Phishing, kekseksa ? De la cybercriminalité bien sûr !

Bonjour le Monde !

Le phishing (anglais) ou hameçonnage (français), est une tentative de vol d'information personnelle pour perpétrer une usurpation d'identité le plus souvent dans le but de voler de l'argent bien entendu…

Cela peut se faire de multiples façons mais les messages (instantanés, SMS et mails) sont le vecteur le plus courant de ces tentatives et je vais me concentrer là-dessus dans ce qui suit…

En 2016 et 2017, j'ai écrit une **série d'articles sur la cybercriminalité** qui mettait en lumière le manque total de concertation et d'efficacité dans la lutte contre les Ransomware et le phishing et puis les frémissements d'amélioration …

Nous sommes en 2020 et la lecture d'un petit encart dans Test-Achats me fait

revenir sur ce sujet toujours brûlant !

Comme déjà mentionné au rayon Geek dans Les News de Mars 2020, les signalements de phishing explosent en 2019 et ont déjà permis à la **Computer Crime Unit** de bloquer 4000 faux sites faisant du phishing !

La tendance actuelle des pirates est de vous envoyer un mail ressemblant à s'y méprendre à un mail provenant d'une grande enseigne (Colruyt, Lidl, votre banque, etc) et soit piquant votre curiosité soit essayant de vous faire peur pour que vous cliquiez sur des liens qui vous enverront évidemment sur un site pirate et qui vous soutirera un maximum d'information et/ou d'argent ! C'est ce genre de site que peut fermer la Computer Crime Unit grâce aux signalements !

Dans Les News de Mai 2019, je vous suggérais de vous entraîner à détecter un mail de phishing sur le site **https://www.cybersimple.be/fr/quiz/phishing** qui est toujours d'actualité, essayez ou ré-essayez donc !

Prenons quelques exemples complètement fictifs:

- **Promotion Colruyt**

1. vous recevez un message de Colruyt vantant une "promotion que vous ne pouvez pas rater"
2. **ne cliquez sur aucun des liens contenus dans ce message**
3. fermez ce message
4. visitez manuellement le site colruyt.be en entrant l'adresse du site vous-même dans votre navigateur Internet ou en faisant une recherche du site
5. vérifiez que cette promotion existe vraiment
6. si la promotion est soi-disant uniquement pour vous, prenez contact par un autre moyen avec Colruyt pour vérifier

- **Bon d'achat chez Lidl**

1. vous recevez un mail de Lidl vous offrant un bon d'achat de 500 €
2. **ne cliquez sur aucun des liens contenus dans ce message**
3. fermez ce message
4. visitez manuellement le site lidl.be en entrant l'adresse du site vous-même dans votre navigateur Internet ou en faisant une recherche du site
5. vérifiez que cette promotion existe vraiment
6. si la promotion est soi-disant uniquement pour vous, prenez contact par

un autre moyen avec Lidl pour vérifier

- **Solde impayé chez Carrefour**

1. vous recevez un mail de Carrefour vous enjoignant de payer le solde d'une facture en souffrance (ce qui peut arriver si vous avez acheté un article payable en plusieurs fois)
2. **ne cliquez sur aucun des liens contenus dans ce message**
3. fermez ce message
4. prenez contact par un autre moyen avec Carrefour pour vérifier

Si vos doutes sont confirmés, c'est une bonne idée de signaler cette tentative de phishing, voici comment faire:

En gros, il faut envoyer le message de phishing reçu à **suspect@safeonweb.be** mais de préférence sous forme de pièce jointe, ce qui fournira beaucoup plus d'informations utiles sur ce message frauduleux qui si vous le transférez simplement !

Si vous ne savez pas comment faire pour envoyer un message en pièce jointe, vous pouvez soit le transférer quand même soit suivre mes instructions ci-dessous…

Comment envoyer un mail reçu en pièce jointe d'un autre message ?

