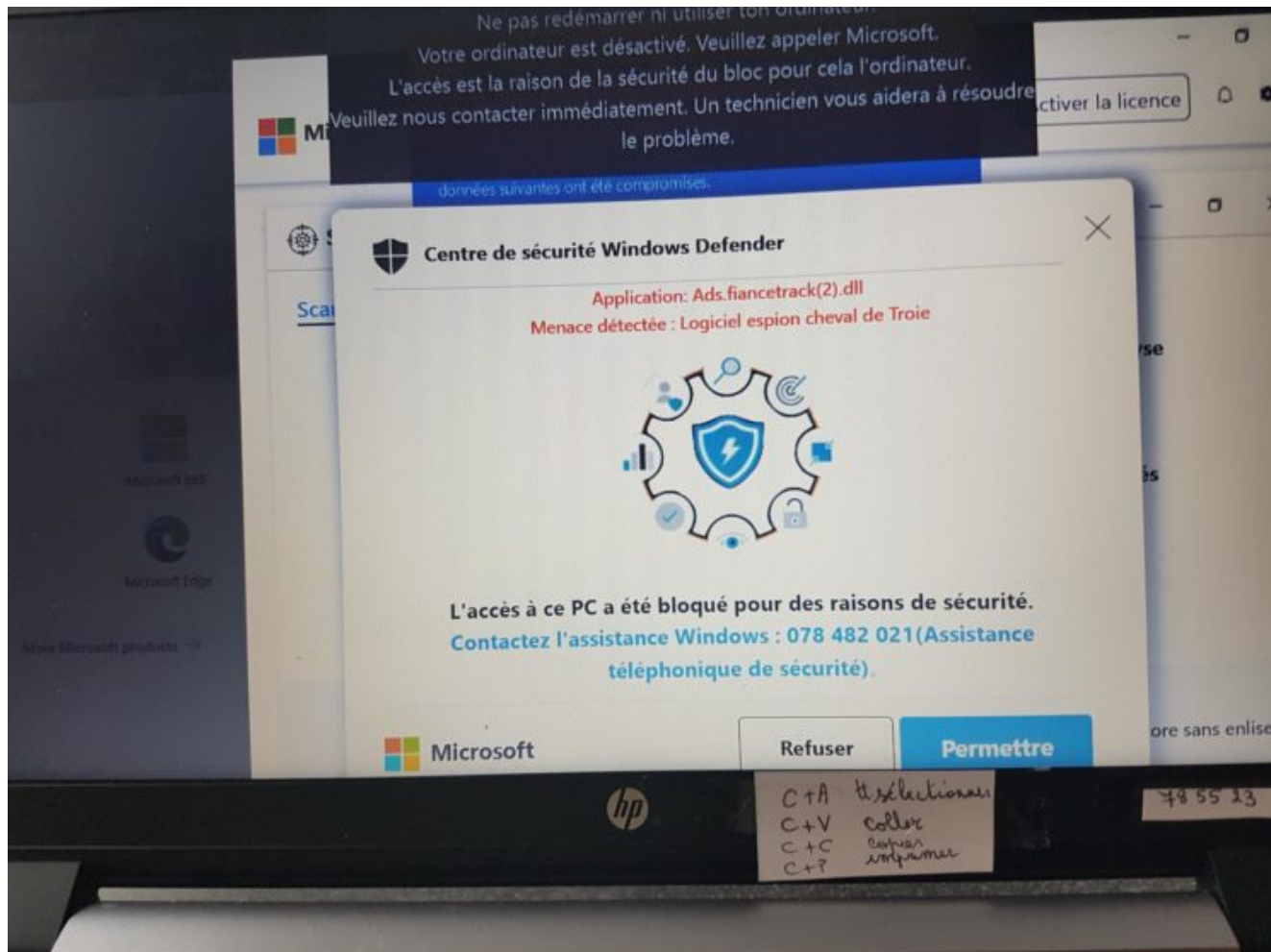


Arnaque au Support Microsoft - Ne vous faites pas avoir !

27/06/2022



Bonjour le Monde !

Vous surfez tranquillement sur des sites tout ce qu'il y a de plus sérieux quand ça vous arrange et merdiques quand ça ne vous arrange pas genre fesses de bouc, rasta gramme, what the fu... heu non, ouate sap et autres, nous faisons tous ça, pas vrai, et tout d'un coup, le bazar se met à gueuler qu'il y a un problème sérieux à régler très vite et vous n'avez plus droit qu'à une image qui à l'air tout-à-fait sérieuse et semble venir de chez Microsoft qui vous dit que Microsoft Defender a trouvé une grosse saloperie qu'il ne sait pas gérer tout seul et que vous devez appeler le support Microsoft de toute urgence et il s'agit bien sûr d'un numéro 078 surtaxé !

