Signes d’un Courriel de Phishing

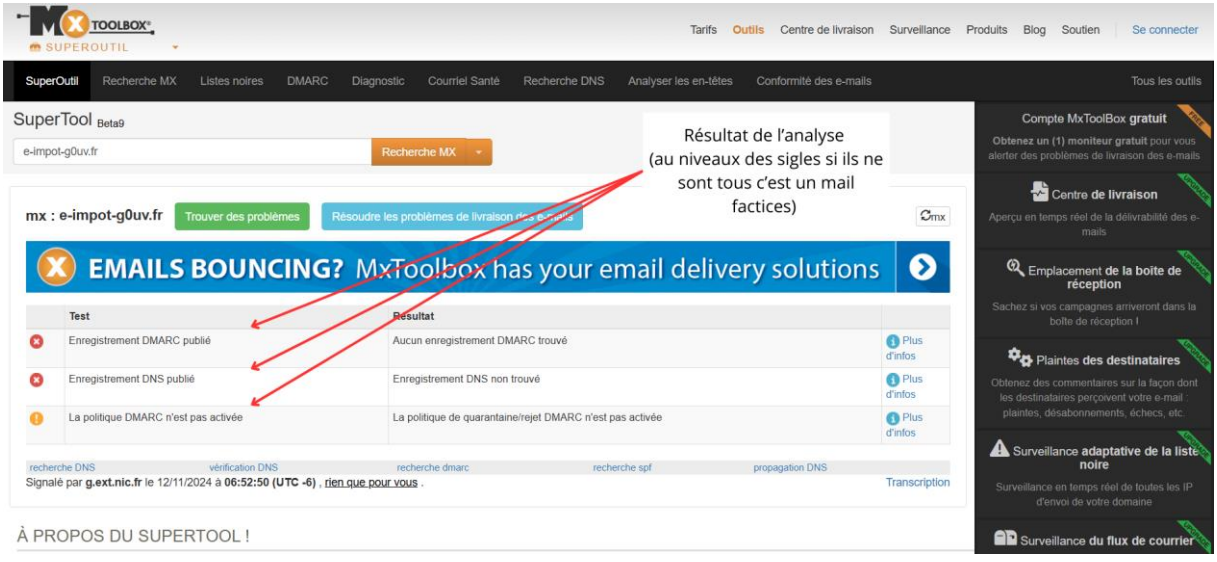
Technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles et/ou financières par des liens suspects, des pièces jointes inconnues là où une organisation légitime ne vous demandera jamais de partager vos données personnelles.

Comment Se Protéger du Phishing ?

1. Ne jamais cliquer sur des liens ou des pièces jointes dans les courriels suspects.
2. Vérifier l’authenticité de la demande.
3.

Procédure à suivre en cas de phishing :

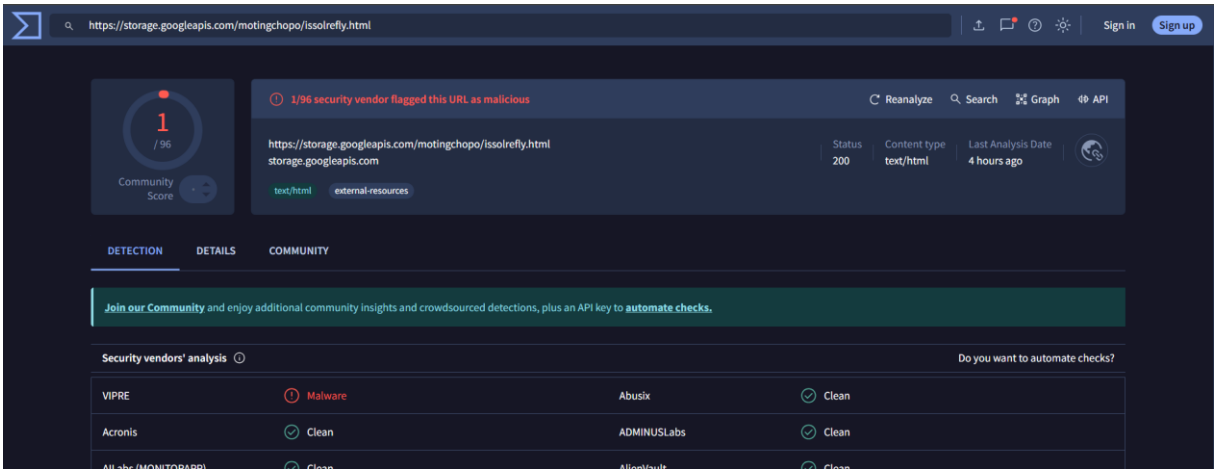
1. Ne répondez pas au message.
2. Vérifier les informations du mail :
    - Vérifier l’expéditeur avec https://mxtoolbox.com/SuperTool.aspxet (1 utilisation/par semaine) s’il apparaît ceci :



Alors c’est un **PHISHING** ⍰

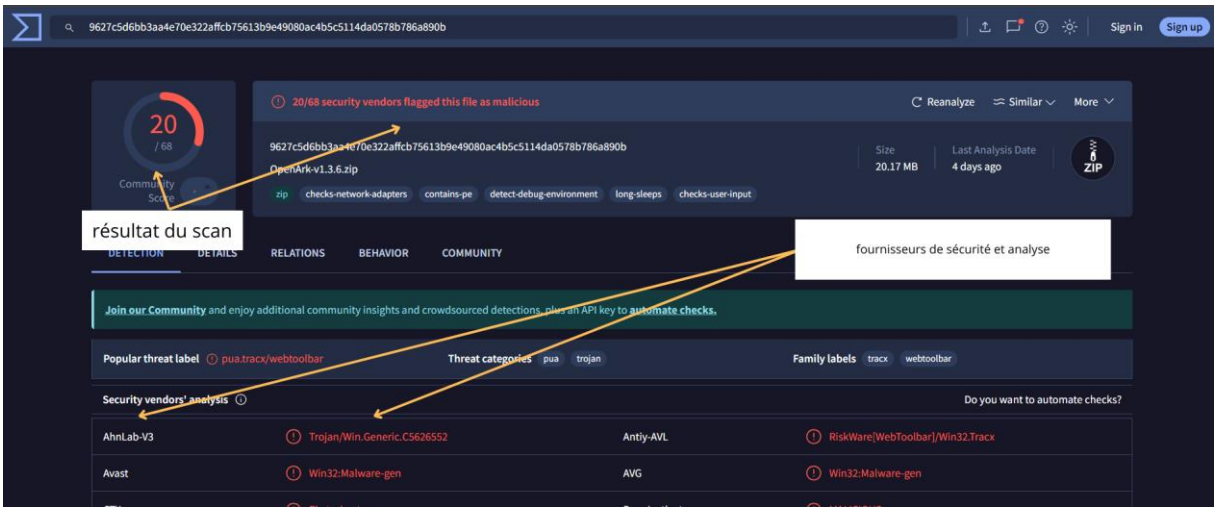
- Vérifier l’url avec celui du site original. (S’il diffère, alors votre mail est une tentative de **PHISHING** ⍰)

- Vérifier l'url avec https://www.virustotal.com/gui/home/upload et s'il apparaît ceci :



Alors c'est un site avec un **VIRUS** et donc très probablement un **PHISHING** 🤣

- Avec https://www.virustotal.com/gui/home/upload vous pouvez aussi vérifier les documents téléchargeables :



Alors c'est un fichier remplie de **VIRUS**

- Si vous n'avez trouvé aucune information à la suite de ces étapes permettant de définir s'il s'agit d'une tentative de phishing alors vous pouvez ouvrir le **bac à sable** (Annexe 1) ou **Microsoft Defender** (Annexe 2) et fouiller le mail par vous-même **sans** conséquence. Pour cela suivez la procédure en annexe pour l'activer et l'utiliser.

3. Alerter votre service IT.
4. Transmettre le mail à spam@ac-rennes.fr.
5. Surveillez toute activité suspecte sur vos comptes bancaires et en ligne si vous avez partagé des informations sensibles.

Salon le cas vous pouvez également:

1. Selon les sites et systèmes d'authentification, vous avez parfois la possibilité d'activer l'authentification en deux étapes (double facteur). Par exemple avec un mot de passe puis un code de vérification (envoyé par mail, par sms), un process biométrique ou un code OTP (one time password) comme les clés OTP académiques mais qui existe aussi en système logiciel gratuit pour certains sites comme 365 avec Microsoft Authenticator.
2. Sur vos machines personnelles vous pouvez également recourir à des logiciels antivirus avec des filtres anti-fishing (en général ce sont des offres payantes).

