Virus et autres menaces sur Internet

La sécurité d'un système passe également par le contrôle de ce que font les applications sur ce système, et la détection de tout comportement anormal.

Voici une liste des principaux types d'applications qui peuvent être néfastes pour votre ordinateur :

- Virus : c'est un programme qui est capable d'infecter des fichiers et de se propager en utilisant des supports amovibles ou les réseaux.
- Ver : programme qui se répand d'un ordinateur à l'autre via les réseaux.
- Ransomware : crypte et bloque l'utilisation de vos données en échange d'un paiement.
- Spyware ou logiciel espion : désigne un programme qui espionne puis transmet des informations confidentielles vous concernant à une tierce personne.
- Adware : traque vos habitudes sur Internet et peut, par exemple, afficher des fenêtres publicitaires en fonction du profil qui a été défini. De nombreux sites web peuvent installer, à votre insu, ce type de logiciel.
- Enregistreur de frappe (keylogger) : programme qui enregistre toutes les données saisies au clavier et les transmet (mots de passe, numéro de carte bancaire...).
- Drive-by download : désigne un programme qui se télécharge sans votre consentement. Cela peut arriver quand vous essayez de fermer une boîte de dialogue.
- Redirecteur de page : désigne un programme qui va rediriger une partie ou l'ensemble des pages prédéfinies (page d'accueil, de recherche, etc.) vers un site malveillant.
- Spam : désigne un e-mail commercial qui n'est pas sollicité.
- BHO ou *Browser Helper Objects* ou Hijacker : désigne un programme qui permet de personnaliser et de contrôler certains paramètres d'un navigateur comme Internet Explorer. Il peut donc être proposé soit à des fins "pacifiques" (la barre d'outils proposée par Google) ou malveillantes.
- Dialer : désigne un programme qui va établir, en plus de votre connexion par défaut, une connexion d'accès à distance à un tarif surfacturé.
- Trojan ou Cheval de Troie : désigne un programme qui contient des fonctions cachées pouvant s'exécuter en arrière-plan à l'insu de l'utilisateur. Ils donnent un accès à la machine sur laquelle il est exécuté en ouvrant une porte dérobée (Backdoor).

Signalons que la frontière entre ces types de menaces reste floue et que beaucoup de programmes malicieux peuvent utiliser différentes techniques pour se développer.

1. Le centre de Sécurité Windows

Windows 10 propose par défaut et de manière centralisée un système de protection, **Sécurité Windows**, une sorte de panneau de configuration vérifiant différents paramètres de votre ordinateur :

- **Protection contre les virus et menaces** : il détecte la présence d'un antivirus tiers ou propose l'antivirus Windows Defender et s'assure de sa mise à jour.
- **Protection du compte** : gestion des informations du compte de l'utilisateur et sa synchronisation.
- **Pare-feu et protection du réseau** : il redirige vers l'interface de gestion du pare-feu, vue précédemment.
- **Contrôle des applications et du navigateur** : cette partie, également appelée SmartScreen, permet de filtrer les applications téléchargées via le navigateur ou Windows Store et les sites web consultés, en s'assurant qu'ils sont sans danger. Il compare les fichiers téléchargés ou les sites visités à une liste de fichiers dangereux ou de sites de hameçonnage et, le cas échéant, bloque le téléchargement ou le chargement du site tout en vous prévenant. Ce filtre est désactivable si vous constatez qu'il vous empêche de télécharger un fichier fiable ou de visiter un site de