

A conceptual image showing a hand holding a cityscape, with a glowing pink arc representing a protective shield or a path. The background is dark with purple and blue hues.

Abusing – And protecting - Office 365

Juan Garrido

Senior Security Consultant

Juan.Garrido@nccgroup.trust



- Juan Garrido

- nccgroup[®]

- Juan.garrido@nccgroup.trust



Índice

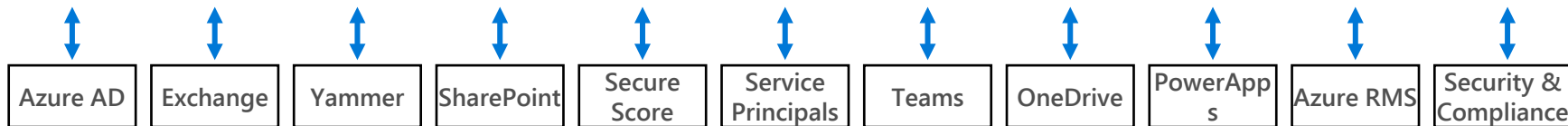
1. Office 365 & Azure AD
2. Identidades
3. Oauth Social engineering
4. Licencias de uso en O365
5. Abuso de APIs ocultas
6. Abuso de características
7. Contramedidas

One endpoint
Multiple services
All information



Azure AD
Exchange
Skype for Business
Teams
Yammer
SharePoint
Etc...

<https://portal.office.com>



Identidades

- Azure define varias identidades en función del rol a desempeñar
 - Usuario
 - Generalmente se genera para acceder a los recursos finales (Mail, Yammer, Office, etc..)
 - Dispositivo
 - Se genera un objeto por cada dispositivo administrado por Azure/O365 (dispositivo móvil, PC, laptop, etc..)
 - Aplicación
 - Se genera para uso en aplicaciones que consuman recursos de Azure/Office 365
 - En función del rol asignado podrá acceder a diferentes partes de Office365 / Azure AD /recursos

Azure Consent Framework

- Cada vez más usamos el permiso y el consentimiento para las aplicaciones (Piensa en las aplicaciones de tu teléfono por ejemplo)
- Azure Consent Framework es muy similar en conceptos
- Los permisos que se definan para la aplicación se mostrarán en el formulario de acceso
- Una aplicación puede ser configurada para acceder a otras suscripciones (Multi-Tenant)
- Cuando el usuario accede por primera vez:
 - El cliente mostrará el formulario de consentimiento
 - Si se aceptan las condiciones, la aplicación podrá realizar con el token obtenido acciones **en nombre del usuario**



