Windows 10 et la protection contre les virus et attaques informatiques

malekal.com/windows-10-protection-contre-virus-attaques-informatiques/

malekalmorte 05/09/2017

Microsoft a pris à bras le corps les aspects de sécurité informatique depuis Windows XP Service pack 2. Windows 10 ne fait pas exception et Microsoft continue d'améliorer la sécurité au fil des mises à jour de Windows 10.

Les grands axes de Windows 10 contre les virus : améliorer Windows contre les vulnérabilités, améliorer Windows Defender et offrir une meilleur protection contre les malwares, améliorer la sécurité du navigateur internet Microsoft Edge.

Voici un tour d'horizon des mécanismes de sécurité de Windows 10 qui visent à mieux protéger Windows contre les attaques informatiques et les virus.

Table des matières [masquer]

Protection contre les vulnérabilités sur Windows 10

Les premières améliorations de Windows 10 consistent par l'ajout de nouveaux mécanismes pour atténuer les vulnérabilités logicielles.
Pour rappel, les vulnérabilités peuvent permettre l'infection de l'ordinateur à partir d'une simple visite d'un site internet (WebExploit) ou pire à distance sans la moindre interaction de l'utilisateur, c'est le principe des vers informatique.
Pour rappel, les vulnérabilités sont exploitées par des exploits qui ont des fonctionnements assez similaires (Dépassement de tampon [buffer overlow], dépassement de tas [*heap overflow], etc).
La protection des vulnérabilités est donc importante, puisqu'ils s'agit d'une porte d'entrée aux virus, cheval de troie et autre logiciels malveillants.
Courant 2010 et 2011, le WebExploitKit BlackHole puis par la suite Angler EK ont fait des ravages. Les protections ajoutées aux navigateurs internet ont pu atténuer ce phénomène, les WebExploit sont devenus de plus en plus, marginales ce qui a provoqué un retour des campagnes de mails malveillants.

D'où l'importance de maintenir Windows à jour ainsi que vos logiciels : Logiciels pour maintenir ses programmes

à jour

Le but de ces protections est de proposer des mécanismes de mitigation contre ces exploitations. On trouve des méthodes différentes comme compartimenter certains accès au noyau de Windows, sécuriser l'accès à la mémoire.
Ces derniers sont invisibles pour l'utilisateur puisqu'il s'agit du fonctionnement interne de Windows.

Mitigation des vulnérabilités logicielles

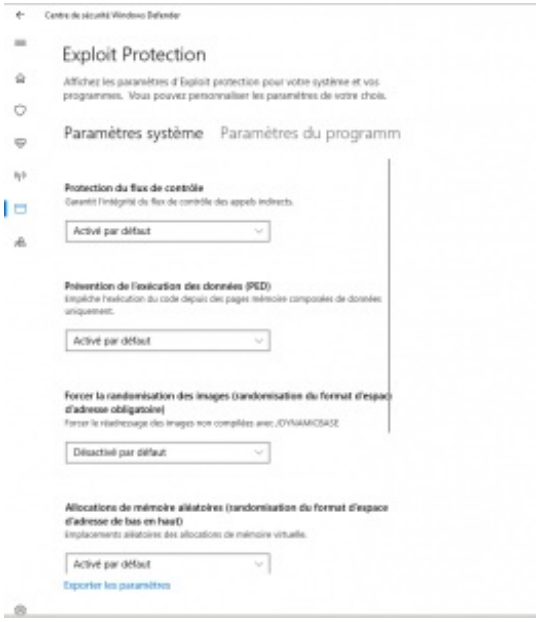
Parmi les mécanismes de protection et de mitigation des vulnérabilités de Windows 10 :

