

ÉRIC FILIOL • PHILIPPE RICHARD

CYBER CRIMINALITÉ

Enquête sur les mafias
qui envahissent le web



DUNOD



Table des matières

Avant-propos	IX
Chapitre 1 – Internet : le nouveau filon des organisations criminelles	1
1.1 Une exploitation professionnelle de la cybercriminalité	2
1.2 Des pertes estimées en million d’euros	6
Chapitre 2 – Les maillons faibles de la sécurité informatique	13
2.1 L’internaute et l’ingénierie sociale	14
2.1.1 L’ingénierie sociale	14
2.1.2 La phase de renseignements	16
2.1.3 Quelques exemples	19
2.1.4 Comment lutter contre l’ingénierie sociale	22
2.2 Les failles de sécurité logicielles	23
2.2.1 L’attaque Scob/Padodor	25
2.2.2 L’attaque GDI+	26
2.2.3 Les attaques du protocole Bluetooth	27
Chapitre 3 – Vols et pertes de données personnelles	29
3.1 DonnÉes personnelles : pertes et profits	29
3.2 Les pertes de données sensibles	31
3.3 Le vol des données : le marché aux puces	32



Chapitre 4 – Le phishing : l’approche artisanale	39
4.1 Introduction	40
4.2 Les techniques du phishing	42
4.2.1 <i>Comment harponner la victime</i>	43
4.3 Les mécanismes d’attaques	47
4.3.1 <i>Attaque par le milieu</i>	48
4.3.2 <i>Obfuscation d’URL</i>	49
4.4 Les différentes protections	52
Chapitre 5 – Le phishing : l’approche industrielle	55
5.1 Le pharming	55
5.1.1 <i>L’attaque par empoisonnement du cache DNS et le pharming.</i>	56
5.1.2 <i>Quelques exemples d’attaques</i>	56
5.1.3 <i>Quelques mesures de lutte</i>	57
5.2 Les botnets	58
5.2.1 <i>Quelques chiffres</i>	59
5.2.3 <i>Les attaques par botnets</i>	60
5.3 Le vishing	63
Chapitre 6 – Le racket numérique	65
6.1 Les attaques contre les entreprises	66
6.2 Les attaques contre les particuliers	67
6.3 Les spams	69
6.3.1 <i>Le spam nigérian</i>	70
6.4 Des parades plus ou moins efficaces	72
6.4.1 <i>Les logiciels antispams</i>	73
6.5 Les spammeurs ont toujours un coup d’avance	74
6.5.1 <i>L’e-mail furtif</i>	74
6.5.2 <i>Des e-mails qui leurrent les logiciels antispams</i>	75
6.5.3 <i>Faux blogs, vrais spams</i>	75
Chapitre 7 – La sécurité du commerce en ligne	77
7.1 La fraude aux paiements	78



7.2 Les différentes solutions de paiement sécurisé	81
7.2.1 Les protocoles de sécurité	82
7.2.2 Les solutions de micro paiement	85
7.3 Les sites de paiement sont-ils fiables ?	88
Chapitre 8 – Les entreprises sont mal protégées	91
8.1 Les différentes menaces	93
8.1.1 Le vandalisme	93
8.1.2 La vengeance	93
8.1.3 L'attaque programmée	94
8.1.4 L'espionnage économique	95
8.1.5 Les moteurs de recherches	97
8.2 Les obstacles à la sécurité informatique	98
8.3 La prévention des risques	100
Chapitre 9 – Antivirus : l'intox marketing	107
9.1 La détection de tous les virus ou la quadrature du cercle	108
9.2 La détection virale : quand les antivirus font mieux que les cryptanalystes	109
9.3 Le fonctionnement des antivirus	111
9.4 Le contournement des antivirus	113
9.5 les autres logiciels de sécurité	114
Chapitre 10 – Les systèmes de défense des réseaux d'entreprise	117
10.1 Les menaces contre l'entreprise	118
10.2 L'architecture d'un réseau sécurisé	121
10.2.1 La DMZ (zone démilitarisée)	121
10.2.2 Le serveur proxy	122
10.3 Le temps	124
10.4 L'argent	125
10.5 Le personnel	127
Chapitre 11 – La protection des données	131
11.1 La sûreté de l'information	133

11.2 La confidentialité des informations : le chiffrement	134
11.3 L'intégrité des informations	139
11.4 La disponibilité des informations	140
11.5 La protection du canal de transmission	142
11.6 Le chiffrement des données dans la pratique	145
Chapitre 12 – La pédophilie sur Internet	149
12.1 La traque policière	150
12.1.1 Des programmes spécifiques	151
12.2 Les logiciels de filtrage	152
12.2.1 Des fournisseurs d'accès laxistes ?	154
Chapitre 13 – Banques en ligne : une sécurité limitée	157
13.1 Un manque de volonté	158
13.2 Les parades (officielles) des banques	160
13.2.1 Le pavé numérique	160
13.2.2 L'antivirus de la banque	160
13.2.3 Les systèmes d'authentification forte	161
Chapitre 14 – Les vigies d'Internet	163
14.1 Les organismes officiels français	164
14.1.1 La DCSSI	165
14.1.2 Le Ministère de l'Intérieur	168
14.1.3 Le Ministère de la Défense	170
14.2 Les organismes étrangers	171
14.2.1 Les Etats-Unis	171
14.2.2 Le Royaume-Uni	172
14.2.3 L'Allemagne	172
Chapitre 15 – Les États qui copient les pirates	175
15.1 L'état des forces	176
15.1.1 Les Etats-Unis	177
15.1.2 La Russie et les anciens pays du bloc communiste	178
15.1.3 Les deux Corées	179



15.1.4 La Chine et l'Asie	179
15.1.5 Le Proche et Moyen-Orient	181
15.1.6 Les autres pays	182
15.2 Les projets Carnivore et Magic Lantern	183
15.3 L'affaire Hans Buehler	186
Chapitre 16 – La législation face à la cybercriminalité	191
16.1 Un arsenal juridique adapté	192
16.1.1 La Convention sur le cybercrime	193
16.2 Des condamnations exemplaires	193
16.2.1 La guerre contre les spammeurs	194
16.2.2 Les phishers sont dans le collimateur	196
16.2.3 Les logiciels espions mis à l'index	197
16.3 L'évolution de la législation	198
Chapitre 17 – L'avenir de la cyberdélinquance : les prochaines cibles	201
17.1 La mobilité	201
17.2 L'invisibilité et l'omniprésence	205
Bibliographie	211
Ouvrages et articles de référence	211
Sites utiles	213
Sites gouvernementaux	213
Autres sites	213
Index	215

Creative Commons BY-NC-ND



Avant-propos

En 1983, le film *Wargames* relate les « exploits » de Kevin Mitnick, un pirate rendu célèbre pour avoir notamment réussi à s'infiltrer dans l'ordinateur du commandement de la défense aérienne américaine. Vingt ans plus tard, la réalité a largement dépassé la fiction. Les virus informatiques, ou de façon plus générale les codes malveillants, sont partout. Les effets de cette pandémie sont multiples. Tout le monde est concerné, le particulier comme l'entreprise.

L'époque où quelques étudiants en informatique créaient des virus est révolue. Place à la cybercriminalité. Le principal objectif des pirates et des organisations criminelles est l'argent. Tous les moyens sont bons : faux sites de banque incitant les clients à donner leurs coordonnées bancaires pour ensuite faire des prélèvements (technique du *phishing*), intrusions dans les réseaux d'entreprises pour voler des informations stratégiques ou mener des opérations de désinformation afin de faire capoter un projet, espionnage d'ordinateurs, tentative de racket d'une entreprise en saturant son site, etc.

Cette nouvelle forme de délinquance coûte très cher. Selon le FBI, les virus, les intrusions sur les réseaux et les autres incidents relatifs à la sécurité coûtent, chaque année, environ 70 milliards d'euros aux entreprises américaines ! En France, des statistiques similaires sont rares et ne sont pas rendues publiques. C'est la culture du secret, une particularité qui n'est pas propre à notre pays¹ mais qui semble néanmoins plus développée chez nous... Résultat, il est très difficile d'estimer l'étendue de ce fléau. Les banques, les sites ou les entreprises victimes de piratage ne communiquent que très rarement. Même les services spécialisés de la police ont le plus grand mal à connaître ces affaires ou à convaincre les victimes de porter plainte afin de lancer des enquêtes !

Aujourd'hui, les escrocs du net emploient des méthodes de plus en plus sophistiquées et de plus en plus ciblées. Il ne s'agit plus d'infecter la toile entière mais d'atteindre une cible précise : une entreprise ou un profil d'internautes (les clients de

1. Selon le FBI, seulement 25% des entreprises américaines victimes d'attaques avertissent les autorités.



telle ou telle banque). Pour mener à bien leurs opérations ils peuvent même faire leurs emplettes sur Internet.

Des sites plus ou moins discrets permettent d'acheter toute une panoplie : virus, logiciels espion, programmes permettant de prendre le contrôle à distance d'un PC, etc. On peut même y trouver des numéros de carte bancaire et des codes entre 3 et 100 euros.

Le plus inquiétant est qu'en faisant quelques requêtes précises sur un moteur de recherches on peut trouver ce même genre de programmes en libre accès sur des blogs éphémères. Frustré de ne pas avoir obtenu une promotion, un employé peut ainsi se venger en infectant le réseau de son entreprise. Un ancien amant peut lui aussi se venger en espionnant le PC de son ex-compagne. Il peut ainsi récupérer le numéro et le code d'accès de sa carte bancaire afin de faire des achats sur Internet. Cette évolution inquiète de plus en plus les responsables de la sécurité informatique.

Mais le plus grand danger se situe au niveau des données personnelles. Selon Privacy Rights Clearinghouse, quelque 90 millions de personnes (pas uniquement américaines compte tenu de la mondialisation des réseaux informatiques) ont été victimes d'un vol d'identité aux États-Unis entre avril 2005 et juillet 2006. Selon cette ONG spécialisée dans les questions de sécurité de données sensibles, près de la moitié de ces pertes sont classables dans la colonne des « vols prémédités à fins d'exploitations nuisibles ». Il ne se passe plus un jour sans qu'on apprenne la « disparition » de l'ordinateur portable d'un cadre supérieur ou l'intrusion dans une entreprise. Fin août 2006, la boutique en ligne du géant américain des télécommunications AT&T a été piratée. Les fiches client (avec le numéro de carte de crédit) de plus de 19 000 personnes ont été dérobées.

Parfois, le travail des pirates est « facilité » par des entreprises. Début août 2006, AOL a divulgué par erreur les données personnelles de 650 000 abonnés.

L'avenir est plutôt sombre. Messagerie instantanée, téléphone IP, téléphones portables... Tous ces moyens de communication vont être, à plus ou moins brève échéance. Les particuliers et les entreprises doivent donc redoubler de vigilance car les différents logiciels de sécurité (antivirus, antispams, pare-feu...) ne peuvent pas garantir une sécurité à 100 %. Quoiqu'en disent certains éditeurs qui confondent marketing et efficacité.

En matière de sécurité informatique, le maillon faible est - et restera toujours - l'utilisateur. Les pirates le savent. Vous aussi vous en serez persuadé après avoir lu ce livre.



1

Internet : le nouveau filon des organisations criminelles

« Les braquages de fourgons blindés existeront toujours mais on ne peut pas en faire plusieurs dans la journée ou dans la semaine ! C'est le cas des attaques informatiques : on peut « automatiser » des opérations quotidiennes. Et en plus, le coût (en termes de moyens nécessaires à l'attaque et de risques juridiques et physiques) est moins élevé... ». Pour ce spécialiste très au fait de la cyberdélinquance, l'avenir apparaît donc comme une évidence : les hold-up virtuels vont augmenter.

Pour tous les experts que nous avons rencontrés, cette évolution est très récente. L'information est bien sûr très difficile à vérifier mais il semblerait que, pour la première fois en 2005, le montant des vols générés sur Internet soit supérieur à celui du trafic de biens réels. Selon les estimations des chercheurs de l'organisation Computer Economics, en 2004, le montant des pertes engendrées par ces différentes attaques était de presque 18 milliards de dollars.

L'époque des informaticiens qui créaient des virus dans leur chambre est révolue. Le développement des moyens de télécommunication et la très forte dépendance des entreprises, et de la société en général, ont favorisé l'émergence de la cybercriminalité. Ce terme regroupe trois types d'infraction différents :

- Les infractions relatives au **contenu** : diffusion intentionnelle sur le web de textes ou d'images illégaux (insultes à caractère raciste, xénophobe ou négationniste, pédopornographie...) ;
- L'atteinte à la **propriété intellectuelle** : mise en ligne de fichiers musicaux et vidéo gratuits sans l'accord des auteurs, vol d'un prototype d'appareil ou des codes d'un nouveau logiciel...



- Les infractions liées aux **technologies de l'information et de la communication** : diffusion de virus, vol de données personnelles, escroqueries en ligne...

En fait, dans la définition de la cybercriminalité, il est d'usage de considérer tout crime ou délit dans lequel l'ordinateur est soit le moyen, soit le but.

1.1 UNE EXPLOITATION PROFESSIONNELLE DE LA CYBERCRIMINALITÉ

Plusieurs signes tendent à confirmer cette tendance. « L'année 2003 était une année de virus ciblant notamment les banques. L'année 2004 a été marquée par des affaires de chantages afin d'extorquer des fonds. L'année 2005 me semble avoir été celle où de vraies connexions sont apparues entre criminalité hors l'Internet et cybercriminalité »¹ explique Pascal Lointier, président du Clusif, le Club de la sécurité des systèmes informatiques français.

Créer un virus pour « planter » un ordinateur n'a plus beaucoup d'intérêt. Sauf à prouver qu'on sait le faire. Ce qui intéresse les malfrats du net c'est l'efficacité. « Depuis moins de deux ans, nous sommes passés du crime informatique « ludique » — basé notamment sur le *proof-of-concept* (voir encadré ci-dessous) avec des hackers éthiques ou historiques (cherchant à montrer les faiblesses du système en général) — à une exploitation professionnelle de la cybercriminalité. La preuve : depuis Slammer, il n'y a plus de vagues de virus qui plantent tous les ordinateurs, nous explique Patrick Pailloux, directeur central de la sécurité des systèmes d'information. L'ère des attaques virales de masse est terminée. C'est le gain financier qui compte maintenant. »

Le « proof-of-concept »

Cette notion désigne un code conçu et réalisé dans le but de prouver qu'un risque donné et identifié est bien réel. Dans le domaine de la virologie, ce concept est fondamental. Il permet de prouver techniquement, selon une démarche scientifique avérée, qu'un risque existe. Il permet également de lutter contre les rumeurs, faux bruits et autres fantasmes. Ainsi, les « évolutions majeures » en virologie sont le fait d'auteurs qui ont publié des *proof-of-concept* (premier virus polymorphe, premier code métamorphe, premier virus pour téléphone portable...). Cette notion divise les opinions : alors que les éditeurs d'antivirus diabolisent systématiquement tous les auteurs de ce genre de codes, qu'ils soient chercheurs reconnus ou simple programmeurs — lesquels se contentent de les rendre publics sans les utiliser — le monde scientifique et universitaire considère cela comme relevant d'une démarche scientifique et intellectuelle rigoureuse. Le débat n'est pas près d'être clos.

1. Libération, 13/01/2006.



Publiée en avril 2006, la neuvième édition de l'*Internet Security Threat Report* de Symantec, le numéro 1 mondial de la sécurité, confirme en effet que les codes malveillants sont devenus des armes très ciblées et sophistiquées. Ce rapport, qui couvre la période du 1er juillet au 31 décembre 2005, fait état d'une nette augmentation du nombre de menaces conçues pour faciliter la cybercriminalité : « Alors que les attaques étaient auparavant conçues pour détruire les données, celles d'aujourd'hui visent davantage à voler discrètement les données, sans provoquer de dégâts notables qui avertiraient l'utilisateur ».

Types d'attaque ou de détournement identifiés ces 12 derniers mois
(par pourcentage de correspondants)

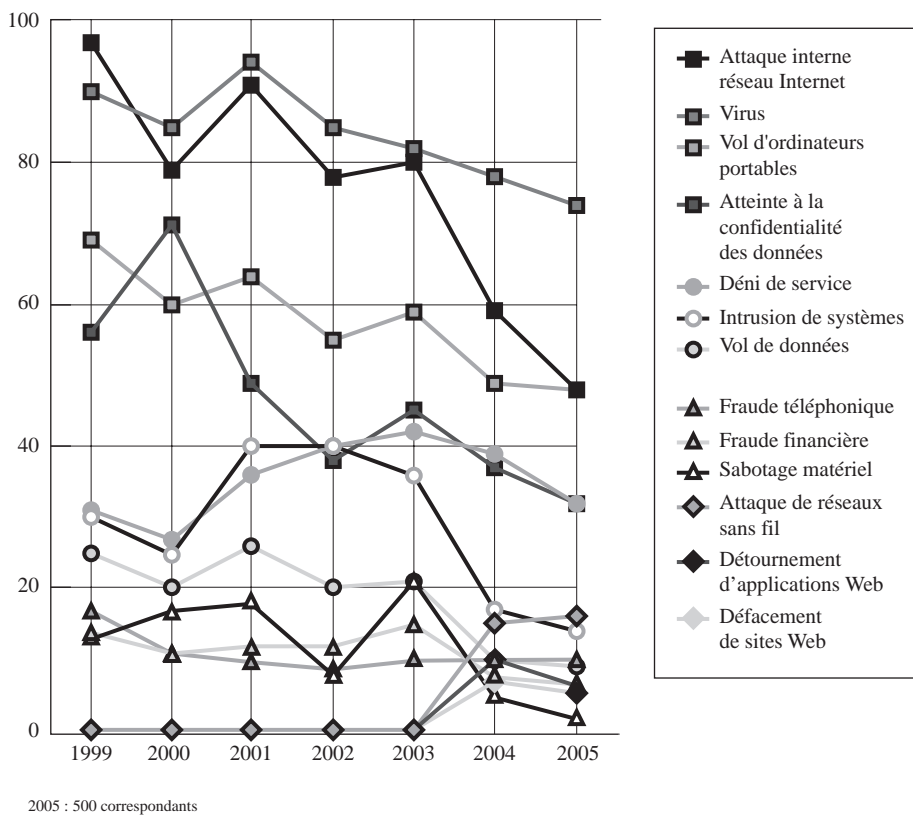


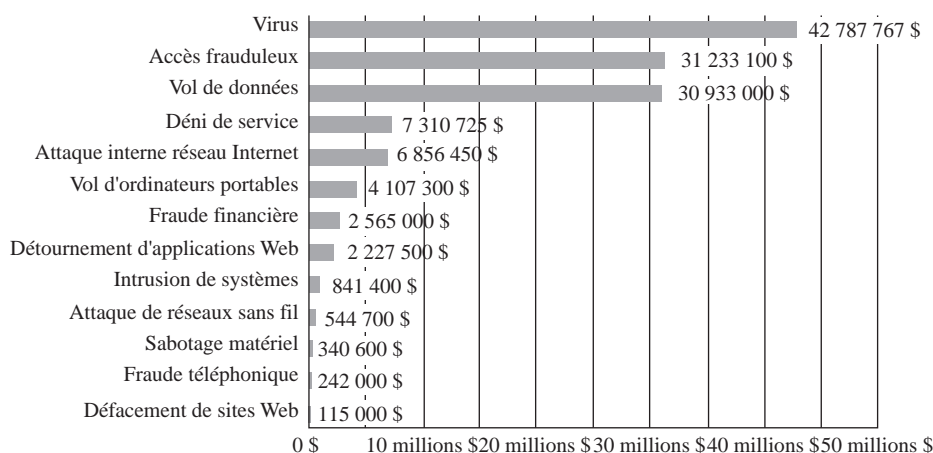
Figure 1.1 — La palette des codes malveillants devient de plus en plus large, la tendance étant à l'utilisation « d'armes » ciblées et sophistiquées.

Dans son précédent rapport (premier semestre 2005), Symantec signalait une progression des codes malicieux conçus à des fins financières. Cette tendance s'est maintenue tout au long du deuxième semestre 2005. « Les codes malicieux permettant d'accéder à des informations confidentielles représentent aujourd'hui 80 % des 50 principaux codes malicieux répertoriés, contre 74 % au cours du premier semestre 2005 ».

Autre constat selon Symantec : « le déclin notable des menaces de catégories 3 et 4 (modérées et extrêmement graves) et l'augmentation proportionnelle des menaces de catégories 1 et 2 (faibles et très faibles). Le nombre de nouvelles familles de virus **Win32** a lui aussi baissé de 39 % (de 170 nouvelles familles au cours du premier semestre 2005, à 104 au cours du deuxième semestre). Les codes dits Win32 sont des codes exécutables écrits pour les plateformes Windows nouvelle génération fonctionnant en 32 bits (depuis W95 et NT).

Ces chiffres semblent indiquer que les développeurs de codes malicieux préfèrent modifier le code source déjà en circulation plutôt que de créer de toutes pièces de nouvelles menaces ».

Coût financier total par type d'attaques en dollars



Pour 2005, le total des pertes s'est élevé à 130.104.542 \$

Figure 1.2 — Malgré une protection accrue (antivirus, firewall...) les dégâts occasionnés par les codes malveillants ne cessent d'augmenter.

Les organisations criminelles qui sévissent sur Internet seraient donc entrées dans une logique économique qui consiste à minimiser les coûts de fabrication (en l'occurrence des codes malveillants) pour optimiser leur forfait... Pour atteindre cet objectif, elles s'engouffrent dans les différents maillons faibles de la sécurité informatique (voir chapitre 2) et les limites intrinsèques aux antivirus (chapitre 11). Des *hackers* ont même mis sur pied des sites e-commerce proposant des « exploits »¹ privés capables de contourner ces logiciels de sécurité.

Encore plus surprenant, deux sites vendaient des chevaux de Troie indétectables par les antivirus conventionnels. Fermés il y a quelques mois, ils permettaient à qui-

1. Tout ou partie d'un code permettant d'utiliser une vulnérabilité ou un ensemble de vulnérabilités d'un logiciel (système ou application) à des fins malveillantes. Source : CERTA.

Petite annonce : « A louer bataillon de robots »

Rien à voir avec de la science-fiction : pour les spécialistes en sécurité informatique, ces robots-là sont devenus une vraie plaie. L'ennemi public à abattre. Ces robots sont en réalité les ordinateurs de monsieur-tout-le-monde ou d'entreprises dont des pirates ont pris le contrôle. A l'insu de leur utilisateur ! C'est ce qu'on appelle des « PC zombies » ou « **botnet** ». Selon l'éditeur d'antivirus McAfee, il y a « aujourd'hui dans le monde entre 4 et 6 millions de machines infectées ».

Après avoir placé un programme malveillant, le pirate peut commander à distance n'importe quelle fonctionnalité : il peut ouvrir le lecteur DVD, lancer un traitement de texte, brouiller l'écran... Mais son but n'est pas de se divertir ou d'épater la galerie. En prenant le contrôle d'une machine il cherche à masquer ses traces sur la toile et à augmenter sa puissance de feu. Car son objectif principal est d'attaquer une entreprise ou un site en saturant son serveur. Dans ce cas, la victime ne peut plus rien faire car elle est justement dépendante de l'informatique et du développement des connexions Internet permanentes. C'est ce qu'on appelle une « attaque en déni de service » ou **DDoS** (Distributed denial of service). Une arme redoutable : « un botnet de 20 éléments peut suffire à mettre off line un site », avertit Lionel Morer, responsable du pôle conseil et audit en sécurité chez Bull. Une arme d'autant plus efficace qu'elle n'est pas chère : selon le Clusif (Club de la Sécurité des Systèmes d'Information Français), un réseau de 500 robots peut se louer 380 euros. L'accès exclusif à une seule machine zombie peut se négocier à partir de 0,35 euro par utilisation. Enfin, une attaque DDoS peut se « vendre » entre 38 et 750 euros.

conque de concevoir son propre programme malveillant en sélectionnant ses caractéristiques, en particulier l'établissement financier ou bancaire auquel il devait s'attaquer. D'après l'éditeur d'antivirus Panda Software, qui a repéré ces deux magasins un peu particuliers, les clients recevaient également des outils de surveillance et de récupération de données leur permettant d'obtenir des informations détaillées sur les PC infectés, notamment des mots de passe.

Ce développement de la cyberdélinquance signifie-t-il que les mafias ont trouvé avec le web un nouveau terrain à conquérir ? Certains experts que nous avons rencontrés relativisent, pour l'instant, cette menace. Des mafias ont bien développé des « branches » Internet mais elles sévissent surtout en Asie et en Russie. La majorité des attaques proviennent principalement des États-Unis puisque le « hit parade » des pays pirates émetteurs de virus et autres codes malveillants s'établit comme suit : USA, Chine, Nigeria, Allemagne, Russie et Roumanie.

L'Internet n'est donc pas encore victime d'une pandémie due à la propagation de codes malveillants. Mais la situation ne devrait pas s'améliorer. Ces organisations criminelles font en effet appel à des informaticiens chevronnés qui sont organisés en commandos spécialisés. « Certains sont chargés d'écrire les codes. D'autres de les propager. D'autres encore d'effectuer des transferts d'argent, etc. »¹ explique Eugène Kaspersky, un ancien du KGB qui a créé l'éditeur d'antivirus Kaspersky. Et pour ne



Guerre des gangs sur Internet

Le milieu du piratage informatique n'est pas un long fleuve tranquille. Selon Yuri Mashevsky, analyste chez Kaspersky, il y aurait des chasses gardées : « Certains utilisent des programmes malicieux qui détruisent les autres logiciels développés par les groupes rivaux ». Autre exemple : des confrontations en ligne pour prendre le contrôle d'ordinateurs infectés appartenant à une autre bande.

rien arranger, les pirates utilisent différentes techniques permettant de brouiller les pistes (techniques d'anonymisation, implications de plusieurs pays pour faire s'opposer les différentes législations, sociétés écrans...) afin de rendre plus compliquées les enquêtes des autorités compétentes. Cette guérilla numérique est d'autant plus difficile à repérer et à démanteler que « ces équipes sont éclatées sur plusieurs continents », précise Eugène Kaspersky.

1.2 DES PERTES ESTIMÉES EN MILLION D'EUROS

Les principales victimes sont les entreprises et les organismes financiers car ils détiennent différents « trésors » : fichiers clients avec des données plus ou moins personnelles, dossiers confidentiels sur des projets et prototypes, forte dépendance aux moyens de communication (et notamment d'Internet), etc.

Publié en août 2005, le rapport *IBM Global Business Security Index* indique qu'il y a eu 237 millions d'attaques virales et informatiques lancées dans le monde... durant le premier semestre 2005. Un peu plus de la moitié (137 millions) se sont concentrées sur quatre domaines : les sites gouvernementaux, les services financiers, les constructeurs (tous domaines confondus) et les industries de la santé. Pour évaluer cette situation, le géant de l'informatique a interrogé 2 700 professionnels de la sécurité et s'est appuyé sur les enregistrements et statistiques fournis par 500 000 outils de surveillance dans le monde.

La principale cible reste les agences gouvernementales avec un peu plus de 50 millions d'attaques lors des six premiers mois 2005. Viennent ensuite le secteur industriel (36 millions) et la finance (34 millions). Les États-Unis ne sont pas un paradis pour les entreprises puisque c'est dans ce pays qu'a lieu la majorité (12 millions) des opérations menées par des bandes criminelles ou des individus. Les deux autres pays les plus touchés le sont beaucoup moins : la Nouvelle Zélande (1,2 million) et la Chine (1 million).

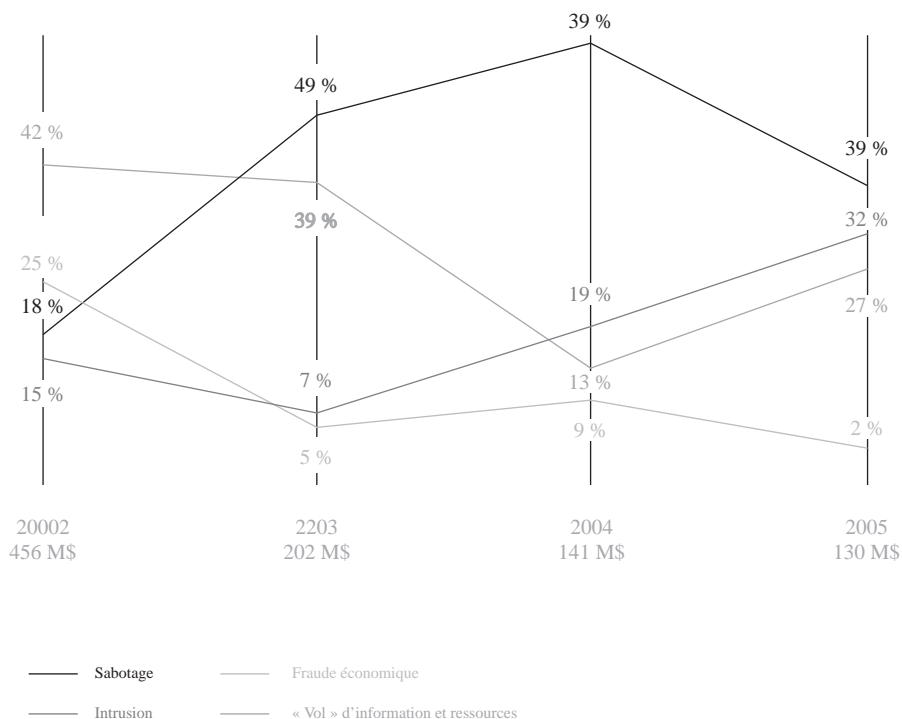
La cyberdélinquance a donc un impact sur l'économie des entreprises. Dans la dixième édition de son étude (réalisée avec la participation du bureau de San Francisco du FBI) le *Computer Security Institute* (CSI) ne se montre pas optimiste. Basé sur les réponses fournies par 700 responsables de la sécurité au sein d'entreprises,

1. Libération. 11/02/2006.



d'agences gouvernementales, d'universités et de différentes institutions, ce rapport ¹ chiffre à environ 130 millions de dollars le montant des pertes en 2005.

Pertes économiques par type de cyber-risques



Source Comprendre et Réussir à partir des chiffres du CSI

Figure 1.3 – Les attaques informatiques deviennent un vrai fléau

Les entreprises ne sont pas les seules victimes. Les particuliers paient aussi un lourd tribut à cette avalanche de codes malveillants. Une enquête réalisée, auprès de 3 200 foyers américains équipés d'une connexion Internet, par l'association de défense des consommateurs Consumer Reports évalue à 9 milliards de dollars le montant des frais occasionnés, dans 61 % des cas, par un virus. Le coût moyen de la remise en état de marche de l'ordinateur serait de 300 dollars. La cybercriminalité aurait même été à l'origine de près de 8 % des ventes d'ordinateurs... Et ne parlons pas de l'envolée du marché des logiciels de sécurité (voir le chapitre 11). Selon cette enquête, les consommateurs américains ont investi 2,6 milliards de dollars dans l'achat de ces logiciels entre 2003 et 2004. Ce marché devrait encore se développer

1. Rapport « Computer Crime and Security Survey » disponible sur : www.gocsi.com.

puisque 17 % des Américains interrogés n'ont pas encore installé d'antivirus et 10 % naviguent sur Internet sans pare-feu (firewall). L'enquête ne dit pas, par contre, combien de foyers équipés des logiciels de sécurité oublient de les mettre à jour régulièrement et d'installer les mises à jour de sécurité de Windows et autre...

En France, les statistiques sur l'équipement en logiciels de sécurité sont rares. Mais les entreprises et les particuliers semblent, pour l'instant, relativement épargnés par le cybercrime. Plusieurs raisons peuvent, en partie, expliquer cette situation. L'informatique étant en anglais, il faut maîtriser cette langue pour créer des codes. Cette raison devient bien sûr de moins en moins valable au fur et à mesure que cette langue devient courante. Les deux autres facteurs sont premièrement l'absence de Milieu depuis les années 70, à part quelques poches à Marseille et Grenoble par exemple, et deuxièmement le fait qu'il n'y ait pas encore de spécialistes de l'Internet chez les voyous ».

Cela ne signifie pas pour autant que l'Hexagone n'a pas connu d'affaires de cyberdélinquance. Dans un discours tenu en mai 2000 lors d'une importante réunion d'experts du G8, Jean-Pierre Chevènement, alors ministre de l'Intérieur, indiquait : « nos services ont recensé en 1999 plus de 2 500 affaires impliquant d'une manière ou d'une autre Internet ». La situation ne s'est pas améliorée selon notre enquête. Quelques réseaux très organisés ont été démantelés en 2005. L'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication) a par exemple arrêté six personnes qui sont soupçonnées d'avoir effectué des virements frauduleux après avoir accédé aux comptes de clients d'Axa Banque. « Utilisées comme « mules », elles détournaient l'argent sur leur propre compte avant de le transférer via Western Union vers un compte en Ukraine, moyennant une commission de 10 % » explique Marie Lajus, adjointe au chef de l'office¹.

« En 2005, nous avons arrêté des personnes de l'Est qui effectuaient des achats sur Internet avec des fausses cartes bancaires et des identités trafiquées, déclare Yves Crespín, chef de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI). La personne réceptionnait la marchandise à l'hôtel. Lors de son arrestation, nous avons appris qu'elle « travaillait » pour un couple de Biélorusses qui se trouvait en France depuis quelques semaines. Après avoir monté un piège pour les arrêter nous avons découvert que leur domicile ressemblait à une caverne d'Ali Baba spécialisée dans les produits high-tech. Ce couple fait partie d'une bande très organisée qui envoie des équipes dans plusieurs pays européens. Avant de partir pour un pays, chaque bande reçoit des cartes bancaires ainsi que des papiers d'identité et une liste précise d'achats à effectuer sur certains sites de commerce électronique ».

D'autres affaires sont en cours. Mais il est très difficile de faire une estimation juste de ce genre d'affaire. « Cette délinquance ne fait pas l'objet d'une analyse précise », explique un expert. « Le « chiffre noir » (infractions commises mais non portées à la connaissance des forces de police ou de gendarmerie) est particulière-

1. *L'Expansion*. Novembre 2005.



ment important et les outils statistiques utilisés ne sont toujours pas adaptés.»¹ Selon Yves Crespin, « 90 % de la cybercriminalité nous échappe ».

Le commissaire Marie Lajus précise que « de nombreuses entreprises victimes de ce type d'attaques ne font pas appel aux services de police. Pour différentes raisons. Premièrement, elles connaissent mal les capacités des services de police qui ont pourtant de vraies compétences dans ce domaine. Deuxièmement, plusieurs de ces entreprises vivent grâce à la confiance que leur prêtent leurs clients sur Internet. Porter à la connaissance de tout le monde la réalité d'une vulnérabilité n'est pas bon pour l'image. Or, porter plainte ne signifie pas pour autant rendre publique cette affaire. Nous pouvons travailler de façon discrète et c'est un moyen efficace pour que ça ne se reproduise pas. »

Une autre raison, moins officielle, explique le décalage entre la réalité et le nombre de faits constatés. « Le parquet va être amené à classer de nombreuses affaires à cause d'une nouvelle loi d'orientation, explique un spécialiste. S'il reçoit une plainte et s'il estime que le coût des préjudices est inférieur à celui des réquisitions, il peut décider de classer l'affaire. Cela arrive de plus en plus souvent. »

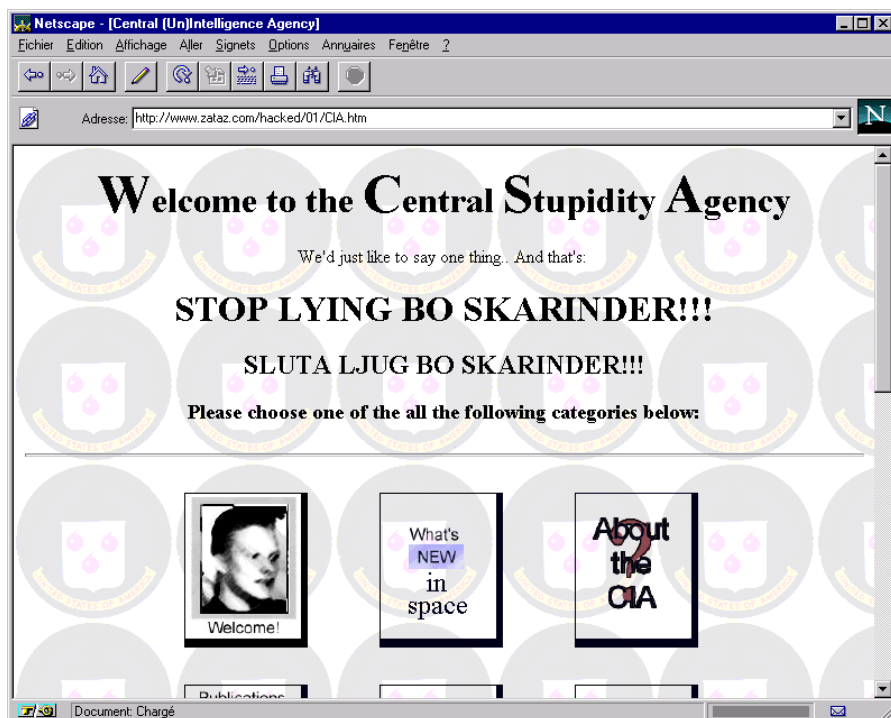
Le hooliganisme version numérique

En janvier 2006, la police a arrêté un *hacker* français de 25 ans spécialisé dans le **defacement**. Cette technique appelée aussi « tag numérique » consiste à s'introduire sur un serveur et à modifier les pages web de différents sites français (de commerce électronique, d'hommes politiques et de conseils régionaux). A son palmarès : 1 200 opérations. Pour le plaisir. Repérés depuis quelque temps, les faits et gestes de cet individu étaient suivis en permanence. Au moment de l'affaire des caricatures de Mahomet, « son attitude a radicalement changé », explique un policier. D'origine musulmane, il décide de signer ces actes sous le pseudonyme de « Oussama Ben » et non plus sous son surnom habituel et de viser des sites danois et britanniques. Lors de ses nouvelles attaques, il place sur les pages d'accueil des images des soldats américains décapités. Lors de son arrestation, les policiers sont surpris par son équipement informatique très rudimentaire. « Vivant chez sa sœur et maîtrisant un peu l'informatique, c'est le prototype de hacker qui commence à poser des problèmes. Son seul but : embêter le monde », constate un policier.

C'est bien sûr aux États-Unis que les arrestations sont les plus nombreuses. Début 2006, un Californien a plaidé coupable lors de son procès devant une cour fédérale américaine. Il était accusé de s'être servi d'une armée de 400 000 PC infectés (dont certains appartenaient au département de la Défense...) pour endommager des systèmes (attaques DDoS), lancer des *spams* et installer des logiciels espions (*spywares* et *keyloggers*) sur des systèmes. Il louait aussi ses PC zombies à des pirates et à des

1. Source : « Chantier sur la lutte contre la cybercriminalité ». Rapport présenté par Thierry Breton. Février 2005.





Figures 1.4 et 1.5 — N'importe quel site peut être victime d'un defacement. Ici celui de France Telecom et de la CIA.



spammeurs. Agé d'une vingtaine d'années, il ferait partie du groupe Botmaster Underground démantelé en novembre 2005. Ses revenus illicites auraient atteint les 60 000 dollars. De quoi s'offrir le modèle haut de gamme d'une célèbre marque de voiture allemande qu'il affectionnait plus que tout. Mais il a été condamné à 57 mois de prison ferme.

Autre exemple, aux Pays-Bas. L'année dernière, trois jeunes Hollandais ont été arrêtés. A la tête d'une armée de 100 000 PC zombies, ils ont volé des milliers de codes bancaires et des mots de passe. Ils ont menacé des entreprises. « Si elles ne voulaient pas payer la rançon, ils sabotaient tout leur réseau », explique Taco Stein, substitut du procureur à Amsterdam.

Ces quelques exemples ne reflètent pas la réalité. On n'arrête que les « seconds couteaux » estiment des experts. Ou des illuminés comme Gary McKinnon. Accusé d'avoir causé plus de 700 000 dollars de dommages dans le système informatique du Pentagone, de l'US Navy et de la NASA, cet Anglais de 40 ans a été arrêté en 2002 par Scotland Yard. S'il est extradé pour être jugé aux Etats-Unis, il risque un maximum de 70 ans de prison, assortis de 1,75 million de dollars d'amende. Son avocat affirme même craindre que l'anglais ne soit envoyé dans la base de Guantanamo Bay, la zone américaine de l'île de Cuba. Sa défense était très originale : il enquêtait sur les Ovnis. « J'ai utilisé des logiciels disponibles sur le marché pour scanner les plus grands réseaux américains, tous ceux susceptibles de contenir des informations à propos des Ovnis. Je voulais juste prendre connaissance de choses que le gouvernement ne nous aurait pas communiquées. »

En résumé

L'époque du pirate en chambre est révolue. La création de virus visant simplement à prouver ses compétences n'est plus d'actualité. Aujourd'hui, des organisations criminelles, ou des individus, ont pris le relais et mènent des attaques de plus en plus sophistiquées (et donc de plus en plus difficilement détectables) et ciblées sur les entreprises. Dernier maillon de la chaîne, le particulier paie aussi un lourd tribut à cette expansion de la cybercriminalité.



Creative Commons BY-NC-ND



2

Les maillons faibles de la sécurité informatique

En matière de sécurité, quel que soit le domaine considéré, la cause des problèmes relève toujours de deux aspects qui peuvent intervenir séparément ou simultanément :

- Une erreur, volontaire ou non de l'utilisateur ;
- Un défaut dans le système concerné, soit au niveau de l'outil lui-même, soit au niveau de la fonctionnalité mise en œuvre par cet outil (le protocole).

Pour illustrer ce constat, prenons un exemple de la vie quotidienne, celui de la conduite automobile. Quelles peuvent être les causes d'un accident ?

- Une mauvaise « conduite » du conducteur, provoquée par l'environnement (la publicité par exemple), par une tendance naturelle (laxisme, indiscipline...) ou par des contraintes diverses telles le manque de temps ;
- Un défaut d'entretien du véhicule (assimilable au système informatique) ;
- Le mauvais état ou la mauvaise conception des routes et de la signalisation (assimilable au protocole).

Il est intéressant de remarquer que ces trois causes sont classées par ordre décroissant de probabilité de réalisation, les accidents étant plus souvent engendrés par la faute directe des usagers que par le mauvais état des routes. Cet exemple s'applique parfaitement au domaine de la sécurité informatique et les causes d'accidents sur nos routes sont transposables sur les « autoroutes de l'information ».

2.1 L'INTERNAUTE ET L'INGÉNIERIE SOCIALE

Un mauvais comportement de la part de l'internaute a toujours deux causes possibles :

- Ses dispositions « naturelles » au laxisme et à la facilité qui, entre plusieurs alternatives, lui font très souvent choisir le moindre effort ;
- Son attirance tout aussi « naturelle » pour certaines choses (pornographie, jeux, sports...).

Mais ces comportements ne sont mauvais dans l'absolu que parce qu'il existe un autre acteur important dans toute attaque : le pirate, le hacker, l'escroc... Bref, celui que nous nommerons le malfaisant informatique. Pour atteindre sa cible, il va déployer une stratégie très efficace : mettre à son profit les mauvaises habitudes des usagers pour les transformer en comportements dangereux pour la sécurité informatique. C'est que l'on appelle l'*ingénierie sociale*¹.

2.1.1 L'ingénierie sociale

Parmi les nombreuses définitions, plus ou moins précises, de l'expression « ingénierie sociale » nous adopterons la suivante : ensemble des techniques de manipulation psychologique ou d'exploitation comportementale d'un individu, ou d'un groupe d'individus, par des personnes malfaisantes dont le but est l'incitation inconsciente à amoindrir, contourner ou supprimer les mesures de sécurité d'un système par ce ou ces individus.

La sécurité des systèmes d'information repose sur les trois piliers suivants :

- **La confidentialité** : les informations ne doivent être accessibles qu'aux seules personnes autorisées ou habilitées. Un mot de passe ou un code de carte bancaire sont les meilleurs exemples d'informations confidentielles ;
- **L'intégrité** : les informations (un fichier système par exemple) ne doivent être modifiées que par une action légitime et volontaire ;
- **La disponibilité** : le système doit répondre aux sollicitations des utilisateurs autorisés (accès aux informations, action particulière...) dans le délai imparti par le cahier des charges, propre à chaque application et/ou système.

L'attaquant a alors deux axes d'approche pour tenter de porter atteinte à la sécurité du système considéré : soit il en vise directement les éléments techniques (exploitation de failles, de la mauvaise gestion, de mauvaises configurations... — cet aspect-là sera développé plus loin dans ce chapitre), soit il s'attaque directement à l'utilisateur ou à l'administrateur pour l'amener à effectuer certaines actions lui permettant de porter atteinte au système. En clair, le pirate peut soit exploiter un « bug » déjà présent,

1. E. Filiol : « L'ingénierie sociale ». *Linux Magazine* 42, 2002.



soit transformer l'élément humain lui-même en « bug ». Dernière alternative : utiliser les travers de l'utilisateur pour le transformer en « code malveillant ».

L'attaquant dispose de plusieurs moyens pour modifier le comportement de l'utilisateur :

- **L'usurpation d'identité** : le but est de se faire passer auprès de l'utilisateur cible pour une personne ou une entité connue et/ou identifiée comme appartenant bien à un groupe autorisé et dépositaire d'une légitimité certaine dans la politique de sécurité de l'organisme ou auprès de l'utilisateur. C'est l'une des techniques employées lors d'attaques de **phishing** (voir chapitres 4 et 5) : l'internaute reçoit un e-mail venant soi-disant de sa banque qui lui demande — sous le prétexte d'une mise à jour de sécurité — de cliquer sur un lien Internet pour redonner son identifiant et son mot de passe. Dans ce premier cas, il y a toujours défaut d'identification et/ou d'authentification. Le résultat est, au minimum, une atteinte à tout ou partie de la confidentialité du système ;

Les fausses mises à jour de sécurité

Les banques et autres organismes financiers ne sont pas les seules victimes de l'usurpation. Il y a aussi Microsoft. Des pirates ont en effet envoyé des e-mails provenant soit disant de cet éditeur. Sous un prétexte de mise à jour logicielle, ils demandaient aux internautes d'ouvrir la pièce jointe ou de cliquer sur un *lien* URL. Évidemment, le colis était piégé et contenait un virus ou un cheval de Troie.