1. il faut sauver le mail reçu en tant que fichier (explications plus bas) – c'est l'étape inhabituelle et un peu difficile…
2. il faut ensuite créer un nouveau mail et lui joindre celui que vous venez de sauver (comme joindre un document ou une photo)
3. et enfin envoyer le tout à suspect@safeonweb.be

C'est le même principe que d'envoyer un document ou une photo en pièce jointe mais la difficulté est la première étape: sauver un mail en tant que fichier car la procédure est différente pour chaque client de messagerie !

Allons-y pour les explications plus complètes:

Certains clients de messageries permettent de sauver un mail en tant que fichier en utilisant "enregistrer sous" ou "exporter", d'autres ne permettent même pas de faire cela…

Dis donc Li P'ti Fouineu, **c'est quoi un client de messagerie ?**

Il faut d'abord savoir que vos mails sont conservés sur les disques durs d'un serveur mail (gros PC) localisé quelque part sur l'Internet et qui permet à un client de messagerie de se connecter pour gérer ces mails.

Un client de messagerie est le programme avec lequel vous consultez vos mails en vous connectant au serveur mail !

Il peut s'agir de votre navigateur Internet (**Firefox**, **Chrome**, **Safari** ou autres) qui accède au site web de votre messagerie (gmail.com, gmx.com, outlook.com, skynet.be ou autres) => on parle alors d'un **webmail** ou client web pour le mail !
Le webmail communique avec le serveur de mail via le protocole **HTTP**. Un protocole est une convention de langage qui permet à plusieurs appareils de communiquer entre eux, chaque protocole possède ses qualités et limitations propres.

Il peut aussi s'agir d'un programme installé sur Linux, Windows, macOS, Android, IOS ou autres comme par exemple **Thunderbird, Courrier, Mail** et **Outlook**.
Dans ce cas, le client de messagerie communique avec le serveur via le protocole **IMAP** pour la gestion de vos messages (lecture, effacement, etc) et via le protocole **SMTP** pour envoyer un nouveau mail à vos correspondants

Note: il ne faut pas confondre outlook.com qui est un webmail et Outlook 2010/2013/2016/2019 qui est un client de messagerie installé sur votre PC Windows avec Microsoft Office…

La communication entre les différents serveurs de mail se fait aussi via le protocole **SMTP**.
À chaque étape du trajet d'un mail, SMTP ajoute des informations dites de routage à votre message. Ces informations sont attachées au message mais ne sont pas visibles dans ce que vous présente votre client de messagerie.
Ce sont ces informations de routage qui sont perdues si vous transférez un mail plutôt que de le sauver en tant que fichier et de l'envoyer comme pièce jointe.

Comment sauver un mail reçu en tant que fichier sur votre disque dur ou SSD ?

- **Depuis Thunderbird** (Linux, Windows et macOS)

- Ouvrir le mail à sauver
- Menu “**Fichiers**“
- Option “**Enregistrer comme**“
- Option “**Fichier** Ctrl-S”
- Sélectionner où sauver le fichier
- Bouton “**Enregistrer**“
- Le mail est sauvé en tant que fichier au format EML

- **Depuis Courrier** (Windows 10)
  - Ouvrir le mail à sauver
  - Cliquez sur **les trois point horizontaux** du menu Autre dans le coin supérieur droit
  - Dans le menu, cliquez sur “**Enregistrer sous**“
  - Sélectionner où sauver le fichier
  - Bouton “**Enregistrer**“
  - Le mail est sauvé en tant que fichier au format EML

- **Depuis Outlook** 2010/2013/2016/2019 (Windows) ou Outlook 2011/2016/2019 (macOS)
  - Ouvrir le mail à sauver
  - Menu “**Fichiers**“
  - Option “**Enregistrer sous ...**“
  - Sélectionner où sauver le fichier
  - Sélectionner le format Texte (TXT) ou HTML (EML n’existe pas)
  - Bouton “**Enregistrer**“
  - Le mail est sauvé en tant que fichier au format TXT ou HTML

- **Depuis Mail** (macOS)
  - Ouvrir le mail à sauver
  - Menu “**Fichiers**“
  - Option “**Enregistrer sous ...**“
  - Sélectionner l’emplacement où sauver le ficher
  - Sélectionner le format “**Source du message brut**“
  - Le mail est sauvé en tant que fichier au format EML à l’emplacement sélectionné