- **User Mode Font Driver (UMFD) :** Permet d'écrire des pilotes plus facilement (moins d'erreurs de codes etc). Depuis Windows 10 des mécanismes d'isolation pour UMFD ont été ajoutés, ces derniers tournent dans un conteneur d'application (App container). UMFD est géré par le processus fontdrvhost.exe.
- **Win32k Syscall Filtering :** Réduit le nombre d'API accessibles par un processus afin de réduire la surface d'attaque.
- **Less Privileged App Container (LPAC):** Limite les accès à certains ressources par le containeur d'application à travers un mécanisme de SID.
- **Structured Exception Handling Overwrite Protection (SEHOP) :** Protège contre les exploits de type Structured Exception Handler (SEH)
- **Address Space Layout Randomization (ASLR)** : Charge les DLL de Windows, au démarrage de ce dernier, dans des adresses aléatoires afin de protéger des malwares qui utilisent des adresses de mémoires pré-enregistrées.
- **Heap protections :** Protection contre les attaques de dépassements de tas. Utilise des adresses mémoires aléatoires pour rendre l'écrasement de mémoire plus difficiles par un attaquant. Ce mécanisme ajoute aussi des pages de protections qui devront être écrasées par l'attaquant, cela peut alors aboutir à un BSOD de corruption de mémoire.
- **Kernel pool protections :** Ajoute de mécanismes de protection de la mémoire utilisée par le noyau Windows.
- **Control Flow Guard :** Mécanisme de protection pour des applications prévues pour utiliser ce dernier (doivent être compilés avec le CFG), c'est notamment le cas de Microsoft Edge.
- **Protected Processes :** Protège de l'accès à des processus signés par des processus non signés, ainsi des antivirus ou logiciels de protections peuvent utilisés cet espace de protection pour ne pas être altérés par des malwares.
- **Universal Windows apps protections :** mécanisme de vérifications des éditeurs du Windows Store pour s'assurer qu'ils sont crédibles.

L'exploit Protection du centre de sécurité Windows Defender depuis la mise à jour Windows 10 Fall Creators Update.

Anti-Ranwomware

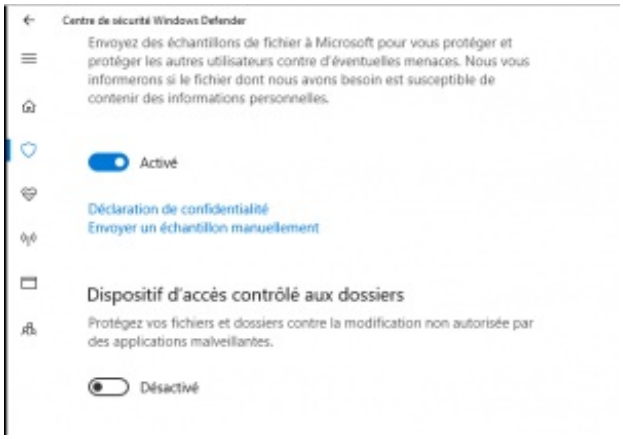
La mise à jour Windows 10 Fall Creators Update propose aussi un anti-ransomware qui vise à protéger vos documents contre les attaques de ransomwares.
Plus d'informations : Comment activer la protection Anti-Ransomware de Windows 10

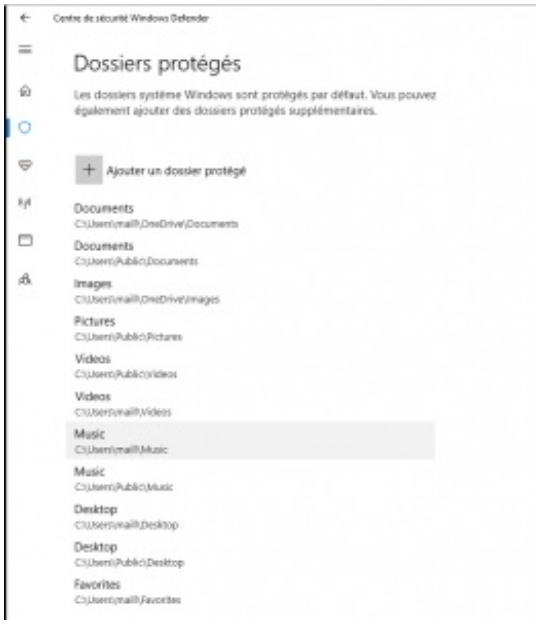


Vous choisissez alors les dossiers à protéger :

