Lâ□□Internet que nous connaissons existera-t-il encore en 2013 ?
Internet
PostÃ© par : JPilo
PubliÃ©e le : 4/1/2013 13:00:00

Est-ce un bouleversement sur Â« Qui contrÃ´le Internet Â» ? La dÃ©couverte dâ□□une nouvelle Ã©pidÃ©mie de malware Mac ? Une attaque de type DDoS des Smart TV? Peu importe ce que nous rÃ©serve 2013, il est certain que ce sera une annÃ©e charniÃ¨re. Voici ce que le **F-Secure Labs prÃ©voit pour lâ□□annÃ©e Ã venir.**

1. Et si câ□□Ã©tait la fin dâ□□Internet tel que nous le connaissons ?

Â« *Selon les Ã©changes survenus lors de la World Conference on International Telecommunications (qui a eu lieu en dÃ©cembre Ã DubaÃ¯), 2013 devrait Ãªtre une annÃ©e riche en Ã©vÃ¨nements* Â», dÃ©clare **Sean Sullivan**, Security Advisor chez F-Secure Labs. Cette confÃ©rence pourrait avoir un impact majeur sur Internet tel que nous le connaissons aujourdâ□□hui: Â« *Internet pourrait se morceler en une sÃ©rie de petits Internets* Â», avance **Sean Sullivan**. Â« *Il est aussi possible quâ□□Internet devienne un espace financÃ© par des grands groupes de fournisseurs de contenus, tels que Facebook, Google ou Youtube. Et que ceux-ci imposeraient des taxes aux internautes souhaitant accÃ©der aux informations quâ□□ils proposent.* Â»

Le WCIT (World Congress on Information Technology) est une confÃ©rence organisÃ©e par lâ□□International Telecommunication Union (ITU) pour finaliser le traitÃ© des Â« International Telecommunications Regulations Â». Parmi les participants, on trouve des reprÃ©sentants des gouvernements de tous les pays, dont de nombreux opposants Ã une utilisation libre dâ□□Internet. Il sâ□□agit notamment de rÃ©gimes gouvernementaux qui aimeraient reprendre le contrÃ´le dâ□□Internet, actuellement aux mains des Â« geeks Â», explique **Sean Sullivan**. De nouvelles mesures ont mÃªme dÃ©jÃ Ã©tÃ© proposÃ©es, avanÃ§ant des raisons de sÃ©curitÃ©. Toutefois, les dÃ©fenseurs de la vie privÃ©e estiment que ces mesures entraÃ®neraient la fin de lâ□□anonymat sur Internet.

2. Des fuites nous rÃ©vÃ¨leront une augmentation des outils dâ□□espionnage financÃ©s par les gouvernements

Â« *Il est clair que depuis les derniÃ¨res fuites liÃ©es Ã Stuxnet, Flame et Gauss, la course aux cyber-armement est belle et bien lancÃ©e* Â», dÃ©clare **Mikko Hypponen**, Chief Research Officer chez F-Secure. MÃªme si nous ne serons pas toujours au courant des cyber-opÃ©rations lancÃ©es par des Ã©tats-nations, nous pouvons nous attendre Ã ce que ces activitÃ©s soient de plus en plus utilisÃ©es par les gouvernements. En 2013, il est fort probable de voir une augmentation de telles fuites, y compris en provenance de pays qui nâ□□ont jamais Ã©tÃ© Ã lâ□□origine dâ□□attaques Ã ce jour. Avec le lancement dâ□□une vÃ©ritable course Ã lâ□□armement, les fuites ne cesseront dâ□□augmenter.

