Arnaque au faux support technique

Actuellement, nous entendons beaucoup parler d'une arnaque dite « arnaque au faux support technique ».

Cette arnaque consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l'apparition d'un message, d'une fenêtre sur l'écran, qui bloque son ordinateur ou tout au moins son écran, lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement afin de la pousser à contacter un prétendu support technique officiel (Microsoft, Apple, Google, fournisseur d'accès, marque de matériel informatique…), pour ensuite la convaincre de payer un pseudo-dépannage informatique et/ ou à acheter des logiciels inutiles, voire nuisibles.

But recherché :

Soutirer de l'argent à la victime en la poussant à laisser prendre le contrôle de sa machine pour faire semblant de la dépanner et lui vendre et lui installer des logiciels inutiles et quelques fois générateurs d'adwares (logiciel indésirable conçu pour afficher des publicités intempestives sur votre écran), lui faire souscrire des abonnements inutiles et inefficaces qui lui seront facturés.

Comment les pirates procèdent-ils ?

1er épisode : « l'introduction » dans votre ordinateur.

- Vous avez ouvert un mail douteux (publicitaire en général) qui vous a incité à visiter un site internet,
- Vous avez cliqué sur une publicité (sur une page internet, sur Facebook…),
- Vous êtes allé sur un site pas très sûr, ou un site qui a été infecté par un pirate…

2ème épisode : le « popup ».

Le popup est une fenêtre qui s'ouvre de façon intempestive sur votre ordinateur.

En temps normal un popup n'est pas malveillant (sur un site, cela peut être une information complémentaire à l'article que vous lisez, une aide pour remplir un formulaire en ligne, une invitation à s'inscrire à une newsletter, une incitation à cliquer sur un lien, une publicité, etc…

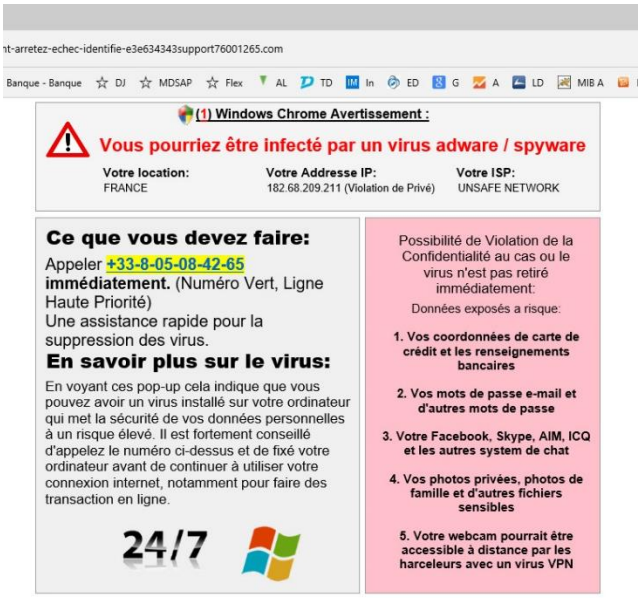
Ceux qui ont des antivirus gratuits type Avast ou Avira doivent en voir régulièrement (alertes et publicités pour inciter à passer à la version payante ou acheter des logiciels de l'éditeur).

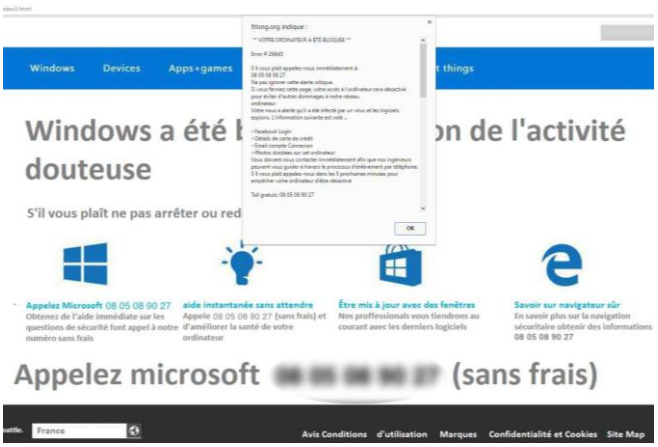
Si le popup arrive à prendre tout l'espace de l'écran, vous pensez que l'ordinateur est bloqué.