Il s'agit bien entendu d'une escroquerie qui essaie de forcer l'achat d'un contrat de support cher et vilain et sans doute factice aussi et qui n'a rien à voir avec Microsoft !

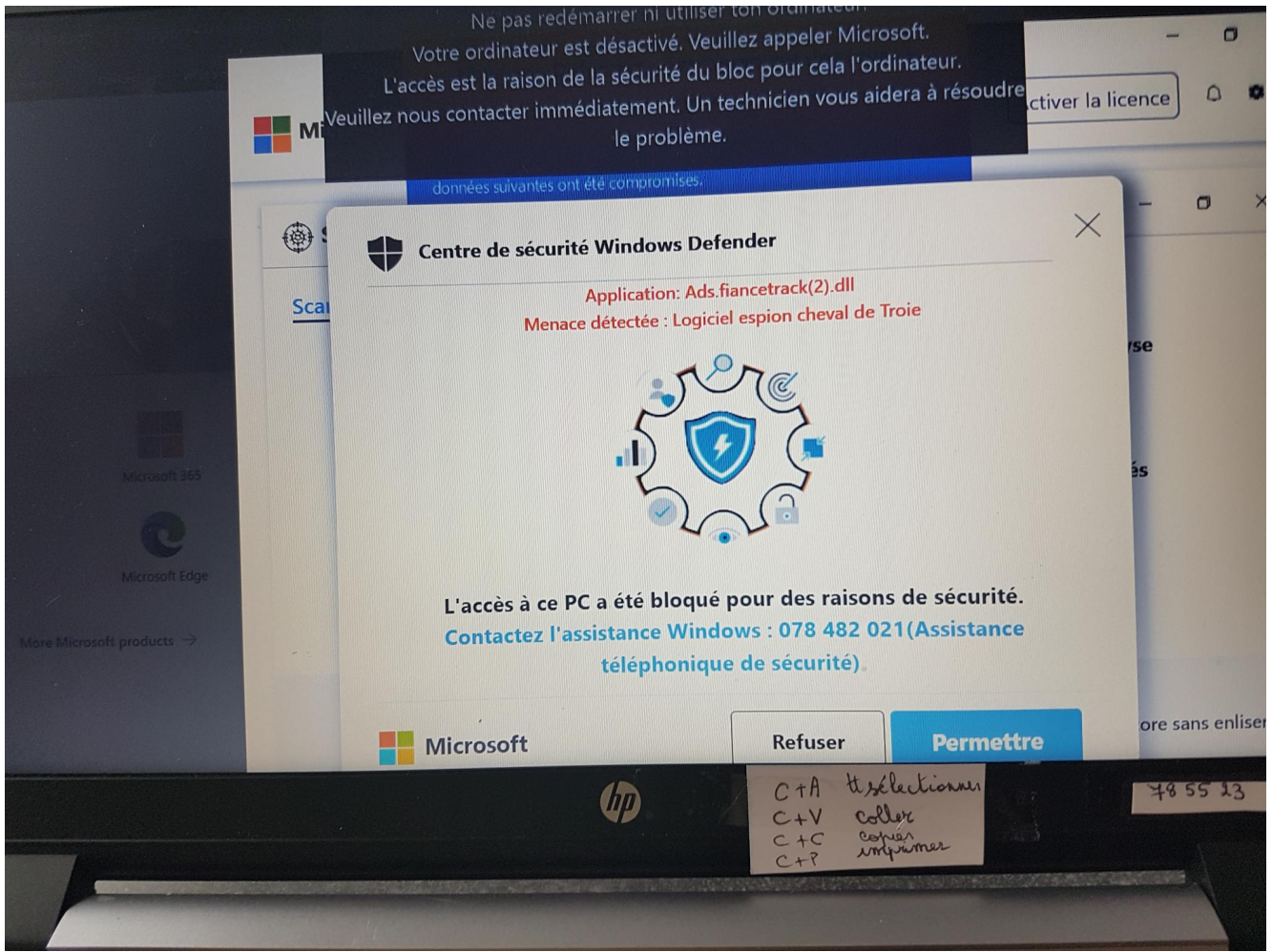
Il ne s'agit pas d'un virus (il n'y en a jamais eu sur votre PC) mais d'un malware appelé SCAM...

