Sécurité : le virus informatique a 30 ans

Nous sommes le **10 novembre 1983**. **Fred Cohen** est un étudiant en informatique de la School of Engineering de l'Université de Californie du Sud. Il vient d'écrire un court programme qu'il a glissé dans une commande Unix et qui va en 5 minutes prendre le contrôle d'un mainframe.

Certes ce n'est pas la première fois qu'un programme de ce type est écrit. C'est en effet un peu plus tôt, en **1982**, qu'un gamin de 15 ans, **Rich Skrenta**, un lycéen de Pennsylvanie, a écrit un programme pour Apple II qui prend le nom de Elk Cloner. Celui-ci se réplique automatiquement lors du boot (démarrage) de la machine sur une disquette afin, tous les 50 boots, d'afficher un message :

It will get on all your disks
It will infiltrate your chips
Yes, it's Cloner!

It will stick to you like glue
It will modify RAM too
Send in the Cloner!

Alors pourquoi fêter aujourd'hui les 30 ans du 'virus' ? Parce qu'à l'époque, cela s'appelait un programme. Ce n'est en effet qu'un an plus tard, le 10 novembre 1983, que Fred Cohen a employé pour la première fois l'expression 'virus'. Une expression qui va rester et faire le tour du monde. Même si les menaces ont évolué. L'expression sera reprise et vulgarisée par un certain **Len Adleman**. Ce nom ne vous dit rien ? Il est le 'A' de RSA Security.

Rich Skrenta avait écrit un vrai virus informatique, destiné à perturber le fonctionnement de la machine. Fred Cohen a quant à lui écrit un *proof of concept* (PoC), un programme informatique destiné à être testé, ou à démontrer une théorie, ici la capacité à prendre le contrôle d'un mainframe. Le PoC, volontaire, est d'ailleurs la seconde source des virus, la première, involontaire, étant tout simplement les développements de lignes de code dont l'exécution entraine des réactions inattendues de l'ordinateur, à la surprise de leur auteur. La plupart d'entre eux ne quitteront pas l'ordinateur qui a servi à les programmer, et ne représentent donc pas de menace.

Le virus, intimement lié à l'histoire de l'informatique

Depuis l'adoption de son expression, l'histoire de l'informatique est riche en virus. Nous avons relevé quelques dates concernant les phénomènes viraux :

– **1986**, le premier virus **Brain** fait son apparition. Il cible précisément l'IBM PC. En plus de se glisser dans un programme médical, sa particularité provient de l'égo de ses auteurs, deux frères Pakistanais, qui ont glissé leur nom et numéro de téléphone dans le code ! Pour se faire 'vacciner', ils invitent leurs victimes à prendre contact avec eux. Une première. Le virus se fait mafieux, la prochaine fois il faudra payer pour se délivrer de la menace affichée…

– Le **2 novembre 1988**, **Robert Morris**, encore un étudiant de Cornell, a lâché le premier '***worm***'

(ver), un virus qui avance caché à l'intérieur du code d'une application. Ce programme de 99 lignes sous Unix, encore un PoC, a infecté les environnements Sun Microsystems et Digital Equipment VAX.

– **1999**, **Melissa** est le premier virus worm diffusé en masse via des **e-mails**. 250 000 PC sont infectés. Il sera suivi en **2000** par **Love Bug**, repris et modifié par un étudiant philippin sous le nom de **I Love You**, le virus qui aura probablement fait le plus de dégâts connus. Hébergé contre leur volonté par 55 millions d'ordinateurs, il fera 2,5 à 3 millions (impossible de connaitre les chiffres exacts) de victimes en effaçant des fichiers de leurs PC. Tous deux sont des **macro-virus**. Ils exploitent des scripts du langage Visual Basic de Microsoft. Ils auront au moins eu le 'mérite' de sensibiliser l'éditeur, qui va entièrement restructurer sa démarche de sécurité de ses développements et de ses produits.

– **2001**, **Code Red**, premier virus dédié aux serveurs Microsoft, cible Microsoft IIS (*Internet Information Server*) pour attaquer les sites web par **DoS** (Denial-of Service). Il affiche sur les serveurs vérolés le message « *Hacked by Chinese* ». 300 000 serveurs seront infectés au cours du premier mois.

– Suivront **Nimba**, **Slammer**, **Blaster**, **MyDoom**… Il s'attaquent en priorité aux environnements Microsoft, Windows 95, MS SQL, etc. les plus répandus. Il faudra attendre **2004** et le SP2 de Windows XP pour que l'éditeur place enfin et, pour la première fois, un pare-feu dans son OS.

– En **2008** apparait **Conflicker**, l'un des **botnets** les plus virulents. En avril 2009, il aura infecté 300 000 domaines.

– Quant au **malware Stuxnet**, qui ciblait le programme nucléaire iranien, il nous apprend (ou confirme) que tous les virus ne sont pas mafieux, et que même de très sérieuses agences de renseignement jouent au jeu des menaces virales. Stuxnet a été programmé par des développeurs israéliens et par la célèbre NSA (National Security Agency), l'agence de renseignement américaine au centre du scandale des écoutes massives sur la Toile.

La prochaine grande vague de virus est déjà attendue, elle devrait cibler… les smartphones et tablettes.

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes