Virus : Windows a détecté des activités suspectes

Dernièrement, quelques internautes se plaignant d'un Trojan Winlock qui pousse des arnaques téléphoniques.
Le but ici est de bloquer l'ordinateur en faisant croire à une erreur de Windows afin de faire contacter une hotline téléphone.
Cette dernière va désinfecter l'ordinateur et vous faire abonner à leurs support mais aussi d'acheter des logiciels de désinfection et de nettoyage.
En général, les prix pratiqués sont très exorbitants.

Les Trojans WinLock ne sont pas nouveaux, fin 2011, des Trojan Winlock se faisant passer pour les autorités sont apparus, voir cet article : Trojan.Winlock / Trojan.Ransomware : Virus Police
Le procédé des arnaques téléphoniques depuis 3 ans ne l'est pas non plus, ces derniers tentaient plutôt de bloquer les navigateurs internet à travers des pages internet, comme Trojan Browlock (Browser Locker).

Ici il s'agit un peu d'un mixte des deux, puisque ce Trojan Winlock va demander à contacter une hotline téléphonique pour pousser ces arnaques de support téléphoniques.
Pour cela, l'avertissement affiché par le trojan tente de se faire passer pour un message d'erreur de Windows.

Le virus : Windows a détecté des activités suspectes

D’un point de vue fonctionnement n’apporte rien de nouveau depuis les trojan Fake Police.
Ce dernier se fait passer pour une mise à jour de Windows avec un pourcentage d’avancement rapide.

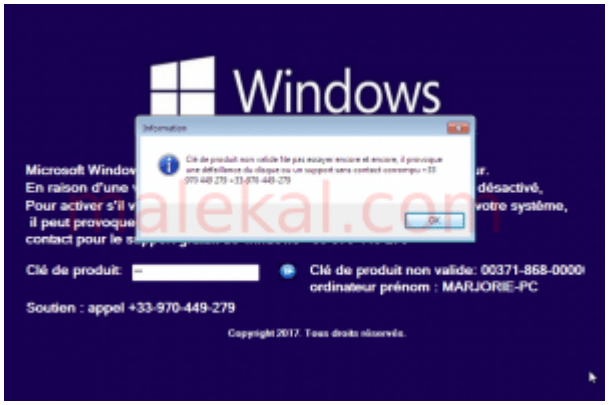
puis une erreur apparaît… afin de faire croire que la mise à jour s’est mal passée.
Le message de blocage de l’ordinateur s’affiche ensuite :

Microsoft Windows a détecté des activités suspectes sur cet ordinateur.
En raison d'une violation de sécurité réseau, Microsoft Windows s'est désactivé
Pour activer s'il vous plaît entrer la clé de produit. Ne pas redémarrer votre système, il peut provoquer une défaillance du disque dur ou corrompu
contact pour le support gratuit de windows +33 970 449 279

Clé de produit non valide:
Copyright 2017. Tous droits réservés.

Et si vous saisissez une mauvaise clé de déblocage, un avertissement bidon apparaît :

Clé de produit non valide. Ne pas essayer encore et encore, il provoque une défaillance du disque ou du support sans contact corrompu +33 970 449 279



L’ouverture du gestionnaire de tâches est bloqué afin de ne pas pouvoir tuer le processus du Rogue.TechSupportScam.

Cette infection est propagée par des cracks vérolés (je rappelle ce sujet : Le danger des cracks et keygen) et a été vu avec l’adware Mail.Ru.
En clair donc, ceux qui utilisent torrent ou le premier site venu pour télécharger un crack seront des victimes de cette infection.

Informations techniques

Le malware se loge dans deux dossiers :

- C:\ProgramData\windowsupdate
- C:\ProgramData\windiskutility

Les clés startup suivantes sont utilisées pour démarrer le malware au lancement de la session :

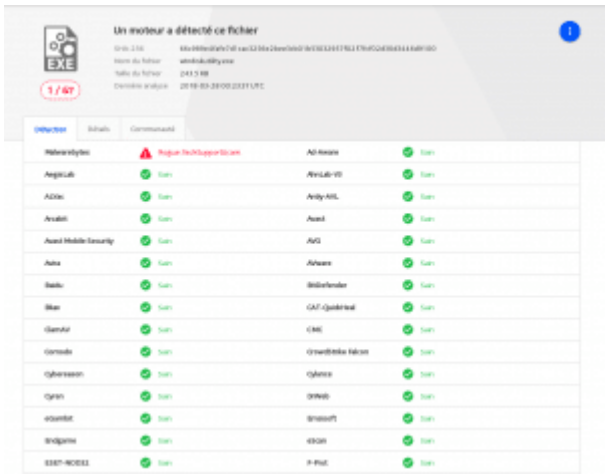
```
Startup:      C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\windowsdriver.lnk
Startup:      C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\windowsupdate.lnk
```

Il faut supprimer les deux dossiers ProgramData pour supprimer ce Trojan Winlock.

