Internet : IPv6, quelles consÃ©quences sur la sÃ©curitÃ© informatique ?
Accessoire
PostÃ© par : JulieM
PubliÃ©e le : 8/6/2011 11:30:00

Quâ□□on le veuille ou non, dans les prochaines annÃ©es, chaque entreprise devraÂ probablement mettre Ã jour chaque appareil qui est actuellement connectÃ© Ã sonÂ rÃ©seau Internet. Câ□□est Ã cause dâ□□un changement technologique fondamental appelÃ© **Internet Protocol Version 6** (IPv6).

En rÃ©sumÃ©, le Protocole Internet attribue une â□□adresseâ□□ Ã chaque appareil qui est attachÃ© au rÃ©seau. Tout appareil qui tente de se connecter Ã un rÃ©seau ou Internet; que ce soit un ordinateur portable, une tÃ©lÃ©phone mobile, une imprimante, un scanner, une tablette, etc., doit avoir une adresse qui lui est attribuÃ©e pour lui permettre de se connecter. Ne pas avoir une adresse revient Ã essayer de tÃ©lÃ©phoner Ã quelquâ□□un, sans avoir de tonalitÃ©.

Le problÃ¨me qui se prÃ©sage pour les rÃ©seaux est que le Protocole Internet actuel (IPv4) nâ□□a plus aucune nouvelle adresse Ã allouer. Lâ□□IPv6 corrige ce problÃ¨me en offrant un plus grand nombre de nouvelles adresses qui resteront disponibles pendant de nombreuses annÃ©es.

Ainsi, alors que lâ□□iPv6 va nous permettre de rester â□□connectÃ©â□□, on peut se demander quelles seront les implications dâ□□un point de vue de la sÃ©curitÃ©.

Est-ce que ce protocole facilitera la propagation de logiciels malveillants?

Le nombre dâ□□adresses uniques possibles en IPv6 est largement plus Ã©levÃ© quâ□□en IPv4, reprÃ©sentant un total dâ□□environ 3.4x1038 adresses. Pour se faire une idÃ©e de ce que reprÃ©sente un tel nombre, on peut utiliser la mÃ©taphore suivante: si une adresse Internet unique a la taille dâ□□un grain de sable (1 millimÃ¨tre cube), alors il faudrait lâ□□Ã©quivalent de 340 millions de planÃ¨tes creuses (chacune de la taille de la Terre) pour contenir toutes les adresses possibles disponibles en IPv6. Or, en IPv4, il faudrait seulement 4 mÃ¨tres cubes! On comprend alors que scanner tout lâ□□espace dâ□□adresses IPv6 est impossible.

De mÃªme quâ□□il sera trÃ¨s improbable dâ□□identifier une adresse attribuÃ©e en gÃ©nÃ©rant des adresses IPv6 de faÃ§on alÃ©atoire.

La consÃ©quence positive de cela câ□□est que les menaces sur le rÃ©seau, telles quâ□□elles existent aujourdâ□□hui, auront beaucoup plus de difficultÃ©s Ã se propager. En effet, leur propagation est basÃ©e sur la gÃ©nÃ©ration alÃ©atoire dâ□□adresses IP.

Avec lâ□□IPv6, la probabilitÃ© de gÃ©nÃ©rer au hasard des adresses dÃ©jÃ Â attribuÃ©es, est pratiquement nulle. Les hackers devront donc adapter les logiciels malveillants sur le rÃ©seau pour les rendre efficaces dans lâ□□espace dâ□□adressage Ã©tendu prÃ©vu par le protocole IPv6.

Malheureusement, les menaces sur le rÃ©seau sont loin de reprÃ©senter la majoritÃ© des logiciels malveillants et la transition du protocole nâ□□a aucun effet sur tous les autres types de menaces Internet : ceux opÃ©rant au niveau de la couche dâ□□application, comme les vers qui se propagent par emails, les virus et les bots; ou ceux ciblant le contenu, comme les logiciels malveillants dÃ©livrÃ©s via YouTube, Facebook, etc. Ces menaces, qui correspondent Ã la majoritÃ© des logiciels malveillants aujourdâ□□hui, fonctionneront de la mÃªme maniÃ¨re et auront la mÃªme capacitÃ© Ã compromettre les systÃ¨mes, voler les donnÃ©es, dÃ©tourner les appareils en bots, etc.

Sera-t-il encore plus difficile en iPv6 dâ□□identifier la source des attaques Internet?

Compte tenu du nombre quasi infini dâ□□adresses IPv6, on pourrait penser quâ□□il est dÃ©sormais pratiquement impossible de dÃ©tecter lâ□□origine dâ□□une attaque. La rÃ©alitÃ© câ□□est que ce sera beaucoup plus facile quâ□□en iPv4, parce que **lâ□□IPv6 impose le support dâ□□IPSec** (Ã lâ□□inverse de lâ□□IPv4), qui est utilisÃ© pour authentifier lâ□□origine dâ□□un paquet IP. Bien que cela nâ□□empÃªchera pas les attaquants de se â□□cacherâ□□ derriÃ¨re des proxies, cela devrait empÃªcher la falsification de lâ□□adresse dâ□□origine dans des protocoles "non connectÃ©sâ□□ (type UDP).

Le passage Ã lâ□□iPv6 ne sera certainement pas un inhibiteur pour la cybercriminalitÃ© qui continue Ã se dÃ©velopper trÃ¨s fortement, avec des logiciels malveillants toujours plus sophistiquÃ©s et combinant plusieurs types dâ□□attaques. Il est donc essentiel pour toutes les organisations de sâ□□Ã©quiper dâ□□une premiÃ¨re ligne de dÃ©fense efficace en dÃ©ployant des solutions de sÃ©curitÃ© multi-menaces. Cette mesure combinÃ©e avec une meilleure Ã©ducation des utilisateurs reste la meilleure protection contre la tromperie et lâ□□innovation pure des cybercriminels.