Acronis anti-ransomware: alerte au phishing !

Bonjour le Monde !

Dans **la brouette de news pour les geeks** en juillet, j'ai parlé de de l'antivirus **BitDefender Free** et de **Acronis Protection contre les Ransomwares** (gratuit également).

J'ai installé les deux en juillet et n'ai eu aucun problème jusqu'à aujourd'hui où **BitDefender** a tout d'un coup généré des **alertes au phishing** à peu près toutes les 5 secondes !

Les messages d'erreur étaient très incompréhensibles (comme trop souvent) mais parlaient des ports 6109 et 9110 qui sont utilisés par les programmes Acronis (**StartPage** est mon ami) !
=> désinstallation du programme Acronis et redémarrage du PC et les erreurs sont calmées !

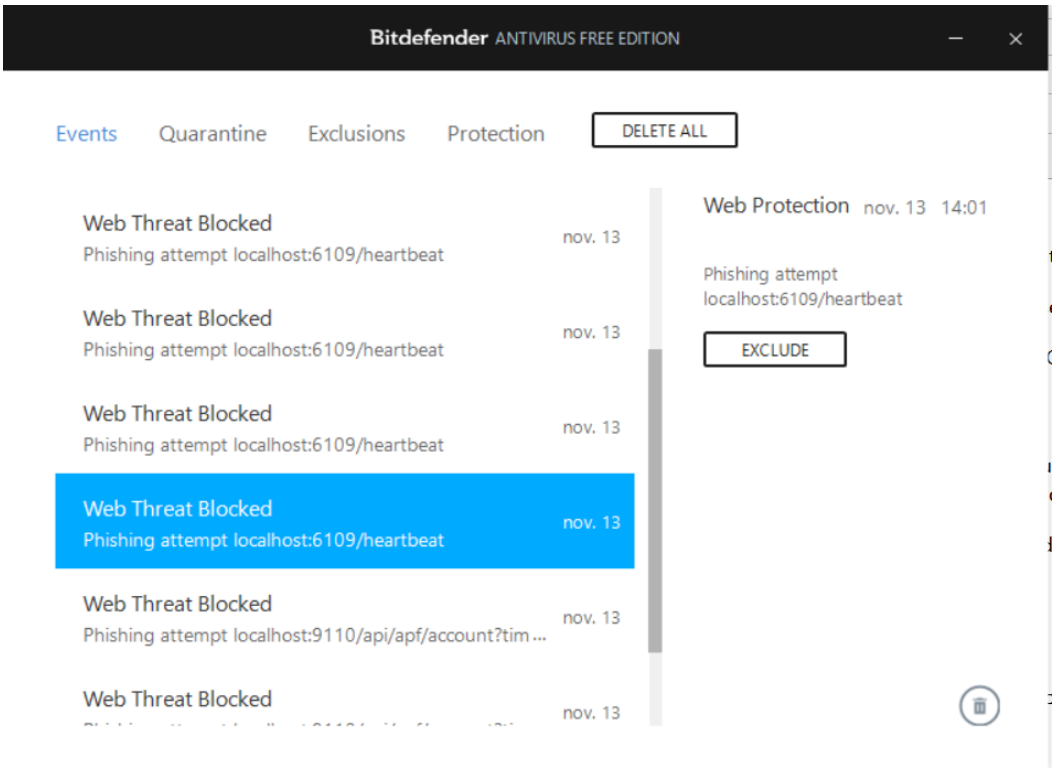
Scan antivirus (BitDefender) et anti-rootkit (MalewareBytes) avec chacun ayant trouvé une saloperie => effacement des cochonneries et nouveau redémarrage du PC.
Nettoyage avec Ccleaner (dernière version) => 1.8GB de fichiers temporaires effacés et environs 750 erreurs corrigées dans la base de registre (je n'avais plus fais cela depuis pas mal de temps).

