 https://www.google.com/search?q=site:linkedin.com/in+"[redacted]"&num=100
&start=100 (200)
[*] 299 https://www.google.com/search?q=site:linkedin.com/in+"[redacted]"&num=100
&start=199 (200)
[*] 314 https://www.google.com/search?q=site:linkedin.com/in+"[redacted]"&num=100
&start=299 (200)
[*] 314 https://www.google.com/search?q=site:linkedin.com/in+"[redacted]"&num=100
&start=314 (200)
[*] 314 https://www.google.com/search?q=site:linkedin.com/in+"[redacted]"&num=100
&start=314 (200)
[*] 314 https://www.google.com/search?q=site:linkedin.com/in+"[redacted]"&num=100
&start=314 (200)
[*] 0 http://www.bing.com/search?q="[redacted]"&site:linkedin.com/in&first=0 (2
```

Descubrir cuentas activas

```
(xorxe@kali) - [~/Desktop/o365creeper-ng]
$ python3 o365creeper-ng.py -f names.txt -o validitdemos.txt
```

```
- VALID
- VALID
- INVALID
- VALID
- VALID
- VALID
VALID
- VALID
- VALID
INVALID
- VALID
- VALID
VALID
LID
ALID
- VALID
INVALID
- VALID
ALID
VALID
VALID
- TNVALID
- INVALID
INVALID
VALID
```

```
(xorxe@kali)[~/Desktop/Uh0h365]
$ python3 Uh0h365.py /home/kali/Desktop/o365creeper-ng/valid.txt
```

[illegible]

Identity **Attack** Man-in-the-middle using **evilginx2**



¿De qué se trata?

1. Escrito en Go
2. Proxy inverso Man-in-the-middle
3. Proxy del sitio web al usuario.
4. Captura nombre de usuario y contraseña.
5. Captura las cookies de autenticación.
6. Captura el token de sesión (bypass 2FA).
7. Phislets predeterminados (O365, LinkedIn, Facebook).
8. Personalizable con phishlets personalizados.

Descargo de responsabilidad:

Evilginx proyecto se libera con fines educativos y sólo debe utilizarse en demostraciones o tareas legítimas de pruebas de penetración con el permiso por escrito de ser phished partes. El objetivo es demostrar que 2FA no es una bala de plata contra los intentos de phishing.

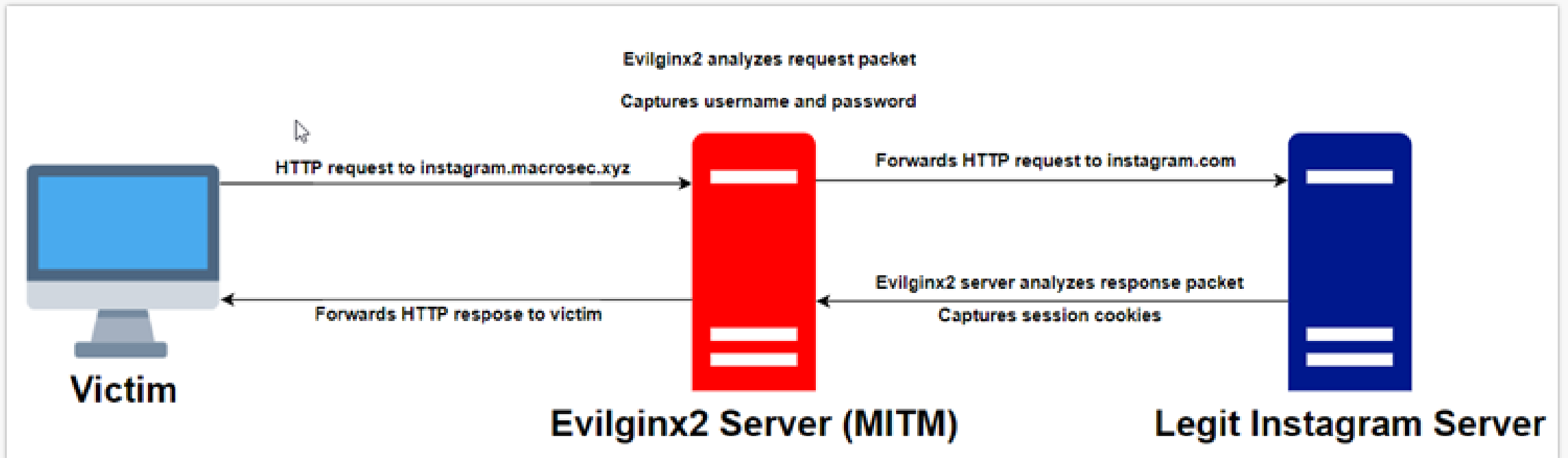


Eludir ataques/ limitaciones

- Derivación (Microsoft Authenticator App, MFA, 2FA)
- Sin éxito para Fido2/hardware tokens (YubiKey)
- Sin éxito en eludir las capacidades MFA junto con el Acceso Condicional (Azure)
 - Afiliación a dominios, afiliación a AD
 - Cumplimiento de MEM
 - Inscripción de dispositivos
 - Certificado
 - Control de aplicaciones de acceso condicional
 -

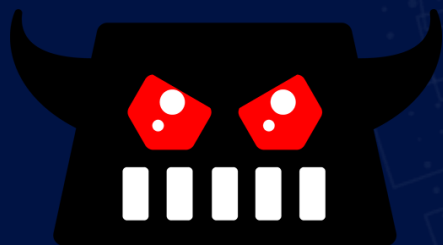
¿Cómo funciona?

Eludir ataques/ limitaciones



#GABMUGPeru

Demo



#GlobalAzure

Microsoft Defender for Endpoint

Resultado final (Tiempo 1-2 horas)

Alerts > Potential phishing web site

ⓘ

The MDE SIEM API deprecation that was announced earlier this year has been postponed for now, more details expected in Q3, 2022.

ⓘ

Part of incident: Potential phishing web site on one endpoint. [View incident page](#)

vm-pc-win05

Risk level

■

■

■

 High

⋮

Windows10

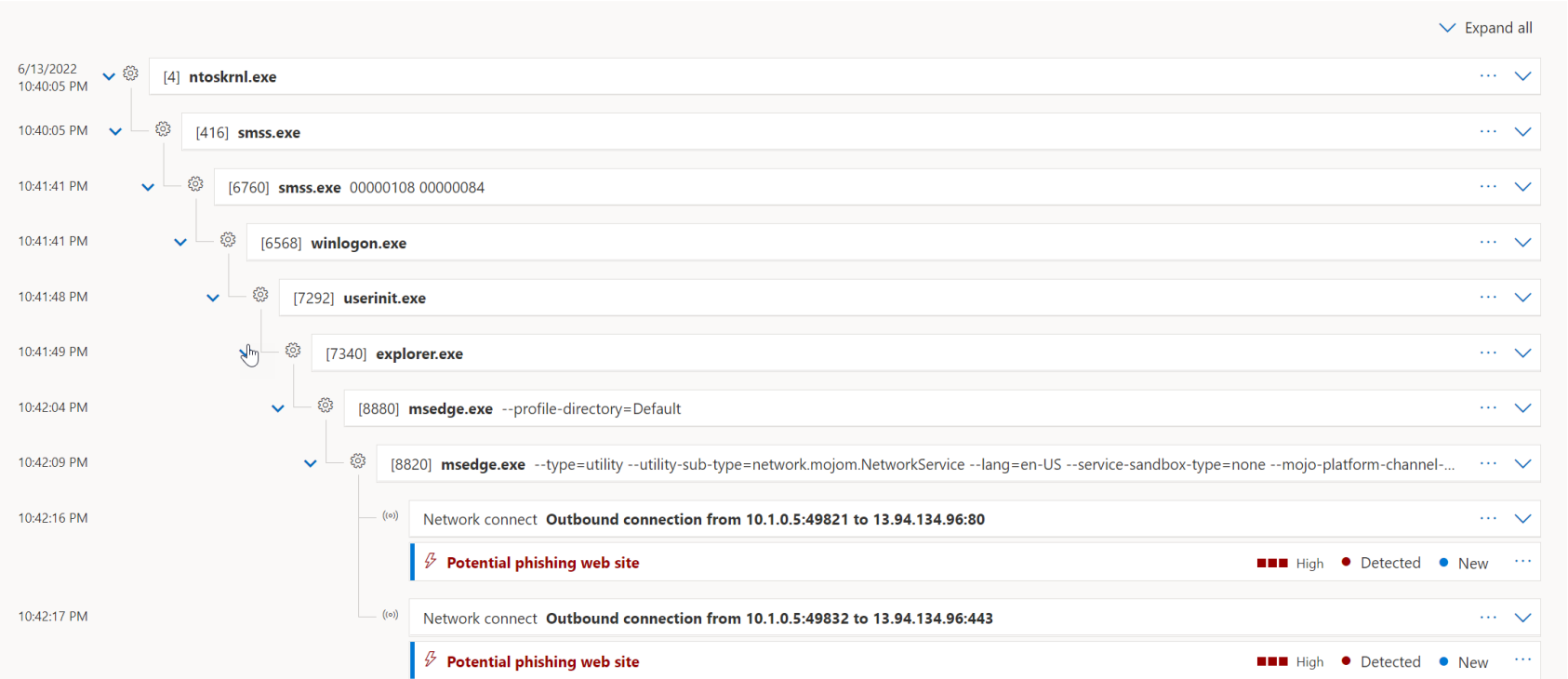
MDE-Management

+1

vm-pc-win05\azureuser

⋮

ALERT STORY



⚡

Potential phishing web site

■

■

■

 High

●

 Detected

●

 New

[Manage alert](#) [See in timeline](#) [Create suppression rule](#) ⋮

Details Recommendations

INSIGHT

Quickly classify this alert

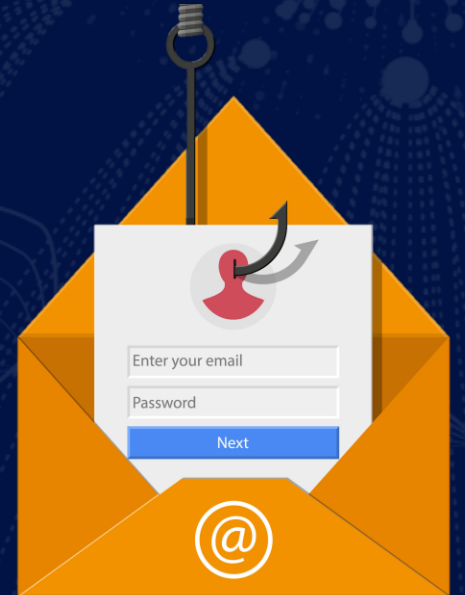
Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state	
Classification	Assigned to
Not Set	Unassigned
Set Classification	
Alert details	
Category	MITRE ATT&CK Techniques
Credential access	-
Detection source	Service source
EDR	Microsoft Defender for Endpoint
Detection status	Detection technology
● Detected	Behavior,Network,ThreatIntelligence

#GABMUGPeru


Identity **Attack** Consent Phishing




#GlobalAzure

Ataque de identidad OAuth

Phishing de consentimiento

 Microsoft Security Intelligence
@MsftSecIntel

Microsoft is tracking a recent consent phishing campaign, reported by @ffforward, that abuses OAuth request links to trick users into granting consent to an app named 'Upgrade'. The app governance feature in Microsoft Defender for Cloud Apps flagged the app's unusual behavior.

 **App with suspicious OAuth scope was flagged high-risk by Machine Learning model, made graph calls to read email and created Inbox Rule**
Medium • Unknown • New

[Manage alert](#) [Link alert to another incident](#) [Consult a threat expert](#)

☐ Classify this alert ☒ True alert ☐ False alert

This detection identifies an OAuth App that was flagged high-risk by Machine Learning model that consented to suspicious scopes, creates a suspicious inbox rule, and then accessed users mail folders and messages through the Graph API. Inbox rules, such as forwarding all or specific emails to another email account, and Graph calls to access emails and send to another email account, may be an attempt to exfiltrate information from your organization.

3:26 PM · Jan 21, 2022 · Twitter Web App

 Trending Innovation Security Business Finance Education Home & Office More

MUST READ: [Want a happy team at work? Make sure you don't forget this vital ingredient](#)

Microsoft warns about this phishing attack that wants to read your emails

Attackers have targeted hundreds of organisations, says Microsoft security.

