

OUCH!

Dans ce numéro...

- Vue d'ensemble
- Le cycle de vie d'un système d'exploitation
- Savoir se protéger

La Fin de Windows XP

Vue d'ensemble

Windows XP s'est avéré être l'un des systèmes d'exploitation les plus populaires de l'histoire de l'informatique à tel point qu'il a même été utilisé sur la plupart des ordinateurs dans le monde. Cependant Windows XP est vieux, et l'ensemble du support fourni par Microsoft va bientôt prendre fin. D'abord publié il y a plus de douze ans, la fin de vie (End of Life – EOL) de Windows XP est prévue pour le 8 Avril 2014. Cela signifie que Microsoft ne publiera plus de mises à jour ou de correctifs de sécurité aux utilisateurs finaux. Avec environ 25% des ordinateurs de par le monde fonctionnant encore sous Windows XP (seul Windows 7 est plus populaire), des millions de personnes seront soumises à davantage de risques une fois que cela arrivera. Gardez à l'esprit que les utilisateurs privés ne sont pas les seuls qui seront touchés car XP est encore largement utilisé dans les bureaux, les systèmes de contrôle industriels, les distributeurs automatiques, les systèmes médicaux, les terminaux de point de vente (PoS) et encore d'autres équipements. Ci-dessous, nous décrivons quelle sera la nature des risques une fois que Windows XP ne sera plus supporté ainsi que les mesures que vous pouvez prendre pour vous protéger.

Editeur invité

Jason Fossen spécialisé dans la sécurité sous Microsoft Windows au sein de la société Enclave Consulting LLC, est l'auteur du cours Securing Windows with the Critical Security Controls (SEC505) d'une durée de six jours dispensé au SANS Institute, et partage des scripts de sécurité PowerShell à <http://cyber-defense.sansorg/blog/>.

Le cycle de vie d'un système d'exploitation

Vous ne le savez peut-être pas, mais le système d'exploitation de votre ordinateur a une durée de vie limitée. L'éditeur qui a développé le système d'exploitation fournit des mises à jour et des correctifs qui ajoutent de nouvelles fonctionnalités, améliorent la stabilité et les performances, et sécurisent votre système. Le problème est qu'à un moment donné, l'éditeur ne supportera plus votre système d'exploitation car il devra concentrer ses ressources sur le développement de ses technologies plus récentes et plus innovantes. Cela signifie qu'une fois qu'un système d'exploitation n'est plus supporté, l'éditeur ne diffusera plus de correctifs ou de mises à jour, même lorsqu'il sait que votre ordinateur est vulnérable et que les cybercriminels peuvent le pirater. C'est ce qui va se passer avec Windows XP après Avril. Même si Microsoft sait que votre ordinateur Windows XP est vulnérable, et que les cybercriminels exploitent activement ces vulnérabilités, Microsoft cessera de fournir des correctifs pour ce problème.

Savoir se protéger

Pour vous protéger, vous devez utiliser un système d'exploitation qui est actuellement supporté. Si vous pouvez vous le permettre, nous vous recommandons fortement d'acheter un nouvel ordinateur. De nombreux ordinateurs fonctionnant sous Windows XP ne peuvent pas supporter les systèmes d'exploitation plus récents de la génération

La Fin de Windows XP

actuelle. Si vous ne pouvez pas vous permettre l'achat d'un nouvel ordinateur, mettez au moins à niveau le système d'exploitation. Pour les entreprises, la migration vers Windows 7 au lieu de Windows 8 peut constituer une transition moins perturbante de par une interface graphique similaire à celle de Windows XP. Cependant, Windows 8 est mieux sécurisé que les précédentes versions en raison d'importantes améliorations logicielles. En outre, il existe d'autres éditeurs de systèmes d'exploitation que vous pouvez également envisager, comme Mac OS X d'Apple. Quoi qu'il en soit, le moment est venu de changer et il ne vous reste que très peu de temps devant vous. Si vous ne pouvez pas migrer Windows XP avant Avril, alors prenez en considération les conseils suivants :

