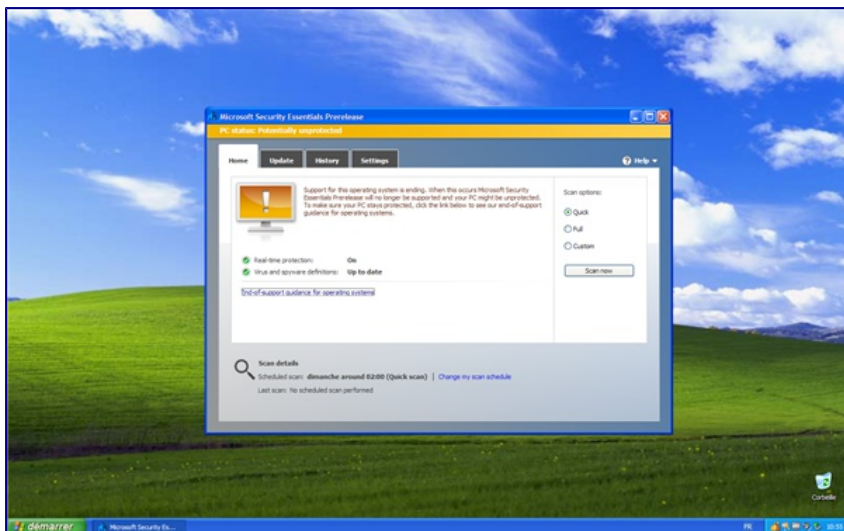


Les pirates préparent déjà des listes de failles exploitables pour Windows XP

Doom's Day

Comme on le sait, Windows XP verra son support technique terminé dans moins d'un mois. Le 8 avril marquera une étape importante dans le paysage mondial de la sécurité puisque les failles de l'ancien système, encore largement utilisé, ne seront plus corrigées. Certains experts mettent d'ailleurs en garde : les pirates font déjà des listes des failles exploitables.



Quand le support s'arrête, les pirates lâchent les chiens

Le support technique de Windows XP s'arrêtera le 8 avril. Comme prévu depuis plusieurs années maintenant par Microsoft, les brèches dans le système ne recevront plus aucun correctif. À cette date, Windows XP recevra donc ses dernières mises à jour, et on peut s'attendre à une dernière fournée assez riche. Le problème, évidemment, se situera au-delà de cette date.

Quand un produit ne dispose plus d'aucun support, il devient rapidement vulnérable aux attaques concentrées des pirates. Dans le cas d'un système d'exploitation encore utilisé par environ 30 % de la population mondiale, avec parfois plus de la moitié des utilisateurs dans des pays [tels que la Chine](#), la situation s'annonce sérieuse. Le problème majeur sera sans doute la constitution de parcs de machines zombies, contrôlables à distance par un unique individu qui peut alors piloter plusieurs dizaines de milliers de PC. Les objectifs sont alors variés, allant de la génération de spams aux attaques distribuées par déni de service (DDoS).

Les pirates créent déjà des listes de failles exploitables

La question qui reste en suspens est donc de savoir quel est l'état actuel des connaissances chez les pirates sur les failles restant ouvertes à ce jour. [Interrogé par le site CIOL](#), le directeur technique du cabinet de consulting en sécurité Help AG, Nicolai Solling, a indiqué que les pirates étaient déjà en train de référencer les failles potentielles. Ce qui signifierait évidemment qu'au lendemain des dernières mises à jour, toute une flopée de nouvelles attaques surviendraient un peu partout.

À partir de ce moment, les utilisateurs n'auront que très peu de recours. Solling précise en effet qu'une partie des antivirus ne sera plus mise à jour, bien que certains éditeurs, [dont Microsoft lui-même](#) et Kaspersky notamment, aient annoncé une continuité pour leurs produits respectifs. Mais un antivirus peut s'occuper des malwares, pas colmater des brèches de sécurité. La solution de temporisation la plus « efficace » sera d'utiliser un navigateur alternatif, tel que Chrome ou Firefox, pour éviter que les failles d'Internet Explorer ne soient utilisées.

VIXANE vous donne le pouvoir
sur vos ordinateurs

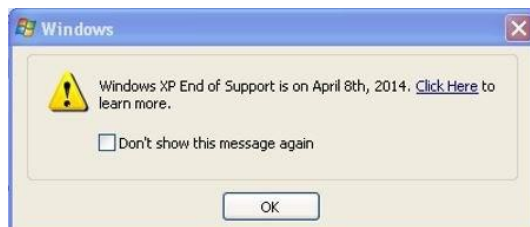
Téléphone: 06 09 41 76 89

Mail: francois.deguerry@vixane.fr

Internet: vixane.fr

Peu de solutions pour compenser l'effondrement du niveau de sécurité

Dans tous les cas, les failles de sécurité sont une activité commerciale souterraine. Il existe un véritable réseau de vente de ces informations, et celles de Windows XP s'achètent sans doute désormais à prix d'or. Car les pirates ne peuvent que se frotter les mains : toute faille qui ne sera pas corrigée le 8 avril deviendra par définition une faille 0day, autrement dit exploitable dès le premier jour. Les méthodes d'attaques qui les utiliseront auront davantage de garanties de rester effectives et on risque de voir fleurir un grand nombre de nouvelles vagues de faux emails. Le pire étant évidemment que la liste des failles connues ne fera que grandir avec le temps.



La situation est d'autant plus problématique que Windows XP ne possède aucune protection moderne. Help AG estime ainsi que le risque d'être contaminé par un logiciel malveillant est 400 % plus élevé sur le vieux système que sur Windows 8, même si le cabinet n'explique pas la méthode de calcul. On peut citer très facilement plusieurs exemples de techniques apparues avec Vista et dont ne bénéficie pas XP, telles que l'ASLR, qui change de place en mémoire les composants principaux pour qu'ils ne puissent pas être visés par des attaques « fixes », ou encore la sandbox d'Internet Explorer, qui isole le navigateur du reste du système.

Peu de temps pour réagir

Le paysage de la sécurité sera donc en effervescence durant les prochains mois et nous serons évidemment attentifs aux évolutions dans ce domaine. Microsoft avait pour rappel répondu à nos questions en affirmant que cette fois-ci, [plus rien ne serait fait](#) pour maintenir le support de Windows XP actif. En d'autres termes, les utilisateurs doivent impérativement mettre à jour leur machine sous peine d'affronter une situation désagréable.

On rappellera également que ces mêmes utilisateurs reçoivent désormais des avertissements pour les informer de la situation. Si les mises à jour automatiques sont activées, [une fenêtre de notification apparaîtra](#). La prochaine mouture de l'antivirus gratuit Security Essentials [affichera lui aussi un message](#), sous la forme d'un bandeau jaune qui ne disparaîtra pas, même après une analyse réussie. On aurait malheureusement souhaité que l'éditeur démarre cette campagne de communication il y a plusieurs mois car cela ne laisse que quelques semaines aux concernés pour trouver une solution qui risque, dans bien des cas, de se solder par le rachat d'un PC récent.

Vicent Hermann

Rédacteur/journaliste spécialisé dans le logiciel et en particulier les systèmes d'exploitation. Ne se déplace jamais sans son épée.

Publiée le 12/03/2014 à 16:40

[Télécharger l'article sur le site de PC INpact](#)

VIXANE vous donne le pouvoir
sur vos ordinateurs

Téléphone: 06 09 41 76 89

Mail: francois.deguerry@vixane.fr

Internet: vixane.fr