 Search Developer 5G Security Cloud Artificial Intelligence More Newsletters Forums Resource Library

Microsoft warns organizations of consent phishing attacks

     by **Lance Whitney** in **Security**
on July 9, 2020, 10:21 AM PDT

In this type of phishing campaign, attackers trick people into giving a malicious app consent to access sensitive data, says Microsoft.

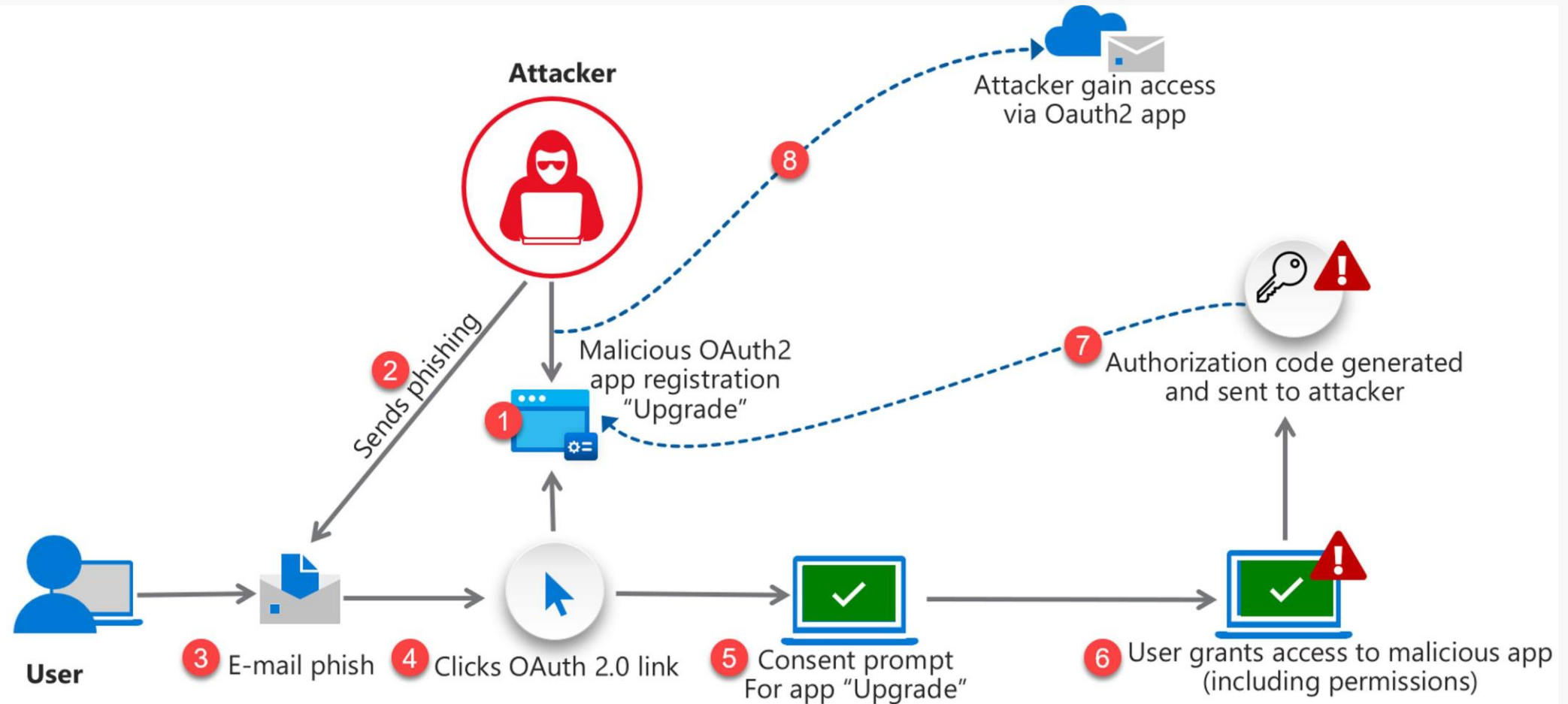


 Get up to speed with Azure with over 100 training for \$39

 Get unlimited access

Ataque de identidad OAuth

Phishing de consentimiento



Ataque de identidad OAuth

Phishing de consentimiento #1



Ataque de identidad Oauth

Phishing de consentimiento #2

Home > m365securitylabs > Update App

Update App | API permissions

Search (Ctrl+ /)

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as pa all the permissions the application needs. [Learn more about permissions and](#)

Add a permission

Grant admin consent for m365securitylabs

API / Permissions name	Type	Description
Microsoft Graph (4)		
TeamsActivity.Read.All	Application	Read all users' teamwork activity feed
TeamsActivity.Send	Application	Send a teamwork activity to any user
User.Read	Delegated	Sign in and read user profile
User.ReadWrite.All	Application	Read and write all users' full profiles

To view and manage permissions and user consent, try [Enterprise applications](#).