- **Depuis Gmail** (webmail)
  - Ouvrir le mail à sauver

        - Cliquer sur les 3 points verticaux à droite de la date du message
        - Choisir "**Télécharger le message**"
        - Le mail est sauvé en tant que fichier au format EML dans votre dossier de téléchargement

- **Depuis Outlook.com** ou Hotmail.com ou MSN.com (webmail)
    - **il est impossible de sauver un mail en tant que fichier !**

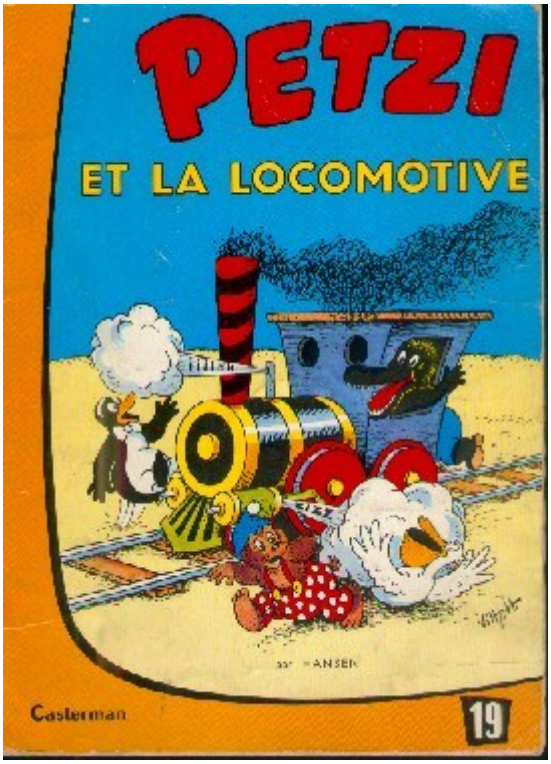
- **Depuis GMX.com** (webmail)
    - Ouvrir le mail à sauver
    - Cliquer sur le bouton "**Sauvegarder**" en haut à droite (icône disquette)
    - Le mail est sauvé en tant que fichier au format EML dans votre dossier de téléchargement

Il faut noter que le fichier ainsi sauvé peut être ouvert/consulté avec un éditeur de texte et inclut toutes les informations de routage.
Ouvrez donc le fichier sauvé avec Notepad (Windows) ou TextEdit (macOS) ou Gedit (Linux) pour voir à quoi ça ressemble…

Il ne vous reste plus qu'à créer un nouveau message, taper une petite explication avec vos mots à vous, attacher le fichier juste sauvé et envoyer ce message à **suspect@safeonweb.be**

Safeon**web** est une initiative du **Centre for Cyber Security Belgium**

Li P'ti Fouineu vous salue bien !


PETZI
ET LA LOCOMOTIVE
Casterman
19

Les News de Mars 2020

Bonjour le Monde !

J'attendais le 30 février pour écrire les News mais on m'a raconté des salades … Où ça ? Mais sur les usines à salades bien sûr: Facebook, Instagram, WhatsApp, Nord Presse et autres !

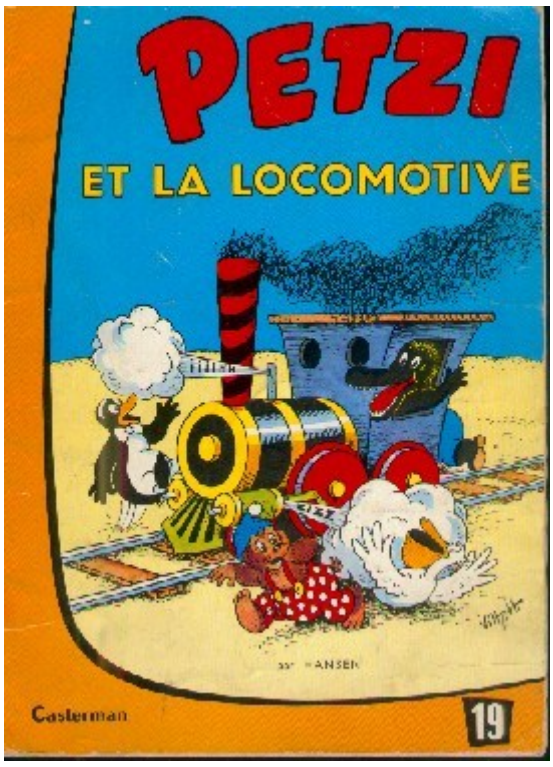
Vous ne saviez pas que ces braves gens faisaient leurs potagers sur notre dos ? Pssst, Nord Presse est nettement plus sympa que les autres mais ne soyez pas crédule lors de la visite du site…

