INTERNET

Crimes et châtiments

Crime et terrorisme prospèrent aussi sur l'internet. Lutter efficacement contre les agresseurs suppose de mieux les connaître. Typologie des crimes et des criminels sur le réseau.

Solange Ghernaouti-Hélie
Professeur à l'Ecole des HEC de l'université de Lausanne

Bertrand Lathoud
Assistant diplômé à l'Ecole des HEC de l'université de Lausanne

Avec la multiplication d'agressions de diverses natures, le monde de l'internet a perdu son ingénuité. Internet n'est plus seulement le réseau libre et ouvert dont les pionniers avaient rêvé. Il est aussi devenu un moyen d'expression de la criminalité, de la guerre et du terrorisme.

Tous les crimes et délits "communs" (racket, traite des êtres humains, trafics en tous genres, escroquerie, vol, destruction, etc.) que les organisations criminelles commettent sont susceptibles de bénéficier de l'utilisation des nouvelles technologies de l'information et notamment de l'internet. Le Business Process Reengineering n'est pas réservé aux seules entreprises légales…

> « Internet est aussi devenu un moyen d'expression de la crimininalité »

Par l'utilisation systématique de moyens récents de communication et de traitement de l'information, les terroristes professionnels peuvent améliorer leur efficacité et leur propre sécurité en limitant la quantité d'information susceptible d'être récupérée par la police. Les données chiffrées sont difficiles à intercepter et les dispositifs de télécommande autorisent le déclenchement à distance de machines infernales.

Cybercriminalité et cyberattaques

Les infrastructures économiques critiques comme l'électricité, l'énergie, les transports, les télécommunications, la banque et la finance, les services médicaux ou les fonctions gouvernementales sont de plus en plus souvent interconnectées. Cela les rend de plus en plus vulnérables à des attaques dirigées contre leur système d'information, notamment par le biais de l'internet. Ces nouvelles formes de la criminalité sont identifiées dans les tableaux décrivant les types d'infractions prévues par le nouveau code pénal français (voir tableaux ci-dessous).

Peu de statistiques relatives à la cybercriminalité sont encore disponibles. Néanmoins, la mise en place d'unités de lutte contre ce type d'actions révèle l'importance accordée par nombre de politiques à la cybercriminalité. Ainsi, les Etats-Unis se sont dotés de "Computer Investigation and Infrastructure Threat Assessment (CITA) squads" décentralisés, coordonnés par le National Infrastructures Protection Center (NIPC).

Une grande variété de délits et de crimes

La facilité avec laquelle l'information numérique peut être reproduite a favorisé l'apparition d'un

marché de la copie illicite. Cela représente un manque à gagner de plusieurs dizaines de milliards de dollars pour les éditeurs dans les domaines de la musique, du film vidéo ou des logiciels.

Internet donne une nouvelle dimension au marché de la pornographie. Il permet en effet à des communautés virtuelles clandestines de se constituer autour de pratiques rigoureusement punies par la loi (pédophilie, "snuff movies", etc.). Les échanges de matériels illicites au moyen des nouvelles technologies sont moins faciles à intercepter par la police. Les serveurs sont implantés dans des pays où les forces de police sont inexistantes, corrompues ou dépassées ; les fichiers sont chiffrés ; les utilisateurs accèdent aux informations via des serveurs Internet Relay Chat (IRC) privés et actifs pendant des durées très limitées.

Le conflit en ex-Yougoslavie a permis de mesurer la portée de la manipulation de l'information. Le pouvoir de Belgrade s'est servi de l'internet pour alimenter des rumeurs sur le nombre d'avions abattus ou l'étendue des dégâts écologiques provoqués par les bombardements. L'objectif visé était la déstabilisation des opinions publiques des Etats occidentaux.

Les réseaux permettent aussi à de nouveaux types d'escrocs de sévir. Il y a tout d'abord ceux qui usurpent une identité afin de bénéficier de prestations sans avoir à les payer. Leur outil de travail est souvent le logiciel de "carding" qui permet de créer des numéros de carte bancaire valides (bien que ne correspondant pas nécessairement à un compte réel). Il suffit ensuite d'acheter en ligne et de se faire livrer à une adresse de complaisance qu'on utilisera une seule fois. Certains réseaux spécialisés préfèrent se procurer des numéros de carte de crédit correspondant à des comptes sûrement existants. Il leur suffit de les acheter auprès de pickpockets ou de commerçants indélicats.

Une autre famille d'escrocs est constituée par tous ceux qui proposent des prestations inexistantes ou imaginaires. Une variante consiste à utiliser les sites de ventes aux enchères pour écouler des produits de mauvaise qualité ou volés.

Il est relativement aisé de se procurer sur l'internet des recettes pour la fabrication d'explosifs, la préparation de substances psychotropes ou la mise en œuvre de cyberattaques . Enfin, le réseau peut constituer un outil de communication pratique pour des groupes clandestins.

Typologie du cyberdélinquant

La protection d'un système d'information est plus facile lorsqu'on connaît celui contre qui on doit se protéger. Or il existe différents profils de cyberdélinquants.

Pendant longtemps, les "hackers" avaient pour motivation essentielle le désir de maîtriser toujours mieux les technologies. Si cette variété n'a pas totalement disparu, elle laisse progressivement la place à deux grands type de cyberdélinquants :
- les professionnels ;
- les amateurs.

Les professionnels sont guidés principalement par un intérêt économique. On peut ranger dans cette classe :
- les concurrents directs de l'entreprise visée ;
- des salariés, fonctionnaires ou militaires au service d'Etats (ou éventuellement d'organisations structurées non étatiques, du type organisations terroristes) ;
- les mercenaires (pouvant agir aussi bien pour le compte d'institutions privées que publiques) ;
- les truands des toutes sortes.

Parmi les amateurs, on trouve en particulier :
- les techniciens, successeurs des premiers passionnés ;
- les curieux ;
- les psychopathes ;
- les militants mus par idéologie ou religion (qui sont d'ailleurs souvent à cheval entre amateurisme et professionnalisme).

Lorsqu'on essaie de déterminer l'appartenance d'un délinquant à un de ces types, une bonne

> “Internet permet à des communautés virtuelles clandestines de se constituer autour de pratiques rigoureusement punies par la loi”

> “Il est relativement aisé de se procurer sur l'internet des recettes pour la fabrication d'explosifs”

➲ Infractions prévues par le nouveau code pénal français

➲ Crimes et délits contre les personnes

Atteinte à la personnalité

- Atteinte à la vie privée (226-1 ; 226-2)
- Atteinte à la représentation de la personne (226-8)
- Dénonciations calomnieuses (226-10)
- Atteinte au secret professionnel (226-13)
- Atteinte aux droits de la personne résultant de traitements de fichiers informatiques (226-16 à 226-24 loi du 6 janvier 1978 "informatique et liberté")

Atteinte aux mineurs

- Diffusion de messages pornographiques susceptibles d'être vus par un mineur, etc.(227-23 ; 227-24 ; 227-28)

➲ Crimes et délits contre les biens

- Escroquerie (313-1 et suivants)
- Atteinte aux systèmes informatiques (323-1 à 323-7 loi du 7 janvier 1988 sur la fraude informatique).

➲ Infraction au code de la propriété intellectuelle

- Contrefaçon d'une œuvre de l'esprit (y compris logiciel) (335-2 et 335-3)
- Contrefaçon d'un dessin ou d'un modèle (521-4)
- Contrefaçon de marque (716-9 et suivants)

➲ Infraction aux dispositions concernant le chiffrement

- Article 28, loi du 29 décembre 1990
- Article 17, loi du 26 juillet 1996

➲ Infraction de Presse, loi du 29 juillet 1881 modifiée

- Provocation aux crimes et délits (art. 23 et 24)
- Apologie des crimes contre l'humanité (art.24)
- Apologie et provocation au terrorisme (art.24)
- Provocation à la haine raciale (art.24)
- "Négationisme" : contestation des crimes contre l'humanité (art.24 bis)
- Diffamation (art.30 ; 31 ; 32)
- Injure (art.33)