User.ReadWrite.All

Microsoft Graph

Remove permission

https://graph.microsoft.com/User.ReadWrite.All

Admin consent required

Yes

Display Name

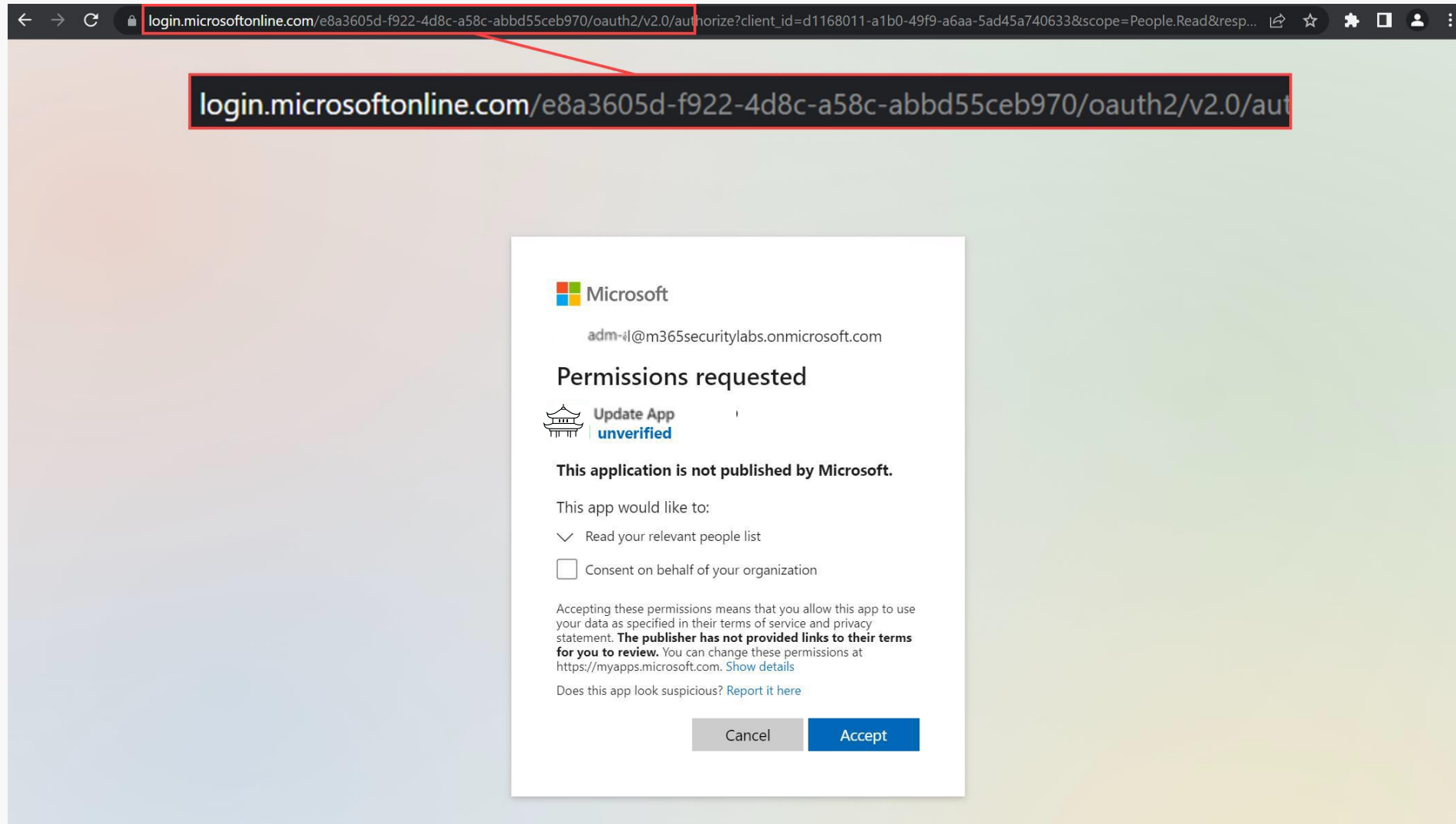
Read and write all users' full profiles

Description

Allows the app to read and update user profiles without a signed in user.

Ataque de identidad OAuth

Phishing de consentimiento #3



Analizar gráficos de ataque

"Los defensores piensan en la lista. Los atacantes piensan en gráficos. Mientras esto sea cierto, los atacantes ganan"

John Lambert, inteligencia de amenazas de Microsoft

Encontrar el camino más corto




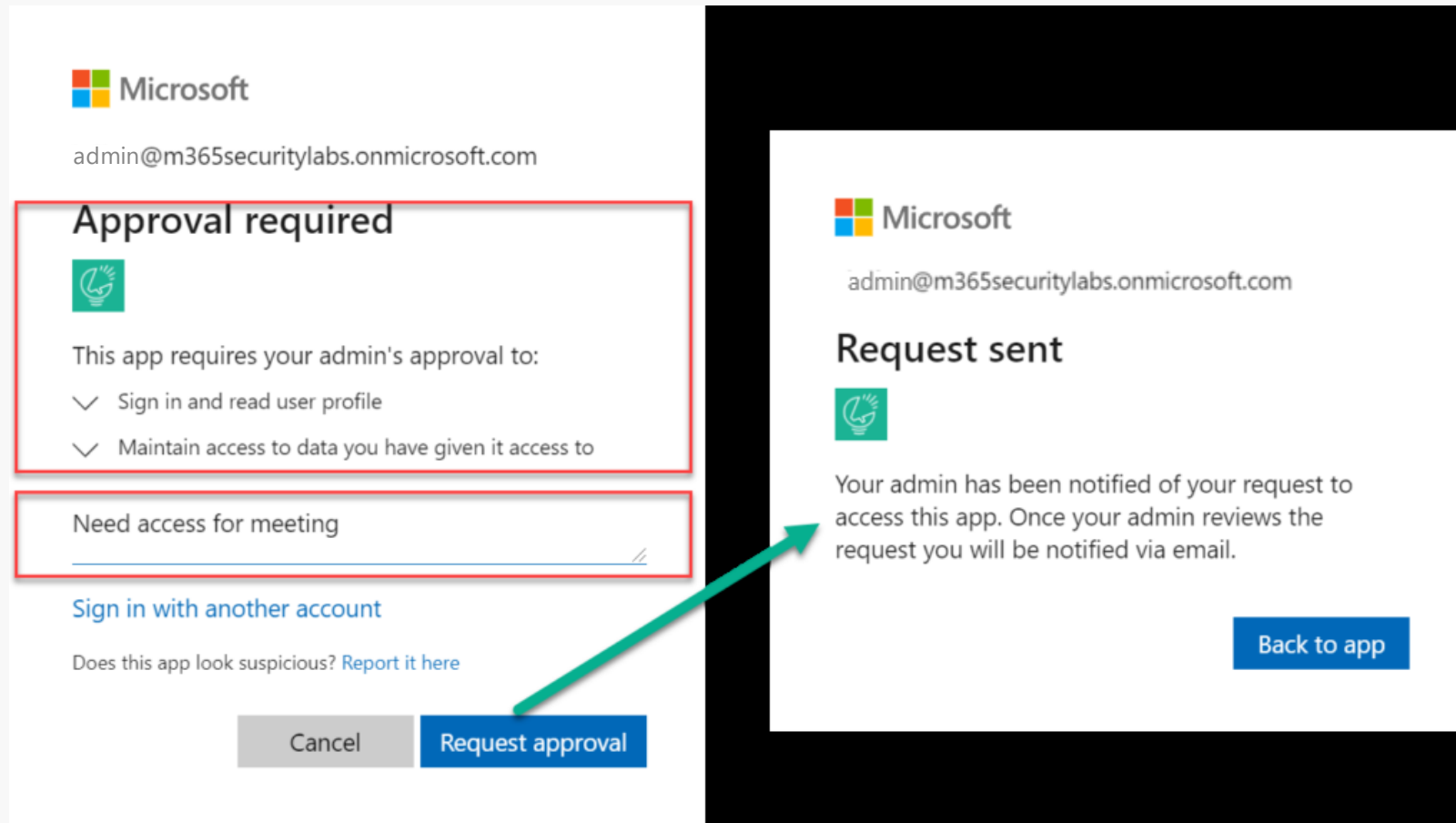
Ataque de identidad OAuth

Prevención

1. Desactivar el flujo de consentimiento OAuth para los usuarios.
2. Habilitar el consentimiento de Azure AD Admin.
3. Habilitar las políticas de aplicaciones de Defender for Cloud Apps (MDA).
4. Protección de identidades de Azure Active Directory - Identidades de carga de trabajo.
5. Caza con Defender for Endpoint/Microsoft Sentinel.
6. Entrenamiento de simulación de ataque - Simulación de consentimiento de OAuth.

Ataque de identidad OAuth

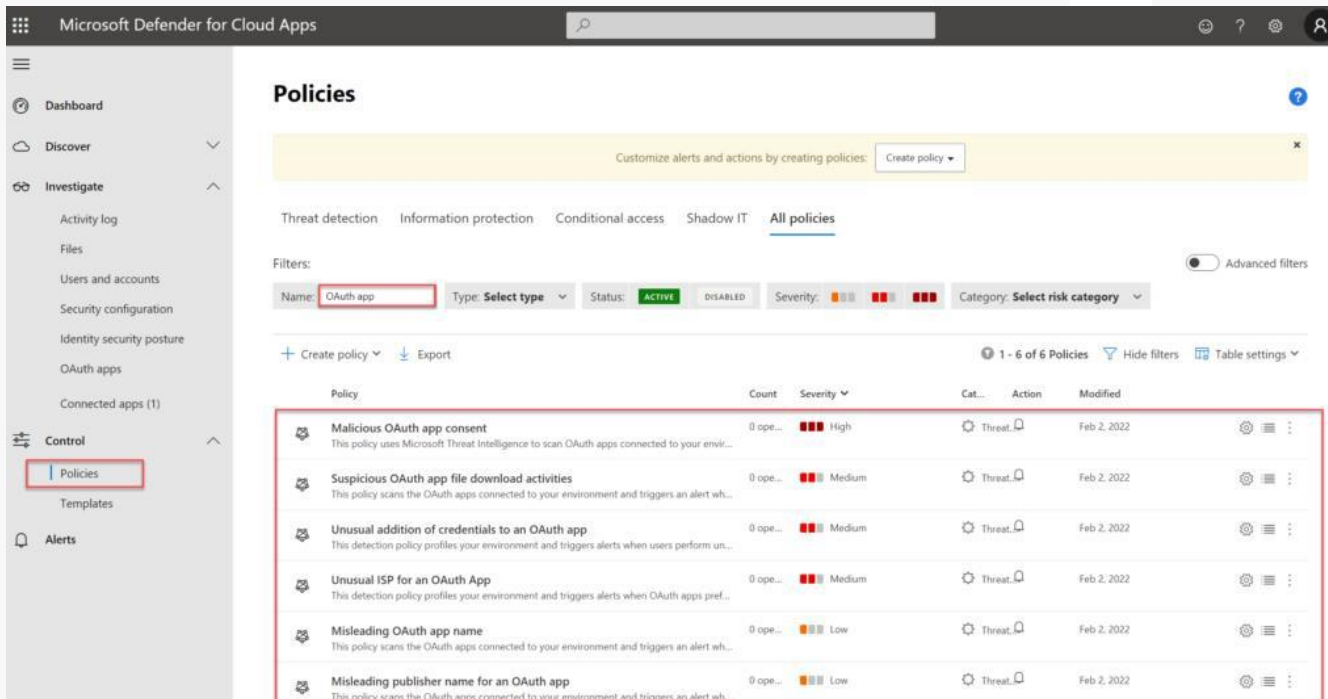
Prevención  1 – App Consent flow



Ataque de identidad OAuth

Prevención 2 – Defender for Cloud Apps

1. Consentimiento malintencionado de la aplicación OAuth
2. Actividades sospechosas de descarga de archivos de la aplicación OAuth
3. Agregación inusual de credenciales a una aplicación OAuth
4. ISP inusual para una aplicación OAuth
5. Nombre engañoso de la aplicación OAuth
6. Nombre de editor engañoso para la aplicación OAuth



Microsoft Defender for Cloud Apps

Policies

Customize alerts and actions by creating policies: [Create policy](#)

Threat detection Information protection Conditional access Shadow IT **All policies**

Filters: Name: Type: **Select type** Status: **ACTIVE** Disabled Severity: Category: **Select risk category** ☐ Advanced filters

[+ Create policy](#) [↓ Export](#) 1 - 6 of 6 Policies [Hide filters](#) [Table settings](#)

Policy	Count	Severity	Cat...	Action	Modified
Malicious OAuth app consent This policy uses Microsoft Threat Intelligence to scan OAuth apps connected to your env...	0 ope...	High	Threat		Feb 2, 2022
Suspicious OAuth app file download activities This policy scans the OAuth apps connected to your environment and triggers an alert wh...	0 ope...	Medium	Threat		Feb 2, 2022
Unusual addition of credentials to an OAuth app This detection policy profiles your environment and triggers alerts when users perform un...	0 ope...	Medium	Threat		Feb 2, 2022
Unusual ISP for an OAuth App This detection policy profiles your environment and triggers alerts when OAuth apps pref...	0 ope...	Medium	Threat		Feb 2, 2022
Misleading OAuth app name This policy scans the OAuth apps connected to your environment and triggers an alert wh...	0 ope...	Low	Threat		Feb 2, 2022
Misleading publisher name for an OAuth app This policy scans the OAuth apps connected to your environment and triggers an alert wh...	0 ope...	Low	Threat		Feb 2, 2022

Identity **Attack** Primary refresh token

PRT token

Primary Refresh token (PRT) es un token de refresco especial de alto privilegio. Comparado con Active Directory es equivalente al Ticket Granting Ticket (TGT). PRT es un token almacenado en el dispositivo. (Las claves criptográficas se almacenan en el TPM). PRT es un requisito para SSO.

