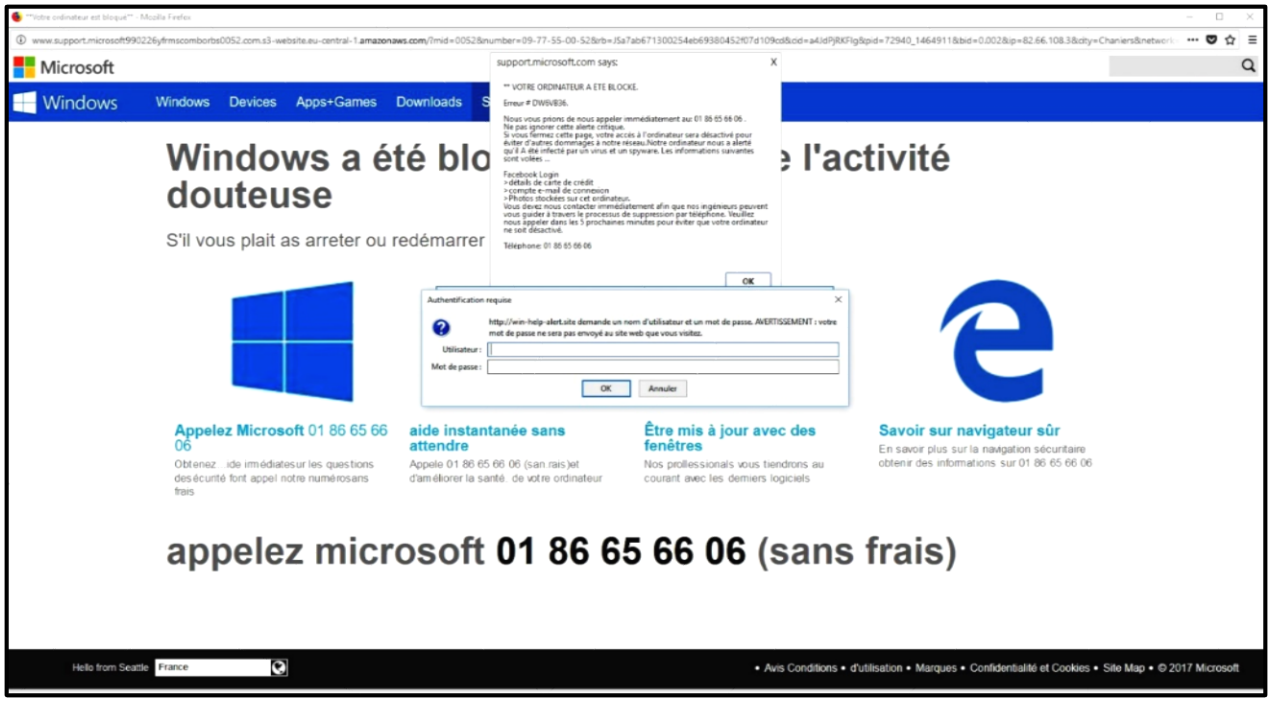
Ordi bloqué par rançongiciel

Vous surfez tranquillement sur un site web, légal ou non (streaming, torrent, porno), lorsqu'une alerte critique du Support Microsoft par exemple, vous indique que votre ordinateur a été bloqué et vous invite à appeler un numéro de téléphone.

Selon ce message, si vous n'appelez pas dans les 5 prochaines minutes ou si vous fermez simplement la page affichée, vous ordinateur sera bloqué. Vos données personnelles seront cryptées inutilisables.



Il s'agit bien évidemment d'une arnaque. **N'appelez surtout pas le numéro**. De nombreux internautes se sont déjà fait soutirer plusieurs centaines d'euros et ont laissé un contrôle total de leur ordinateur à des personnes malveillantes capables de paralyser l'ordi voire tous les ordis connectés au réseau via la Box.

L'intrusion de ce script malveillant sur votre ordinateur est dû au fait que votre machine était probablement insuffisamment protégée, ouverte à tous vents, peu ou pas assez sécurisée de façon préventive :

- Windows, navigateurs, antivirus, applications obsolètes ou **non régulièrement mis à jour**,
- Ordinateur mal paramétré, contaminé, mal nettoyé, mal entretenu,
- Absence d'antivirus ou antimalwares,
- Navigation sur sites web frauduleux etc…

Voici quelques pistes pour tenter de vous dépêtrer de ce script malveillant de plus en plus présent sur web, une procédure en plusieurs étapes :

1. D'abord pas de panique, la situation est critique mais pas désespérée, donc inutile de l'aggraver :
    a. Ne pas toucher à la souris pour ne pas authentifier l'intrusion, ne pas payer de rançon,
    b. Appuyer sur les touches Alt et F4 du clavier pour fermer fenêtres et boîtes de dialogue contenant du code malicieux,
    c. Sinon fermer le navigateur à l'aide du gestionnaire de tâches de Windows (Alt+Contôle+Sup suivi de fin de tâche du navigateur).
2. Arrêter la propagation
    a. Débranchez les disques externes encore sains pour éviter le chiffrement de vos fichiers encore intacts et isolez l'ordinateur dans votre réseau pour éviter que le logiciel malveillant se propage à d'autres ordinateurs.
    b. Déconnecter internet.
3. Décontaminer l'ordinateur
    a. Désinstaller complètement le navigateur corrompu (en supprimer toutes les traces)
    b. Utiliser les méthodes de décontaminations des logiciels malveillants (simples du genre Malwarebytes ou plus complexes à mettre en œuvre).
    c. Réinstaller le navigateur, ne pas hésiter à le tester pour vérifier si la fenêtre d'alerte ne surgit pas à nouveau, sinon tout reprendre à zéro.
    d. Les ransomwares qui ne chiffrent pas les fichiers sont plus faciles à retirer, cependant les fichiers chiffrés par les ransomwares ne seront pas automatiquement récupérés en supprimant le programme ransomware lui-même
4. Eventuellement initialiser la Box si elle a été contaminée
5. Restaurer si besoin (système et données) à partir des sauvegardes, restauration nécessaire si les fichiers ont été cryptés pour les rendre inutilisables.
6. Sécuriser l'ordi en appliquant les mesures préventives pour éviter une nouvelle intrusion de ransomware
7. Signaler aux autorités (pour combattre ce fléau)

<u>En conclusion :</u>

La décontamination de cette prise de contrôle va s'avérer de plus en plus difficile voire impossible avec le développement exponentiel de ce code malveillant de plus en plus spécifique et complexe à éradiquer.

Attention aux faux outils de décontamination diffusés sur le net capables d'être encore plus frauduleux !

Dans tous les cas, des **solutions préventives efficaces existent** et sont vivement recommandées en cette année 2018, sinon tout laxisme et inconscience sont à payer au prix fort par les internautes imprudents.

Guy NEAULEAU

Notes :

https://www.pcastuces.com/pratique/astuces/4977.htm

https://www.bitdefender.fr/tech-assist/self-help/removing-police-themed-ransomware-malware.html

https://www.avast.com/fr-fr/c-ransomware

https://stopransomware.fr/nettoyer-son-ordinateur/

http://www.cnetfrance.fr/produits/guide-protection-fichiers-ransomware-39836850.htm

https://www.etsmtl.ca/Services/sTI/A-propos-des-sTI/BSTI/Rancongiciels