Autre victime : les éditeurs d'antivirus. En avril 2006, un e-mail malveillant a usurpé l'identité de Symantec, l'éditeur des solutions antivirales Norton. En lisant ce courrier, l'internaute apprend que son PC est soi-disant infecté par le virus « w32.aplore@mm ». En cliquant sur le lien URL pour désinfecter son système, la personne déclenche le téléchargement d'un programme qui empêche les mises à jour des logiciels anti-virus.

- **La manipulation psychologique** : il s'agit d'exploiter diverses « faiblesses » ou « tendances » psychologiques de la victime en particulier et/ou humaines en général : manque d'affection, bons sentiments, ego, appât de gains faciles, manque de bon sens, de perspicacité, de prudence, laxisme, manque de conscience professionnelle, « penchants spécifiques »... La gamme de ces faiblesses (il n'y a pas ici de jugement de valeur, seules les conséquences en terme de sécurité étant considérées) est vaste et l'imagination sans limite des attaquants en révèle régulièrement de nouvelles ;
- **L'exploitation du manque de connaissances** : la méconnaissance technique de la plupart des utilisateurs, voire de certains administrateurs, le manque de formation continue (veille technologique), de sensibilisation régulière sont directement exploités par l'attaquant pour parvenir à ses fins. Bien souvent, la crédulité des utilisateurs amplifie les choses. L'utilisation de canulars (**hoax** en anglais) est l'un des moyens les plus connus.



Trois types d'attaquants

Il peut s'agir du simple pirate qui inspiré par la bêtise, une volonté de nuisance ou l'appât du gain. Autre profil : des groupes très bien organisés, d'inspiration mafieuse ou étatique étrangère. Il y a enfin des sociétés spécialisées dans le renseignement ou la guerre économique qui agissent le plus souvent pour des sociétés concurrentes de celle attaquée¹. Mais, dans tous les cas, l'ingénierie sociale est simplement une forme nouvelle d'escroquerie et à ce titre, ne doit susciter ni admiration ni sympathie.

2.1.2 La phase de renseignements

Dans presque tous les cas, et toujours dans l'attaque ciblée d'individus ou de groupes d'individus, l'assaillant procède d'abord à une collecte de renseignements, même minimale — qui souvent se limite à une bonne expérience du facteur humain. Elle lui permet d'optimiser son attaque. Les différentes informations qu'il obtient lui indiquent alors comment « traiter » au mieux sa victime.

Cette étape est cruciale. Aucun pirate « sérieux » ne saurait s'en dispenser, que ce soit pour une attaque classique ou une attaque par ingénierie sociale. Bien sûr, dans le cas des attaques « grand public », ce renseignement est collecté et se limite à quelques éléments génériques. Dans ce cas, l'attaquant est simplement à la fois un fin psychologue, un bon sociologue et dans une certaine mesure un bon « ethnologue ». Mais dans une attaque ciblée, la phase de renseignements peut être longue et complexe. Mais elle détermine le succès de l'opération. Dans notre cas, le but est d'obtenir suffisamment d'informations pour parvenir à convaincre la future victime de la légitimité de ce qui va lui être demandé (données à fournir ou action à accomplir).

L'expérience prouve (et les cas sont malheureusement nombreux) que bien souvent la tâche de l'attaquant se trouve facilitée par la ou les futures victimes elles-mêmes. De trop nombreuses entreprises ou administrations font encore preuve d'un incroyable manque de prudence. Leurs personnels ne sont pas suffisamment sensibilisés aux risques de compromission d'informations concernant leur société. Ces informations, qui d'ailleurs leur semblent assez souvent anodines, permettront au pirate, notamment par compilation et recoupement, d'être efficace.

Les informations recherchées sont principalement les suivantes :

- **Tout ou partie de l'organigramme** de la société et de son activité (noms, coordonnées, dossiers traités ou en cours...).
- **Informations techniques sur la société** : plan d'adressage, matériels et logiciels utilisés, procédures, noms des responsables...
- **Données annexes** : prestataires extérieurs (maintenance, nettoyage, fournisseurs...) ou intérimaires (personnels, stagiaires), informations non techniques concernant les personnels de l'entreprise...

1. La guerre de l'information, Le journal de la sécurité MISC 3, page 18-23.



- **Mots de passe et noms de login** : aussi incroyable que cela puisse paraître, encore trop de personnes — et même des « professionnels » — donnent par téléphone ou par e-mail leur code de carte bancaire ou leur mot de passe informatique ! Plusieurs études l'ont démontré. Lors du colloque Infosecurity Europe 2004, organisé à Londres, une expérience a été menée à l'entrée d'une station de métro. Une personne accostait les usagers de la façon suivante : « Je vous offre cette barre chocolatée si vous acceptez de me révéler le mot de passe que vous utilisez pour vous connecter à Internet ». Sept personnes sur dix ont craqué pour la friandise. Ce petit test n'a évidemment pas une portée scientifique puisqu'il n'a concerné que 172 personnes. Mais il reste néanmoins intéressant. L'analyse de l'attaque opérée en 1999 contre l'hébergeur français Multimania est plus significative puisqu'elle a occasionné la publication de 70 000 mots de passe. Elle va rassurer les pirates car le mot de passe qui décroche la première marche du podium est... «123456». Sur les deux autres marches il y a « azerty » et « Nicolas » !

Les principaux moyens utilisés par les attaquants pour découvrir les mots de passe sont les suivants :

- **Consultation de différents fichiers** : annuaires, pages web personnelles, panneaux d'affichage dans les halls d'accueil, bases de données en ligne, informations publiques concernant le système, recherche sur Internet, annuaires d'anciens élèves d'écoles d'ingénieurs, offres publiques de marché...
- **Analyse des rebuts** : expérience personnelle à l'appui, nous avons pu constater à plusieurs reprises que les poubelles étaient de véritables mines d'informations. Les personnels — et futures victimes — jettent dans leur corbeille les papiers, brouillons, post-it (quelquefois celui sur lequel est inscrit le mot de passe !), dossiers... Ils ne se doutent pas que, bien souvent, ces corbeilles sont vidées dans une poubelle plus grande qui se retrouve sur le trottoir à la disposition de l'attaquant. Combien d'entreprises en sont conscientes ? « Certains présidents de grandes entreprises, conscients de ce risque, écrivent leurs notes administratives sur des brouillons qui passent ensuite dans un broyeur tandis que d'autres, moins prudents, les tapent sur un ordinateur portable ou un PDA connecté à Internet », nous révèle Patrick Pailloux, directeur central de la sécurité des systèmes d'information.
- **Utilisation de logiciels spécialisés dans la collecte de renseignements techniques sur votre environnement informatique** : ils sont nombreux et redoutables. Pour vous faire une petite idée, allez sur le site de la CNIL¹ et vous pourrez constater comment, en un clic de souris, il est possible, de l'extérieur, d'obtenir des informations techniques sur votre propre ordinateur. Et les informations retournées par ce lien sur le site de la CNIL, à des fins de sensibilisation, ne représente qu'une infime partie de ce qu'il est possible de collecter.

1. <http://www.cnil.fr/traces/index.htm>



- **Visite des locaux** : lors de visites d'entreprises, un futur attaquant peut glaner beaucoup trop d'informations. Si une visite n'est pas possible, il peut se faire passer pour un prestataire de service ou un personnel de maintenance. En période de vacances, cela marche encore mieux, les personnels intérimaires pouvant se faire abuser plus facilement.
- **Observation à distance de moniteurs** : promenez-vous près de certaines sociétés ou de certains ministères, et comptez le nombre d'ordinateurs dont l'écran est tourné vers l'extérieur. Vous serez surpris. Le nombre d'ingénieurs ou de décideurs offrant à la vue de quiconque son ordinateur portable dans les lieux publics (le train par exemple) est un autre exemple de mines d'informations techniques rentables.

Mais le plus redoutable est l'indiscrétion quasi malade des personnes vis-à-vis de l'extérieur. Beaucoup d'ingénieurs ou de décideurs connaissent une « baisse de vigilance » devant la jolie fille sur le stand d'un salon ou assise à quelques places d'eux dans un train. Et cet ingénieur de faire le paon — verbalement du moins — pour épater la galerie. Pour étayer ce propos, nous prendrons un exemple réel qui, malheureusement, s'observe fréquemment. Lors d'un voyage en TGV entre Rennes et Paris, deux professionnels de l'informatique discutaient « boulot ». En moins de deux heures, entre l'observation de leur ordinateur portable et l'écoute de leur conversation, nous en avons appris suffisamment sur leur entreprise, son environnement sociologique et son environnement informatique pour potentiellement mener une attaque par ingénierie sociale : logiciels utilisés, habitudes, penchants et « travers » de l'administrateur système, nom du directeur technique, informations sur des dossiers commerciaux en cours... Et si la jolie blonde qui leur faisait face — et qui était la cible involontaire de leurs propos hâbleurs — avait été un pirate informatique ou la complice d'un hacker assis plus loin, leur entreprise aurait pu payer un prix très élevé pour leurs fanfaronnades verbales.

Autre exemple ahurissant : un ingénieur commercial a communiqué son mot de passe et son login par téléphone à sa secrétaire (les mobiles étant d'ailleurs une aubaine pour les attaquants) et discuté avec elle d'un dossier d'un client, avec force détails. Le TGV ou autres transports en commun, mais aussi le café et le restaurant (où les personnels d'une entreprise ou d'une administration ont l'habitude de se retrouver) sont des lieux propices pour la collecte d'informations.

Une autre approche, plus active, consiste à discuter de façon anodine avec des personnels de la société visée (la standardiste, une secrétaire...). Il est toujours très intéressant de savoir que l'administrateur système est un mordu de jeux ou est particulièrement sensible à la gent féminine.... Et pourtant, ce ne sont pas des informations techniques !

La ruse et l'inventivité des attaquants d'un côté, la crédulité ou le manque coupable de professionnalisme et de sérieux des utilisateurs d'un autre côté, montrent régulièrement que la liste précédente n'est malheureusement pas exhaustive.



2.1.3 Quelques exemples

Une usurpation d'identité

Il provient d'une attaque réelle menée contre une société dont nous tairons l'identité. Par discrétion sur cette affaire, nous avons volontairement modifié quelques points essentiels. L'attaque s'est déroulée selon le scénario suivant. Lors de la phase de renseignements, les attaquants étaient parvenus à recueillir des informations : noms, coordonnées, dossiers traités et renseignements divers (habitudes, anecdotes récentes...) de plusieurs ingénieurs commerciaux, du directeur technique et des administrateurs systèmes. Ils avaient aussi collecté des informations relativement détaillées (dates, lieux, personnes impliquées...) sur la négociation en cours d'un contrat très important. La plupart de ces renseignements avaient été obtenus sans grande difficulté, notamment par les indiscretions (involontaires) en milieu « ouvert » de certains employés.

Simultanément à une réunion chez le gros client, le pirate mène son attaque. Il téléphone à l'administrateur système, en se faisant passer pour l'ingénieur commercial responsable de la négociation. Feignant la panique, il déclare qu'il ne parvient pas à se connecter sur l'ordinateur de la société à partir de son PC portable malgré des essais répétés : son mot de passe est constamment refusé. Il affirme, avec force effets de persuasion et détails sur le contrat et la négociation en cours, qu'il est vital pour lui de se connecter afin de fournir des informations au client, sans quoi le contrat risque d'être remis en cause, voire annulé. Bien sûr, les informations en question ne sont accessibles qu'à partir de son compte !

Au final, grâce à de nombreux détails convaincants et avec beaucoup de persuasion (où alternent pêle-mêle l'appel à la solidarité, la menace de reporter la faute d'un éventuel échec sur l'administrateur système ou le risque pour la société), l'administrateur accepte de changer le mot de passe en le remplaçant par un autre, constitué par une information commune aux deux (en l'occurrence le prénom de la secrétaire), discrétion au téléphone oblige ! Bien sûr, l'attaquant assure que par mesure de précaution, il va immédiatement mettre un mot de passe plus robuste.

Que dire de la grave faute commise par cet administrateur système ? Rien sinon qu'elle a permis à l'attaquant de s'introduire sur le réseau de cette entreprise, selon le principe de mutuelle confiance et de dérober en très peu de temps de nombreuses informations et notamment une partie de la base clients.

Des manipulations psychologiques

L'exploitation de penchants spécifiques

L'approche s'appuie sur le fait qu'un utilisateur (information ciblée obtenue durant la phase de renseignement) est attiré par un domaine particulier : les échecs, certains types de jeux, la musique... L'attaquant peut aussi exploiter des sentiments ou réflexes généralement répandus : solidarité, pitié, amour (le plus bel exemple est le ver IloveYou, en 2000), amitié, humour (exécutable humoristiques ; nombreux



sont les utilisateurs qui ont envoyé à leurs collègues, sur le réseau d'entreprise le petit jeu de massacre où la cible n'est autre qu'un Ben Laden apparaissant aléatoirement, des cartes de vœux électroniques ou des diaporamas Power Point humoristico-pornographiques¹)...

Mais la plus redoutable des approches est celle qui utilise la pornographie. Combien d'attaques ont utilisé ce ressort avec succès. Et malheureusement, dans ce cas-là, les neurones cèdent devant les hormones. L'exemple le plus typique restera celui du macro ver W97M/Melissa. Initialement, ce ver est apparu en mars 1999. Il a été distribué dans un fichier LIST.DOC dans le forum de discussion alt.sex. Le fichier en attachement contenait une liste de login (identifiant) et de mots de passe pour des sites pornographiques. Le ressort utilisé (le sexe) se révéla extraordinairement efficace. Melissa est l'un des « macro vers » dont la propagation a été l'une des plus foudroyantes. Des multinationales comme Microsoft ont dû, pendant plusieurs heures, fermer leur service de messagerie pour endiguer la dissémination. Il n'est donc pas étonnant que des codes malveillants faisant appel au sexe apparaissent régulièrement.

Un autre exemple rapporté² est particulièrement intéressant. La collaboratrice de la société Quartier Libre Productions reçoit un e-mail à l'objet engageant : « Une journée à Belle-Ile ». Cette invitation est d'autant plus attractive que c'est précisément le titre d'une nouvelle écrite par le frère de cette collaboratrice (pure coïncidence ou attaque ciblée ?). Au final, un dossier du disque dur envoyé à tout son carnet d'adresses et 99 % des fichiers détruits en une heure (notamment la comptabilité et les courriers avec les clients). Et pourtant cette société était protégée par un antivirus mis à jour régulièrement. Le sentiment de sécurité induit par ces logiciels diminue souvent la vigilance des utilisateurs qui leur accordent une confiance inconsidérée (voir le chapitre 11). Dans notre cas précis, il est possible d'imaginer qu'un renseignement judicieusement utilisé permette une attaque d'autant plus efficace qu'elle est ciblée.

Ego ou appât du gain

Dans cette catégorie, la proposition d'une récompense (quelle que soit sa nature) est le ressort utilisé par l'attaquant. L'exemple suivant a été rapporté par B. Hatch, J. Lee et G. Kurtz³ dans leur livre. Le lecteur intéressé trouvera d'ailleurs dans cet ouvrage d'autres exemples d'attaques par ingénierie sociale.

Dans le dortoir d'une université, une affiche avec le texte suivant avait été collée :

Concours de mots de passe !

Vous voulez faire la preuve de votre créativité ? Vous voulez gagner un prix ?

Inscrivez ici votre nom d'utilisateur pour le réseau du campus et votre mot de passe. Les cinq mots de passe les plus originaux et les plus drôles recevront des maillots de l'équipe de football de l'Université. Ceux-ci devront respecter les

1. De nombreux exemples sont répertoriés sur le site <http://hoaxbusters.ciac.org/>.

2. Quand le virus informatique tue la mémoire, *Ouest-France*, 27/02/2002.

3. B. Hatch, J. Lee et G. Kurtz, *Halte aux Hackers Linux*, Osman Eyrolles Multimedia Editions, 2001.



contraintes d'UNIX pour les mots de passe : pas plus de 8 caractères, respect des majuscules/minuscules. Le mot de passe devra être vérifiable par notre jury.

Les auteurs rapportent que rien n'indiquait la provenance de cette annonce, ni les informations usuelles (composition du jury, remise des prix...). Malgré cela, une cinquantaine d'utilisateurs ont inscrit les données demandées sur cette affiche. Il va sans dire que leurs comptes ont été attaqués presque immédiatement.

Dans le même registre, et plus récemment, certaines attaques de déni de service ont été réalisées en exploitant l'appât du gain. Les « chaînes » de courriers électroniques proposant de gagner des téléphones mobiles en faisant suivre l'e-mail à dix personnes et en mettant en copie la société visée (en l'occurrence un des leaders de la téléphonie mobile), provoquaient l'effet de saturation désiré.

Un autre exemple récent concerne un cas d'infection de téléphones portables par le virus Skulls.L. L'utilisateur reçoit un message l'invitant à installer une copie pirate de l'antivirus pour mobiles de F-Secure.

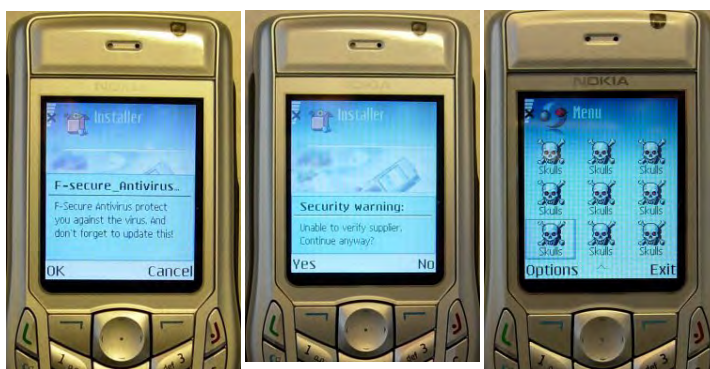


Figure 2.1 — Les téléphones vont devenir l'une des nouvelles cibles des pirates.

Motivé par le gain d'une fonctionnalité acquise gratuitement — mais frauduleusement —, l'abonné qui accepte se fait alors infecter par le code qui modifie l'environnement, dégrade les fonctionnalités et les performances et installe deux autres vers tout en défaçant le bureau de travail du mobile (voir figure de droite). Là encore, une simple manipulation exploitant le manque de scrupules des utilisateurs a permis la réalisation de l'attaque (voir également [4]). A l'avenir, les utilisateurs de téléphones mobiles devront être plus vigilants car ils vont devenir l'une des nouvelles cibles des pirates (voir le chapitre 18).

Exemples d'exploitation de manque de connaissances

Dans ce cas de figure, l'attaquant va exploiter les lacunes techniques de l'utilisateur pour l'amener à effectuer une action précise (en général, la modification de l'intégrité du système, saturation du réseau...). La technique de base (il y en a beaucoup d'autres) est le canular qui peut être plus ou moins ciblé. L'exemple suivant est bien réel mais malheureusement peu connu car l'attaque a été très ciblée. Il illustre parfait-

tement notre propos. Il s'agit d'un virus dit « psychologique ». Ce genre de « virus » et autres canulars sont recensés sur le site www.hoaxbuster.com.

Dans le courant février 2002, certains utilisateurs ont reçu un message alarmiste les avertissant qu'un virus particulièrement destructif venait d'apparaître. Pour vérifier une éventuelle infection, le destinataire du message était invité à regarder si un fichier `KERNEL32.DLL` se trouvait dans le répertoire `C:\WINDOWS\SYSTEM` de son disque dur. Dans l'affirmative, l'utilisateur devait effacer au plus vite ce fichier et redémarrer immédiatement son ordinateur. Or, ce fichier est un exécutable légitime et essentiel à Windows. Il est chargé au démarrage du système d'exploitation et gère la mémoire, les entrées-sorties et les interruptions. L'e-mail, par son style et son apparence, ressemblait à s'y méprendre à une alerte sérieuse. Il n'était pas demandé de diffuser ce message. Mais généralement, les destinataires le diffusent à leur entourage, par solidarité. L'utilisateur sans connaissance technique de base sur le système d'exploitation de Microsoft qu'il utilise, paniqué par l'idée d'avoir sa machine infectée (et la peur d'une éventuelle sanction de la part de sa hiérarchie s'il travaille dans un bureau), effectue les opérations conseillées. Le mal est fait et Windows ne peut plus redémarrer. Il y a atteinte à la disponibilité et éventuellement perte des données si aucune sauvegarde n'a été faite et qu'aucun CD ou DVD de sauvetage n'a été prévu.

2.1.4 Comment lutter contre l'ingénierie sociale

Il ne semble pas facile de contrer ce genre d'attaques, tant les possibilités et les approches sont nombreuses et tant la détermination et la ruse des pirates sont fortes. Mais l'observation de certaines règles de base permet de limiter les risques :

- Être suffisamment paranoïaque et ne pas faire spontanément confiance. Il est bon d'exercer un doute salutaire et constant. Il est important de se renseigner et de remettre en question ce qui semble évident ;
- Ne jamais communiquer d'informations sensibles (en premier lieu login et mots de passe) sans une authentification certaine et si possible physique et en interne. Il faut toujours refuser ce genre de communication. Dans le premier exemple évoqué, il valait mieux courir le risque de passer à côté d'un contrat, que celui de mettre en péril les ressources informatiques toutes entières de la société ;
- Vérifier l'origine des demandes et surtout rendre compte aux échelons supérieurs. Cela permet de recouper les informations ;
- Restreindre les possibilités d'obtention d'informations de l'extérieur en édictant des règles précises et rigoureuses dans le contenu et la gestion de la messagerie électronique, des pages web, des annuaires, des brochures publicitaires, des cartes de visite, pages jaunes, de la gestion des rebuts (l'usage d'un broyeur devrait être systématique)...
- Etablir des règles et des procédures strictes concernant les interventions extérieures (maintenance, stagiaires, entretien, assistance technique...) et la sécurité en général. Dans ce dernier cas, il est par exemple essentiel que le



responsable sécurité soit parfaitement identifié comme le seul autorisé à diffuser des alertes (gestion hiérarchisée et centralisée des alertes).

Il faut surtout sensibiliser et former les personnels, quels qu'ils soient, par le biais de stages ou lors de réunions régulières. Le point le plus important étant de les sensibiliser aux risques de l'indiscrétion hors de l'entreprise.

Il est surtout fondamental de garder constamment à l'esprit que personne n'est à l'abri ou « naturellement immunisé » (par la grâce d'une position hiérarchique supérieure ou d'une forte expertise) contre ce genre d'attaque. C'est ce qu'a découvert la directrice de la sécurité de Bouygues. « En faisant ensemble un « audit » de sécurité nous avons en effet remarqué que ce n'étaient pas les employés qui faisaient le plus d'erreurs en matière de sécurité mais les cadres supérieurs, nous explique le Commissaire principal Yves Crespin, Chef de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI). Estimant être protégés par leur direction informatique, ils font des fautes de sécurité que ne ferait même pas un débutant. Cet exemple montre qu'il faut une vision globale en matière de sécurité. Cela implique une coopération entre la direction informatique et celle des ressources humaines pour mieux éduquer les employés. »

Il vaut mieux surestimer l'attaquant que l'inverse. Mais surtout il convient de garder à l'esprit que dans une politique de sécurité, l'élément humain (c'est-à-dire les utilisateurs en y incluant les administrateurs système) restera toujours le facteur limitant.

2.2 LES FAILLES DE SÉCURITÉ LOGICIELLES

Ce genre de failles, encore connues sous le nom de vulnérabilités, est **l'autre** facteur très important permettant de réaliser des attaques avec une facilité déconcertante.

Une vulnérabilité est un défaut de programmation ou de gestion affectant soit un logiciel ou soit l'implémentation d'une fonctionnalité ou d'un protocole. Elle permet de pénétrer *sans aucune procédure d'autorisation ou de contrôle*, un système et ce *avec des privilèges maximaux* (qui sont ceux du système lui-même). On appelle « exploit » le code permettant d'exploiter cette vulnérabilité.

A côté de la notion de vulnérabilité, il est nécessaire de définir la notion de vulnérabilité 0-Day (et donc également d'exploit 0-Day). Il s'agit d'une vulnérabilité permettant de compromettre des systèmes mis à jour. L'existence de ces vulnérabilités particulières a plusieurs explications [1] :

- L'éditeur est au courant de la faille mais n'a pas encore publié de correctif (cas de la faille WMF de janvier 2006).
- L'éditeur n'est pas au courant de la faille, cette dernière n'est partagée que par un nombre restreint de personnes.



Ce dernier cas — il est difficile voire impossible d'en évaluer l'importance — est le plus grave puisque non seulement les systèmes sont totalement vulnérables, mais cette situation est aggravée par l'ignorance totale de la part des professionnels de sécurité. Comment en effet se protéger contre quelque chose que l'on ne soupçonne même pas. Ce qui est clair, c'est que des groupes — et notamment dans les pays de l'Est ainsi qu'en Asie — connaissent et exploitent ce genre particulier de vulnérabilités. Le cas de la faille WMF (*Windows Meta File*) lors d'une attaque venant de Chine (voir chapitre 11) le démontre clairement. Nous verrons un autre exemple d'attaque de ce type.

Les Français en retard d'un patch

La précipitation est parfois mauvaise conseillère en matière de sécurité informatique. Mais il ne faut pas non plus être trop négligent. De façon plus ou moins régulière et rapide, les éditeurs découvrant des failles proposent des mises à jour ou des patchs de sécurité. En la matière, les Français semblent un peu lents. Selon une étude publiée en avril 2006 par l'éditeur de sécurité McAfee, 27 % des entreprises nationales prennent une bonne semaine pour appliquer les correctifs, et 39 % plus de 2 jours. A titre de comparaison, les sociétés espagnoles ne sont que 8 % à attendre deux jours.

Deux remarques importantes doivent être faites concernant le problème des vulnérabilités :

- Les vulnérabilités concernent tous les systèmes d'exploitation et toutes les applications, en particulier les logiciels de sécurité comme les antivirus ou les pare-feux. Si les logiciels Microsoft et Mac sont les plus touchés, cela s'explique, en partie, par la position dominante de ces éditeurs. De nombreuses vulnérabilités sont découvertes chaque année pour tous les autres systèmes.
- Un développement logiciel dans une situation de concurrence extrême est la principale cause de vulnérabilités. Les programmeurs ne disposent pas de conditions ou de formation suffisantes leur permettant un développement logiciel de qualité. Il est à parier qu'un système comme Linux — déjà touché, pour certaines distributions, par ce problème — s'il devenait majoritairement répandu, serait concerné avec la même ampleur par les vulnérabilités. Dans ce domaine, il n'existe pas de sanctuaire ni de Nirvana logiciels.
- Cela concerne également — du moins potentiellement car les exceptions commençant à devenir moins fréquentes, pour ne pas dire rares — tous les environnements : la téléphonie ou les environnements mobiles (Wi-fi et la faiblesse dans le protocole de gestion des clefs [2], le protocole Bluetooth [3]...

En mai dernier, une alerte a annoncé une vulnérabilité concernant le logiciel Word de la suite Office. La faille pourrait être exploitée via des pièces jointes infectées envoyées avec les e-mails. Un code malveillant pourrait être exécuté sur l'ordinateur.

1. Source : CERT sur http://www.cert.org/stat/cert_stats.html



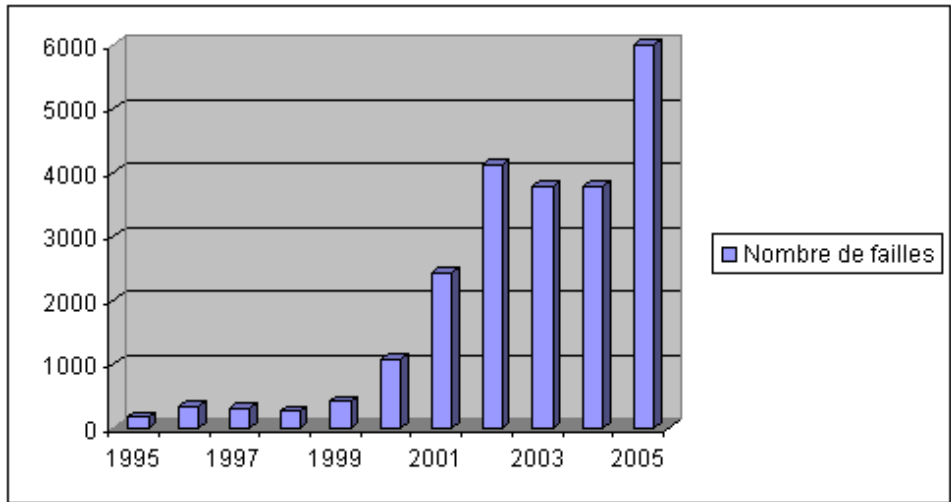


Figure 2.2 — Ce graphique montre l'évolution du nombre des vulnérabilités¹, tous systèmes confondus, entre 1995 et 2005.

2.2.1 L'attaque Scob/Padodor

Orchestrée en juin 2004, elle est assez remarquable par de nombreux aspects [5] : deux codes malveillants agissent de concert et exploitent deux vulnérabilités logicielles simultanément. L'attaque s'est déroulée de la manière suivante :

- Le 22 juin 2004, plusieurs serveurs dans le monde ont été infectés par le code malveillant SCOB — la liste n'a pas été publiée mais il semble très probable que de nombreux serveurs (importants qui plus est) aient été concernés.. L'infection a été rendue possible par la présence d'une faille affectant le logiciel Web serveur IIS¹ de Microsoft.
- Tout utilisateur consultant ces sites, à l'aide d'une version vulnérable d'Internet Explorer 6 – SP1 a été automatiquement infecté par le cheval de Troie PADODOR (téléchargé à partir d'un autre site). Ce code réalise une attaque par *phishing* (voir chapitres 4 et 5). De plus, cette attaque — comme la plupart de celles s'appuyant sur l'hameçonnage — utilise l'ingénierie sociale (simulation d'une requête de sécurité semblant émaner d'un site bancaire et incitant l'utilisateur à fournir des données confidentielles). Toutes les données saisies par l'internaute imprudent sont volées et envoyées vers plusieurs sites russes.

1. Ce logiciel est indispensable pour organiser un serveur web, mettre à disposition des pages et services attachés et permettre aux internautes de se connecter sur un tel serveur.

Une course contre la montre

Dans la neuvième édition de son *Internet Security Threat Report* (avril 2006), Symantec a calculé le temps nécessaire aux attaquants pour compromettre la sécurité de systèmes d'exploitation nouvellement installés :

« S'agissant des serveurs, Windows 2000 Server sans patch est en moyenne compromis plus rapidement que les autres systèmes, tandis qu'il a été impossible de compromettre Windows 2003 Web Edition avec patch et RedHat Enterprise Linux 3 avec ou sans patch durant la période de test. S'agissant des ordinateurs personnels, Microsoft Windows XP Professional sans patch est en moyenne compromis plus rapidement que les autres systèmes, tandis que le même système doté de tous ses patches et le système SuSE Linux 9 Desktop n'ont pas été compromis.

Au cours de la période rapportée (dernier semestre 2005), il s'est écoulé en moyenne 6,8 jours entre la publication d'une vulnérabilité et l'apparition du code d'exploitation correspondant, contre 6 jours pour le précédent semestre. Les fournisseurs diffusent les patches requis en moyenne 49 jours après la publication de la vulnérabilité. Les entreprises et le grand public sont donc exposés à des attaques potentielles pendant 42 jours, ce qui montre que les utilisateurs doivent appliquer les patches disponibles aussi vite que possible. Selon Symantec, la commercialisation des recherches de vulnérabilité devrait augmenter, en parallèle avec le développement des forums de marché noir et l'accroissement des achats de vulnérabilités à des fins criminelles. »

2.2.2 L'attaque GDI+

Elle a exploité le 29 septembre 2004 la faille du même nom (faille GDI+ corrigée le 13 octobre 2004 — bulletin MS04-28 ; donc une vulnérabilité 0-Day au moment de l'attaque). Les attaquants ont utilisé simultanément deux axes : des images pornographiques (disponibles sur des forums de discussion) et la messagerie instantanée d'AOL. La faille affecte un grand nombre de versions de Windows et d'applications, et notamment Internet Explorer 6 – SP1.

Cette attaque utilisait des images au format JPEG dans lesquelles du code malveillant avait été préalablement inséré. Lorsqu'elles étaient visualisées avec un logiciel concerné par cette faille, ce dernier exécutait automatiquement et en parallèle le code malveillant. En l'absence de faille, ce code malveillant n'aurait pas pu être activé. L'attaquant pouvait alors obtenir les mêmes privilèges que l'utilisateur et prendre le contrôle de son système.

Dans le cas de la messagerie instantanée d'AOL, les utilisateurs recevaient le message suivant : « Check out my profile. Click GET INFO ». En cliquant sur le lien contenu dans le message, la personne était redirigée vers une image contenant le code malveillant et l'affichait. Le code malveillant était ipso facto activé (grâce à la faille). Il prenait le contrôle du carnet de contacts AOL pour se propager et installait une porte dérobée (**backdoor**) dans le système.



2.2.3 Les attaques du protocole Bluetooth

Ce protocole de connexion sans fil est présent sur un très grand nombre d'environnements mobiles (téléphones mobiles, ordinateurs portables, PDA...). Ces appareils nomades sont des cibles privilégiées pour les attaquants. En 2005, des vulnérabilités au niveau de l'implémentation des fonctions de sécurité de ce protocole ont été découvertes. Elles affectaient un très grand nombre d'environnements.

Parmi les attaques possibles, exploitant ces vulnérabilités, citons les trois principales, dont nous conserverons la dénomination originelle.

Attaque BlueJacking

Elle consiste à envoyer un fichier pour transmettre un message et, ce sans authentification, à un autre équipement Bluetooth. Le nom de l'équipement Bluetooth émetteur peut être modifié afin de faire croire à une communication légitime et normale (fournisseur de services de téléphonie par exemple). Cela autorise une forme nouvelle de spam et une méthode d'envoi de codes malicieux.

Attaque BlueSnarfing

Le pirate peut accéder en lecture et en écriture aux informations contenues dans l'environnement mobile visé (répertoire téléphonique par exemple). Les données contenues dans l'appareil visé peuvent être modifiées. De nouvelles variantes de cette attaque sont découvertes régulièrement. Dans tous les cas, un défaut d'authentification est à l'origine de la faille.

Attaque BlueBugging

Elle permet de prendre le contrôle des appels (et ainsi, par exemple, permet de transformer le téléphone en micro). Il est également possible à l'attaquant d'émettre, de lire ou d'effacer des SMS ainsi que de lire ou d'écrire les entrées du carnet d'adresse. Il peut également rediriger le trafic téléphonique...

En résumé

Ingénierie sociale et vulnérabilités sont les deux principaux angles d'approche que tout attaquant qui se veut efficace doit connaître et maîtriser. En face, tout « défenseur » se doit de connaître l'existence de ces possibilités. Si la lutte contre les vulnérabilités reste encore une chose relativement facile — quoique vite contraignante dans un système informatique complexe — la gestion technique des vulnérabilités dites 0-Day est impossible. Quant à la gestion de l'utilisateur et de sa sensibilité vis-à-vis de l'ingénierie sociale — la gestion du fameux « facteur humain » — existe-t-il seulement un espoir à défaut d'une solution. Tout officier de sécurité est passé par suffisamment de grands moments de solitude pour savoir ce qu'il en est. Et l'attaquant le sait aussi...

Creative Commons BY-NC-ND



3

Vols et pertes de données personnelles

Les étourdis ne devraient jamais prendre l'avion seul ! En décembre 2005, un employé du cabinet d'audit Deloitte & Touche oublie un CD-Rom dans un avion. Pas un CD de musique ou de jeu vidéo. Mais un support contenant les données personnelles de quelque 9 000 employés de McAfee, une entreprise américaine spécialisée dans la sécurité informatique. Et le comble, c'est que ce fichier n'était pas, selon les informations publiées dans la presse, protégé par un système de chiffrement.

Si ce précieux document est tombé entre les mains de pirates, les personnes concernées peuvent craindre le pire, d'autant que l'étourdi en question n'aurait averti sa hiérarchie que trois semaines après sa bétise... Grâce à ces précieuses données, des malfaçons pourraient en profiter pour effectuer des achats personnels ou des virements sur des comptes en Russie ou ailleurs. Ils pourraient aussi acheter du matériel informatique et des logiciels pour les revendre ensuite sur des sites d'enchères ou via des **spams**, ces e-mails non sollicités qui inondent le web. Apparemment, McAfee était prévoyant, ou pas rassuré sur la sécurité informatique, car elle avait souscrit une assurance garantissant à ses employés un service de surveillance de leurs comptes bancaires gratuitement pendant deux ans. Mais il est bien sûr très difficile d'en savoir plus sur les conséquences réelles pour les employés. Comme dans toutes ces affaires, les entreprises restent très discrètes...

3.1 DONNÉES PERSONNELLES : PERTES ET PROFITS

L'affaire McAfee/ Deloitte & Touche peut prêter à sourire tellement elle paraît invraisemblable ! Malheureusement, il ne s'agit pas d'un cas isolé. Depuis un peu plus d'un an, différentes affaires de pertes et de vols de fichiers informatiques



défrayent la chronique surtout aux États-Unis. Une étude publiée au printemps 2006 par le ministère de la Justice américain estime à 3,6 millions le nombre de victimes. La majorité d'entre elles aurait entre 18 et 24 ans et se situerait dans les couches sociales aisées (revenu annuel supérieur à 75 000 dollars). La moitié des cas recensés concernent des escroqueries à la carte de crédit et 15 % des vols d'identité dans le but d'ouvrir de nouveaux comptes ou de bénéficier de prêts.

Il n'est donc pas surprenant que bon nombre d'Américains commencent sérieusement à douter des capacités des entreprises et surtout des organismes financiers à protéger efficacement les données personnelles qu'ils stockent. Plus de la moitié des consommateurs américains utilisant l'Internet craignent davantage depuis un an le détournement de données confidentielles comme les codes bancaires. Beaucoup ont même changé leurs habitudes, décidant de moins recourir aux achats en ligne.

Ces affaires de pertes de données sont en effet d'autant plus inquiétantes qu'elles concernent des banques réputées. C'est le cas de la *Bank of America*. En février 2005, la troisième banque américaine (quelque 38 millions de comptes privés et d'entreprises) a perdu des données financières de 1,2 million de fonctionnaires de l'État fédéral américain. Cet organisme semble d'ailleurs avoir quelques soucis avec la sécurité informatique. En février 2006, il a annulé les cartes de crédit de nombreux clients suite à un mystérieux incident technique... Le palmarès de Javelin Strategy & Research, une société américaine spécialisée dans les finances, apparaît dans ce cas très surprenant. Pour la seconde année consécutive (2004 et 2005), la *Bank of America* a décroché la première marche du podium de la sécurité en ligne. Dans cette étude comparant vingt-huit banques, elle a aussi obtenu la première place concernant... la prévention et la résolution de vol d'identité.

Les clients des autres banques ou organismes ne sont pas mieux lotis. En avril 2005, Citigroup a perdu des bandes magnétiques contenant les données privées d'environ 4 millions de comptes. Le fichier se serait égaré lors d'un envoi dans un avion affrété par une société connue pour ses livraisons express.

En mars 2005, LexisNexis, spécialisée dans la recherche et la vente d'informations personnelles de millions de consommateurs américains, annonce la disparition frauduleuse de 32 000 fichiers de données.

Mais l'affaire la plus retentissante a lieu en février 2005. Le service américain de renseignements financiers ChoicePoint a vendu par erreur un extrait de son fichier clients à de mystérieux acheteurs. Une mine d'or pour tous les cyberdélinquants puisqu'il contient l'identité personnelle (numéro de sécurité sociale, numéros de téléphone, adresses e-mails...) et la situation bancaire (état d'endettement notamment) de quelque 160 000 personnes. Un vent de panique s'empare du pays. Vingt-deux États ouvrent une enquête afin de vérifier notamment si le nombre de victimes potentielles (dont une bonne partie se trouve en Californie) annoncée par l'organisme n'est pas sous-évalué. Les magistrats s'appuient notamment sur le « Privacy Act of 2005 » qui stipule que citoyen américain doit être informé dès qu'un « incident » informatique concerne ses données. Mais comme cette législation n'est



pas appliquée partout, des procureurs de ces États-là ont demandé des compléments d'informations auprès de ChoicePoint et ont averti le grand public.

Cette absence d'une législation homogène explique en partie la difficulté à évaluer, avec plus ou moins d'erreurs, le nombre de vols ou de pertes de fichiers de ce genre. Image de marque oblige, les banques et les organismes de crédit restent très discrets sur ces dégâts « collatéraux ». Il faut donc se tourner vers des institutions plus indépendantes pour obtenir des renseignements plus précis. Ainsi, la *Federal Trade Commission* (Commission Fédérale du Commerce aux États-Unis) estime qu'en 2005 un peu plus de 9 millions de ses concitoyens auraient été victimes d'un vol ou d'une arnaque par usurpation de leur identité durant les 12 derniers mois ! Le coût pour les entreprises ou les internautes est estimé à 50 milliards de dollars. Une récente étude¹ de la *Privacy Rights Clearinghouse*, une association de défense des consommateurs américains, évalue à 53 millions le nombre de personnes qui auraient perdu des informations personnelles entre mars 2005 et le printemps dernier.

3.2 LES PERTES DE DONNÉES SENSIBLES

Une thèse ne peut pas s'appuyer que sur des anecdotes. Mais celles-ci ont au moins le mérite d'être significatives si elles sont choisies à bon escient. C'est la même chose pour les exemples qui suivent. On peut en tirer toutes les conclusions que l'on veut et estimer que les exemples que nous allons présenter sont rares. Cela reste à prouver. Tous les spécialistes en sécurité que nous avons rencontrés nous ont raconté quelques bévues croustillantes. Les Gaston Lagaffe sont partout, y compris dans l'Armée ou la police... Quelques officiers français ont par exemple oublié dans des véhicules des téléphones portables contenant quelques numéros « classés »...

Mais l'histoire la plus connue remonte à 2004. Lors de l'opération Licorne en Côte d'Ivoire, les militaires français sont repartis un peu trop vite et ont laissé derrière eux un ordinateur contenant des renseignements « classifiés » : cartes, inventaires de matériel des forces gouvernementales et rebelles, 200 fiches biographiques dressées par les services du renseignement sur de hautes personnalités ivoiriennes et des diplomates étrangers... Quelques jours après, un curieux CD ROM² se retrouvait sur les étals de quelques commerces d'Abidjan. A un prix défiant toute concurrence : moins de 6 euros ! Sa pochette affichait le titre sibyllin « Le CD ROM oublié » et la photographie du général Henri Poncet, le chef de cette opération.

Les pertes de données concernant des centrales thermiques sont toutes aussi inquiétantes. Elles prouvent que les réseaux informatiques d'infrastructures sensibles ne sont pas toujours bien protégés. En mai 2006, une infection virale a provoqué la fuite sur Internet d'informations confidentielles (concernant la sécurité et des données sur le personnel) sur une centrale thermique appartenant à l'entreprise japo-

1. <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

2. Le monde. 14/04/2005.



naise Chubu Electric Power. Les données se seraient retrouvées sur le web via le logiciel de partage de fichiers Share. Quelques mois plus tôt, la même société avait connu un incident similaire... Enfin, en juin 2005, l'éditeur d'antivirus Sophos avait révélé la diffusion d'informations secrètes sur une centrale nucléaire, dérobées sur l'ordinateur privé d'un employé de Mitsubishi Electric Plant Engineering.

Toujours au Japon, des données sur des victimes japonaises de violences sexuelles sont apparues sur Internet à la suite de l'infection de l'ordinateur d'un enquêteur de la police.

Ces exemples peuvent paraître « anecdotiques » et le lecteur peut objecter que somme toute, de tels cas sont fort heureusement peu nombreux. Que faut-il en penser ? S'il est effectivement très difficile, voire impossible, d'établir des statistiques, c'est en partie parce que le secret est de rigueur et qu'à moins d'indiscrétions, ces affaires et autres fautes graves ne sont jamais rendues publiques. C'est parfaitement compréhensible si l'on considère que leur révélation donne aux attaquants sinon des idées du moins des informations utiles pour savoir où chercher. Une autre illustration du duel entre l'épée et le bouclier.

3.3 LE VOL DES DONNÉES : LE MARCHÉ AUX PUCES

La consultation du rapport de la Privacy Rights Clearinghouse¹, une organisation non gouvernementale américaine de défense des intérêts des consommateurs, montre à quel point les ordinateurs portables sont devenus des proies faciles pour les voleurs en tout genre mais aussi pour les organisations criminelles. Elles cherchent surtout à exploiter les fichiers stockés dans le disque dur qui sont rarement protégés par des mots de passe et un système de chiffrement. Voici les faits plus marquants constatés entre avril 2005 et mars 2006.

- Avril 2005, San Jose Médical Group (San Jose, Californie) : le PC contenait un fichier de 185 000 noms.
- Mai 2005, Département de la justice (Washington) : 80 000 références.
- Décembre 2005, Firsttrust Bank : 100 000 noms.
- Février 2006, cabinet Ernst & Young : 38 000 références (données personnelles et numéros de sécurité sociale d'employés de BP, Sun, Cisco et IBM).
- Mars 2006, Metropolitan State College (Denver) : un fichier volé contenant les données privées de 93 000 étudiants scolarisés entre 1996 et 2005.

Le record a pendant un temps été détenu par la Fidelity Investments, un fonds d'investissement situé à Boston. En mars 2006, un ordinateur contenant des informations personnelles de 196 000 salariés travaillant notamment pour l'entreprise informatique HP a été volé. Fidelity a tenu à préciser qu'aucun mot de passe permettant de s'identifier sur ses services n'était dans le PC...



Mais deux mois plus tard, ce record est tombé. Une base de données contenant les informations personnelles d'environ 26 millions d'anciens combattants américains a été dérobée. En cambriolant le domicile d'un analyste du ministère des anciens combattants, les malfrats ont en effet mis la main sur un PC portable contenant ce précieux document.

Une autre étude publiée en mai 2006 est tout aussi révélatrice. A la demande du groupe Kensington, le cabinet IDC a interrogé 200 entreprises européennes. Conclusion : en moyenne, une PME perd quatre ordinateurs portables par an, avec très peu de chances (5 %) de les retrouver. Le quart des vols serait dû à des employés. Ce n'est pas tellement la perte d'un PC qui inquiète le plus les entreprises mais le coût lié à la disparition des données. Dans cette même enquête, IDC annonce que seulement 13 % des entreprises interrogées font de la sécurité matérielle de leur matériel informatique une priorité...

