

Nicolas Clémot

Cybercrime et entreprise

Avec l'essor des nouvelles technologies s'est développée une nouvelle forme de criminalité : la cybercriminalité. Commençons d'abord par la définir: *la cybercriminalité, c'est l'ensemble des infractions pénales qui se commettent sur le réseau Internet*¹. Cette dernière touche les particuliers mais également les entreprises (et c'est ce dont je traiterai ici). Je ne parlerai donc pas de la pédophilie (qui fait partie de la cybercriminalité), d'incitation à la haine sur internet ou de propos xénophobes car ils ne touchent pas l'entreprise directement.

Dans un premier temps, nous verrons les différents acteurs criminels qui la composent, les techniques que les criminels utilisent, l'impact qu'elle peut avoir et enfin quelles sont les solutions de management possibles.

1/ Les acteurs criminels

Les acteurs criminels de la cybercriminalité peuvent se diviser en plusieurs catégories. Tout d'abord, les particuliers.

A) Les particuliers

Je ne parlerai pas ici du grand public, qui a malgré tout un impact fort (bien que ceci puisse être relativisé) sur l'entreprise (notamment sur les industries du jeu vidéo, de la musique, du cinéma et des logiciels) via le piratage (copie de cds...).

Nous allons commencer par parler de ce que les médias appellent communément (et souvent à tort) les hackers (ou *pirates* en français), mais qui désigne en fait un virtuose de l'informatique (et non pas forcément un cybercriminel); on peut les diviser en plusieurs types:

*"Curious Joe"*² (ce sont des personnes qui sont très curieuses de leur art et en connaissent assez pour faire des dégâts. Leurs vecteurs d'apprentissage ont été Telnet³, les sites FTP⁴. Ces "Curious Joe" veulent tester leurs trouvailles et leurs outils sans intention foncièrement mauvaise. Souvent par leur inexpérience ils sont involontairement néfastes).

*"Script Kiddies"*⁵ (par le biais de sites comme astalavista.box.sk entre autres, on trouve de nombreux programmes de hacks prêts à l'emploi. Ces personnes ont pour seul objectif d'essayer de nuire avec ces programmes tout prêts car cela leur donne un sentiment de puissance incomparable par rapport au temps qu'ils mettent pour nuire (rapport effort/plaisir très favorable). Ils sont très méprisés par les "vrais" hackers).

*"Wannabes"*⁶ (ce sont les nouvelles forces du hacking. Ces personnes ont une véritable ambition de recherche de la connaissance dans le milieu du hacking. Ils souhaitent devenir des Elites. Ils pratiquent souvent l'amélioration de scripts de hacks déjà existants; une fois que ces wannabes développent leurs propres scripts, ils deviennent des élites).

*"Elites"*⁷ on les divise en trois catégories:

_ Les White Hats (hackers): *ce sont des consultants en sécurité, les administrateurs réseaux, voire les cyber-policiers. Ils ont un grand sens de l'éthique et de la déontologie. Ce qu'ils aiment dans le hacking est un subtil mélange de défi, de jeu, de fierté et d'argent.*

1

Source: http://www.interieur.gouv.fr/sections/a_votre_service/votre_securite/internet/cybercriminalite/view

2, 5, 6, 7 Source: <http://cybercrime.ifrance.com>

³ Telnet (TErminaL NETwork ou TELecommunication NETwork, ou encore TELetype NETwork) est un protocole réseau utilisé sur tout réseau supportant le protocole TCP/IP. (Source: wikipedia)

⁴ Le File Transfer Protocol (*protocole de transfert de fichiers*), ou FTP, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. (Source: wikipedia)

_ Les Black Hats (hackers): *ce sont eux les véritables nuisances de la famille des hackers. Ce sont eux les cybercriminels: créateurs de virus, cyber espions, cyber terroristes et cyber escrocs.*

_ Les Grey Hats (hackers): *ils ont une position un peu intermédiaire entre les deux catégories précédentes. Ils ne rechignent pas à pénétrer dans des systèmes mais ne veulent pas tout mettre sens dessus dessous.*

Chaque type de hackers a une (ou plusieurs) spécialité(s): phreaker, cracker, cypher punk... mais je détaillerai plus ces spécialités dans la partie sur les techniques utilisées par les cybercriminels.

Quelques cybercriminels célèbres: John Drape (inventeur du phreaking), Kevin Mitnick (le premier hacker à faire partie de la liste des individus les plus recherchés du FBI; sa spécialité était l'intrusion dans les systèmes informatiques), Kevin Poulsen (piratage de systèmes gouvernementaux et militaires)....