juanito@trianamia.onmicrosoft.com

Permissions requested Accept for your organization



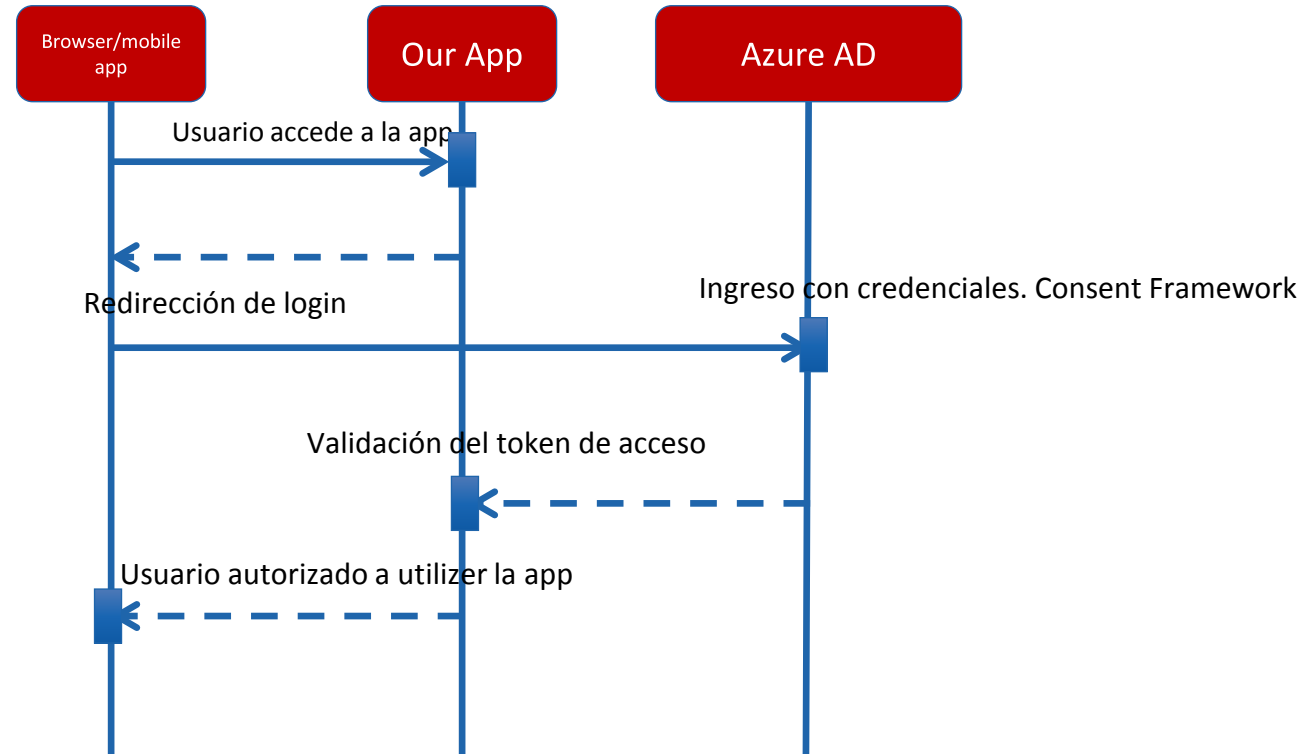
This app would like to:

- ✓ Access directory as the signed in user
- ✓ Read directory data
- ✓ Read and write directory data
- ✓ Read user mail
- ✓ Read user basic mail
- ✓ Send mail as a user
- ✓ Sign in and read user profile
- ✓ Read all users' basic profiles
- ✓ Read and write access to user profile
- ✓ Manage all delegated permission grants
- ✓ Read directory data