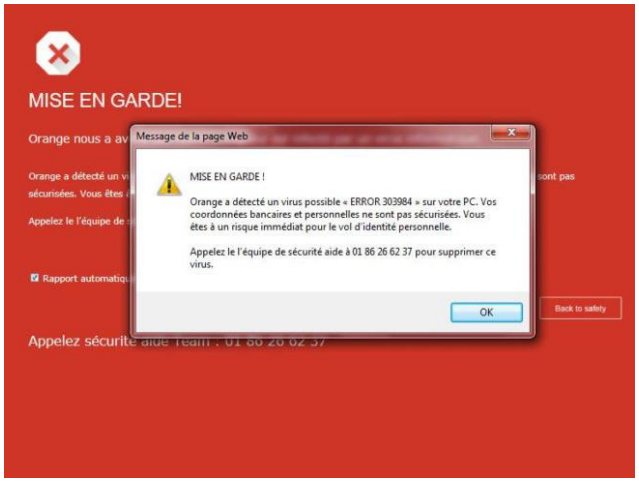
Un popup n'est pas un virus, ni un logiciel espion (même si c'est peut-être un logiciel espion qui a favorisé son apparition), ce qui explique que les antivirus, même à jour peuvent les laisser passer.

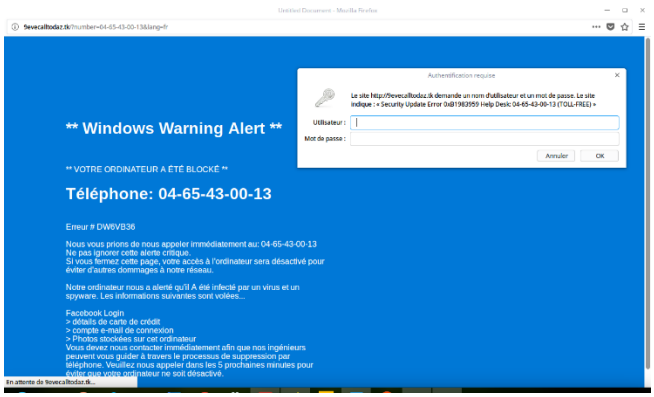
Cette image est là pour vous faire peur.

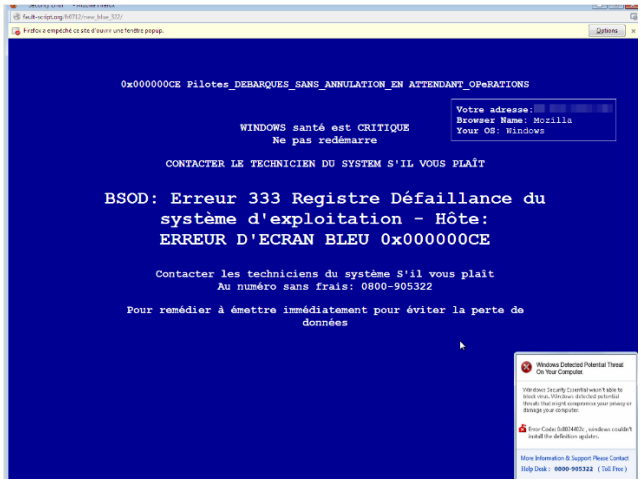
En voici quelques exemples visuels :











3ème épisode : l'intervention du faux support

Comment ça se déroule en général

Vous êtes en train de surfer sur Internet. Tout à coup, une fenêtre s'ouvre et un message semblant provenir de Microsoft, (ou éditeur de logiciel antivirus, ou de SFR, ou d'Orange, etc…) apparait sur votre écran.

Cette page affiche de faux messages, toujours très inquiétants, indiquant que votre ordinateur est bloqué, infecté ou en passe de l'être. « Votre ordinateur a été bloqué » « Windows a été bloqué en raison d'une activité douteuse » « ne redémarrez pas votre ordinateur car vous risquez de perdre toutes vos données » « si vous fermez cette fenêtre, votre accès à l'ordinateur sera désactivé pour éviter d'autres dommages à notre réseau » « ERREUR #DW6VB36 » « votre ordinateur est devenu lent et affiche des publicités indésirables » « Windows a détecté une altération des données, un virus »… bref beaucoup d'imagination dans ces messages sensés provoquer la panique chez l'utilisateur.

Bien sûr, quelque part dans la fenêtre un numéro de téléphone à appeler (support gratuit !) de toute urgence pour résoudre ce problème.