B) Les groupes

Les hackers forment une grande famille (voire une communauté) aux motivations très différentes; elle se veut (et est en théorie) élitiste, underground et fermée. Beaucoup d'entre eux n'ont pas d'intentions néfastes et sont plus à la recherche de "l'exploit" que de saboter/détourner/détruire/voler des données mais toute intrusion sur un système (même sans conséquence) est punie légalement et suffit pour être considéré comme un cybercriminel. Une partie des hackers n'a pas "l'impression" de faire du mal (même s'ils savent que leur activité est pénalement répréhensible) et se sent investie d'une "juste mission" en rétablissant la balance entre les industriels qui profitent des consommateurs et les particuliers (on pourrait faire une quasi analogie avec certaines idées du communisme)... mais aussi, pour protéger Internet des Etats qui veulent faire main basse dessus (en somme, une lutte "Cyberpirates contre Big Brother"). C'est en cela, et parce que leur motivation n'est pas le profit et que leur but est idéologique, qu'on peut les rapprocher du terrorisme (même si leurs modes d'actions sont différents (pas de destruction, par exemple)). On parle même d'"hacktivisme".

a) Le warez

Les hackers aiment se retrouver (notamment sur des forums) et partager leurs connaissances (ou se "vanter" de leurs divers exploits). Une partie non négligeable de la cybercriminalité réside dans le warez*¹ et dans ce qu'on appelle la scène*² (la scène warez) (cette notion est aussi présente pour le hacking mais dans une proportion moindre).

Les groupes, comme ceux qui les utilisent, ont développé un langage bien spécifique (*leecher, appz, fxp, release, 0-days, release, rip, proper, retail...* malheureusement celui-ci est bien trop étendu pour que j'en explique toutes les définitions). Les grands groupes de pirates hackent les données (parfois avant même leur sortie dans le commerce) mais ne s'occupent pas de leur "distribution". Pour ceci, il y a ce les "board(z)"*³; il en existe plusieurs milliers et cela assure une distribution exponentielle. A cela il faut ajouter les protocoles P2P*⁴ (comme émule ou

¹ Le terme warez désigne des contenus numériques protégés par les lois du copyright mais diffusés sans reversement de droits. (Source: [wikipedia](#))

² La scène warez est l'ensemble des groupes piratant et mettant à disposition aux utilisateurs les fichiers piratés (on trouve une scène par pays).

³ Les boards sont des forums dont les membres mettent les versions pirates sur internet à disposition des autres membres.

⁴ Peer to peer; littéralement, pair à pair. Protocole permettant l'échange de fichiers via internet entre plusieurs utilisateurs et ceux de façon simultané.

bittorent) voire les newsgroups.

Voici quelques grands groupes de warez: DrinkOrDie, PARADOX, DEViANCE, HATRED, CLASS, Fairlight, MYTH, Razor 1911, ECHELON, MOJITO, RELOADED, KALISTO....

Pour revenir au fait que certains groupes pouvaient être assimilés au terrorisme; on peut le remarquer déjà dans les noms des groupes (avec l'exemple de Fairlight (*littéralement: lumière de justice/d'honnêteté*)) mais aussi dans leur NFO*¹ (exemple avec le groupe HATRED qui condamne fermement la vente de fichiers warez ou le groupe DEViANCE qui incite les gens à acheter les jeux (comme eux le font)). On retrouve ici la motivation principale des hackers qui est avant tout la prouesse technique, le 'fun' et le plaisir à casser les protections (raisons pour laquelle les groupes de warez ne s'occupent jamais de la distribution des données et méprisent plutôt ceux qui le font).

Ces groupes, bien qu'illégaux, ne font pas partie d'organisations criminelles telles que les mafias ou du crime organisé et ne tirent aucun profit financier de leurs actions (seulement un bénéfice 'moral': la gloire de l'avoir fait (et encore plus si le groupe est le premier à avoir réussi), l'exploit technique (défi personnel) et la reconnaissance des pairs (des autres hackers)).

b) Le reste des hackers

Une autre des notions-clés du hacking, c'est celle de la liberté (aucune entrave à la circulation des informations et à la connaissance: la communauté partage et communique) ainsi que celle de l'underground (le hacking est une communauté d'élites ainsi qu'un monde caché et fermé). Les blackhats (les plus dangereux des cybercriminels) ne sont pas appréciés par le reste des hackers. Parfois nihilistes, souvent anti-capitalistes, la grande majorité des hackers restent inoffensifs (seul l'utilisation de ce qu'ils découvrent et de ce qu'ils font est dangereux; eux-mêmes ne les utilisant pas, seul le plaisir de la découverte et du partage comptent).

Les hackers ont leurs conventions: la DEF CON (la plus célèbre des conventions; a lieu tous les ans à Las Vegas depuis 1983), le Chaos Communication Congress (organisé par le CCC (Chaos Computer Club)) et ayant lieu depuis 1984 à chaque fin d'année en Allemagne)... ainsi que leur magazine 'officiel' (le très célèbre: Phrack*²).

Quelques groupes de hackers célèbres: le CCC, cDc (Cult of the Dead Cow)... Cependant ces groupes ne sont connus que parce que ce sont des greyhats; la scène étant un endroit très secret, il est quasi impossible de savoir quels sont les groupes de blackhats actifs et leurs actions; ces derniers ne cherchent pas à se faire connaître et veulent rester dans l'ombre et l'anonymat le plus total. Ils agissent soit pour leur compte personnel soit pour celui d'organisations criminelles.

Plus anecdotique, il existe par exemple en Suède, un parti pirate officiel*³ qui a quand même réussi à réunir près de 35000 voix lors d'une élection nationale ainsi qu'un parti pirate français*⁴ (mais qui lui est tout récent et très petit).

