Club des Vigilants – Groupe de réflexion — Cumul des menaces

Bruno Kerouanton — 1er mai 2005

Cybercriminalité – Menaces liées aux systèmes d'information

Introduction

Ce petit développement n'a pas l'ambition de présenter les menaces technologiques liées aux systèmes d'information dans un futur lointain. Comme le démontre parfaitement Jacques Blamont dans son ouvrage, la loi de Moore aura fait son œuvre d'ici là, et nous sommes bien loin d'imaginer ce que l'avenir nous apportera en bien ou en mal sur le plan des systèmes d'information.

Dans une première partie, je présente quelques faits qui me semblent nécessaires à la compréhension des menaces qui nous entoureront dans un futur proche, menaces relatives aux extraordinaires développements des technologies de l'information, et à l'ingéniosité débordante de ses concepteurs et utilisateurs, bienveillants ou non.

La seconde partie tente d'ébaucher l'évolution de ces menaces, et quels seraient les axes de réflexion à envisager pour les éviter, ou du moins les rendre moins importantes.

1ère PARTIE : CONSTATS

1er CONSTAT : Démocratisation et banalisation

L'un des faits les plus marquants depuis l'avènement du nouveau millénaire est l'importante démocratisation de l'ordinateur relié à Internet dans les foyers dans les pays développés. On pourrait même parler de banalisation comme cela l'a été pour le téléphone, le réfrigérateur ou la télévision.

Cette banalisation de l'informatique présente pour la majorité des internautes des avantages considérables. Ils peuvent désormais bénéficier de liaisons de qualité à haut débit, leur permettant de rester connectés en permanence sur Internet, ont accès à un volume extraordinaire de connaissances notamment par le biais des moteurs de recherche, peuvent connaître leur heure de gloire grâce aux *blogs* et autres *wikis*.

Cependant, si la plupart des utilisateurs sont satisfaits des nouveaux services rendus par la fée Internet, tout comme l'étaient autrefois les premiers bénéficiaires de la fée électricité, il convient de leur rappeler que tout n'est pas rose, et que le danger guette non loin.

L'un de mes amis m'avait demandé conseil en début d'année, car il constatait qu'une fois connecté au réseau Internet, son ordinateur ralentissait au point de ne plus être utilisable. Un premier coup d'œil me permit de constater que celui-ci était infesté de virus et autres bestioles

antipathiques consommant un certain nombre de ressources sur son ordinateur, et ce, *malgré* les antivirus présents. Notre malheureux avait tout simplement installé et activé plusieurs antivirus, pensant bien faire. Or la plupart du temps cela entraîne des dysfonctionnements, voire inhibe carrément le mécanisme et laisse la porte ouverte aux virus et vers. Je ne pouvais pas lui en vouloir, cette contre-indication n'étant pas mentionnée chez les éditeurs d'antivirus. De plus, un logiciel de partage de fichiers *peer-to-peer* avait été installé par cet utilisateur insouciant et j'ai donc dû lui expliquer que si celui-ci permettait en effet de récupérer différents fichiers *chez les autres*, c'était également parce que lui aussi *mettait à disposition* le contenu de son disque dur aux autres. Quelle ne fut pas sa stupeur lorsque j'ai déconnecté les quelque 25 personnes en train de récupérer différents fichiers présents sur son disque dur à son insu !

En généralisant, il est en fait facile de constater dans une majorité des cas que l'utilisateur n'est pas au courant des subtilités de l'informatique en réseau, et il serait bien anormal de le blâmer, cette science étant finalement très complexe et évoluant sans cesse. Du coup les pirates et criminels en tous genres exploitent cette relative naïveté et méconnaissance de l'utilisateur pour faire subir à son ordinateur toutes sortes de traitements, sans que celui-ci ne s'en rende compte.

2ème CONSTAT : Interconnexion à outrance

La standardisation des protocoles de communication entre réseaux et d'échanges de données a également permis d'interconnecter l'ensemble des équipements susceptibles de véhiculer de l'information, et de les relier à Internet : ordinateurs fixes et portables, assistants personnels, téléphones cellulaires, et maintenant équipements ménagers et automobiles… Si cela semble ouvrir des opportunités extraordinaires tant pour les équipementiers et fournisseurs de services en ligne que pour les utilisateurs, il faut cependant prendre conscience des enjeux pour un criminel qui serait capable d'en prendre le contrôle ou de perturber un tel réseau global.

Cet engouement pour l'interconnexion de tout et n'importe quoi sans vraiment réfléchir aux conséquences m'inquiète réellement. Par exemple, malgré le manque de robustesse initial des réseaux sans fil Wi-Fi, de nombreux fournisseurs de systèmes d'alarme ont proposé des solutions de protection et de vidéosurveillance des bâtiments basés sur cette technologie. Il devient courant de constater en entreprise que les systèmes d'alarme, les enregistreurs vidéo numériques et de télésurveillance sont désormais de simples PC (maquillés par l'équipementier), et assez souvent reliés au réseau de l'entreprise voire directement au réseau Internet. Quelle imprudence !

Dès à présent, des « démonstrateurs » dont le présomptueux titre anglo-saxon est *Ethical Hacker*, proposent leurs services en ligne, pour se connecter à partir d'Internet sur *votre* système d'alarme, puis pour vous monter ce que visualisent *vos* caméras de vidéosurveillance, et même en guise de bouquet final peuvent déclencher telle ou telle alarme, ou déverrouiller des accès si tel est votre souhait. Si ces démonstrations ont le mérite d'attirer l'attention sur la menace qui pèse sur ces dirigeants de sociétés mal informés, il est indéniable que les criminels ont aussi eu vent de l'affaire, et il y a au moins eu plusieurs précédents de cambriolages (réels, pas virtuels) liés à l'utilisation d'Internet pour effectuer les repérages,

analyser les lieux et allées- venues, voire carrément pour neutraliser les systèmes d'alarme et ouvrir les bâtiments ! Méfiance donc…

Dans un autre ordre d'idées, les technologies d'interconnexion des téléphones cellulaires par le biais de protocoles radio tels que Bluetooth, ou d'ordinateurs via Wi-Fi ont entraîné les pirates en herbe puis les criminels, à mettre au point différentes attaques. Il est si fréquent de trouver un téléphone ou un ordinateur dont la connexion radio n'est pas verrouillée, que cela laisse songeur. Les termes *wardriving*, *warchalking* ou *toothing* sont désormais banalisés, tellement ces techniques permettant de prendre le contrôle de l'équipement du voisin de couloir (dans le TGV) ou de la rue d'en face sont connues et maîtrisées. Les constructeurs ont tendance à vanter les mérites de l'interconnexion, ce qui est tout à leur honneur, mais ils passent trop rapidement, voire omettent carrément de sensibiliser sur les dangers d'une interconnexion à outrance. Pire encore, pour des raisons principalement liées au maintien de la compétitivité et à la mise sur le marché avant le concurrent, ces mêmes constructeurs bâclent le travail, en allant parfois jusqu'à oublier de sécuriser ces fonctions, ou en donnant seulement au consommateur une seule illusion de sécurité.

3ème CONSTAT : L'éternelle naïveté de l'Homme

Le premier pirate informatique à avoir suscité autant d'intérêt médiatique était Kevin Mitnick. Celui-ci avait par ses exploits, réussi à s'attirer les foudres de certaines grandes sociétés américaines, puis du FBI. Son arrestation lui a valu l'interdiction d'utiliser le moindre outil de télécommunication, téléphone ou fax compris, nous verrons de suite pourquoi.

Sans pour autant détailler les techniques utilisées lors de ses sympathiques méfaits (il convient de rappeler qu'il n'agissait que par motivation personnelle, par esprit de découverte et de compétition), en général Kevin utilisait des méthodes de piratage liées aux failles informatiques, mais l'essentiel de l'opération reposait sur son aptitude à maîtriser l'art de l'ingénierie sociale.

Dans son dernier ouvrage intitulé « l'art de la supercherie », il détaille par le biais d'exemples vécus la grande fragilité des hommes, et la facilité déconcertante pour une personne malveillante de manipuler son interlocuteur pour lui faire communiquer un mot de passe, ouvrir un accès distant ou toute autre chose qui permettra au criminel d'accomplir son méfait.

Ce ne sont en tout cas pas les mafias et organisations criminelles qui auront des scrupules à utiliser les techniques d'ingénierie sociale, afin de tromper un employé voire un dirigeant pour obtenir ce dont ils ont besoin. Il y a d'ailleurs une nouvelle forme d'ingénierie sociale qui se propage sur Internet depuis peu, et qui a le mérite de combiner différentes formes de techniques d'attaque. Il s'agit du *phishing*.

Le phishing (de l'anglais *fish* : aller à la pêche…aux données !) consiste à mettre en place sur Internet un ou des sites internet imitant plus ou moins l'aspect d'un site internet de commerce électronique ou bancaire respectable. Par diverses techniques communément employées par la communauté des cybercriminels, tels que l'envoi de messages non sollicités – *spams*, le détournement des sessions web - failles XSS *cross-scripting*), les espiogiciels – *spywares*, ou bien encore les attaques et détournements des serveurs de noms de domaines DNS (phénomène s'accentuant depuis avril 2005), l'utilisateur se retrouvera sur la page du serveur

web imitant l'original, et sera invité à saisir lui-même des informations personnelles, telles que son numéro de carte bancaire ou bien ses informations de sécurité sociale.

Il est désormais prouvé que certaines entités mafieuses et criminelles, notamment originaires des pays de l'Est, récupèrent des sommes d'argent importantes par le biais de telles méthodes, soit en effectuant des virements permettant de vider le compte des victimes, soit en effectuant des achats sur Internet et en revendant les biens acquis, soit en monnayant les précieuses informations acquises qui serviront par la suite à amplifier le phénomène très inquiétant aux États-Unis lié aux usurpations d'identité.

Les responsables sécurité des plus grands organismes financiers et experts sont réellement soucieux vis-à-vis de ce phénomène, d'autant plus qu'en l'état actuel des choses il n'existe pas de parade simple pour endiguer cette menace. En effet, c'est bel et bien l'utilisateur qui envoie volontairement ses informations au pirate, de plus l'arnaque ne se fait pas sur les serveurs informatiques de la banque, mais directement sur l'ordinateur de l'utilisateur qui est bien évidemment hors de contrôle de la banque, si bien qu'au final il n'y a pas d'autre solution pour l'organisme que d'informer ses clients par le biais de courriels ou de courriers papiers pour le mettre en garde, sans grands résultats. Belle aubaine pour nos mafieux en tous genres…

4ème CONSTAT : Professionnalisation des attaquants

Parmi les nouvelles menaces liées à cette masse d'ordinateurs reliées au réseau Internet via des liaisons à haut débit, et sans grande protection, car appartenant à des particuliers ne soupçonnant rien, on constate une recrudescence des attaques informatiques utilisant des relais, ou *zombies*. Cette technique consiste tout simplement à installer à l'insu de l'utilisateur un petit programme robot sur son ordinateur relié à Internet. Cet agent est résident, mais reste à l'état inerte, en attente d'un ordre de déclenchement (pouvant venir d'Internet ou bien de facteurs autres tels qu'une date précise par exemple). Cette installation se fait en général automatiquement et de manière massive, par le biais de vers Internet ou par la messagerie.

Lorsque le cybercriminel estime que le temps est venu de lancer l'attaque, il envoie l'ordre de déclenchement à un réseau d'agents primaires qui eux-mêmes déclencheront un réseau d'agents secondaires et ainsi de suite. Cette technique d'attaque a plusieurs avantages. D'une part, les agents *zombies* installés sur un grand nombre d'ordinateurs, parfois de l'ordre de plusieurs centaines de milliers, permettent de concentrer l'attaque sur une cible en saturant totalement les réseaux intermédiaires. D'autre part, compte tenu de l'utilisation d'agents relais, il est quasiment impossible de retracer l'origine du signal, d'autant plus que les réseaux étant saturés ; aucune action autre que la coupure du réseau de la part des équipes de sécurité n'est possible.

Il est intéressant de savoir que la plupart des attaques majeures actuelles fonctionnent de cette manière, mais que le phénomène n'est pas récent (Yahoo, eBay etc. furent victimes de cela en 2000). L'évolution de ces techniques d'attaque sont désormais également liées à l'incorporation de technologies issues du monde militaire ou biologique, telles que les virus combinés, le polymorphisme, la furtivité ou bien encore les leurres. Nombre de ces agents zombies sont de plus en plus difficiles à détecter par les antivirus, utilisent des canaux cachés chiffrés pour communiquer et sont proactifs, car ils possèdent désormais des mécanismes de

désactivation ou d'inhibition des systèmes de protection et des antivirus. On voit bien qu'il ne s'agit plus vraiment de l'œuvre d'un seul étudiant passionné, mais d'équipes spécialisées.

On note également que les concepteurs de virus ont comme préoccupation la qualité de leurs vecteurs d'attaque. Il y a quelques années, les virus étaient développés de manière empirique et comportaient eux-mêmes des failles ou des erreurs enrayant parfois leur progression. Puis on vit apparaître des variantes améliorées, certains concepteurs de virus allant jusqu'à numéroter leurs créations avec des numéros de versions, améliorant au passage les fonctionnalités et faisant en sorte que la propagation en soit améliorée. Ainsi, certains agents *zombies* se basaient initialement sur l'horloge de l'ordinateur pour se déclencher. L'auteur constatant que la plupart des ordinateurs ne donnaient pas la même heure et que l'attaque n'avait alors qu'un impact faible, développa une version améliorée basée sur les horloges atomiques consultables sur Internet, ce qui eut pour effet de coordonner l'attaque avec succès.

L'un des phénomènes également marquants pour le citoyen et l'internaute est l'augmentation flagrante du nombre de messages électroniques non sollicités, appelés *spams* ou pourriels. Il est désormais possible d'obtenir des chiffres estimatifs de ce nouveau fléau. Environ 70 à 80% du trafic de messagerie en circulation sur le réseau Internet est désormais constitué de ce type de messages nuisibles, et cette tendance semble augmenter de jour en jour. Les sociétés d'édition de logiciels antispam sont actuellement en pleine effervescence et effectuent des profits records. Il est intéressant de noter que les *spammeurs* se livrent à une lutte acharnée contre ces différentes sociétés, car à chaque mise au point d'une méthode permettant de détecter puis d'éradiquer ces pourriels, ceux çi ne manquent pas d'ingéniosité pour trouver des parades et moyens de contournement permettant de leurrer les logiciels de sécurité. De plus, une symbiose s'est opérée entre les plus gros spammeurs, les pirates et créateurs de virus afin d'accroître l'efficacité de la diffusion de tels messages. Un cartel est né.

On constate dès lors une recherche d'efficacité des attaques par le biais de « partenariats » entre les cybercriminels. Ainsi, la quasi-totalité de ces pourriels sont désormais émis non pas directement par le criminel, mais par le biais d'une multitude d'agents relais installés par les méthodes décrites précédemment sur les ordinateurs d'individus insouciants… qui se plaignent que leur ordinateur ralentisse ! Il est certain que la démocratisation de l'Internet, ainsi que l'augmentation massive des débits proposés par les fournisseurs d'accès Internet aux particuliers sont une aubaine pour les criminels en tous genres.

Parmi les nombreuses applications intéressantes liées à ces fameux agents installés à l'insu des utilisateurs, on peut également citer les grilles de calcul (*Grid computing*), permettant aux cybercriminels d'utiliser les ressources de calcul de centaines de milliers d'ordinateurs pour casser des clefs de chiffrement.

Enfin, ces agents servent également assez souvent à effectuer une cartographie internet des ressources présentes, par analyse des caractéristiques des ordinateurs et équipements connectés au réseau mondial. Les données collectées sont ensuite renvoyées via des canaux furtifs chiffrés à différents niveaux de relais, puis agrégés au niveau des serveurs du cybercriminel, qui obtient ainsi une base de données topologique cybergéographique d'Internet, tout comme le ferait un moteur de recherche au niveau des pages web. Cette cartographie lui permettra ensuite d'agir tel un état-major, en positionnant ses forces à des endroits stratégiques, en connaissant les points vulnérables et les forces de l'ennemi. Il est intéressant de savoir que 1 à 2 % du trafic de données circulant sur Internet semble être lié à cette activité de collecte d'informations, et ce depuis plusieurs années.

Enfin, nombre de pays envisagent la cyberguerre non comme une fiction, mais comme une réalité. Au sein des armées, les laboratoires de recherche en cryptologie, virologie et cyberattaques existent et mènent différents travaux très intéressants en rapport notamment avec les techniques évoquées dans ce document. Les ressources en capitaux des organisations mafieuses, criminelles ou terroristes ne les laisseront probablement pas en reste, d'autant plus que la plupart des pays d'où sont issues ces organisations regorgent souvent de jeunes informaticiens « motivés et compétents ». À suivre…

5ème CONSTAT : Progrès en furtivité et anonymat

La troisième évolution dans le domaine de la cybercriminalité correspond à l'émergence d'outils et de méthodes rationalisant de manière intelligente les réseaux informatiques mondiaux, dont Internet est le plus connu. Jusqu'à présent chaque ordinateur relié au réseau mondial puisait de l'information auprès d'un serveur (messagerie, web, base de données, etc.). Le serveur était par conséquent vulnérable aux attaques, pouvait être l'objet d'une surveillance, et n'était par conséquent pas « fiable » pour les cybercriminels.

L'invention du concept « peer-to-peer » ne date certainement pas d'aujourd'hui, mais sa démocratisation par l'utilisation de logiciels simples à mettre en œuvre a permis de décupler son intérêt. L'atout majeur pour tout utilisateur d'un tel réseau de données informel, est que plus de personnes seront membres d'un tel réseau, plus celui-ci devient riche en contenu, mais surtout que la mise sous surveillance d'un tel réseau devient alors quasiment impossible, chaque utilisateur étant à la fois demandeur et offreur de données, qui peuvent être légales ou illégales, mais dont la distinction n'est souvent pas évidente.

Le développement de ce type de réseaux a très vite attiré les cybercriminels, car ceux-ci peuvent s'en servir très facilement pour transférer des informations sensibles et/ou illégales de manière quasi anonyme, sans crainte de se faire repérer puisque l'information sera répliquée sur une partie des autres ordinateurs membres du réseau, la plupart d'entre eux étant « innocents à l'affaire ». Il ne sera alors pas possible pour un enquêteur de suspecter les centaines de milliers de personnes connectées à un tel réseau mondial informel.

Pour que ce concept soit réellement intéressant à l'échelle criminelle, il faut par conséquent cacher l'information à transmettre dans un document qui ait un caractère neutre (image, fichier musical, clip vidéo, etc.), de manière à ce que les personnes qui le récupéreraient ne soient pas alertées par le message véhiculé. Cette pratique, appelée stéganographie, existe en fait depuis l'antiquité, et se base sur les techniques cryptographiques, afin d'incorporer un message court dans un document, de manière à ce que seul le destinataire au courant soit en mesure d'extraire ledit message.

Les débuts de l'application de cette science à l'informatique ont été motivés par les activistes se trouvant dans des pays politiquement instables, et où certaines informations devaient être stockées et/ou transmises de manière invisible, sous peine de représailles voire de mort certaine. Malheureusement, tout comme pour la cryptographie, les travaux de recherche en cryptanalyse et en rétrostéganographie ont permis de casser, ou du moins de mettre en évidence les méthodes de camouflage les plus simples, mettant en péril la vie de certains activistes.

Actuellement, les laboratoires de cryptanalyse dans le monde entier mettent au point des méthodes avancées de camouflage et d'attaques basées sur des technologies militaires telles que l'étalement de spectre ou les analyses statistiques. Certains résultats de travaux, et notamment les thèses d'étudiants sur le sujet, sont publics et peuvent à juste titre intéresser les cybercriminels.

Pour en revenir aux récents développements en matière de communications, un certain nombre de travaux et d'implémentation de réseaux dits « furtifs » existent. Il s'agit grosso modo de réseaux basés sur le concept du « peer to peer », associant de plus des mécanismes de cryptographie avancée, afin de protéger et d'isoler chaque nœud du réseau.

L'objectif avoué (et atteint) des concepteurs de telles méthodes est de rendre impossible toute identification de l'émetteur et du récepteur d'un message, d'empêcher toute altération ou interception du message, de masquer l'itinéraire, et de se prémunir contre des nœuds de transit corrompus, sous surveillance ou en panne. Le projet libre TOR « The Onion Router » en est à sa version 3, et a corrigé un certain nombre d'erreurs de jeunesse, atteignant désormais l'ensemble des objectifs souhaités. On imagine déjà les applications cybercriminelles qui peuvent en découler.

Un autre point marquant concerne les évolutions récentes en termes de chiffrement, mais surtout d'attaques associées. Lorsque l'on interroge certaines personnes au sujet de la possibilité de casser certains systèmes de chiffrement considérés comme sûrs, ils évoquent le fait que les algorithmes utilisent des principes de factorisation de nombres premiers très élevés, et que par la nature même des calculs ceux-ci requièrent des années, voire des siècles de calculs. Ces estimations simplistes ne tiennent malheureusement pas compte de facteurs importants et bien réels.

D'une part, comme le souligne Jacques Blamont dans son ouvrage, il ne faut pas négliger la loi de Moore qui est à l'œuvre dans la plupart des domaines techniques, et dont bénéficient également les cryptanalystes. Ce qui était difficilement cassable il y a dix ans avec un supercalculateur le devient facilement avec un ordinateur de bureau. De plus, l'augmentation non seulement des capacités de calcul, mais également des capacités de stockage et des réseaux , permettent des innovations en matière de cryptanalyse.

La récente mise au point des tables « *Rainbow* » par un étudiant de l'université Polytechnique de Lausanne a contribué à diminuer d'un facteur considérable le temps de cassage d'une clef cryptographique. Outre une méthode innovante sur le plan mathématique utilisant des méthodes de tri et les probabilités, il a également su tirer parti de l'importante mémoire de stockage dont nos ordinateurs personnels disposent de nos jours. Sa méthode consiste donc en gros à précalculer un sous-ensemble des possibilités permettant de retrouver un mot de passe, avec une occurrence de n%.

Le précalcul prend certes du temps, et génère plusieurs milliards de valeurs qui seront stockées sur disque dur ou sur support amovible (DVD), mais une fois ces valeurs calculées, le temps de recherche d'un mot de passe est inversement proportionnel au temps passé à effectuer ces calculs. À titre d'exemple, il a pu lors de sa thèse sur le sujet démontrer mathématiquement puis par la pratique que le temps maximum requis pour retrouver n'importe quel mot de passe Windows était de moins d'une seconde, grâce à cette méthode.

Du coup, un certain nombre d'autres personnes ont implémenté sa méthode de cryptanalyse dans différents logiciels spécialisés, dont « Cain&Abel », le plus abouti et disponible librement, qui permet *a priori* de collecter automatiquement puis de casser en un minimum de temps et avec peu de connaissances la quasi-totalité des mots de passe circulant sur les réseaux filaires ou sans fil, protégeant les messageries, les bases de données, équipements réseaux, et systèmes d'exploitation.

D'autre part, les avancées des recherches en mathématiques permettent la mise au point de méthodes de cryptanalyse novatrices. Les spécialistes en la matière ont tous en mémoire la découverte de la cryptanalyse différentielle, qui a permis de casser des algorithmes réputés auparavant inviolables. Adi Shamir, l'un des cryptographes ayant marqué notre époque, a récemment et à deux reprises mises au point des techniques pour casser le protocole de chiffrement du téléphone GSM, en quasi temps réel.

Enfin, un troisième facteur permettant de réduire considérablement le temps de cassage de clefs, consiste tout simplement à contourner le problème en cherchant des failles d'implémentation des algorithmes. En effet les mathématiciens ne sont pas souvent programmeurs, et les programmeurs ne connaissent pas souvent les mathématiques. Il en résulte très souvent un phénomène de mauvaise implémentation, voire d'erreurs grossières qui fragilisent réellement l'algorithme, et réduisent d'autant plus les difficultés à retrouver les mots de passe. Ainsi, on retrouve pêle-mêle des failles d'implémentation autour des systèmes de chiffrement de Windows, de sécurisation des réseaux sans fil Wi-Fi (WEP), des protections de documents bureautiques et bases de données, voire d'équipements réseau ou de téléphonie.

À côté de la stéganographie, on sait mesurer l'impact cognitif d'un message subliminal (à approfondir si vous le souhaitez)

6ème CONSTAT : Mondialisation et recherche d'économies

Un risque nouveau tend à intéresser les spécialistes en sécurité des systèmes d'information. La tendance actuelle chez les directeurs informatiques est d'externaliser un certain nombre de tâches de conception de logiciels, certains services informatiques tels que les centres d'appels, voire carrément de déplacer toute l'informatique vers un pays tiers, dont le niveau de vie est moindre. Les conséquences liées à cet aspect sont certes bénéfiques *au premier abord* sur le plan financier, mais les criminels et terroristes pourraient être tentés de profiter de cette situation intéressante sur bien des points pour eux aussi.

La plupart des pays choisis par les pays occidentaux pour effectuer cette sous-traitance ne sont pas totalement stabilisés, et leur population se rapproche plus souvent des 1$ que des 50$. Les pays de l'Est et le proche orient sont des lieux de prédilection pour les centres d'appel et l'hébergement des salles informatiques. Un certain nombre d'opérateurs de télécommunications européens ont ainsi récemment délocalisé une partie de leur personnel sur place. L'Asie et l'Inde sont aussi des lieux où il est courant de trouver des équipes de recherche, de conception et développement de nouveaux logiciels, matériels, etc. pour le compte de sociétés américaines ou européennes.

Supposons maintenant que l'instabilité politique ou religieuse s'instaure dans de tels pays, ou bien que des organisations criminelles prennent le contrôle partiel de l'économie locale. Il se pourrait alors bien que ces centres d'appels, salles d'hébergement et laboratoires de développement deviennent un moyen privilégié pour attaquer l'économie occidentale.

Une première option consisterait tout simplement à ce que des programmeurs et concepteurs intègrent discrètement dès la conception des produits des portes dérobées et chevaux de Troie, permettant lorsque cela sera nécessaire de rendre inopérant le système en question, de faciliter la fuite de données ou bien encore de permettre à des personnes précises de prendre son contrôle à distance. Compte tenu de la complexité des programmes informatiques actuels, des nombreuses clauses juridiques interdisant la rétro-ingénierie, et du nombre de programmes circulant partout dans le monde, il semble très difficile de détecter de telles portes dérobées, à moins d'assurer un véritable contrôle qualité tout au long des phases de développement. Ce qui ne semble pas encore intégré dans les mœurs des industriels du logiciel.

Une seconde option concerne les attaques sur les infrastructures. De nombreux prestataires informatiques embauchés souvent sans vérification préalable de leurs intentions pacifiques, puis mis à disposition par une quantité considérable de sociétés de services ont accès de par leurs fonctions à des segments plus ou moins importants d'infrastructures informatiques et de leurs données, plus ou moins sensibles. Le phénomène de délocalisation de ces infrastructures dans des pays émergents peut induire un phénomène similaire, puisque l'entrepreneur occidental se repose sur des actes juridiques pour transférer la responsabilité du bon fonctionnement de l'infocentre à la société tierce. Si ce mécanisme juridique fonctionne bien dans les pays dits développés, grâce notamment à une certaine stabilité, cela est moins certain dans les pays cités précédemment. On risque par conséquent différents problèmes, tels que le *kidnapping* de l'infocentre avec demande de rançon, le vol et détournement de données, voire encore pire l'utilisation des structures de calcul et de traitement de ce même infocentre pour lancer des attaques informatiques.

Une troisième option viserait les clients et utilisateurs des centres d'appel. Imaginons un instant qu'un centre d'appel offrant des services de support aux utilisateurs soit « véreux », et se mette à donner des instructions aux appelants afin qu'ils déverrouillent certaines fonctions de sécurité, sans le savoir. Ou bien que ce même centre d'appel réponde aux clients de manière à provoquer la panique. Lorsque l'on sait que de plus en plus de centres d'appel délocalisés dans ces pays concernent des fonctions semi-critiques, cela devient inquiétant. Dernier point marquant : une bonne partie des opérateurs de télécommunications, des fournisseurs d'accès internet, des vendeurs de systèmes de sécurité et antivirus sont également en train d'opter pour ce type de solutions. Une action coordonnée sur ces centres pourrait dès lors paralyser tous les nœuds de communication en cas d'incident majeur.

7ème CONSTAT : Surinformation

Un autre danger à ne pas négliger est lié à l'augmentation de puissance des moteurs de recherche, et à leur diversification. Autrefois, ceux-ci n'indexaient que des pages Internet. De plus en plus, et afin de garder un avantage compétitif vis-à-vis de leurs concurrents, ceux-ci sont désormais capables de mémoriser de nombreuses données différentes, en gardant l'historique au fil du temps. Cette puissance accrue permet également pour certains experts malveillants de peaufiner des attaques informatiques,ou de collecter des informations sensibles, voire confidentielles, à l'insu de leurs propriétaires. Un certain nombre de travaux de démonstration ont été menés en ce sens par des universitaires et pirates en herbe, et on se doute bien que les organisations criminelles sont déjà au courant de telles pratiques.

Un autre moyen pour les criminels de tirer profit du réseau Internet est tout simplement d'utiliser ce formidable vecteur de communication pour désinformer ou manipuler l'opinion. Par sa nature même, chacun d'entre nous est en mesure de publier différentes informations véridiques ou non, et si l'on s'y prend bien il est possible d'influencer de manière notable les foules accédant à ces données. Aucun organisme de contrôle de la véracité des informations n'existe sur Internet, ce qui permet aux criminels une désinformation parfaite, et l'introduction de rumeurs permet par exemple de déstabiliser le cours financier d'une entreprise, de bloquer des décisions importantes ou de mobiliser certains citoyens ou activistes à leur insu… c'est l'une des facettes de la fameuse *Netwar* dont Jacques Blamont fait état dans son ouvrage.
Il y a aussi un droit de l'Internet …(à développer si vous le souhaitez,notamment les jurisprudences d'internautes opérant en France)

2ème PARTIE : OPPORTUNITES ET AXES DE REFLEXION

Les différents constats mentionnés précédemment laissent songeur. L'économie et le fonctionnement de la quasi-totalité des pays développés reposent sur des technologies de l'information et de communication. Compte tenu de la très grande fragilité de ces mêmes infrastructures et du peu de moyens nécessaires pour les bloquer, on est en droit de penser que nous avons eu jusqu'à présent beaucoup de chance… mais jusqu'à quand ?

PISTE : Appliquer les conseils des experts

La menace cybercriminelle ne concerne en fait pas seulement les personnes et entreprises directement connectés à l'Internet, mais tous les citoyens connectés ou non, voire carrément la partie de l'humanité qui dépend des ressources fournies par les pays développés. Fort heureusement jusqu'à présent, Internet a tendance à se comporter de manière conforme à ses objectifs initiaux, c'est-à-dire « capables de résister à une explosion nucléaire », étant un réseau fortement décentralisé, ce qui explique pourquoi les attaques ayant eu lieu jusqu'à présent n'ont pu saturer que quelques sites, mais jamais la totalité du réseau. Reste le talon d'Achille d'Internet : les 12 serveurs primaires de noms de domaine, qui ont déjà été soumis à des attaques d'intensité moyennes, et qui en cas d'attaque prolongée pourraient mettre à mal l'ensemble d'Internet. Sur ce point, nos homologues américains veillent, de concert avec les organismes militaires et le *Department of Homeland Security*.

Le risque cyberterroriste pourrait être lié à une action physique : coupure des liaisons à haut débit transatlantiques, par exemple. Cela provoquerait un ralentissement (en cas de coupure partielle) voire une interruption des connexions entre notre continent et les États-Unis, où se trouve une grande majorité des infrastructures Internet. Les attaques massives par déni de service distribué (dDoS) et/ou redirection vers un serveur terroriste ciblant un ou des serveurs critiques (médias, nœud d'échange internet, moteur de recherche majeur, etc.) pourraient avoir des conséquences au niveau des internautes. L'indisponibilité par saturation et la redirection des internautes vers par exemple un message terroriste peuvent inquiéter, et seraient à classer dans le cadre de la guerre psychologique. Ces attaques sont d'actualité, puisque depuis mars 2005 un certain nombre d'internautes voulant accéder aux pages d'accueil de certains sites américains sont redirigés vers des sites… chinois.

Les interconnexions massives de toutes sortes de réseaux et équipements, dont j'ai rappelé les dangers en première partie, facilitent grandement les attaques visant des infrastructures critiques, voire nationales. Les États-Unis ont mis en place un certain nombre d'organisations, dont le Department of Homeland Security, et sa doctrine de février 2003, « National Strategy for Protecting Cyberspace », afin de mener une réflexion sur des scénarios catastrophes et à envisager des solutions visant à se prémunir de telles actions. Fait intéressant, parmi les différentes actions menées dans le cadre de ces mesures, les USA ont mis en place un partenariat d'échange d'informations avec quatre autres pays alliés *clef* que sont…le Royaume-Uni, l'Australie, le Canada et la Nouvelle-Zélande et qui ne sont autres que les signataires du projet Échelon ! Une première étape serait de toute manière pour nous autres Européens, de commencer par s'inspirer des actions, méthodes et documents fournis par nos confrères américains pour leur usage quotidien. Le Conseil de l'Europe a également lancé une initiative en ce sens, *Convention sur la Cybercriminalité*, qui serait judicieux d'appliquer au sein de nos réseaux domestiques, privés et nationaux.

La quasi-totalité des infrastructures civiles (transports et logistique, énergie, finance, médias, distribution et alimentation) est reliée à l'Internet d'une manière ou d'une autre. Bien qu'il soit quand même difficile pour un cyberterroriste de s'attaquer à l'ensemble de ces domaines simultanément, il peut assez facilement viser un nombre limité de cibles et en paralyser les équipements, voire pire encore modifier certaines données critiques. Les centaines de milliers de mécanismes de protection des systèmes informatiques déjà opérationnels face aux différentes menaces (antivirus, espiogiciels, etc.) ne sont pas suffisants et sont aveugles face à certaines attaques, notamment parce que les attaquants savent comment les contourner. Les spécialistes de la sécurité informatique s'accordent à dire qu'à l'heure actuelle aucun mécanisme de protection n'est efficace à 100%, et que la meilleure méthode permettant de réduire le risque d'une attaque, lorsqu'il n'est pas possible de dissocier les systèmes informatiques critiques du réseau Internet, consiste simplement à chaîner différents systèmes de protection les uns aux autres, en veillant à alterner différentes technologies, afin de former une succession de remparts de nature différente.

Les quelques experts en sécurité des systèmes d'information présents en France se plaignent souvent entre eux que leur discours est vain, que leur direction ne les écoute pas toujours, car la sécurité est perçue comme une dépense difficile à justifier, un frein de productivité, un carcan pour les utilisateurs. Des auditeurs ont tenté de mettre en place des méthodes de calcul de rentabilité et de retour sur investissement des projets sécurité, mais sans grand succès. D'autres responsables ont tenté de crier au loup, mais ont à ce jeu décrédibilisé le discours et les enjeux. Il y a pourtant un réel plaidoyer de ces mêmes experts qui doit être entendu, à condition que ceux-ci jouent également le jeu de l'indépendance, de l'objectivité et de l'intérêt collectif. Quelques groupes de réflexion sont déjà opérationnels entre responsables sécurité de grandes entreprises françaises et européennes, mais ceux-ci fonctionnent en vase clos et ne permettent à leurs membres que se rendre compte du problème vécu de manière similaire chez leurs confrères. Il faut par conséquent apporter à ces groupes d'experts un moyen d'agir… aux États-Unis on a créé pour cela des *think tanks*. Pourquoi pas en France ou en Europe ?

PISTE : Protéger l'utilisateur domestique de manière transparente

L'un des problèmes majeurs est en fait lié à l'utilisateur domestique, qui ne configure pas bien son ordinateur face aux menaces (mais est-ce son rôle ?), mettant inconsciemment un matériel transformable en outil d'attaque à la disposition du criminel. Les spécialistes de la sécurité s'accordent dire que l'on compte désormais en millions le nombre d'agents relais ou zombies installés sur les ordinateurs personnels des particuliers. Il me paraît illusoire de sensibiliser chacun des internautes, d'une part car il leur faudrait acquérir un certain nombre de notions abstraites en informatique ainsi qu'une connaissance partielle de la langue anglaise, et d'autre part, car il se trouvera toujours des personnes malveillantes qui profiteront de leurs connaissances pour induire en erreur l'utilisateur par le biais de l'ingénierie sociale.

Mon raisonnement pour tenter d'apporter une solution à ce problème repose simplement sur une observation courante : le réseau domestique EDF. Celui-ci fournit une interconnexion des foyers, mais chaque foyer est protégé par un disjoncteur qui se déclenche en cas de problème. Au niveau inférieur on retrouve un disjoncteur par pièce, et au niveau supérieur un disjoncteur de quartier. Dans la mesure où des mécanismes similaires existeraient sur le réseau Internet en analysant les flux et en bloquant automatiquement certains d'entre eux sous certaines conditions, il serait alors possible de limiter certains problèmes.

Les alertes correspondantes pourraient alors être remontées à nos différents CERTs (Computer Emergency Response Teams) nationaux afin de traiter l'incident. Les technologies permettant cela existent (IPS, *Intrusion Prevention System*) mais ne sont à mon avis pas suffisamment matures pour pouvoir être déployées ainsi. Il convient cependant d'y porter attention à l'avenir. Un tel déploiement pourrait également heurter les sensibilités de certains, car il engendrait un sentiment de restriction de liberté (cybersurveillance), même si cela n'est pas tout à fait vrai, les systèmes se déclenchant sans intervention humaine. Les États-Unis ont déjà mis en place un certain nombre de mesures de surveillance des utilisateurs du réseau Internet, sans pour autant opérer le rôle de disjoncteur. Un problème éthique se pose alors, il convient d'y réfléchir.

PISTE : Sensibiliser, former et certifier les acteurs professionnels

Du côté des professionnels des systèmes d'information, il y a encore un certain nombre de lacunes, voire d'incompréhensions à traiter face à ces nouvelles menaces. Nombre de concepteurs d'applications ne prennent pas ces risques au sérieux, et le contrôle qualité n'est souvent pas au rendez-vous, tant pour des raisons liées à la méconnaissance des développeurs (on n'apprend toujours pas à programmer de manière sécurisée dans les écoles informatiques) que pour des raisons économiques visant à réduire le cycle de développement et mettre le produit sur le marché avant le concurrent.

Ce problème se retrouve également du côté des prestataires de service, où la plupart des techniciens et ingénieurs n'ont pas les réflexes et notions de sécurité qui permettraient pourtant de limiter à moindres frais quantité de risques potentiels. Une des solutions à ce problème se pose en termes de sensibilisation et de formation des acteurs du monde informatique.

Des certifications professionnelles en sécurité accompagnées de chartes éthiques et de déontologie (CISSP) rencontrent un succès important notamment aux États-Unis, mais celles-ci sont encore trop « pointues » pour le professionnel non expert, et on ne compte à ce jour en

France que moins de 140 certifiés de cette catégorie. À noter que le Moyen-Orient et l'Asie sont très demandeurs de ce type de certifications.

Il existe au moins une initiative franco-française récente visant à certifier les responsables sécurité, mais elle ne semble pas adaptée à l'ensemble des professionnels de l'informatique non plus. Espérons que ce n'est qu'une étape vers une vraie professionnalisation du métier, tout comme pour les professions libérales qui ont leur Ordre. Cela permettrait peut-être de trier le bon grain du mauvais, et de limiter les risques.

Les médecins, les pharmaciens, les comptables, les avocats ont des responsabilités importantes, dans le respect de codes de déontologie et des règles éthiques.* A priori les systèmes d'informations sont devenus le centre nerveux de l'économie, et en sont l'un des pivots les plus sensibles. Pourquoi les informaticiens qui ont un tel poids ne pourraient-ils bénéficier d'une structure ordinale ou d'un « barreau » et pourquoi ne devraient-ils pas respecter un code de déontologie leur permettant d'exercer leur métier ? On rencontre malheureusement encore trop souvent des charlatans qui pourraient causer du tort aux structures, soit de leur propre fait, soit manipulés par des criminels.

Et le DMP (dossier médical personnel et le respect du secret médical distinct du secret professionnel, égal à celui de l'avocat ou du prêtre ou des représentants d'autres religions
**J'espère avoir saisi votre pensée, car les ordres sont contestés (à discuter ensemble) même si d'autres professions les souhaitent aussi pour reconnaissance de la part des pouvoirs publics et une certaine protection…

CONCLUSION

Cette brève introduction manque d'exhaustivité, et n'est qu'une mise en bouche pour sensibiliser les acteurs de la vigilance que nous sommes. Il est nombre de domaines liés à la sécurité des systèmes d'information, voire de la protection du patrimoine informationnel, qui restent à développer.

Parmi ces points, dans le désordre : les aspects juridiques et les failles liées à leur inadéquation face à l'évolution permanente des développements technologiques, les risques liés à la ***désinformation*** et à ce que l'appelle « le risque média », les dangers pouvant être liés à la gestion des droits numériques et le verrouillage des ressources informatiques contre le gré de l'utilisateur, les attaques électroniques et l'engouement des criminels pour la rétro-ingénierie logicielle et matérielle, les attaques terroristes combinées (cyber / réelles), l'hégémonie de certaines firmes sur les technologies induisant certains risques, les infrastructures de surveillance globaux des ressources par les états pouvant être détournées (Cloudshield, etc.), les risques se profilant derrière les grands moteurs de recherche ou à cause des stratégies de certaines entreprises, l'impact des logiciels libres en sécurité, etc.

Il est certain que chacun de ces domaines nécessite une réflexion conséquente, car ils impactent de manière importante la manière dont chacun est à même d'utiliser l'outil informatique… nous-mêmes, mais aussi les criminels qui y verront un potentiel jamais atteint jusqu'à présent pour atteindre leurs objectifs, à faibles coûts et sans prendre de risques. À ce jeu nous voyons assez clairement qui serait le gagnant si nous ne prenons pas nos précautions rapidement, tout comme nos homologues d'outre-Atlantique sont en train de le faire tant bien que mal.

Notons simplement que d'une part l'évolution de la loi de Moore, et d'autre part l'augmentation de l'étendue de certaines puissances criminelles dans des pays instables ou dont la population possède peu de moyens, mais a les capacités intellectuelles lui permettant d'imaginer une guerre informatique ou la netwar, provoqueront à coup certain un certain nombre d'incidents majeurs liés à la cybercriminalité, il ne nous reste qu'à nous préparer à cette éventualité au mieux dans un premier temps, puis à réfléchir à la possibilité de riposte et de disjonction intelligente des réseaux viciés.