Les liens pour savoir de quoi il s'agit !

- <https://www.police.be/5306/actualites/le-microsoft-scam-lescroquerie-deg-uisee-en-intervention-technique>
- <https://support.microsoft.com/fr-fr/windows/prot%C3%A9gez-vous-contre-les-escroqueries-au-support-technique-2ebf91bd-f94c-2a8a-e541-f5c800d18435>

Ici cela s'est passé en ouvrant une image pour la voir en plus grand sur Facebook avec Firefox mais ça pourrait arriver sur beaucoup d'autres sites avec n'importe quel navigateur Internet...

Un exemple d'image affichée par votre navigateur Internet lors d'une fausse alerte Microsoft (Merci Jackie)



Le truc vous dit que votre PC est bloqué mais c'est de la vaste blague, c'est juste que cela ne marche pas quand vous cliquez sur Refuser ou sur la croix... Qui c'est qui a cliqué sur « Permettre » ?

Cette fenêtre à des airs de Microsoft sauf que le logo central est complètement fantaisiste, que la phrase « L'accès est la raison de la sécurité du bloc pour cela l'ordinateur » est du tellement bon français qu'on y croit dur comme fer et que jamais Microsoft ne vous demandera de téléphoner au support via un 078, jamais il ne vous demandera votre mot de passe ni votre carte de crédit (il vous a déjà pris des sous quand vous avez acheté le PC avec Windows dessus) !

Pour vous convaincre que le PC n'est pas bloqué, il suffit de taper Ctrl+Esc pour voir apparaître le menu démarrer...

La plupart du temps vous pouvez aussi taper Ctrl+Alt+Tab pour changer d'application si une ou des autres sont démarrées...

Donc pour s'en sortir:

- essayez de couper le son pour ne pas devenir dingue (comment ça c'est

trop tard ?)

- tapez **Win+R** pour faire apparaître une boîte de dialogue « Exécuter » (pour une fois ça porte bien son nom)
- tapez **taskmgr.exe** puis Enter/Entrée (taskmgr, c'est le gestionnaire de tâches)
- une petite fenêtre apparaît listant les programmes qui sont actifs (si c'est une grande fenêtre avec des trucs compliqués, tapez Alt+D)
- faites un clic droit sur le navigateur Internet (Firefox, Chrome, Edge ou autre)
- sélectionner « fin de tâche » (ça va flinguer le navigateur Internet et cette fausse alerte avec)
- et tout redevient normal ! Aaaaaah, ça fait du bien !!!!

Heureusement que vous n'avez pas cru un seul instant que cette alerte était réelle !

(j'aime bien taquiner...)

Bon, après ça, il va falloir retrousser un peu ses manches et nettoyer le navigateur Internet que vous avez utilisé et là c'est un peu moins sympa !

Il ne faut évidemment pas démarrer votre navigateur de la façon habituelle sous peine de relancer la cochonnerie...

Attention ! Il est possible que votre navigateur ne se souvienne plus des mots de passe de vos comptes après ce nettoyage mais vous avez tout noté dans un carnet magique, n'est-ce pas ?

Cré vindiou, ousske je l'ai mis ce carnet ? Mince, je n'ai jamais fait un tel carnet ou je ne l'ai pas tenu à jour !!!! Pas grave, préparez-vous à faire beaucoup de « Mot de passe oublié » !

Ah mais oui mais non hein ! Ça ne marche pas avec la banque... Ben laissez donc le malware sur votre PC si vous l'utilisez aussi pour la banque, ça fera plaisir au pauvre pirate qui doit bien gagner sa vie aussi !!!!

- Avec Firefox:
 - il faut à nouveau taper **Win+R** pour faire apparaître la boîte de dialogue « Exécuter »
 - taper (sans les guillemets) « **firefox.exe -safe-mode** » puis appuyer sur Enter
 - choisir « **Réparer** » dans la fenêtre qui s'ouvre