- Utilisez votre ordinateur Windows XP uniquement pour la fonctionnalité ou les applications dont vous avez absolument besoin. Par exemple, peut-être que vous ou votre organisation utilisez un ancien programme qui ne fonctionne que sur XP et c'est la raison pour laquelle vous ne pouvez pas le mettre à jour. Si tel est le cas, alors il ne faut pas utiliser l'ordinateur à d'autres fins, comme par exemple pour accéder à votre courrier électronique ou naviguer sur Internet.
- Si vous devez utiliser votre ordinateur sous Windows XP pour la navigation Internet, cessez d'utiliser Internet Explorer et passez à un autre navigateur, tel que Mozilla Firefox, Google Chrome ou encore Opera. Assurez-vous également de toujours maintenir le navigateur à jour et que l'éditeur continue de supporter son utilisation sur Windows XP.
- Arrêtez d'utiliser d'autres applications intégrées dans Windows XP qui ouvrent des fichiers directement depuis Internet, tels que Windows Media Player. Préférez plutôt des applications distinctes venant d'autres éditeurs et qui sont toujours supportées et veillez à les maintenir à jour.
- Pensez à utiliser un service de sécurité réseaux tels que le service gratuit OpenDNS. Ces services protègent notamment vos systèmes de la visite de sites Web malveillants connus. En outre, certains services peuvent détecter si votre ordinateur tente de se connecter à un serveur de Command and Control appartenant à un botnet connu, ce qui constitue un indicateur que votre système est infecté.
- Assurez-vous que tout logiciel de sécurité installé, tels que les anti-virus, soit toujours actuellement supporté et officiellement maintenu pour Windows XP.



Une fois que Windows XP n'est plus supporté, la meilleure façon de vous protéger est de migrer vers un nouveau système d'exploitation qui est activement supporté par son éditeur, et de s'assurer que celui-ci est toujours actuel.

La Fin de Windows XP

- Si votre ordinateur n'a pas besoin d'être connecté à Internet (par exemple, si vous l'utilisez juste pour le traitement de texte), débranchez-le du réseau. S'il doit être connecté à un réseau, assurez-vous qu'il est derrière un pare-feu, et que le pare-feu système bloque tout le trafic. Pour les entreprises, vous pouvez isoler l'ensemble de vos ordinateurs Windows XP sur un réseau séparé, ainsi s'ils viennent à être infectés, ils n'infecteront pas le reste de votre entreprise.
- Enfin, sauvegardez régulièrement vos données hébergées sur les postes XP en vue de l'éventualité où ils seraient infectés. De plus, conservez au moins une de ces sauvegardes hors ligne, par exemple sur un périphérique USB déconnecté. Si vous êtes obligés de procéder à une récupération du système, alors envisagez sérieusement de repartir sur un nouveau poste. Si vous repartez de nouveau sur un Windows XP, il sera très probablement réinfecté.

Si vous utilisez Windows XP à votre travail, votre employeur peut avoir des étapes supplémentaires à effectuer. Rappelez-vous, ce ne sont que des mesures palliatives de courte durée, elles ne sont pas un substitut d'une migration vers un système d'exploitation à jour et bien sécurisé. Tôt ou tard, vous devrez migrer vers un nouveau système.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients.

Pour en savoir plus, veuillez vous référer aux liens suivants :

<http://www.answersolutions.ch> et <http://answersecurity.com/>

Ressources

Annonce Microsoft EOL:

www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx

OpenDNS:

www.opendns.org

Guide de migration:

<http://www.zdnet.com/windows-xp-end-of-life-migration-guide-7000023800/>

OUCH: Sauvegarde & Restauration:

<http://www.securingthehuman.org/ouch/2013#september2013>

OUCH! est publiée par le programme SANS « sécuriser l'humain » (Securing The Human) et est distribuée sous la licence « [Creative Commons BY-NC-ND 3.0](http://creativecommons.org/licenses/by-nc-nd/3.0/) ». La distribution de cette lettre d'information est autorisée tant que vous faites référence à la source, qu'elle n'a subi aucune modification et qu'elle n'est pas utilisée à des fins commerciales. Afin d'obtenir des traductions ou plus d'informations, merci de contacter ouch@securingthehuman.org.

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner

Traduit par : Julien Bouillot, Marilyn Combet