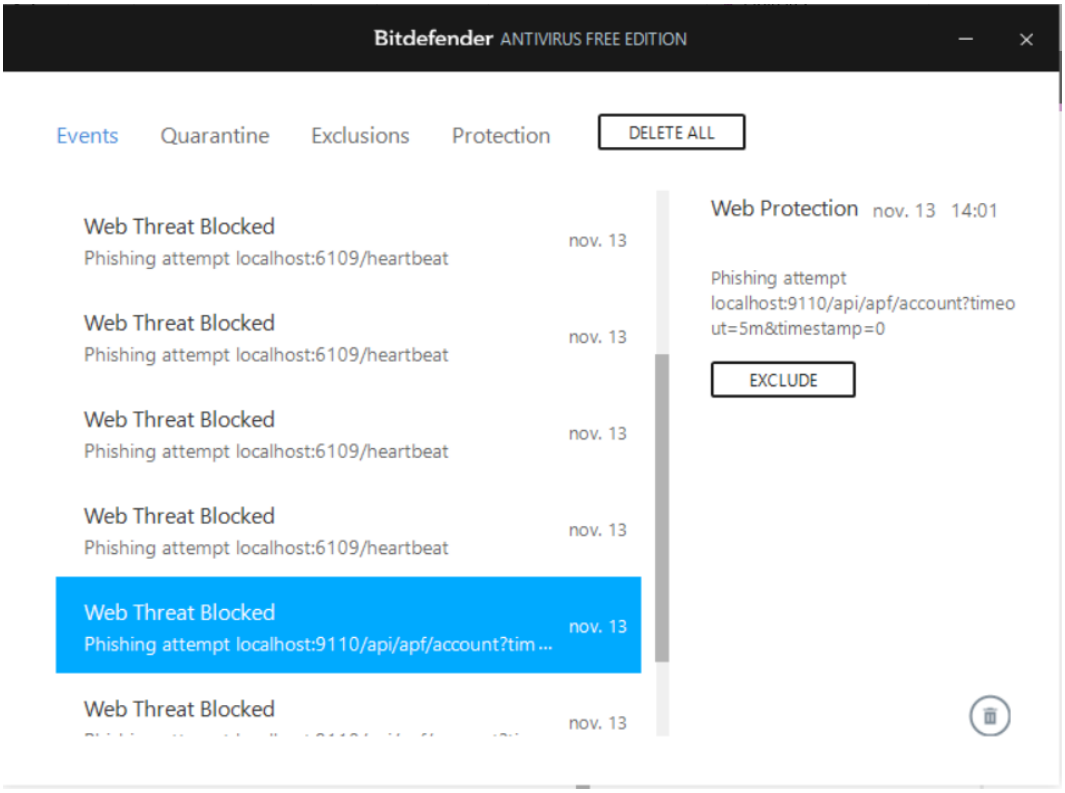
Vérification sur le site d'Acronis: il n'y a pas de nouvelle version du programme de protection anti-ransomware (ou pas encore) => je vais essayer de les informer du problème…

Bref, si vous avez aussi installé Acronis Protection contre les ransomwares sur un PC Windows, je vous conseille de le désinstaller par précaution !

Pour les geeks: lors d'un tel incident, il faut d'abord collecter les infos données par les alertes, puis il faut vérifier quels programmes utilisent les ports cités dans les alertes sur votre PC pour désinstaller ces programmes car ils présentent un faille de sécurité exploitée par le malware qui tente de faire du phishing à vos dépends.

Voici les alertes générées de BitDefender qui montrent ici que les ports 6109 et 9110 sont utilisés par le malware pour tenter de collecter certaines de vos infos personnelles (phishing); localhost signifie qu'il s'agit de ports utilisés sur votre PC:





Pour trouver le programme qui utilise ces ports et qui se fait exploiter par le malware voici trois manières de faire:

- Démarrer une **invite de commande en mode admin** (clic droit sur le bouton Windows, bouton “Démarrer” avant) et taper **netstat -ab** et vérifier la liste pour les port cités dans l’alerte
- Télécharger **TCPview** qui vous fait ça en mode graphique… => regarder quel programme utilise les ports cités dans l’alerte
- Faire une recherche sur Internet pour “tcp port xxxx” en remplaçant “xxxx” par les numéros de ports cités dans l’alerte

J’ai utilisé la 3e méthode et le 2e article retourné par StartPage est la liste des ports à ouvrir dans un pare-feu pour les produits Acronis; dans cette liste, le port 6109 est utilisé par Acronis pour la protection active => Acronis utilise bien ce port 6109 => j’ai désinstallé Acronis et plus de problème => CQFD !

Trois remarques pour conclure:

- **Ne soyez pas parano** ! Un programme de protection (ici BitDefender) peut prendre une activité normale pour un problème; on parle alors de faux-positifs ou fausse alerte. Comme on n'en sait encore rien, il faut d'abord réagir et stopper le problème, puis vérifier plus loin…
- **Restez vigilant** ! Un programme de protection n'est pas une protection infaillible; ne faites pas une confiance aveugle à votre protection et restez vigilant !
- **Ré-évaluez régulièrement vos protections**; la malhonnêteté sur Internet est en évolution constante !
- **Un port TCP** est un point d'entrée de votre PC; imaginez que votre PC ait une adresse sur Internet comme un building à appartement a une adresse postale, on dira que le port TCP est la boîte aux lettre d'un appartement. Si la boîte aux lettres est mal fermée, on peut vous piquer votre courrier… Idem sur le PC via un port TCP mal protégé…

Li P'ti Fouineu vous salue bien !