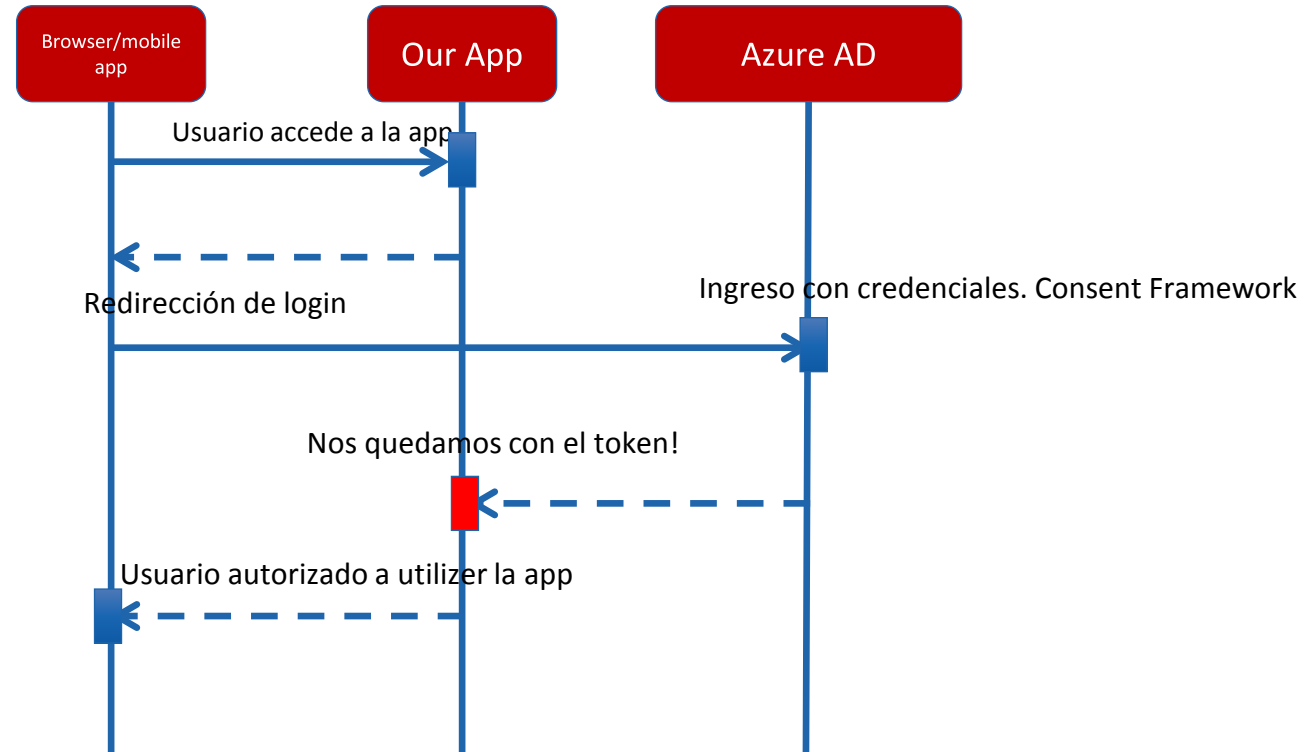
Oauth en Azure/Office 365

- Oauth
 - Mecanismo usado por aplicaciones para autenticar usuarios
 - El servicio obtiene un token de acceso que podrá usar para autenticar/autorizar al usuario
 - Pros
 - El usuario no comparte su contraseña con la aplicación
 - El token obtenido tendrá una caducidad que variará en función de la aplicación/permisos/etc (mínimo 1 hora)
 - Cons
 - Si se roba el token Oauth de un usuario, se podrán realizar acciones en nombre de éste hasta que el token caduque
 - En función del rol y los privilegios del usuario, se podrá mapear la suscripción al completo

Azure Consent Framework



Oauth Social Engineering

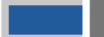
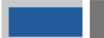
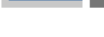
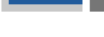
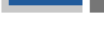


Robo de Token Oauth



Licencias de uso en O365

- Cuando un nuevo usuario de O365 se genera
 - Se le asignan una serie de licencias de uso
 - Azure AD
 - Exchange
 - Yammer
 - SharePoint
 - Etc..

Microsoft Forms (Plan E1)		On
Flow for Office 365		On
PowerApps for Office 365		On
RETIRED - Outlook Customer Manager		On
Microsoft Teams		On
Microsoft Planner		On
Sway		On
Mobile Device Management for Office 365 (These licenses do not need to be individually assigned)		Off
Office for the web		On
Office 365 Business		On
Yammer Enterprise		On
Exchange Online (Plan 1)		On
Skype for Business Online (Plan 2)		On
SharePoint Online (Plan 1)		On

Abuso de APIs ocultas

- Cada uno de estos servicios tiene como mínimo una API asociada (O un Web Service) para ser consumida desde el portal de Office o por módulos de PowerShell
- Muchos servicios tienen múltiples APIs
- Estas APIs a su vez pueden tener un sistema de versiones. En función de la version utilizada, ésta mostrará mas o menos información
- Muchas de estas APIs exponen un fichero de metadatos en donde se indican los métodos existentes, así como los parámetros de entrada