Le premier hold-up virtuel

En juin 2005 le groupe Mastercard publie un communiqué qui fera date dans l'histoire de la cybercriminalité. Le groupe révèle qu'environ 40 millions de titulaires de cartes de crédit (dont près de 14 millions de cartes MasterCard, les autres concernant Visa et Discover) venaient de passer du côté obscur, en l'occurrence celui du casse informatique. Un pirate est en effet parvenu à accéder aux données confidentielles de ces comptes (numéros des cartes ainsi que les codes de sécurité mais pas les adresses des usagers parmi lesquels 70 000 Français). Pour réussir son hold-up, il s'est attaqué au maillon faible du système, Card-Systems Solutions... une société américaine chargée d'assurer la sécurité des transactions par carte bancaire. La disparition de 40 millions de cartes ne signifie pas que ce braquage a fait autant de victimes. « Cela signifie qu'elles étaient dans le système au moment de l'intrusion. Nous avons informé les établissements émetteurs afin qu'ils prennent les mesures nécessaires auprès de leurs clients », indique Hervé Kergoat, directeur général de Mastercard Europe¹.

Le vol de données bancaires passe aussi par l'utilisation de chevaux de Troie conçus spécialement pour la récupération de ce genre d'informations. Selon l'éditeur de sécurité Kaspersky, ces codes malicieux sont de plus en plus nombreux. Le taux de croissance de cette catégorie est le plus élevé parmi les programmes malicieux. Il représente 402 % à la fin de l'année 2005.

Les Américains ne sont pas les seuls à être concernés. Les pertes liées à ce genre de larcins atteindraient 1,7 milliard de livres Sterling en Angleterre selon les propos tenus début 2006 par Andy Burnham, le secrétaire d'État du ministère de l'Intérieur. L'une des dernières affaires remonte au mois d'avril 2006. Le quotidien britannique *The Times*² révèle que des informations liées aux cartes de crédit de 300 à 400 Britan-

1. 01Net.com. 21/06/2005.

2. 15/04/ 2006.



Classe	Progression
Chevaux de Troie	+ 8,76%
Virus	- 6,53%
MalWare	- 2,23%

Progression de chaque catégorie entre 2004 et 2005

Source : kaspersky. 2005

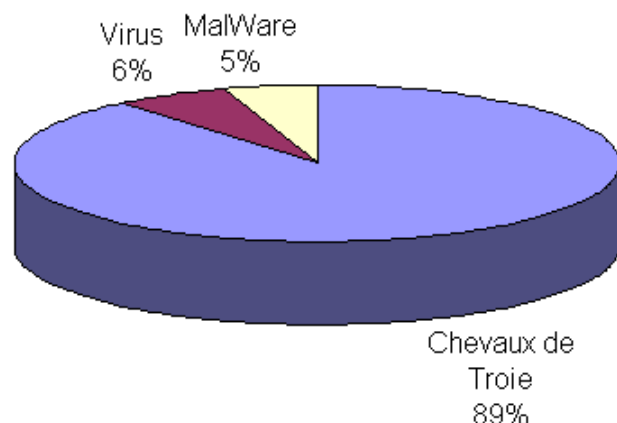


Figure 3.1 — Les codes malicieux deviennent de plus en plus spécialisés.

Source : Kaspersky. 2005.

niques ont été mises en vente sur l'Internet par des pirates qui les ont volées sur des systèmes informatiques d'entreprises mal protégées. Un vrai marché aux puces ! Un numéro de carte coûte 1 euro environ. Plus on paie, plus on obtient d'informations facilitant les achats comme le code de sécurité de trois chiffres coûte (quelques euros) et le code secret (entre 10 et 100 euros). Pour différentes raisons, liées notamment à la législation, ces sites ne se trouvent pas en France. « Ils sont en principe hébergés hors d'Europe et bien souvent aux États-Unis, explique Yves Crespin, chef de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI). Dans ce pays, les pirates profitent de la liberté d'expression et de communication (1er amendement de la Constitution) » Autres terres d'accueil : les pays de l'Est et d'Asie.

En France, les données officielles concernant ce genre de délits sont rares, tous les organismes bancaires (c'est aussi la même chose à l'étranger) restant très discrets sur ce genre de sujet. Selon l'Observatoire de la sécurité des cartes de paiement (créé en 2003), le taux global de fraudes sur les cartes de paiement, toutes transactions nationales et internationales confondues, a été estimé en 2004 à 0,07 %. Il était de 0,09 % en 2003 et de 0,08 % un an plus tôt. Le montant de la fraude est passé de 273,7 millions d'euros en 2003 à 241,6 millions d'euros en 2004 (soit une diminution de 11,7 % alors que dans le même temps les capitaux échangés ont augmenté de 7,8 %, passant de 320 à 345 milliards d'euros.



Mais le plus intéressant est que cet observatoire constate une augmentation des piratages des bases de données : « la fréquence est à peu près d'un piratage par semaine, alors que celle-ci était d'une par mois, voire une par année, il y a peu de temps. Ces piratages proviennent notamment des États-Unis et de Turquie » peut-on lire dans un compte-rendu récent¹.

L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) fournit aussi des statistiques. Sur les 59.964 faits enregistrés en 2004, 83,24 % concernent la falsification et l'usage de cartes de crédits, en diminution de 0,45 % par rapport à 2003.

Concernant la protection des données personnelles, de sérieux doutes concernent la carte Vitale. Il y a un an, deux ingénieurs ont démontré qu'elle n'était pas sécurisée. Ils ont démontré qu'il était possible d'avoir accès aux données confidentielles mais aussi de créer des cartes « compatibles » acceptées par les professionnels de la santé. Cette facilité serait due au fait que les données sont codées et non pas chiffrées (il n'y a pas d'algorithme de cryptographie).

Ces deux informaticiens n'en sont pas à leur première révélation. L'un d'entre eux affirme avoir prévenu le GIE Sesam Vitale, dès 2000, de la présence d'un bogue qui permettait d'intercepter les codes porteurs confidentiels. Son compère avait de son côté consacré deux articles, publiés dans *Pirates Mag* de mai et août 2005², dans lesquels il indiquait qu'il était possible de lire et de copier l'ensemble des données présentes dans cette carte et donc de la cloner.

Mais c'est en Russie que la situation est la plus catastrophique. Du numéro de sécurité sociale à la date de naissance en passant par le prénom de sa mère, le numéro de compte bancaire ou de carte de crédit avec son code, toutes ces données peuvent permettre d'accéder à différents comptes, le plus souvent à des fins d'extorsion financière, mais aussi pour fabriquer de fausses pièces d'identité, de faux certificats, etc. Ces données piratées sont stockées sur des sites clandestins fonctionnant comme des self-services d'informations volées. Pour pouvoir y accéder, il faut montrer patte blanche, et prouver sa bonne foi criminelle en apportant un lot de données piratées³.

La gangrène russe va-t-elle s'étendre à d'autres pays ? Il est difficile d'apporter une réponse précise car les législations, les mœurs, l'organisation des réseaux financiers varient d'un pays à un autre. Faut-il en conclure que les sociétés spécialisées dans la sécurité informatique crient au loup pour mieux vendre leurs solutions ? La menace est-elle vraiment élevée ? Des spécialistes estiment en effet que les exploitations de données personnelles piratées seraient assez rares. Dans le cas de l'affaire Choice-Point, les données privées auraient servi essentiellement à détourner l'e-mail des victimes et il n'y aurait eu que 800 victimes sur les 160 000 noms figurant sur les fichiers. Les risques seraient donc limités. Ce sont du moins les conclusions de deux

1. Commission des finances de l'économie générale et du plan. Compte rendu n° 48. 8/02/2006.

2. http://www.acbm.com/pirates/num_18/carte-vitale-ald.html et http://www.acbm.com/pirates/num_19/problemes-securite-carte-vitale.html.

3. Libération. 11 /02/2006.



études réalisées en 2005. Celle commandée par le Better Business Bureau (créée en 1912 aux États-Unis, ce bureau d'éthique commerciale est une organisation à but non lucratif) et par Javelin Strategy & Research¹, indique que seulement 11,6 % des fraudes relatives à l'identité auraient été commises via Internet.

Selon cette enquête, les internautes qui accèdent à leurs comptes financiers en ligne pourraient plus rapidement détecter les transactions suspectes que ceux qui n'utilisent que la version papier. Cette rapidité pourrait expliquer que les pertes encourues par les premiers s'élèvent en moyenne à 550 euros contre 4 500 euros pour les seconds.

La seconde étude a été réalisée par ID Analytics. Selon ce cabinet, un vol d'identité sur 1 000 seulement aboutirait à un détournement de fonds ou à un dommage réel. Les analystes d'ID Analytics ont suivi le quotidien de 500 000 consommateurs américains victimes d'une des affaires de vols de fichiers. Principale cause de ce faible « taux de transformation » : la rapidité avec laquelle une carte ou une information bancaire est annulée lorsque sa disparition est avérée. Encore faut-il que les clients en soient informés le plus tôt possible. Or dans l'affaire du casse du sous-traitant CardSystems Solutions, les possesseurs de cartes de crédit n'ont été informés que quinze jours après le forfait ! Les victimes se sont d'ailleurs regroupées pour déposer une plainte en nom collectif auprès d'une cour en Californie. Même lenteur du côté de ChoicePoint. Le courtier a attendu plusieurs mois avant de reconnaître publiquement sa terrible erreur.

Un peu plus d'un an après, la sanction est tombée. La FTC (*Federal Trade Commission*) a condamné ChoicePoint à une amende de 10 millions de dollars. L'hébergeur de données personnelles devra aussi verser 5 millions de dollars de dommages intérêts aux victimes. C'est la plus grosse amende jamais infligée par la FTC pour un vol de ce genre. Avec ce type de record, l'organisme public espère faire comprendre aux entreprises la nécessité de mieux se protéger.

En février 2006, c'est au tour de la banque d'investissement américaine Morgan Stanley d'être sur le devant de la scène. Elle devrait payer 15 millions de dollars dans un arrangement à l'amiable avec le ministère de la justice et la SEC, la *Securities and Exchange Commission*, le gendarme de la Bourse aux États-Unis. La banque est coupable de ne pas avoir suffisamment protégé la confidentialité des courriers électroniques d'Américains.

Ces premières condamnations visent notamment à sensibiliser encore plus les entreprises — ainsi que leurs clients — qui deviennent de plus en plus dépendants des technologies de la communication. La protection des données personnelles est devenue un enjeu majeur pour toute la chaîne des transactions financières : du commerçant au consommateur en passant par tous les organismes détenant des données confidentielles (centres de traitement informatique de cartes de crédit, organismes de crédits, éditeurs de cartes bancaires...). Cette pratique touche aussi les sites de commerce électronique et ceux qui sont spécialisés dans les enchères.

1. The 2005 Javelin Identity Fraud Survey Report. <http://www.bbb.org/alerts/article.asp?ID=565>.



Commerce électronique : le business de la parano

Peur sur le Web ! Publiées quelques semaines avant les fêtes de Noël 2005, deux études américaines ont dû refroidir quelques inconditionnels du commerce électronique. Ainsi, 67 % des internautes interrogés par Harris Interactive pour Sun Microsystems ont confirmé qu'ils mettraient fin à leurs achats en ligne s'ils découvraient que leurs informations personnelles sont compromises. Un tiers des personnes a déclaré avoir été victime personnellement d'une usurpation d'identité ou quelqu'un de leur entourage.

Une autre étude, signée Forrester Research, a révélé que la majorité des consommateurs américains se sentent particulièrement concernés par les pratiques de vente des fichiers amassés par les sites. Ces résultats doivent malgré tout est pris avec toutes les précautions d'usage. L'une de leur conclusion est que les sites marchands doivent renforcer la protection de leur réseau informatique... en faisant appel notamment à des spécialistes comme Sun Microsystems !

En résumé

Les données des internautes deviendraient-elles de moins en personnelles ? Les différentes affaires que nous relatons tendraient à le montrer. D'autant, qu'il est très difficile d'estimer le nombre de ces fichiers qui ont disparu ou qui ont été volés puis revendus. En France, la police estime qu'elle n'a connaissance que de 10 % des affaires de cybercriminalité. Les victimes, qu'il s'agisse de particuliers ou d'entreprises, portent rarement plainte.

Creative Commons BY-NC-ND



4

Le phishing : l'approche artisanale

Un nouveau type de pêche fait fureur sur le Web : le *phishing* contraction des mots anglais *fishing*, qui veut dire pêche en français, et *phreaking*, désignant le piratage de lignes téléphoniques. Pratiquée par les pirates, cette technique profite notamment de la naïveté des internautes pour leur soutirer leurs données personnelles (notamment bancaires) afin effectuer des achats avec leur numéro de carte bancaire.

Contrairement à ce que l'on pourrait croire, cette technique n'est pas apparue avec le développement des connexions internet. « Cette arnaque existait déjà avec le papier, précise Patrick Pailloux, directeur central de la sécurité des systèmes d'information. Des entreprises recevaient de faux fax de France Telecom leur demandant de payer leur facture. Cette escroquerie marchait surtout avec les PME ou les artisans car ils n'avaient pas le temps de tout contrôler comme dans une grande société où il y a des comptables, un service de sécurité... »

Aujourd'hui, à l'ère du tout numérique, ce procédé représente le *nec plus ultra* de ce qu'il est possible de faire en ingénierie sociale (voir chapitre 2). Même lorsqu'elles s'appuient sur des techniques basiques, ces attaques font de nombreuses victimes par la simple manipulation des esprits.

Les risques sont d'autant plus élevés que ce genre d'escroquerie ne concerne pas uniquement les banques. Il y a aussi les sites de commerce électronique et ceux des opérateurs télécoms sur lesquels on peut acheter des cartes prépayées ou des forfaits. Très souvent, plus la ficelle est grosse, plus l'attaque a de chances de réussir ! « En 2005, il y a eu une tentative de phishing qui reprenait les logos de la CIA et du FBI », déclare Yves Crespin de la BEFTI. Le texte de l'e-mail était à peu près celui-ci : « Vous avez surfé sur des sites interdits et vous avez été repéré par nos services. Mettez-vous rapidement en relation directe avec nous par retour d'e-mail sous peine de poursuites. Indiquez-nous toutes vos coordonnées, y compris bancaires et code secret... ».



Le chef de la BEFTI évoque aussi les faux e-mails de sécurité provenant soi-disant de Microsoft. « Les pirates ne proposent plus aux internautes de télécharger le dernier tube de Madonna car le grand public commence à savoir que la pièce jointe peut contenir un virus. Par contre, ils sont moins vigilants concernant un e-mail leur demandant de cliquer sur un lien pour une mise à jour de sécurité ! », constate ce spécialiste.

Le plus frustrant est donc de constater que, attaques après attaques, les victimes sont toujours aussi nombreuses, bien que les ressorts psychologiques du phishing n'aient guère évolué depuis l'origine.

Cette situation amène deux constats : le manque d'informations des internautes est encore extrêmement important et, deuxièmement, certains acteurs impliqués dans la sécurité des utilisateurs (éditeurs de logiciels, constructeurs, fournisseurs de services — bancaires par exemple —, assureurs, médias...) n'ont pas œuvré avec suffisamment d'énergie pour déjouer les attaques par phishing...

Le *phishing* recouvrant de multiples facettes, nous allons l'aborder en deux chapitres, en allant des procédés « artisanaux » aux techniques les plus « sophistiquées ».

4.1 INTRODUCTION

Le terme de *phishing*, appliqué au numérique, date de 1996. Il a été identifié dans le célèbre forum de hackers alt.2600 pour désigner des techniques de vol de mots de passe d'utilisateurs d'AOL. Ces mots de passe étaient ensuite utilisés comme monnaie virtuelle d'échange entre les pirates pour acheter des logiciels crackés (10 mots de passe contre un logiciel piraté). Depuis cette date, les techniques évoluant et les cibles se diversifiant, cette expression désigne la mise en œuvre de techniques visant à voler des données personnelles confidentielles en vue d'une utilisation frauduleuse, délictuelle ou criminelle.

Dire que le *phishing* est une technique répandue est un doux euphémisme. Il s'agit en réalité d'une sorte de « peste électronique » moderne avec laquelle nous devrions vivre sans espoir de rémission ou de guérison.

Pour mesurer l'ampleur du phénomène voici d'autres chiffres édifiants. Selon le Anti-Phishing Working Group (association américaine regroupant plus de 2 300 membres provenant de 1 500 entreprises) et selon l'éditeur d'antivirus Sophos¹ (membre de l'APWG), 58 % des utilisateurs en entreprises reçoivent au moins un message de *phishing* par jour, 22 % en reçoivent plus de cinq par jour.

Ce groupe a reçu pour le seul mois de décembre 2005, 15 244 signalements de *phishing* à comparer aux 8 829 en décembre 2004. Un autre rapport² précise que

1. <http://www.sophos.fr/pressoffice/news/articles/2006/02/phishstats.html>.

2. A. Litan, *Phishing Victims Likely Will Suffer Identity Theft Fraud*, Gartner Research Note, 14 Mai 2004.



57 millions d'internautes américains ont identifié une attaque reposant sur ce procédé. Cette même étude estime qu'environ 1,7 million d'entre eux en ont été victimes et ont divulgué des informations confidentielles.

Toujours selon les chiffres du groupe APWG, l'évolution du nombre des sites construits chaque mois, pour réaliser des attaques de *phishing*, est en constante augmentation comme le montre la figure 4.2. Entre 2000 et 7 000 nouveaux sites apparaissent chaque mois. L'APWG affirme également que le temps moyen d'existence d'un site d'escroquerie est de 6 jours et que 80 % des faux sites copient des sites financiers (banques, organismes de crédit...).

De son côté, le leader mondial de la sécurité, Symantec, estime qu'il y avait au premier semestre 2006 quelque 8 millions de tentatives de *phishing*... par jour. Lors de la période précédente, l'éditeur n'en avait comptabilisé « que » 5,70 millions.

Des statistiques plus détaillées concernant la France sont plus rares. Mais cela ne signifie pas pour autant que notre pays soit épargné. Quelques cas ont été repérés en 2005. Mais « l'une des grandes nouveautés est l'apparition d'attaques de *phishing* en français », constatent différents spécialistes. Les premières s'appuyaient sur des traductions approximatives. Mais les plus récentes sont parfaites ou en tous les cas suffisamment bien conçues pour que le grand public n'y voit que du feu. Cette évolution peut être inquiétante. Les pirates ont peut-être déniché la méthode d'apprentissage d'une langue la plus efficace ou alors ils sont... Français.

Pays d'origine (adresse IP)	Pourcentage des attaques
Etats-Unis	27,74 %
Corée du sud	17,35 %
Chine	8 %
France	6,27 %
Allemagne	4,85 %
Royaume-Uni	3,95 %
Espagne	3,59 %
Japon	3,49 %
Italie	2,43 %

Figure 4.1 — Malgré l'armada judiciaire et technique, de nombreux « phishers » travaillent depuis les Etats-Unis. Source : APWG.

Toutes ces données démontrent l'activité incessante des phishers, laquelle n'est encouragée que par la réussite des attaques pour un nombre non négligeable des victimes visées. Les chiffres couramment cités évoquent une moyenne de 5 % de personnes tombant dans le piège tendu par les phishers. Mais le « taux de

réussite » pourrait être plus élevé. Un sondage réalisé par l'institut TNS-Sofres en 2005 outre-Rhin révèle que 80 % des clients de la Deutsche Postbank (première banque de détail allemande) se laisseraient tromper par un e-mail frauduleux !

L'exploitation des données

Elles sont utilisées à des fins lucratives et mafeuses. Les mots de passe de compte serviront à prendre possession à distance d'un ordinateur et à l'utiliser pour organiser un crime ou un délit (traître d'êtres humains, trafics divers, pédophilie...) — impliquant au passage les innocents propriétaires légitimes des machines ainsi compromises. Les codes de cartes bleues et autres informations relatives serviront quant à elles — entre autres possibilités — à fabriquer des vraies fausses cartes bancaires utilisées par des organisations criminelles pour débiter les comptes des victimes.

Ces informations volées se négocient selon des cours variables. Alors qu'un simple numéro de carte vaut de 1 à 5 dollars selon que le pictogramme visuel est fourni ou non, la fourniture additionnelle d'un code secret valide fait monter les prix jusqu'à 100 dollars.

Il est également difficile d'estimer correctement les préjudices financiers causés par cette arnaque. Pour deux raisons principales : les statistiques ne sont généralement pas rendues publics et, deuxièmement, 90 % de délits ne seraient pas signalés. Le rapport Gardner indique un préjudice de 1,2 milliard d'euros pour les seuls établissements bancaires en 2003 avec un coût estimé à 88,5 millions d'euros pour le seul Royaume-Uni.

4.2 LES TECHNIQUES DU PHISHING

Elles sont nombreuses et l'imagination des attaquants n'a pas de limites. Toutefois, il est possible de distinguer deux principaux groupes de techniques :

- Certains s'appuient sur un simple procédé d'ingénierie sociale (voir chapitre 2), sans réelle astuce technique. D'autres reposent toujours sur la manipulation psychologique mais utilisent des ressorts techniques qui peuvent être très évolués et requérir des organisations plus complexes. Dans ce chapitre, nous présentons celles que l'on peut qualifier « d'artisanales ». Les méthodes plus sophistiquées seront détaillées dans le chapitre suivant.
- Les secondes, abordées dans le chapitre 5, constituent une approche plutôt « industrielle ».



4.2.1 Comment harponner la victime

Le courrier électronique

La technique la plus simple mais également la plus répandue est celle utilisant le *spam* (voir chapitre 6) ou des e-mails ciblés. Le cas le plus simple est un courrier électronique provenant de l'adresse `support_technique@votrebanque.com` (l'adresse est usurpée ; une manipulation très simple à réaliser). Prétextant un contrôle de sécurité de votre compte, cet e-mail vous invite à cliquer sur le lien `www.votre-banque-validate.info` (ce nom de domaine qui ressemble à s'y méprendre au site réel de la banque appartient à l'attaquant) et à fournir des informations confidentielles pour vous authentifier. Le tour est joué.

Cette astuce est souvent automatisée à l'aide des outils traditionnels des *spammeurs*. L'objectif est bien sûr d'envoyer à moindre coût et risque (utilisation de PC zombies) plusieurs millions de courriers chaque jour. Comme pour le spam, les auteurs de ces attaques achètent également des noms de domaine (les adresses des sites qui vont voler vos données) en grand nombre. Les ressorts psychologiques utilisés sont trop nombreux pour être tous énumérés mais signalons les principaux :

- Mise à jour de logiciels ou de la sécurité du site nécessitant la confirmation de détails bancaires (attaque de la Société Générale, voir figure 4.2).



Figure 4.2 — Phishing de la Société Générale (mars 2006).

Fin 2005 et début 2006, les clients des banques LCL et BNP Paribas ont été la cible des mêmes types d'e-mails (voir figure 4.3). Le lecteur remarquera que la texture des courriers est quasi-identique. Les pirates adoptent une démarche systématique et aucune banque (ou autre cible ainsi exploitable) n'est épargnée.



Figure 4.3 — Attaque par phishing de la banque BNP Paribas (mars 2006).

- Activation de nouvelles options sur le site (site AGF en août 2005). Des données confidentielles doivent être fournies pour l'activation
- Lutte contre le vol d'identité et renforcement des mesures de sécurité. L'utilisateur doit fournir des données personnelles bancaires sinon son compte est suspendu (site de Citibank)
- Sécurisation du compte suite à des tentatives de connexions douteuses. Là encore, cette sécurisation est activée en donnant des données bancaires.
- Mise à jour des données personnelles sous peine de ne plus pouvoir accéder à certains droits (site eBay en 2005).

Tous ces courriers électroniques utilisent les mêmes approches. Les plus fréquentes étant :

- La simulation par un courrier d'un contenu professionnel, officiel ou commercial.
- La duplication de contenus connus ou reconnus auxquels sont insérés une ou plusieurs modifications imperceptibles, dans l'URL par exemple.
- L'utilisation du format HTML pour dissimuler l'adresse du site de phishing.
- L'utilisation de courriers ciblés ou fabriqués pour une victime ou un groupe de particuliers. Récemment des attaques par *phishing* ciblé utilisaient le nom de jeune fille. Une telle approche ciblée a de plus grandes chances de réussir.
- L'utilisation de codes malveillants en pièce jointe (voir plus loin figure 4.6).



Les sites web malicieux

C'est comme pour la pêche : on utilise un leurre (un faux poisson aux couleurs vives) et on attend qu'un plus gros poisson morde à l'hameçon. Rapportée à Internet, l'astuce consiste à créer un site frauduleux et attendre que des victimes s'y connectent. Une autre approche consiste à s'introduire sur un site tiers et à y inclure une page web malicieuse (en utilisant par exemple une vulnérabilité du serveur hébergeant le site compromis). Il est évident que pour attirer des victimes en grand nombre les sites malicieux doivent être attractifs. La pornographie, les contenus piratés (appelés « *warez* »)... sont de bonnes chausse-trappes en terme d'ingénierie sociale.

Les attaques par sites web utilisent en général :

- Des liens HTML cachés au sein de sites très populaires (donc piratés) et renvoyant sur des sites administrés par le *phisher*.
- De fausses bannières publicitaires ou autres liens sponsorisés renvoyant vers des sites de *phishing*.
- Des techniques dites de « web-bugs » (des objet cachés dans une page HTML comme une image de taille nulle) pour identifier et tracer de futures victimes.
- Des fenêtres *pop-up* pour dissimuler l'origine véritable d'un message de *phisher*.
- Des codes malveillants dans des pages HTML de serveurs vulnérables qui permettent alors d'exploiter les vulnérabilités du navigateur de tout utilisateur consultant ces sites et les infecter à l'aide d'un code offensif qui réalisera l'attaque proprement dite (cheval de Troie, *keylogger*...). C'est le cas, par exemple du code Padodor (voir chapitre 2) qui affiche la fenêtre suivante :

Mesures de sécurité

Dans le cadre de notre engagement permanent à protéger votre compte et à réduire les cas de fraude sur notre site web, nous procédons à une phase de vérification des comptes de nos clients

Avant de vous enregistrer, confirmez, s.v.p., que vous êtes bien le possesseur du compte

Remplissez, s.v.p., les informations correctes afin de vérifier votre identité

Nom complet

Type de carte et date d'expiration

Votre numéro de carte

Pictogramme visuel (verso de la carte)

Code PIN

Cliquez pour continuer

Figure 4.4 — Le piège est gros mais il est efficace !

La messagerie instantanée, IRC et VoIP

L'adoption de la messagerie instantanée (IM — Instant Messaging) en tant que média de communication en entreprise est aujourd'hui une réalité. Le cabinet IDC évalue à un milliard le nombre de messages instantanés échangés quotidiennement en entreprise, un chiffre qui devrait dépasser celui de l'e-mail en 2006 selon les prévisions de Gartner.

Quant aux forums de messagerie instantanée, ils sont devenus également des canaux de communication très prisés des *phishers*. Leur popularité est due notamment à l'inclusion de contenus dynamiques (images, sons, liens hypertexte, URL...). Toutes les techniques connues de *phishing* sont transposables à ces nouveaux moyens de communication, avec d'autant plus de succès pour les attaquants, il faut le craindre, que les utilisateurs n'ont pas encore conscience du risque attaché à ces nouveaux canaux de communication.

Et la situation ne risque pas de s'améliorer car les escrocs ont plus d'un tour dans leur sac. En mai 2006, la société Cloudmark, spécialisée dans le filtrage de courriers électroniques, a annoncé avoir identifié une nouvelle forme de phishing utilisant la téléphonie sur Internet. Le serveur vocal exploité pour l'attaque se fait passer pour un établissement financier et demande à la personne de rentrer ses identifiants de compte (mot de passe inclus). Selon cette société, l'utilisation de la voix sur IP (VoIP) devrait accentuer ce type de procédé car ce genre de communication est encore trop nouveau pour que les utilisateurs le perçoivent comme risqué. L'explosion de la téléphonie sur Internet présente deux aspects favorisant le phishing : elle permet de toucher un grand nombre de victimes et la simulation d'un serveur vocal devient économiquement moins onéreux que celle d'un serveur vocal classique.

Les PC domestiques piratés

Avec l'augmentation des vulnérabilités (voir chapitre 2) et autres techniques d'infection classiques (virus, vers, chevaux de Troie...), un grand nombre d'ordinateurs domestiques sont attaqués par les *phishers* et ensuite utilisés comme vecteur d'attaques par *phishing* (ils deviennent en effet des PC zombies). Comme pour les autres formes de cybercriminalité, tracer et remonter jusqu'aux auteurs véritables de l'attaque devient de plus en plus difficile pour ne pas dire impossible.

La compromission de milliers d'ordinateurs (réseau de *botnet*) permet non seulement de les utiliser comme des relais pour des attaques mais également comme de formidables sources d'information sur de futures victimes (analyse des courriers électroniques de la victime par exemple).

Un exemple récent d'utilisation de vulnérabilité (avril 2006) montre comment les malfrats peuvent agir et profiter de toutes les faiblesses dans nos environnements informatiques. Bien que révélée, cette vulnérabilité n'a été corrigée qu'après plus... d'une semaine. Elle permet d'exécuter une animation Flash quelconque (envoyée comme pièce jointe humoristique par exemple) en faisant afficher au navigateur Internet Explorer n'importe quelle adresse. Ainsi le *phisher*



peut faire afficher l'adresse de son choix dans la barre du navigateur de la victime tout en contrôlant le contenu apparaissant à l'écran. Cela permet de concevoir des sites de *phishing* quasi-indétectables puisque la barre d'adresse indiquera la vraie URL du site imité au lieu de celle du serveur contrôlé par le pirate et utilisée pour l'attaque.

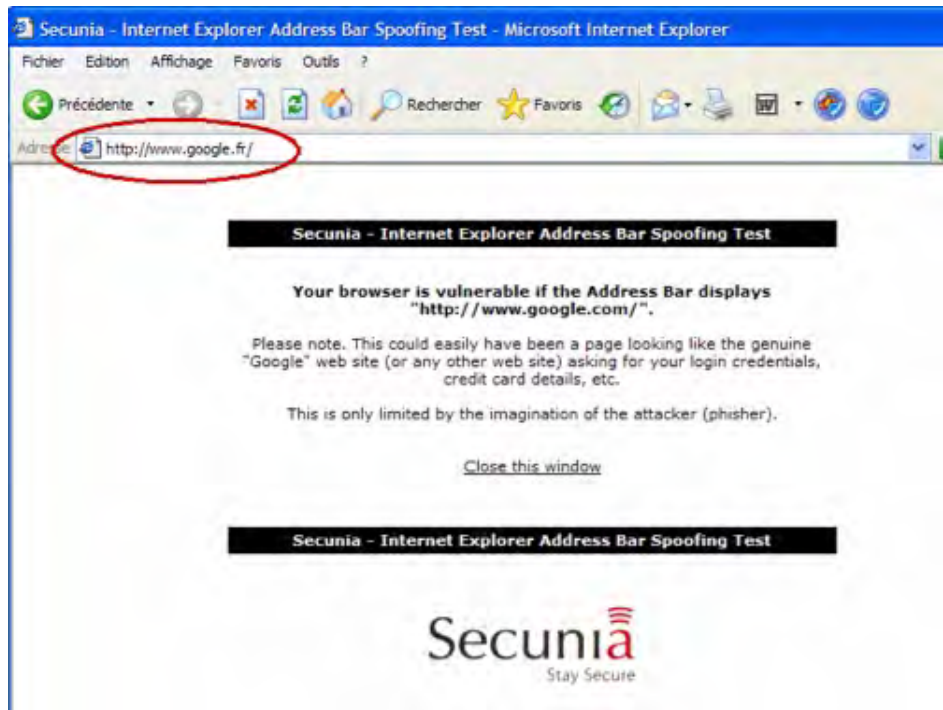


Figure 4.5 — Alors que l'URL est celle de Google, la page en elle-même correspond à un tout autre site.

4.3 LES MÉCANISMES D'ATTAQUES

D'un point de vue technique, ces attaques sont souvent perçues comme requérant un haut niveau de savoir-faire et donc accessible à une élite peu nombreuse. Par exemple, les sites de banque étant souvent utilisés, le grand public imagine que cela nécessite d'attaquer préalablement le ou leurs serveurs. Ces organismes étant bien protégés, le risque est *ipso facto* réduit. Pour la majorité des attaques de *phishing*, il n'en est rien. La plupart du temps, une bonne utilisation de l'ingénierie sociale suffit. Le *phisher* aura réussi son coup si, sur des millions de tentatives, un pourcentage même faible d'utilisateurs y succombent. Ces attaques deviennent alors rentables.



Toutefois, assez souvent les mécanismes mis en place par les escrocs ne peuvent fonctionner que si les victimes elles-mêmes réalisent des actions précises. Les techniques étant très nombreuses, nous n'en détaillerons que les principales¹.

4.3.1 Attaque par le milieu

Le principe est élémentaire : comme toute communication relie un poste client (l'utilisateur qui consulte une page web) et un serveur hébergeant des pages, il suffit à l'attaquant de se placer au milieu de la communication pour observer et analyser toutes les transactions et échanges entre les deux points. L'aspect le plus intéressant est que cette technique fonctionne aussi bien pour le protocole HTTP que pour sa version sécurisée (HTTPS). La situation est résumée sur la figure suivante :

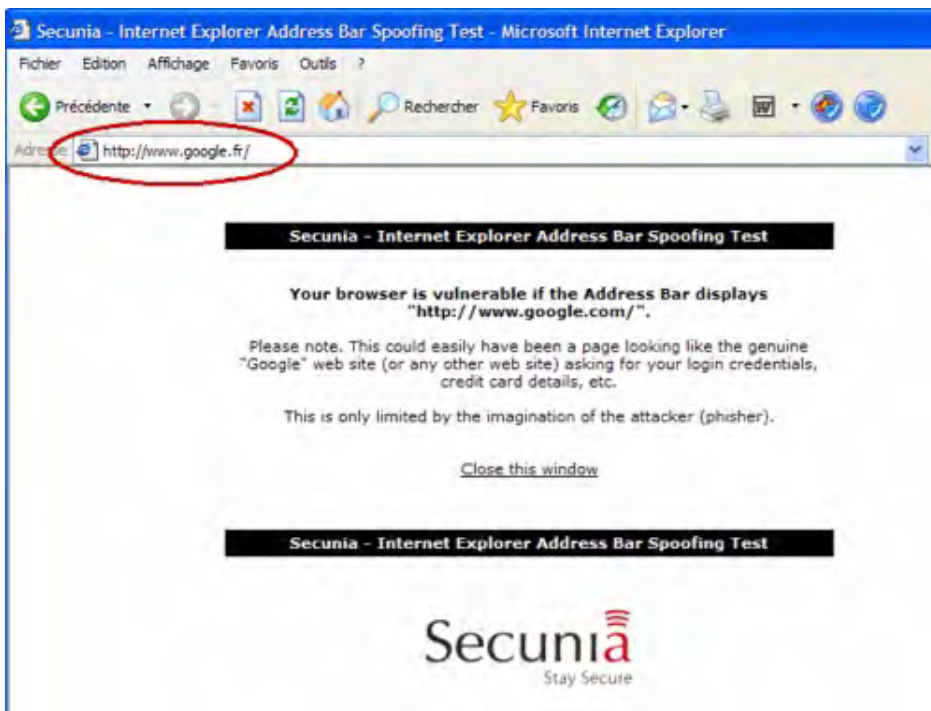


Figure 4.6 — Une connexion sécurisée n'est pas une garantie...

Résultat ? Le client se connecte sans le savoir (de manière transparente) sur le site du *phisher* (incitation par un e-mail au format HTML par exemple) comme s'il s'agissait du site légitime. Le malfrat opère une connexion en temps réel sur le site légitime mais tout en utilisant à ses propres fins les données fournies par le client. Dans le cas de communications chiffrées (par protocole SSL par exemple), la liaison

1. Pour plus de détails, vous pouvez consulter : Gunter Ollman, *The Phishing Guide : Understanding and Preventing Phishing Attacks*, NGSSoftware Insight Security Research, 2004.

client/pirate est bien chiffrée, déchiffrée par le pirate puis rechiffrée pour la liaison pirate/serveur réel. En clair, l'internaute n'hésite pas une seconde à taper toutes ses coordonnées personnelles puisqu'il croit être à l'abri de tout risque de pirate grâce à cette fameuse connexion chiffrée ! On vous laisse imaginer les conséquences pour le commerce électronique (voir chapitre 7).

La partie la plus délicate consiste, pour le *phisher* à parvenir à intercaler un serveur de type proxy¹ entre le client et le serveur. Plusieurs techniques existent :

- **Technique du serveur proxy transparent** : le serveur installé par l'attaquant est situé sur le même segment réseau que celui de la victime (ou le même chemin de routage). L'intérêt de cette approche est qu'aucune modification de la configuration réseau de la victime n'est nécessaire (d'où le terme transparent ; l'interception des données est totalement passive).
- **Technique dite de l'empoisonnement DNS** : le but est de perturber le chemin normal (routage) existant entre la machine de la victime et le serveur d'un site victime de *phishing*. En injectant le cache DNS d'un firewall avec de fausses adresses IP, le routage vers le serveur est dérouté vers le serveur du *phisher*.
- **Modification de la configuration proxy du navigateur** : le truand va modifier la configuration proxy de la victime (avec un code malveillant par exemple) de façon à rerouter le trafic vers un serveur contrôlé par l'attaquant.

4.3.2 Obfuscation d'URL

Le principe de base de toute attaque de *phishing* consiste à inciter la victime, sans l'alerter, à consulter le lien (URL) du site sous la maîtrise du *phisher*. Ce dernier va donc obfusquer ce lien, autrement dit le dissimuler dans le message à destination de la victime. Il est important d'avoir conscience qu'un examen minutieux — certes quelquefois un peu complexe pour un néophyte — d'un message de pirate suffit à détecter une tentative d'attaque. Les principales techniques sont :

Utilisation de noms de domaine modifiés

C'est la méthode de dissimulation la plus couramment utilisée. Les *phishers* achètent des noms de domaine très proches de ceux existants. Imaginons le nom de domaine banque-picsou.com (nom de domaine appartenant à la banque du même nom). Cette banque gère un site de transactions dont l'URL est <http://transactions.banque-picsou.com>. Le pirate peut alors aménager et utiliser des sites, dont il a la maîtrise, dont l'adresse peut être (les possibilités étant bien sûr très nombreuses) :

- <http://banque-picsou.transactions.com>
- <http://transactions.banque-picksou.com>
- <http://transactions.banque-pîcsou.com>

1. Un serveur proxy est un fait une sorte de pare-feu applicatif (couche 7 du protocole ISO).

Dans le dernier cas, il est important de noter la présence discrète d'un « î » rendue possible par le fait que depuis très récemment les noms de domaine peuvent être régionalisés et tenir compte des particularités linguistiques de chaque pays. Ainsi, il y a quelques années, une société russe a acquis le nom de domaine microsoft.com tout simplement en remplaçant un « o » du mot Microsoft par un « o » cyrillique. De même le « i » majuscule, en caractère ASCII peut très facilement être confondu avec le « L » minuscule. Les possibilités sont très variées.

Cette approche a donc de beaux jours devant elle pour trois raisons principales :

- **Le manque d'attention des utilisateurs** : il est dû, en grande partie, à un abus d'ergonomie (trop de fonctionnalités destinées à faciliter — de façon exagérée — le travail des utilisateurs et qui constituent autant de fonctionnalités exploitables par un attaquant).
- **Certains ressorts psychologiques naturels** : un nom est facilement lu et reconnu quel que soit l'ordre de ses lettres à la condition que la première et la dernière restent non permutées.
- **Le manque de vigilance et de contrôle de l'enregistrement des noms de domaine** : les sociétés chargées d'enregistrer les nouveaux sites font parfois preuves de légèreté... « Il y a même des sites de phishing qui ont des certificats serveurs puisque l'enregistrement des .com est très laxiste », révèle Pascal Lointier, président du Clusif.

Liens ergonomiques

Dans un but d'ergonomie, certains navigateurs autorisent des liens incluant directement des informations d'authentification tels que le login et le mot de passe. Une faute grave en matière de sécurité ! Le format général de ces liens est nom_utilisateur:mot_de_passe@nom_hote/chemin_du_site. Un *phisher* peut alors substituer les champs login et mot de passe par le lien du site vers lequel il souhaite attirer la victime. Ainsi, en remplaçant le champ nom_utilisateur par celui de la banque et le champ mot de passe par le nom d'hôte correspondant au serveur du phisher, ce dernier peut parvenir à leurrer les victimes. Ainsi l'adresse suivante :

`http://banque-picsou.com:e-bank@site_du_phisher.com/phishing/fausse_page.html`

peut réussir à faire croire à un utilisateur peu attentionné qu'il consulte une page légitime de la banque Picsou. Face à ce type d'attaque, la plupart des versions récentes des **navigateurs** actuels n'autorisent plus ce type de codage ergonomique.

Détournement de service de simplification d'URL

la complexité et la longueur croissantes des URL de sites ont fait apparaître de nombreuses sociétés proposant des services de simplification d'adresses web. Ainsi des adresses de type `http://petite_url.com` ou `http://min_url.com` sont substituées par ces sociétés de services (en gros, il s'agit d'un service d'alias) en lieu et place des liens démesurément trop longs. Cette facilité — avec de l'ingénierie sociale et des URL volontairement incorrectes et/ou trop longues — a été exploitée avec succès par les *phishers* pour cacher la véritable destination d'un lien.



Fausse lettre, vraie arnaque !

Voici un exemple d'attaque tiré du guide de Gunter Ollman (modifié et traduit pour le lecteur français) :

« Cher client de la banque Picsou,

Nos systèmes de sécurité automatisés ont indiqué que l'accès à votre compte en ligne a été temporairement bloqué le vendredi 13 septembre entre 22h 32 et 23h46 suite à des tentatives répétées de connexion.

Nos journaux de connexions indiquent que votre compte a refusé 2 935 tentatives de connexion pendant cette période. Il est plus que probable que votre compte a fait l'objet d'une attaque par force brute (pour plus d'information, consulter le site <http://support.banque-picsou.com/definitions/attacks.aspx?type=bruteforce>).

Bien que notre banque ait pu bloquer ces attaques, nous recommandons cependant de vous assurer que votre mot de passe est suffisamment complexe pour prévenir des attaques futures. Pour vous connecter et changer ce mot de passe, cliquez s'il vous plait sur le lien suivant :

https://banque-sécurisée.banque-picsou.com/banque-sécurisée/e-banque_v2/secure/support_client.aspx?messageID=332434l&Sess=asp04&passwordvalidate=true&changepassword=true. Si ce lien ne fonctionne pas, utilisez s'il vous plait le lien suivant qui vous redirigera vers la page souhaitée — http://min_url/4outd

Sincères salutations.

Service clients de la Banque Picsou »

L'adresse https est volontairement fausse afin d'inciter la victime à se connecter via l'adresse réduite qui est... sous le contrôle du phisher. Le tour est joué.

Techniques d'obfuscation proprement dites

Le phisher utilise les multiples façons de coder une adresse de site. Rappelons qu'un lien Internet est généralement représenté par une adresse du type <http://banque-picsou.com>. Mais le système travaille lui avec des adresses IP à quatre champs du type 222.102.41.125. La traduction de la forme habituelle (nom d'hôte) en adresse IP est assurée par les serveurs de noms de domaine. Un phisher peut alors jouer de multiples manières en utilisant des codages variés à la fois site d'un pirate dont le nom d'hôte est www.site-phisher.com et l'adresse IP correspondant est 208.132.201.40. Ainsi le lien malicieux <http://banque-picsou.com:e-banque@site-phisher.com/phishing/fausse-page.html> peut être obfusqué par l'adresse suivante :

<http://banque-picsou.com:e-banque@209.132.201.40/login.html>

Il existe de très nombreuses autres possibilités de modification de lien par obfuscation. Les différents types de codage de l'information (caractères d'échappement, bases octales, décimales, hexadécimales, codages unicode, codage UTF – 8...). A moins de décortiquer tous les liens proposés — ce que ne fera jamais un utilisateur — il est très difficile de détecter la nature malicieuse d'un lien.

4.4 LES DIFFÉRENTES PROTECTIONS

L'expérience montre que dans la très grande majorité des cas les attaques reposaient d'une manière plus ou moins importante sur l'ingénierie sociale et la connaissance des habitudes des utilisateurs génériques. Cela implique qu'au-delà des techniques de protection, la sensibilisation des internautes et leur niveau de connaissances restent les meilleures parades. Les techniques de phishing évoluant très rapidement, les techniques de protection doivent évoluer constamment. Or, dans ce duel sans fin entre la lance et la cuirasse — qui est toujours en faveur de l'attaquant — l'utilisateur n'a aucune chance de survie s'il base sa protection sur la seule technique.

D'un autre côté, nous sommes surpris que les banques et autres sociétés visées par le phishing ne s'impliquent (ou ne communiquent) pas plus dans la sensibilisation de leurs clients. A l'heure actuelle, la principale protection développée (du moins la plus visible) est le pavé numérique virtuel. Il est utilisé pour saisir les mots de passe de connexion aux comptes en ligne et ainsi défaire les keyloggers qui enregistrent les frappes de clavier. Pour entrer son mot de passe, le client doit cliquer avec sa souris sur les bonnes touches.

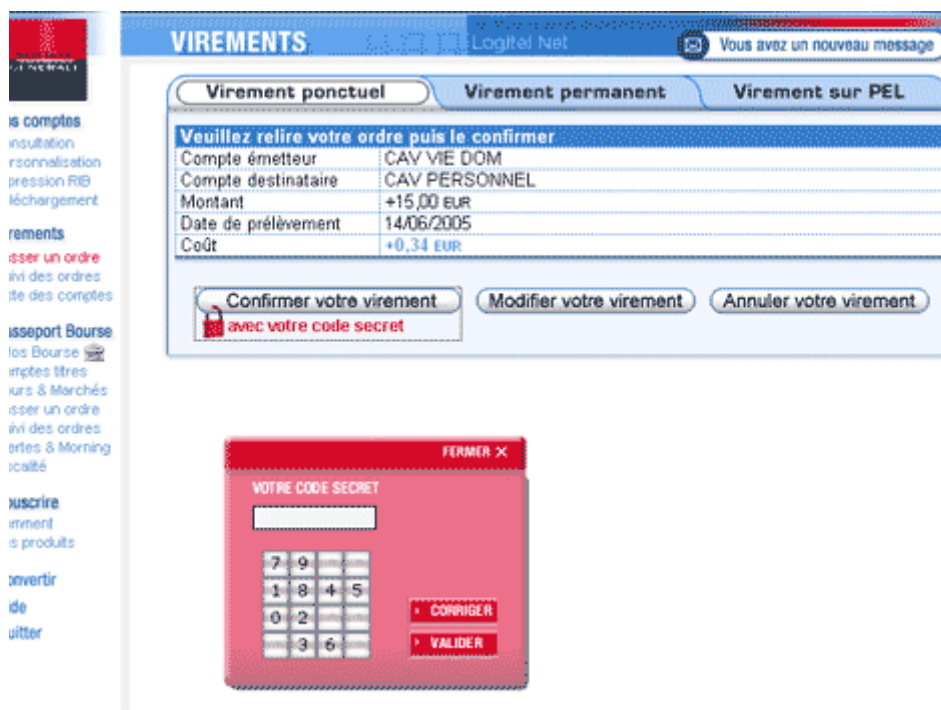


Figure 4.7 – La Société Générale a été l'une des premières à recourir au clavier virtuel.

