NOUVEL HAY MAGAZINE
SANS FRONTIÈRES

Un million et demi de personnes sont hackées chaque jour dans le monde

Les internautes ne savent plus à quel saint se vouer .En effet on a appris que la NSA (National Security Agency) US espionne Google,Yahoo!,Microsoft, Facebook , etc..

Maintenant on sait qu'environ 1 million et demi de gens subissent le hacking, phishing & autres mots anglais , chaque jour .De quoi rendre paranoïaque dès qu'on se rend sur la toile.

Le Hacker :

Un **hacker** est une personne qui montre une passion pour la compréhension du fonctionnement intime des systèmes, ordinateurs et réseaux informatiques en particulier[1].

En sécurité informatique, un **hacker** est un spécialiste dans la maîtrise de la sécurité informatique et donc des moyens de déjouer cette sécurité. Certains d'entre eux utilisent ce savoir-faire dans un cadre légal et d'autres l'utilisent hors-la-loi. Dans ce dernier cas, on parle de **pirates informatiques**[2].

Hacker, dans sa signification relayée par les médias de masse, se réfère aux chapeaux noirs (pirate informatique). Afin de lever l'ambiguïté sur le terme hacker, *cracker* est souvent utilisé pour désigner les *black hats*, le démarquant ainsi de la culture académique des hackers telle que définie par Eric Raymond[3].

Sommaire

[masquer]

• 1 Terminologie
• 2 Associations de hackers célèbres
• 3 Manifestations de hackers
• 4 Hackers célèbres
• 5 Hackers dans les œuvres de fictions
• 6 Publications francophones en sécurité informatique
• 7 Productions audiovisuelles
• 8 Notes et références
• 9 Voir aussi
- 9.1 Articles connexes
- 9.2 Bibliographie
- 9.3 Filmographie

Terminologie[modifier]

Le jargon informatique classe les hackers en plusieurs catégories en fonction de leurs objectifs, de leur compétence et de la légalité de leurs actes. Ce vocabulaire fait référence aux films de western, où le héros porte un chapeau blanc, et les méchants portent des chapeaux noirs. Par respect nous utiliserons le terme cracker et non hacker pour désigner ces personnes.

- Les **chapeaux blancs** ou *white hat* : professionnels de la sécurité informatique (consultants en sécurité, administrateurs réseaux...) effectuant des tests d'intrusions en accord avec leurs clients et la législation en vigueur afin de qualifier le niveau de sécurité de systèmes. Certains hackers se considèrent comme white hat alors qu'ils transgressent les lois, leur but étant de prévenir les responsables des failles de leurs systèmes. Certains d'entre eux s'infiltrent dans les systèmes de sécurités les plus coriaces juste pour la connaissance, pour se dire qu'ils savent le faire
- Les **chapeaux noirs** ou *black hat* : créateurs de virus, cyber-espions, cyber-terroristes ou cyber-escrocs, agissant la plupart du temps hors-la-loi dans le but soit de nuire, de faire du profit ou d'obtenir des informations. Ces hackers n'ont pas la même éthique que les White hats et sont souvent malveillants. Les plus malveillants sont alors appelés *crashers*.

- Les **chapeaux gris** ou *grey hat* : s'ils n'hésitent pas à pénétrer dans les systèmes sans y être autorisés, ils n'ont pas de mauvaises intentions. C'est souvent l'« exploit informatique » qui les motive, une façon de faire la preuve de leur agilité. Cette catégorie recouvre le large panel de personnes se situant entre le *black hat* et le *white hat*.
- Les **script kiddies** ou *lamer*, littéralement « gamins qui utilisent des scripts » : sans grande compétence, ceux-ci piratent surtout par désir de se faire remarquer, en utilisant des programmes codés par d'autres. Ces personnes ne sont pas à proprement parler des hackers, mais elles se considèrent généralement comme tels.
- Les **hacktivistes** : agissant afin de défendre une cause, ils n'hésitent pas à transgresser la loi pour attaquer des organisations afin de les paralyser ou d'obtenir des informations.