- la sale bestiole devrait avoir été éliminée
- Avec Chrome (de Google):
 - il faut à nouveau taper **Win+R** pour faire apparaître la boîte de dialogue « Exécuter »
 - taper (sans les guillemets) « **chrome.exe -disable-extensions** »
 - cliquer sur le menu dit « ellipsis » (3 points verticaux)
 - cliquer sur « Réinitialiser les Paramètres » ou d'abord sur « Paramètres Avancés »
 - cliquer sur « Restaurer les paramètres par défaut »
 - cliquer sur « Réinitialiser les paramètres »
 - la sale bestiole devrait avoir été éliminée
- Avec Edge (de Microsoft):
 - il faut à nouveau taper **Win+R** pour faire apparaître la boîte de dialogue « Exécuter »
 - taper (sans les guillemets) « msedge.exe -disable-extensions »
 - cliquer sur le menu dit « ellipsis » (3 points horizontaux ici)
 - cliquer sur « Rétablir les paramètres » dans la colonne de gauche
 - cliquer sur « Rétablir la valeur par défaut de tous les paramètres » dans la partie droite
 - cliquer sur « Réinitialiser »
 - la sale bestiole devrait avoir été éliminée

Je vous conseille fortement également d'effacer tout l'historique de votre navigateur !

<https://www.commentcamarche.net/securite/confidentialite/747-effacer-l-historique-ou-le-cache-d-un-navigateur-web/>

Ensuite, il faudra faire faire une analyse approfondie avec votre antivirus et éliminer tout ce qu'il va trouver ! C'est long mais nécessaire au cas où la cochonnerie a réussi à installer autre chose sur votre PC !

Comment ça vous ne savez pas comment on fait ? Pas grave vous n'êtes pas tout seul, moi non plus ! ... Je rigole !

Avec Defender: <https://www.pcastuces.com/pratique/astuces/5279.htm>

Avec Avast: <https://support.avast.com/fr-be/article/antivirus-pc-virus-scan/>

Avec

AVG:

https://support.avg.com/SupportArticleView?l=fr&urlname=avg-antivirus-pc-virus-scan&retUrl=support_Free

Avec Bitdefender: pas trouvé !

Si vous vous prenez cette alerte sous Linux ou Mac, vous savez sans aucun doute possible qu'il s'agit d'une crasse puisque ce n'est pas Microsoft et encore moins Microsoft Defender qui tourne sur votre PC.

Il faudra néanmoins nettoyer votre navigateur Internet de la façon adaptée à Linux ou Mac !

Hé quoi, Li P'ti Fouineu, tu ne nous explique pas comment on fait ?

Ben non, parce qu'il y a peu de chance que ça arrive et je ne veux pas vous faire un article indigeste de 500 lignes !

Je connais une personne qui a appelé le numéro affiché et quelqu'un a pris le contrôle de son PC, travaillé dessus pendant 2 heures et fait acheter un contrat de support bien cher (300€ pour 1 an) sans qu'on sache si il n'a pas installé d'autres saloperies ni capturé les informations de paiement (car l'achat s'est bien évidemment fait via le PC) !

Une autre personne m'a appelé et le PC a été nettoyé en moins d'une heure en appliquant la recette expliquée ici !

Si j'ai la patience, je ferai une petite vidéo pour montrer comment nettoyer votre navigateur Internet... Ben oui, moi aussi je suis fainéant...

En conclusion:

Il est quasi impossible de se protéger à 100% de ce genre de cochonnerie mais vous pouvez opter pour une navigation privée (dite aussi incognito) sur votre navigateur.

Cela n'empêchera pas la bestiole mais ce sera nettoyé automatiquement lorsque vous quitterez votre navigateur.

Comment démarrer une session incognito/privée sur votre navigateur Internet préféré:

- Firefox: Ctrl+Shift+P
- Autres: Ctrl+Shift+N (Cmd-Shift N sur Mac)

Il y a aussi moyen d'activer la navigation privée en permanence...

Et comment que c'est-y qu'on fait avec un Smartphone ou une tablette ?

Un peu plus d'info pour tout le monde sur https://www.frandroid.com/comment-faire/tutoriaux/569837_comment-passer-en-navigacion-privee-sur-chrome-safari-firefox-opera-tutoriel-pour-debutants

Li P'ti Fouineu vous salue bien !

Ps: la touche Win, c'est la touche entre la touche Ctrl et la touche Alt et qui arbore 4petits carrés ondulés (symbole de Windows d'où le nom de la touche)

Quand on indique Win+R, ça veut dire appuyez et maintenir la touche Win, puis appuyer sur la touche R pour enfin relâcher le tout...

La touche Shift est la touche qui permet temporairement de taper une majuscule...(elle arbore souvent une flèche vers le haut) et est située juste au-dessus de la touche Ctrl (sur la gauche du clavier)

Cette gymnastique étrange s'appelle « utiliser des raccourcis clavier »