Sébastien Dhinaut

LE PIRATAGE INFORMATIQUE

session 2005-2006

Introduction

A côté de notre monde réel il en existe un virtuel. Ces deux univers interagissent chaque jour et parfois même sans que l'on ne s'en aperçoive. Cette omniprésence dans notre vie quotidienne (à la maison, au bureau, dans la voiture, à la banque…) doit son existence à la mise en réseau des systèmes informatiques. Mais cette mise en réseau est aussi le point faible de la sécurité informatique.
Il existe deux types de réseaux :
Les réseaux fermés accessibles uniquement par les membres du réseau, comme les Intranet, permettant aux membres d'une même entreprise de faciliter la communication et le partage du travail (exemple : la SNCF dont les informations relatives à la circulation ferroviaire sont centralisées et transmises dans l'Intranet de la société)
Les réseaux ouverts où toute personne est autorisée à pénétrer, c'est le cas d'Internet qui est le seul réseau ouvert à caractère international.
Aujourd'hui l'utilisation d'Internet est en pleine expansion. Elle permet un accès à la connaissance et favorise le commerce. Cependant Internet représente aussi un nouveau terrain de malveillance exploité par certains individus peu scrupuleux, appelés pirates informatiques, face auxquels les systèmes répressifs nationaux demeurent bien souvent impuissants.
Ce mémoire tentera de répondre à une question légitime qui est :
Existe t-il une guerre virtuelle liée au piratage informatique ?
Nous découvrirons tout d'abord les camps qui s'opposent, puis la stratégie des pirates et enfin l'arsenal défensif.

Comme dans une guerre il y a tout d'abord deux camps qui s'opposent.

D'une part, les pirates, qui font leur apparition dans les années quatre-vingts et dont le grand public prend conscience de l'existence et de leur fascination pour le cyberespace et son côté ludique par le film Wargames de 1983. Ce film met en scène un très jeune enfant pénétrant les systèmes informatisés de la défense nationale américaine et déclenchant une guerre mondiale. Une telle performance était bien sûr impossible avec le matériel de l'époque. Cependant ce film aura pour vertu principale de présenter l'engouement des pirates pour défier les systèmes informatiques complexes et mesurer ainsi leurs capacités techniques.

Les pirates informatiques sont souvent désignés par le terme «hackers ». Ce néologisme définit à l'origine une personne qui aime comprendre et utiliser les finesses techniques des programmes. Désormais il qualifie aussi les personnes entrant illégalement dans des sites informatiques.

Qui sont-ils ? Même s'ils sont issus de sociétés très différentes ils ont souvent des critères identiques :

- Leur idéologie est commune et fortement teintée de liberté. Elle est basée sur le premier amendement de la Constitution américaine protégeant la liberté d'expression laissant penser aux pirates qu'ils ne sont pas des criminels mais des activistes. Le mouvement littéraire d'anticipation, le cyberpunk, né vers 1984 et représenté par les romanciers américains William Gibson et Bruce Sterling renforce cette idéologie. Le cyberpunk est une contre-culture née de la peur du Big Brother et a pour principe que dans une société démocratique, il ne saurait y avoir de contrôle, ni de limite à la circulation de l'information numérique. Ils en déduisent que les gouvernements n'ont pas à restreindre la liberté d'expression sur les réseaux numériques. En 1992 Bruce Sterling édite un ouvrage reprenant les idées du cyberpunk, qui fut très largement diffusé et faisant office de référence en la matière, intitulé : « The Hacker Crackdown : Law and Disorder on the Electronic Frontier ».