Même si les groupes warez font perdre (indirectement) de l'argent aux industriels, même si les découvertes des hackers en général sont (potentiellement) dangereuses quand elles se

¹ Un fichier NFO est fourni avec chaque release (sortie) pour promouvoir le groupe et fournir des informations générales tel que le format, la source, la taille des fichiers, et toutes les notes qui peuvent être utiles. (Source: wikipedia)

² <http://www.phrack.org/> ou pour une traduction non officielle: <http://arsouyes.org/info/phrack.html>

³ [Http://www2.piratpartiet.se/international/english](http://www2.piratpartiet.se/international/english)

⁴ [Http://parti-pirate.fr/](http://parti-pirate.fr/)

retrouvent entre des mains malintentionnées, il n'y a qu'une partie infime (mais dont on parle le plus) de la scène hacking qui est vraiment dangereuse pour l'entreprise: celle des blackhats!

2/ Les techniques utilisées par les cybercriminels

Je traiterai cette partie à travers trois angles, celui des spécialités des blackhats, leurs techniques et les différentes applications qu'ils utilisent.

A) Les différentes spécialités

J'en avais brièvement parlé dans la partie précédente, mais c'est ici que je développerai plus en profondeur les différentes spécialités usitées par les hackers et plus précisément, par les blackhats (c'est pourquoi j'utiliserai dorénavant ce mot (ou celui de cracker) pour éviter toute confusion avec le reste des hackers).

*"Cracker"*¹ (personne qui s'applique pour les hackers criminels. Ces personnes tirent parti de leurs compétences informatiques à dessein d'en tirer un bénéfice financier ou dans le but de nuire à des individus ou à des organisations. Les crackers existent à différents niveaux: cela va de la "petite frappe" au cyber-terrorisme gouvernemental en passant par le crime organisé, la mafia russe et les cartels de drogue. Tous ces crackers représentent les soldats de la guerre de l'information. Leur nombre ne cesse de grandir étant donné la valeur de plus en plus grande des l'information dans la guerre économique).*

*"Phreaker"*² (s'applique plus particulièrement aux individus qui se sont spécialisés dans le piratage des réseaux téléphoniques et internationaux. Leur activité peut être criminelle ou non. Leur principale action est de 'rerouter' les communications téléphoniques, de faire des écoutes téléphoniques ou de couper certaines lignes du réseau. Ces compétences leur ont souvent permis d'échapper à la police, d'escroquer les opérateurs de téléphone pour s'amuser ou pour gagner de l'argent. Beaucoup de vrais hackers ont été des phreakers pour diminuer le montant de leur facture téléphonique et pour pouvoir continuer à écumer les réseaux de manière plus sereine. L'émergence d'Internet et la baisse sensible des coûts des télécommunications a remédié en grande partie à ce genre de problèmes).*

*"Cypher Punk"*³ (maîtres du cryptage/décryptage de données).*

B) Les différentes méthodes

Internet, du fait de son relatif anonymat (sentiment d'impunité) et parce qu'il permet d'agir à distance, encourage et a fait se développer des pratiques telles que le blanchiment d'argent ou les communications entre groupes terroristes. Cependant, ces pratiques ne relèvent pas directement de la cybercriminalité, c'est l'utilisation d'internet pour pratiquer des actes criminels, elles peuvent être pratiquées sans avoir de grandes connaissances informatiques, c'est pourquoi je ne les traiterai pas ici longuement et que je m'attarderai sur les actes commis par les cybercriminels (en accord avec la convention sur la cybercriminalité du Conseil de l'Europe (CETS n°185)).

Les blackhats disposent de nombreuses méthodes pour commettre leurs méfaits.

¹ , ², ³ Source: <http://cybercrime.ifrance.com>

On peut commencer par le *spam**¹ (ou pourriel); selon un article du site znet.fr, en 2006 en France, 95% des mails envoyés étaient du spam. Ceci occupe énormément de bande passante et coûte beaucoup d'argent aux fournisseurs d'accès internet et a également un coût pour l'entreprise car les gens perdent du temps à trier leurs mails et séparer les bons des mauvais. De plus, le spam est un des vecteurs principaux du *phishing**² ('hameçonnage' en français). A priori, cette arnaque ne pouvait toucher que les particuliers mais quand on sait que selon cette étude*³, les salariés passent environ 50 minutes par jour à surfer sur internet à des fins personnelles sur leur lieu de travail (et que 13% d'entre eux téléchargent des logiciels, de la musique ou des films), on se rend compte de la dangerosité du phishing qui peut servir à voler des données (bancaires notamment) de l'entreprise.

Le spam a trouvé des variantes avec le SPIT*⁴ qui permet la publicité en masse sur les téléphones mobiles. Une variante existe, cela consiste en des appels en masse sur des GSM via la technologie de téléphone par internet, la communication interromptue dès la première sonnerie (donc pas de facturation pour l'attaquant); la victime voit que quelqu'un a tenté de la joindre et parfois rappelle le numéro (qui bien sûr est surtaxé). Certains particuliers se retournent contre les opérateurs de téléphonies et cela va parfois jusqu'au procès!

Il y a également la manipulation des cours de bourses via le stock spam ou "pump and dump" qui consiste à envoyer des spams contenant des fausses informations sur des entreprises pour faire baisser ou monter leur cours en bourse et les personnes derrière ce spam en profitent en achetant ou en vendant leurs actions.

Il existe de nombreuses variantes de l'utilisation du spam.