Tout ça pour trouver une excuse pour vous avoir privés de News en février …

On va commencer par l'agenda des loisirs de mon coin:

- Cinégrez ASBL projettera **Girl** le 6 mars 2020 à 20h – C'est à Grez-Doiceau, plus d'info sur le site http://www.cinegrez.be
- Resto Jazz aux Brasseries Maxime à Wavre le 6 mars 2020 avec **The Blue Train Big Band** – Dès 19h, réservation obligatoire
- C'est La Foire du Livre du 5 au 8 mars
- Bourse livres, CD et DVD à Mont-St-Guibert le 8 mars
- Nouvelle brocante tous les 2e dimanches du mois d'avril à octobre à Hannut sur le parking de **SOS Troc** (aussi ouvert le dimanche)
- Concert d'un cover des ZZ Top au Zik-Zak le 28 mars 2020; plein d'autres spectacles chez Zik-Zak !
- Quelques annonces de brocantes sont seulement sur ma page Facebook car partagées depuis l'usine à salades qui a parfois de chouettes côtés…(je ne suis pas pour mettre le calendrier du blog à jour)
- Les habituels marchés et brocantes

10 BDs ajoutées à la collection dont un **Trigan** et 3 **Petzi** – 1735 albums !



Au rayon musique, **Florence Cayron** alias **Florence Cha Cayron** a réalisé un clip pour le titre **Contacting The Aliens** de **Refurrin Kitsune** (une autre facette de Florence) ! **Rejoignez Refurrin Kitsune sur sa chaîne Youtube !**
Kiss & Ride: Florence, si tu as un peu de temps pour m'aider à mettre à jour la partie de mon site qui t'est consacrée, ce serais chouette, j'ai un peu de mal à suivre !

Au rayon réparations de vieux trucs: un PC portable, un enregistreur d'émissions TV (non, pas un magnétoscope) et un micro sans fil – 3 anciens tourne-disques sont en attente depuis des mois mais deux d'entre eux sont vraiment très vieux, je ne me décourage pas pour le 3e …

Au rayon informatique, je (re)découvre **le monde Mac** avec un iMac de 2009 et **le monde RaspBerry** avec un RaspBerry 4 que certains d'entre vous ont très gentiment sponsorisé et qui est utilisé en PC Linux (Raspian) pour l'instant (pas encore de page RaspBerry).

Au rayon voyage, escapade à **Heerlen aux Pays-Bas** où les commerces ferment le samedi (jour du marché) à 18h mais ouvrent le dimanche de 12 à 17h ! Centre-ville piétonnier très sympa avec un petit carillon et plein de chouettes magasins comme **T K Maxx** (fins de série), **Cheap Cheap** (moins cher tu meurs) ou **Berden** (design, magnifique et très cher) en passant par une espèce de Cash Converter et plein, mais alors plein, de cafés, snacks et restaurants… Un bon plan

est le snack Damas: bon, copieux et pas cher. La gare est moderne et originale…
On a l'impression que, le samedi, les Hollandais font les magasins jusqu'à 18h, puis vont tous au resto (qui sont bondés) jusque 21h et puis rentre chez eux ! Dépaysant et relaxant. Bientôt une page avec quelques photos sur https://ecollart.info/voyages/
Kesskidi lui ? Si on a acheté des CBD et des médocs pas libres en Belgique ? Joker ! Mais non, ce n'est pour ça qu'on est venus…

