

La cybercriminalité en mouvement

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 octobre 2012

<https://www.bortzmeyer.org/cybercriminalite-mouvement.html>

Auteur(s) : Éric Freyssinet
ISBN n°9782746232884
Éditeur : Hermes-Lavoisier
Publié en 2012

Un livre utile pour celui qui s'intéresse à la cybercriminalité sous tous ses aspects. En 200 pages, l'auteur, un expert du domaine, réussit à couvrir à peu près tout. Évidemment, cela veut dire que les passionnés de tel ou tel aspect resteront un peu sur leur faim mais, pour celui qui ne connaît pas encore bien la cybercriminalité, voici un livre sérieux et bien expliqué.

Quand même, je trouve l'ouvrage mince, surtout pour son prix très élevé (56 €). Mais il couvre pourtant plein de choses. On y trouve tout le panorama de la cybercriminalité actuelle, sans sensationnalisme et avec beaucoup de concret (et plein de références). Ainsi, l'importance du caractère organisé et professionnel de la cybercriminalité est bien expliqué, ainsi que l'organisation complexe du cybercrime : le type qui écrit le malware n'est pas celui qui gère le botnet et celui qui commande une attaque DoS comme on commande un livre à Amazon est encore un autre. C'est tout un écosystème qui s'est ainsi développé. L'auteur parle d'ailleurs de CaaS, « *Crime as a Service* » pour illustrer le fait qu'on peut louer des services de délinquants. De même, l'auteur explique bien le fonctionnement des botnets, sujet sur lequel il participe au projet <<http://www.botnets.fr/>>.

Comme toujours en matière de sécurité (pas seulement de sécurité informatique), les questions politiques de droit et de liberté ne sont jamais loin. J'y apprends par exemple qu'il n'y a pas encore de jurisprudence pour savoir si une attaque DoS peut être assimilée au droit de manifestation. En parlant des Anonymous, l'auteur regrette que le temps passé à les pourchasser soit au détriment d'autres tâches plus utiles. Le reproche-t-il aux Anonymous ou bien aux politiciens qui mettent en avant le danger de la contestation plutôt que celui de la criminalité? On ne le saura pas.

Globalement, l'auteur, un gendarme, n'hésite pas devant la déformation professionnelle. Il privilégie le point de vue des enquêteurs : disposer de plus de moyens mais aussi de plus de possibilités légales, de plus de données enregistrées, et de plus de contrôles (par exemple des papiers d'identité dans les cybercafés, comme obligatoires en Italie). Et, concernant, l'anonymat, j'ai été surpris de voir qu'il était

considéré dans ce livre comme un privilège (pour les opposants aux dictatures féroces, uniquement) et pas comme un droit.

Ah, et puis les défenseurs fervents d'IPv6 noteront que celui-ci est accusé de compliquer les enquêtes, via les techniques de coexistence avec IPv4 qui sont nécessaires.

On peut aussi consulter la critique des Échos <<http://www.lesechos.fr/culture-loisirs/livres/0202478632648-internet-un-territoire-a-securiser-sans-cesse-526225.php>>, la bonne analyse de Gof dans la Mare <<http://lamaredugof.fr/blog/2012/11/lecture-lcem/>> (où il reproche notamment à l'auteur de ne pas assez donner son opinion), le blog de l'auteur <<http://blog.crimenumerique.fr/>> et le site officiel autour du livre <<http://lcm.fr/>>.