➲ Participation à la tenue d'une maison de jeux de hasard ("cyber-casino")

- Article 1, loi du 12 juillet 1983 modifiée par la loi du 16 décembre 1992

méthode consiste à croiser le niveau de technicité de l'attaque, évalué par le biais de sa signature, avec la motivation supposée du pirate.

Cinq motivations fondamentales

On identifie généralement cinq motivations principales, fondées sur des composantes d'ordre social, technique, politique, financière ou étatique.

La motivation sociale trouve ses racines dans le besoin de reconnaissance par ses pairs. Il veut prouver sa valeur à ses compagnons en se référant aux critères culturels internes à ce groupe. Il s'agit d'un phénomène analogue à celui des "taggers", et qui est relié à une vision très primaire des rapports sociaux. On le retrouve fréquemment chez les personnes immatures pour lesquels le "hacking" apporte un sentiment de supériorité et de revanche sur des institutions qu'ils subissent dans leur quotidien.

> « La motivation financière peut susciter des "vocations" de criminel en col blanc sur l'internet »

La motivation technique reste rare. Elle a pour objet premier la recherche des limites de la technologie afin d'en mettre en lumière les limites et les faiblesses et d'en mieux comprendre les atouts.

Les motivations politique ou religieuse, dans leurs variétés les plus "douces", incitent les cybercriminels à créer des événement propres à alerter les médias pour les focaliser sur un problème grave, en espérant provoquer une prise de conscience collective qui amènera sa résolution . Mais elles peuvent conduire au terrorisme et à des actes de guerre.

La motivation financière peut s'avérer très forte et susciter des "vocations" de criminel en col blanc sur l'internet.

Enfin, on peut distinguer une motivation nationale ou gouvernementale. Qu'il s'agisse de guerre de

l'information ou d'espionnage, elle concerne des services agissant pour le compte de puissances étatiques.

Concilier contrôle policier et liberté

Les délinquants ont su s'adapter aux nouvelles technologies pour faire fructifier leurs activités traditionnelles. On peut légitimement s'inquiéter en voyant à quel point ils peuvent être créatifs lorsqu'il s'agit d'inventer de nouveaux usages pour ces technologies. Les organisations criminelles n'ont pas attendu que l'Europe et les USA se mettent d'accord sur les futures normes en matière de téléphonie mobile pour adopter largement le téléphone mobile.

Force est de constater qu'il serait dangereux de laisser les forces de police prendre un retard dans le domaine technologique, quand on sait que le rattrapage aura non seulement un coût financier direct (sous forme d'investissements dans de nouvelles infrastructures) mais aussi et surtout un coût social par l'accroissement de l'emprise des structures mafieuses ou terroristes sur la société, avec tous les risques que cela comporte.

Toutefois, un accroissement excessif de la "présence policière" sur le réseau ne serait pas non plus forcément la meilleure des choses et pourrait entrer en conflit avec les besoins de confidentialité des échanges et de respect de la sphère privée des individus.

Solange Ghernaouti-Hélie et Bertrand Lathoud

Revue d'auteurs, l'Informatique Professionnelle accueille des opinions qui n'engagent pas la rédaction.

> “Un accroissement excessif de la “présence policière” sur le réseau ne serait pas non plus forcément la meilleure des choses”

Bibliographie

Solange Ghernaouti-Hélie, Sécurité internet – Stratégies et technologies, Dunod, 2000.

J. Scambray, S. McClure, G. Kurtz, Hacking Exposed, Network Security Secrets & Solution, Mac Graw Hill.

Anonymous, Maximum Security, a Hacker's Guide to Protecting Your Internet Site and Network, SAMS Publishing.