Au rayon des bons plans, citons **SOS Troc**, 151 rue de Huy à Lens-St-Rémy (Hannut), énorme salle d'exposition en cours d'agrandissement avec de très belles choses, c'est ouvert du mercredi au dimanche de 10 à 18h et il y a même un petit bistrot pour se désaltérer et qui propose même une bière locale (Li Grigneuse, la cervoise des Borlatis)… À quelques centaines de mètres de là se trouve **L'Atelier** qui est une plaine de jeux couverte pour enfants avec un resto-brasserie proposant de bons petits plats pas chers et … une autre bière spéciale (la One Two Triple) … Troc/brocante, bière, resto pas cher, mon cocktail favori !

Au rayon Un Peu de Tout:

- **Du café à torréfaction lente à Hamme-Mille** chez **Ray & Jules**, torréfaction lente (12 minutes à 200° au lieu de 6 minutes à 600°) et écologiquement neutre avec une machine de leur création alimentée à l'énergie solaire qu'ils espèrent bien vendre aussi; bientôt dans les rayons des commerces locaux. Boutique en ligne seulement en anglais: https://www.ray-jules.com/en/store/. Prix actuel autour de 5€ les 250gr, c'est un peu cher mais si vous voulez les aider un peu … Une vidéo sur RTL…
- D'après Test-Achats, si vous avez un contrat fixe **c'est le moment de comparer les offres gaz et mazout dont les prix sont actuellement bas** et d'éventuellement changer de contrat et/ou de fournisseur.
- 5 organisations de consommateurs ont testé l'achat de 250 produits de 18 catégories chez **AliExpress**, **Wish**, **LightInTheBox**, **eBay** et **Amazon** pour conclure que **deux tiers des produits achetés sur Internet ne sont pas sûr !!!!**
  Source: Test-Achats n°650 (mars 2020)
- **Les infusions à la camomille** dont les prix au kilo font le grand écart (de 26.4 à 190 €) **contiennent trop souvent des résidus de pesticides ou autres produits chimiques**. Après l'enquête de Test-Achats, La Camomille de chez Kruidvat a été retirée du marché par l'AFSCA.
  Source: Test-Achats n°650 (mars 2020)
- **Cet article est garanti sans coronavirus** et les blog et site de **Li P'ti Fouineu** peuvent sans danger être consommés sans modération bien à l'abri que vous êtes dans votre chez vous douillet !
  Si vous avez des questions ou voulez en savoir plus, rendez-vous sur **https://www.info-coronavirus.be/fr/** et le **0800 / 14 689** est aussi à votre disposition…
  Source: Lettre d'information de la commune de Beauvechain (3 mars 2020)
- La Mutualité Chrétienne a sorti son 15e baromètre hospitalier et mis un module en ligne permettant de **comparer les pratiques tarifaires des hôpitaux belges** ! Édifiant !
  Source: Magazine En Marche Brabant Wallon n°1645 (20 février 2020)

Au rayon Geek:

- **Bon deal chez Aldi** à partir de samedi 7 mars 2020 **pour un**

Smartphone Nokia 6.2, écran 6.3″, Android 9, 4GB de RAM, Bluetooth 5, 2 nanoSIM, 64GB de stockage extensible à 512GB via microSD, batterie de 3500mA/h (2 jours), USB-C… Il n'est pas 5G mais à 189€, on lui pardonne (la 5G n'est pas tout à fait pour demain)…
Source: folder Aldi valable du 2 au 13 mars 2020