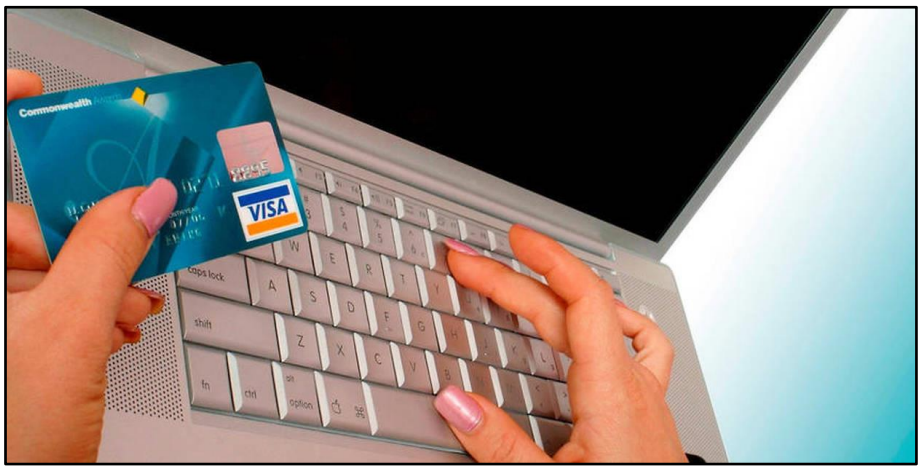
Au bout du fil un « soi-disant technicien » qui laisse entendre qu'il fait partie du support technique de Microsoft ou qui en tout cas est agréé par Microsoft. Au bout du fil, la personne est compatissante et inquiète. Elle affirme être en capacité de résoudre le problème.

La première chose qu'elle vous demande est d'installer un logiciel de prise en main à distance (Logmein ou autre).

Vous donnez identifiant et mot de passe et la personne prend la main sur votre ordinateur.

Elle va faire un tas de manipulations dans le but de renforcer chez vous l'idée que votre ordinateur est effectivement bien infecté (en allant dans des secteurs de l'ordinateur que vous ne connaissez pas, en faisant passer pour inquiétants des fichiers systèmes légitimes, en faisant des copier/coller d'alertes dans des fichiers textes qu'ils ouvrent…).

Une fois que vous êtes complètement stressé, ils vous proposent de vous vendre et de vous installer des logiciels de protections (qui au mieux ne servent à rien, au pire seront une porte d'entrée pour de prochaines attaques, réelles celles-là), de souscrire un abonnement à leur assistance technique, bref à faire chauffer la carte bleue…



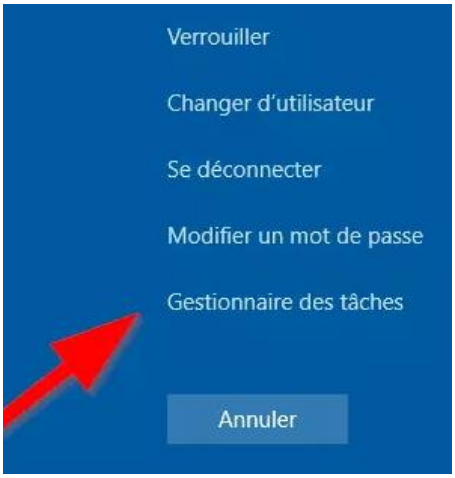
Que faire si le pop-up apparait et bloque le système

Fermez votre navigateur.

Si vous ne pouvez pas atteindre la croix rouge pour fermer le navigateur (si le pop-up prend tout l'écran) : appuyer simultanément sur les touches CTRL + ALT + SUPR

Une fenêtre bleue s'ouvre.

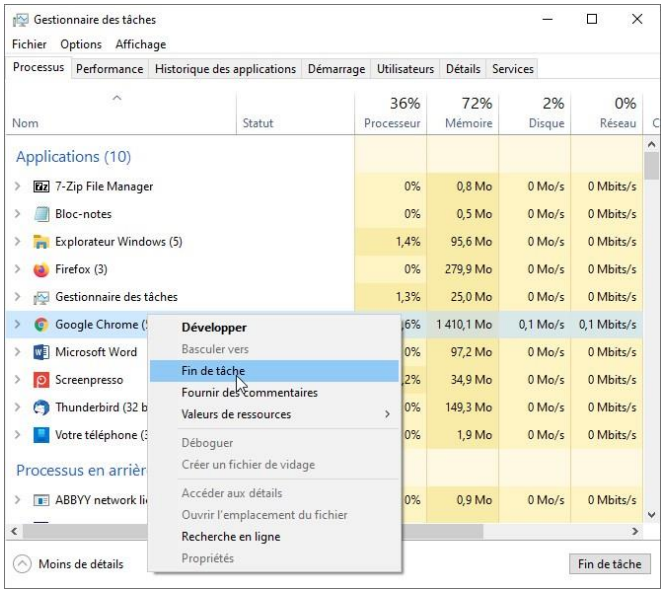
Cliquez sur « gestionnaire des tâches »



Une fois le gestionnaire de tâches ouvert, repérez votre navigateur dans la liste des applications qui fonctionnement (Firefox, Chrome…).

