

# Les enjeux de la cybercriminalité

Par Ali EL AZZOUZI

Paru en Juillet 2009

Afrique Challenge

L'image de l'adolescent cherchant désespérément un serveur vulnérable sur Internet depuis sa chambre au sous-sol est révolue. Aujourd'hui la cybercriminalité s'impose comme métier à part. Il s'agit d'une activité qui obéit de plus en plus aux logiques de l'activité économique conventionnelle telles que la croissance, la rentabilité financière, la gestion des risques, l'organisation et la division du travail.

## I) Démystification de la cybercriminalité

---

### ***La cybercriminalité : Une activité en pleine croissance***

Grâce notamment à la diffusion sur le Web de nouveaux services et outils s'adressant à une population mondiale de plus en plus disposée à les adopter, la croissance des actes cybercriminels s'est particulièrement accélérée ces trois dernières années. Cette tendance risque de s'amplifier avec la mise à profit du Web 2.0 : réseaux sociaux, blogs, forums, wikis, FaceBook, MySpace, YouTube, Twitter, etc.. En effet, tous ces services en ligne jouent sur la facilité de téléchargement, de publication et d'autres techniques d'échange des informations, qui rendent leurs utilisateurs vulnérables aux infections de logiciels malveillants<sup>1</sup>.

Rappelons qu'en cette période de marasme économique, les attaques cybercriminelles sont censées connaître une forte hausse. En effet, il est reconnu que les périodes de ralentissement économique sont systématiquement caractérisées par des augmentations de la criminalité. Les pertes d'emplois et l'augmentation des pressions financières, entraînent un brusque mouvement ascendant de l'activité criminelle en général, et l'on doit s'attendre dans le ralentissement actuel à une forte croissance de l'activité cybercriminelle.

### ***La cybercriminalité : Une activité rentable***

---

<sup>1</sup> Défis de la cybercriminalité, Eugène Kaspersky, dossier « Cybercriminalité, une guerre perdue ? » Documentation française. Hiver 2008-2009

Pour attirer l'attention de son auteur, une opération de piratage devrait désormais générer du revenu. La cybercriminalité est devenue au fil des temps une activité extrêmement profitable. Des sommes importantes ont été détournées avec succès. Rien qu'en 2008, la cybercriminalité a coûté 1.000 milliards de dollars, d'après une étude de McAfee<sup>2</sup> présentée au forum de Davos. Certaines sources estiment que la cybercriminalité a dépassé le commerce illégal de la drogue en termes de profits en 2007.

### ***La cybercriminalité : Une activité facile***

Avec la vulgarisation des modes opératoires cybercriminels sur Internet, aujourd'hui il n'est pas nécessaire de disposer de compétences techniques pour lancer une opération cybercriminelle. Le niveau d'expertise technique requis pour un projet cybercriminel n'a plus du sens du moment où il est possible aujourd'hui d'acheter librement les logiciels espions les plus élaborés ainsi que les données collectées par ces mêmes logiciels: informations bancaires et informations personnelles suffisantes pour acheter en ligne ou transférer des fonds. En outre, il est aussi possible de commander un acte cybercriminel ponctuellement auprès de prestataires spécialisés qui viennent chacun apporter leur part d'expertise dans l'opération, chaque maillon générant des bénéfices dont le montant répond uniquement aux lois de l'offre et de la demande, la rareté d'une compétence augmentant les prix en conséquence.

### ***La cybercriminalité : Une activité à faible risque***

Internet est parfaitement adapté à l'activité frauduleuse (anonymat, faibles barrières à l'entrée, difficultés d'application de la loi à des juridictions multiples), et donc, comparé à la perpétration d'un crime « traditionnel » les coûts sont plus faibles et il est beaucoup moins probable d'être arrêté. Il s'agit donc d'une activité à faible risque comparé aux chances de réussite. Dans le monde réel, la dimension psychologique avec la prise de risques concrets du crime assure un certain effet de dissuasion. Mais dans le monde virtuel, les criminels ne sont jamais directement en contact avec leurs victimes ni avec les différentes sociétés qu'ils décident d'attaquer.

### ***La cybercriminalité : Une activité organisée***

---

<sup>2</sup> [http://www.vnunet.fr/news/cyber\\_criminalite\\_la\\_fraude\\_qui\\_valait\\_mille\\_milliards\\_de\\_dollars-2030036](http://www.vnunet.fr/news/cyber_criminalite_la_fraude_qui_valait_mille_milliards_de_dollars-2030036)

Une étude conjointe entre le CERT et le FBI démontre que dans 81% des incidents recensés dans les entreprises, les attaquants avaient planifié leur action à l'avance. Il ne s'agit donc nullement d'opérations lancées au hasard. La réussite d'un acte cybercriminel exige une discipline de fer en amont, durant et en aval de toute opération cybercriminelle. Cette discipline a comme pré requis de base, un travail en équipe dont les éléments ne se sont probablement jamais rencontrés réellement. Ce travail d'équipe engage une segmentation et une spécialisation à outrance dans les différents maillons de la chaîne cybercriminelle. Ainsi au lieu de maîtriser l'ensemble de la chaîne des opérations, les cyberdélinquants se concentrent sur l'un de ses maillons, afin de le maîtriser à la perfection, ce qui permet de réduire considérablement leurs prises de risques. Analysons l'écosystème qui gravite autour par exemple des chevaux de troie. Souvent, ils sont conçus par des développeurs logiciels, qui en général n'exploitent plus par eux-mêmes leurs créations. Ils concentrent leurs efforts sur l'innovation technologique nécessaire à la conception de ces codes malicieux, et s'organisent en micro-entreprises de deux ou trois développeurs, comprenant une cellule de support technique et un « commercial » chargé de développer les débouchés économiques du groupe. Ces développeurs vendent leurs créations comme de véritables produits, packagés avec une documentation utilisateur dans la langue de leurs clients. Certains groupes proposent même un support client 24/24 et offrent même une garantie de non détection du malware par les anti-virus.

## **II. Moyens de lutte contre la cybercriminalité**

---

### ***L'arsenal juridique***

La lutte contre la cybercriminalité commence d'abord par la mise à niveau de l'arsenal juridique. Ce dernier doit réprimer non seulement l'activité criminelle dans laquelle le système ou le réseau informatique est une partie essentielle du crime, mais également l'activité criminelle traditionnelle dans laquelle les ordinateurs ou les réseaux sont utilisés pour réaliser une activité illicite. Dans le premier cas, les technologies sont la cible de l'attaque ; dans le second, elles en sont le vecteur.

Toutefois, le manque de jurisprudence ainsi que de définitions communes entre le technicien et le magistrat sont autant de limites à la mise en place d'une réelle politique judiciaire de répression de la cybercriminalité.

### ***Le partenariat public-privé***

Si les Etats ont clairement un rôle à jouer dans la régulation de l'activité cybercriminelle, il ne faut pas pour autant écarter de cette lutte le secteur privé. Riches d'expériences et de savoir-faire, ces acteurs doivent pouvoir s'inscrire dans une telle démarche. Ce partenariat est de nature à améliorer la sécurité de l'écosystème en établissant la sûreté et la confiance des internautes comme cyberconsommateurs. Concrètement, ce partenariat public-privé doit se structurer autour de processus clairement identifiés de partage d'informations. C'est la raison pour laquelle des institutions doivent pouvoir exister et disposer de capacités tant matérielles que légales pour permettre et encourager justement cette diffusion de l'information. Par exemple, des industriels américains ont développé avec les partenaires publics des institutions comme le CERT ou l'ISACs.

Les conclusions du séminaire Octopus tenu à Strasbourg en avril 2008 sont exemplaires. Elles fondent le socle d'un guide des bonnes pratiques dans le partenariat privé-public dans le cadre de la lutte contre la cybercriminalité. Ce guide est un outil de progrès indéniable pour les pays africains.

### ***La coopération internationale***

L'absence ou l'insuffisance de dialogue et de coordination au niveau international rend plus difficiles la détection des opérations cybercriminelles et la poursuite de leurs auteurs. Il y a bien des initiatives diverses mais elles sont encore trop éparses ou indépendantes les unes des autres pour qu'il en émane réellement une cohérence dans la politique de lutte contre la cybercriminalité à l'international. En outre, trop d'Etats ont des législations différentes au point que les criminels profitent de ces failles juridiques. D'où la nécessité de mettre en place un Interpol pour Internet et accélérer le rythme de collaboration au niveau international.

### **III. Conclusion**

---

Compte tenu de l'attractivité dont réjouit l'activité cybercriminelle en raison de sa forte rentabilité, de l'absence de barrières à l'entrée et du faible risque, il devient extrêmement urgent de se lancer dans la lutte sérieuse contre ce phénomène qui touche aussi bien les pays occidentaux que les pays de sud. Cette lutte ne doit pas se limiter à la pénalisation des activités criminelles, il faudra surtout imaginer les moyens permettant l'instauration d'une véritable confiance numérique.