- Ils appartiennent à la même génération. Les pirates sont le plus souvent des adolescents ou de jeunes personnes privées d'emploi. Une étude du Fédéral Bureau of Investigation (FBI) nous montre que les pirates les plus dangereux ont entre dix-huit et trente-cinq ans, même s'ils sont parfois beaucoup plus jeunes. Ainsi en 1987 un jeune adolescent de seize ans a réussi à pénétrer le département de la défense américaine au delà des

barrières de sécurité informatique des sites. Il a été accusé de nombreux délits dont la divulgation de mots de passe secrets et d'informations techniques pour violer les systèmes de sécurité informatique. Son jeune âge lui permit d'obtenir une réduction de peine ; il fut condamné à neuf mois d'emprisonnement et dix mille dollars d'amende alors qu'il encourait une peine de treize années d'emprisonnement et quatre-vingt mille dollars d'amende.

- Ils répondent aux mêmes motivations criminelles. L'une d'elles réside dans la vengeance suite par exemple à un licenciement comme ce responsable informatique qui en 1991 installa un programme de destruction dans les ordinateurs de l'employeur et causa ainsi la paralysie de l'entreprise durant un mois. Le besoin d'autodéfense rentre aussi dans le cadre des motivations des pirates. En effet certains programmeurs utilisent des programmes de destruction afin de protéger leurs oeuvres d'éventuelles contrefaçons.

- Une autre motivation et non des moindres concerne l'appât du gain. Les possibilités de détourner de l'argent sur Internet sont considérables. L'une des plus fréquentes et des plus lucratives passe par les cartes de crédits. Lors d'un achat sur Internet il est fréquent que celui-ci soit réglé par carte de crédit. Pour ce faire il est demandé d'indiquer des informations confidentielles la concernant (numéro de la carte, nom du porteur, date d'expiration) Ces informations sont cryptées lorsqu'on les entrées mais ne le sont plus dès lors qu'elles sont stockées au sein de l'entreprise et sont alors accessibles aux pirates. C'est de cette manière que Kevin Mitnick avait utilisé vingt mille numéros de cartes de crédit avant d'être arrêté en 1995.

- La dernière motivation principale est d'ordre social puisque les pirates revendiquent bien souvent leurs actes dans un but de reconnaissance de leurs compétences techniques qui compense la pauvreté de leurs relations sociales. Un grand nombre de pirates présentent sur une page Web leurs actions classées dans des « tableaux de chasse ». Les pirates souhaitent également mettre en évidence la fragilité de systèmes informatiques perçus comme étant infaillibles. Ainsi les sites attaqués en priorité relèvent des institutions politiques et des organismes d'état ; par exemple l'administration américaine a, pour la seule année 1995, décelé deux cent cinquante mille attaques de pirates sur les sites de la défense américaine. Même s'il s'agit d'avantage d'un jeu technologique que d'une réelle volonté

de destruction, l'administration américaine se lasse de ces attaques qui décrédibilisent leur politique de communication.

D'autre part, les entreprises, qui grâce à l'apparition d'Internet ont pu améliorer la qualité et la rapidité des transmissions propres à la vie de l'entreprise. Elles sont d'autant plus séduisantes vis à vis de leurs clients car l'image de marque et leurs services se sont vus grandement améliorés et mondialisés par l'existence d'un site relatif à l'entreprise. Par exemple La Redoute offre un site permettant au client de commander depuis son domicile, de connaître tous les services de la société et d'accéder à toutes les informations pratiques. Au delà le client peut au fil de ses recherches découvrir totalement une société dont il ignorait jusqu'à l'existence. On comprend donc aisément qu'une perturbation de ces services peut être très dommageable à l'entreprise.

Certains employés dont le travail repose sur l'ordinateur ou Internet comme les programmeurs, les webmasters, les administrateurs réseau, les infographistes… voient leur emploi menacé par les malveillances des pirates.

Les administrations étatiques utilisent Internet comme moyen de communication et de propagande (concours administratifs, inscription dans l'armée nationale…) Une perturbation de ses sites ridiculise l'Etat et discrédite la sécurité nationale.

Le grand public et pour sa part otage de ce conflit car il est à la fois victime de l'incitation à utiliser Internet par les administrations publiques (déclarations d'impôts, inscriptions aux concours administratifs…) et ils sont aussi victimes des méfaits des pirates.

Nous avons découvert qui sont les pirates et leurs intentions, les autres acteurs de la vie virtuelle et leurs intérêts liés à l'utilisation d'Internet. Voyons à présent quelle est la stratégie des pirates et les nuisances engendrées.

Loin d'agir au hasard les pirates font preuve d'une véritable stratégie pour attaquer.

Les pirates agressent leurs victimes de manière directe ou indirecte. Les attaques directes commencent souvent par une intrusion dans le système informatique de la victime pour se livrer à des actes criminels.

- Il pirate la ligne téléphonique de la victime (cette action est également appelée phreaking) afin de ne pas payer la communication Internet et de ne pas être localisé. Pour ce faire, il utilise un boîtier capable de générer des tonalités de commandes comme les techniciens de maintenance des compagnies de téléphonie.

- Le pirate va ensuite chercher à entrer en communication avec l'ordinateur piraté pour en prendre le contrôle. Cette démarche exige que l'ordinateur visé ait une connexion Internet et qu'il réponde automatiquement aux instructions transmises par le pirate. Le plus souvent le pirate utilise un cheval de Troie c'est-à-dire que le programme malveillant est dissimulé dans un autre programme au-dessus de tout soupçon afin que la victime ne se méfie pas.

- Ce dernier est souvent utilisé pour introduire une « bombe logique », programme de destruction, qui une fois installée sur l'ordinateur attend un signal externe pour exploser (démarrage d'un programme, passage à une certaine date, une certaine heure…) Les dommages que causent les bombes logiques sont importants et la surcharge électrique qu'elles engendrent détruit souvent certains périphériques informatiques.

- Quant aux mots de passe qui sont la première sécurité de l'ordinateur contre la violation des biens informatiques, le hacker va les déverrouiller à l'aide d'un programme de déchiffrage qui fonctionne comme un dictionnaire et propose au système un grand nombre de mots de passe à une cadence très élevée jusqu'à ce que le bon code soit trouvé. On appelle cette méthode le «cracking». Ce procédé est également utilisé pour générer des identités, des numéros de téléphone et de carte bancaire qui soient acceptés par le site sur lequel le criminel progresse.

- Les criminels informatiques créent de faux sites de service clientèle d'entreprises réputées notamment les banques. Ils invitent par e-mail

l'utilisateur à se rendre sur ces sites par l'intermédiaire de liens et, sous prétexte d'une panne informatique, de réactualiser ses données confidentielles. Le pirate se trouve alors en possession de tous les éléments nécessaires pour voler le compte.

Une autre attaque directe mais ne nécessitant pas d'intrusion dans le système informatique de la victime consiste à bloquer la messagerie électronique de la personne visée en lui envoyant un nombre très élevé d'e-mails (ou courriels) cet acte est nommé « Mailbombing ».
Le même type d'attaque existe à l'encontre des groupes de discussion. On l'appelle cette fois « Pollupostage » ou « Spamming » et il s'agit pour le hacker d'inonder le groupe de discussion avec le même message, inutile, souvent provocateur et sans rapport avec le sujet de discussion causant ainsi une véritable pollution des réseaux.

Les agressions indirectes à la différence des agressions directes ne visent pas une personne en particulier mais frappent de manière aveugle et diffuse. Elles sont véhiculées de divers manières (courriers électroniques, chevaux de Troie…)

- La plupart du temps il s'agit de virus, petits programmes ayant pour finalité d'altérer, d'endommager ou de détruire un système informatique. Il faut savoir que deux cents virus apparaissent chaque mois. Leurs effets sont variables : si « Gingrich » convertit spécifiquement les documents Word les rendant inutilisables le virus « Lecture » quant à lui procède au formatage du disque dur c'est-à-dire qu'il efface de manière complète et définitive toutes les données qui y sont stockées. Certains virus exécutent des opérations combinées comme le virus mouchard « SPA » qui détecte les logiciels installés sur le disque dur et qui ne possèdent pas de licence puis utilise le modem de l'ordinateur pour composer un numéro d'urgence et dénoncer l'utilisateur. Enfin certain virus ne causent pas dommages importants sur le plan des informations contenues dans l'ordinateur mais rendent son utilisation inconfortable comme par exemple en provoquant l'apparition permanente d'un message ou d'une image à l'écran ou en perturbant le déplacement du pointeur de la souris.
  D'autres virus informatiques ont une attaque plus subtile comme les virus polymorphes qui, comme leur nom l'indique, utilisent des méthodes de cryptage aléatoire de leurs codes, leur permettant de se dissimuler efficacement puisqu'il devient impossible de les identifier.
  Les virus furtifs renvoient des informations fausses au système

d'exploitation qui n'affichant que des données erronées ne permet plus de localiser le virus.
Certains virus sont célèbres : « Brain »est le premier virus connu, « Michelangelo » a créé une psychose en 1992, il se déclenche le 6 mars jour anniversaire de la naissance de Michel-Ange en 1475, « 1260 », « v2p1 », « v2p2 »et « v2p6 »sont les premiers virus polymorphiques et enfin « Iloveyou »qui s'est propagé par e-mails.

- A côté du virus, le « ver » est nocif dans son essence même dans la mesure où il s'agit d'un programme autoreproducteur se clonant au travers du réseau. Cette activité surcharge le système de programmes à exécuter et perturbe le réseau.

Ces actes de piraterie informatique forment une menace importante.

D'abord pour l'entreprise : son activité est mise en danger car pour l'année 1996 on évalue à près de cent soixante six millions d'euro les pertes directes et indirectes subies par les entreprises françaises du fait d'attaques logiques non physiques. Ce phénomène est croissant puisqu'en 2002 on observe une augmentation de vingt pour cent des attaques à l'encontre des entreprises.
Le développement du commerce électronique est également considérablement freiné : pour trois cent millions de personnes connectées à Internet dans le monde seulement soixante-huit milliards de dollars en matière de commerce. La rigidité de ce marché est principalement due aux réticences par peur des actes de piratage.
L'activité des entreprises est mise aussi en danger par le piratage de logiciels. Cela inclut : le téléchargement de copies de logiciels sur Internet sans licence ; la réalisation de copies ; l'installation sur plusieurs ordinateurs d'un logiciel sous licence monoposte ; la vente sur Internet ou non de contrefaçons ou de copies de sauvegardes ou encore l'utilisation de ces copies.
Pour les industries de pointe ou les marchés émergeants, le cybercrime représente un risque d'espionnage industriel par lequel le cybercriminel collecte des informations techniques, organisationnelles ou commerciales. Il peut aussi substituer les données de l'entreprise par des données inexactes ou simplement les détruire ou encore mettre hors service les serveurs ou les moyens de communication avec la clientèle.

Ensuite le crime informatique est une menace envers l'Etat.
Le hacker peut se livrer à une désinformation massive en attaquant les sites web

des organismes institutionnels dans un but de déstabilisation de l'action de l'Etat, en mettant en valeur une revendication à caractère politique. Par exemple suite au bombardement par les forces de l'OTAN de l'ambassade de Chine à Belgrade, des pirates informatiques ont réussi depuis Hong-Kong à pénétrer le site Web de la Maison-Blanche et à y laisser des messages revendicatifs dénonçant ce bombardement. Même si la technique est similaire l'objectif est différent d'un démarche visant la valorisation des prouesses techniques.
Sur le plan militaire on peut légitimement imaginer une guerre informatique totale. Or les réseaux numériques sont utilisés pour véhiculer un grand nombre d'informations opérationnelles. Bien que peu de postes informatiques militaires soient reliés à Internet, ils sont autant de brèches permettant d'accéder à des réseaux plus confidentiels. Durant la guerre du Golfe un groupe de hackers Hollandais a proposé aux Irakiens leur service pour perturber le commandement de l'armée américaine moyennant un million de dollars.
En dehors des actions militaires les hackers oeuvrent dans le cyberterrorisme. Ils détruisent ou corrompent des systèmes informatiques dans le but de faire pression sur un gouvernement. Le plus souvent il est demandé une rançon pour éviter l'exécution de menaces (déclenchement d'une bombe logique, attaque d'un système…) comme le 29 janvier 1993 date à laquelle une rançon de dix millions de Livres Sterling fut versée à un groupe criminel qui menaçait, preuves techniques à l'appui, de saboter le réseau informatique des sociétés de courtage londoniennes.

Nous avons vu que les pirates informatiques ont développé de nombreuses armes et des stratégies élaborées pour nuire aux entreprises et aux institutions étatiques. Les conséquences sur celles-ci sont dévastatrices. C'est pourquoi elles ont dû développer un arsenal défensif que nous allons découvrir.

Pour répondre aux agressions que subissent les entreprises et les institutions étatiques, elles ont mis en place un arsenal défensif.

D'une part, pour pouvoir punir légalement les fraudes informatiques il était nécessaire de les criminaliser aux yeux de la loi.

Les Etats-Unis furent les premiers à pénaliser les accès frauduleux aux systèmes informatiques selon la finalité de l'opération d'intrusion effectuée. Ils défendent ainsi les secrets d'Etat, l'honneur national, les données financières confidentielles et le commerce intérieur.

En France, on punit l'accès ou le maintien frauduleux dans un système de traitement automatisé des données (STAD) c'est-à-dire que la loi considère que tout accès à un système de manière irrégulière est considéré comme frauduleux (article 323-1 du code pénal) et puni de deux ans d'emprisonnement et trente milles euro d'amende. Le maintien dans un système par un accès frauduleux ou même par erreur est puni de la même manière. Un élément primordial est à prendre en compte à savoir la conscience morale de l'utilisateur et sa volonté de frauder. En effet sur les sites de certains hackers il y a des liens hypertexte permettant l'accès libre à des sites payants ou à accès limité par des « Backdoor » (porte d'accès dissimulée) préalablement piratées. La loi jugera de la criminalité de l'acte en fonction des connaissances informatique et Internet de l'utilisateur qui a pu ne pas avoir conscience de l'irrégularité de son acte.

Outre l'accès frauduleux dans un STAD les atteintes à son fonctionnement sont punies par la loi (article 323-2 du code pénal) de trois ans d'emprisonnement et quarante cinq milles euro d'amende. La loi punit uniquement l'introduction volontaire de virus ou bombe logique dans un système de traitement automatisé des données à l'exclusion des transmissions automatiques d'un virus par contamination des membres du répertoire de la victime. En plus de cet aspect volontaire, il faut que l'acte reproché ait un effet sur la capacité de traitement de la machine si minime soit-il. (exemple : un ralentissement du STAD)

Les atteintes volontaires aux données d'un STAD sont punies par la loi de trois ans d'emprisonnement et quarante cinq milles euro d'amende (article 323-3 du code pénal). Les atteintes concernent l'introduction, la suppression ou la modification frauduleuse de données. On définit les données protégées comme

tout programme, tout type de données quel que soit son support de stockage (disquette, CD, clef USB…) y compris les données non encore entrées dans un STAD mais destinées à l'être (comme les résultats d'un sondage)
La participation à un groupement formé ou à une entente établie en vue de commettre un délit informatique est puni en fonction de l'infraction commise comme stipulé dans les articles 323-1 à 323-3 (article 323-4 du code pénal)

D'autre part, après avoir légiféré il a fallu se donner les moyens techniques et humains d'appliquer les lois.

L'Etat français s'est doté de plusieurs services de lutte contre la cybercriminalité :

- Depuis 1978 la Commission Nationale de l'Informatique et des Libertés (CNIL) contrôle la stricte application des lois et protège les données nominatives en réglementant la collecte, l'enregistrement et la conservation de ce type d'informations.

- La Direction de la Surveillance du Territoire (DST) a créé un service spécialisé en informatique en 1986 destiné à renseigner le gouvernement sur l'évolution des phénomènes de criminalité informatique, sensibiliser les administrations et les entreprises concernées et agir dans un cadre judiciaire.

- En 2000, un Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) est créé au ministère de l'intérieur associant aux activités de cette office le ministère de la défense, et le ministère de l'économie, des finances et de l'industrie.

- En 1994, la police judiciaire française se dote de deux services spécialisés dans la lutte contre la criminalité informatique : la Brigade Centrale de Répression de la Criminalité Informatique (BRCI) Elle remplit trois missions : soutenir les services de police régionaux dans la résolution d'enquêtes ; être une passerelle de collaboration avec les organismes de lutte à caractère international comme Interpol et mener ses propres enquêtes souvent transfrontalières. Le Service des Enquêtes sur les Fraudes aux Technologies de l'Information (SEFTI) est quant à lui chargé d'apporter des informations et de remplir une mission pédagogique auprès

d'organismes privés ou publiques susceptibles d'être ciblés. Il apporte également son concours aux enquêtes liées à la criminalité informatique.

- La gendarmerie nationale a créé en 1990 un département informatique et électronique de l'institut de recherche criminelle qui a pour fonction d'apporter son aide dans la résolution des délits impliquant l'informatique et les réseaux (notamment les affaires de pédophilie) et forme des techniciens spécialisés.

- Les douanes ont créé en 1990 une cellule de Traitement du Renseignement et Action contre les Circuits Financiers (TRACFIN) qui assure une bonne coordination des services luttant contre le blanchiment des capitaux et le transfert des fonds occultes (surveillance des virements électroniques de fonds)

A l'échelle du consommateur, les premières précautions à prendre reposent sur des manipulations simples à effectuer dès l'installation de l'accès à Internet :

- Il faut modifier le mot de passe permettant l'accès au menu d'installation du rooter ADSL.

- Il est nécessaire de protéger le système par des antivirus et leurs mises à jour, un pare-feu qui bloque l'accès extérieur aux données du disque dur.

- Il est conseillé de désactiver le partage des fichiers et de procéder à des sauvegardes régulières sur un support externe des documents importants.

Et pour protéger sa boîte e-mail :

- Il faut savoir reconnaître les courriers suspects.
  En général, les expéditeurs que l'on ne connaît pas, les erreurs typographiques, les fautes d'orthographe sont des indices de la nature frauduleuse du courrier.

- Il est déconseillé de répondre aux courriers suspects. Même si ceux-ci nous invitent à y répondre pour nous « désabonner », il pourrait s'agir d'un piège.

Conclusion

Au cours de notre développement, nous avons vu qu'il existe **deux camps qui s'opposent** dans le monde virtuel : d'un coté les entreprises et les administrations étatiques dont l'utilisation d'Internet a permis l'accroissement de l'efficience et celui de la qualité de la communication interne ; de l'autre les pirates informatiques, qui ont vu dans l'apparition d'Internet un nouveau territoire sur lequel est surtout reconnu l'exploit technologique.
Ces derniers ont développé de véritables **stratégies de guerre** pour parvenir à leurs fins créant ainsi une menace importante contre tout voyageur du net.
Afin de protéger les intérêts économiques des entreprises et **la sécurité intérieure**, les gouvernements ont mis en place **un arsenal défensif** basé sur des lois et des moyens techniques et humains de les appliquer.
A la vue des différents éléments mis en jeu par le piratage informatique on peut légitimement affirmer qu'il existe bien une guerre liée à ce phénomène.
Lorsque le progrès conduit à une guerre, comme c'est le cas ici, on peut se demander s'il est réellement bénéfique à l'homme.