Se utiliza para:

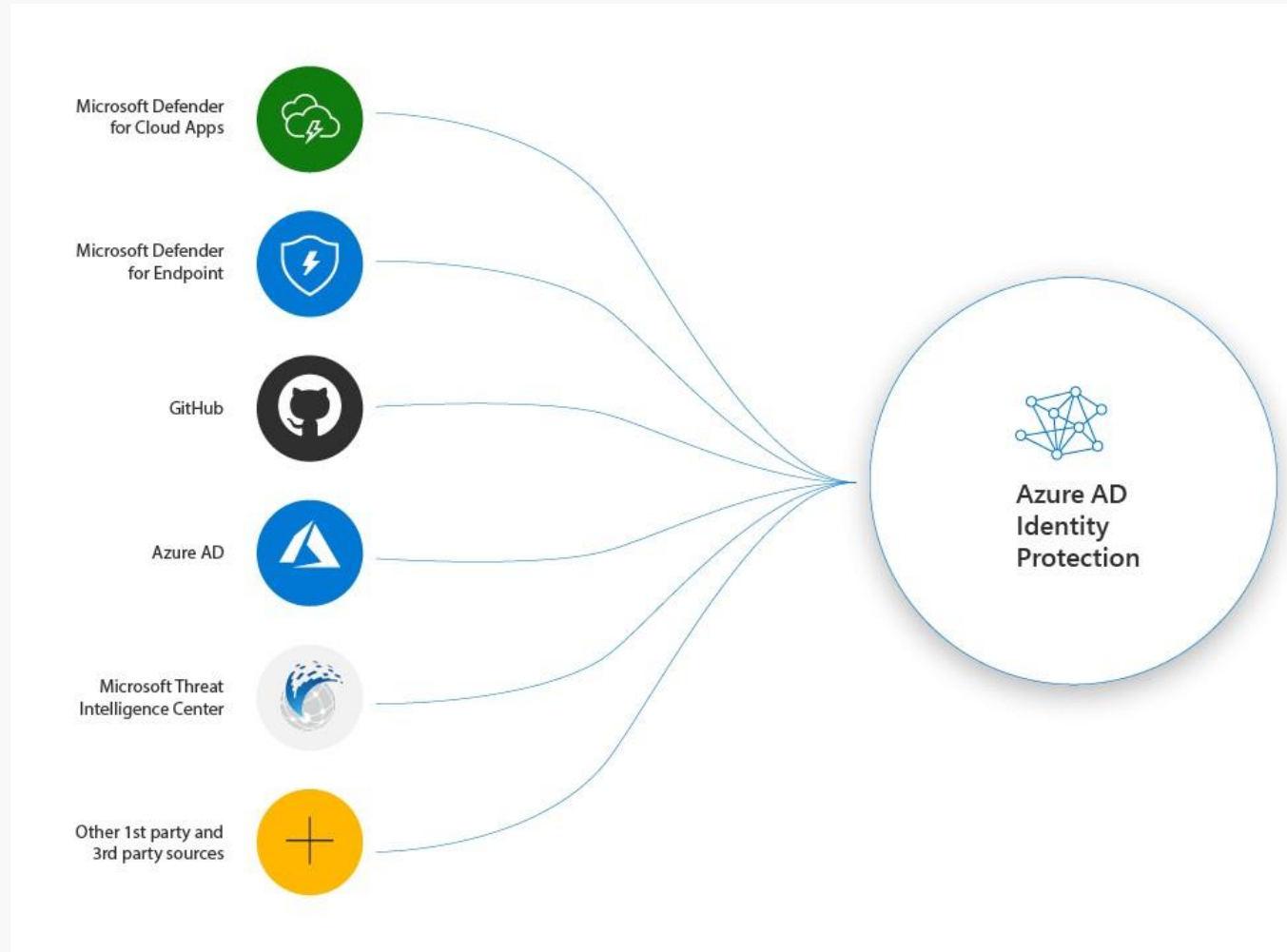
- Dispositivos registrados en Azure AD
- Dispositivos unidos a Azure AD
- Dispositivos híbridos Azure AD Joined

¿Por qué es interesante?

- Autenticación contra cualquier aplicación
- Se puede actualizar con una solicitud MFA
- Ruta de interés; C:\Program Files\Windows Security\BrowserCore\BrowserCore.exe

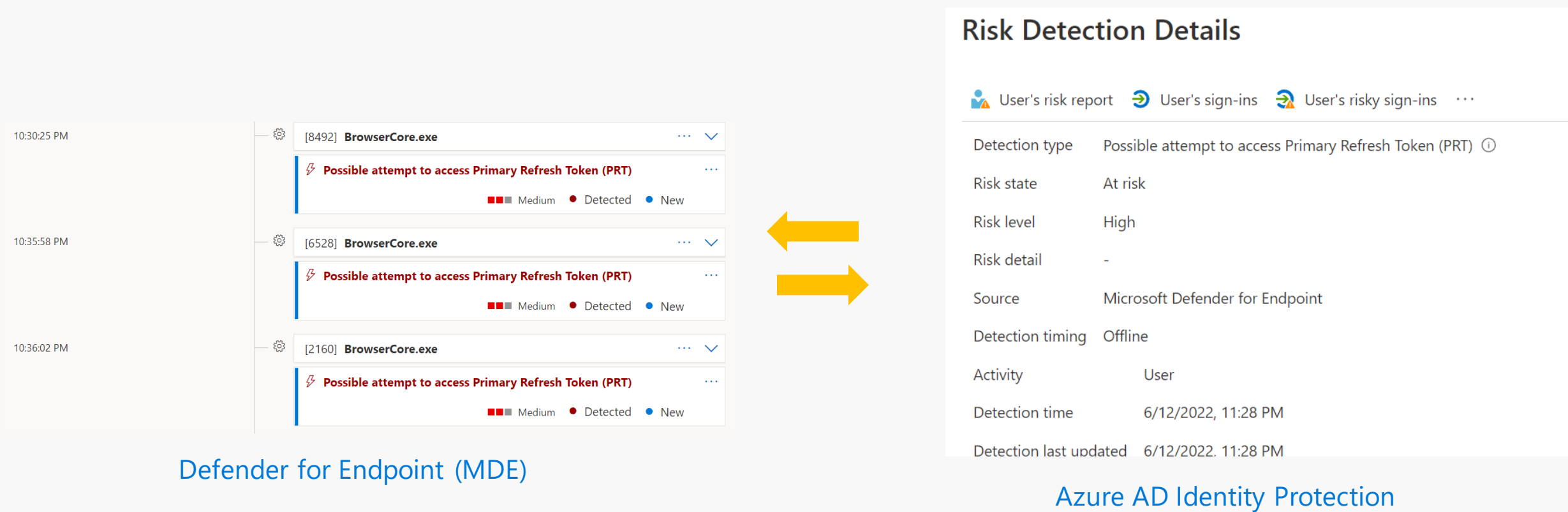
PRT token – Detección / Prevención

Combine [Azure AD Identity Protection](#) y [Defender for Endpoint \(MDE\)](#) para obtener señales holísticas de identidad comprometida.