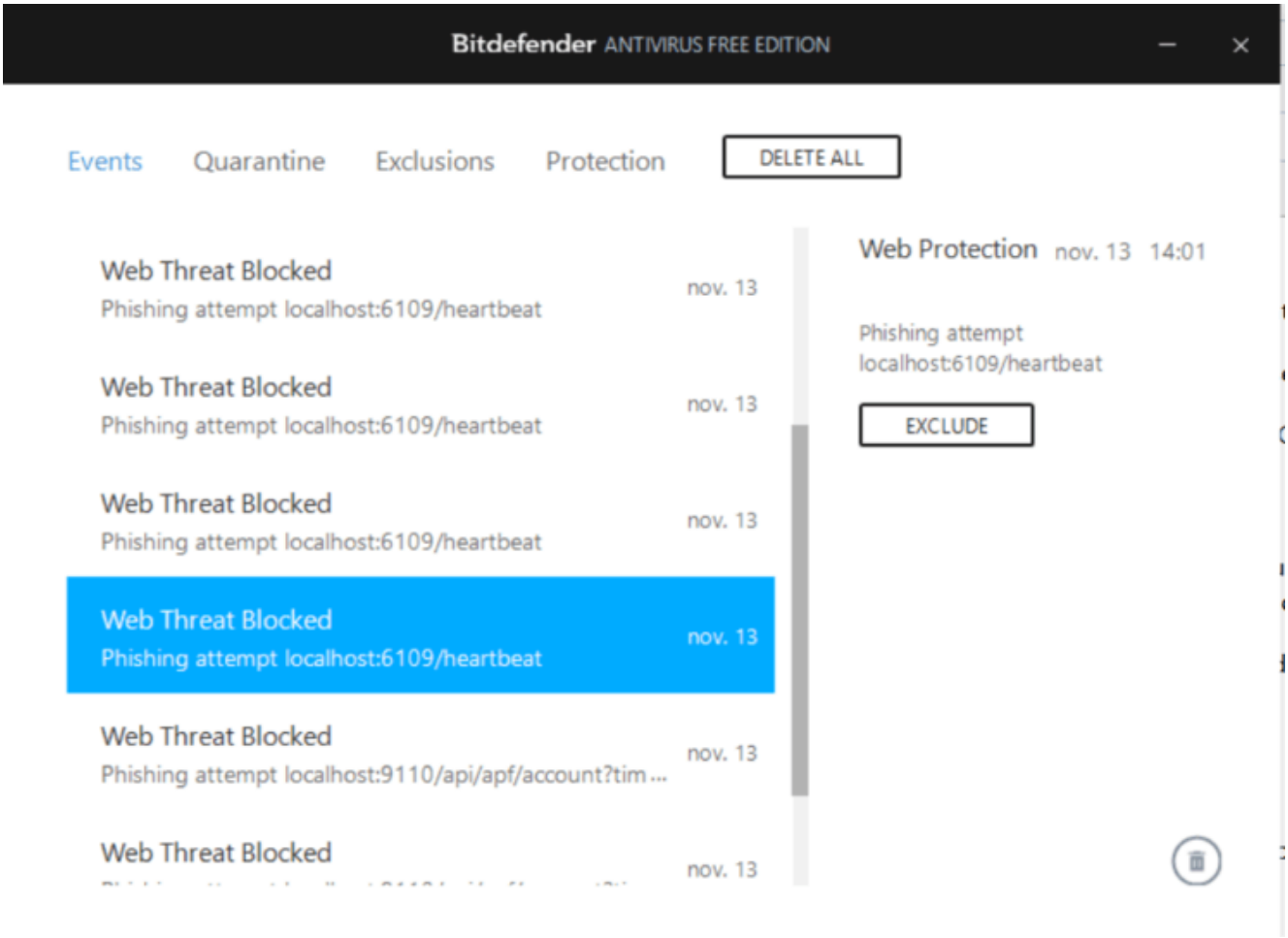
- **Explosion des signalements de messages de phishing** (hameçonnage) à la Computer Crime Unit qui ainsi pu bloquer 4000 faux sites ! La tendance actuelle des messages de phishing est de se faire passer comme provenant d'une grande enseigne et d'éveiller votre curiosité ou de vous faire peur. Si vous recevez un message suspect, ne cliquez pas sur les liens fournis mais rendez-vous manuellement sur le site de l'enseigne en question pour vérifier l'authenticité du message… Si vous pensez qu'il s'agit d'une tentative de phishing, le mieux est de sauver le message en tant que fichier et de l'envoyer en pièce jointe à **suspect@safeonweb.be**. Si vous ne savez pas comment sauver un message comme fichier, transférez simplement le message à la même adresse mail (il contiendra moins d'information utile pour l'analyse). Je vais publier un article plus complet là-dessus… **Safe**on**web** est une initiative du Centre for Cyber Security Belgium
  Source: Test-Connect n°27 (mars-avril 2020)
- **Certains zigomars** peu scrupuleux sur le Microsoft Store **essaient de vendre des copies d'applis Open Source après avoir juste modifié l'icône** de sorte que vous pourriez payer pour une appli à la base gratuite ! Il n'y a pas de raison que cela ne se produise pas sur le Google Play store ou l'Apple store.
  Source: Idées NET n°15 (juillet-août-septembre 2019)
- **La NASA offre photos, vidéos et enregistrements** libres pour une utilisation non-commerciale depuis **https://images.nasa.gov/**
  Source: Idées NET n°15 (juillet-août-septembre 2019)