3. Lâ□□utilisation des malware mobile se dÃ©mocratisera

Android sâ□□est dÃ©veloppÃ© comme aucun autre systÃ¨me dâ□□exploitation par le passÃ©, passant des smartphones aux tablettes puis aux Smart TV. Et plus un systÃ¨me dâ□□exploitation se gÃ©nÃ©ralise, Â« plus il est facile de crÃ©er des malware performants, et plus il y aura dâ□□opportunitÃ©s pour les criminels de mettre en place des activitÃ©s lucratives, Â» dÃ©clare Sean Sullivan. Les malware ciblant les mobiles seront facile dâ□□accÃ¨s, grÃ¢ce Ã des kits dâ□□outils crÃ©Ã©s et vendus par des cybercriminels spÃ©cialistes du hack Ã dâ□□autres criminels, non experts.

En quelques sortes, des Â« malware-as-a-service Â», pour Android.

4. Une autre Ã©pidÃ©mie de malware frappera lâ□□univers du Mac

Le scareware appelÃ© Mac Defender fut propagÃ© en 2011 ; En 2012, Flashback profita des failles de Java. Pour 2013, le Labs prÃ©voit la dÃ©couverte dâ□□une autre Ã©pidÃ©mie de malware Mac qui devrait faire des ravages au sein de la communautÃ© Mac.

Â« *Lâ□□auteur du Cheval de Troie FlashBack est toujours en fuite. Il paraÃ®trait mÃªme quâ□□il serait en train de travailler sur une nouvelle offensive*Â» estime **Sean Sullivan**. Â« *MalgrÃ© les amÃ©liorations en sÃ©curitÃ© apportÃ©es Ã Mac OS, une partie des utilisateurs Mac continue de rester inconsciente des risques encourus, ce qui les rend vulnÃ©rables face aux nouveaux malware.* Â»

5. Les Smart TV deviendront une nouvelle cible pour les hackers

Les Smart TV sont connectÃ©es Ã Internet. Elles sont trÃ¨s puissantes mais ne sont gÃ©nÃ©ralement pas sÃ©curisÃ©esâ□¦ et deviennent donc vulnÃ©rables aux attaques. Elles sont dâ□□autant plus vulnÃ©rables que, contrairement aux ordinateurs, elles sont souvent connectÃ©es Ã Internet sans le nÃ©cessaire pour empÃªcher le trafic indÃ©sirable. Par ailleurs, les consommateurs oublient souvent de changer le nom dâ□□utilisateur et le mot de passe par dÃ©faut, ce qui facilite lâ□□accÃ¨s aux hackers.

Â« *Câ□□est trÃ¨s facile pour les hackers de rechercher et trouver les Smart TV sur Internet,* Â» dit Sean Sullivan. Â« *Une fois trouvÃ©es, ils nâ□□ont plus quâ□□Ã utiliser le nom dâ□□utilisateur par dÃ©faut et le mot de passe de la TV en question, et le tour est jouÃ©.* Â» En 2012, une famille de malware, LighAidra, a infectÃ© des dÃ©codeurs. En 2013, les Smart TV pourraient Ãªtre utilisÃ©es pour des fraudes utilisant les clicks (le Bitcoin mining) ou encore des attaques de type DDoS.

6. Les logiciels espions pour mobiles seront de plus en plus nombreux

2013 sera lâ□□annÃ©e des logiciels de tracking, dont la cÃ´te qui monte en flÃ¨che. Ces derniers seront utilisÃ©s pour des raisons autres que celle du contrÃ´le parental.

Il y a eu une nette croissance du nombre dâ□□applications de sÃ©curitÃ© pour les enfants, permettant de surveiller les activitÃ©s et comportements de ces derniers sur la toile, et notamment

sur Facebook.

"*Il apparaÃ®t Ã©vident que ce type de logiciel peut Ã©galement Ãªtre utilisÃ© pour espionner nâ□□importe qui, et pas seulement les enfants*," dÃ©clare **Sean Sullivan**. Â«*Plus lâ□□utilisation du Smartphone sera rÃ©pandue, plus les gens chercheront ce type de logiciels, par exemple pour savoir ce que deviennent leurs ex !* Â».

Lisez notre article sur : **Et si Internet s'arretait.**