Ces techniques ont efficaces mais elles ne prennent en compte qu'une partie des attaques existantes. Il existe en effet quelques *keyloggers* spécialisés dans l'enregistrement des mouvements de souris... On les appelle des **screenloggers**.

Toutefois les dimensions de ces pavés ne varient pas tellement d'une banque à une autre et, surtout, sa position sur l'écran n'est pas assez aléatoire. Nous avons pu constater — en tant que client de la Société Générale et en nous rendant plusieurs fois par semaine sur le site pendant plusieurs mois — que le pavé ne va jamais à certains endroits de l'écran...

La vigilance de l'utilisateur étant la meilleure des protections, voici un rappel des mesures qu'il doit prendre et les règles qu'il doit observer sont les suivantes :

- **Ne jamais communiquer des données confidentielles** que ce soit par e-mail, par téléphone ou par quelque autre moyen. Un banquier ou une autre « autorité » (police, service de sécurité informatique...) — ne doit pas vous demander ni votre code PIN ni votre mot de passe. Au pire, il vaut mieux avoir son compte bloqué par la banque que vidé par un pirate.
- **Ne jamais autoriser la mémorisation des mots de passe par le système d'exploitation** : ils sont stockés sur votre disque dans des fichiers en général peu protégés. Un simple code malveillant peut les récupérer et les envoyer à un pirate qui saura les extraire facilement.
- **Faire preuve de méfiance et de bon sens** : Les courriers d'alerte concernant des comptes ou autre ressources sont souvent des pièges. Rappelez-vous qu'en cas de problèmes, votre conseiller bancaire vous contactera. En cas d'alerte par courrier électronique, contactez-le par téléphone. Méfiez-vous de tout formulaire HTML dans un courrier électronique. Ne succombez pas aux propositions alléchantes et autres attrape-nigauds. Contrairement à ce que l'on peut faire croire, on ne gagne rien par e-mail et on ne fait pas non plus fortune. Enfin, analysez et contrôlez un minimum les liens sur lesquels vous cliquez et rejetez tous ceux pour lesquels vous avez un doute.
- **Se méfier de l'ergonomie** : l'industrie informatique nous offre chaque jour un peu plus de facilité et d'aisance d'utilisation (liens automatiques, mémorisation des liens et des mots de passe, la souris...). Mais cette ergonomie devient chaque jour un peu plus incompatible avec une sécurité efficace. Plutôt que de cliquer sur un lien, ressaisissez-le ou utilisez uniquement des liens de confiance.
- **Vérifier manuellement vos comptes régulièrement** : c'est la meilleure manière de détecter des actions frauduleuses. Or, trop d'utilisateurs ne font pas ces vérifications et ne tiennent même pas leur compte à jour.
- **Installer un antivirus, un firewall, un anti-spam et un détecteur de spyware** : Leur installation ne suffit pas. Mettez-les à jour régulièrement. Mais rappelez-vous encore une fois que ces produits ne font pas de miracles et que ce sont des solutions imparfaites (voir chapitre 11) ayant toujours un temps de retard.



- **Porter plainte** : trop de victimes ne le font pas. Or, sans plainte, il n'est pas possible — notamment quand le code PIN n'a pas été utilisé par le *phisher* — d'être indemnisé par la banque. De plus, porter plainte permet aux forces de police de lancer des enquêtes, aux décideurs d'avoir des statistiques fiables. Bref, porter plainte participe du civisme.

En résumé

Les attaques par *phishing* augmentent jour après jour et avec elles le nombre de victimes, provoquant outre des préjudices financiers considérables, une crise de confiance croissante dans les technologies de l'information et de la communication. Faut-il jeter le bébé avec l'eau du bain ? Certainement pas, mais la situation s'explique en grande partie par la folie consumériste dans le domaine des services, notamment des services en ligne. Domaine dans lequel le maître mot est fonctionnalité et non pas sécurité. Il ne faut jamais oublier, en dépit d'un discours marketing absurde que tous ces services, logiciels et fonctionnalités ne doivent pas remplacer l'humain dans la chaîne de communication. Or, c'est précisément parce que beaucoup l'ont oublié que le *phishing* fait des ravages. Alors que la société a pour vocation de protéger les plus faibles, les services et outils mis à notre disposition — la société de consommation — les livrent aux malfrats numériques. Mais les techniques présentées dans ce chapitre restent encore assez rudimentaires. Les *phishers* semblent être passés à la vitesse supérieure comme vous pourrez le constater dans le chapitre suivant. La vigilance est plus que jamais de rigueur.



5

Le phishing : l'approche industrielle

Dans le chapitre précédent, les techniques de phishing présentées agissaient au niveau de l'utilisateur, lequel prenait une part déterminante dans le déclenchement de l'attaque. La protection passait par la sensibilisation des utilisateurs, l'information et la vigilance. Les pirates ont très vite compris que les techniques de *phishing* classiques trouveraient de fait naturellement leurs limites.

La phase suivante a consisté à « industrialiser » les techniques pour évoluer vers des attaques beaucoup plus évoluées, contre lesquelles l'utilisateur, s'il n'est pas un minimum paranoïaque, est quasi-désarmé. Ces techniques sont de différents types : soit l'action du pirate se situe bien en amont du poste client de l'utilisateur, il s'agit alors du *pharming*, soit le pirate utilise la loi du nombre en mobilisant une véritable armée de programmes, les fameux *botnets*, soit enfin il utilise des technologies tellement récentes que l'utilisateur ne se doute pas de la possibilité d'une attaque, et c'est le *vishing*.

5.1 LE PHARMING

Cette technique, dont le véritable nom est *DNS Pharming*¹, consiste à piéger les utilisateurs non plus en s'attaquant à leur propre ordinateur, mais en attaquant les infrastructures du réseau Internet. Ainsi, des millions de connexions légitimes et anodines ont pu être détournées vers des sites sous le contrôle des attaquants. La technique de *pharming* est mise en œuvre par le biais d'une attaque pourtant ancienne (fin des années 90) appelée *DNS Poisoning* (empoisonnement du cache DNS)

1. Le terme provient de la contraction de deux termes : *phone breaking* (piratage téléphonique) et *farming* (culture).

5.1.1 L'attaque par empoisonnement du cache DNS et le pharming.

Rappelons tout d'abord ce qu'est un serveur DNS (*Domain Name Service*) et à quoi il sert. Le TCP/IP, protocole de base pour les réseaux, fonctionne avec des adresses numériques du type 193.205.23.100. Ces adresses ne sont pas d'un usage ergonomique. Aussi associe-t-on à chaque adresse IP numérique un nom de domaine et plus exactement une adresse « en clair » — plus facile à gérer — du type *banque-picsou.com*. L'association d'une adresse IP à une adresse en langage courant s'appelle une *résolution*. Un serveur DNS est en fait un serveur dont le rôle est de réaliser ces résolutions. D'un point de vue pratique, lorsqu'un serveur interroge un autre serveur DNS pour réaliser une résolution (obtenir l'adresse IP d'un nom de domaine) à l'occasion d'un requête, il stocke temporairement le résultat dans sa mémoire cache (en moyenne deux à trois jours). L'objectif de cette mémorisation temporaire est d'accélérer les résolutions en cas de requêtes répétées.

Le principe de l'attaque est alors très simple. Si le serveur est vulnérable (faille de sécurité logicielle, défaut d'administration...) et qu'un attaquant parvient à s'y introduire il peut facilement manipuler les résultats des résolutions contenus dans la mémoire cache et associer à un nom de site connu, l'adresse IP d'un autre site, qui est lui sous le contrôle du malfaisant. L'utilisateur sera alors redirigé en toute transparence vers le site du pirate. C'est l'attaque par empoisonnement de cache.

Le principe général d'une attaque par *DNS Pharming* est alors très simple. Elle se déroule en trois étapes :

1. Corruption des caches DNS de plusieurs serveurs.
2. Redirection des requêtes à destination d'un site de confiance (généralement des sites bancaires, financiers ou commerciaux) vers un site sous le contrôle d'un attaquant.
3. Tentative d'installation de logiciels malveillants (keyloggers, logiciels espions, vers...) ou de captation de données confidentielles par ingénierie sociale et *phishing* traditionnel.

Depuis peu, une version sécurisée du DNS, DNSSEC a été publiée. Elle rend ces attaques théoriquement impossibles du fait de l'utilisation de signature électronique à l'aide de certificats électroniques de confiance. Mais en 2006, ce protocole est encore très peu déployé et de très nombreux serveurs sont vulnérables à l'attaque par empoisonnement de cache DNS.

5.1.2 Quelques exemples d'attaques

Les années 2004 et 2005 ont vu de nombreuses attaques par DNS Pharming et l'année 2006 ne semble connaître qu'une très relative diminution. En 2005, trois attaques majeures ont visé les sites *americanexpress.com*, *msn.com* et *trendmicro.com* ainsi que des milliers d'autres sites. Le trafic vers tous ces sites (courriers électroniques compris) a été redirigé vers des sites sous le contrôle des attaquants. En février



2005, une première vague a visé près de 1 000 sociétés qui disposaient de leurs propres serveurs DNS. Un peu plus tard, en 2005, tous les sites en .com ont été détournés¹. La plupart du temps, la corruption du cache a été permise par l'existence d'une ou plusieurs failles de sécurité dans l'installation par défaut du serveur DNS de Windows NT4 et 2000 SP2. Cela illustre le fait qu'une bonne administration des serveurs couplée à une veille technologique permanente est indispensable si l'on veut éviter ce type d'opérations. Le plus surprenant est de constater que des sociétés de grande envergure, pour lesquelles la sécurité est soit le fonds de commerce (comme la société d'antivirus TrendMicro), soit une part essentielle de son activité (americanexpress.com ou msn.com), puissent souffrir de carences d'administration de leurs serveurs aussi graves que le suivi des correctifs de sécurité.

5.1.3 Quelques mesures de lutte

Pour l'utilisateur méfiant mais un peu versé dans la technique, il est possible de vérifier le DNS d'un site. Ainsi avant d'aller sur le site www.banque-picsou.com, consultez le site Netcraft (<http://news.netcraft.com>). Si ce dernier vous indique que l'adresse est en Chine, l'utilisateur devra renoncer à se connecter à ses comptes.

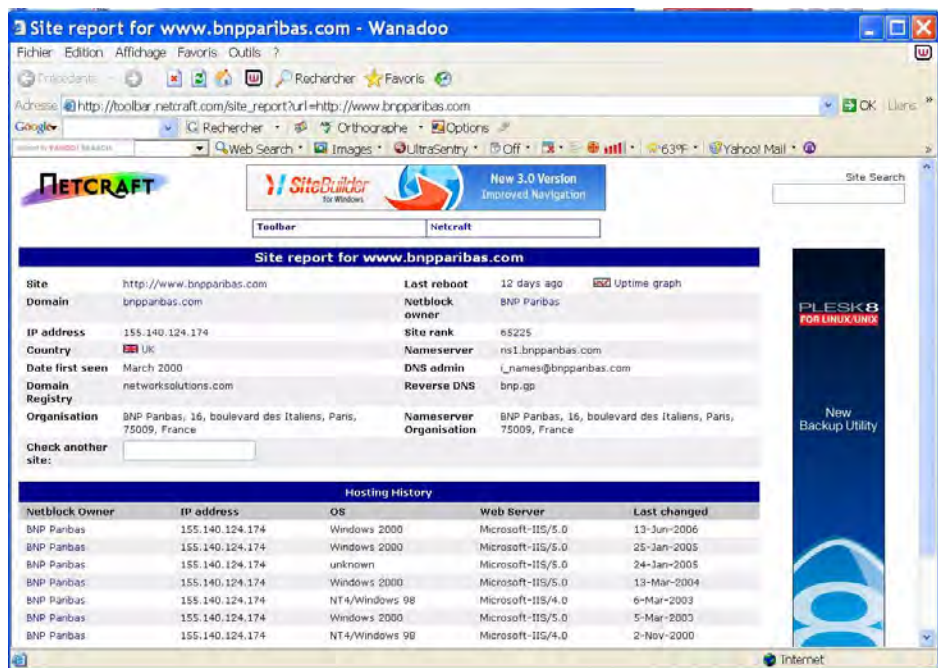


Figure 5.1 — Voici les informations renvoyées par Netcraft pour vérification de DNS sur le site *bnpparibas.com*.

1. Jérôme Saiz, « Internet : l'attaque des serveurs DNS clones ». 4/04/2005. <http://www.lesnouvelles.net/attaques>.

La société Fortinet propose quant à elle cinq méthodes pour stopper un site web utilisé pour du *pharming* :

- 1- Le site n'a pas l'air « normal ». Par exemple, certains éléments nouveaux sont apparus sur le site auquel vous êtes habitués. Sans doute parce que le site est une copie imparfaite de la version légitime. La méfiance est alors de mise.
- 2- Le site demande plus d'informations que nécessaires. Toute demande d'informations confidentielles non habituelles (numéro de carte de bleue alors que vous ne faites pas d'achat en ligne, mot de passe...) est à rejeter.
- 3- L'icône du cadenas SSL (protocole de chiffrement des informations) n'apparaît pas sur le navigateur alors que le site vous demande des informations sensibles (code de carte bancaire lors d'un achat en ligne).
- 4- Le préfixe HTTPS (S pour sécurisé) n'apparaît pas dans la barre d'adresse URL. Les sites « pharmés » n'ont généralement pas de certificats de sécurité et par conséquent le site reste en mode HTTP même lorsqu'il vous est demandé des informations confidentielles normales (achat en ligne).
- 5- Le navigateur émet une alerte concernant un problème de certificat. Le site utilise des faux certificats SSL. Le site est très probablement frauduleux.

Dans tous les cas, si vous avez un doute, notamment après un achat en ligne, n'hésitez pas à contacter votre banque.

5.2 LES BOTNETS

Un **botnet** (littéralement réseau de *bots*) est un réseau de machines compromises (appelées *bot* de « robot » ou encore machine *zombie*) qui ont été infectées par un cheval de Troie, un ver ou un virus, et qui sont administrées par un attaquant. Les logiciels malveillants de ces machines peuvent communiquer ensemble. Le pirate a en fait déployé un véritable réseau parallèle, utilisant les machines d'entreprises ou de monsieur tout-le-monde. Ce réseau va lui servir pour commettre des actions frauduleuses — la plus connue étant le *phishing* ou le *pharming* — voire des délits ou pire des crimes (organisation de réseau mafieux). Cela signifie que des milliers de machines appartenant à de simples utilisateurs ou des serveurs d'entreprises sont utilisées à l'insu de leur propriétaire pour réaliser des exactions numériques. Et l'ADSL et le câble ne font que rendre l'organisation et la gestion de tels réseaux malveillants encore plus aisées. Le pire est que ceux qui déploient ces *botnets* ne sont pas forcément ceux qui les utilisent. Ainsi, trouve-t-on dans des forums des offres de location de temps d'utilisation de *botnets* (quelques centaines d'euros les mille machines pendant une heure). Les mafias de tous ordres n'ont plus qu'à se servir...



5.2.1 Quelques chiffres

Les machines compromises sont essentiellement sous les différentes versions de Windows et l'ont été par utilisation de failles logicielles ce qui laisse augurer, tant au niveau des simples utilisateurs que de nombreux serveurs d'entreprises, des ressources énormes pour les attaquants.

La taille de ces botnets peut être extrêmement importante. Des réseaux de 10 000 à 100 000 machines *zombies* sont couramment rencontrés. Selon honey-net.org, la moyenne des *botnets* comprend 2 000 machines avec un maximum observé de 226 585 machines ! La plupart des études font état d'un total de 500 000 à deux millions de machines *zombies* dans le monde. Selon plusieurs sources (CipherTrust, Trend Micro), en 2005, en moyenne apparaissent 170 000 machines *zombies* infectées par un ver comme Sober... par jour ! Chaque machine *zombie* propageant à son tour l'attaque, les adresses IP infectées, quant à elles, montaient à 250 000 par jour. Le coût induit en termes de bande passante, de stockage et consommations de ressources informatiques en interne est également très élevé.

Pour se faire une idée plus précise, selon l'éditeur d'antivirus Sophos, près de 40 % du spam mondial serait aujourd'hui émis par les PC familiaux devenus des machines *zombies*. Chez Comcast¹, l'un des plus gros fournisseurs d'accès Internet aux Etats-Unis, sur les 800 millions d'e-mails envoyés chaque jour par ses abonnés, 100 millions seulement transitent par ses serveurs officiels. Le reste part des PC de ses abonnés.

EN ce qui concerne la localisation des machines « détournées », les chiffres suivants de 2005, permettent de se faire une idée assez précise².

USA	19,08 %
Chine	14,56 %
Corée du Sud	9,61 %
Allemagne	5,99 %
France	5,69 %
Brésil	5,56 %
Japon	3,70 %
Royaume-Uni	3,13 %
Espagne	2,96 %
Taiwan	2,31 %

1. Jérôme Saiz, La guerre aux zombies est déclarée, 2005, les Nouvelles.net

2. P. Judge et D. Alperovitch, Mapping the Email Universe, Conference Virus Bulletin, 2005.



5.2.3 Les attaques par botnets

Les *botnets* représentent un outil puissant permettant de lancer de nombreuses attaques. Une seule personne — l'attaquant — peut lancer des commandes sur des milliers de machines de manière synchronisée et anonyme (via les canaux IRC notamment). Détaillons les principales attaques possibles.

Le lancement de dénis de service distribués, dans un but de nuisance (atteinte à la disponibilité) ou crapuleux (faire tomber le site d'un concurrent ou rançonner une entreprise). Ce genre d'attaque est quasi-impossible à bloquer car les sources des paquets proviennent du monde entier et de sources diverses. Ainsi, avec un *botnet* de 1 000 machines, disposant chacune de 512 kbits par seconde, on peut générer un trafic total de plus de 100 Mbits, ce qui est très largement supérieur à la grande majorité des débits des accès Internet. Selon honeynet.org, un *botnet* de 13 machines peut suffire à faire tomber un site !

L'envoi de spam. L'installation de serveurs SOCKS permet de faire partir de chaque machine *zombie* des courriers non sollicités (voir figure).

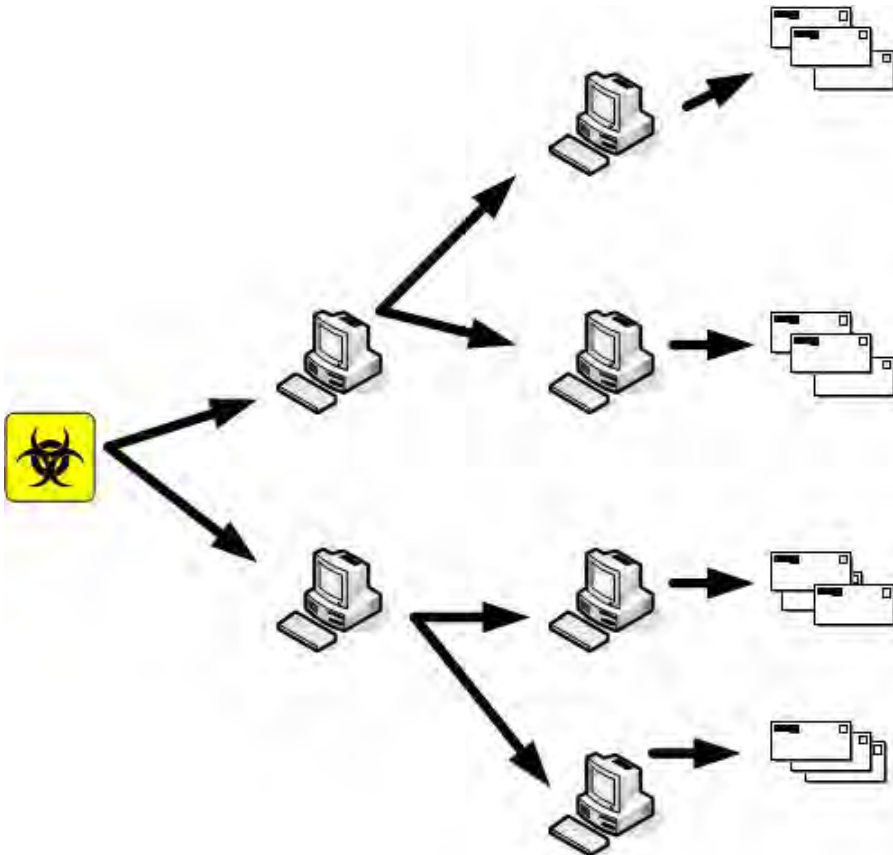


Figure 5.2 — Une grande partie des spams sert aux attaques par phishing.

Espionnage de flux. Chaque machine zombie peut être configurée en « écoute passive » pour *sniffer* les trames réseaux et récupérer des adresses de courriers électroniques (qui deviendront des cibles pour le *spam* ou d'autres attaques), des identifiants/mots de passe, lesquels pour beaucoup circulent en clair sur le réseau.

Espionnage de clavier et récupération de mot de passe et autres informations confidentielles introduites via le clavier.

Diffusion et installation de virus ou de vers, de spywares, lesquels pourront participer, éventuellement à l'action du *botnet* ou à son développement.

Abus de publicités sur Internet. Un grand nombre de publicités fonctionnent sur le principe du paiement au clic. Une armée de bot peut donc générer des millions de clic au profit du gestionnaire du botnet.

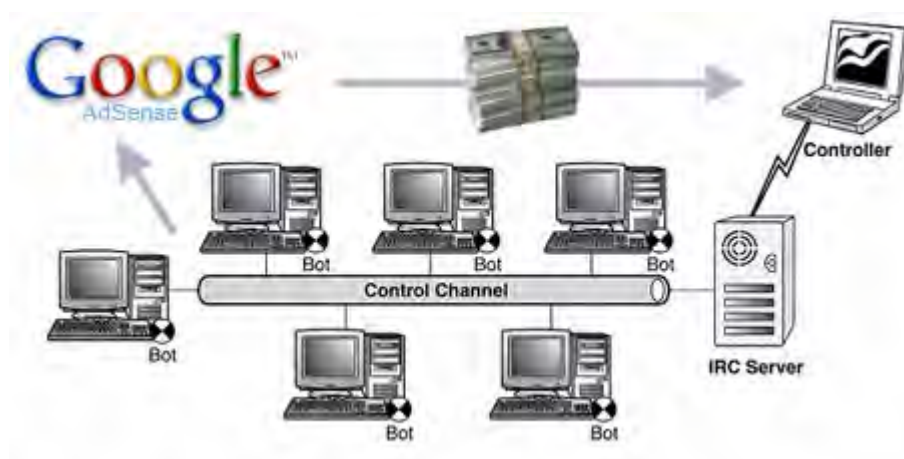


Figure 5.3 — En mai 2006, le service Google AdSense a été victime d'une arnaque aux clics.

Manipulation de sondages ou de jeux en ligne.

Attaques massives par phishing. Des milliers de mails de type *phishing* sont générés. Mais les machines zombies peuvent aussi héberger des faux sites de phishing sur lesquels les victimes seront redirigées pour se faire dérober leurs données confidentielles.

De telles attaques peuvent avoir une ampleur sans précédent. Ainsi, le 2 août 2006, des sociétés du Royaume-Uni ont été bombardées de millions de courriers électroniques de *phishing*. Le botnet utilisé contrôlait plus de 20 000 adresses IP zombies. Pendant 24 heures, plus de 8 millions de courriers de *phishing* ont été envoyés. Ils semblaient provenir de la banque NatWest ou de la banque d'Ecosse :

Official Information To Client Of NatWest bank Mon, 31 Jul 2006 16:58:33 -0800
 Bank of Scotland: Urgent Security Notification For All Clients Mon, 31 Jul 2006 23:49:13 -0100
 NatWest bank: Important Fraud Alert
 Verify Your Data With NatWest bank
 NatWest bank: urgent security notification [Tue, 01 Aug 2006 03:57:17 +0300]
 Verify Your Details With NatWest bank Mon, 31 Jul 2006 16:59:35 -0800
 PROTECT YOUR NatWest bank ACCOUNT Mon, 31 Jul 2006 16:56:07 -0800
 NatWest bank: URGENT SECURITY NOTIFICATION FOR CLIENT

Chaque message contenait une image et si les destinataires de ces courriers cliquaient dessus, ils étaient immédiatement redirigés vers des sites de *phishing*.

Mais les pirates s'adaptent très vite et savent user de finesse. Ainsi, le ou les serveurs web d'attaque du *botnet* peuvent être dupliqués sur le *botnet* lui-même. Il sera ainsi aisé de déplacer ce serveur très rapidement et très souvent, d'un point à un autre de la planète. A chaque fois, il suffira de modifier la résolution du nom de domaine dans la table du DNS.

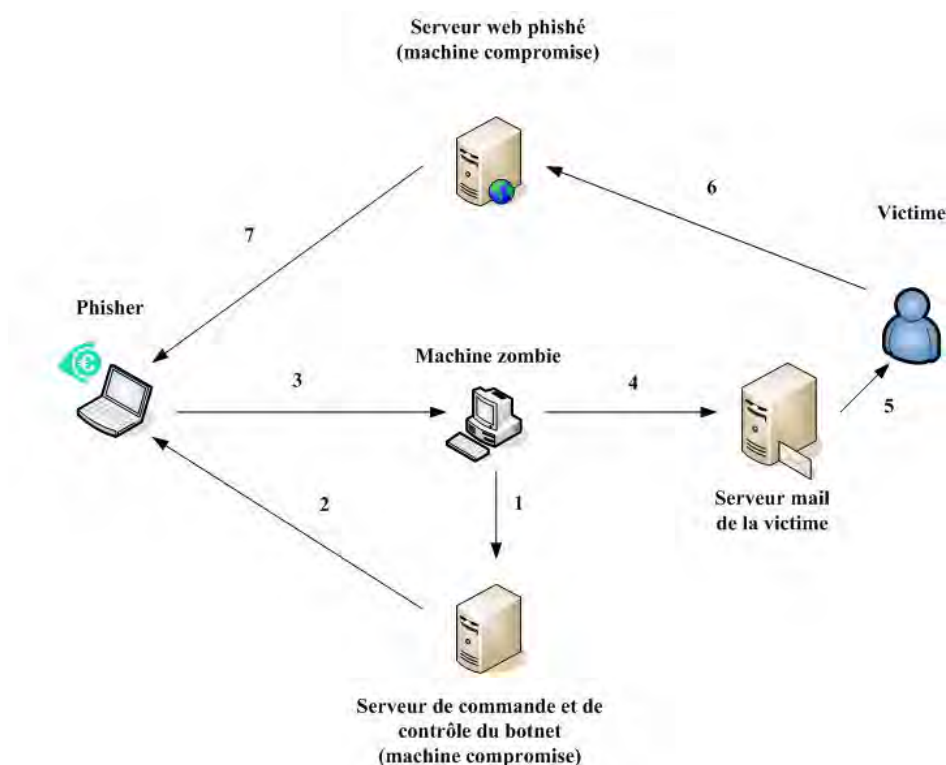


Figure 5.4 — Une fois collectées, les informations seront envoyées au maitre du botnet.

5.3 LE VISHING

Ce terme qui résulte de la contraction de VoIP (voix sur IP) et *phishing* décrit une évolution récente des techniques d'hameçonnage des victimes. L'utilisation des nouveaux moyens de communication permet aux attaquants d'innover en permanence et de piéger des victimes qui ne sont pas encore conscientes du danger. Gageons que les prochaines évolutions technologiques (le monde de la 3G : la vidéo en ligne par exemple) seront ainsi exploitées par les attaquants... La technique du *vishing* mérite d'être détaillée. Ces attaques se sont développées depuis le printemps 2006 et les organismes américains (Bureau fédéral de la consommation et de la protection des consommateurs) et canadiens (Agence de la consommation en matière financière du Canada) ont dû émettre plusieurs alertes tant le phénomène prenait de l'ampleur. En Europe, des cas d'attaques via des téléphones mobiles envoyant des SMS aux victimes ont été enregistrés au Royaume Uni et en Islande.

La technique est simple. L'escroc met en place des serveurs de VoIP, lesquels composent de manière aléatoire des numéros de téléphones fixes commençant par des indicatifs des régions qu'il souhaite écumer. Lorsqu'une personne finit par décrocher, un message enregistré sur une boîte vocale, l'incite à appeler un serveur vocal, dont le numéro est fourni. On lui demandera, pour prétendument l'identifier, de fournir ses identifiants de carte bancaire ou autres informations confidentielles, par saisie sur le clavier du téléphone. Une variante consiste non pas à utiliser un serveur vocal mais de simples courriers électroniques ou des SMS.

Ces attaques sont très faciles à monter. D'une part, les sociétés de téléphonie sur IP sont peu nombreuses et les vérifications à l'ouverture d'un compte, quasi-inexistantes, à l'inverse d'une ouverture de ligne téléphonique traditionnelle. Le tour est joué, il suffit ensuite de maîtriser un minimum les outils de base de la téléphonie sur IP.

A titre d'exemple, voici quelques attaques récentes :

- **Juillet 2006, Angleterre** : Des courriers électroniques sont envoyés indiquant que votre compte *Paypal* ou *eBay* fonctionne mal. Ce courrier, au lieu de vous inciter à consulter un faux site — technique classique de *phishing* — vous indique un numéro de téléphone correspondant à un service clientèle *eBay* ou *PayPal*. A ce numéro, un répondeur automatisé vous demande de fournir vos identifiants (numéro de compte et mot de passe) en les saisissant sur le clavier de téléphone. Si la victime le fait, il est trop tard : l'escroc peut exploiter ces informations pour acheter par exemple un appareil photo sur *eBay* en puisant dans son compte *Paypal*.
- **Juin 2006, Etats-Unis** : la Banque de Santa Barbara a été victime d'une attaque de ce genre de grande ampleur semble-t-il. Un e-mail, usurpant l'adresse de la banque et ayant pour objet « *Message 156984 Client's Details Confirmation (Santa Barbara Bank & Trust)*. » est envoyé aux clients de cette banque.



Le message est le suivant¹ (traduction) :

Cher client,

Nous avons constaté que vous avez eu des problèmes pour vous connecter au site en ligne de la banque Santa Barbara Bank & Trust.

Après trois tentatives infructueuses de connexion, votre compte en ligne sur le site de la banque Santa Barbara Bank & Trust Online Profile a été verrouillé. Ceci a pour but de sécuriser votre compte et protéger ainsi vos informations confidentielles. La Santa Barbara Bank & Trust s'est en effet engagée à toujours protéger vos données et à faire en sorte que vos transactions en ligne soient sécurisées.

Appelez ce numéro de téléphone (1-805-XXX-XXXX) pour vérifier et valider votre compte et votre identité.

Sincèrement

Santa Barbara Bank & Trust Inc.

Service clientèle.

Le lecteur remarquera le ciblage précis des victimes et l'ingénierie sociale mise en œuvre. Il est à craindre que les victimes aient été nombreuses.

En résumé

Le pire est devant nous. Les escrocs ont de l'imagination et certains maîtrisent parfaitement les dernières techniques. Face au *pharming*, au *vishing* et aux techniques qui immanquablement vont apparaître, il est essentiel de rappeler qu'il ne faut jamais communiquer des données confidentielles que ce soit par courrier électronique ou par tout autre moyen. Les attaques de demain prendront peut-être la forme de communications vidéo (avec la téléphonie 3G) dans laquelle votre conseiller financier (ou plutôt sa doublure, son sosie ou tout bêtement son remplaçant) vous demandera de vous « authentifier ». Couplées à des techniques de *morphing*, qui sait ce que pourront être ces attaques. Mais la défense s'organise jour après jour, même si les grands noms de l'industrie de la sécurité informatique affichent un certain pessimisme¹. Trois partenaires de Microsoft — Cyota, Internet Identity et Mark-Monitor — se sont alliés pour alimenter la base anti-phishing de Microsoft. Cette base contient les informations de toutes les attaques répertoriées², lesquelles alimentent les outils de filtrage de l'éditeur (*Phishing Filter*, *SmartScreen Technology*). Ces solutions ne sont pas suffisantes en elles-mêmes mais c'est un début d'autant plus intéressant que les techniques d'attaques actuelles ne laissent plus beaucoup d'espoirs de résoudre les choses au niveau de l'utilisateur seul.

1. Le lecteur pourra écouter le message vocal qui avait été mis en place par l'attaquant en consultant le lien suivant http://www.websense.com/securitylabs/images/alerts/june_vishing.wav.

2. TrendMicro affiche son pessimisme, 2005, <http://www.Silicon.fr>.

3. Microsoft : trois listes noires pour lutter contre le phishing, 2005, <http://www.Silicon.fr>.



6

Le racket numérique

Cette technique, qui consiste selon le droit français à « *obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* », existe depuis des lustres. Les malfrats ont toujours su l'adapter aux moyens de l'époque. En ce XXI^e siècle, les racketteurs utilisent l'informatique. Exit donc les brigands stoppant des diligences et les organisations criminelles enlevant le fils d'un grand patron. La méthode est certes moins violente mais le résultat semble tout aussi efficace.

Des bandes ou des mafias d'Europe de l'Est, du Brésil et de Chine en ont fait leur spécialité. Le racket informatique n'est pas nouveau. Des chantages à la « bombe logique » sont devenus des cas d'école pour les spécialistes en sécurité. Il s'agit d'un programme malveillant qui ne se déclenche que lorsque certaines conditions sont réalisées (date système, présence ou absence d'une donnée dite « d'activation », action particulière de l'utilisateur...). La bombe peut être introduite de deux manières différentes :

- Par programmation directe, ce qui impose que l'attaquant dispose d'un accès logique au système et de bonnes connaissances en programmation ;
- Par l'introduction dans le système à l'aide d'un support matériel (média) ou par le biais des réseaux, de logiciels déjà infectés, ce qui impose là également de disposer d'un accès physique ou logique au système.

Cette bombe est camouflée dans un virus ou un ver, deux codes qui ont la faculté soit de se reproduire en de nombreux exemplaires (le premier), ou de se déplacer d'un ordinateur à un autre (le second). « Après une phase d'installation, de reproduction ou de déplacement, durant laquelle ils passent généralement inaperçus, et lorsque les conditions définies pour l'« explosion » de la bombe logique sont remplies, la charge finale du virus ou du ver devient active : l'action de la bombe logique est généralement brève et définitive. Le but est essentiellement destructif (informations et parfois matériels) » explique-t-on à la Direction centrale de la sécurité des

systèmes d'information (DCSSI) qui dépend des services du premier ministre (Secrétariat général de la défense nationale ou SGDN).

Ces bombes logiques sont généralement utilisées dans le but de créer un « déni de service » en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise. Mais les racketteurs disposent de différentes techniques.

6.1 LES ATTAQUES CONTRE LES ENTREPRISES

Les blogs sont à la mode. Il n'est donc pas étonnant que les sites qui hébergent ces journaux personnels soient devenus depuis quelques années les cibles des pirates. L'une des dernières grosses attaques a eu lieu en mai 2006. Plus de 10 millions de sites personnels et blogs hébergés par la société américaine Six Apart ont été inaccessibles pendant plusieurs heures le 2 mai. L'attaque a été contrée en filtrant les *spams* envoyés.

Les pirates ont en effet réalisé une attaque DDoS (voir chapitre 1) qui consiste à bloquer l'activité d'un serveur en le submergeant de requêtes (des millions en quelques secondes) afin d'engendrer un trafic de connexions ingérable. Dans quel but ? Selon les propos de Loïc Le Meur, directeur général de Six Apart Europe, recueillis par le site Silicon.fr, l'attaque visait prioritairement Blue Security, qui cherche à développer des outils contre le spam et dont le site Web est hébergé par Six Apart. L'indisponibilité des blogs n'en a été que la conséquence.

Victoire des spammeurs

Cible de l'attaque contre l'hébergeur Six Apart, la Blue Security a jeté l'éponge quelques jours plus tard. Cette société israélienne avait développé une solution qui semble-t-il était efficace puisqu'elle a entraîné cette vive réaction des spammeurs et plus précisément de PharmaMaster, basé en Russie et soupçonné d'être à l'origine de l'attaque. Le logiciel israélien avait trouvé l'un des points sensibles. Comme d'autres logiciels antispams, il filtrait les e-mails de ses dizaines de milliers de clients. Mais en plus, il envoyait automatiquement des avertissements aux sites sources et aux hébergeurs à l'origine de ces courriers non sollicités. Si l'expéditeur en question ne répondait pas, Blue Security l'inondait à son tour d'e-mails.

Mais une tentative de racket n'est pas à exclure. Ce ne serait d'ailleurs pas la première fois. L'année dernière, un hébergeur de sites à Paris a été victime de racket. Son réseau a été saturé pendant plusieurs heures. En août 2003, le site de Microsoft a été bloqué pendant plus de deux heures. Durant le Superbowl 2003 aux États-Unis, un racketteur avait menacé plusieurs sites de paris en ligne d'une attaque en déni de service s'ils ne s'acquittaient pas d'une somme allant de 10 000 à 50 000 dollars.



En 2004, c'est au tour d'Akamai, l'un des principaux fournisseurs de services réseaux, d'être touché avec pour conséquence l'interruption du trafic de sites parmi les plus fréquentés au monde tels que Yahoo !, Google, Microsoft ou Apple.

La même année, la banque japonaise Softbank est à son tour touchée. Une somme de 28 millions de dollars lui est réclamée contre la non divulgation de données personnelles touchant 4,5 millions de clients. Depuis, quatre suspects ont été arrêtés au pays du soleil levant. La même année, Google est visé par un maître chanteur. Il réclame 100 000 dollars pour la non utilisation d'un logiciel qui fausserait le système de paiement des publicités postées sur le célèbre moteur de recherche. L'auteur présumé de ce chantage a été inculpé. C'est d'ailleurs pour cela que l'affaire s'est ébruitée.

Comme dans de nombreuses affaires de cyberdélinquance, il est en effet très difficile de savoir si des entreprises ont été visées et encore moins si elles ont finalement payé la rançon. Les pertes occasionnées par la paralysie du système sont par contre un peu plus connues. Les sites de bookmakers anglais Tote et SportingBet ont été victimes d'escrocs il y a quelques années. Ils n'ont pas payé mais les pertes financières auraient atteint plus de 20 millions d'euros.

Apparues au début des années 2000, ces attaques se multiplient selon différentes sources. Les auteurs sont en général des mafias des pays de l'Est ou d'Asie. Il est en revanche difficile d'avoir des chiffres précis.

6.2 LES ATTAQUES CONTRE LES PARTICULIERS

Les internautes ne sont pas non plus à l'abri d'une tentative de racket. Évidemment, il ne s'agit pas pour les malfrats de récupérer autant d'argent que s'ils s'attaquaient à une entreprise. Il s'agit dans ce cas-là d'extorquer de petites sommes d'argent à des particuliers. Inutile dans ce cas de déployer la grosse artillerie (attaque DDoS). Le courrier électronique suffit. Pour atteindre son but, le pirate va essayer d'immiscer dans le PC visé des données compromettantes (photographies pédophiles notamment) ou d'y glisser un petit programme qui va rendre inaccessible une partie du disque dur. Et comme toujours, à l'insu de la personne.

Que ce soit les images ou la prise d'otage de documents personnels, l'internaute ne peut pas y accéder pour les supprimer (système de chiffrement) à moins d'être un spécialiste de ce genre de protection. Il n'y a donc que le pirate qui détient la clé permettant de déverrouiller la partie du disque dur. Il exige quelques dizaines d'euros qu'il faut verser sur un compte bancaire bien à l'abri d'un paradis financier ou sur un compte eGold.

Les premières tentatives remontent à 1991 avec un cheval de Troie baptisé AIDS. Sous couvert d'un logiciel d'information sur le SIDA, il utilisait le chiffrement de données pour extorquer une somme de 378 dollars. Ce genre d'attaque est ensuite réapparu sous diverses formes. On en a beaucoup reparlé avec le code Tro-



jan.PGPcoder en 2005. Ce type d'attaque relève de la crypto-virologie définie par Young et Yung¹.

Selon différents éditeurs d'antivirus, plusieurs attaques de ce genre auraient été repérées au printemps 2006. SophosLabs aurait ainsi identifié un cheval de Troie qui encrypte les données de ses victimes, avant d'exiger 300 dollars de rançon contre le mot de passe permettant de les retrouver. Baptisé Zippo-A (également dénommé CryZip), il recherche sur l'ordinateur les fichiers de type documents Word, bases de données ou feuilles de calcul et les transforme en fichiers ZIP.

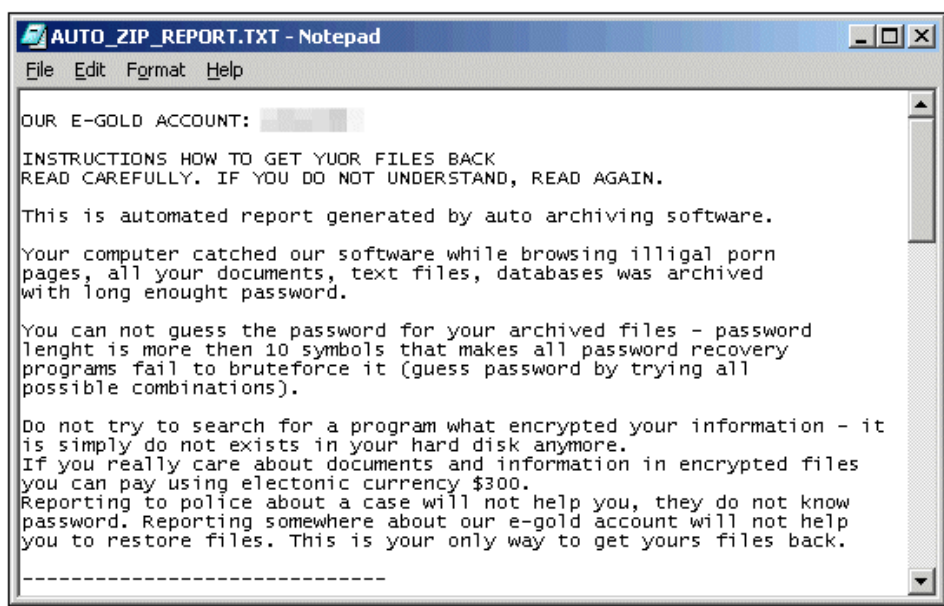


Figure 6.1 — Le cheval de Troie Zippo rançonnerait les internautes

Deux mois plus tard, c'est au tour de Ransom A de faire parler de lui. Du moins, il permet surtout à Sophos de faire reparler de lui. Ce cheval de Troie menace sa victime de détruire un fichier toutes les 30 minutes sur son ordinateur jusqu'à ce qu'elle paie une rançon de 10,99 dollars pour obtenir le code de désactivation.

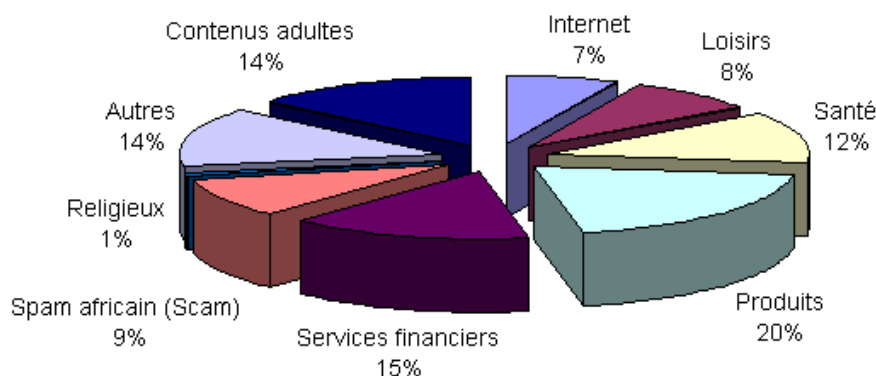
Les salariés peuvent aussi être visés. F-Secure, un éditeur informatique finlandais spécialisé dans la sécurité, a révélé que le personnel d'une grande université scandinave avait été la cible d'une tentative d'extorsion de ce genre. Ils avaient reçu un e-mail, apparemment en provenance d'Estonie, qui indiquait que l'expéditeur avait découvert plusieurs failles de sécurité dans le réseau informatique et menaçait d'effacer un grand nombre de fichiers, sauf si les destinataires payaient 20 euros sur un compte bancaire en ligne.

1. Adam L. Young et Moti Yung *Malicious cryptography : exposing cryptovirology*, Wiley.

Il ne faut bien sûr pas accepter ce chantage car ensuite l'escroc pourra récidiver et demander plus... Quelles sont alors les solutions pour s'en sortir ? Il faut mettre beaucoup de sécurité en amont car une fois que ce type de code a frappé, il n'existe aucune solution, du moins accessible à un utilisateur ou une PME.

6.3 LES SPAMS

Les programmes malveillants ne sont pas les seules techniques utilisées pour extorquer une somme d'argent plus ou moins conséquente à un internaute. Le spam est aussi très efficace et beaucoup plus répandu que les chevaux de Troie qui bloquent quelques dossiers. Le spam est même devenue une véritable pandémie. Les boîtes aux lettres électroniques (e-mail) des internautes sont parfois envahies par ces messages publicitaires sauvages envoyés à des millions de personnes qui n'ont rien demandé. « Achetez du Viagra à bas prix », « Obtenez les prêts les plus bas », « Rendez les femmes heureuses »... ce genre de messages racoleurs envahit de plus en plus les e-mails des internautes



Source : Brightmail's Prove Network (2003), *The State of Spam – Impact & Solutions*, Brightmail Incorporated.
(www.brightmail.com/press/state_of_spam.pdf, consulté le 9 janvier 2004).

Figure 6.2 — Répartition des spams par contenu.

Après avoir touché les États-Unis depuis le milieu des années 90, ce phénomène tend à se généraliser en Europe. Selon une étude réalisée en octobre 2004 dernier par le Pew Internet & American Life (un des organismes américains à but non lucratif les plus respectés en matière d'analyse du réseau), la part du spam est évaluée à 50 % du trafic e-mail total. 90 % des internautes français recevraient du spam selon une étude AOL-Novatris d'octobre 2003.

Les particuliers, les entreprises et les fournisseurs d'accès à Internet (FAI) paient très cher cette avalanche de spams. En Europe, la facture est estimée à plus de 10 milliards d'euros. Selon l'éditeur Sophos, les spams envoyés au cours du premier trimestre 2006 proviennent essentiellement des États-Unis (pour plus de 23 %), de la Chine (22 %) et de la Corée du sud (9,8 %). En Europe, la France est le principal pays pourvoyeur de spam (avec 4,3 %), suivie de la Pologne (3,8 %), de l'Espagne (3,3 %) et de l'Allemagne (3 %). D'après l'association américaine à but non lucratif Spamhaus — qui exploite un « Registre d'opérations spam connues » (ROKSO, *Register of Known Spam Operations*) —, 90 % des spams reçus par les internautes en Amérique du Nord et en Europe sont envoyés par un groupe restreint de quelque 180 personnes seulement, presque toutes fichées dans la base de données ROKSO.

Des millions de spams en une heure !

Pour inonder la planète en quelques heures, les spammeurs ont souvent recours à une méthode très efficace : ils utilisent les PC d'abonnés à haut débit. La technique est simple : un petit fichier exécutable est caché dans le corps d'un e-mail qu'ils vous adressent. Ce procédé leur permet ainsi d'utiliser votre PC comme relais, le fameux « PC zombie ». A moindre frais (c'est vous qui payez en quelque sorte la bande passante) et de façon incognito (c'est votre adresse IP qui apparaît). L'autre technique consiste à se connecter illégalement au serveur (mal protégé) d'une entreprise afin d'utiliser sa ressource pour expédier des spams. Grâce à ces méthodes, des millions de spams peuvent être envoyés en une journée. Selon le site américain www.spamhaus.org, le numéro 1 mondial des spammeurs serait Eddy Marin. Habitant en Floride, cet homme de 41 ans est capable d'expédier quelque 50 millions de spams en une journée.

Comment les spammeurs récupèrent-ils les adresses e-mails ? Ils disposent de différentes pistes. La principale ? les forums de discussion. Une étude américaine estime que 100 % des e-mails des « chat room » sont détournés. La proportion atteint 86 % pour les newsgroups et les pages Web d'un site. Ils peuvent aussi récupérer un listing d'e-mails qu'un FAI a revendu à un tiers, qui l'a lui-même revendue à un autre, etc.

Une fois sa base de données alimentée, le spammeur se transforme en commerçant. Il vend tout et n'importe quoi mais surtout des produits miracles ou des « affaires en or ». Et ça marche ! Une étude de Pew Internet & American Life Project indique que 7 % des internautes ont commandé un bien ou un service proposé par un e-mail non sollicité (mais ils n'étaient pas tous de purs spams) et 33 % d'entre eux ont au minimum cliqué sur le lien proposé pour avoir plus d'informations.

6.3.1 Le spam nigérian

Imaginée par des escrocs du Niger il y a une dizaine d'années, cette technique consiste à demander aux internautes de verser une certaine somme d'argent afin de



Arrestation de spammeurs

En mai 2006, les autorités sud-coréennes ont arrêté un homme soupçonné de gérer une armée de 16 000 ordinateurs « zombies ». Elle lui aurait permis d'envoyer 18 millions de spams par jour. Quelques mois plus tôt, en Australie, un homme a été arrêté pour avoir envoyé 56 millions de spams. Il s'appuyait sur une base de données de 11,8 millions d'adresses. Il risque une amende d'environ 660 000 euros

toucher une commission plus élevée sur une plus grosse somme. Très souvent, l'e-mail est soi-disant envoyé par un haut fonctionnaire, un haut gradé de l'armée, un politicien, un membre d'un fonds pétrolier ou une très jolie femme. Son problème : faire sortir du pays une somme de plusieurs millions d'euros (dans le cas de la jeune femme, il s'agit d'obtenir les quelques euros qui lui manquent pour acheter un billet d'avion et rejoindre sa cousine en France par exemple). Il recherche un prête-nom et vous demande donc d'ouvrir, à votre nom, un compte dans une institution financière de votre pays et de lui en communiquer le numéro. Pour vous récompenser, il vous offrira une commission qui peut atteindre 25 % du montant transféré. Quelques semaines après l'ouverture du compte, une deuxième lettre vous informe que les fonds sont sur le point d'être débloqués... mais que vous devez au préalable vous acquitter de frais juridiques minimales (environ 300 €) qui correspondent à de soi-disant frais de douanes ou d'avocat. Évidemment, vous ne verrez jamais la couleur de l'argent !

« Cette arnaque marche toujours très bien car elle vise ce que les gens ont de plus sensible : le sexe, le désir d'argent immédiat, l'affection », indique Yves Crespin de la BEFTL.

Mais la police a du mal à repérer les personnes à l'origine de ces arnaques car très souvent les victimes n'osent pas porter plainte. Selon Yves Crespin, les cas de spams nigériens sont rarement connus car les personnes n'osent pas contacter les autorités avant d'avoir été escroquée de 15 000 euros : « en dessous, elles portent rarement plainte », nous a-t-il indiqué.

Il existe néanmoins quelques cas de démantèlement de réseau. Début 2006, les autorités néerlandaises ont arrêté douze personnes à Amsterdam. Elles sont soupçonnées d'avoir monté une arnaque du type spam nigérian. Leur affaire leur aurait rapporté quelque 2 millions d'euros. En 2005, les autorités espagnoles avaient mis fin aux agissements d'un réseau encore plus important. Environ 310 personnes avaient été arrêtées à Malaga car elles étaient soupçonnées d'avoir détourné près de 300 millions d'euros. Cette escroquerie aurait fait plus de 20 000 victimes dans 45 pays, dont la France, l'Espagne, le Royaume Uni, l'Allemagne, les États-Unis, l'Australie et le Japon.

Microsoft s'attaque au spam nigérian

Fin 2005, le géant américain a annoncé qu'il allait collaborer avec la Commission gouvernementale nigériane chargée des délits financiers et économiques (*Nigerian Economic and Financial Crimes Commission*). L'objectif est de renforcer la collaboration entre Microsoft et l'Etat nigérian. L'EFCC indique enquêter sur plusieurs centaines de suspects dans le cadre d'une cinquantaine de cas d'actes identifiés jugés malveillants. Des investigations qui auraient permis la mise en accusation d'une centaine de personnes.

6.4 DES PARADES PLUS OU MOINS EFFICACES

L'OCDE aurait-elle accouché d'une souris ? En avril 2006, l'Organisation de coopération et de développement économiques, (club des pays riches du bloc occidental) s'est dotée d'une « *task force anti spam* ». Son premier travail a été de publier un document intitulé « *Oecd AntiSpam Toolkit* » (www.oecd-antispam.org). C'est un dossier très complet sur l'état du spam. Mais les solutions préconisées pour endiguer ce fléau laissent septiques bon nombre de spécialistes. Les mesures restent générales. « Des formations sur le spam et la sécurité sur l'Internet devraient être intégrées aux cours d'informatique dispensés dans les écoles et à la population âgée », estime par exemple l'OCDE.

La position de cet organisme diffère de celle de l'UIT¹ (Union internationale des télécommunications) qui s'est clairement prononcée pour une véritable prise de conscience politique et une volonté d'échange Nord-Sud efficace :

- Activités de sensibilisation, promotion de la coopération et de l'éducation
- Organisation de conférences sur le spam, groupes de travail, etc.
- Sensibilisation des pays membres sur les problèmes et l'impact du spam et sur les solutions possibles
- Développement de normes techniques.

A l'occasion de la « Journée Mondiale des Télécommunications », qui commémore chaque 17 mai sa naissance en 1865, l'UIT a lancé une campagne de sensibilisation et d'éducation des consommateurs. Ces derniers sont invités à être très vigilants et à protéger leur boîte aux lettres électroniques en utilisant des solutions logicielles...

1. www.itu.int/osg/spu/spam/.



6.4.1 Les logiciels antispams

Ces solutions antispams peuvent être classées en trois catégories : les logiciels à installer sur son ordinateur, les gestionnaires d'e-mails en ligne et les services en ligne. L'internaute a l'embarras du choix puisqu'il existe plus d'une centaine de références. Les deux tiers sont payants (de 30 à 50 €) et la majorité ne fonctionne que sous Windows. Mais sont-ils vraiment efficaces ? Principal reproche : ils laissent toujours passer des spams mais bloquent par erreur des e-mails valides.

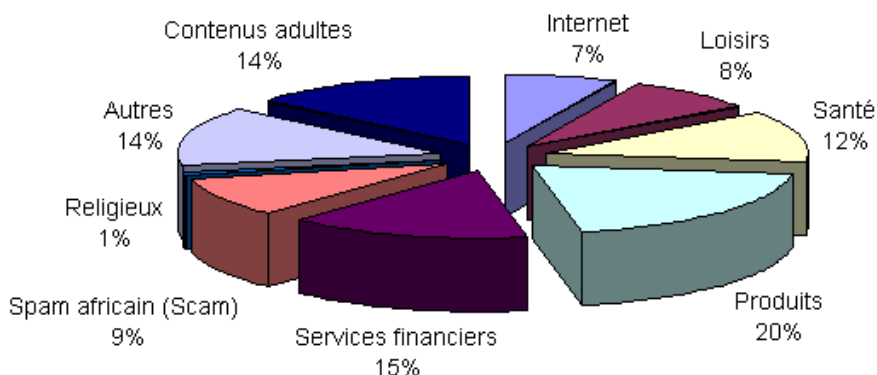
Quelle que soit la catégorie, ces solutions reposent sur deux types de technologies :

- Les techniques (statistiques) de filtres bayésiens qui utilisent des estimateurs statistiques lesquels sont affinés en permanence en « apprenant » à partir du spam reçu. Ces techniques, par leur nature statistique même, sont faillibles. Les probabilités de fausse alarme et de non détection ne peuvent être nulles et ne le seront jamais.
- Les techniques de Turing. Il s'agit de faire la différence entre un humain et un automate. Ces techniques sont fiables à 100 % mais requièrent un pré-traitement initial des e-mails. L'autre contrainte tient au fait que le trafic e-mail de l'utilisateur est en général hébergé pour le traitement du spam ce qui peut poser des problèmes de confidentialité pour certaines entreprises. Une solution quasi-parfaite est par exemple le logiciel/service proposé par la société française MailInBlack.

Des logiciels perfectibles

Une étude comparative publiée en 2004 par le mensuel *60 Millions de consommateurs* indique qu'ils ne sont pas la panacée. Voici quelques-unes de ses conclusions : « Ils ne permettent pas à eux seuls de résoudre le problème. (...) Pour être efficaces, la plupart de ces programmes exigent de passer beaucoup de temps à peaufiner les réglages et à comprendre les différentes notions de filtrage. (...) La plupart des antispams testés par « 60 » mériteraient d'avoir un paramétrage et une interface plus accessibles pour le grand public... ». Ils sont donc encore perfectibles.

Ces antispams en ligne sont, à notre avis, plus efficaces car ils s'attaquent au point faible des logiciels-robots des spammeurs : ils ne savent pas lire et écrire ! Avant de transmettre l'e-mail à son client, le site antispams demande à l'expéditeur de s'authentifier en tapant un code confidentiel de 6 caractères fourni dans cette requête. S'il répond, l'e-mail est immédiatement transmis et son adresse est ajoutée à la liste des expéditeurs autorisés. Ses prochains messages seront directement récupérés (sans procédure d'authentification). Comme le logiciel-robot ne va pas répondre, son courrier sera donc bloqué.



Source : Brightmail's Prove Network (2003), *The State of Spam – Impact & Solutions*, Brightmail Incorporated.
(www.brightmail.com/press/state_of_spam.pdf, consulté le 9 janvier 2004).

Figure 6.3 — schéma d fonctionnement du service proposé par la société française Mailinblack.

D'autres solutions sont envisagées. Les logiciels antispams pourraient s'appuyer sur une technique de filtrage issue de la bio-informatique. Au lieu d'analyser des séquences d'ADN, l'algorithme Chung-Kwei (nom d'un talisman censé protéger la maison des esprits diaboliques) a été utilisé pour démasquer des spams. Développé par IBM, ce programme en a repéré 64 665 sur 66 697 messages identifiés comme « spam » lors d'un test. IBM pourrait l'intégrer à SpamGuru, son produit antispam.

6.5 LES SPAMMEURS ONT TOUJOURS UN COUP D'AVANCE

« L'innovation est forte dans ce domaine car les spammeurs ont les moyens (financiers) pour leur propre R&D », reconnaît François Paget, chercheur chez l'éditeur d'antivirus McAfee. Pour contourner les différents obstacles mis en place notamment par les éditeurs et les fournisseurs d'accès à Internet, les spammeurs sont à l'affût de tout nouveau procédé.

6.5.1 L'e-mail furtif

« Pour vivre de son business, vivons cachés ». Telle pourrait être la devise des spammeurs. Pour ne pas éveiller les soupçons, ils commencent à privilégier les petits volumes de spams plutôt que les énormes vagues, qu'on appelle « mass mailing ». Envoyer une quarantaine d'e-mails par heure permettrait de passer inaperçu. C'est en effet le meilleur moyen pour échapper aux sondes de surveillance sur Internet (pour les vers par exemple).



6.5.2 Des e-mails qui leurrent les logiciels antispams

Pour contourner ces obstacles, les spammeurs sont à l'affût de tout nouveau procédé. Publiée début 2006, l'étude¹ menée par deux chercheurs du département « Computer Science » de l'université de Calgary au Canada pourrait donc les intéresser. Ils annoncent avoir découvert une nouvelle technique de spam capable de passer au travers des filtres les plus efficaces et donc de tromper les internautes.

Les chercheurs canadiens se sont appuyés sur deux bases de données. La première contient des courriers électroniques écrits par des particuliers. La seconde comprend des e-mails publicitaires. Un programme informatique a ensuite combiné les données en identifiant de manière statistique les tournures de phrases types (et les fautes d'orthographe ou de grammaire les plus classiques), les abréviations et les signatures. Un second programme utilise ensuite cette écriture « naturelle » pour écrire des spams.

Pour mettre en pratique ce procédé, « les spammeurs pourraient infecter les ordinateurs des particuliers pour « enregistrer » à leur insu leurs e-mails. L'objectif serait alors de s'inspirer des courriers échangés entre les internautes pour faire des spams moins repérables », explique John Aycock, l'un des deux scientifiques canadiens. Pour l'instant, ils n'ont pas encore mis en pratique cette nouvelle technique. « Ce n'est qu'une question de temps », estime le chercheur canadien. « Quant aux solutions, elles sont réalisables techniquement mais elle n'existent pas encore sous forme commercialisable », précise-t-il. En publiant les résultats de leurs travaux, ces chercheurs ne font-ils pas le travail des pirates ? En fait, leur objectif est d'aider le monde de la sécurité informatique à mettre au point des parades tenant compte des dernières techniques en matière de spam. Cette activité était autorisée par l'université et légale car couverte par l'activité de recherche scientifique.

Pour Yves Roumazeilles, du site www.SpamAnti.net, « cette technique ne marche qu'avec les adresses e-mail collectées sur les PC zombies. Cela risquerait sans doute d'améliorer le taux de pénétration du spam dans une population de plus en plus considérée comme « à risque » mais cela toucherait beaucoup moins la population générale. Or, l'objectif d'un spammeur est de toucher 10 à 100 millions d'internautes répartis dans la population. Avec 100.000 zombies, il faudrait avoir 100 adresses « indépendantes » par zombie. Même en supposant la technique très efficace, le rendement pourrait bien rester très faible par rapport à l'effort à déployer pour implémenter une telle approche. »

6.5.3 Faux blogs, vrais spams

Les journaux personnels sont-ils victimes de leurs succès ? Attirant beaucoup d'internautes, les blogs deviennent une nouvelle cible pour les spammeurs. Ces spam blogs sont en train d'envahir le web. Selon l'annuaire spécialisé Technorati, sur environ 35 millions de blogs, 9 % seraient en réalité des blogs créés par des spam-

1. http://pharos.cpsc.ucalgary.ca/Dienst/UI/2.0/Describe/ncstrl.ucalgary_cs/2006-808-01.
Ces travaux ont été présentés à la conférence EICAR 2006 à Hambourg en mai 2006.



meurs. Autre signe inquiétant : 60 % des messages signalant des nouveaux contenus à un annuaire spécialisé proviendraient de sources identifiées comme spam.

Malgré les filtres mis en place par Technorati, « un cinquième des messages indexés par le site serait du spam », estime Tim Finin, professeur d'informatique à l'université du Maryland qui a présenté une étude sur la détection de spam blogs en mars dernier.

Faux concours, vraie escroquerie

Plus le piège est grossier, plus il est efficace ! Comme pour le *phishing*, qui permet de récupérer notamment l'identifiant et le mot de passe d'internautes un peu trop crédules (ou pas assez sensibilisés par les FAI et les banques), les concours qui promettent la Lune sont aussi une redoutable arnaque. Cette escroquerie semble surtout sévir sur le continent africain.

Dans son édition du 18 mai 2006, le quotidien *Mutations*, situé à Yaoundé (au Cameroun) rapporte cette histoire invraisemblable. Une journaliste camerounaise s'inscrit sur un site organisant un jeu-concours sur le Sida. A la clé : la possibilité de participer à une conférence au Canada, tous frais payés par le comité d'organisation. Pour être l'heureux élu, il suffit de répondre correctement à quelques questions très simples. Moins d'une semaine plus tard, un e-mail envoyé à notre journaliste lui apprend qu'elle a décroché le gros lot. Pour d'obscures raisons administratives, elle doit scanner une photo couleur et envoyer une copie de sa carte d'identité.

Le courrier précise aussi : « Votre réservation de 61 euros doit parvenir au Pr Eugène H. de la République du Bénin par Western Union au plus tard le 12 mars 2006. Voici l'adresse que vous utiliserez à l'agence Western Union pour le transfert (...) » Pour la convaincre définitivement, son correspondant lui précise qu'elle reviendra dans son pays avec le titre d'ambassadeur de lutte contre le Sida. Pour expliquer ce fléau à ses compatriotes, elle disposera d'un téléviseur, d'un lecteur DVD, de dépliants, de préservatifs, etc. Une semaine plus tard, et malgré de nombreuses relances, toujours pas de nouvelles des organisateurs. Un mois plus tard, non plus ! La journaliste doit alors admettre qu'elle a eu affaire à des escrocs.

En résumé

Le spam est un fléau qui encombre les e-mails des particuliers et des entreprises. Ces courriers indésirables peuvent être à l'origine d'une infection virale (intrusion d'un code malveillant) ou d'une escroquerie financière. Face au développement des différentes techniques de racket, les polices manquent de moyens et d'un réel soutien des États. Quant aux internautes, ils doivent faire avec le peu de moyens qu'ils peuvent plus ou moins contrôler : les logiciels antisphams. Autant dire, une arbalète face à une armée de robots...



7

La sécurité du commerce en ligne

L'éclatement de la bulle Internet au printemps 2000 n'est plus qu'un mauvais souvenir. Six ans plus tard, la sélection « naturelle » a permis aux sites les plus compétents de résister et de prospérer. Hésitants au début, les Français se sont depuis rattrapés et multiplient les achats sur la toile. Selon les résultats de la dernière étude menée par Médiamétrie//NetRatings en avril 2006 pour le compte de la Fédération des entreprises de vente à distance (Fevad), la part des acheteurs en ligne a augmenté de 21 % entre le premier trimestre 2005 et le premier trimestre 2006. Une croissance supérieure à celles de nos voisins européens (Royaume-Uni + 2 %, Allemagne + 6 %, Espagne + 17 %). Le nombre d'acheteurs en ligne croît même quatre fois plus vite que celui des internautes. Ils sont 15 millions à avoir acheté sur le web au premier trimestre 2006.

Comme le nombre de connexions à haut débit ou encore le téléphone mobile, les Français se sont donc convertis plus rapidement que prévu à l'ère numérique. Cette expansion du commerce électronique n'est pas propre à l'Hexagone. Pour le cabinet d'études Forrester Research, les ventes en lignes vont progresser de 20 % en 2006 et atteindre 211 milliards de dollars à l'échelle mondiale.

Les internautes commencent à avoir moins peur. Mais il reste encore quelques réticences à lever. Selon une étude menée par le Credoc (juin 2004), 32 % des Français interrogés estiment que la sécurité des paiements sur l'Internet ne semble pas assurée. En 2001, ils étaient 48 %. L'une des principales craintes est le détournement du numéro de carte bancaire lors d'un achat en ligne. Un mythe qui a la vie dure mais qui ne reflète pas du tout la réalité. « L'ensemble des auditions menées par l'Observatoire confirme cependant qu'aucune interception d'un numéro de carte bancaire, à l'occasion d'un achat en ligne sur un site marchand doté d'un espace sécurité, n'a eu lieu en France », peut-on lire dans le « Deuxième rapport de l'Obser-



vatoire de la Cyber-Consommation », publié en mai 2005, par le Forum des droits sur l'Internet. Cette crainte n'est donc pas justifiée pour deux raisons principales. « Le cyber-marchand ne conserve que dans de très rares occasions (cas des paiements récurrents par exemple, enregistrement d'un profil pour réaliser des achats en un clic, etc.) le numéro de carte bancaire ayant servi à la transaction. D'autre part, le mécanisme de cryptage mis en place autour des espaces de paiement en ligne demeure très difficilement contournable », explique le Forum.

Passée cette crainte, les consommateurs n'hésitent pas à acheter sur le Web. D'ailleurs, 80 % environ des paiements en ligne effectués en France en 2005 utilisaient cette solution.

Ce développement des achats électroniques ne semble pas entraîner plus de fraude que pour les paiements classiques. Publiée en mai 2006, une étude de Merchant Risk Council (Etats-Unis) indique que le taux de fraude du commerce en ligne ne dépasse pas celui des boutiques du monde réel. Qu'il s'agisse d'un site ou d'un vrai magasin, il serait inférieur à 0,1 % des ventes. Il faut néanmoins relativiser ce chiffre. Ce taux de 0,1 % n'est annoncé que par 48 % des boutiques en ligne interrogées par l'institut. Par comparaison, l'assureur Fia-Net a annoncé en juin 2006 un taux de fraudes détectées proche des 2 %.

D'autres informations trouvées dans l'étude américaine laissent en effet à penser que la fraude est peut-être sous estimée. De nombreux sites de commerce électronique (80 % environ) disposent en effet d'un système de vérification des adresses et des codes des cartes bancaires et ils demandent très souvent l'autorisation de la carte bancaire en temps réel. Ce n'est pas le cas des 20 % restants. De là à penser que le paiement électronique présente quelques failles...

7.1 LA FRAUDE AUX PAIEMENTS

La tentation de payer moins cher ou de ne pas payer du tout une marchandise a toujours existé. Mais avec le commerce électronique, elle devient un peu plus tentante. Ni vu, ni connu, l'internaute indélicat se cache derrière l'écran de son ordinateur pour commettre son forfait. Le moyen le plus utilisé, du moins par les escrocs les moins au fait des techniques de cyberdélinquance, consiste à utiliser la carte bancaire.

Le règlement frauduleux en ligne s'appuie généralement sur deux méthodes très connues :

- **Le vol d'une carte ou l'exploitation de faux numéros de cartes** : dans le premier cas, c'est un vol classique de la carte en elle-même ou d'un ticket. Dans le second cas, la personne utilise un petit programme spécialisé (générateur) dans cette application. On en trouve facilement sur Internet. Dans les deux cas, l'escroquerie repose sur l'utilisation à l'insu d'un porteur de carte de bonne foi, de son numéro.



- **L'utilisation abusive et détournée de la Loi sur la sécurité quotidienne du 15 novembre 2001** : l'acheteur affirme à son banquier ne pas être à l'origine des achats afin de pouvoir les révoquer et ne pas les régler. Dans ce cas de figure, à la différence du précédent, il y a coïncidence entre le fraudeur et le porteur du numéro de carte.

Nombre de fraudeurs en 2005 (Identités différentes)	9 752
Nombre de fraudeurs recensés par FIA-NET depuis 2000	25 171
Nombre de fraudes commises en 2005	31 518
Montant total des fraudes en 2006	10 942 668 €
Nombre moyen de fraudes par individu	3,23
Montant moyen par fraude	347 €
Montant moyen par individu	1 122 €

Figure 7.1 — Nombre de fraudeurs et volume de fraude par individu.

Source : Fia-Net, mai 2006

Selon le spécialiste de la garantie des transactions par Internet, Fia-Net, « la fraude à la carte bancaire sur Internet est une menace de mieux en mieux maîtrisée par les sites marchands. En extrapolant les taux de tentatives de fraudes du portefeuille Fia-Net à l'ensemble du marché, estimé à 7 milliards d'euros en 2005 par le Benchmark Group, on aboutit à plus de 120 millions d'euros de tentatives sur l'ensemble de l'année (contre un peu plus de 100 millions en 2004) »¹.

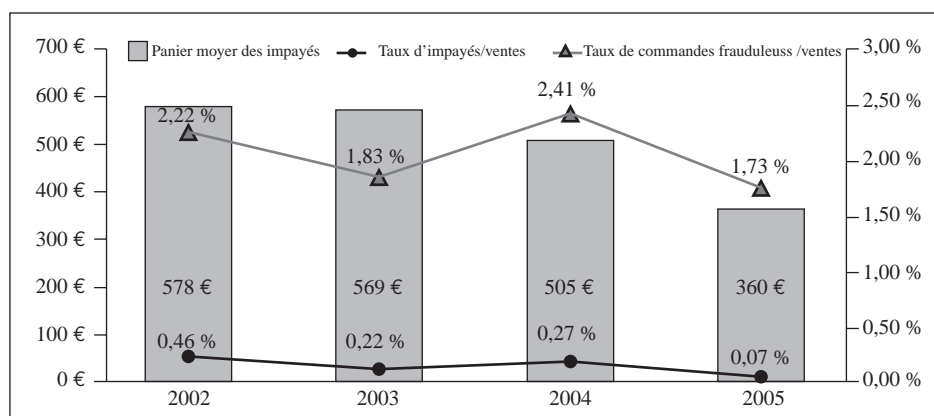


Figure 7.2 — Evolution annuelle de la fraude depuis 2002. Source : Fia-Net, mai 2006.

1. Livre Blanc « La sécurité des transactions commerciales sur Internet ». Fia-Net, mai 2006.

Selon l'assureur, « cette baisse du panier moyen des impayés est clairement le résultat des efforts des commerçants afin de lutter contre les fraudes à la carte bancaire : devant l'impossibilité de détourner des marchandises de valeur élevée, les fraudeurs concentrent leurs efforts sur des produits de valeur plus faible, sur lesquels les contrôles des commerçants ne sont pas forcément aussi poussés et aussi systématiques que pour des articles plus chers ».

9 752 fraudeurs actifs ont été repérés en 2005 (nombre d'identités distinctes employées), soit une augmentation de 16 % par rapport à l'année précédente. Depuis 2001, plus de 25 000 identités différentes ont été employées pour commettre des escroqueries à la carte bancaire. Ces fraudeurs ont réalisé plus de 31 000 commandes en 2005 pour environ 11 millions d'euros, soit 3,23 fraudes et 1 112 euros par identité employée.

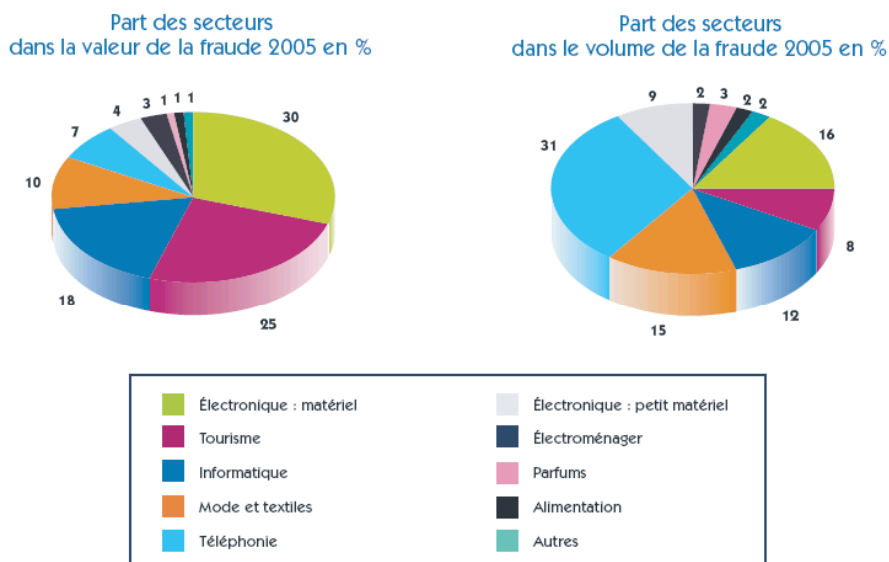


Figure 7.3 — Poids respectifs de chaque secteur dans la fraude en 2005 en valeur et en volume.

Source : Fia-Net, mai 2006.

Dans son étude, portant sur 1 109 sites marchands et l'analyse d'environ 961 millions d'euros de ventes réalisées par les commerçants Fia-Net en 2005, l'assureur note une évolution inquiétante : « Les réseaux organisés identifiés (groupe présentant au moins deux identités et deux adresses de livraison distinctes, utilisées pour commettre des tentatives de fraudes et reliées entre elles par au moins un élément personnel commun, comme le numéro de téléphone, l'e-mail ou encore le numéro de carte bancaire employés lors de la commande) ont clairement évolué par rapport à 2004. Ils sont nettement plus nombreux en 2005 qu'en 2004 : 679 contre 378, soit une hausse de près de 80 % ».



Comme les spammeurs qui tentent de ne pas éveiller l'attention des sondes mises sur Internet pour repérer les énormes envois d'e-mails (technique du *mass mailing*, voir chapitre 6), les escrocs sont devenus moins gourmands. « A la différence des années précédentes, ces fraudeurs organisés présentent un panier moyen nettement inférieur à celui du fraudeur type. Ceci peut laisser penser qu'ils ajustent leurs stratégies de détournement de marchandises », peut-on remarquer dans le Livre blanc de Fia-Net. En clair, les malfrats se sont aperçus que les sites marchands surveillaient en priorité les gros achats, au détriment de ceux ne dépassant pas une certaine somme. Autres données surveillées : les coordonnées téléphoniques et numériques. Les fraudeurs organisés se sont mis à changer plus souvent de coordonnées : d'e-mail tous les 4,49 achats (4,24 en moyenne en 2004), d'adresse postale tous les 3,59 achats (2,97 en 2004) ou de téléphone tous les 3,87 achats (3,13 en 2004).

Comme les spammeurs, ils essaient de passer au travers des mailles du filet mis en place ! Résultat : ils représentent toujours plus de la moitié des tentatives de fraudes en nombre, ils représentent en valeur moins de la moitié des fraudes contre lesquelles doit lutter un commerçant.

La généralisation du paiement électronique

Le 1^{er} janvier 2008 sera une date importante pour tous les acteurs du monde de la finance. Quelque 7 000 établissements bancaires travaillent en ce moment aux derniers réglages du SEPA (*Single Euro Payments Area*). Si aucun grain de sable ne vient enrayer cette « cash machine », dans quelques mois, les entreprises et les particuliers pourront effectuer à coût réduit des paiements électroniques par virement, prélèvement ou carte bancaire partout dans la zone euro. Pour traiter ses énormes flux, les banques vont devoir mettre en place des plates-formes technologiques très efficaces et parfaitement sécurisées. Selon la Commission européenne, cette généralisation du paiement électronique permettrait de réduire le nombre de chèques et de transactions en liquide. A la clé : 20 à 30 milliards d'euros d'économies par an. Mais cette politique pourrait aussi favoriser le développement de la cybercriminalité...

7.2 LES DIFFÉRENTES SOLUTIONS DE PAIEMENT SÉCURISÉ

« A partir du moment où vous envoyez des informations sur le net, de manière sécurisée ou non, il y a toujours un risque de les voir détournées. Concernant les achats en ligne, les sites les plus fiables proposent systématiquement plusieurs moyens de paiement, à savoir : carte bancaire, chèque, mandat et contre remboursement. Privilégiez le contre remboursement, c'est le moyen de paiement le plus sécurisant. Pour l'acheteur : même s'il ne reçoit pas sa marchandise, il ne paiera pas une promesse. Pour le vendeur : il est sûr d'être réglé. Par contre, fuyez comme la peste les sites qui n'acceptent que les règlements par carte bancaire ». Ces propos extraits d'un forum sur la sécurité du ministère de l'Intérieur sont suffisamment clairs : le risque zéro n'existe pas !



Comme d'autres solutions, le paiement électronique a des failles plus ou moins inquiétantes. Le principal maillon faible reste le stockage des données bancaires et personnelles. Le serveur central qui les stocke peut faire l'objet d'une attaque ou d'une défaillance technique. Les exemples sont peut être rares (ou jamais rendus officiels) mais ils n'en restent pas moins angoissants. Le cas le plus médiatique concerne le fournisseur d'accès Internet américain Netcom. En 1995, le célèbre hacker américain Kevin Mitnick a réussi à lui dérober plus de 17 000 numéros de cartes de crédit avant de se faire interpeller.

Autre exemple : Ikea. En 2000, son site de commerce électronique a dû être arrêté après la découverte d'une faille de sécurité. Elle permettait de consulter des informations sur les clients du site. A cause d'une surcharge de la base de donnée, un message d'erreur était envoyé à l'internaute. C'est à partir de ce message d'erreur qu'il devenait possible d'accéder aux informations clients. Pour limiter les risques, différentes solutions ont été mises en place.

7.2.1 Les protocoles de sécurité

A l'heure actuelle, la plupart des sites de commerce électronique utilise les protocoles SSL (*Secure Socket Layer*)/TLS (*Transport Layer Security*) pour chiffrer les informations sensibles comme votre numéro de carte bancaire. Problème : ces protocoles n'ont pas été conçus à l'origine pour garantir la sécurité du paiement mais pour assurer la confidentialité des informations échangées entre deux postes, votre ordinateur et le serveur du site marchand par exemple.

Cette situation présente différents inconvénients. Le numéro de la carte bancaire du client peut se retrouver à la vue de tout le monde ou presque si le serveur du site n'est pas bien configuré et protégé. D'un autre côté, le commerçant ne peut savoir si le client a tapé son vrai numéro ou l'a obtenu avec un générateur...

A l'heure actuelle, le seul moyen de lutter contre les fraudes consiste à demander à l'internaute de taper les trois chiffres du cryptogramme visuel figurant au dos de la carte.

Cette technique consiste simplement à ajouter un mot de passe supplémentaire. Elle est a priori efficace dans la mesure où les générateurs de faux-vrais identifiants de cartes bancaires ne peuvent produire cette information. Mais si pictogramme visuel réduit le risque de fraude, il ne le supprime pas. Et cela est vrai pour tous les autres protocoles, présentés ci-après. Il ne faut pas oublier que la sécurité informatique environnante est primordiale. Tous les protocoles connus réclament de saisir un ou plusieurs mots de passe, code PIN, pictogramme visuel... Ce sont autant de données critiques que des virus, *keyloggers*, chevaux de Troie pourront aisément dérober au moment où vous les saisissez si l'ordinateur est infecté par de tels codes. A l'autre bout de la transaction, au niveau du serveur, l'absence de sécurité peut être tout aussi critique et permettre aux attaquants d'agir de la même manière. Il faut juste conserver à l'esprit que tous ces protocoles ne protègent que le tuyau — celui par lequel passe la transaction — mais nullement ce qui est connecté au tuyau — le client et le serveur. La sécurité informatique et la vigilance des utilisateurs restent essentielles.



Pour mettre un terme à cette situation anxiogène, de nouveaux protocoles¹ ont été annoncés. Citons pour mémoire ceux qui ont été des échecs comme l'initiative française Cyber-COMM (terminal de paiement installé chez l'internaute) ou la norme SET (Secure Electronic Transaction) de Visa qui était considérée comme trop complexe à utiliser. D'autres sont en cours de développement :

La norme EMV

Développé à la fin des années 90, l'Europay Mastercard Visa (EMV) est proposée par les deux réseaux prestataires de services de paiement par carte Eurocard-Mastercard et Visa. Le groupe a été rejoint depuis par le japonais JCB International. L'essentiel de la protection réside dans la puce intégrée à la carte. Cette solution permet :

- Une interopérabilité internationale, quel que soit l'émetteur de la carte et quel que soit le terminal de paiement.
- Une vérification et un chiffrement de la clé personnelle par la puce. La saisie du code remplace la signature de la facturette.

La norme 3D-Secure

Prévue pour 2007 au plus tôt, cette norme est à l'étude depuis 2001 par Visa et Mastercard. L'objectif est de permettre l'authentification en ligne au moment de l'acte de paiement de façon logicielle. 3D-Secure est un protocole beaucoup moins contraignant — que le SET — pour l'acheteur comme pour le marchand. Principale raison : la complexité du système de paiement se trouve au niveau des plates-formes Visa et des banques.

Le principe est le suivant : le détenteur de la carte s'enregistre auprès de sa banque et choisit ensuite un mot de passe, qui assurera son authentification auprès de sa banque. Pour que l'authentification soit réciproque, le client sélectionne une phrase secrète qui sera affichée par la banque sur l'écran du client. Cette phase ne se déroule qu'une seule fois par session.

1. Le client navigue sur le site web du marchand et sélectionne les produits qu'il souhaite acheter. Une fois la sélection terminée, il saisit son numéro de carte bancaire. Toutes ces informations sont transmises au plug-in du marchand (*Merchant Server Plug-in*) qui est activé. Ce plug-in peut être situé sur le site marchand, sur celui de la banque du marchand, ou chez un tiers.
2. Le plug-in émet une requête contenant le numéro de carte de l'acheteur au *Visa Directory Server*.
3. Le *Visa Directory* interroge grâce au numéro de carte, le serveur d'accès (*Access Control Server*) de la banque de l'acheteur pour savoir si le numéro est inscrit au service 3D Secure.
4. Le serveur d'accès (*Access Control Server*) indique au *Visa Directory* si une authentification est disponible pour le numéro de carte.

1. Un comparatif très clair a été réalisé par la société Teamlog : <http://www.securite.teamlog.com/publication/9/20/27/217/index.html>.



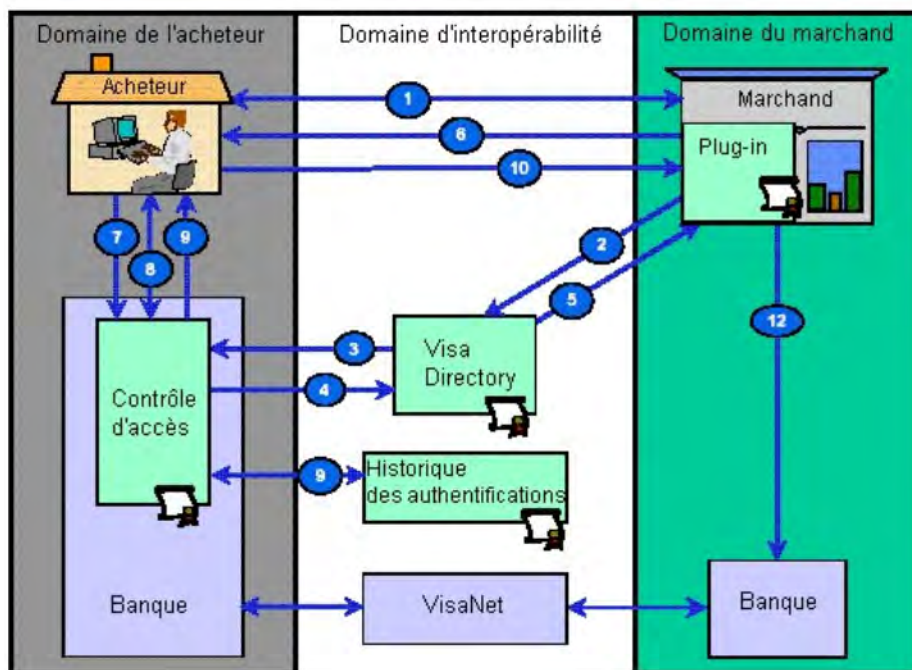


Figure 7.4 – Principe de fonctionnement. Source : Teamlog.

5. Le *Visa Directory* transfère la réponse du serveur d'accès au plug-in du marchand. Si le porteur de la carte n'est pas inscrit, ou si l'authentification, n'est pas disponible, le marchand et sa banque arrêtent le procédé.
6. Sinon le plug-in du marchand émet une demande de paiement (*Payer Authentication Request*) au serveur d'accès via le navigateur de l'acheteur.
7. La demande de paiement est reçue par le serveur d'accès.
8. Le serveur d'accès authentifie l'acheteur par exemple par un mot de passe (défini à l'inscription) ou par biométrie (La méthode d'authentification est choisie par la banque). Ensuite il formalise la réponse de paiement (*Payer Authentication Response*) et la signe.
9. Le serveur d'accès transmet la réponse de paiement au plug-in du marchand via le navigateur de l'acheteur. Le serveur d'accès envoie une copie de la réponse de paiement à l'historique des authentifications (*Authentication History*) qui conserve une trace de la transaction, utile en cas de litige.
10. Le plug-in reçoit la réponse de paiement signée.
11. Il vérifie la signature pour s'assurer que le message n'a pas été modifié durant la transmission.
12. Le marchand émet une autorisation de paiement auprès de sa banque.

Source : Teamlog, une société de conseil en ingénierie située à Paris.

Le SPA/UCAF

MasterCard a développé son propre outil qui s'articule autour de deux dispositifs : la *Secure Payment Application* et la *Universal Cardholder Authentication Field*.

La carte à puce sécurisée

L'un des points-clés de la sécurisation des paiements en ligne est l'authentification de l'acheteur. Or, les mots de passe statiques sont loin d'être la panacée (voir chapitre 11) ! Pour de nombreux experts, la seule réponse offrant une véritable garantie de sécurité consiste à utiliser un mot de passe imprévisible et non rejouable. C'est ce qu'on appelle *mot de passe dynamique* (OTP ou *One Time Password*) de 6 à 8 chiffres. Il est généré par un objet que seul l'utilisateur habilité détient (il est donc l'authentificateur) et il est complété par un code que lui seul connaît (le code PIN). C'est le principe retenu pour les cartes à puce sécurisées développées par quelques entreprises et notamment la française nCryptone. Rachetée en avril 2006 par Prosodie, elle a conçu en partenariat avec InCard Technologies la nC DisplayCard. De la taille d'une carte bancaire, elle est constituée d'une batterie, d'un écran flexible, d'un crypto processeur et d'un bouton déclencheur. Une pression sur le bouton permet de générer un mot de passe dynamique. L'utilisateur saisit alors ce mot de passe sur son terminal (ordinateur, téléphone, PDA...), complété par un code PIN.



Figure 7.5 — Principe de la nC DisplayCard (Source : Prosodie).

Pour l'instant, cette solution est encore testée par les banques.

7.2.2 Les solutions de micro paiement

Pour inciter les internautes à acheter sur le web sans utiliser leur carte bancaire, différentes entreprises ont lancé leur solution. Avec plus ou moins de succès. Qui se rappelle encore de Kline ? Apparue en 1996, cette solution logicielle avait été lancée par BNP-Paribas. Il s'agissait à la fois d'un porte-monnaie virtuel pour de petits montants et une parade contre le piratage de la carte bancaire puisque le numéro du client était stocké sur les serveurs de Kline. Environ 500 sites de commerce électronique avaient adopté ce système dont 80 % d'origine étrangère.

Mais en janvier 2000, le groupe bancaire décide de jeter l'éponge et de miser sur une solution cette fois matérielle (lecteur de cartes à puce) dénommée Cyber-Comm (nom d'un consortium réunissant une dizaine de banques, Visa, Mastercard...). Mais cette solution n'a pas non plus duré très longtemps. En 2002, les banques jettent à nouveau l'éponge ! Il est vrai que le prix du boîtier (60 euros environ) n'était pas très attractif...

Autre exemple d'échec : Cybercash. Créée par William Melton, l'un des fondateurs de Verifone (système de vérification des cartes de crédit) cette société avait mis au point un système permettant aux clients d'utiliser un logiciel gratuit pour faire des achats. Le numéro de leur carte bancaire avait été enregistré sur le serveur de Cybercash qui était lui-même relié au réseau bancaire. Cette solution s'appuyait sur une connexion cryptée. Mais en 2002, la société a fait faillite.

Avec le développement des sites de téléchargement légal de musique et de vidéo et le succès des sites d'enchères et de vente entre particuliers, le micro paiement devrait trouver un second souffle. Ce marché a représenté, aux Etats-Unis, 1,6 milliard de dollars en 2003 et 1,8 milliard de dollars un an plus tard. En Europe, le chiffre d'affaires atteignait 544 millions d'euros en 2003. Il pourrait atteindre un volume de 2,37 milliards d'euros en 2007.

Voici quelques-unes des solutions les plus développées.

PayPal

C'est la solution la plus connue et la plus utilisée. Selon Paypal (qui appartient à eBay), A l'été 2005, il y avait environ 71,6 millions de comptes à travers 56 pays. Le volume total des transactions transitant par le système PayPal, dans le monde, a atteint 6,2 milliards de dollars au premier trimestre 2005.

Cette solution présente plusieurs avantages mais aussi quelques limites. Pour la réception d'un paiement, Paypal offre des tarifs compétitifs : par exemple entre 0 et 2 500 euros, les frais pour le vendeur sont de 3,4 % + 0,25 euro. Le crédit du compte Paypal peut être viré sur le compte bancaire (le coût est d'1 € pour une somme inférieure ou égale à 99,99 euros. Un système d'assurance garantit l'achat dans une limite de 500 euros, mais pour un nombre de recours limité.

PayPal envoie une confirmation par e-mail de chaque transaction sur le compte. Si la personne reçoit la confirmation d'une transaction inconnue, elle doit contacter le service clientèle de Paypal. Selon PayPal, sa solution repose sur les « technologies anti fraude le plus sophistiquées ». La société crypte automatiquement les données confidentielles qui transitent entre l'ordinateur de l'acheteur et le système PayPal grâce au protocole SSL (*Secure Sockets Layer*) et avec une longueur de clé de cryptage de 128 bits (niveau le plus élevé actuellement disponible sur le marché). Toutes ces précautions expliqueraient que le taux d'impayés lié à la fraude soit très bas. Au premier trimestre 2005, ce taux s'établissait à 0,3 % ¹.

1. Interview de président de Paypal, Jeff Jordan, au Journal du net du 1/7/2005.



PayPal victime de phishing

Aucune solution de paiement en ligne n'est infaillible. Les utilisateurs de PayPal l'ont appris à leurs dépens. Fin juin 2006, une vulnérabilité permet d'exploiter un certificat de sécurité valide dans une fausse page PayPal ! Révélée par la société de services Internet NetCraft elle permet de dérober le log-in d'un client du service, son numéro de carte de sécurité sociale (important aux Etats-Unis) et les détails de sa carte bancaire.