Il serait réducteur de généraliser le cas et d'en déduire que les *white hats* sont les gentils et les *black hats* sont les méchants. En effet, de nombreux débats se font entre les deux camps et aucun camp n'a réussi à prouver que le sien était la voie à suivre. De nombreux *white hats ne servent que leurs intérêts alors que d'autres* black hats protègent ceux des autres. C'est d'ailleurs un sujet de troll récurrent.

Associations de hackers célèbres[modifier]

Les principaux **groupes de hackers** sont :

- *Chaos Computer Club* (groupe allemand, le plus grand groupe de **hackers** européen, créé en 1981). Attention à ne pas confondre avec son homonyme français.
- *The Cult of the Dead Cow* (créateur de Back Orifice 2000, un logiciel de prise de contrôle à distance)
- *2600* (groupe hacker new-yorkais ; la fréquence du sifflet du *Captain Crunch* était de 2600 Hz) ; et la branche 2600 pour la France.
- *Hacking For Girliez* (groupe de hackers féminins) ; responsable de nombreux piratages de sites comme ceux de la NASA, du *New York Times* ou de la firme Motorola.

Manifestations de hackers[modifier]

Depuis la fin des années 1980, certains groupes organisent des « manifestations » régulières, comme :

- *DEF CON* : de nombreuses def cons ont été organisées depuis 1983
- *Chaos Communication Congress* (organisé par le Chaos Computer Club, tous les ans entre Noël et le jour de l'An)
- *Chaos Communication Camp* (organisé par le Chaos Computer Club, tous les quatre ans, depuis 1999)
- *Black Hat Briefings*
- *Hackers on Planet Earth*
- *ToorCon*
- *Hackathon (organisé par le projet OpenBSD, tous les ans depuis 1999)*
- *Nuit du Hack* : de nombreuses nuit du hack ont été organisées en France depuis 2003
- *Hacker Space Festival : en France*

D'autres rassemblements changent de nom à chaque fois, comme ceux organisés initialement par ce groupe des Pays-Bas uni autour du magazine Hack-Tic :

- Galactic Hacker Party en 1989
- Hacking at the End of the Universe en 1993
- acking In Progress en 1997 qui a rassemblé près de deux mille personnes
- *Hackers At Large* en 2001 qui a rassemblé plus de trois mille personnes
- *What The Hack* en 2005 qui a rassemblé plus de deux mille personnes

Hackers célèbres[modifier]

- Daniel J. Bernstein : auteur de qmail et djbdns, également mathématicien et cryptographe.
- Bill Landreth : auteur du best-seller *Le Pirate de l'Informatique : Guide de la sécurité informatique* en 1985.
- Kevin Mitnick : s'infiltra dans certains des plus grands sites internet sécurisés, comme celui du Pentagone.
- Islam Brahimi : connu pour avoir accédé illégalement à plusieurs ordinateurs reliés à Internet en créant l'un des plus grands réseaux

Botnet de 500 000 ordinateurs infectés.

- H.D Moore[4] : créateur de Metasploit
- Jon Ellch : plus connu sous le pseudonyme de Johnny Cash, il a particulièrement fait parler de lui en 2006 en démontrant avec son acolyte David Maynor l'existence de vulnérabilités dans les pilotes Wi-Fi, dont ceux d'Apple.
- Joanna Rutkowska : elle s'est fait connaitre de la communauté en 2006 grâce à la fameuse Blue Pill, un rootkit exploitant la technologie de virtualisation Pacifica d'AMD pour prendre le contrôle de Windows Vista.
- Gary McKinnon : accusé d'avoir pénétré dans 97 ordinateurs appartenant à l'US Army et à la NASA.
- Kevin Poulsen : connu sous le pseudonyme Dark Dante, il fut le premier hacker à être accusé d'espionnage aux États-Unis.
- R1NZL3R : hacker d'Anonymous rejeté pour avoir trop fouiné. Désormais reconverti chez 2600
- Jon Lech Johansen….

Source : WIKIPEDIA.fr