Annexe 1 (Mise en place du bac à sable) :

Le bac à sable Windows (ou Windows Sandbox) est une fonctionnalité incluse dans certaines versions de Windows (comme Windows 10 Pro, Enterprise et Windows 11) permettant de lancer un environnement de bureau temporaire et isolé. Cet environnement est idéal pour tester des logiciels potentiellement risqués sans impacter le système principal. Voici une explication détaillée pour ouvrir et utiliser le bac à sable Windows.

1. Vérifier la compatibilité du système

Avant de pouvoir utiliser le bac à sable Windows, il faut vérifier si votre système d'exploitation le prend en charge.

- Version de Windows : Assurez-vous que vous utilisez Windows 10 Pro/Enterprise ou Windows 11 Pro/Enterprise.

- Matériel : Vous devez disposer d'un processeur compatible avec la virtualisation matérielle (Intel VT-x ou AMD-V), et cette fonctionnalité doit être activée dans le BIOS/UEFI.

2. Activer la virtualisation matérielle

Si la virtualisation n'est pas activée, voici comment l'activer dans le BIOS/UEFI :

1. Redémarrez votre ordinateur et entrez dans le BIOS/UEFI (souvent, cela se fait en appuyant sur des touches telles que F2, Delete, Esc, ou F10 **pendant le démarrage**).

2. Recherchez une option nommée Intel Virtualization Technology, VT-x, AMD-V, ou SVM Mode.

3. Activez cette option et enregistrez les modifications.

4. Redémarrez l'ordinateur.

3. *Activer le bac à sable Windows :*

1. Accédez aux fonctionnalités de Windows :

- Allez dans Panneau de configuration > Programmes > Programmes et fonctionnalités > Activer ou désactiver des fonctionnalités Windows.

- Recherchez et cochez la case Windows Sandbox.

2. Validez et redémarrez :

- Cliquez sur *OK* pour installer la fonctionnalité. Vous serez invité à redémarrer l'ordinateur pour que les modifications prennent effet.

4. Ouvrir le bac à sable Windows

1. Recherchez "Sandbox":

- Cliquez sur l'icône de recherche ou appuyez sur la touche *Windows* et tapez Windows Sandbox.

- Cliquez sur l'application lorsqu'elle apparaît dans les résultats.

2. Lancer le bac à sable:

- Le bac à sable s'ouvre dans une nouvelle fenêtre, ressemblant à un bureau Windows basique et isolé.

- Vous pouvez copier des fichiers de votre système principal vers le bac à sable pour les tester sans risque. Ces fichiers seront perdus dès que vous fermerez la session du bac à sable.

5. Utilisation et fermeture

- Exécution : Utilisez le bac à sable comme un environnement Windows normal. Installez et testez des logiciels en toute sécurité.

-Clôture : Fermez simplement la fenêtre pour effacer tout ce qui s'y trouve. Tous les changements et fichiers dans le bac à sable seront supprimés automatiquement.

Remarques importantes

- Sécurité : Le bac à sable est isolé de votre système principal, ce qui signifie qu'il ne conserve aucune donnée ou paramètre entre les sessions.

- Ressources système : Le bac à sable utilise des ressources de votre ordinateur pour fonctionner. Assurez-vous d'avoir suffisamment de mémoire RAM (idéalement 8 Go ou plus) pour garantir une expérience fluide.

Cette fonctionnalité est idéale pour tester des applications potentiellement dangereuses sans compromettre la sécurité de votre système.

Annexe 2 (Mise en place du Microsoft Defender) :

Pour activer Microsoft Defender Application Guard :

Activer la fonctionnalité :

- Accédez à Menu démarrer > Programmes > Activer ou désactiver des fonctionnalités Windows.
- Cochez la case Microsoft Defender Application Guard et redémarrez votre ordinateur si nécessaire.
- Ensuite lancer Edge Explorer

alternative

Prérequis

- installer le bac à sable

- changer les paramètres par défaut pour l'ouverture des types de fichiers par edge sécurisé ou microsoft application defender guard