**PROJET ENTREPRISE :
 Configuration et sécurisation d’un poste informatique**

Table des matières

[**Contexte** 2](#_Toc199930399)

[**Prise en charge du pc fixe & diagnostic :** 2](#_Toc199930400)

[**Solutions** 4](#_Toc199930401)

[**Prise en charge du Mac & diagnostic :** 4](#_Toc199930402)

# **Contexte**

Un client nous ramène deux ordinateurs (un ordinateur fixe & un Mac). Le client nous signale des « virus » présents sur ses ordinateurs.



N.B : Afin de respecter la loi RGPD, toutes les informations sensibles ont été volontairement modifiés.

# **Prise en charge du pc fixe & diagnostic :**

Configuration du pc fixe :

Carte mère : MSI B450 Gaming plus MAX

CPU : AMD Ryzen 5 5600

RAM : 2x8 Gb DDR4 3200 MHz

Carte graphique : GeForce RTX 4060 8Gb



Dans un premier temps, nous remarquons que les pop-ups « d’alerte virus » ne sont en réalité que des notifications de sites web présentes à cause de cookies/notifications activés par défaut.

Il suffit de se rendre dans les paramètres de son navigateur -> notifications -> désactiver toutes les notifications du site en question.

Le client étant inquiet d’une présence d’un vrai virus sur son pc, nous lui proposons une sauvegarde/nettoyage de ses données et une réinstallation de son système.

 Lorsque nous réinitialisons Windows, nous faisons un nettoyage de ses données en cochant le nettoyage des données sur l’interface de réinstallation Windows. Mais également avec notre anti-virus Bit defender qui à détecter un TROJAN.

Qu’es qu’un TROJAN ?

*Un cheval de Troie (Trojan horse en anglais) est un type de logiciel malveillant, qui ne doit pas être confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Son but est de faire entrer cette fonctionnalité malveillante sur l'ordinateur et de l'installer à l'insu de l'utilisateur.*

L’anti-virus a pu éliminer la menace.

# **Solutions**

Nous ferons donc la réinstallation et le passage à Windows 11 sans aucun souci supplémentaire. Le client était précédemment sur Windows 10, dont le support de mise à jour se termine en octobre 2025. Nous conseillerons et montrerons au client comment mettre en place des sécurités supplémentaires pour tous ces comptes (Authentification à double facteurs par exemple). Le client demandera également une installation d’un Anti-virus.

# **Prise en charge du Mac & diagnostic :**

Concernant le Mac, un pop-up indiquant une alerte virus Windows. Le pop-up indique volontairement pleins de facteurs de temps avant de tout perdre pour faire paniquer la victime et appeler le numéro de téléphone du soi-disant service technique de Microsoft.

Le client, du au facteur de stress causés par le pop-up ne remarquera pas qu’un virus détecté par Microsoft par son pc n’est pas possible car il est sur un OS n’appartenant pas à Microsoft.



(Image équivalente au pop-up détecté)

Les arnaqueurs pousseront la victime à installer « Anydesk », un logiciel de prise de contrôle d’un pc à distance) afin de pouvoir voler toutes les données présentes sur le mac.

La victime à néanmoins bloqué l’accès à distance car il a remarqué la prise de ces données. C’était LE réflexe à avoir dans cette situation.

Nous conseillerons pour rassurer le client une suppression de toutes les applications installées par les arnaqueurs, une sauvegarde des données et une réinstallation du système.