Windows 10 dans un processus de sécurisation

Microsoft cherche donc à protéger les utilisateurs de Windows 10 en minimisant les impacts des vulnérabilités et en rendant leurs exploitations plus difficiles.
Notez que ces protections sont ajoutées au fur et à mesures des versions de Windows 10. On voit donc bien, que Windows 10, suit un processus général et en continue de Microsoft de sécurisation.





Amélioration des protection de Windows Defender

Un autre aspect des protections apportées par Windows 10 est l'amélioration constante de Windows Defender qui n'a rien à voir avec les version de Windows 7 et Windows 8.
En plus, de tenter de capter le plus de malwares possibles pour ajouter des protections, de nouvelles fonctions ont été apportées à Windows Defender.
Petit à petit, Windows Defender n'a pas à rougir de certains antivirus.

Cloud Antivirus et Machine Learning

Le nombre de malware grandit chaque mois, il faut donc être en mesure de capter un maximum pour ajuster les protections en conséquence.
Windows 10 introduit un Cloud Antivirus sur Windows Defender, qui permet de déporter les définitions virales sur les serveurs pour alléger le client antivirus.
Le client Antivirus alimente ce cloud pour partager ces définitions à l'ensembles du parc Windows Defender.

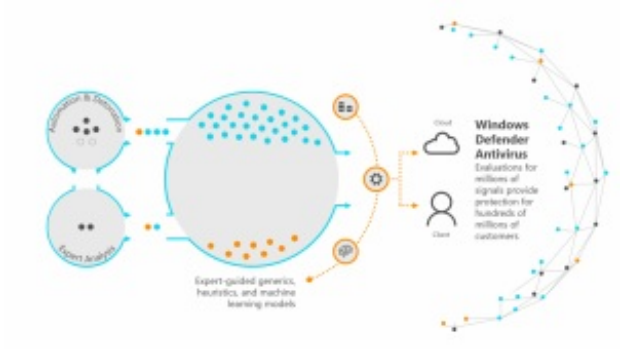
L'alimentation se fait à travers du machine learning ou apprentissage automatique en français. C'est donc une intelligence artificielle qui ajuste les détections pour alimenter la base de données Cloud.
Ce système Cloud inclut des détections heuristiques ainsi que des détections comportementales.

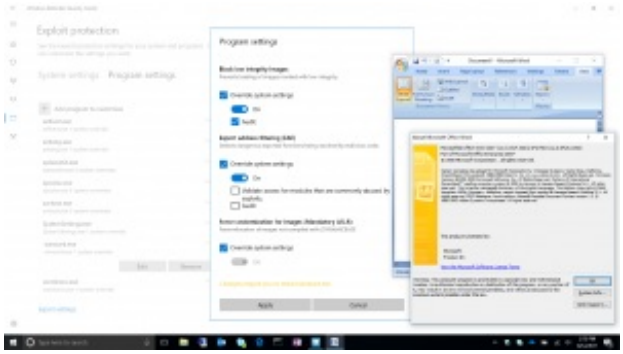
Le schéma donne un aperçu de la protection Windows Defender à l'ensemble des clients Windows 10 :

Windows Defender Exploit Guard

La prochaine mise à jour de Windows 10 (Fall Creators Update pour Octobre 2017) devrait intégrer **Windows Defender Exploit Guard**.
Il s'agit de l'ancienne application EMET (Enhanced Mitigation Experience Toolkit) qui vise à protéger l'ordinateur des vulnérabilités.