PRT token – Detección / Prevención

Premium Azure AD Identity Protection User risk detection, detected by Defender for Endpoint (MDE)



#GABMUGPeru

Identity **Attack** MFA Spamming

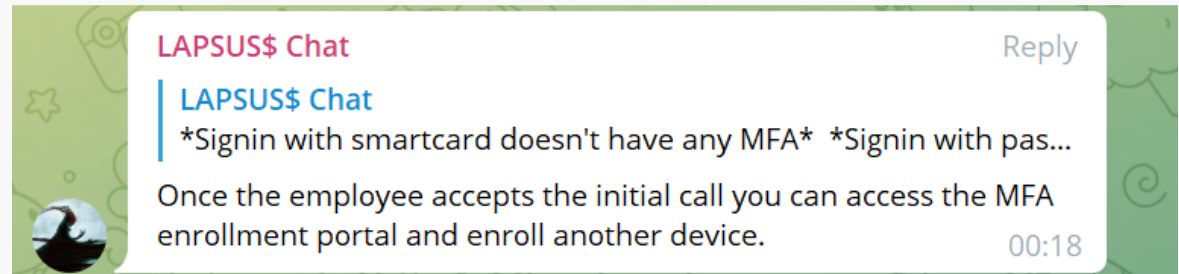
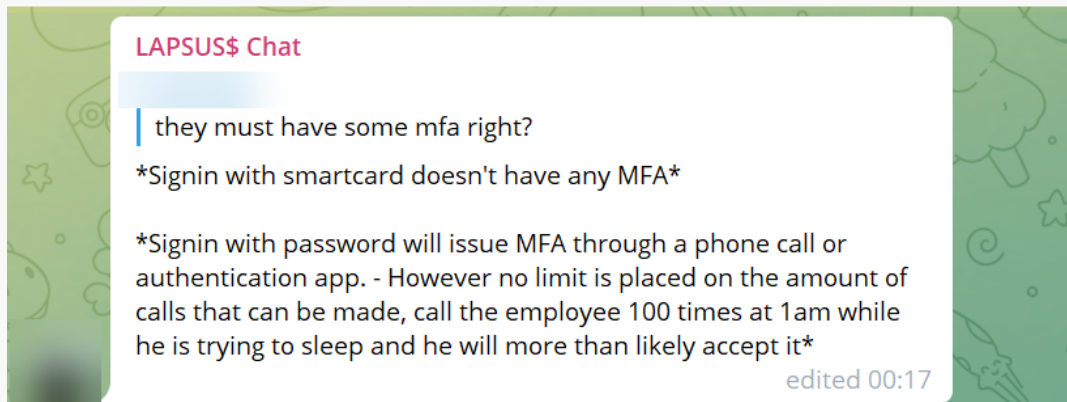


#GlobalAzure

MFA Spamming

Utilizado durante el ataque LAPSUS\$

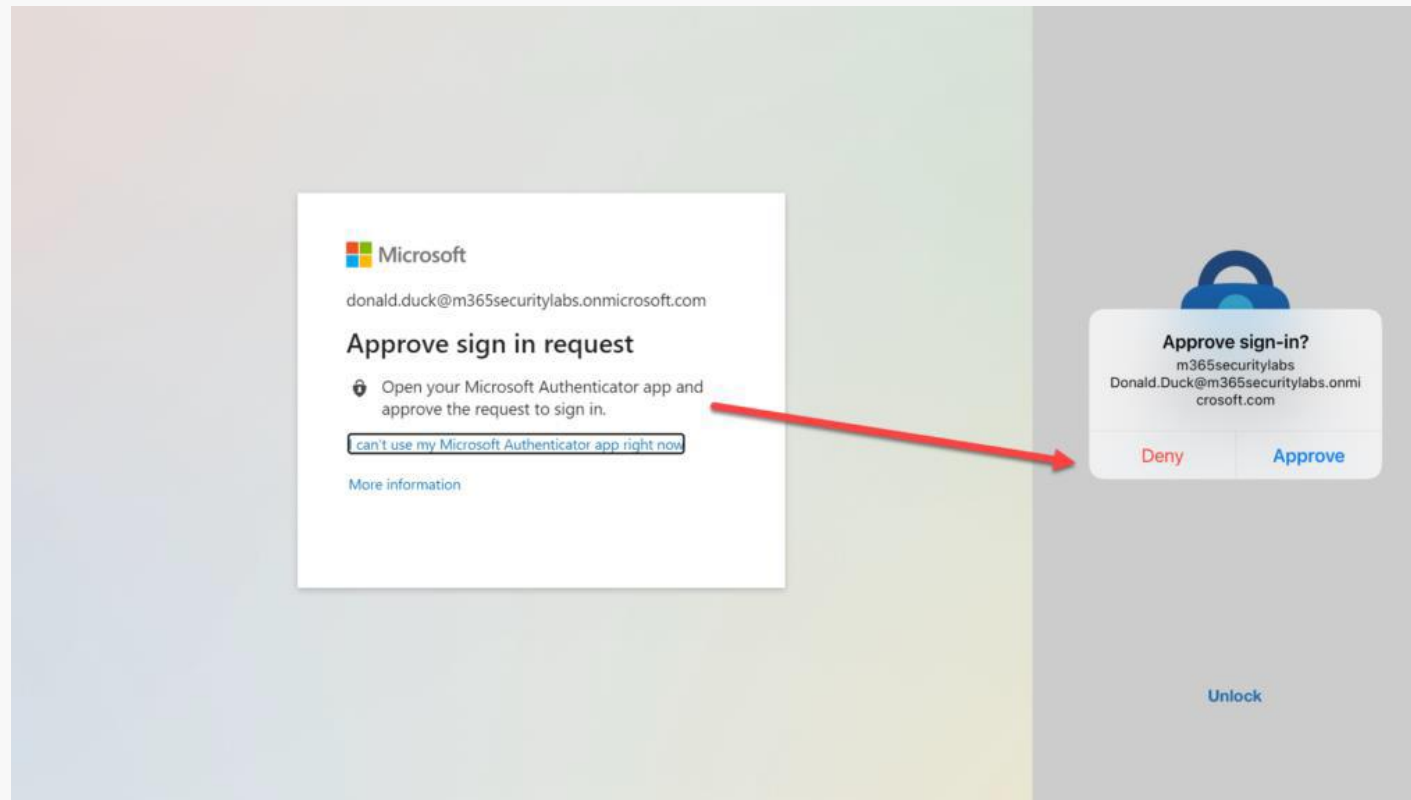
" Llame al empleado 100 veces a la 1 de la madrugada mientras intenta dormir, y lo más probable es que acepte la llamada. Una vez que el empleado acepte la llamada inicial, puede acceder al portal de inscripción MFA e inscribir otro dispositivo".