Abuso de APIs ocultas

- Ejemplo: Azure Active Directory
- Número de APIs: 3

Endpoint	Tipo de Acceso	Versiones
https://graph.microsoft.com	Información básica de O365 y Azure Active Directory	V1.0 & beta
https://graph.windows.net	Acceso básico a Azure Active Directory	V1.5 / v1.6 / v1.6.1 /v1.6.1.internal
https://main.iam.ad.ext.azure.com/api/	Acceso completo a Azure AD	

Abuso de APIs ocultas

- Un administrador podrá denegar el acceso al portal de Azure AD
- Pero no podrá denegar el acceso a ciertas APIs

App registrations

Users can register applications ⓘ

Yes

No

Administration portal

Restrict access to Azure AD administration portal ⓘ

Yes

No

No lets a non-administrator use this Azure AD administration portal experience to access Azure AD resources that the user has permission to read, or manage resources they own. Yes restricts all non-administrators from accessing any Azure AD data in the administration portal, but does not restrict such access using PowerShell or another client such as Visual Studio.

LinkedIn account connections

Allow users to connect their work or school account with LinkedIn.

Data sharing between Microsoft and LinkedIn is not enabled until users consent to connect their Microsoft work or school account with their LinkedIn account.

[Learn more about LinkedIn account connections](#) ⓘ

Yes

Selected group

No

Abuso de APIs ocultas



Abuso de características

- De manera genérica cuando un usuario es generado en Office 365 éste podrá consumir los servicios mediante un cliente:

Servicio	Cliente
Exchange	Outlook, Outlook mobile
Lync/Skype/Teams	Teams Client, Skype for business
SharePoint	SharePoint Portal
OneDrive	Cliente de OneDrive
Yammer	Yammer Client

```
C:\AzureAD\Enumerate> Get-User Dorsey.Barela | Select-Object *
```

```
UnspaceId : beb1dd43-0f52-4db9-a756-b31ff6090f1e
IsSecurityPrincipal : True
OnPremisesAccountName : Dorsey.Barela@trianamia.onmicrosoft.com
ObjectId : S-1-5-21-1612083179-4102000699-3785483694-12642142
ObjectIdHistory : {}
UserPrincipalName : Dorsey.Barela@trianamia.onmicrosoft.com
ResetPasswordOnNextLogon : False
CertificateSubject : {}
RemotePowerShellEnabled : True
WindowsLiveId : Dorsey.Barela@trianamia.onmicrosoft.com
MicrosoftOnlineServicesId : Dorsey.Barela@trianamia.onmicrosoft.com
ObjectId : 100320008FC88CAB
IsCloudCacheProvisioningComplete : False
IsCloudCache : False
CloudCacheProvider : 0
CloudCacheAccountType : Other
CloudCacheScope : 0
CloudCacheRemoteEmailAddress :
CloudCacheUserName :
IsCloudCacheBlocked : False
ConsumerNetId :
UserAccountControl : NormalAccount
OrganizationalUnit : eurp190a001.prod.outlook.com/Microsoft Exchange Hosted Organizations/trianamia.onmicrosoft.com
IsLinked : False
LinkedMasterAccount :
```

Abuso de características

- De manera predeterminada los servicios de Office 365 permiten interactuar mediante PowerShell
- En determinados servicios una cuenta sin privilegios tendrá acceso de lectura sobre la organización
- En determinados servicios este privilegio puede ser revocado
 - **Set-User Identity-RemotePowerShellEnabled \$false**

Contramedidas

- Revisa los permisos de las aplicaciones desplegadas y autorizadas en Office 365
- Configura y habilita las auditorías en el portal de Security & Compliance Manager
- Realiza análisis de logs de manera periódica
- Revisa los privilegios de los usuarios y revoca el acceso a servicios que no vayan a usar
- Configura el acceso a recursos basados en Conditional Policies
- Deshabilita la autenticación básica en todos los servicios de Office 365
- Revoca privilegios que no sean necesarios:
 - Acceso a Exchange desde PowerShell
 - Acceso a la aplicación de Graph Explorer

Abuso de características



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional