

PANORAMA DES PRINCIPALES MENACES SUR OFFICE 365 EN 2020

THIBAUT JOUBERT -
WAVESTONE

QUEL ÉTAT DE LA MENACE POUR OFFICE 365 ?

Plus de 50% des données sensibles dans
Office 365

**92 % des logiciels malveillants sont
délivrés par emails**

**38% des attaques de phishing ciblent
les services SaaS (1^{er} devant les
services bancaires)**

**Microsoft est la marque la plus ciblée
depuis 2018**

**43% des fichiers malveillants sont des
documents Microsoft Office**

Rapport Verizon, 2020



Gains financiers directs

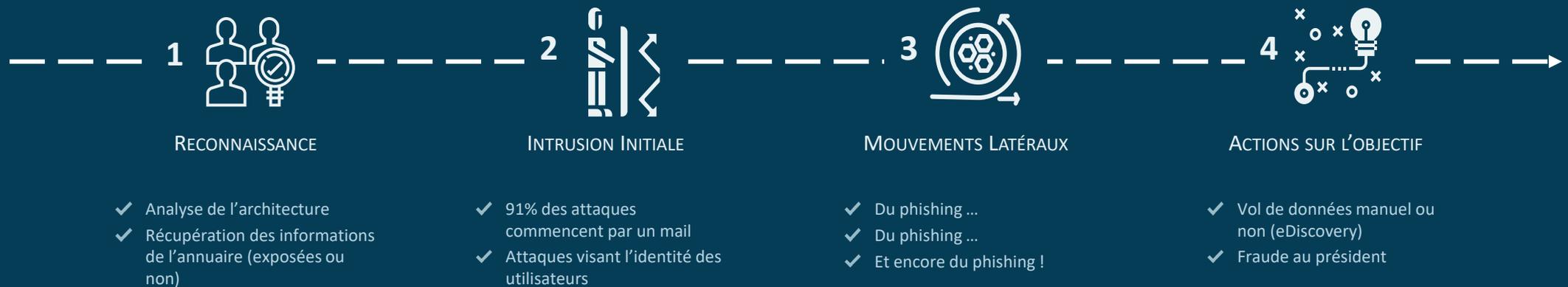


Vol de données



**Récupération
des authentifiants**

LES ATTAQUES SUR OFFICE 365 SUIVENT UN SCHÉMA CLASSIQUE ADAPTÉ AU CONTEXTE CLOUD



LES TENTATIVES D'INTRUSION CIBLENT PRINCIPALEMENT L'IDENTITÉ ...

AUTHENTIFIANTS

Récupération des authentifiants de
l'utilisateur

JETONS

Interception des jetons d'accès ou de
rafraîchissement afin de les réutiliser

OAUTH

Délégation du consentement à des
applications malveillantes afin de récupérer
des informations sur l'annuaire, les mails ou
les données d'un utilisateur

... et peuvent être couvertes avec une bonne hygiène et l'implémentation d'une
stratégie "Zero Trust"

FOCUS SUR LES ATTAQUES CIBLANT LES JETONS O365 / AZURE AD

L'authentification multi-facteur n'est plus une option !

Des chercheurs et des attaquants ont commencé à mettre en place des stratégies permettant de contourner l'authentification multi-facteur.

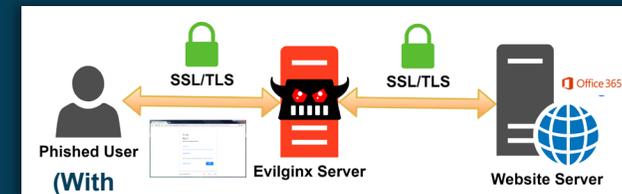
/ Ex : Man-in-the-middle – Evilginx (2018)

/ Ex : Device code flow (2020)

Le contexte de la demande d'accès doit être pris lors de l'évaluation de l'authentification et l'autorisation.

- ✓ CMI-1 Mettre en place une authentification renforcée
- ✓ CMI-5 Maîtriser les appareils autorisés à accéder à Office 365
- ✓ CMP-6 Mettre en place le contrôle d'accès conditionnel
- ✓ CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité

Un exemple d'attaque sur les jetons : Evilginx 2.0



<https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/>



Au lieu de forger une simple page d'authentification, Evilginx devient un relais entre office 365 et l'utilisateur victime d'un hameçonnage.

L'utilisateur interagit avec le site web réel, tandis qu'Evilginx capture toutes les données transmises entre les deux parties.



FOCUS SUR LES PERMISSIONS OAUTH

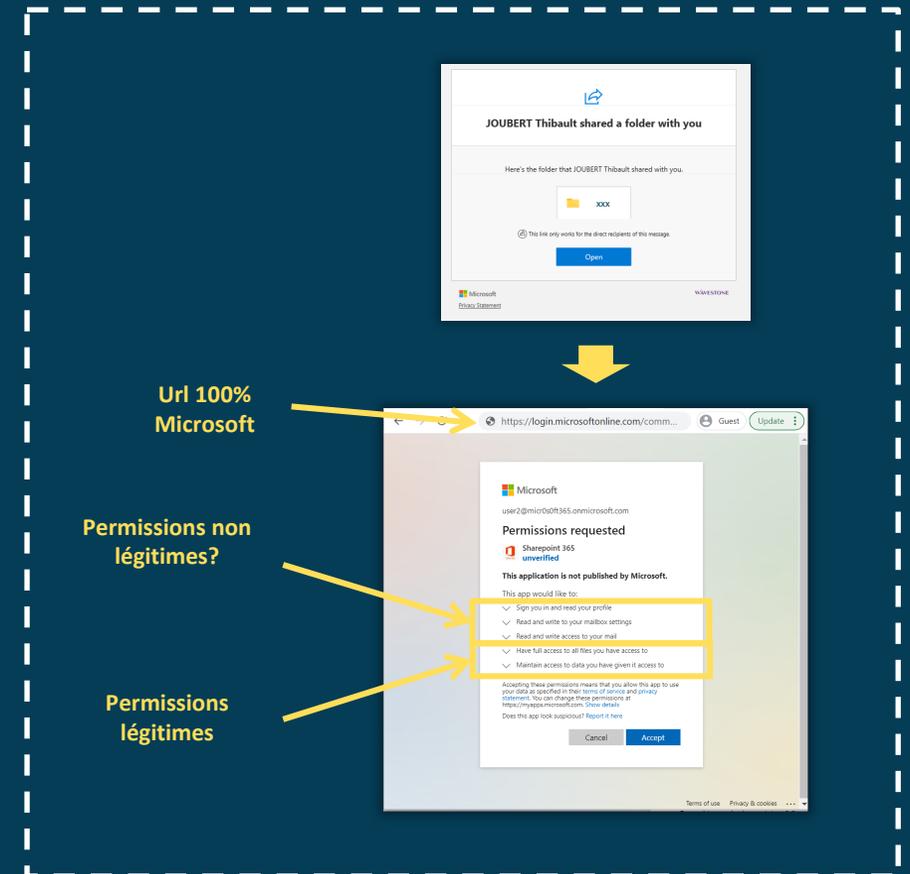
Oauth est un *framework* permettant d'autoriser des applications tierces d'effectuer des actions au nom d'un utilisateur.

Par défaut, un utilisateur peut consentir à des permissions « non sensibles ». Mais la notion de sensibilité est relative !

/ Ex : Synchronisation One Drive à Google Drive

/ Ex : Lecture de l'annuaire

- ✓ CMG-5 Former les administrateurs et les développeurs
- ✓ CMI-6 Mettre en place un processus de gestion des services tiers
- ✓ CMD-1 Monitorer les modifications de configuration
- ✓ CMD-3 Monitorer les accès aux données



The diagram illustrates the OAuth permission flow through three stages:

- Notification:** A message from Joubert Thibault sharing a folder named 'XXX'.
- Microsoft Login:** A browser window showing the Microsoft login page at <https://login.microsoftonline.com/comm...>, labeled as 'Url 100% Microsoft'.
- Permissions Requested:** A dialog box asking for permissions. The permissions list includes:
 - Sign you in and read your profile
 - Read and write to your mailbox settings
 - Read and write access to your mail
 - Have full access to all files you have access to
 - Maintain access to data you have given it access to
 The first two permissions are highlighted as 'Permissions non légitimes?' (illegitimate), while the last three are highlighted as 'Permissions légitimes' (legitimate).

MOUVEMENTS LATÉRAUX ET PERSISTENCE : LES ATTAQUANTS S'APPUIENT SUR LES DÉFAUTS DE GOUVERNANCE ET DE DURCISSEMENT



Création d'un compte invité

/ Politiques de sécurité moins sécurisée & Pas de cycle de vie

Enregistrement d'une nouvelle application avec le secret associé

/ Réalisation d'actions au nom de l'utilisateur

/ Elévation de privilège (si le rôle d'Administrateur d'application est compromis)

Consentement à des permissions d'applications Azure AD

/ Réalisation d'actions au nom de l'utilisateur via les applications OAuth



Création de règle de transfert de mail ou de délégations

/ Redirection de tout ou partie des mails entrants à une adresse mail externe

A noter : Microsoft est en train de désactiver les redirections automatiques par défaut



Création d'un Power Automate (ex-Microsoft Flow)

/ L'utilisation de Power Automate ne peut pas être bloqué (mais les connecteurs peuvent être maîtrisés)

/ Contournement du durcissement : redirection automatique, Synchronisation avec des SaaS tiers