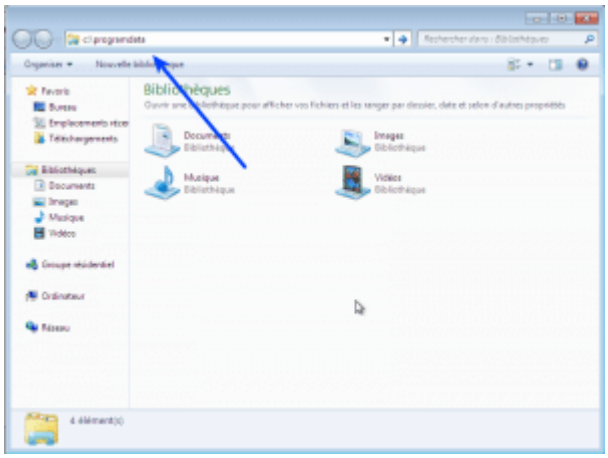
Supprimer le virus « Windows a détecté des activités suspectes »

Ce Trojan Winlock n'est pas non plus actif en mode sans échec.
Vous pouvez donc utiliser ce mode pour scanner l'ordinateur, pour rappel le mode sans échec avec prise en charge du réseau permet d'avoir internet.
Pour démarrer en mode sans échec, lire ce lien : Démarrer Windows en mode sans échec

Toutefois, la détection est plutôt mauvaise, donc votre antivirus risque de ne rien détecter.
Sur la version récupérée, seule MalwareBytes Anti-Malware est capable de le détecter en **Rogue.TechSupportScam**

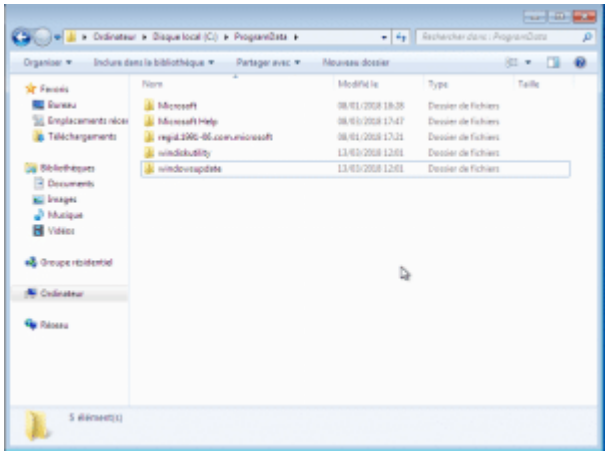


Pour le supprimer manuellement, saisissez C:\ProgramData dans la barre d’adresse de l’explorateur de fichiers.



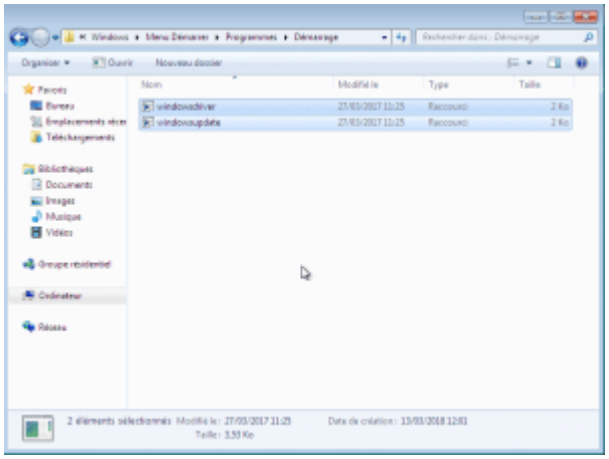
Localisez les dossiers suivants et supprimez les :

- C:\ProgramData\windowsupdate
- C:\ProgramData\windiskutility



Enfin, il faut supprimer les points de chargement du malware,

pour cela dans la barre d'adresse saisissez : *shell:common startup*
Ensuite supprimer les deux raccourcis windowsdriver et windowsupdate



Redémarrez en mode normal, vous devriez être débarrassé de ce malware.
Vous pouvez terminer par un nettoyage Malwarebytes Anti-Malware ou un scan en ligne NOD32.

Il est probable que le malware évolue et que les auteurs cherchent à bloquer le mode sans échec afin de rendre sa suppression plus difficile.

Supprimer le virus « Windows a détecté des activités suspectes sur cet ordinateur » en vidéo

Autres liens

La leçon du jour, arrêtez de télécharger des cracks, si vous ne savez pas les choisir.

A lire ce article sur les virus et trojans : Comment les virus informatiques sont distribués

et pour sécuriser Windows : Comment sécuriser mon Windows