- Pour compléter les palmarès des tests pour élire le meilleur antivirus/antimalware dont j'ai parlé il y a peu, voici un autre site indépendant à visiter même si il est en anglais; il a testé 16 programmes antivirus pour Windows. Les résultats de AV Comparatives.
  Source: Idées NET n°15 (juillet-août-septembre 2019)
- **Une faille de sécurité affectant près d'un milliard de Smartphones** et autres appareils utilisant certaines puces WIFI a été découverte par **ESET**. Certaines marques ont déjà fournit un correctif mais lesquelles ? Mystério !
  Source: sais plus… (ben ouais, ça arrive, non ?)
- Je vous ai déjà parlé des serveurs de noms ou DNS précédemment mais **il est maintenant possible de crypter les requêtes DNS** et donc de les rendre moins faciles à capturer pour savoir quels sites vous visitez. **Firefox, Chrome et Brave peuvent utiliser le DNS over HTTPS ou**

DoH de son petit nom; il faudra évidemment diriger les requêtes DNS vers des serveurs qui comprennent ce nouveau système, essayez d'éviter Cloudflare. Vous trouverez les explications et réglages à faire sur le site de Korben.
Source: sais plus non plus… (oui, je sais, je fatigue un peu là)

Voilà de quoi vous occuper quelque peu en vous souhaitant bonne lecture et, peut-être, découverte !

Li P'ti Fouineu vous salue bien !



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 !

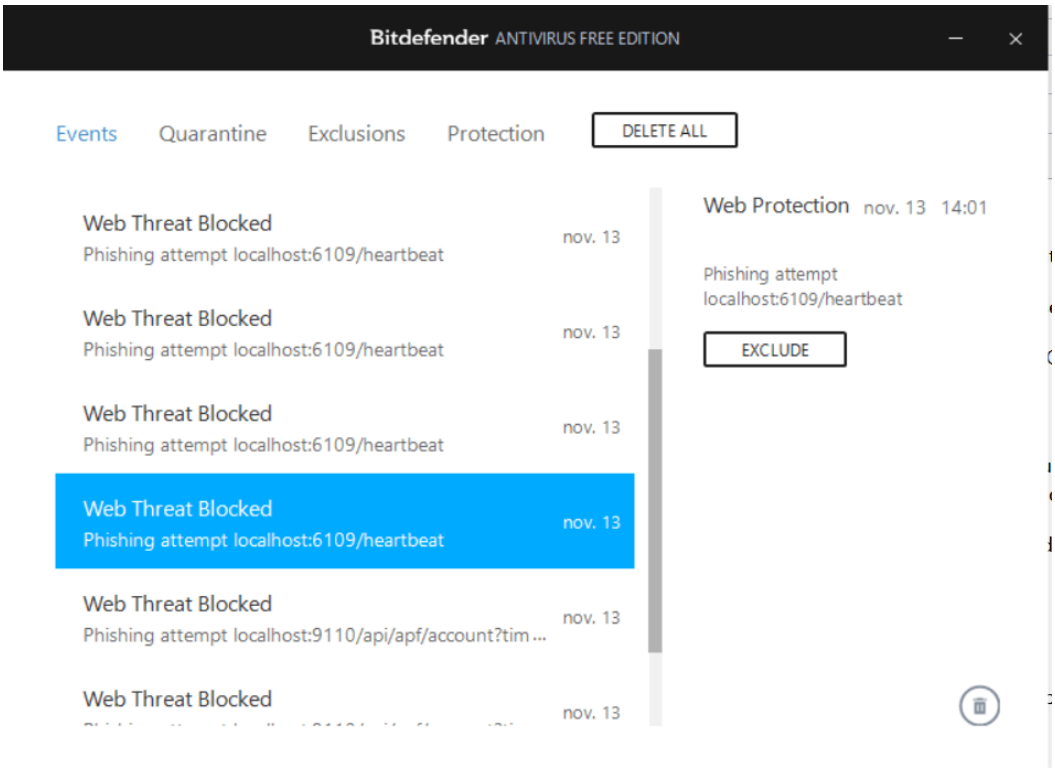
Scan antivirus (BitDefender) et anti-rootkit (MalewareBytes) avec chacun ayant trouvé une saloperie => effacement des cochonneries et nouveau redémarrage du PC.
Nettoyage avec Ccleaner (dernière version) => 1.8GB de fichiers temporaires effacés et environs 750 erreurs corrigées dans la base de registre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