On peut aussi noter la technique de botnet qui désigne un ensemble de machines robot ou zombies*⁵; un blackhat peut contrôler des milliers d'ordinateurs. Selon des études menées par Sophos ou Symantec (deux gros éditeurs de logiciels anti virus), en fin 2007, 22% du parc informatique américain sont des zombies et 5,4% en France. Selon Vinton Cerf (président de l'ICANN*⁶) (cité dans un article du site lemondeinformatique.fr), près d'un quart du parc machine mondial connecté à internet (soit environ 600 millions d'ordinateurs) sont des zombies. Ceci permet de commettre des délits comme le vol de données bancaires et identitaires à grande échelle (via le spam et le phishing comme vu précédemment) ou de faire des attaques de type DoS*⁷. Depuis plusieurs années, ce type d'attaques sert à des fins de chantage et tentative d'extorsion auprès d'entreprises dont l'activité commerciale repose sur la disponibilité de leur site Web (bien souvent, ce n'est pas le fait de pirates isolés mais de groupes de blackhats au service d'organisations criminelles).

Petit aparté sur le blanchiment d'argent, qui se fait de plus en plus par internet, souvent via des "mules" (comme pour la drogue) plus ou moins au courant de la légalité de leurs agissements (certaines sociétés jouent sur la bonne foi et la méconnaissance de la loi des gens

³ ¹ Le spam désigne une communication électronique, notamment du courrier électronique, non sollicitée par les destinataires, expédiée en masse à des fins publicitaires ou malhonnêtes. (Source: wikipedia)

² Technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. L'hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques. (Source: wikipedia)

³ Source: <http://www.lentreprise.com/3/1/3/article/14294.html>

⁴ SPam over Internet Telephony: cela désigne la publicité indésirable faite via les réseaux de communication téléphonique sur IP.

⁵ Une machine zombie est un ordinateur contrôlé à l'insu de son utilisateur par un pirate informatique. Ce dernier l'utilise alors le plus souvent à des fins malveillantes, par exemple afin d'attaquer d'autres machines en dissimulant sa véritable identité. (Source: wikipedia)

⁶ Internet Corporation for Assigned Names and Numbers (ICANN) est l'autorité de régulation de l'Internet.

⁷ Le déni de service ou *Denial of Service* (DoS) est, d'une manière générale, l'attaque qui vise à rendre une application informatique incapable de répondre aux requêtes de ses utilisateurs en la submergeant de requêtes inutiles soit pour la ralentir ou pour la rendre inutilisable. (Source: wikipedia)

et leurs proposent un travail avec contrat... mais qui leur fait faire du blanchiment d'argent). Ce business est très pratiqué par les mafias.

Pour parler aussi des cas particuliers, on peut évoquer celui du piratage des cartes pour pouvoir accéder au contenu proposé sur satellites gratuitement, ou la commande de produits de contrefaçon à l'étranger (ou de produits légaux mais sans payer la T.V.A), la pose de puces sur des consoles pour lire les jeux piratés, le désimlockage de gsm... tous ces comportements et actions impactent directement l'entreprise mais on ne peut pas vraiment parler de cybercriminalité ici; on parlera donc plus de cyberdéviance*¹.

Et enfin, pour clore cette partie, la plus efficace et une des plus dangereuse des méthodes utilisées par les cybercriminels (et qui n'est pas purement informatique), c'est l'ingénierie sociale*². C'est le célèbre Kevin Mitnick qui a popularisé et théorisé cette méthode et qui pourra fonctionner quelque soit le niveau de sécurité d'un système.

C) Les différentes applications

Les blackhats utilisent divers applications pour arriver à leurs fins. Pour ceci ils utilisent des logiciels malveillants (*malware*); ce sont des logiciels développés dans le but de nuire à un système informatique. Parce que les virus ont été historiquement les premiers à apparaître, le terme "virus" est souvent employé abusivement, spécialement par les mdia, pour désigner toutes sortes de logiciels malveillants*³.

Tout d'abord avec les virus informatiques, ce sont des programmes informatiques écrits dans le but de se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés "hôtes". Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme l'internet, mais aussi les disquettes, les cédéroms, les clefs USB, etc. En fait, le virus comporte un en-tête de programmation qui s'incruste dans les applications que vous utilisez et dès que vous démarrez ces derniers, en fait vous démarrez le virus qui lui-même lance votre application... tout ça de façon complètement transparente. A partir de là, il peut commencer à se multiplier et à infecter d'autres programmes*⁴.

Quelques virus connus: Cabir, MyDoom. A, Yamanner ou Tchernobyl.

Il y a aussi les vers (*worms*); c'est le malware des réseaux par excellence. C'est un programme qui s'auto-multiplie à l'infini et se déplace au travers de réseaux de tout type (Internet, Intranet, réseau local...). Ce malware, à la différence des virus, n'a pas besoin de 'support physique' pour se déplacer; pour se propager, il peut utiliser les adresses du carnet du pc et se reproduire en se dupliquant pour chaque destinataire. Mais le véritable but de tels programmes peut aller au delà du simple fait de se multiplier: espionner, offrir un point d'accès caché, détruire des données, faire des dégâts, transformer la machine en zombie.... En raison de leur structure, ils peuvent être intégrés via un script dans une page internet ou dans un mail.

⁴ ¹ Théorie donnée par Franck Franchin, auteur d'un livre sur le business de la cybercriminalité

² L'ingénierie sociale (social engineering en anglais) est la discipline consistant à obtenir quelque chose (un bien ou une information) en exploitant la confiance mais parfois également l'ignorance ou la crédulité de tierces personnes. Il s'agira pour les personnes usant de ces méthodes d'exploiter le facteur humain, qui peut être considéré comme le maillon faible de tout système de sécurité. (Source: [wikipedia](#))

^{3,4} Source: [wikipedia](#)

Les vers les plus connus sont: Bagle, Blaster, Code Red, I love you, Melissa, Nimda, Sasser ou Sobig....

On trouve aussi les enregistreurs de frappe (ou *keylogger*); ils ont la particularité d'enregistrer les touches frappées sur le clavier sous certaines conditions et de les transmettre via les réseaux. Par exemple, certains enregistreur de frappe analysent les sites visités et enregistrent les codes secrets et mots de passe lors de la saisie. Certains keyloggers sont mêmes capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur*¹! Ils sont donc très utiles pour n'importe quel pirate.

Un cheval de Troie (*trojan* en anglais) est un type de logiciel malveillant, c'est-à-dire un logiciel d'apparence légitime, mais conçu pour subrepticement exécuter des actions nuisibles à l'utilisateur ; un cheval de Troie, dans un programme, tente d'utiliser les droits appartenant à son environnement d'appel pour détourner, diffuser ou détruire des informations*².

Il existe une forme de trojan appelée porte dérobée (*backdoor*), c'est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel. Elle permet à un utilisateur de s'introduire à nouveau au cœur de la machine sans pour autant exploiter une nouvelle fois la faille avec laquelle il a pu obtenir l'accès initial, qui serait tôt ou tard comblée. Grâce à ceci, on peut contrôler un pc à distance tant que celui-ci est connecté à internet. Les portes dérobées n'ont pas forcément un usage illégal, on peut l'utiliser par exemple pour contrôler son propre ordinateur à distance, ou pour une entreprise voulant effectuer une action de maintenance à distance sur la machine d'un de ses clients... c'est selon l'utilisation faite de la porte dérobée qu'on la qualifie de trojan ou non. Back Orifice (jeu de mot un peu grivois avec le programme de Microsoft, Back Office), programmé par le groupe Culte of the Dead Cow (cDc) est sûrement la backdoor la plus connue.

En sus des backdoors, il existe les rootkits: ce sont des programmes qui ne s'utilisent qu'après l'installation d'une backdoor (donc sur une machine déjà "infectée") et qui servent à camoufler tous les changements effectués lors de l'intrusion

Les logiciel espions (*spyware*) sont des logiciels malveillants qui s'installent dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur n'en ait connaissance*³. Un spyware peut télécharger un virus, installer un trojan ou faire office de keylogger... mais généralement, leur fonction est plutôt d'"espionner" les sites internet visités par l'utilisateur, les programmes exécutés (et à quelle heure)... tout cela dans un but de profilage par des sociétés peu scrupuleuses de publicité ciblée sur internet.

Les spywares connus sont: Gator, DirectRevenue, Cydoor, Bonzi Buddy....

Et enfin, les bombes logiques qui peuvent être intégrées dans un virus ou un troyen; c'est un dispositif programmé dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel autre appel au système. L'exemple typique est le virus Tchernobyl qui ne s'active que le 26 avril (*date de l'anniversaire de l'explosion de la centrale nucléaire de Tchernobyl qui a eu lieu le 26 avril 1986*)*⁴.

Donc, après avoir vu les techniques utilisées par les blackhats, nous allons maintenant voir quels peuvent être les impacts sur l'entreprise. On sait actuellement qu'une machine avec un Windows nouvellement installé et qui se connecte sans protection à internet, est piratée en moins de vingt minutes sans même surfer sur internet (les blackhats font des attaques sur des ports de Windows qui sont ouverts et utilisent des failles critiques*¹).

3/ Les impacts sur l'entreprise de la cybercriminalité

En 2001, une enquête menée par le Conseil de l'Europe dans les milieux d'affaires aux Etats-Unis a révélé que 85% des entreprises sondées avaient été victimes d'actes de piratages et que cette même année, le manque à gagner pour les industries victimes de la contrefaçon s'élevaient à 250 milliards de dollars par an, soit près de 5% des échanges mondiaux.

Selon une récente étude menée par IBM auprès de 3000 entreprises dans le monde (dont 150 en France), les deux sources de coûts les plus importantes dues aux cyber-attaques sont la diminution du chiffre d'affaires (79% en France et 72% pour la moyenne des autres pays) et la perte de clients (60% et 67%). Deux tiers des sondés sont persuadés que les menaces sécuritaires proviennent essentiellement de l'intérieur de l'entreprise (54% en France).

Selon le rapport (en 2006) du bureau fédéral d'investigation américain (FBI), le cybercrime coûte au marché américain 67,2 milliards de dollars par an. 98,2 % des entreprises étudiées ont répondu utiliser un antivirus, 90,7 % un pare-feu, et environ 75 % un anti-malware. 84 % des entreprises interrogées ont souffert de virus, 80 % de spywares, et 32,9 % de tentatives d'intrusion réseau.*²

Selon une enquête annuelle en 2006 du Computer Security Institute faite sur plus de 600 hauts dirigeants et cadres d'entreprises de toutes tailles et de tous les secteurs de l'économie américaine, 34% des personnes interrogées affirment que leur entreprise alloue plus de 5% de leur budget informatique à la sécurité. Les principales causes des pertes sont, dans l'ordre, les virus (15,7 millions de dollars), l'accès non autorisé à l'information (10,6 millions de dollars), le vol d'ordinateur portable ou d'appareils mobiles (6,6 millions de dollars) et le vol de propriété intellectuelle (6 millions de dollars).*³

Selon un rapport très récent qui porte sur 180 pays fait par Symantec*⁴ (*données à cependant relativiser, les éditeurs d'antivirus ayant la mauvaise habitude de gonfler des chiffres pour créer une certaine peur et pousser les gens à acheter leurs programmes... cependant leur analyse reste assez pertinente*) sur le premier semestre de l'année 2007, montre que la cybercriminalité se "professionnalise" et que les cybercriminels sont des groupes organisés à travers le monde qui s'attachent à déployer des attaques en ligne ciblées, élaborées et rentables.

On trouve des kits quasi *plug and play* en vente sur internet (pour le phishing par exemple, cela coûte entre 25 et 75 euros) ainsi que des informations volées (c'est une sorte de marché noir). Avec par exemple: des cartes de crédit (22 %; de 0,35 à 3,62 euros), des comptes

¹ Une faille critique est caractérisée par les risques élevés qu'elle fait peser sur un système vulnérable. D'une manière générale, une faille critique est exploitable à distance et permet l'exécution arbitraire de commandes sur le système attaqué.

² Source: <http://www.pcimpact.com>

³ Source: <http://www.gocsi.com/>

⁴ Le plus gros des éditeurs d'antivirus et qui édite Norton

bancaires (21 %; 22 à 290 euros), des mots de passe de courriers électroniques (8 %; 0,73 à 254 euros), des numéros de sécurité sociale (3 %; 3,6 à 5 euros), des identités complètes (6 %; 7,3 à 108 euros)... Ce type de site continue d'augmenter et les prix de baisser.

Toujours selon ce même rapport, dans l'espace de ces 6 mois, ce sont plus de 210 000 nouveaux programmes malveillants qui ont été détectés (c'est une hausse de 185% par rapport au semestre précédent et de 318% sur 1 an), ce qui porte leur nombre à 622 500. Les chevaux de Troie sont de plus en plus utilisés (54%, hausse de 9% par rapport au semestre précédent) car ils sont plus discrets (et donc moins facilement détectables) que les vers et les virus. Les secteurs les plus concernés par les fuites de données dues au piratage sont les agences gouvernementales (26%), la santé (15%), les finances (14%), la vente au détail (6% mais représentent 85% des identités exposées) et les causes des identités exposées sont à 76% dues au hacking.*¹

En plus de ces données "vérifiables", le cybercrime permet aussi de faire de l'espionnage industriel (donc difficilement décelable et quantifiable): il est fait soit par une entreprise pour espionner son concurrent ou soit par une organisation criminelle qui fait du chantage en menaçant de revendre ses secrets (ou qui les vend directement sans en avertir "l'intéressé"). L'espionnage peut se faire de deux façons différentes, l'espionnage de l'ordinateur ou par des écoutes téléphoniques (rendues très accessibles avec les nouvelles technologies). On peut aussi noter la manipulation des cours de bourses qui peuvent faire chuter le cours d'actions grâce à des malversations ou des fausses rumeurs via du spam.

Les études menées sur la cybercriminalité montrent qu'elle vient parfois d'un élément de l'entreprise (en effet, "le travail" pour un cybercriminel est beaucoup plus aisé de l'aide de l'intérieur). Les attaques cybercriminelles sont soit l'œuvre d'une personne agissant seule dans l'entreprise, soit par un groupe criminel utilisant un des travailleurs (soit le salarié a lui-même contacté un groupe criminel (soit par peur de se faire prendre ou parce qu'il n'a pas lui-même les compétences pour commettre le méfait), soit le groupe criminel a repéré une personne et là, deux moyens, soit on assiste à des pressions (chantage, piratage de comptes...), soit c'est l'appât du gain qui motive le salarié)). Ce type de problème arrive majoritairement dans les établissements financiers.

Pour conclure, la cybercriminalité a de fortes répercussions sur l'entreprise; déjà à travers les nombreux coûts qu'elle engendre (directs et indirects) mais aussi, elle fait changer les comportements des salariés et oblige à la prudence. Son impact n'est pas toujours visible et une grande partie de la cybercriminalité n'est pas révélée au grand jour (espionnage par exemple). Il est difficile de lutter contre car elle se professionnalise et devient de plus en plus élaborée.

4/ Les solutions de management possible

La cybercriminalité fut longtemps niée ou minimisée mais depuis près de 4 ans, on commence à en parler et à mettre en place des techniques pour lutter contre elle.

Je différencierai ici la cybercriminalité ayant cours à la contrefaçon ou le vol de la propriété intellectuelle, de celle qui touche le reste des activités.

¹

Source: http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20070917_01

A) Lutter contre la contrefaçon et contre le vol de propriété intellectuelle

Le vol de propriété intellectuelle est actuellement au centre de tous les débats et cristallise les avis. Le choix du gouvernement s'est porté sur une législation basée sur la répression à travers la loi DADVSI*¹ et la mission Olivennes (qui a donné la loi de lutte contre la contrefaçon).

Ces lois ont été très mal accueillies par les consommateurs; concernant la loi de lutte contre la contrefaçon, c'est la transposition de la directive du 29 avril 2004 sur le respect des droits de la propriété intellectuelle et qui veut unifier la lutte contre la contrefaçon à l'échelle européenne. Cependant, le rapporteur de cette directive, est l'eurodéputé Mme Janelly Fourtou (épouse de J-R Fourtou, président du conseil de surveillance de Vivendi Universal). Avec la loi DADVSI, les majors ont les pleins pouvoirs et beaucoup ont dénoncé l'influence trop prononcée des lobbies de l'industrie du disque. De plus, certaines dispositions sont aberrantes car les ayants-droits sont à la fois enquêteur, huissier et partie civile; de plus ils bénéficient d'outils "utiles" via des mesures dites conservatoires... etc.

Pour finir, certains décrets sont impossibles (techniquement) à mettre en place (comme le filtrage d'internet), d'autres sont complètement inadaptés à la réalité d'internet et seront donc difficiles à mettre en place; cela montre bien la volonté de l'état de contrôler et de faire main basse sur internet... et renforce donc le côté idéologique du warez qui se veut pour la défense du consommateur contre le législateur (et jouit donc d'une grande popularité... phénomène de "Robin des Bois").

Les majors ont essayé de mettre en place la vente de musique en ligne mais avec prix prohibitifs (le cd téléchargé revient presque aussi cher qu'un vrai acheté) et contient des DRM (*Digital Right Management*) qui limite sa lecture (parfois même demande à se connecter sur internet pour autoriser la lecture) et qui empêche d'être lu sur certains lecteurs mp3. Ces offres n'ont eu, bien sûr, aucun succès et ce n'est que depuis peu, qu'on voit la levée de ces drm et une légère baisse des prix. Pour la vidéo, les majors ont mis en place la VOD (*Video On Demand*) mais avec des prix toujours prohibitifs, un catalogue de choix de films réduit, des rapatriements très longs, des problèmes de lecture des films et une durée de conservation très limitée... et bien évidemment, le succès ne s'est pas fait sentir.

L'industrie de la musique et des films est donc très mal vue: des prix prohibitifs, des artistes qui font de la musique ou des films souvent de piètre qualité et qui croulent sous l'argent et des majors qui prennent les consommateurs pour des vaches à lait. De plus, aucune étude sérieuse n'a prouvé l'impact négatif du téléchargement illégal de musiques ou de films sur les ventes de cds ou de dvds (les quelques études en faveur des majors étaient financées par les majors elles-mêmes et donc n'ont eu aucune crédibilité).

Une solution de management possible pourrait être une baisse des prix, une levée totale des DRMs et un catalogue plus fourni (les premiers tests faits dans ce sens ont du succès).

En ce qui concerne les jeux vidéos, des prix trop élevés pour des durées de vie trop limitées, des jeux souvent remplis de bugs et pas encore terminés ainsi qu'un manque d'originalité ont poussé de nombreux utilisateurs vers le téléchargement illégal. Les majors du secteur ont essayé diverses mesures telles que les clés d'activation, la mise en place de logiciels d'authentification (qui ralentissent les jeux et pénalisent les "bons acheteurs"), l'activation sur internet... mais tout a été facilement contourné par les hackers.

Ici aussi, une baisse des coûts pourrait être envisagée (qui passerait peut être par un

changement de mode de distribution ou par de la publicité dans les jeux (idées en cours dans certains jeux)).

Pour les logiciels, le constat est à peu près similaire à celui du jeu vidéo: trop cher, trop de bugs, peu d'originalité... Là aussi des méthodes pour contrecarrer le piratage ont été mises en place sans grand succès. C'est aussi la baisse des coûts qui pourrait être envisagée ou des offres spécialement pour les étudiants (qui sont ceux qui piratent le plus); Microsoft l'a mis en place pour son logiciel Office et cela fonctionne très bien. Une autre alternative est de se tourner vers le monde du logiciel libre (notamment Linux) qui peu à peu, s'impose dans de plus en plus de domaines.

En sus de lutter au niveau du consommateur contre le vol de la propriété intellectuelle, le législateur associé aux majors a tenté de s'en prendre directement aux pirates eux-mêmes via plusieurs opérations (à portée mondiale et souvent organisées par le FBI) visant à démanteler des réseaux entiers (opération Buccaneer en décembre 2001, opération Fast Link en avril 2004, opération Site Down en juin 2005...). Ces opérations ont certes permis d'arrêter de nombreux pirates... mais force est de constater qu'ils ont été vite remplacés et que la scène warez s'est plutôt bien remise de ces attaques.