Comme l'arnaque s'appuie sur une véritable adresse URL d'une page du site de paiement, la fraude est difficilement détectable par la majorité des internautes.

Source : *Silicon.fr*

Signalons qu'il existe un autre système semblable à Paypal : eGold¹

Ticket Surf

Créée en 2003, cette start-up française issue du groupe France Télécom propose des cartes de paiement à gratter de 2 à 10 euros. Il suffit de taper le numéro de son Ticket Surf dans le champ de la page de paiement d'un site partenaire pour valider et payer sa transaction. Chaque ticket est unique et possède 11 caractères alphanumériques, garantissant ainsi à l'acheteur et au vendeur une sécurité optimale. « Les deux cibles que nous visons sont très porteuses, explique Gilles Moro, PDG de Ticket Surf. Même si le risque de fraude baisse, de nombreuses personnes hésitent encore pour de petits achats. Cette population représente 60 % de nos clients. Le reste, ce sont les jeunes non "banquérisés" qui peuvent ainsi payer pour jouer en ligne ou acheter des fichiers comme des images ou des sonneries de mobile. »² Seul problème : cette société n'a pour l'instant que 147 sites partenaires.

eCarte Bleue

Apparue en 2002, l'e-Carte Bleue est un service optionnel de la carte de paiement internationale. Elle est aujourd'hui proposée aux clients de certaines banques françaises (Société générale, la Poste, Crédit Lyonnais, Groupe Banque populaire et groupe Caisse d'Epargne). D'autres banques proposent des produits analogues (P@yweb Card et Virtualis au Crédit mutuel). Entre 2002 et le printemps 2005, ce service a enregistré près de 1,5 million de transactions pour un montant total de 110 millions d'euros.

Pour chaque achat, elle délivre en ligne un numéro de carte bancaire à usage unique. L'acheteur ne transmet donc plus son numéro de carte réel et il est possible de fixer soi-même le plafond du paiement. Mais cette sécurité a parfois un prix. Si certaines banques la proposent gratuitement d'autres facturent 2.5 euros chaque acte. D'où son développement assez limité.

1. Ce site explique comment utiliser cette « monnaie » : <http://goldstrategie.lovadoo.com/index24.html>

2. Silicon.fr du 22/5/06.



Les tokens (jetons en anglais)

Il s'agit de mini lecteurs de carte ressemblant à une calculatrice de poche. Mais la procédure est un peu contraignante. L'utilisateur donne toujours son numéro de carte bancaire (ainsi que la date d'expiration et son nom) et valide l'opération. Il obtient ensuite un code aléatoire sur le site du commerçant. Il doit le taper sur son token, puis son traditionnel code PIN à quatre chiffres. Ensuite, un numéro (valable uniquement pour l'achat en cours) s'affiche sur l'écran du token. L'acheteur devra le retaper sur le site du commerçant pour finaliser sa commande.

Fastidieux et pas si sécurisé que ça selon un représentant de Visa : « Outre son prix de fabrication [élevé], le petit lecteur de cartes que l'on branche sur un PC doit résoudre trop de problèmes », précise David Main, directeur du développement technologique de Visa Europe. « D'abord des problèmes de compatibilité entre les boîtiers, les systèmes d'exploitation et les pilotes ; ensuite, il faut être sûr que le code PIN ne soit pas stocké sur l'ordinateur. Autant de soucis que l'on oublie avec les tokens. »¹

7.3 LES SITES DE PAIEMENT SONT-ILS FIABLES ?

Très en vogue, les sites d'enchères attirent de plus en plus de particuliers mais aussi quelques escrocs. Début 2006, deux Roumains résidant à Londres ont arnaqué des milliers d'acheteurs du monde entier via le site Internet d'enchères eBay. Ils leurs vendaient des biens qui n'existaient pas ! Un super filon : ils ont amassé environ 370 000 € en moins de deux ans. L'argent était récupéré par un troisième larcin qui se chargeait ensuite de blanchir l'argent en Roumanie.

Cette affaire ne signifie pas pour autant que eBay soit un repaire de malfrats en tous genre. Dans la majorité des cas, ce site permet de dénicher la perle rare ou de faire de bonnes affaires sans être escroqué. Comme d'autres sites de commerce électronique, les eBay et consorts ne sont pas plus risqués. Ils exigent néanmoins un peu plus de vigilance car ils mettent en relation un acheteur et un vendeur qui n'est pas toujours « professionnel ». Notons au passage que cet amateurisme a néanmoins tendance à s'estomper. Selon une étude publiée en avril 2006 par eBay, il y a plus de 170 000 personnes en Europe qui l'utilisent comme source de revenus unique ou complémentaire. 70 % d'entre elles affirment que leur présence sur ce site leur a permis d'augmenter leurs ventes. En France, 15 240 utilisateurs se déclarent comme vendeurs professionnels. Ce chiffre n'intègre pas les internautes qui ne sont pas en règle avec la loi, en ne se déclarant pas comme professionnels malgré les montants et la régularité de leurs ventes sur le site. Un internaute français a d'ailleurs été récemment condamné pour ce motif.

Cette professionnalisation d'eBay va de pair avec l'arrivée d'escrocs d'un nouveau genre. Ils ne se contentent pas de vous vendre du vent comme le couple de Roumains. Leur dernière combine consiste à mettre en avant de faux sites de paie-

1. ZDNet.fr 5/11/04.



ment. Le principe est simple : au moment de conclure l'affaire, le vendeur vous propose de passer par un autre système de paiement, dit aussi « tiers de confiance » (« *escrow* » en anglais), soi-disant plus avantageux que celui proposé par le site (eBay mettant en avant Paypal qu'il a racheté). Il s'agit bien sûr d'un faux site de transaction (technique d'usurpation de nom de domaine). Signalons aussi que certains malfrats dirigent les acheteurs vers de faux sites de Paypal en mode sécurisé...

Une méthode plus élaborée consiste à utiliser un programme malveillant. L'escroc vous envoie un fichier exécutable « anodin » censé vous expliquer la procédure à suivre. L'internaute se croyant à l'abri de ce genre de manœuvre grâce à son antivirus n'y verra que du feu car ce programme malveillant n'est pas assimilé par les anti-virus comme étant malicieux. Son rôle ? Modifier certains éléments de votre système d'exploitation (fichier host) pour détourner — de manière invisible — les requêtes initialement dirigées vers le site web du tiers de confiance vers le site géré par le pirate.

Quelle que soit la technique utilisée, le résultat est le même : les acheteurs ne reçoivent jamais leur colis. Par contre, ils ont bien été débités...



Figure 7.6 — Exemple d'un faux site de tiers de confiance. Source : Escrow Fraud.

Plusieurs affaires de ce genre ont été signalées en Belgique en 2006. Chez eBay-Belgique, on minimise le phénomène : « Dans 99,9 % des transactions, tout se passe bien. L'arnaque est un problème qui touche toute l'industrie de l'e-commerce, et pas seulement eBay. Chez nous, plus de 1 000 personnes dans le monde s'occupent de la

sécurité et luttent contre les faux e-mails ou les sites non vérifiés », précise Peter Burin, porte-parole d'eBay Belgique¹. Quant à Western Union, eBay en déconseille l'usage sur son site et recommande de régler ses achats par PayPal.

Pour ne pas se faire arnaquer vous pouvez consulter les sites <http://escrow-fraud.com> et escrow.com qui signalent les faux sites de paiement. Respectez aussi les quelques points suivants délivrés par le CERT :

Conseils utiles

- Ne pas exécuter des fichiers dont l'origine (e-mail ou site web) n'est pas clairement identifiée et approuvée.
- Ne pas cliquer sur des URL référençant des moyens de paiement en ligne et contenues sur des sites marchands ou dans des e-mails liés aux transactions.
- Saisir manuellement les adresses des sites de paiement en ligne dans la barre d'adresse du navigateur.
- Vérifier que ces sites proposent des connexions sécurisées (SSL) ET un certificat légitime.
- Actualiser votre anti-virus chaque jour (toutes les heures si possible).

Si malgré ces conseils, vous vous faites avoir vous pouvez porter plainte auprès des organismes cités à la fin de l'ouvrage ou auprès de la DGCCRF (www.finances.gouv.fr/DGCCRF).

En résumé

En juin 2006, une étude menée par Médiamétrie//NetRatings, pour le compte la Fevad (Fédération des Entreprises de Vente à Distance), indique que la France est championne d'Europe de la croissance du e-commerce. Près de 57 % des internautes sont clients d'un site e-commerce, réalisant un chiffre d'affaires de près de 9 milliards d'euros en 2005. Une bonne nouvelle... qui n'est pas une énorme surprise. Tout a été fait pour le commerce électronique se développe : un peu de sécurité et beaucoup de facilité. La priorité étant de séduire et de convaincre le chaland pour qu'il achète sur le Web. La sécurité des paiements n'était donc pas une priorité comme le reconnaissent différents experts que nous avons rencontrés. Beaucoup de choses restent à faire.

1. Le Soir. 6/02/2006



8

Les entreprises sont mal protégées

« A l'heure où la sécurité de l'information reste sous les feux de l'actualité, tous les acteurs ont-ils pris conscience des risques, et mis en œuvre les mesures qui s'imposent en conséquence ? En réponse à cette question, nous dressons un constat mitigé ». En matière de sécurité informatique, les entreprises françaises peuvent donc mieux faire. C'est l'un des principaux constats que tire le Club de la Sécurité de l'Information Français (CLUSIF) dans sa dernière étude sur « Les politiques de sécurité des systèmes d'information et sinistralité en France », publiée fin juin 2006.

Réalisée par le cabinet GMV Conseils, cette enquête est un baromètre intéressant. 400 entreprises d'au moins 200 salariés ont été interrogées ainsi que des mairies et des hôpitaux.

Les principaux points intéressants de cette étude sont les suivants :

- Le système d'information : il est devenu critique et stratégique pour 98 % des entreprises.
- Les niveaux de dépense en matière de sécurité : ils varient d'une entreprise à une autre mais la tendance est à la hausse pour 38 % des entreprises. Le plus inquiétant est que 21 % d'entre elles ne sont pas capables de mesurer cette dépense.
- La politique de sécurité de l'information : seulement 56 % des entreprises interrogées en sont dotées. Logiquement, la proportion augmente dans les grands comptes (+ de 1 000 salariés) avec 72 % mais elle est de 52 % dans les entreprises de 200 à 499 salariés.
- Les logiciels de sécurité : la majorité des entreprises utilise les outils classiques (antivirus, firewall, antispams). Très peu ont recours à des solutions de chiffrement et d'authentification forte pour protéger leurs données ou leur parc de terminaux mobiles (téléphones, assistants numériques, ordinateur portable).



- La prévention : c'est le point noir. Les mises à jour des logiciels (correctifs de sécurité notamment) ne sont malheureusement pas automatiques. 42 % des sondées reconnaissent ne pas avoir formalisé de procédures. A peine la moitié (58 %) collectent et traitent les incidents de sécurité. 24 % procèdent à une évaluation financière de ces incidents.

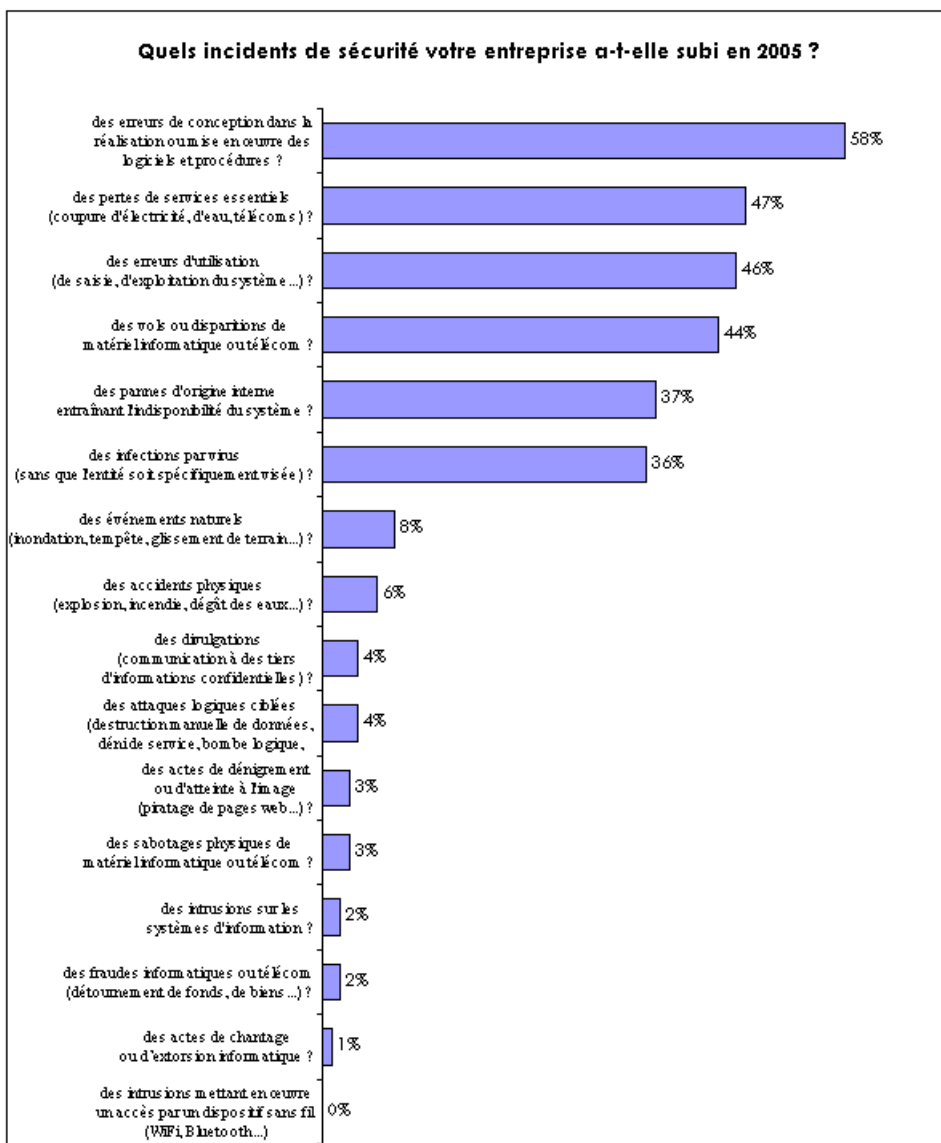


Figure 8.1 — Typologie des incidents de sécurité en entreprise¹.

1. Source : Etude du CLUSIF, « Politiques de sécurité des systèmes d'information et sinistralité en France – Bilan de l'année 2005 ».

Malgré la multiplication des risques, de nombreuses entreprises n'ont pas encore pris toute la mesure du fléau. « Le système d'information d'une entreprise est l'un des points d'entrée, explique Thierry Durand, de la Direction prévention et gestion des risques de PSA Peugeot Citroën. Ce système est aussi un outil de production, de pilotage (aide à la décision) et c'est une vitrine de l'entreprise. Donner, ouvrir un point d'entrée c'est donc foncièrement grave. »

8.1 LES DIFFÉRENTES MENACES

L'informatique est partout dans une entreprise et Internet est devenu en quelques années un des rouages essentiels. Ces deux points-clés sont aussi d'importants vecteurs de contamination.

8.1.1 Le vandalisme

Pour la personne malveillante, l'investissement est quasi nul mais les conséquences peuvent être désastreuses pour la santé financière et l'image d'une entreprise. Comme de plus en plus de sociétés ont créé un ou plusieurs sites, les risques qu'ils soient endommagés sont importants. Pour de nombreux experts que nous avons rencontrés c'est même la première menace pour les sociétés. « Officiellement, nous avons au moins une page web de défigurée par mois, révèle le responsable de la sécurité d'une entreprise internationale qui a plusieurs sites. Ce vandalisme peut donc un peu perturber le fonctionnement de l'entreprise mais c'est réparable ».

8.1.2 La vengeance

« Furieux de son licenciement, un chef informatique de la société Beghin Say implante en 1991 une bombe logique dans le programme de gestion. Elle s'est déclenchée trois mois après son départ forcé et a bloqué l'activité de la sucrière durant une semaine, raconte le commissaire Daniel Padouin, responsable du SEFTI. Contrairement à la détection d'une bombe physique placée dans une banque, celle du bombe logique est quasiment impossible »¹.

Après le vandalisme, la vengeance est la seconde menace pour de nombreuses entreprises. Dans la majorité des cas, c'est un ancien salarié ou un employé qui estime qu'il devrait déjà être directeur et qui ne comprend pas pourquoi il ne l'est pas encore ! Il peut aussi s'agir d'un prestataire déçu par le manque de reconnaissance de son client ou frustré de ne pas avoir remporté l'appel d'offres (ce fut le cas d'une société informatique qui avait voulu se venger d'un important service de la police judiciaire...).

1. Libération. 12/12/1997

« Ce cas de figure est dangereux car la personne est animée d'une intention malveillante. A la fois profondément excitée dans son action et généralement peu compétente, elle laisse généralement des traces qui peuvent être exploitées à temps », explique Thierry Durand. La situation est néanmoins beaucoup plus problématique lorsque la personne aigrie est encore en poste car elle dispose de codes d'accès au réseau interne de l'entreprise. Ils peuvent lui permettre de lancer une attaque virale de l'intérieur. Si la personne place un code malveillant, les systèmes de défense et de prévention de l'entreprise peuvent être pris au dépourvu. Lorsque le virus est repéré, l'infection est déjà répandue sur un grand nombre de postes. « Cette situation conduit rarement à des pertes de données mais à des pertes de temps », précise Thierry Durand.

La mesure des risques

Selon la taille d'une entreprise, toutes les attaques ne sont pas traitées de la même façon. Les risques sont hiérarchisés. Telle multinationale estimera par exemple qu'un coût de remise en ordre inférieur à 150 000 € ne justifie pas d'engager des plans de prévention coûteux si la probabilité du sinistre est faible. Cette action malveillante sera néanmoins surement retenue dans le plan de sensibilisation du personnel de manière à ce qu'il ne prête pas le flanc à des attaques de ce genre. La même entreprise considèrera au contraire qu'elle n'a pas le droit de ne rien faire si l'action malveillante ou sa répétition conduisent à des coûts estimés de réparation supérieurs à 1,5 million d'euros. Ce serait alors la survie de la société qui serait en jeu.

8.1.3 L'attaque programmée

Ce genre de risque concerne les grandes entreprises (publication d'une photo d'un prototype, opération de désinformation entraînant le capotage d'un nouveau projet...) ou celles qui sont plus petites mais qui disposent d'un savoir-faire exceptionnel et dont la perte ou la divulgation la mettrait en péril. Ce genre d'opération est mené par un spécialiste ou une bande organisée. Ils ont reçu une commande pour faire du tort ou voler des données dans une entreprise. Si la rémunération est suffisamment importante, ils n'hésitent pas devant les moyens. La seconde possibilité consiste à visiter de nombreux sites pour y repérer les maillons faibles et les butins potentiels. La bande recherchera ensuite un commanditaire avant de passer à l'action.

Quel que soit le point de départ, l'opération peut se dérouler de deux façons :

- L'attaque brutale : les pirates mettent en œuvre d'importants moyens pour parvenir à leurs fins. Dans ce cas, l'entreprise visée a du mal à faire face car elle n'a pas toujours mis les protections nécessaires pour ce genre d'opération.
- L'attaque réfléchie : elle est menée en toute connaissance de cause. Les repérages des points faibles du réseau de l'entreprise ont été effectués quelques mois auparavant. Là aussi, la victime a du mal à réagir car il y a de très fortes chances qu'elle ne voit pas l'attaque !



Des données sensibles pas assez protégées

Publié en mai 2006¹, un rapport de l'ESG (*Enterprise Strategy Group*) montre à quel point la sécurité des données est devenu le problème n° 1 de nombreuses sociétés. Ce cabinet américain a analysé les réponses de 227 responsables de sécurité d'entreprises (de 1 000 à 20 000 employés). Le résultat est accablant : 68 % d'entre eux confirment que les données confidentielles sont plus exposées sur les ordinateurs portables que sur les fixes. Près d'un quart des répondants s'estiment « vulnérables », voire « très vulnérables » aux menaces sur les données. Et ils ciblent même les vecteurs d'échange non sécurisés de ces informations confidentielles avec des tierces personnes : 30 % par les e-mails, 27 % les web services, 27 % les serveurs FTP et 8 % les messageries instantanées. Et de façon plus globale, les nouvelles applications collaboratives ou de bureautique en ligne comme les propose Google.

8.1.4 L'espionnage économique

La naïveté n'est pas compatible avec la sécurité. Valeo l'a appris à ses dépens. En mai 2005, la petite Lily devient célèbre en France. Cette jeune stagiaire chinoise est soupçonnée d'avoir copié sur un disque dur personnel des données confidentielles stockées sur le réseau interne (Intranet) de cet équipementier automobile français.

L'année 2005 a d'ailleurs été riche en affaires. En avril de cette année-là, en Suède, un homme d'origine hongroise est condamné à trois ans de prison pour espionnage industriel. De mars 2002 à juin 2004, il s'est introduit dans les systèmes informatiques d'Ericsson et a accédé à différentes informations : mots de passe et noms d'utilisateur de personnel, codes source de logiciels et des données cryptées (parmi lesquelles des documents militaires²). Lorsqu'il a été arrêté, il a justifié ses intrusions par la volonté de démontrer que le réseau d'Ericsson présentait des failles. En révélant ces données, il espérait trouver un emploi. En réalité, il cherchait surtout à monnayer ces précieuses données en les proposant sur internet !

La cupidité et la vengeance sont souvent à l'origine d'affaires de ce genre. Le cas Lightwave IT Microsystems en est un exemple parfait. En 2005, l'ancien responsable de la direction informatique de cette société américaine reconnaît avoir volé des sauvegardes informatiques (comprenant des secrets de fabrication) de sa société pour les revendre à un concurrent, JDS-Uniphase. Mais ce dernier a prévenu le FBI. « La même année, l'ancien PDG de la société américaine BES reconnaît avoir planifié l'intrusion du système informatique d'un concurrent. Pendant dix mois, lui et quelques cadres ont mis au point un plan pour recopier des secrets de fabrication d'avant-projets. Ils avaient profité d'une session en ligne de formation organisée par le concurrent, à travers un site web spécialisé dans le e-learning, pour s'introduire dans le système »³.

1. Zdnet.fr. 2/05/2006.

2. L'équipementier compte en effet parmi ses clients le ministère de la Défense suédois.

3. Danielle Kaminsky. Panorama de la cybercriminalité 2005 du Clusif.



En juin 2006, le FBI a arrêté deux anciens employés de la société NetLogic Microsystems¹. Ces deux californiens de 42 et 34 ans sont accusés d'« organisation de malfaiteurs afin de voler des secrets commerciaux, et de cinq vols de secrets industriels ». Les vols concernaient à la fois des secrets appartenant à leur ancien employeur mais aussi au fondateur taïwanais TSMC (*Taiwan Semiconductor Manufacturing Co.*), un partenaire industriel. Les deux hommes avaient créé une société « dans le but de développer et de vendre des produits utilisant ces secrets industriels volés » a expliqué le procureur. Ils risquent une peine maximale de 10 ans de prison accompagnée de 250 000 dollars d'amende.

Echelon et Blackberry

Ce terminal mobile est devenu la coqueluche de tous les cadres dirigeants. C'est aussi devenu la bête noire de tous les responsables de la sécurité informatique. Il est vrai que le Blackberry présente de sérieux atouts : il tient dans la poche d'un costume et il permet d'envoyer et de recevoir ses e-mails en temps réel. Bref, tous les patrons français le veulent ! Les responsables de la sécurité que nous avons interrogées ont le plus grand mal à convaincre leurs supérieurs de ne pas l'utiliser ou de l'utiliser avec vigilance. Pour les spécialistes, le risque ne se situe pas au niveau du serveur du Blackberry ou du terminal en lui-même. Le problème se situe aux Etats-Unis. Toutes les données qui transitent par le Blackberry passeraient par Echelon. Les grandes oreilles américaines pourraient ainsi mettre la main sur des e-mails confidentiels échangés entre un grand patron et l'un de ses adjoints ou l'un de ses partenaires industriels. Pour éviter ce risque, les responsables de la sécurité informatique demandent donc à leur dirigeant de n'envoyer que des e-mails anodins ou chiffrés. Mais ces deux options ne semblent pas convenir à ce patron d'une grande entreprise. Pour deux raisons présente-t-il en substance : « si je ne peux pas envoyer de courriers confidentiels, mon Blackberry ne me sert à rien. Et si je dois chiffrer mes courriers il faut que mon correspondant puisse les déchiffrer ; trop compliqué ». Pour les responsables de la sécurité informatique, le chiffrement des échanges est pourtant la seule solution. Ce n'est pas la panacée. Mais Echelon ne peut pas traiter en temps réel toute l'information. On peut donc espérer que le contenu de cet e-mail ne sera plus confidentiel (l'information aura été publiée dans la presse par exemple) lorsque ce programme le déchiffrera..

Mais l'affaire d'espionnage économique — du moins parmi celles connues du grand public — qui a eu le plus de retentissements remonte à 2004. L'histoire débute chez un écrivain et professeur d'histoire israélien. En surfant sur le web, il découvre des extraits d'un livre qu'il est en train d'écrire mais qu'il n'a pas encore publié. Après enquête, les policiers constatent qu'un cheval de Troie a été placé dans son PC. Ce code malveillant a pu s'infiltrer grâce à une pièce jointe à un e-mail que l'ex-gendre de l'écrivain lui avait envoyé sous différents prétextes. Arrêté en mai 2005 à Londres — avec un mandat d'extradition israélien — il est soupçonné d'avoir vendu des

1. Pcinpact du 16/6/2006.



variantes de son cheval de Troie à des agences de détectives privées. Celles-ci avaient été mandatées par des clients pour trouver des renseignements sur des entreprises spécialisées dans la téléphonie, l'automobile, la mode, l'agroalimentaire, la finance et la presse. Il y a eu une quarantaine d'arrestations et des inculpations. Comme dans d'autres domaines, il est très difficile d'en savoir plus. Pour ne pas égratigner leur image de marque ou dévoiler leurs faiblesses, les victimes sont restées très discrètes...

Ces quelques exemples montrent à quel point l'espionnage économique est facilité avec le développement de l'informatique. La généralisation des clés USB mais aussi des baladeurs MP3 dotés d'une grande capacité de stockage n'encourage pas à l'optimisme. Sans aucune protection (chiffrement, mot de passe) des données confidentielles peuvent être copiées en quelques minutes sur ce genre de périphérique amovible. Cette menace commence d'ailleurs à être prise en compte par les entreprises. Si l'on en croit un sondage réalisé à la demande de Sun Microsystems Canada par Ipsos Reid près d'une entreprise sur deux (49 %) — soit un peu plus d'une centaine sur les 259 interrogées —, a adopté un règlement intérieur visant à bannir les ordinateurs portables et les clés USB sur le lieu de travail, et une sur trois (30 %) considère les iPod et autres lecteurs MP3 indésirables dans l'entreprise. Cette prise de décision ne signifie pas pour autant que les dirigeants de ces entreprises soient plus informés que les autres. Selon ce sondage, publié durant l'été 2006, « 17 % d'entre eux avouent comprendre très mal les risques impliqués par l'accès à distance ou sans fil. »

Ces lecteurs amovibles seront donc peut-être bannis des entreprises. Mais le sourire désarmant d'une stagiaire qui a perdu son mot de passe et qui vous demande gentiment le vôtre restera toujours l'arme absolue...

8.1.5 Les moteurs de recherches

Qui peut aujourd'hui se passer de Google et des autres moteurs de recherches ? Certainement pas grand-monde. En quelques années, ils ont révolutionné la manière de trouver de l'information en indexant des milliards de pages web. Malheureusement, cette facilité est à double tranchant.

Le « *Google Hacking* »¹ est une menace inconnue de la majorité des entreprises. C'est pourtant un risque potentiellement majeur. Cette expression désigne le recueil d'informations confidentielles à partir de requêtes spécifiques effectuées sur Google. « Mais ce problème concerne tous les moteurs de recherches ne respectant pas les protocoles Internet qui empêchent un robot d'indexer, précise Pascal Lointier, président du Clusif. Normalement, le robot ou le logiciel aspirateur de web devrait s'arrêter à ce moment-là. Ces moteurs ont mis en évidence la visibilité involontaire — des portes du réseau Intranet n'ont pas été fermées — que crée des entreprises ».

Dans son livre, Johnny Long explique que la requête de Google peut notamment être traitée via un relais proxy, ce qui permet de bénéficier d'un certain anonymat.

1. Titre d'un livre écrit par Johnny Long et publié par les éditions Dunod.



Parmi les nombreuses fonctionnalités de Google, l'option "cache" est une arme redoutable. Cette fonction permet de consulter des pages sauvegardées par le moteur de recherches mais qui ne sont plus disponibles sur le site d'origine. « Les entreprises doivent donc se soucier des documents qu'elles mettent en ligne même pendant quelques instants », prévient Pascal Lointier.

Un espion dans son PC ?

Après l'indexation des milliards de pages d'Internet, les moteurs de recherches s'attaquent maintenant aux fichiers stockés sur les ordinateurs des particuliers ou des employés. Cette nouvelle application est pratique. Elle permet en quelques instants de retrouver un document Word ou un classeur Excel niché dans les entrailles d'un Intranet ou de son disque dur. Mais comme pour la version web, ces logiciels représentent une réelle menace ; Là aussi, les entreprises n'en n'ont pas conscience. Comment savoir si l'information indexée sur le disque dur ne va pas être aussi transmise au serveur de l'application ? Le risque semble d'autant plus grand avec Google Desktop 3: la fonction de recherche croisée (appelée « *Search Across Computers* ») de fichiers sur plusieurs PC représente un « risque de sécurité inacceptable » pour les grands comptes, dénonce un analyste du Gartner. Pour faciliter cette recherche, Google Desktop 3 stocke temporairement des copies textuelles des objets présents sur... les propres serveurs de Google pendant une durée de 30 jours. « Oui, il y a un risque, et nous comprenons les préoccupations des sociétés » commente à ZDNet Andy Ku, le responsable Europe et marketing manager de Google. Il ajoute aussi que « Théoriquement toute la propriété intellectuelle de la société pourrait être diffusée à l'extérieur. Nous comprenons qu'il y ait de nombreuses préoccupations sécuritaires autour de cette fonction, mais Google ne sauvegardera pas de l'information, sauf si l'utilisateur ou la société cliente a activé la fonction ».

8.2 LES OBSTACLES A LA SÉCURITÉ INFORMATIQUE

« L'épaisseur d'un rempart compte moins que la volonté de le défendre ». Au moment de boucler le budget sécurité informatique de leur entreprise, tous les dirigeants devraient méditer cette maxime de Thucydide (historien grec, IV^{ème} avant J.-C.). Malheureusement, ces responsables d'entreprises manquent de recul et d'informations objectives. « Les patrons de PME s'en remettent soit à leur responsable informatique (mais il n'a pas nécessairement le temps ni la culture sécuritaire...) soit à une société extérieure, constate Pascal Lointier. Il faudrait au moins que l'entreprise envoie son responsable à des formations sur la sécurité. »

Aujourd'hui, la sécurité informatique est l'affaire — d'aucuns parleront plutôt de « chasse gardée » — des informaticiens. Pour la plupart des experts que nous avons rencontrés, cette problématique devrait être rattachée au service juridique ou aux



La meilleure protection ? Le sac plastique !

Les ordinateurs portables sont devenus à la mode. Ils deviennent de plus en plus puissants et leurs prix deviennent attractifs. Mais leur richesse ne se trouve pas dans la vitesse de leur processeur ou la performance de leur carte graphique mais dans leur disque dur. « Ceux qui volent dans le TGV ont bien compris que les données d'un ordinateur sont monnayables, parfois mieux encore que le matériel lui-même, explique Hervé Schauer. Mais aussi surprenant que cela puisse paraître, la plupart des entreprises ne chiffrent pas les données sur leurs portables. Les voleurs ne sont généralement pas des génies en informatique ; une simple protection suffirait ». Un sac plastique aussi ! La DST préconise en effet l'emploi d'un sac plastique ou banalisé pour ne pas attirer la convoitise de curieux. Exit donc les belles pochettes portant le logo d'une marque informatique. Evidemment, cette technique de camouflage s'applique aussi aux petits terminaux mobiles comme les PDA et les smartphones...

ressources humaines. Cette évolution est encore lente. Très peu d'entreprises ont rapproché la sécurité informatique du service juridique.

Selon une étude réalisée en 2006 par Ernst & Young, d'autres obstacles empêchent la mise en œuvre d'une sécurité efficace. Peu d'entreprises, même parmi les plus importantes, ont une approche de sécurité globale. Seuls 51 % des répondants français (contre 71 % au niveau mondial), ont répertorié les informations sensibles ou confidentielles.

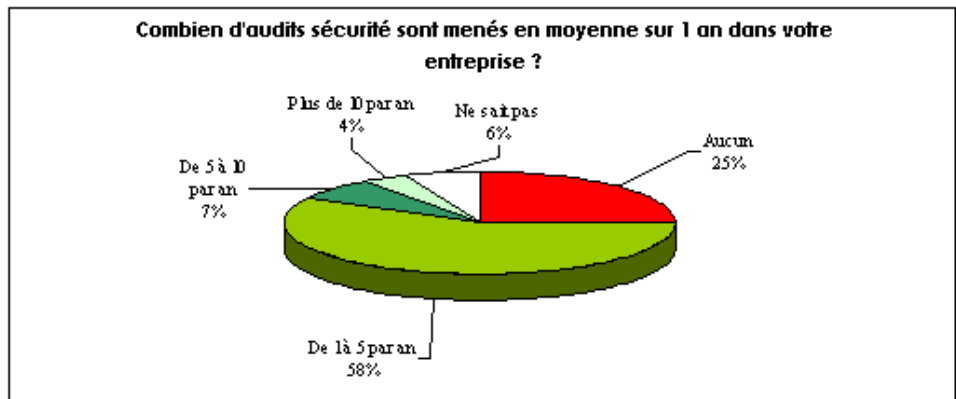


Figure 8.2 – Nombre d'audits sécurité en 2005 dans l'entreprise.¹

Les restrictions budgétaires sont aussi un frein. Selon l'étude CSI/FBI 2005, 27 % des sondés dépensent plus de 6 % de leur budget informatique en SSI, près d'un quart de 3 à 5 %, autant de 1 à 3 % et un dernier quart moins de 1 % ou ne savent

1. Source : Etude du CLUSIF, « Politiques de sécurité des systèmes d'information et sinistralité en France – Bilan de l'année 2005 ».

pas. Pour Christophe Grenier, RSSI chez Global Service Provider, « toutes les sociétés ont des problèmes de budget et le ROI (retour sur investissement) de la sécurité est l'un des points les plus difficiles à défendre. La sécurité est encore loin de représenter une préoccupation de premier plan... Elle est surtout perçue comme un coût. Lorsqu'une entreprise doit se lancer dans la coupe franche d'un budget, la colonne « sécu » est la première à être visée. Par exemple, à l'occasion d'un audit, un grand compte connu du monde internet découvre une multitude de failles sur ses systèmes. Plus d'un an après, une partie seulement d'entre elles ont été revues. Même face à un risque identifié, il est parfois difficile de faire entendre raison et cela souvent à cause de contraintes de temps et d'investissement »¹.

La sécurité : un marché florissant

Selon l'enquête IDC Sécurité 2005, les dépenses informatiques globales sur le marché professionnel en France ont atteint 41 009 M€, en croissance de 3,5 %. Les dépenses de sécurité informatique des entreprises et des administrations atteignent 1 113 M€, en hausse de 17,4 % (contre 15,4 % de hausse entre 2004 et 2003). Parmi ces dépenses de sécurité informatiques en 2005 :

- les services représentent 612 M€ (55 %) en hausse de 15,5 % ;
- les logiciels représentent 405 M€ (36,4 %) en hausse de 16,4 % ;
- les appliances (boîtiers physiques intégrant de une à plusieurs fonctionnalités : pare-feu/VPN, anti-virus, anti-spam, prévention et détection d'intrusion) représentent 96 M€ (8,6 %) en hausse de 37,1 %.

Source : « La sécurité des systèmes d'information », rapport du député Pierre Lasbordes. 26 novembre 2005

La rareté des personnes qualifiées en sécurité informatique est aussi pointée du doigt dans la 8e édition de l'enquête sécurité des SI réalisée par Ernst & Young fin 2005. Pascal Lointier renchérit : « Il n'y a pas de cursus en France qui permettrait de donner les bases fondamentales de la sécurité informatique pour un « grand public » de professionnels et responsables en entreprise ». De son côté, maître Eric Barbry, directeur du département nouvelles technologies au cabinet Alain Bensoussan rappelle que « la sécurité informatique n'existe en France que depuis un ou deux ans ! Ce n'est que depuis quelques temps que je fais des contrats de travail et des chartes pour des RSSI ».

8.3 LA PRÉVENTION DES RISQUES

« La prévention des risques n'est pas quelque chose qui peut être livrée avec des logiciels. Elle ne nécessite pas toujours des actions de sécurité, rappelle Thierry Durand.

1. CSO magazine n°12. Juillet 2006.



Beaucoup de grands patrons imaginent aussi qu'en externalisant leur informatique ils n'auront plus de problèmes de sécurité. C'est faux ».

Pour assurer une bonne protection de leurs réseaux, les entreprises doivent mettre en place différents gardes fous en amont. Il s'agit notamment d'assurer une gestion parfaite des droits d'accès des employés. Pour les grosses entreprises, c'est parfois un casse-tête mais qui doit être impérativement réglé. « Le système d'information d'une grande entreprise voit plusieurs dizaines de milliers de PC directement connectés et près d'un demi-million d'utilisateurs identifiés dont plus de 80 % sont des partenaires. Ces partenaires extérieurs sont des fournisseurs, des industriels, des commerciaux, des sous-traitants », indique Thierry Durand de PSA Citroën. Autant dire que la gestion des droits est une priorité. Un mauvais inventaire peut être à l'origine de deux problèmes :

- Une personne qui devrait avoir des droits mais qui ne les a pas encore est en situation pénalisante pour l'entreprise car elle ne peut pas travailler dans de bonnes conditions. Si elle utilise les droits d'un autre employé c'est dangereux car il s'agit d'une faille de sécurité. Ouvrir un compte en trois jours est jugé encore trop long par les responsables.
- Un ancien employé qui conserve des droits est également un danger. Chez PSA Peugeot Citroën par exemple 10 à 20 minutes sont généralement suffisantes pour informer l'ensemble des serveurs concernés lorsqu'une fermeture de droits d'accès est engagée. D'autres entreprises sont beaucoup plus laxistes et mettent une à deux semaines pour les clôturer ! Les conséquences peuvent être dramatiques pour l'entreprise. Voici un exemple relaté par le commissaire Crespin de la BEFTI : « un établissement financier de la place de Paris a découvert dans un journal des informations connues seulement d'un cercle très restreint d'initiés. Une enquête est menée et l'on s'aperçoit que les boîtes aux lettres des dirigeants étaient reroutées vers l'extérieur. Un ancien directeur informatique, rayé des cadres de la société depuis un an, possédait encore ses fonctions d'administrateur »¹.

Pour Pascal Lointier « l'insouciance et la méconnaissance des risques sont les vrais éléments qui permettent le développement de la cybercriminalité. Les entreprises ne sont pas assez sensibilisées ». Des propos confirmés par une étude réalisée en 2006 par Ernst & Young : seulement 20 % des entreprises françaises assurent à leurs salariés une formation régulière sur la sécurité et la maîtrise des risques, contre 47 % des entreprises dans le monde. Il faut que les salariés comprennent que leurs identifiant et mot de passe ne doivent pas être donnés à leurs enfants pour qu'ils se connectent depuis la maison au site de l'entreprise. Cela peut paraître comme une évidence mais plusieurs exemples de ce genre nous ont été relatés... Quelles peuvent être les conséquences ? Si l'ordinateur personnel du salarié n'est pas bien protégé, il peut être une cible parfaite pour un pirate qui souhaite s'infiltrer dans le réseau de la société.

1. CSO magazine n°12. Juillet 2006.



« Il est également nécessaire de sensibiliser les employés à l'importance des données qu'ils ont eux-mêmes, explique Thierry Durand. Chez nous, il se passe souvent plusieurs années entre le lancement d'un nouveau projet de voiture et la sortie en bout de chaîne du premier modèle. Les techniciens ou les ingénieurs passent plusieurs mois sur des programmes de conception assistée par ordinateur. Ils en parlent avec passion. Au point même de faire des blogs sur Internet et de l'illustrer avec des photos R&D ! Cela arrive ! Ne s'agit-il pas alors d'une faute lourde lorsqu'un engagement de confidentialité a été signé ? »

Les entreprises qui travaillent régulièrement avec des partenaires commerciaux ou des sous-traitants doivent aussi s'inquiéter de leur niveau de sécurité. Un employé d'une de ces sociétés peut venir au siège social et connecter son ordinateur portable au réseau. Imaginez que ce PC soit contaminé... Autre hypothèse : le réseau d'un des partenaires présente des trous de sécurité. Des informations confidentielles que vous lui avez transmises pourraient être récupérées par un logiciel espion ou une intrusion.

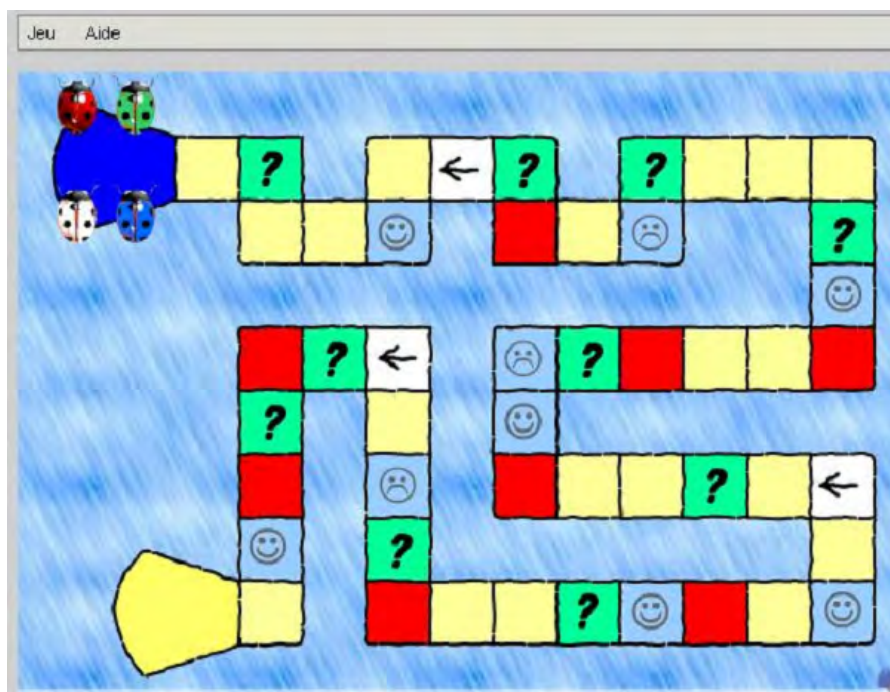
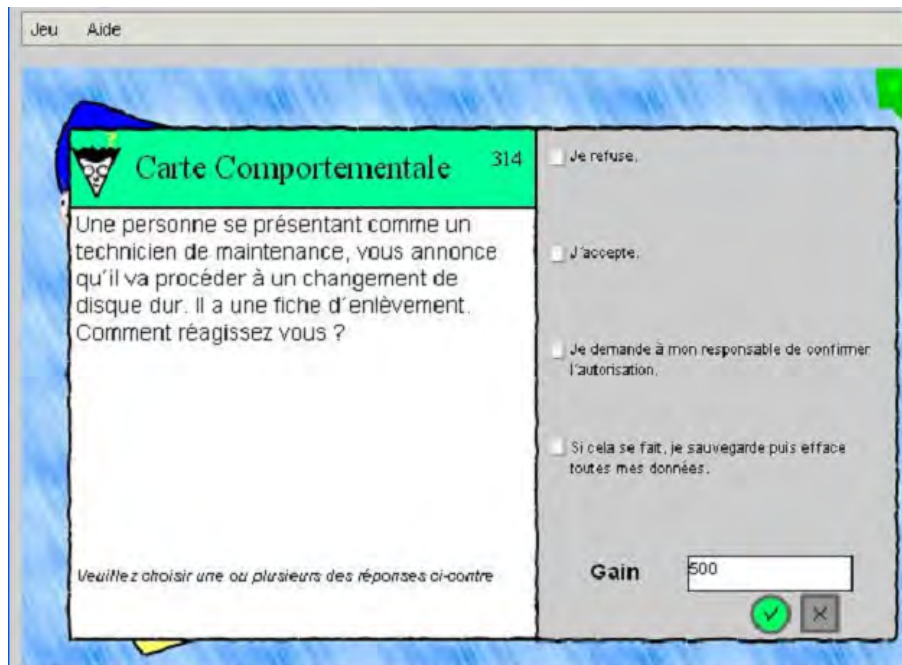
Toutes ces mesures ne nécessitent donc pas des logiciels et des équipements de sécurité. Mais elles ne sont pas toujours mises en place car c'est plus simple d'acheter un antivirus que de former ses salariés. Pour le patron et ses employés, la sécurité informatique est synonyme de propos abscons (ils n'ont pas tort puisque la sécurité informatique est entre les mains d'informaticiens qui utilisent leur jargon !) et d'informations inutiles. « cela ne m'arrivera pas ; je ne suis donc pas concerné », tel est l'argument de bons nombre de responsables. D'autres cadres supérieurs se croient tellement protégés par leur service informatique qu'ils en oublient les précautions élémentaires !

Pour rendre plus attractive cette problématique, Hapsis a eu la bonne idée de créer un jeu. Selon ce cabinet de conseil indépendant, la participation active de l'employé permet de mieux mémoriser, et surtout, de se sentir rapidement impliqué. Deux techniques sont utilisées. Un jeu de l'oie, *Sensirisk*, qui associe plusieurs personnes autour d'une table, ou via l'intranet, et *Computer Crime Investigation*, qui est en quelque sorte un Cluedo version sécurité.

Pour Guillaume Rincé, RSSI chez TDF, cette solution est intéressante¹ : « Jusqu'alors notre approche restait académique, de type présentation PowerPoint classique. Nous avons cherché un moyen un peu plus interactif et ludique pour retenir l'attention et marquer les esprits des gens qui suivent ces formations. Le but étant qu'ils appréhendent mieux le sujet et retiennent plus de choses qu'avec une formation classique. En effet, la sécurité informatique n'est pas forcément un sujet qui passionne les foules et qui donne lieu aux formations les plus attractives... Notre objectif est de mettre en place des formations pour de petits groupes de personnes et de développer les interactions entre elles. L'autre jeu proposé par la société HAPSIS, *Computer Crime Investigation* (CCI), est à mon sens plus adapté à une grande campagne de formation interne, dans le cas où l'on souhaite sensibiliser l'ensemble de l'entreprise. Le jeu Sensirisk est livré avec une base de connaissances et un ensemble de questions standard et offre la possibilité d'adapter tout ce qui correspond au con-

1. Magazine *Antennes*. Octobre 2005.





Figures 8.3 et 8.4 – Le jeu Sensirisk est une façon originale pour sensibiliser les salariés.

texte et à l'environnement de sa propre entreprise. Nous avons donc pu modifier un certain nombre de choses afin de refléter l'univers de TDF et les objectifs que nous souhaitons atteindre... Le fait est que les participants se prennent au jeu car ils ne se contentent pas de suivre un discours ou de visualiser passivement des informations. Ils sont parties prenantes. »

Pour les responsables informatiques, l'avenir de la prévention des risques passe certainement par un tableau de bord. « Actuellement, les seuls indicateurs dont on dispose sont trop souvent des « pompes funèbres » (combien d'attaques ou de failles constatées) ou des justifications d'investissement (en présentant toutes les attaques passées devant un firewall et qui ont été bloquées), constate Thierry Durand. Ce ne sont alors que des démarches ponctuelles qui ne visent qu'à satisfaire un petit bout d'un secteur de l'informatique. La véritable prévention ce n'est pas la somme des actions de sécurité individuelle. Quelque chose de nouveau, apparu début 2006, semble très prometteur : un tableau de bord inspiré de la problématique de gestion financière. Ce « tableau de bord équilibré » reflète les véritables risques pour l'entreprise. Il s'agit de voir quels sont les facteurs clés de succès qui contribuent à réduire ces risques. Des indicateurs sont construits à partir de données terrain mais elles ne sont jamais utilisés brutalement car elles n'auraient alors pas de sens. L'année 2007 devrait être une étape majeure et décisive pour les premières réalisations de ce type de tableaux de bord. »

Et si l'avenir ne consistait pas aussi dans la suppression des intranets ! Ces réseaux internes à une entreprise sont un contresens pour certains spécialistes : Internet, c'est une démarche d'interconnexion des réseaux tandis qu'intranet est une démarche de fermeture et d'isolation. « Les entreprises se sont dotées d'Intranet car Internet était la foire d'empoigne, rappelle Thierry Durand. Mais un intranet coûte très cher car il faut le gérer, le protéger et ça gêne la communication en permanence ».

Il n'est plus rare que des entreprises réfléchissent donc à la suppression de leur intranet. Cette mutation signifiera donc que tout le monde puisse entrer sans montrer patte blanche sur le réseau qui sera fondu dans Internet. Pour relever ce défi, il faudra résoudre différents problèmes. « Avant d'être exposé sur un réseau public chaque serveur doit impérativement disposer d'une protection parfaite et d'un suivi permanent et automatisé, constate Thierry Durand. Cette mise en œuvre préalable est un chantier technique majeur doublé d'une organisation lourde. Le second point concerne la sensibilisation budgétaire. L'informatique est de plus en plus un atout concurrentiel et des fonctions nouvelles sont en permanence attendues pour servir les besoins de l'entreprise. Comment gérer les priorités entre le besoin de disposer de ces fonctions vitales et le chantier colossal d'évolution d'une infrastructure dont on ne perçoit que mal les imperfections ? L'analyse des risques comparés, seul outil objectif d'aide à la décision, ne permettra que difficilement d'y parvenir avant six à dix ans ».



En résumé

Pour de nombreuses entreprises, la sécurité est synonyme de coûts. Elle est aussi synonyme d'un responsable informatique qui est le plus souvent seul à gérer cette problématique. Il n'est donc pas étonnant qu'elles soient incapables de répertorier tous leurs postes de travail et de faire une analyse correcte — et surtout objective — de leurs vulnérabilités. La montée de la cybercriminalité doit inciter fortement les dirigeants à considérer la sécurité informatique comme une donnée essentielle de leur performance économique. Cela implique l'utilisation d'outils spécialisés mais surtout une meilleure sensibilisation de tous les salariés.

Creative Commons BY-NC-ND



9

Antivirus : l'intox marketing

« Détection de 100 % des codes malveillants », « Elimine les virus sous toutes leurs formes », « Sécurise la navigation sur Internet »... Les multiples messages figurant sur les boîtes des logiciels de sécurité sont efficaces : ils font vendre ! Le chiffre d'affaires du marché des solutions antivirus était de 2,7 milliards de dollars en 2003, de 3,3 milliards en 2004 et d'environ 3,8 milliards en 2005 (source : IDC 2005). Voilà un secteur qui ne connaît pas la crise. Symantec, le numéro 1 mondial de la sécurité, a annoncé un chiffre d'affaires de 5 milliards de dollars (en hausse de 8 % en un an) pour son exercice fiscal 2006 (arrêté à mai 2006).

« Surfez tranquille, nous faisons le reste » : c'est en quelque sorte le slogan des éditeurs. Une protection totalement efficace serait donc possible ? Rien n'est moins sûr ! Qui n'a jamais constaté qu'une infection informatique était parvenue à pénétrer dans son ordinateur ?

Quel que soit le type de menace, le maillon faible est, et restera, toujours le même : l'utilisateur. Pour deux raisons principales : d'abord les erreurs de manipulation — accompagnées d'une baisse de la vigilance — et ensuite les réglages parfois compliqués de ces programmes de sécurité. Cette situation serait moins alarmante si les antivirus étaient plus efficaces ! Régulièrement, la presse informatique présente des tests comparatifs. Leurs méthodes d'analyse et leur objectivité (les éditeurs d'antivirus sont aussi des annonceurs...) laissent parfois à désirer. Pour consulter un avis un peu plus pertinent, on peut lire le rapport du ministère anglais du commerce. Publié en 2004 ¹, il indique qu'environ 90 % des grandes entreprises et 90 % des PME. britanniques sont protégées par un antivirus. Malgré cela, environ 68 % d'entre elles ont été victimes d'attaques virales en 2003. L'une des conclusions du rapport est sans appel : les antivirus seuls ne sont plus suffisants. Ils sont incapables d'assurer une protection efficace.

1. S. Stimms, S. Potter et A. Beard, *Information Security Breaches Survey 2004*. UK Department of Trade and Industry. <http://www.security-survey.gov.uk>

Un ver dans une centrale nucléaire !

Janvier 2003. La panique gagne le service informatique de la centrale Besse-Davies dans l'Ohio, aux Etats-Unis. Malgré la présence d'un pare-feu (ou *firewall*) et d'un antivirus, les réseaux de surveillance informatique de la centrale ont été victimes du ver Sapphire/Slammer. Ces réseaux ont été paralysés pendant plusieurs heures. Quelques mois plus tard, la Nuclear Regulatory Commission indiquait que la propagation est passée par le réseau privé d'un prestataire externe. Or, ni cette centrale, ni cet intermédiaire n'avaient appliqué le correctif publié six mois plus tôt par Microsoft et qui permettait de bloquer l'attaque via les serveurs SQL 2000. Le document révélait aussi que d'autres centrales avaient connu des problèmes plus ou moins similaires liés à l'infection Slammer...

Entre les affirmations des éditeurs et l'expérience de tous les jours, l'utilisateur a le plus grand mal à s'y retrouver. Cette situation résulte d'une méconnaissance de la nature même du problème de la détection virale et, de façon plus générale, des codes malveillants. Nature que certains vendeurs d'antivirus ignorent eux-mêmes ou occultent sciemment !

Pour comprendre en quoi le marketing de certains éditeurs frôle la publicité mensongère, il faut se reporter à des travaux de référence dans le domaine de la virologie informatique et à certaines études théoriques ou pratiques.

Attaque du parlement britannique !

Novembre 2005. Le parlement est victime de hackers chinois qui profitent d'une faille de logiciels contenu dans Windows. De simples courriers électroniques ciblaient soixante-dix membres du gouvernement britannique. Ces e-mails contenaient le code malveillant destiné à prendre le contrôle de leur ordinateur en y installant un cheval de Troie. Le code était indétectable par les antivirus au moment de l'attaque. Heureusement, la société gérant pour le parlement le trafic du courrier a pu bloquer cette attaque à temps¹.

9.1 LA DÉTECTION DE TOUS LES VIRUS OU LA QUADRATURE DU CERCLE

Le père de la virologie informatique est sans conteste Fred Cohen dont la thèse² en a jeté les bases rigoureuses. Après avoir formalisé d'un point de vue mathématique la notion de virus informatique, il s'est attaché à répondre à la question suivante : existe-t-il un programme permettant de détecter systématiquement un virus ? Il a

1. T. Espiner, *Hackers attacked parliament using WMF exploit*, ZDNET UK, 23 janvier 2006.

2. Fred Cohen, *Computer Viruses*, Université de Californie du sud, 1985.



prouvé qu'un tel logiciel, dans l'absolu, est une impossibilité mathématique. En clair, le problème de la détection virale est généralement indécidable. Cela signifie qu'il n'existe aucun moyen de choisir systématiquement entre les réponses « infecté » ou « non infecté » quand un programme est soumis à l'analyse. La preuve mathématique étant quelque peu technique, Fred Cohen a imaginé, à titre d'illustration, le code suivant, appelé « virus_contradictoire » :

```
Program virus_contradictoire
{
  si non D(virus_contradictoire) alors
    lancer l'infection
  fin si
}
```

Pour déterminer si un programme P est infecté ou non, considérons une procédure de décision D quelconque (en d'autres termes un antivirus). Le code virus_contradictoire alors invoque D pour l'appliquer sur lui-même et si D répond « non-infecté » alors le virus lance l'infection. Il y a contradiction. Cet exemple peut paraître simpliste. Il n'en illustre pas moins l'indécidabilité générale de la détection virale, démontrée rigoureusement par Fred Cohen.

Ce résultat fondamental montre que les affirmations selon lesquelles un produit peut détecter systématiquement les virus inconnus sont fausses. Mais d'autres résultats théoriques permettent de mieux contrer ces affirmations.

9.2 LA DÉTECTION VIRALE : QUAND LES ANTIVIRUS FONT MIEUX QUE LES CRYPTANALYSTES

Les résultats de Fred Cohen concernent la problématique de la détection virale dans son ensemble. Dans la pratique, beaucoup de codes malveillants sont toutefois détectés. Cela remet-il en cause ses résultats ? Non. La preuve mathématique de son résultat a été maintes fois vérifiée. Il considérerait une détection systématique. Autrement dit, il existe des classes de virus pour lesquelles une détection efficace est possible, sous certaines conditions toutefois. A la suite de ses travaux, des chercheurs ont étudié, et continuent d'étudier, des classes particulières de codes malveillants pour lesquelles il s'agissait de déterminer la complexité calculatoire de la détection dans un ordinateur classique (quand la mémoire et le temps de calcul sont limités comme dans le cas d'un ordinateur réel).

Mais en quoi la complexité calculatoire concerne-t-elle la détection virale ? Certains chercheurs (Leonard Adleman en 1989, Diomidis Spinellis en 2003, Zuo et Zhou en 2004, Bonfante, Kaczmarek et Marion en 2005) ont établi des résultats prouvant que pour beaucoup de classes de virus, rencontrées en pratique dans nos ordinateurs, le problème de leur détection appartenait à la classe NP-complet. D'autres études ont permis de montrer que pour certaines familles de virus, le problème posé par leur détection relevait de classe encore plus difficile que celle des problèmes NP-complets. Que faut-il en conclure ? Si un antivirus pouvait détecter systématiquement de telles classes de virus... il serait capable de percer les systèmes

La complexité calculatoire

Elle peut être définie comme le nombre d'opérations qu'un ordinateur doit effectuer pour résoudre un problème concernant des données de taille n . Cette complexité s'exprime par une fonction mathématique f qui dépend de n soit $f(n)$. Par exemple, la meilleure méthode possible pour trier n nombres requiert $n \cdot \log(n)$ opérations (au moins n car pour trier il faut d'abord lire les nombres). Les spécialistes de la théorie de la complexité ont alors classé les problèmes selon leur facilité de résolution. Sans entrer dans les détails techniques, deux grandes classes ont été identifiées.

La classe P des problèmes faciles (du moins pour un ordinateur) — La fonction $f(n)$ est en général un polynôme en n . Pour cette classe de problèmes, on connaît toujours un moyen de les résoudre (au pire en utilisant un ordinateur).

L'autre classe est la classe NP (non polynomiale). Ce sont les problèmes que l'on ne sait pas résoudre sinon en un temps prohibitif ou avec des ressources mémoire irréalistes. La fonction $f(n)$ est alors non polynomiale et mais plutôt exponentielle. A titre d'exemple, le problème de la factorisation d'un nombre n (écrire tout nombre entier comme produit de nombres entiers premiers, c'est-à-dire divisibles uniquement par 1 et eux-mêmes) requiert environ $e(\sqrt{\ln(n)} \cdot \ln(\ln(n)))$ opérations.

En pratique, dès que n est grand, il devient impossible de le factoriser (le record concerne un nombre de 200 chiffres pour quatre mois de calcul sur des supercalculateurs). Rappelons que la cryptologie utilise, dans les systèmes dits à clef publique, l'impossibilité pratique de la résolution du problème de la factorisation pour protéger nos données. Actuellement, des nombres de plus de 500 chiffres sont utilisés par exemple dans un logiciel comme PGP¹ (*Pretty Good Privacy* ; c'est le standard de chiffrement « grand public »).

Enfin, précisons que dans la classe NP, il existe une sous-classe de problèmes plus difficiles que les autres appelés problèmes NP-complets. Cette classe est très intéressante car toute solution qui permettrait de résoudre en pratique un seul des problèmes de cette classe, permettrait *de facto* de résoudre tous les autres problèmes NP-complets. Le problème du voyageur de commerce en est un : celui-ci doit partir de chez lui, visiter n villes et revenir à son domicile sans repasser par une agglomération déjà visitée. Dès que le nombre de villes est grand (supérieur à 400 ou 500), on ne sait plus résoudre en pratique ce casse-tête.

de chiffrement comme PGP ou le système RSA². Cet antivirus n'existe pas ! De quoi relativiser les affirmations de détection de 100 % des virus, *a fortiori* inconnus.

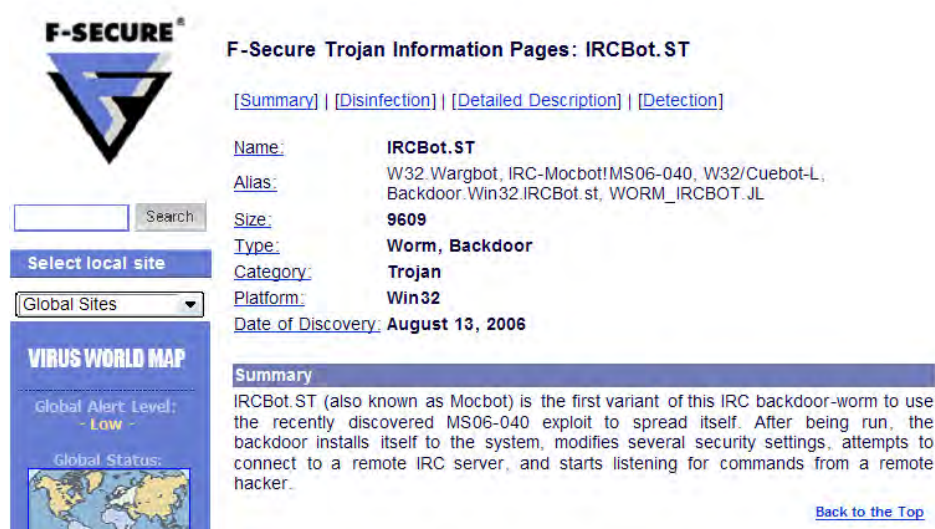
1. <http://www.pgp.com>

2. Le système RSA (acronyme formé du nom de ses trois inventeurs D. Rivest, A. Shamir et L. Adleman) est un système cryptologique dont la sécurité repose sur la difficulté du problème de la factorisation. Le système Pretty Good Privacy (PGP) utilise en partie RSA.



9.3 LE FONCTIONNEMENT DES ANTIVIRUS

Ils s'appuient sur des règles de décision que l'on peut modéliser par des tests statistiques. Ces règles poursuivent un objectif : déterminer si un code malicieux est présent dans un fichier ou dans la mémoire. Elles s'appuient sur une base de signatures¹ dans le cas de l'analyse de forme ou sur une base de comportements malveillants² dans le cas de l'analyse comportementale. Ces banques de données fonctionnent comme un fichier d'empreintes digitales ou anthropométriques de la police. Il n'y a identification possible que si l'élément incriminé est connu au moins dans l'une des bases utilisées. Par conséquent, un code ne sera détecté que lorsque la base de signatures ou de comportements aura été mise à jour ou si le code analysé utilise des techniques (comportements) déjà référencées.



F-SECURE®

F-Secure Trojan Information Pages: IRCBot.ST

[[Summary](#)] | [[Disinfection](#)] | [[Detailed Description](#)] | [[Detection](#)]

Name: IRCBot.ST

Alias: W32.Wargbot, IRC-Mocbot!MS06-040, W32/Cuebot-L, Backdoor.Win32.IRCBot.st, WORM_IRCBOT.JL

Size: 9609

Type: Worm, Backdoor

Category: Trojan

Platform: Win32

Date of Discovery: August 13, 2006

Summary

IRCBot.ST (also known as Mocbot) is the first variant of this IRC backdoor-worm to use the recently discovered MS06-040 exploit to spread itself. After being run, the backdoor installs itself to the system, modifies several security settings, attempts to connect to a remote IRC server, and starts listening for commands from a remote hacker.

[Back to the Top](#)

Figure 9.1 — Les sites des éditeurs présentent chaque jour les dernières menaces.

Mais entre la certitude affichée sur la boîte d'un logiciel et les techniques réellement mises en œuvre, la pratique peut révéler de mauvaises surprises. La raison relève du marketing. Le logiciel doit être d'une part fluide (pour simplifier, il ne doit pas ralentir le PC du consommateur et analyser rapidement tout le disque

1. Une signature est une chaîne de caractères, non nécessairement contigus, qui permet d'identifier un programme donné. C'est en quelque sorte l'équivalent des empreintes digitales, à la différence notable qu'une signature virale donnée peut être retrouvée dans plusieurs fichiers différents, certains non viraux mais détectés comme tels. Ce sont les fameux « faux positifs ».
2. Pour reprendre l'analogie de la note 6, de même qu'un criminel peut être identifié par son mode opératoire, un virus peut être découvert grâce aux actions qu'il tente de réaliser. C'est l'analyse comportementale. Cette technique est entachée des mêmes défauts et limitations que son homologue utilisant les signatures.



dur) et d'autre part afficher de bonnes performances (en clair repérer les intrus et les effacer). Sans ces deux critères, l'utilisateur sera tenté de le désactiver ou, pire, d'opter pour le logiciel d'un concurrent ! D'où la tentation de faire quelques compromis techniques. Résultat : le programme est certes plus rapide pour scanner un disque dur et plus facile à configurer mais son niveau de protection antivirale est amoindri. Ainsi, sur les quelque 100 000 codes malveillants répertoriés, beaucoup d'antivirus n'en gèrent effectivement que quelques milliers. Un test simple suffit à le vérifier : il consiste à soumettre à l'analyse un code déjà ancien. Ainsi, le ver MyDoom, qui a frappé en 2003, n'est plus détecté en 2006 par certains produits. De quoi faciliter le travail des apprentis pirates...

Le meilleur exemple est sans doute celui de la recherche de signatures quasi-systématiquement utilisé soit, directement sous différentes formes, soit comme phase finale de processus plus complexes mais également plus incertains. Détecter un code malveillant et l'identifier suppose de disposer d'une base de références qui associe un nom à chaque code reconnu.

Une étude poussée de la plupart des produits du commerce (Filiol — 2006) a montré que non seulement ces signatures sont généralement implémentées de manière faible, voire très faible, mais surtout de telle sorte qu'il est très facile pour un pirate de les identifier et de les contourner. Le contournement des produits s'avère donc assez facile, comme le prouvent les différentes expériences en laboratoire. Il suffit à un pirate de modifier quelques octets d'un virus connu pour le rendre à nouveau indétectable. La même étude a également montré que les techniques comportementales, dont le marketing des éditeurs vante tout le mérite et le caractère innovant, peuvent être contournées de manière similaire.

Quand les antivirus multiplient les fausses alertes

La précipitation est mauvaise conseillère. A trop vouloir devancer les attaques des pirates, les éditeurs d'antivirus publient parfois des mises à jour pires que le mal. En mars 2006, quelques éditeurs se sont particulièrement distingués.

Le logiciel de l'éditeur américain McAfee signalait la présence du virus W95/CTX dès qu'on ouvrait un fichier Excel. En réalité, il s'agissait d'une fausse alarme due à une mise à jour un peu précipitée... Selon les paramètres de l'utilisateur, le fichier suspect, une fois renommé était transféré dans un dossier différent, voire carrément supprimé. Plus de 1000 personnes auraient signalé ce problème auprès de la société. Quelques heures après la découverte et la révélation par la presse de cette bétise, McAfee diffusait un correctif.

Quelques jours plus tard c'est au tour de l'antivirus de l'éditeur Symantec de faire du zèle. Une mise à jour de son Norton bloquait la connexion Internet des abonnés (essentiellement américains) au fournisseur d'accès AOL (vingt millions d'abonnés). Ce logiciel aurait décidé cette mesure radicale après avoir détecté une attaque vers l'ordinateur de l'internaute. En clair, il prenait les serveurs d'AOL pour des repaires de pirates... Quelques heures après cette bétise, le site de l'éditeur publiait un correctif.



9.4 LE CONTOURNEMENT DES ANTIVIRUS

Les études théoriques menées par Fred Cohen permettent de démontrer que l'ensemble de tous les virus est aussi grand que celui des nombres entiers, autrement dit en théorie, infini. Il est alors aisé de comprendre qu'un antivirus, quelle que soit la technique de détection employée, ne peut pas gérer une infinité de codes, l'espace d'un disque dur étant par essence limitée. Cela signifie qu'un antivirus n'est capable de gérer qu'une fraction infime, non seulement de tous les virus possibles mais également des virus connus, le nombre de ces derniers étant estimé à environ 100 000¹.

Ce constat permet alors de comprendre pourquoi les programmeurs de virus parviennent régulièrement à contourner ces logiciels de protection. Deux solutions s'offrent à eux :

- 1- Modifier une souche ou une variante détectée ou créer une souche en s'inspirant de techniques virales connues. L'opération est généralement assez simple dès lors que l'on dispose de l'antivirus à contourner. Mais ce n'est pas toujours obligatoire puisque la plupart de ces logiciels sont équivalents. Autrement dit, contourner un produit donné, revient à contourner beaucoup d'autres marques. Les expériences menées en laboratoire l'ont malheureusement démontré. Le plus navrant tient au fait que cela ne réclame pas de compétences très développées. Un simple programmeur y parvient aisément.
- 2- Créer une nouvelle souche mettant en œuvre une nouvelle approche algorithmique. Là aussi, l'expérience montre que les antivirus sont incapables de la détecter. Les recherches menées au Laboratoire de virologie et de cryptologie de l'Ecole Supérieure et d'Application des Transmissions ont permis d'identifier, de formaliser et d'évaluer techniquement de nouveaux algorithmes viraux, encore inconnus. Les résultats de tests sont sans appel. Les antivirus restent désespérément muets. Et l'analyse mathématique des modèles correspondants démontre qu'ils le resteront à jamais.

Le plus ironique tient au fait que ces logiciels doivent à la fois gérer « l'imagination » des pirates mais aussi s'adapter aux évolutions techniques de l'industrie logicielle. Dans le but de développer des protections contre la décompilation/désassemblage et plus généralement l'analyse des programmes, les programmeurs ont développé des solutions visant à compliquer cette analyse. Il s'agit des techniques d'obfuscation². La finalité est d'assurer les droits de licence et de limiter le plus possible le piratage des logiciels. Mais ces techniques sont connues et des logi-

1. Ce chiffre est le plus communément accepté en janvier 2006. Il existe des chiffres plus importants mais plus « fantaisistes » portant ce nombre à 200 000. Aucune information sérieuse n'a permis d'étayer cette donnée.
2. L'obfuscation consiste à rendre le code tellement inextricable et incompréhensible que son analyse requière ra des compétences et des ressources en temps telles qu'elle ne sera que difficilement inaccessible pour un humain et très difficilement possible voire impossible par des moyens automatiques. Ces techniques incluent des techniques de compression et de chiffrement.



ciels existent (le plus célèbre est *Armadillo*). Ces derniers permettent de protéger facilement un code contre l'analyse. Lorsque ces produits ou ces techniques, pour les plus efficaces, sont utilisées par les auteurs de virus, les antivirus échouent quasi-systématiquement dans l'analyse automatique des codes malveillants ainsi protégés.

9.5 LES AUTRES LOGICIELS DE SÉCURITÉ

A coté des antivirus, il existe d'autres produits présentés comme complémentaires :

Les pare-feux (ou firewall) — Ces logiciels surveillent et filtrent le cas échéant tout ce qui entre ou sort d'un ordinateur connecté à un réseau. Cette surveillance s'opère essentiellement par l'analyse des flux de données et l'analyse des différentes tentatives de connexion entrantes ou sortantes.

Les anti-spywares — Ils recherchent les bouts de logiciels contenus souvent dans d'autres programmes (commerciaux, shareware et freeware) — et dont la fonction consiste à collecter des informations sur votre machine, vos habitudes informatiques. Une fois récupérées, les spywares les envoient à des sites chargés de les exploiter, le plus souvent à des fins commerciales (proposition commerciale via le courrier électronique, par exemple). Certains spywares sont susceptibles de réaliser des actions nettement plus offensives.



Figure 9.3 — Il faut être informaticien ou maîtriser son jargon pour prendre la bonne décision !

Les anti-spam — Ces logiciels (voir chapitre 6) ont pour fonction de filtrer le courrier électronique non désiré qui inonde nos boîtes aux lettres électroniques. Outre l'effet d'engorgement, ces courriers sont souvent le vecteur d'attaques informatiques.

La plupart des éditeurs d'antivirus proposent des suites logicielles dans lesquelles sont intégrés tous ces produits. Quelle sécurité supplémentaire offrent-elles réellement ? En fait, si elles concourent clairement à augmenter le niveau de protection d'un ordinateur, elles présentent les mêmes limites qu'un antivirus et ne seront jamais un rempart absolu. La problématique de sécurité est identique à celle concernant les antivirus : il n'est pas sérieux de prétendre arrêter ou empêcher une attaque *a priori*, si cette dernière est innovante ou inconnue. De plus, ces produits sont plus délicats à configurer, en particulier pour un utilisateur ne maîtrisant pas les rouages de l'informatique et ses messages abscons. Combien d'internautes ont reçu un petit message de leur pare-feu leur demandant d'accepter ou non la demande de connexion d'une application sans comprendre le moindre mot utilisé ? Certainement la majorité du grand public abonné aux offres d'internet à haut débit ! Encore une fois, les éditeurs de ces logiciels laissent la responsabilité aux utilisateurs...

Les éditeurs ont de la suite dans les idées !

Faut-il acheter un pack rassemblant différents logiciels de sécurité ? L'éditeur y trouve plus un intérêt que l'internaute. Il est rare en effet qu'un éditeur propose un antivirus, un firewall et un antisipam qui soient aussi performants. Ainsi, ZoneLabs est réputé pour son pare-feu ZoneAlarm Pro mais son antivirus ne remporte pas autant d'éloges. De son côté, Symantec a un pare-feu correct mais son antisipam et son antivirus ne sont pas aussi efficaces. Constat inverse pour Bitdefender. Seuls, deux éditeurs semblent sortir du lot. Il y a tout d'abord Kaspersky et sa « Personal Security Suite » (80 €). Elle permet de bénéficier d'une protection satisfaisante grâce à son antivirus, son firewall et son antisipam. Le « F-Secure Internet Security 2006 » (80 €) de l'éditeur F-Secure offre aussi un bon compromis. Mais il est réservé à des ordinateurs puissants car ce logiciel est très gourmand en ressources et exige un processeur très puissant.

En résumé

La lutte antivirale est condamnée, par définition, à une situation de réaction. Un antivirus ne sert-il à rien ? Absolument pas ! Mais il ne faut pas lui prêter plus de vertus qu'il n'en a. Dans une politique antivirale, ce logiciel ne représente que le bout de la chaîne et du processus de réflexion du responsable de sécurité. En d'autres termes, limiter une politique antivirale au déploiement et à l'utilisation d'un antivirus, aussi bon soit-il, est le meilleur moyen, pour avoir à terme des problèmes.

Creative Commons BY-NC-ND



10

Les systèmes de défense des réseaux d'entreprise

Les entreprises représentent de nos jours des cibles privilégiées pour les attaques informatiques. Elles constituent en effet une part essentielle du patrimoine industriel, intellectuel et économique d'un pays. Mais la conscience de leur importance stratégique, du moins en France et dans les pays latins, est encore souvent marginale et il est sidérant de constater qu'il est encore trop souvent facile d'attaquer une entreprise via ses ressources informatiques : vol de données de recherche et développement, vol de fichiers clients ou de tarifs, atteintes aux personnes dirigeantes et déstabilisation de l'entreprise, atteinte à la disponibilité des ressources de l'entreprise... Plus grave encore, si les entreprises commencent à intégrer la notion de sécurité des systèmes d'information, elles ont encore du mal à penser en termes de sécurité de l'information. Autrement dit, une véritable culture dans ce domaine doit être développée pour que les entreprises pensent instinctivement en termes de sécurité globale.

Cette pensée doit se concrétiser par une politique de sécurité, en relation avec une politique fonctionnelle : « je décide de ce que je dois faire et avec quels moyens, puis je détermine le besoin et le niveau de sécurité souhaité et j'adapte la mission et les outils à cette sécurité, et non l'inverse ». Il est donc important de faire de la sécurité une priorité. Si la politique fonctionnelle est établie en premier (c'est le cœur de métier), elle doit l'être en adéquation avec la sécurité finale voulue.

Pour ce faire, deux personnes ont un rôle fondamental dans l'entreprise, deux personnes qui devraient collaborer en permanence, et l'expérience prouve que les problèmes de sécurité proviennent souvent d'un manque de communication et de compréhension entre ces deux acteurs.

- **Le dirigeant d'entreprise** : ce dernier ignore malheureusement souvent qu'il peut être pénalement et civilement responsable d'un défaut de sécurité, des responsabilités qui peuvent le conduire en prison ou grever les ressources



financières de son entreprise en cas d'amendes souvent très lourdes. Il est également responsable devant les actionnaires qui peuvent lui demander des comptes en cas de problèmes de sécurité ayant porté atteinte à l'activité de l'entreprise (vol de données par exemple).

- **L'officier de sécurité (ou RSSI) :** il a la responsabilité de définir en liaison avec le dirigeant la politique de sécurité (dans le respect de la réglementation), les moyens à y consacrer et la manière de l'appliquer. Une fois en place, cette politique de sécurité doit être constamment contrôlée, évaluée et le cas échéant, affinée. Ce dernier doit prendre également en compte les problèmes de sûreté de l'entreprise (incendie, dégâts des eaux, risques électriques...) pour avoir une vision globale de la sécurité. La sécurité est ensuite gérée selon la technique du cercle « Prévention — Détection — Réaction — Reprise »¹. Actuellement, selon les chiffres fournis par le CLUSIF, 56 % des entreprises seulement disposent d'une telle politique de sécurité et seules 48 % s'appuient sur les normes existantes dans ce domaine.

Entre ces deux acteurs, le dialogue doit être permanent et aucune interférence ne doit perturber cette collaboration. On voit trop souvent des dirigeants négligeant les conseils avisés de leur RSSI pour suivre les conseils « intéressés » et par toujours pertinents de consultants et autres commerciaux. Le dirigeant d'une entreprise ne doit jamais oublier que la sécurité est avant tout un processus de pensée et non l'accumulation plus ou moins heureuse de produits de sécurité. L'expérience et le bon sens de son RSSI sont les meilleurs atouts sur lesquels il doit pouvoir compter.

10.1 LES MENACES CONTRE L'ENTREPRISE

Elles sont beaucoup nombreuses et omniprésentes, mais nous n'en avons pas toujours conscience :

- **La plupart des dirigeants d'une entreprise :** lors d'une expertise judiciaire auprès d'une société parisienne² spécialisée dans le conseil et traitant de dossiers sensibles, le dirigeant de cette société a découvert qu'il avait fait l'objet d'une attaque informatique ciblée d'une grande ampleur visant à lui dérober des données concernant plusieurs de ses dossiers sensibles ; c'est ce qui avait motivé l'enquête, initiée par la plainte d'un des clients de cette société. Alors que cette dernière possédait « l'équipement de base » (antivirus, pare-feu et une architecture à peu près correcte) en matière de sécurité, ses employés et ses cadres n'avaient aucune culture de sécurité et n'imaginaient pas qu'une telle attaque fut possible. Ils n'imaginaient même pas qu'ils puis-

1. Lire à ce propos l'article excellent de Philippe Bouvier « *Le cercle de la sécurité du système d'information* », MISC Le journal de la sécurité informatique, numéro 10, novembre 2003.

2. Les cas présentés ici ont été démarqués pour des raisons de confidentialité et du respect du secret de l'instruction.



sent intéresser des attaquants. Erreur fatale mais hélas répandue ! De très nombreuses entreprises n'ont même pas conscience qu'elles peuvent être l'objet d'une attaque ciblée et qu'à ce titre la vie même de leur entreprise est en jeu. Elles s'équipent d'un antivirus et de quelques logiciels de sécurité et les choses s'arrêtent là. « Nous constatons que chez les PME, 80 % du budget sécurité est dévolu à l'achat de solutions de filtrage réseau ou à la sécurité du poste de travail. Le test d'intrusion est pour elles une prestation de luxe ! Il intervient le plus souvent à l'arrivée d'un nouveau DSI, ou à la création d'un poste de RSSI ou après un incident », observe Hervé Schauer, du cabinet Hervé Schauer Consultants. Une décision qui n'est donc pas vraiment prise à titre préventif, ce qui constitue un mauvais point de départ à toute politique sérieuse de sécurité¹.

- **Les grands comptes :** ils sont familiers avec ce type de prestation. Leurs équipes chargées de la sécurité savent tirer rapidement profit du rapport d'intrusion. Les PME, par contre, auraient plutôt besoin d'un accompagnement presque pédagogique, didactique. Justement, les consultants ont su adapter leurs offres au budget et aux attentes des petites entreprises. « Ce que nous vendons aux PME est en réalité une prestation hybride entre un test de vulnérabilité, un test d'intrusion et une prestation de conseil en sécurité », explique Cyrille Barthelemy, consultant sécurité chez Intrinsec. Un service effectué le plus rapidement possible (trois jours le plus souvent) et pour un coût réduit (généralement autour de 3 000 euros HT).

Si cet état de fait concerne essentiellement les PME/PMI, les grandes sociétés ne sont pas non plus à l'abri. L'expérience montre, là aussi, que si l'approche technique de la sécurité des SI est à peu près bien prise en compte, le risque est insuffisamment pris en compte, voire nettement sous-estimé, notamment en ce qui concerne les attaques ciblées. La raison en est que contrairement aux pays anglo-saxons et asiatiques — qui dans le domaine ont développé une véritable culture de la sécurité — les pays latins ont encore une perception « naïve » des attaques. Alors que la sécurité générale, et en particulier celle des SI devrait s'inscrire dans une démarche globale de renseignement, elle n'est le plus souvent perçue que comme une activité « tactique » de plus au même titre que l'activité de RH, de gestion financière ou autre, alors qu'elle devrait être vue au plan stratégique.

Quels sont les différents risques ? Dans un monde de concurrence commerciale acharnée et sans pitié, tous les moyens sont bons et la dépendance vis-à-vis des SI est telle, que ces derniers constituent le vecteur rêvé : universel, omniprésent, discret, il permet d'atteindre les personnes et les ressources. Voici une présentation non exhaustive des risques :

- **Vol de données²** (données de recherche, clients, contrats...) : si l'affaire Valéo en 2005 a fait la une des journaux en France, l'affaire des logiciels israéliens professionnels contenant des chevaux de Troie a autrement frappé les esprits

1. « Sécurité: les tests d'intrusion se mettent à la portée des PME », Zdnet, 2/01/2006.

dans le monde. Ces logiciels étaient vendus à des sociétés et les codes d'accès des chevaux de Troie vendus, eux, aux concurrents de ces sociétés. Plusieurs pays semblent avoir été victimes et l'affaire est toujours en instruction. Cela illustre le fait qu'en termes de logiciel de sécurité, notamment à destination des administrations et des entreprises, des logiciels nationaux sont préférables.

- **Vol de ressources.** En 2005, une vingtaine de pirates ont pénétré les serveurs d'une entreprise et les ont utilisés, de manière discrète, pour distribuer des contenus illicites (vidéogrammes, phonogrammes, logiciels piratés) sur Internet. Outre le fait, dans la phase initiale de l'enquête, d'être soupçonnée d'avoir elle-même organisée cette diffusion, les ressources propres de cette entreprise étaient vampirisées par les pirates.
- **Atteinte à la disponibilité.** Les cas sont très fréquents où, par un simple déni de service commandité par un concurrent, une société se retrouve privée, souvent à un moment crucial pour la vie de l'entreprise, de ses données ou de ses serveurs. Imaginons l'impact d'une société de vente en ligne privée de son serveur web pendant quelques jours. Il existe de nombreuses autres techniques permettant de réaliser des indisponibilités plus ou moins longues. Selon le rapport 2005 du CLUSIF, près de 75 % des entreprises auditées ont une dépendance forte (une indisponibilité de moins de 24 heures a de graves conséquences sur l'activité) alors que seulement 2 % avouent une dépendance plutôt faible.
- **Extorsion de fonds.** Ce cas-là est survenu en 2005 aux Etats-Unis, dans plusieurs grandes sociétés avec des codes malveillants comme le ver Trojan.PGPCoder. Les données des disques durs ont été chiffrées et la clef était demandée contre une rançon. Ainsi, en avril 2006, des codes malicieux comme Crypzip ou Ransom.A ont été utilisés pour pratiquer ce genre d'extorsion numérique.
- **Atteinte à l'intégrité.** Les données sont détruites ou altérées de manière aléatoire. Imaginons une modification aléatoire de 5 % des résultats de recherche d'un laboratoire pharmaceutique sur un nouveau médicament.
- **Atteinte à l'image de l'entreprise.** Le simple « défaçage » d'un site web peut avoir des conséquences dramatiques et nuire gravement à une société. En 2005 et en France, cela a constitué 3 % des sinistres informatiques.
- **Atteinte aux personnes.** C'est probablement la moins connue des attaques potentielles. Elle n'en est pas moins redoutable. Elle autorise toutes les manipulations possibles. Imaginons un dirigeant d'entreprise devant négocier un gros contrat. Son concurrent peut tout simplement lui nuire personnellement pour le discréditer auprès de ses clients. Couplée à une publicité adéquate, l'opération peut être extraordinairement efficace.

2. Un excellent cas, tiré d'une autre affaire réelle qui a fait grand est celui présenté par D. Bénichou et S. Lefranc « L'opération Carbone 14 » Actes de la conférence SSTIC 2003. Disponible sur <http://www.sstic.org/>. Cette attaque ciblée, contre un SI pourtant très protégé, permet de voir qu'une architecture sécurisée n'est pas suffisante.



- **Désinformation.** Là aussi, il existe de nombreux cas tristement célèbres où de fausses informations ou des rumeurs, ont eu des conséquences gravissimes sur le cours des actions de grandes entreprises. Imaginons un serveur de messagerie d'une entreprise piraté par un concurrent qui l'utiliserait pour diffuser de fausses nouvelles sous l'identité de la société victime (son service de presse officiel par exemple)¹ et ainsi affoler les marchés financiers.
- **Sabotage physique de matériels informatiques** (près de 3 % des sinistres en France et en 2005).

Les scénarii ne manquent pas et pour la Direction pour la protection et de la sécurité de la défense² — chargée de la protection des sociétés travaillant pour la Défense — aucun ne relève de la science-fiction. La plupart exploite non seulement des faiblesses d'ordre technique dans les SI, mais surtout des aspects non techniques qui peuvent néanmoins avoir un impact très important sur ces derniers : facteur humain, aspect organisationnel....

10.2 L'ARCHITECTURE D'UN RÉSEAU SÉCURISÉ

Face à ces menaces multiples, la règle d'or est d'organiser des périmètres de sécurité. Il faut « cloisonner » et « bunkériser » tout ce qui doit l'être. Mais il n'existe pas de règle toute faite : c'est la politique de sécurité locale qui doit dicter les choix et non pas l'inverse, encore une fois.

Une politique de sécurité efficace, en matière d'architecture réseau, intervient à différents niveaux :

- Entrée du réseau,
- Serveurs,
- Ordinateurs des utilisateurs.

10.2.1 La DMZ (zone démilitarisée)

Le principe général d'une architecture réseau sécurisée est de disposer d'une ou de plusieurs machines dites « machines bastion », lesquelles servent de rempart face aux attaques venant de l'extérieur (principalement Internet). Toutes les ressources sensibles doivent donc impérativement être situées derrière le ou les bastions. Si ces derniers sont compromis, tout le réseau tombe. Le cas le plus connu de « machine

1. Cet exemple est inspiré d'un cas réel survenu en juin 2006 et qui a frappé le service de presse officiel du ministère de la défense de Taiwan. Une très grande société française, partenaire dans le projet Galileo, a également été victime d'une « mésaventure » en 2003. La sanction a été radicale : le cours de son action été divisé par 10.
2. Cet organisme du ministère de la Défense a pour mission de veiller à la sécurité du personnel, des informations, des matériels et des installations sensibles relevant de la défense nationale.

bastion » est constitué par le routeur d'accès au réseau et par le pare-feu. Cela inclut également les serveurs pour tous principaux services utilisés : web, FTP, courrier électronique, DNS... Mais les « machines bastions » doivent également être protégées. Le principe est alors d'utiliser une zone particulière appelée DMZ (zone démilitarisée). Cette zone est le concept fondamental de sécurité autour duquel tout réseau doit être architecturé. Elle va jouer le rôle de zone tampon entre le réseau interne considéré comme de confiance — et abritant les ressources internes de l'entreprise — et un réseau non maîtrisé et donc potentiellement dangereux (typiquement le réseau Internet mais cela peut inclure une partie plus large d'un réseau d'entreprise ouverte sur l'extérieur). La DMZ a pour rôle d'isoler les machines publiques gérant un certain nombre de services (DNS, courrier électronique, FTP, http...) du réseau critique interne (voir figure 10.1)

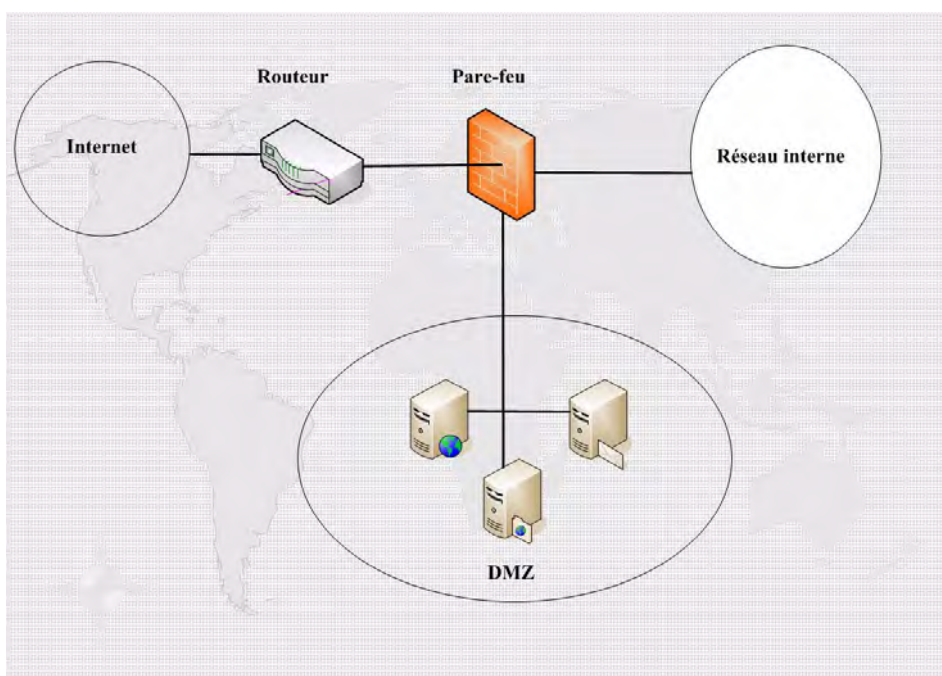


Figure 10.1 – La zone démilitarisée

Il est essentiel de noter que si la DMZ est une étape initiale essentielle dans la sécurisation d'un réseau, elle ne se suffit pas à elle-même. D'autres aspects doivent être pris en compte.

10.2.2 Le serveur proxy

L'utilisation d'un pare-feu est nécessaire pour assurer la protection au niveau du protocole TCP/IP, en filtrant ce dernier mais il ne prend pas en compte les autres protocoles et services. Pour cela, il faut ajouter de nouveaux éléments.



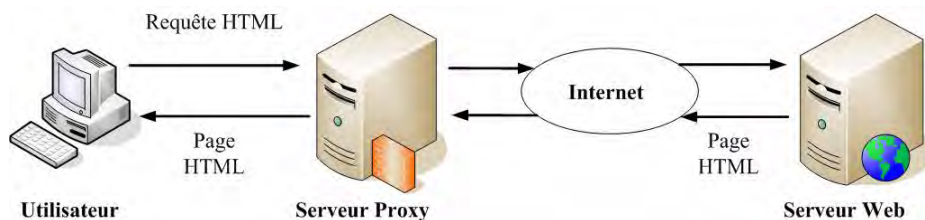


Figure 10.2 — Le serveur Proxy

Le premier est le serveur proxy, que l'on peut considérer comme un pare-feu applicatif. Il va par exemple assurer les fonctions de cache de pages web, le filtrage des URL (protocole HTTP), gérer les authentifications des utilisateurs... En gros, ce proxy va jouer le rôle de relais entre l'utilisateur (le client) et le serveur sollicité. Il va en particulier effectuer certains contrôles, le plus courant étant celui des requêtes web. Le navigateur, pour se connecter à une page donnée, va tout d'abord se connecter au serveur proxy. Ce dernier ensuite se connecte lui-même au serveur hébergeant réellement la page demandée. Cela permet d'une part de ne pas directement mettre en contact les utilisateurs internes d'une entreprise avec le réseau extérieur (Internet) mais d'autre part, il est ainsi possible de contrôler l'accès à certains sites, interdits par la politique de l'entreprise (sites pornographiques, sites de logiciels piratés...). Bien évidemment, le serveur proxy est placé dans la DMZ pour augmenter la sécurité.