C'est donc un nouveau maillon dans la protection contre l'exploitation de vulnérabilité logicielle.





Protection dans Microsoft Edge

Microsoft Edge est le nouvel navigateur internet qui vise à repositionner Microsoft dans la guerre des navigateurs internet et par extension dans la guerre des moteurs de recherche.
L'aspect sécurité n'a pas été oublié, d'autant que ces dernières années Mozilla Firefox et Google Chrome ont aussi dû consolider leurs navigateur respectives à cause des Web Exploit.

Microsoft Edge est donc un maillon important dans la protection de Windows 10 puisque le navigateur internet peut aussi servir de porte d'entrée.

Sécuriser Adobe Flash

Adobe Flash a été un framework très populaire pour les vidéos, jeux et bannières publicitaires (animation flashs).
A cause de problèmes de performances et de mémoires fréquents, Adobe est délaissé. Ce dernier est remplacé par HTML5 et devrait être même entière bloqué sur certains navigateurs internet d'ici quelques années.

Beaucoup de vulnérabilités ont été publiés pour Adobe Flash qui ont été utilisés par les Web Exploit, cela a aussi été le cas de Java (voir en 2011 : Exploit Java toujours aussi efficace).
Mozilla Firefox et Google Chrome ont intégré, pour protéger les internautes, un blocage des versions obsolètes et une activation manuelle des plugins.
Quelques vulnérabilités Adobe Flash sont mentionnées sur la page suivante : Vulnérabilités sur Player Flash et Shockwave Player
Pour corriger ces vulnérabilités, il faut donc maintenir Adobe Flash à jour. Malheureusement, cela nécessite de se tenir au courant et savoir comment le mettre à jour

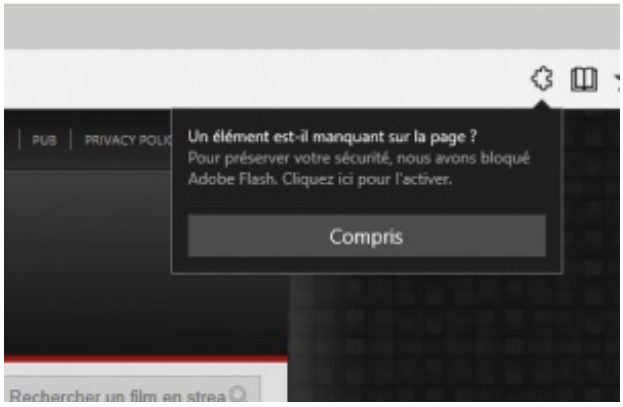
La première chose est l'intégration de mise à jour Adobe Flash dans Windows Update afin de s'assurer que vous avez bien la dernière correctrice.

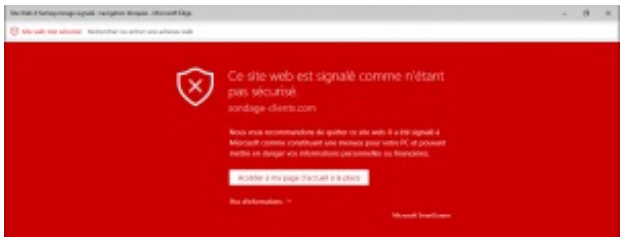
Enfin l'activation de Flash pour certains composants peut être manuelle afin de protéger contre des applets Flash malveillantes :

SmartScreen

La technologie SmartScreen est aussi améliorée sur Windows 10 par rapport aux versions précédentes.
Plus d'informations sur SmartScreen, lire notre dossier : SmartScreen : filtrage URLs et fichiers malveillants

SmartScreen tente notamment de bloquer les arnaques de support de téléphonique, une menace grandissante depuis deux ans.





Autres liens autour de la sécurité sur Windows 10

Quelques autres liens autour de la sécurité sur Windows 10.

- Quelles protections pour Windows 10 contre les virus ?
- Windows Defender est-il efficace?