Faites un clic droit dessus et cliquez (gauche) sur « fin de tâche ».

Si tout va bien, votre navigateur dans lequel s'est ouvert le pop-up est fermé. (Et le pop-up avec).



Dans certain cas le pirate bloque la procédure **CTRL + ALT + SUPR**. Ne paniquez pas !

Recours ultime, éteignez l'ordinateur « à la sauvage » en maintenant le bouton marche arrêt appuyé plusieurs secondes.

Il ne vous reste plus qu'à nettoyer votre navigateur au prochain démarrage (supprimer les cookies, vérifier les paramètres).

Et à faire les scan antivirus, anti adware (Adwcleaner, Malwarebyte), les vérifications de mise à jour (Windows, navigateur, antivirus).

Que faire si on s'est fait piéger :

- Fermer le navigateur. À son redémarrage, nettoyez-le (supprimez les cookies, vérifiez également qu'une extension douteuse n'a pas été installée).
- Désinstaller tous les logiciels que le « technicien » vous a installé (prise en main à distance, logiciels « de sécurité » … Pour plus de sûreté, allez dans le gestionnaire d'application et classez-les par date. Et supprimez toutes celles que vous ne connaissez pas et qui sont de la date de l'intervention
- Changez vos mots de passe.
- Signalez l'arnaque (sur le portail du ministère de l'intérieur internet-signalement.gouv.fr/)
- Vérifiez que votre système (Windows) est à jour, que votre navigateur (Chrome, Firefox) est à jour, que votre antivirus est à jour et actif.
- Contactez au plus vite votre banque pour essayer de faire bloquer la transaction en faisant opposition, ou vous faire rembourser en indiquant que vous allez porter plainte (commissariat ou gendarmerie).
- Essayer de récupérer des éléments sur ce qui s'est passé (prendre des photos de votre écran, noter le numéro de téléphone) pour la suite de la procédure.
- Faites une analyse compète avec votre anti-virus.
- Faites un scan avec les logiciels anti adwares (Adwcleaner puis Malwarebyte).

Comment éviter de se faire piéger :

- Tenez à jour votre système (Windows), vos logiciels et entre autres vos navigateurs, tenez à jour votre antivirus.
- Vérifiez que votre pare-feu est activé.
- Faites régulièrement un scan de votre ordinateur avec Adwcleaner et Malwarebyte. Et dès que vous voyez que votre ordinateur change de comportement (modification de la page d'accueil ou du moteur de recherche de votre navigateur, des pop-up plus fréquents, un ralentissement conséquent de votre ordinateur…).
- Évitez les sites peu sûrs ou inconnus.
- N'ouvrez pas les mails dont vous ne connaissez pas l'expéditeur, avec des contenus douteux ou trop beaux pour être vrais (vous avez gagnez à la loterie, cliquez ici pour récupérer votre gain, profitez de 80% de réduction sur le dernier iPhone…). Comme le dit si bien Jean, le Père Noël n'existe pas sur internet. Ne cliquez par sur des liens dont vous n'êtes pas sûr.
- De la même façon ne cliquez pas sur des publicités trop alléchantes sur Facebook ou sur les sites que vous visitez…
- N'oubliez pas de faire régulièrement des sauvegardes de votre système et de vos données.
- Quand vous souhaitez télécharger un logiciel gratuit, priorisez le site officiel de l'éditeur, sinon, allez sur des sites de téléchargement ayant bonne réputation (par exemple : Clubic, Comment ça marche, PC Astuces) et évitez certains autres (comme 01.net, Softonic, PC tuto, telechargement.com…) qui vous proposent des packages : le logiciel principal + d'autres logiciels annexes, parasites ou vecteurs d'adwares). Dans tous les cas il est conseillé lors de l'installation de demander la procédure détaillée pour avoir la main sur toutes ces installations annexes.

N'oubliez pas,
restez prudent sur internet…
Et en cas de doute, « Allo ADEMIR »

-fig 1 : Le phishing "à l'ancienne"-