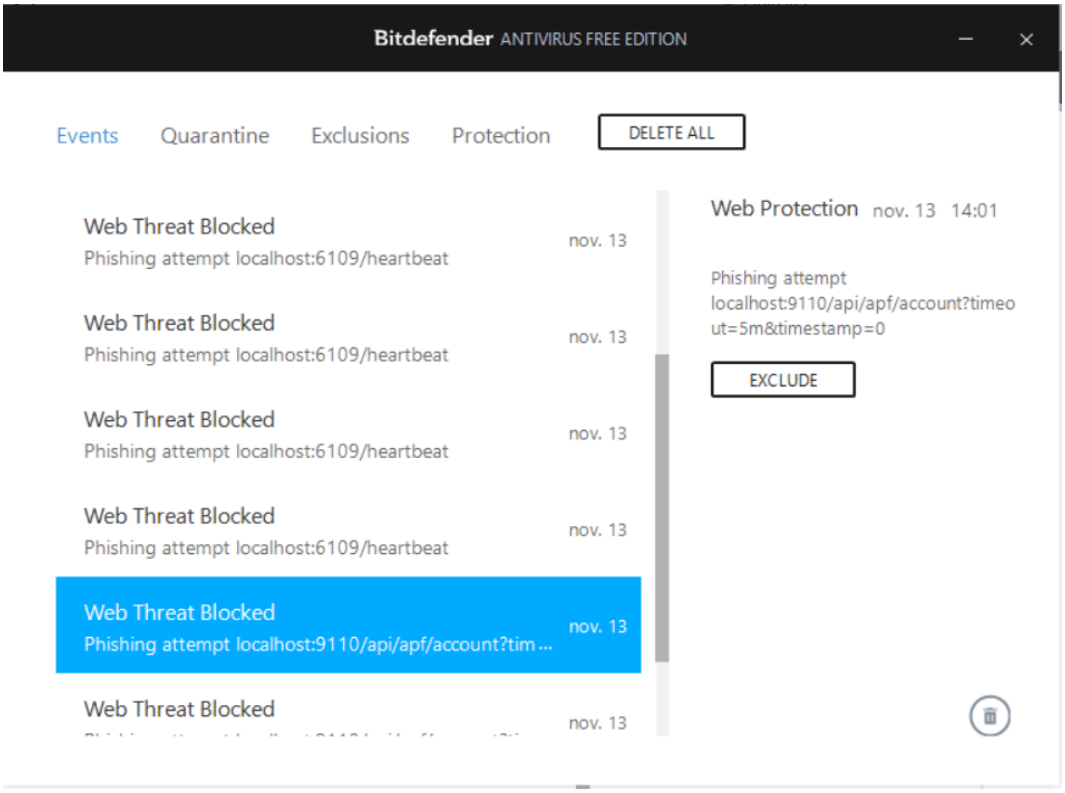
Vérification sur le site d'Acronis: il n'y a pas de nouvelle version du programme de protection anti-ransomware (ou pas encore) => je vais essayer de les informer du problème…

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 !