MFA Spamming

MFA Notificaciones spamming

"Después de 5 notificaciones, ¿qué tan fuerte es el cambio de un usuario lo aprueba?". Lapsus\$ reporta 50% de probabilidad de aceptar.



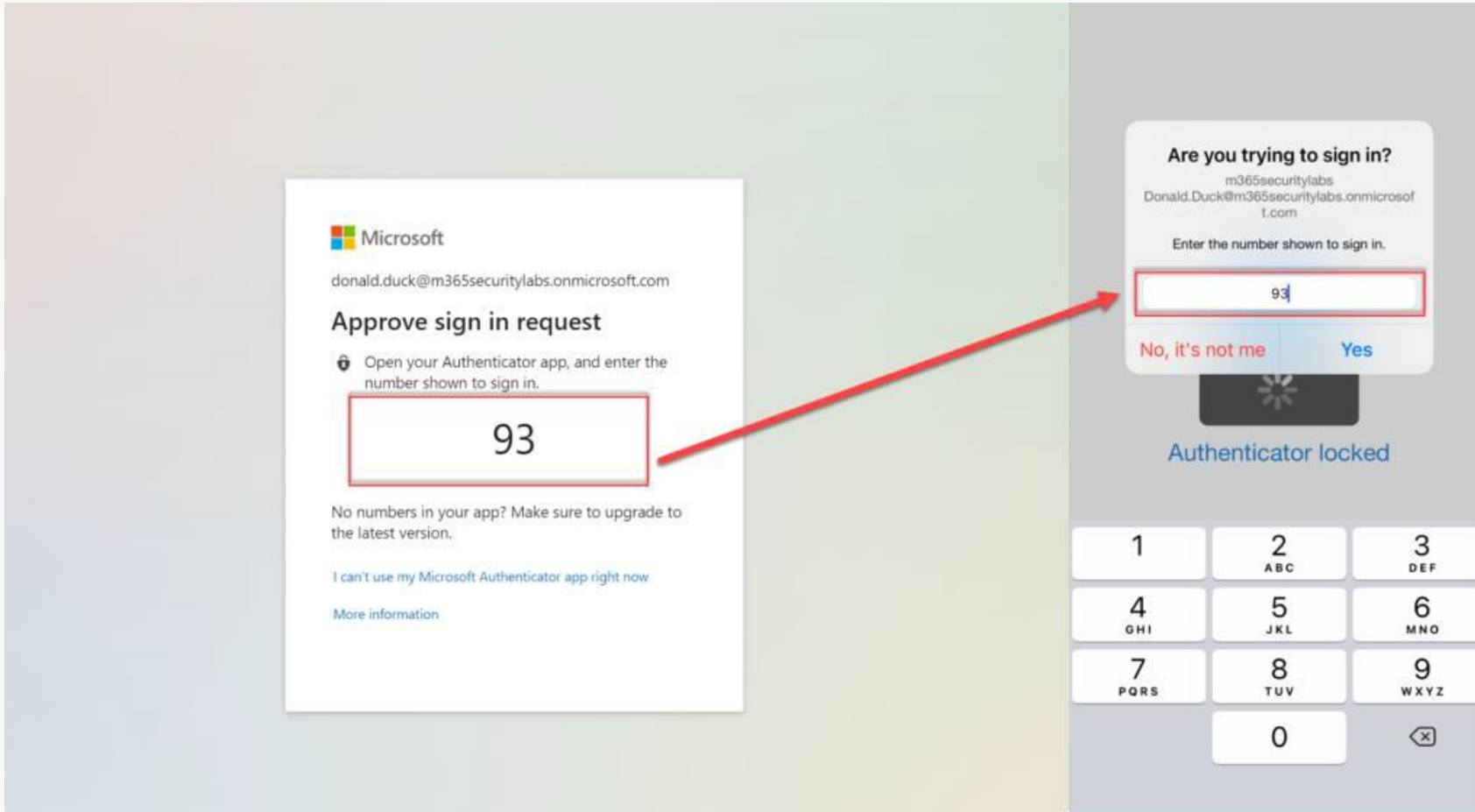
MFA Spamming

Prevención

1. Habilitar la experiencia de coincidencia de números MFA
2. Activar MFA (Acceso condicional)
3. Implementar Azure AD Identity Protection
4. Búsqueda de datos (estado de MFA denegado / el usuario no respondió)
5. Formar a los usuarios para que alerten de los intentos
6. Sin exclusiones de IP basadas en la ubicación
7. Buena línea de base de Acceso Condicional

MFA Spamming

Prevención - Coincidencia de números



Conclusión

#GABMUGPeru

Consultas?



#GlobalAzure

Patrocinadores