Globalement, les consommateurs ont une mauvaise image des entreprises du secteur et pensent se faire exploiter... raison pour laquelle ils piratent sans vergogne (et cela a été rendu d'autant plus facile par la multiplication des offres de haut débit (avec une baisse des prix des connexions)). Si l'on ajoute à cette mauvaise image des représentants d'ayants-droits (SACEM, RIAA*¹...) utilisant parfois des méthodes de hackers pour trouver des consommateurs de biens pirates ou attaquant des sites hébergeant des contenus illégaux à partir d'attaques DoS (déni de service)... et l'on comprend mieux le rapport de force entre d'une part les majors, leurs représentants et l'Etat et de l'autre côté, les consommateurs et les groupes de pirates

Sachant l'ingéniosité des pirates qui ont réussi à contourner toutes les limitations sans trop de peine, il sera très difficile d'endiguer efficacement le vol de la propriété intellectuelle autrement qu'en faisant un business plus éthique et en adaptant les offres aux réalités du marché et du consommateur. On pourrait faire une analogie avec le comportement plus éthique que doivent adopter les pétroliers dans le delta du Niger, qui est la seule méthode pour eux de limiter efficacement les problèmes avec les populations locales.

En ce qui concerne la contrefaçon et l'achat à l'étranger, une méthode pourrait être une sensibilisation du consommateur aux risques d'acheter à l'étranger (risques pour la santé dans le cas de médicaments, risques de mauvaise qualité pour les autres produits en général). On peut aussi durcir la répression et les contrôles douaniers (mais cela reste assez difficile à mettre en place, fort coûteux et l'efficacité n'est pas du tout prouvée). C'est aussi un des effets "pervers" pour les entreprises de la mondialisation et dont les pertes sont équilibrées en quelque sorte et en partie par les économies faites par les délocalisations.

¹

RIAA: Recording Industry Association of America

B) Lutter contre la cybercriminalité

Tout d'abord, la mise en place quasi automatique d'un antivirus dans l'entreprise (mais aussi chez les particuliers pour éviter l'infection d'un fichier lorsque la personne travaille chez elle), d'un pare-feu et d'un logiciel antimalware... et surtout leurs mises à jours quotidiennes (ce que beaucoup trop d'utilisateurs oublient).

Ensuite, allouer plus de fonds pour les services de sécurité informatique qui permettront de ne pas faire d'impasse sur certains logiciels et qui permettra aussi d'engager des personnes compétentes. Ne pas oublier la formation des salariés pour reconnaître un malware et savoir s'en débarrasser. On peut aussi mettre en place le contrôle de la bande passante et du flux d'informations entrant et sortant de l'entreprise.

Certaines entreprises se sont aussi tournées vers le monde du libre qui est plus sécurisé (exemple avec Linux qui comporte beaucoup moins de failles critiques que Windows et sur qui peu de malwares fonctionnent). C'est en plus une alternative vraiment peu coûteuse (les principaux frais étant la formation des salariés à son utilisation).

L'entreprise (ainsi que le législateur) peut aussi intervenir dans les écoles pour, dès le plus jeune âge et tout au long des différentes formations des jeunes, les sensibiliser à l'informatique, aux risques qu'il comporte et comment lutter (ceci est en partie fait actuellement mais pas de façon pratique... notamment dans tout ce qui concerne la cybercriminalité).

On peut également mettre en place quelques solutions pratiques comme les claviers virtuels (le fait de ne pas taper son code avec son clavier mais de cliquer sur un clavier à l'écran) pour éviter les keyloggers, des listes noires pour le spam ainsi qu'un test de turing*¹ (via la description d'une photo, marquer le code inscrit sur une image ou la résolution d'un calcul simple...), des statistiques bayésiennes*², la demande d'empreintes digitales ou l'utilisation de machines de cryptage pour certaines opérations (cela se développe peu à peu)....

Malheureusement, l'humain restera toujours le point faible de toutes organisations (cf. ingénierie sociale); pour lutter contre les menaces qui viennent de l'intérieur, une sécurisation des machines est nécessaire et la possibilité de vérifier et d'inspecter les actions réalisées sur chaque machine (se pose alors le problème de la confidentialité et de la liberté de chacun: cela peut créer une mauvaise ambiance dans l'entreprise et ne favorise pas la confiance). Il faut aussi dans ce cas-là, prévoir des vérifications à plusieurs niveaux pour contrôler les contrôleurs. De plus, le télé-travail se développant à grand pas, on ne peut pas effectuer de contrôle à distance, ce qui limite l'impact de telles mesures.

C'est pourquoi la seule combinaison réellement efficace pour lutter contre la cybercriminalité en entreprise reste l'utilisation de programmes sûrs (comme Linux), une vérification sur les actions de chaque ordinateur (avec des garde-fous pour éviter les dérives), la mise en place de logiciels de protection mis à jour quotidiennement et surtout l'éducation de l'utilisateur pour reconnaître un malware, ne pas se faire infecter et si tel est le cas, savoir s'en débarrasser.

¹ Test inventé par le mathématicien Alan Turing qui vise à savoir si le correspondant est une machine ou pas.

² Découverte par le scientifique anglais T. Bayes et consistant en l'utilisation des expériences passées pour effectuer des prédictions.

Pour conclure ce dossier; la cybercriminalité est en pleine expansion et ce malgré les mesures prises par les entreprises. Elle semble avoir de beaux jours devant elle. Le cybercrime se professionnalise et il devient donc de plus en plus difficile de le stopper. Concernant les utilisateurs, les mentalités et les habitudes sont longues à changer (mais ils représentent un maillon essentiel dans cette lutte) et on peut espérer qu'avec la nouvelle génération qui arrive dans le monde du travail (et qui est plus familiarisée avec l'outil informatique), la cybercriminalité pourra voir son action limitée.