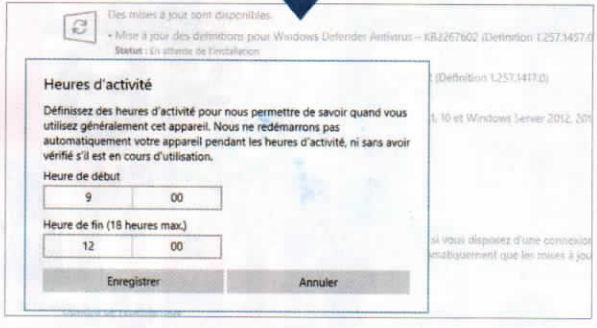
DIFFICULTÉ
Aucune
TEMPS
35 min

Anticipez les ravages des rançongiciels

Nouvelle arme fatale des cybercriminels, les ransomwares bloquent votre PC en chiffrant le contenu du disque dur jusqu'au paiement d'une rançon. Suivez ces quelques conseils pour éviter ces attaques et en minorer l'impact.

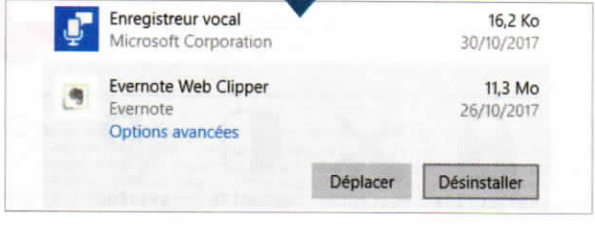
1. Maintenez votre système à jour

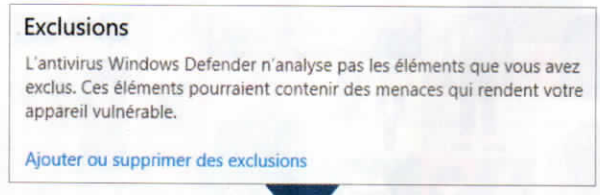
Microsoft publie régulièrement des correctifs de sécurité destinés à combler les failles de Windows. Pour en bénéficier, votre PC doit se mettre à jour automatiquement. Ouvrez ***Paramètres*** (raccourci ***Windows + I***), et choisissez ***Mise à jour et sécurité***. Si des mises à jour sont en attente, cela signifie que votre ordinateur était éteint au moment où Windows a tenté de les installer. Pointez sur ***Modifier les heures d'activité*** pour forcer la mise en place des correctifs à un autre horaire, un clic sur ***Redémarrer*** finalise les mises à jour disponibles.



2. Faites le ménage dans vos logiciels

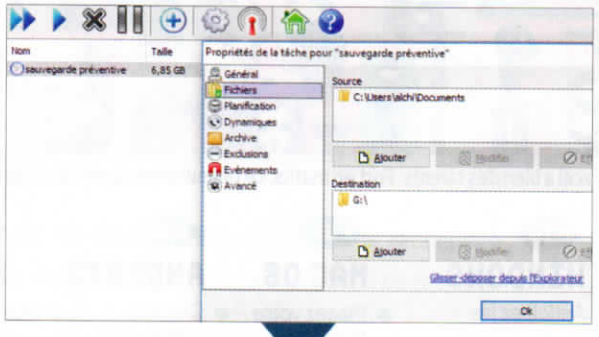
Les ransomwares utilisent les mêmes vecteurs d'infection que les virus et les logiciels malveillants. Ils peuvent se cacher notamment dans les applis ou les macrocommandes. Évitez donc d'ouvrir une pièce jointe inconnue ou d'installer des programmes d'origine indéterminée. Corrigez les failles de Windows, gardez vos programmes à jour. Quant aux applications qui ne bénéficient plus de correctifs, n'hésitez pas à les supprimer. Ce sont des cibles potentielles privilégiées par les pirates. Si vous pensez avoir été infecté, installez ***Malwarebytes*** (***bit.do/dVBQu***), un outil de lutte contre les failles zéro day, à savoir les menaces non encore répertoriées.





3. Activez la protection des dossiers

Depuis la mise à jour Fall Creators Update, Windows Defender est capable de bloquer toute application malveillante essayant de modifier les fichiers et les dossiers. Désactivée par défaut, cette option doit être paramétrée afin d'éviter qu'elle n'entrave des processus dont vous avez besoin au quotidien. Dans le ***Centre de sécurité***, cochez ***Protection contre les virus et menaces***, ***Paramètres de protection contre les virus et menaces***. Activez ensuite ***Dispositif d'accès contrôlé aux dossiers*** et pointez sur ***Ajouter ou supprimer des exclusions*** afin de soustraire vos applications favorites à ce contrôle.



4. Réalisez une sauvegarde de vos données

Victime d'un ransomware, vous n'aurez d'autre choix que de payer ou de reformater votre disque dur pour reprendre le contrôle de l'ordinateur. Cette dernière opération est sans grande conséquence si vous aviez pris soin de réaliser une sauvegarde complète du PC ou de ses données. Pour planifier un backup périodique sur un disque externe ou une clé USB, installez l'application ***Cobian Backup*** (***bit.do/dVBUh***). Utilisez le français comme langue par défaut. Connectez votre support de stockage, appuyez sur ***Ctrl + A*** et nommez la nouvelle tâche. Dans ***Fichiers***, désignez les dossiers à sauvegarder. Indiquez le disque cible dans ***Destination***, et validez par ***OK***. ■