10.2.3 Le serveur reverse proxy

Ce serveur a un rôle inversé de celui du proxy. Il protège un serveur de l'entreprise contre les attaques potentielles d'un utilisateur extérieur à l'entreprise (typiquement un internaute). Ce dernier ne se connecte pas directement au serveur, lequel n'est pas directement exposé. Le serveur de reverse-proxy peut ainsi filtrer et analyser les requêtes extérieures, exiger une authentification... Il interdit également au pirate de scanner les ports du serveur en question.

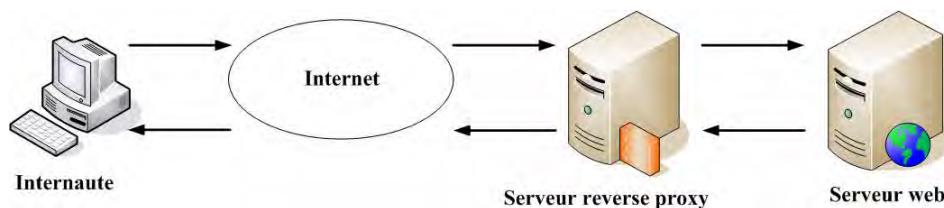


Figure 10.3 — Le serveur reverse proxy

Tous ces éléments (DMZ, serveurs proxy et reverse proxy) doivent être articulés de sorte que si un élément est victime d'une attaque, les autres doivent pouvoir prendre le relais. Autrement dit, aucune relation de dépendance ne doit exister, en termes de sécurité, entre ces divers composants. Seuls des audits constants, des tests de

scenarii d'intrusion — lesquels font partie intégrante du travail du RSSI en liaison avec son administrateur réseau — pourront confirmer la validité d'une architecture réseau sécurisée.

Il est crucial de garder à l'esprit que si une bonne architecture réseau sécurisé est un bon début et un prérequis indispensable, ce n'est en soi pas suffisant. Il est la pièce maîtresse d'une politique qui doit être plus large et intégrer bien d'autres aspects. Ces derniers impliquent des ressources critiques et qui souvent ne sont pas suffisamment bien gérées dans le contexte de la sécurité des SI : le temps, l'argent et le personnel. Une négligence dans leur gestion constituera ainsi autant de zones de faiblesses qu'un attaquant peut connaître par avance (s'il est bien informé sur l'entreprise) et saura utiliser.

10.3 LE TEMPS

Aussi surprenant que cela puisse paraître, c'est la première des ressources critiques. Bien avant l'argent ! Il est souvent possible d'économiser des crédits en donnant suffisamment de temps aux divers acteurs impliqués dans la sécurité des SI. Ce temps concerne essentiellement la veille technologique et la sensibilisation des utilisateurs.

L'informatique évolue presque tous les jours (nouvelles attaques, nouveaux produits, nouveaux concepts...). Sans une veille technologique permanente et conséquente, la sécurité d'une entreprise dans ce domaine deviendra très vite dépassée et obsolète. La simple hygiène logicielle (recherche et applications des correctifs) requiert un temps non négligeable. Et cela ne représente qu'une partie de la veille technologique nécessaire ! Six étapes doivent être considérées¹ :

- Définition des besoins et récupération d'informations internes à l'entreprise.
- Définition des sources (quantification et qualification).
- Collecte des informations.
- Analyse et synthèse des informations.
- Diffusion du renseignement.
- Sécurisation su S.I.

Le meilleur exemple d'une telle lacune est celle de l'attaque par le ver Sapphire/Slammer en janvier 2003. Elle utilisait une vulnérabilité connue et corrigée depuis plus de six mois. Pourtant, 200 000 serveurs ont été gravement victimes de ces attaques. L'expérience montre d'ailleurs que ce genre de lacunes concerne également les grandes entreprises.

1. Le lecteur pourra consulter l'excellent article de Marc Brassier, « *Mise en place d'une cellule de veille technologique* », MISC – Le journal de la sécurité informatique, numéro 5, janvier 2003. Ce dernier est très complet et décrit dans le détail la politique à tenir dans le domaine de la veille technologique, en fonction de la taille de l'entreprise.



Selon la taille de l'entreprise, cette veille sera faite par le RSSI en liaison avec l'administrateur réseau ou système par exemple, ou bien par une cellule spécialisée (coût annuel approximatif de 50 000 euros par an).

Le second volet qui réclame du temps est la sensibilisation des personnels. Elle est indispensable. Pourtant, les différents audits montrent qu'elle est systématiquement négligée. En 2005, seules 30 % des entreprises de moins de 500 salariés disposent de programmes de sensibilisation (source : CLUSIF). Les utilisateurs doivent être régulièrement être informés des risques, des évolutions et des points essentiels de la politique de sécurité (en particulier les interdictions mais également les conduites à tenir en cas d'incidents). L'expérience montre que des utilisateurs informés, sensibilisés et responsabilisés participent activement et efficacement à une meilleure sécurité informatique globale.

De grandes entreprises comme Boeing l'ont compris. En avril 2006, Janette Jarvis, responsable du pôle sécurité chez Boeing, a expliqué lors de la conférence EICAR 2006 à Hambourg, que les sensibilisations en matière de sécurité informatique étaient obligatoires, à raison de deux par an. Elles concernent tous les personnels (du simple employé aux dirigeants), lesquels faisaient l'objet d'une évaluation. En cas de non participation, des sanctions graduées sont prévues (blâmes, retenues financières, renvoi).

Enfin, du temps doit être consacré aux contrôles et à l'évaluation de la mise en place de la politique de sécurité.

10.4 L'ARGENT

La seconde ressource essentielle est l'argent. Il n'est jamais facile pour un dirigeant de financer une politique préventive en matière de sécurité des SI. Le meilleur exemple de la difficulté de perception dans ce domaine concerne le fameux « bug de l'an 2000 ». Alors que plusieurs milliards d'euros avaient été consacrés à la gestion anticipée du risque, de nombreuses voix se sont élevées, après coup pour contester la nécessité d'un tel investissement alors que finalement aucun problème sérieux n'a été enregistré. C'est là un cas typique de mauvaise perception. La bonne attitude aurait été de reconnaître que l'investissement réalisé a précisément permis d'éviter de gros problèmes. Trop souvent encore, les entreprises ne réalisent qu'après un sinistre informatique la nécessité d'une politique fondée sur l'anticipation et la prévention. Or, comment convaincre un dirigeant quand tout va bien ?

Selon l'enquête IDC Sécurité 2005¹, les dépenses informatiques globales sur le marché professionnel en France devraient atteindre en 2005, 41 009 M€, en croissance de 3,5 %. Les dépenses de sécurité informatique, des entreprises et des admi-

1. 103 entretiens réalisés auprès d'un panel de grandes entreprises et administrations en France, composées à 45% de plus de 2000 salariés et 55% de 1000 à 1999 salariés. Novembre 2005.



nistrations atteindraient 1 113 M€, en hausse de 17,4 % (contre 15,4 % de hausse entre 2004 et 2003).

Parmi ces dépenses de sécurité informatiques en 2005 :

- les services représentent 612 M (55 %) en hausse de 15,5 % ;
- les logiciels représentent 405 M (36,4 %) en hausse de 16,4 % ;
- les *appliances* (boîtiers physiques intégrant une ou plusieurs fonctionnalités (pare-feu/ VPN, anti-virus, anti-spam, prévention et détection d'intrusion) représentent 96 M (8,6 %) en hausse de 37,1 %.
- les cartes à puce, dont le taux de croissance en volume attendu sur 2005 est de 18 %
- avec 1 727 millions d'unité après une croissance de 12 % en 2004 ;
- les systèmes biométriques, qui devraient représenter environ 1 Md\$ au niveau mondial en 2007.

Toutefois selon le CLUSIF¹, une part significative des entreprises, soit 21 %, ne semble pas en mesure d'identifier cette dépense. Cela est principalement dû au fait que ce budget n'a pas une définition très claire ou un périmètre bien délimité. Le CLUSIF note cependant que d'une manière générale, le budget dans ce domaine est à la hausse pour 38 % des entreprises ou à la stabilisation pour 46 % d'entre elles. Le pourcentage du budget sécurité par rapport au budget informatique total est donné dans la figure 10-4 (source CLUSIF). Le plus surprenant est que la part de ce budget sécurité ne prend pratiquement pas en compte la formation, continue ou non, des personnels, ni leur sensibilisation régulière.

Budget sécurité / budget informatique

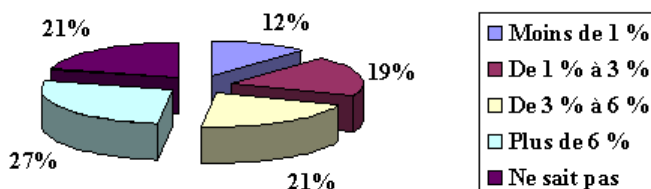


Figure 10-4 – Pourcentage du budget informatique consacré à la sécurité

1. Club de la Sécurité de l'Information Français, *Politiques de sécurité des systèmes d'information et sinistralités en France*, Rapport 2005.

10.5 LE PERSONNEL

La dernière et non la moindre des ressources à considérer est le personnel. Il est essentiel de garder à l'esprit que dans près de 70 % des cas, l'origine d'un sinistre est interne, ce qui illustre la nécessité d'une gestion rigoureuse du personnel : sélection, sensibilisation et formation, et sanctions.

Selon le CLUSIF, pour 58 % des entreprises en 2005, la fonction de RSSI n'est pas formellement définie. Autrement dit, il n'existe aucun personnel spécifique prévu dans les effectifs. Elle alors soit assurée par le personnel au sein du domaine informatique (administrateur réseau par exemple) dans 84 % de ces cas ou, pour le restant (16 %) par des responsables de haut niveau non spécialiste du domaine. Mais quand cette fonction existe, elle n'est exercée souvent qu'à temps partiel. Le plus souvent, le RSSI est seul (63 % des entreprises en 2005 contre 5 personnes dans 5 % des cas). La situation est donc loin d'être idéale.

Un autre aspect essentiel — même s'il est plus délicat à gérer — concerne la fiabilité du RSSI et des personnels impliqués dans la sécurité des SI. Il est essentiel de se rappeler que ces personnels (RSSI, administrateur) sont en quelque sorte les « gardiens des clefs ». Ils ont accès à toutes les ressources de l'entreprise. Une confiance totale doit pouvoir leur être accordée mais avec un certain contrôle. Il est assez surprenant de constater que dans beaucoup d'entreprises, aucun contrôle du RSSI n'est mis en place. Deux exemple réels mais démarqués permettent d'illustrer cela :

- En 2004, le responsable « audit » d'un très grand groupe français est lourdement impliqué dans un grave sinistre informatique. Ses actes ont été dictés par le manque d'argent dû à un train de vie dispendieux et sans proportion avec son salaire. L'enquête a montré que non seulement aucune recherche de base n'avait été entreprise concernant sa moralité et ses antécédents lors de son recrutement mais qu'aucun suivi ou surveillance n'avaient été mis en place, et ce malgré la très grande sensibilité de sa fonction. Ce cas n'est malheureusement pas isolé. Le poste de RSSI est un poste de grande confiance et à ce titre un certain nombre de précaution doivent être prises. Certes, dans notre société où la gestion de la sécurité empiète très vite — trop vite — sur les libertés de l'individu, s'assurer de la confiance d'un personnel n'est pas chose aisée. Des enquêtes de sécurité voire de moralité — le terme peut sembler outrancier mais ce concept est pris en compte dans certains secteurs d'activité — peuvent permettre de limiter les risques lors d'un recrutement.
- En 2005, une PME victime d'espionnage par codes malveillants a été incapable de fournir les mots de passe administrateurs de ses serveurs. Aucun de ses personnels ne les connaissait. Seule la société de service payée pour la maintenance du système informatique les connaissait. Grave dépendance qui se révéla fatale dans la gestion urgente de la crise et les possibilités d'enquêtes.

Ce point amène le problème de la sanction en cas de faute ou de lacune grave. Là encore, les possibilités sont fortement limitées par une société où la notion même de

sanction est considérée comme réactionnaire. Prenons le cas du monde militaire (tous pays confondus). L'avance en matière de sécurité des systèmes d'information, par rapport au monde civil, tient en grande partie aux sanctions réglementaires¹: le volet « répressif » est une partie intégrante d'une politique de sécurité cohérente. Dans le monde civil, une telle politique est difficile à mettre en œuvre si elle ne relève pas directement du pénal. Renvoyer un personnel coupable de graves manquements en matière de sécurité des SI est encore une sanction délicate à appliquer.

D'une manière générale, la gestion classique de chaque utilisateur passe par la signature d'une charte de sécurité, contenant les règles internes liée à la politique de sécurité, les interdictions.... En 2005, seule la moitié des entreprises utilisent ce genre de charte. Or une telle charte permet de fixer certaines règles par avance et d'avertir les employés, leur interdisant par la suite, de prétendre à l'ignorance de ces règles. Cette charte est souvent l'occasion de préciser les interdits en matière de SI. Ainsi, en 2005, en France, les interdictions les plus fréquentes concernent :

- L'accès à Internet à partir d'une poste non maîtrisé (76 % des entreprises).
- L'utilisation de la VoIP (73 % des entreprises) et du Wi-fi (43 % des entreprises).
- L'usage de PDA ou de smartphones (43 % des entreprises).
- L'accès au SI en situation de mobilité, comme la connexion de l'extérieur (20 % des entreprises).

Certes, signer cette charte ne signifie pas que les règles seront respectées. Comment en effet contrôler l'interdiction de connexion de PDA au SI interne ? Mais en cas de manquements, le dirigeant disposera d'une plus grande marge de manœuvre en termes de sanctions. Il est essentiel de faire de toute charte un outil de sensibilisation et de prévention. Sa rédaction doit être précise et rigoureuse en même temps que pédagogique. La sanction ne doit intervenir qu'en cas extrême.

Enfin, la gestion du personnel doit passer par une implication de tous les instants dans la (sur)vie de l'entreprise. Les salariés doivent être sensibilisés au fait que si le SI représente un facteur de risque, l'élément humain en est le point faible et le plus difficile à gérer. Le problème de l'ingénierie sociale évoquée dans le chapitre 2 n'est pas le seul aspect. La discrétion professionnelle en est un autre. Les attaquants, via les salariés, peuvent collecter « en milieu ouvert » (salons, restaurants, transports, cercle familial...) bien des informations relativement anodines qui compilées et croisées vont permettre d'attaquer le SI. Il importe donc de sensibiliser tout salarié à la notion fondamentale de discrétion professionnelle.

1. En France, le règlement de discipline des armées sanctionne tout non respect de règles en matière de sécurité informatique comme une faute professionnelle très grave (motif 502). Une sanction disciplinaire de 20 à 40 jours d'arrêt est applicable, indépendamment des éventuelles sanctions pénales et/ou civiles.



Il est navrant de constater que cette règle pourtant simple non seulement est rarement respectée mais surtout que son non respect est à l'origine de nombre d'attaques finales contre le SI de l'entreprise.

En résumé

La défense des réseaux d'une entreprise, et plus généralement de son système d'information, doit considérer plusieurs aspects. Ils ne sont pas uniquement techniques. Si disposer d'une architecture réseau sécurisée est indispensable, ce n'est pas suffisant. La défense doit également intégrer une gestion cohérente des utilisateurs (recrutement, formation, sensibilisation) et des ressources. Le plus difficile est sans aucun doute de concilier le besoin de sécurité de l'entreprise avec le « droit du salarié ». La simple consultation du courrier électronique ou des répertoires d'un salarié dans le SI de l'entreprise n'est pas aussi évidente et aisée qu'il peut sembler. L'interprétation d'un arrêté de la Cour de cassation (chambre sociale, du 2 octobre 2001 — arrêt Nikon) montre que les situations peuvent être délicates à gérer. En cas de mauvaise interprétation, elles peuvent conduire le dirigeant devant la justice¹. Le RSSI doit donc posséder sinon une forte culture en droit lié aux nouvelles technologies de l'information, du moins une bonne connaissance, actualisée, des textes réglementaires en la matière. Le dirigeant a tout intérêt à lui laisser du temps pour cet aspect capital de la sécurité du SI d'entreprise.

1. Lire à ce propos l'excellent article de Marie Barel, « (In)sécurité du système d'information : quelles responsabilités ? » Actes de la conférence SSTIC 2006, <http://www.sstic.org>



Creative Commons BY-NC-ND



La protection des données

La définition officielle d'un système d'information¹ — celle retenue par les services de l'Etat — est la suivante : « Tout moyen dont le fonctionnement fait appel à l'électricité et destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire de l'information ».

Dans cette définition, il apparaît qu'un système d'information est constitué de deux parties : la partie matérielle (le hardware) et la partie information, laquelle comprend les informations traitantes (le système d'application et les logiciels rassemblés sous le vocable de software) et l'information traitée. Si la protection du matériel est relativement aisée — un simple contrôle d'accès physique suffit dans la plupart des cas, celle des données, qu'elles soient traitantes ou traitées, est beaucoup plus délicate. Cela tient en partie au fait que l'information interagit avec d'autres informations, qu'elle est gérée par du matériel et, enfin que, mobile par nature, elle est communiquée à des tiers légitimes ou non (on est alors dans le cas d'une interception).

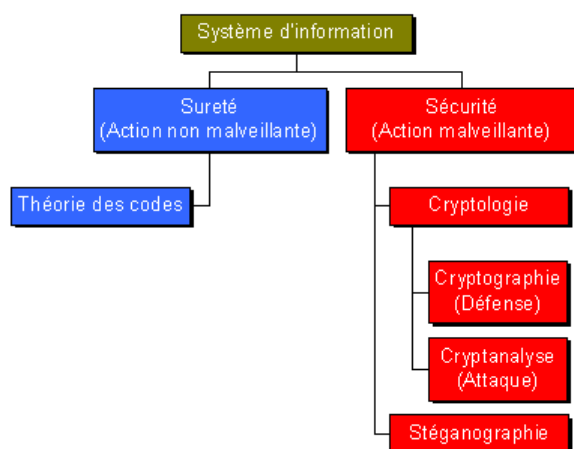
Comme il a été vu dans le chapitre 2, la sécurité de l'information repose sur trois piliers fondamentaux :

- la confidentialité : les informations ne doivent être accessibles qu'aux seules personnes autorisées ou habilitées.
- l'intégrité : les informations (un fichier système par exemple) ne doivent être modifiées que par une action légitime et volontaire.
- la disponibilité : le système doit répondre aux sollicitations des utilisateurs autorisés (accès aux informations, action particulière,...) dans le délai imparti par le cahier des charges, propre à chaque application et/ou système.

Mais à côté de la sécurité des informations, un autre aspect, souvent négligé, concerne la sûreté des informations.

1. La sécurité des systèmes d'information. Disponible sur http://www.esat.terre.defense.gouv.fr/formation/cursus/cpc/doc_sic/ssi.pdf

Protection d'un système d'information

**Figure 11-1** — Il y a une différence entre sûreté et sécurité.

La sûreté des informations concerne l'ensemble des techniques destinées à protéger ces informations contre les atteintes non malveillantes s'exerçant le plus généralement via le support de l'information (le hardware ou assimilé). En première approche, il s'agit de protéger le support contre les effets des lois de la Nature. Nous allons développer ce point dans la prochaine section. La sécurité quant à elle a pour objectif de gérer les attaques malveillantes, qui visent les informations elles-mêmes. La notion de malveillance impliquant un caractère d'adaptabilité de la menace à la protection, résumée dans l'image du duel bouclier contre épée.

Rappelons, avant d'entrer dans le détail, ce que l'on entend par donnée sensible. Il existe aux regards de la législation française — les autres pays ont des visions similaires — deux types de données :

- les informations relevant du secret de défense (confidentiel défense, secret défense, très secret défense, secret OTAN...) et dont la divulgation ou la compromission, volontaire ou non, est sanctionnée par le Code pénal de lourdes peines de prison et d'amendes. Elles concernent tous les ministères et industriels impliqués d'une manière ou une autre dans les moyens et la politique de défense de notre pays. La protection de ces données est obligatoire et fait l'objet de textes de lois spécifiques ;
- les informations dites sensibles mais ne relevant pas du secret de défense : confidentiel médical, confidentiel personnel, confidentiel industrie (hors défense), confidentiel transport... Elles relèvent généralement du secret ou de la discrétion professionnels. La protection de ces données est conseillée.

11.1 LA SÛRETÉ DE L'INFORMATION

La notion d'atteinte non malveillante désigne essentiellement les perturbations que les lois de la Nature (panne d'un appareil, rayures sur un CDRom, bruit de fond lors d'une transmission aérienne...). La caractéristique de ces perturbations est que son comportement statistique est parfaitement connu et modélisé. Or, dans une situation de protection, lorsque l'on est en situation de pouvoir prédire l'évolution des « atteintes », la situation est confortable. Il est donc possible, de manière efficace et définitive, de définir des protocoles de gestion de ces atteintes et ainsi d'annuler leur effet. L'expression de « non malveillant » signifie également que ces atteintes — autrement dit la Nature — ne vont pas adapter leur comportement (statistique) en fonction des protections mises en place. C'est pourquoi on parle alors de sûreté (de fonctionnement, de l'information...) et non pas de sécurité.

La sûreté des informations est assurée principalement par les codes détecteurs et correcteurs d'erreurs. La théorie des codes, dont le père fondateur est Claude Elwood Shannon, date des années 1948-49. Elle a rendu possible la conquête de l'espace profond (programmes Mariner, Voyager...). En effet, si l'on savait à l'époque faire des fusées et des satellites, à quoi auraient-ils servi si les images de Pluton ou de Jupiter qu'ils auraient envoyées avaient été si bruitées que leur exploitation eut été impossible ?

Nous ne rentrerons pas dans le détail de la théorie des codes. Cependant, pour que le lecteur comprenne bien le mécanisme, présentons une variété très simple mais néanmoins très puissante de tels codes : les codes à répétition.

Alice veut envoyer par un canal de transmission le message binaire suivant : 1011. Elle choisit alors un code dit 3-répétition. Il consiste à répéter trois fois le symbole binaire émis. Alice envoie (après « codage ») : 111 000 111 111. Supposons que le canal ait produit un bruit qui a perturbé la transmission. Bob reçoit 101 100 111 101. Il y a eu trois erreurs, lesquelles peuvent rendre un message totalement incompréhensible (imaginez par exemple un fichier compressé, mais heureusement là aussi, il y a de la correction automatique d'erreurs). Il applique alors le « décodage » suivant : pour chaque groupe de trois bits consécutifs, il décide que celui qui est le plus fréquent est celui qui a été envoyé (on appelle cela un décodage par maximum de vraisemblance). Bob décode de la manière suivante : 1011.

Le message est sans erreur.

Si on considère un canal plus bruité, ce code ne fonctionne plus. Il restera des erreurs après le décodage. Il suffit alors de considérer un code à 5 ou 7 répétitions ou d'autres types de codes. Il est donc toujours possible de corriger le bruit lors d'une transmission ou de toute manipulation de l'information. Les codes correcteurs nous entourent : téléphones mobiles (pas moins de trois codes), nos CD, nos mémoires d'ordinateurs, nos logiciels (compression de données par exemple), formats d'images... Bref sans les codes correcteurs, nous ne pourrions plus vivre.

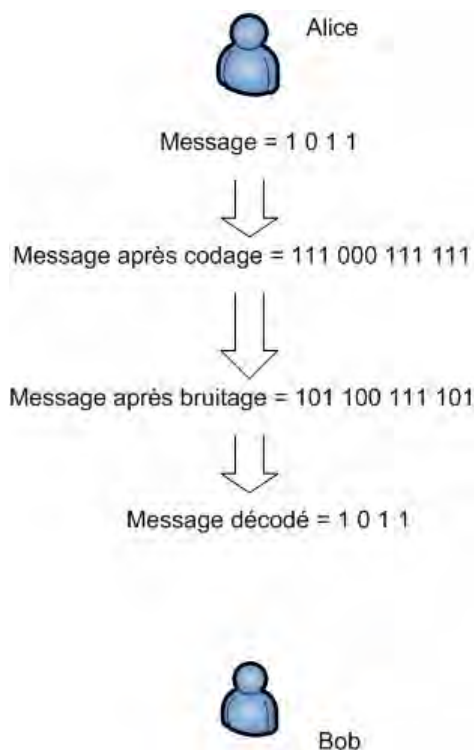


Figure 11-2 — Ce déroulé récapitule toute la chaîne de transmission.

11.2 LA CONFIDENTIALITÉ DES INFORMATIONS : LE CHIFFREMENT

La confidentialité concerne la capacité de gestion d'accès aux données aux seules personnes autorisées. Fonctionnalité historique, elle est assurée par le chiffrement. D'une manière générale, le chiffrement consiste à transformer une donnée dite claire — c'est-à-dire accessible à quiconque — en une donnée incompréhensible, d'apparence la plus aléatoire possible, pour tout tiers non autorisé. Cette transformation se fait en fonction d'un procédé (appelé algorithme) et surtout d'une quantité secrète, appelée clef. Notons qu'un système dépourvu de clef n'est pas un système cryptologique. Il existe deux grandes familles de procédés de chiffrement :

- les procédés de chiffrement par transposition. Le principe consiste à mélanger, en fonction d'une clef, l'ordre des lettres. Ainsi, considérons le système de transposition dite à tableau et la clef formée du mot « Austerlitz ». On écrit alors le texte sous le mot clef, en colonne, comme suit (les lettres apparaissant plusieurs fois dans le mot clef sont supprimées) :



A U S T E R L I Z
 N O U S A T T A Q
 U O N S D E M A I
 A L A U B E

le texte est alors relevé par colonne dans l'ordre alphabétique des lettres du mot clef (ou tout autre ordre choisi préalablement). Cela donne le texte chiffré suivant :

N U A A D B A A T M T E E U N A S S U O O L Q I

Le déchiffrement consiste à faire l'opération inverse et n'est possible que si l'on connaît le mot clef. Le principal inconvénient des systèmes par transposition est qu'ils conservent les statistiques de la langue et fournissent par conséquent une information sur le message. Ils ne sont plus employés de nos jours.

- les procédés dits par substitution. Chaque lettre ou groupe de lettres est remplacée en fonction d'une clef secrète et d'un procédé par une autre lettre ou groupe de lettres. Considérons le mot clef « REPLUBLIQUE ». Et fabriquons l'alphabet suivant à partir de ce mot clef

R E P U B L I Q A C D F G H J K M N O S T V W X Y Z

Toute lettre présente plusieurs fois dans le mot-clef est supprimée puis les lettres non présentes dans le mot-clef sont ensuite rajoutés et ce dans l'ordre alphabétique (ou tout ordre choisi). Il suffit ensuite d'écrire l'alphabet normal en dessous de cet alphabet désordonné pour avoir la correspondance lettre claire et lettre chiffrée :

R E P U B L I Q A C D F G H J K M N O S T V W X Y Z
 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Le mot « attaque » est ainsi chiffré en « RSSRHDB ». Bien sûr ce système basique n'offre aucune sécurité. En revanche le procédé de substitution est celui qui est repris par tous les systèmes modernes de chiffrement.

Les deux systèmes précédents utilisent le même procédé et surtout la même clef, laquelle doit donc être distribuée entre les deux acteurs, Alice (l'émetteur) et Bob (le destinataire). Ces systèmes sont appelés « systèmes symétriques » ou encore « systèmes à clef secrète ». La clef, sur le secret de laquelle repose toute la sécurité, se mesure en bits. Les clefs actuelles ont une taille allant de 128 à 256 bits. Mais la contrainte de devoir distribuer les clefs avant la communication — outre les risques de compromission — font que ces systèmes sont réservés à des usages gouvernementaux et militaires. En effet, cela réclame des infrastructures et une organisation que seuls les services de l'Etat peuvent gérer efficacement et avec le niveau de sécurité voulu. Parmi ces algorithmes, les plus connus sont le DES (56 bits de clefs), l'AES (128, 192 et 256 bits), l'IDEA (128 bits), le GOST (256 bits), le Blowfish (256 bits)...



C'est pour évacuer ces contraintes, qu'en 1977, deux chercheurs Diffie et Hellman ont inventé un autre type de cryptographie¹ : la cryptographie à clef publique. Avec ces nouveaux systèmes, chaque utilisateur crée un couple de clef, l'une publique, qui comme son nom l'indique est destinée à être publiée, l'autre privée qui doit impérativement rester secrète. Donc, un système à clef publique est bien un procédé cryptologique puisqu'il existe une quantité sur le secret de laquelle repose toute la sécurité du système. Bien sûr, la clef publique est fabriquée à partir de la clef privée mais il est calculatoirement impossible de retrouver cette dernière à partir de la clef publique². Si le chiffrement avec des systèmes symétriques se conçoit aisément, comment cela fonctionne-t-il avec un système à clef publique.

Alice veut envoyer un message chiffré à Bob. Pour cela, elle va rechercher dans un annuaire (ou Bob lui aura envoyé via un canal quelconque) la clef publique de Bob. On peut comparer le fait de chiffrer avec un système à clef publique à l'envoi d'une lettre. Pour que ce dernier soit possible, il faut connaître l'adresse de Bob, équivalente à la clef publique³. On la trouve dans un annuaire. Le facteur dépose la lettre envoyée par Alice dans la boîte à lettre de Bob. Comme sa boîte aux lettres ferme à clef, par conséquent seul Bob peut accéder au message chiffré envoyé par Alice. La clef de cette boîte est comparable à la clef privée de Bob. Et l'on voit bien que la connaissance de l'adresse de Bob, ne donne pas pour autant les moyens de forcer sa boîte aux lettres (du moins en mathématique).

Si la cryptologie à clef publique présente d'indéniables avantages, elle comporte également des inconvénients qui limitent son emploi :

- elle met en œuvre des calculs lourds et complexes. De fait, il n'est pas possible de chiffrer, sinon en un temps assez long, de gros volumes de données ;
- elle repose sur des principes qui ne sont pas mathématiquement démontrés. Pour le moment, l'incapacité calculatoire à retrouver la clef privée à partir de la clef publique est seulement une conjecture, étayée par l'expérience seule. Mais personne ne peut sérieusement affirmer qu'il n'est pas calculatoirement⁴ facile de le faire, ni que quelqu'un ne soit pas parvenu à le faire et ait choisi de n'en rien dire. C'est la raison pour laquelle, le chiffrement à clef publique est limité

1. Il est intéressant de noter qu'il a récemment été révélé que les services anglais avaient découvert ce type de cryptographie mais n'avaient pas rendu publics leurs résultats. Comme souvent en cryptologie...
2. Cette impossibilité calculatoire n'a jamais été démontrée ce qui fait peser une incertitude sur la solidité réelle de ces systèmes. Mais cette incertitude, en l'état actuel des recherches publiées est conciliable avec les besoins de sécurité.
3. Dans un système symétrique, en comparaison, Alice et Bob habiteraient à des adresses secrètes, devraient échanger préalablement leurs adresses respectives... et déménager après chaque communication.
4. Le terme *calculatoirement* signifie qu'il n'existe aucune méthode permettant en pratique de trouver un tel fichier F, même si l'on dispose d'une puissance de calcul importante. Une solution possible serait de tester tous les fichiers possibles F. C'est infaisable en pratique. Ce terme indique donc que les solutions qui permettent de résoudre le problème théoriquement sont inatteignables en pratique



au chiffrement de petites quantités d'information et pour des trafics d'une sensibilité peu élevée¹.

Les solutions commerciales actuelles — dont la plus connue est sans conteste le logiciel PGP² — consiste à mélanger cryptologie à clef secrète et systèmes à clef publique : ce sont les systèmes cryptologiques hybrides. Le principe est le suivant :

Alice génère une clef aléatoire de session K de 128 bits. Cette clef de session lui sert à chiffrer les données M à l'aide d'un algorithme symétrique (de nos jours, l'AES). Ces systèmes sont très rapides pour les opérations de chiffrement. Elle produit donc $C = \text{AES}_K(M)$, le texte chiffré.

Bob ne possède par la clef K mais Alice ne peut pas lui envoyer en clair via un canal de transmission qui n'est pas sûr (sinon elle ne chiffrerait pas ses données). Alice chiffre donc la clef avec un système à clef publique S . Pour cela, elle utilise la clef publique de Bob, PUB_{BOB} et produit $S(K, \text{PUB}_{\text{BOB}})$.

Alice envoie à Bob les quantités C (le cryptogramme) et $S(K, \text{PUB}_{\text{BOB}})$, la clef de session chiffrée. Lorsque Bob reçoit ces deux données, il déchiffre $S(K, \text{PUB}_{\text{BOB}})$ avec sa clef privée et récupère K . Il peut ensuite déchiffrer C à l'aide de K . Bien évi-

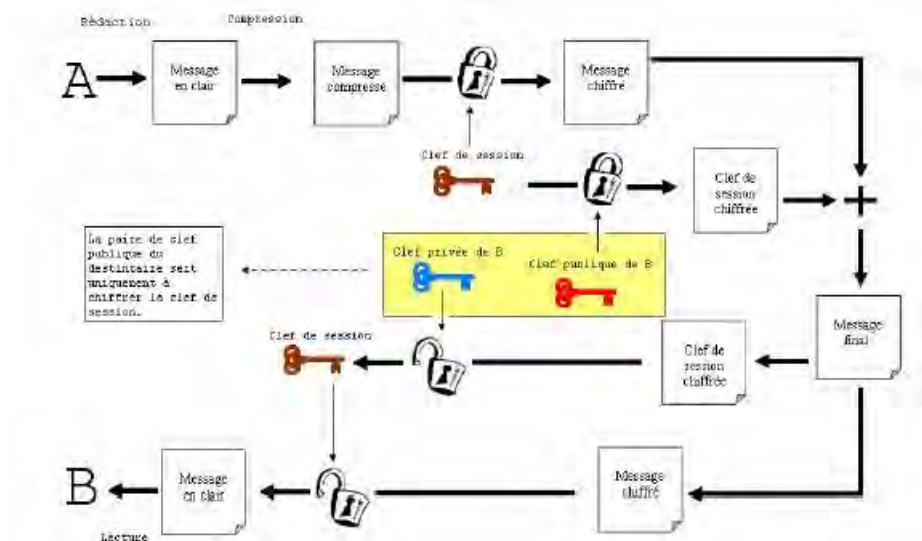


Figure 11-3 — Le schéma³ résume les opérations de chiffrement et de déchiffrement.

1. En tout cas, il devrait être d'un usage limité mais la recherche de toujours plus d'ergonomie et de facilité d'exploitation fait que ces systèmes sont utilisés là où ils ne devraient pas l'être !
2. Pretty Good Privacy, <http://www.pgp.com>
3. Source : Bourgeois Morgan, Initiation à PGP : GnuPG, <http://mbourgeois.developpez.com>

demment, si on parvient à retrouver (par compromission, par cryptanalyse) la clef privée de Bob, alors toute la sécurité s'écroule. Ce problème est également celui de la cryptologie à clef secrète, mais dans une mesure moindre. Existe-t-il des moyens infaillibles de protéger l'information ?

Pour répondre à cette question, il faut auparavant préciser quel est le problème fondamental de la cryptologie. Il réside dans l'opposition de vues entre celui qui conçoit les systèmes (le cryptographe) et celui qui tente de les briser (le cryptanalyste). Ce dernier, s'il est capable de casser un système, peut toujours le prouver. Il lui suffit de lancer un challenge et de décrypter un message chiffré proposé à titre de défi. Mais son intérêt n'est pas forcément de publier cette capacité. Il pourrait ainsi lire toutes les correspondances chiffrées de toute personne qui ne doute pas que son système de chiffrement a été cassé. C'est là le travail des services spécialisés de chaque pays qui développe des compétences secrètes dans le domaine de la cryptanalyse.

En revanche, le cryptographe — dans la cryptologie classique, qu'elle soit symétrique ou à clef publique — ne pourra jamais prouver que son système est incassable, excepté pour les systèmes très particuliers, d'usage exclusivement militaire ou gouvernementaux appelés systèmes à secret parfait¹. Il ne sait pas, par exemple, ce que sont capables de faire les cryptanalystes du monde entier. Son système aura été conçu en fonction des connaissances de cryptanalyses publiées, qui ne représentent qu'une faible partie de toutes les techniques d'attaques connues.

C'est la raison pour laquelle les recherches, depuis quelques années, se tournent vers la *cryptographie quantique* qui permet de concevoir des systèmes à secret parfait. Chaque bit transmis est sous forme d'un photon polarisé. En 1992, le protocole dit de Brassard/Bennet permet de s'assurer de la confidentialité de clefs distribuées via des fibres optiques. Ce protocole permet de nos jours de réaliser ce que l'on connaît sous le nom de *distribution quantique de clef* (QKD). C'est aujourd'hui la seule manière connue de distribuer des clefs avec une sécurité inconditionnelle, c'est-à-dire dans des conditions de secret parfait. La sécurité quantique résulte en premier lieu de l'impossibilité de dupliquer les signaux reçus, principe de non-clonage, ou d'en distraire une partie significative sans signer son intervention par une modification importante du taux d'erreur des signaux reçus. Actuellement le procédé QKD en est à ses balbutiements : les taux de transmissions sont encore trop faibles (quelques Kbits par seconde) pour un usage sur des réseaux réels, il subsiste encore beaucoup de problèmes techniques pour en faire une technologie fiable et surtout le prix des quelques solutions reste exorbitant (environ 200 000 euros pour un boîtier et il en faut au minimum deux).

1. Un système à secret parfait est un système pour lequel il est impossible de déterminer quelle clef et donc quel message, ont été utilisés, même si l'on dispose d'une puissance de calcul infinie et de l'éternité pour les rechercher. Ces systèmes imposent de telles contraintes organisationnelles qu'ils sont réservés aux communications les plus sensibles. Pour tous les autres systèmes, il suffit d'essayer toutes les clefs possibles pour trouver la bonne... ce qui néanmoins requerrait plusieurs milliards de siècles pour une simple clef de 128 bits.



11.3 L'INTÉGRITÉ DES INFORMATIONS

L'intégrité, si elle est moins connue du grand public, est tout aussi importante que la confidentialité. Imaginons une transaction bancaire dont un pirate pourrait modifier de manière indétectable, les données. Par exemple, remplacer le numéro de compte bénéficiaire par celui de l'attaquant, ou modifier les sommes engagées dans la transaction. Un autre exemple tout aussi pertinent est celui des programmes que l'on télécharge sur Internet. Imaginons qu'un pirate tente de s'introduire dans des milliers d'ordinateurs. Il lui suffirait d'insérer les fonctionnalités adéquates dans un ou plusieurs logiciels très utilisés (un navigateur Internet par exemple) et de l'offrir au téléchargement comme la version d'origine. Toute personne installant cette version corrompue sera victime du pirate. Or, nous téléchargeons régulièrement des logiciels que nous installons sans aucune vérification spéciale et volontaire de notre part. Qui, en effet, vérifie l'empreinte MD5 accompagnant beaucoup de logiciels que nous utilisons ?

Ces quelques exemples montrent que l'intégrité des informations que nous manipulons est essentielle. Il est indispensable, dans de très nombreux cas, de vérifier qu'il n'y a pas eu de modifications dans des données critiques. Heureusement, la plupart des logiciels du commerce intègrent des fonctionnalités d'auto-calcul d'intégrité qui vérifient à chaque installation qu'il s'agit de la version officielle et que cette dernière n'a pas été corrompue. Cette vérification est systématiquement faite. Elle l'est également lorsque votre logiciel antivirus met à jour ses bases de signatures. Imaginez que lors du téléchargement le pirate parvienne à manipuler ces bases et à y introduire des informations destinées à modifier comportement du logiciel antivirus. Pire, que se passerait-il s'il parvenait à dérouter les requêtes de mise à jour vers un site pirate ne contenant que des bases de signatures corrompues ?

Comment fonctionnent les outils d'intégrité ? L'intégrité est assurée par ce que l'on appelle des *fonctions de hachage*. Les plus connues sont MD5, SHA-1 et RIMPEMD-160. Le principe est simple. Un fichier F, de longueur quelconque (un simple e-mail, un disque dur entier, un document...) est haché par l'intermédiaire d'une fonction dite de « hachage » H. En pratique, on calcule la valeur H(F). Le terme hachage signifie, entre autres choses, que la valeur H(F), appelée *empreinte numérique*, est beaucoup plus petite que le fichier F. Elle a une taille fixe, qui de nos jours vaut 160 bits. Le calcul de H(F) est très facile. Un programme sera capable en quelques secondes de calculer l'empreinte d'un gros disque dur. De plus, il est calculatoirement impossible, pour une empreinte donnée E de trouver un fichier F produisant cette empreinte par hachage, autrement dit de trouver F tel que $H(F) = E$. Les fonctions de hachage semblent donc très intéressantes. En pratique, on calcule l'empreinte E de la donnée à protéger. On la stocke dans un endroit protégé (elle peut être chiffrée par exemple). Chaque fois que l'on veut vérifier si l'intégrité de la donnée est intacte, on recalcule E et on le compare à la valeur de référence.

Seulement voilà. Il existe des milliards de fichiers qui possèdent la même empreinte numérique. Qu'est ce qui empêche un pirate de modifier un fichier légitime F en un fichier corrompu F', de telle sorte qu'ils aient tous deux la même



empreinte numérique $E = H(F) = H(F')$. On appelle cela une *collision*. Heureusement, pour les fonctions de hachage utilisées, SHA-1, SHA-2 et RIMPEMD-160, trouver de telles collisions est également calculatoirement impossible¹. Un attaquant ne peut donc pas manipuler vos données critiques de sorte à contourner le contrôle d'intégrité. Sauf si la valeur de hachage elle-même n'est pas protégée, par chiffrement par exemple. Si $E = H(F)$ est accessible au pirate, il peut remplacer le fichier F par un fichier F' , corrompu tel que $H(F') = E$. Il lui suffira alors de remplacer E par E' . Ni vu ni connu. C'est la raison pour laquelle les empreintes numériques sont chiffrées afin d'interdire de telles manipulations.

Il existe de nombreux produits permettant de protéger l'intégrité des données. Le plus célèbre est sans conteste le logiciel Tripwire². Il permet non seulement une protection au niveau des fichiers mais également du système de fichier lui-même, ce qui est particulièrement intéressant en cas d'attaque virale.

Pour illustrer la nécessité d'un contrôle d'intégrité, il est intéressant de parler de la tentative de corruption du code source du noyau Linux³, pour y introduire une porte cachée (« backdoor »).

Le code original (extrait) était le suivant :

```
if((options == (__WCLONE|__WALL)) && (current->uid == 0))  
    retval = -EINVAL ;  
Ce code a été modifié comme suit :  
if((options == (__WCLONE|__WALL)) && (current->uid == 0))  
    retval = -EINVAL ;
```

La modification (le simple changement d'un signe « = » en signe « = »), pourtant infime aurait eu des conséquences dramatiques puisque elle permettait de gagner des droits administrateur sur le système. Heureusement, la mise en œuvre de mécanismes d'intégrité internes a permis de détecter immédiatement la tentative de corruption. De plus, ce code source critique existe sur plusieurs serveurs, chaque serveur vérifiant en permanence l'intégrité des autres.

11.4 LA DISPONIBILITÉ DES INFORMATIONS

La disponibilité des informations est certainement la fonctionnalité la moins bien connue, bien qu'elle soit très importante. Imaginons une entreprise qui ne puisse plus accéder à ses données pendant 24 ou 48 heures voire pendant plusieurs jours. Un tel scénario serait catastrophique. Le plus souvent la prévention contre l'indisponibilité des erreurs n'est mise en place qu'à la suite d'un sinistre concernant les

1. En 2004, des chercheurs chinois sont parvenus à produire des collisions pour la fonction MD5 dont la sécurité doit dorénavant être mise en doute.
2. <http://www.tripwire.com>
3. Kevin Poulsen, "Linux kernel backdoor blocked". 7/11/2003, http://www.theregister.co.uk/2003/11/07/linux_kernel_backdoor_blocked/



données. Le cas le plus fréquent est celui de la panne d'un disque dur, lequel contenait des données plus ou moins bien sauvegardées... voire non sauvegardées.

Actuellement, assurer la disponibilité des données ne se fait efficacement que dans un contexte de sûreté uniquement. Des techniques de type RAID (*Redundant Array of Inexpensive Disks*) sont très efficaces mais d'une part elles sont assez onéreuses et d'autre part, elles requièrent quelques compétences, notamment dans le domaine de gros systèmes d'entreprises.

Un système de type RAID répartit et organise les données sur plusieurs disques durs et utilise des techniques de correction d'erreurs. Nous sommes donc bien dans un contexte de sûreté. Le système d'exploitation voit la matrice du raid (ensemble de plusieurs disques) comme un disque unique. Il existe six types de RAID, du RAID 1 au RAID 6. Cette classification est fondée sur la façon de diviser et de répartir les données et sur les codes correcteurs d'erreurs utilisées. Les principaux avantages du système RAID sont :

- d'augmenter la capacité de stockage en mettant bout à bout des disques durs pour accroître la taille du volume.
- d'apporter la tolérance de panne et donc d'assurer la disponibilité des informations : certaines configurations RAID permettent de prévenir les défaillances d'un disque.
- d'améliorer les performances : les données sont écrites sur plusieurs disques à la fois. Ainsi, chacun des disques n'a qu'une partie des données à inscrire.

Les différents types de RAID¹ sont définis par la nature des codes correcteurs utilisés et la manière dont ils sont mis en œuvre.

Les systèmes RAID, aussi efficaces soient-ils dans un contexte de sûreté, sont totalement inopérants dans un contexte de sécurité, autrement dit en cas d'attaque contre les données, à moins d'adjoindre des mesures de sécurité informatique classique (technique et organisationnelle). Une attaque par un code malveillant comme le TrojanPGPCoder ne sera pas gênée par la présence d'un système RAID. Ce code qui a frappé en mai 2005, chiffre tous les fichiers ayant une extension du type ASC, DB, DB1, DB2, DOC, HTM, HTML, JPG, PGP, RAR, RTE, TXT, ZIP et XLS. Ainsi même les fichiers chiffrés avec PGP devenaient indisponibles. Le ver laisse ensuite des instructions dans un fichier pour permettre la récupération de la clef (moyennant finances ; il s'agit donc d'extorsion de fonds). Le fichier, dénommé ATTENTION !!!.TXT est le suivant (traduction de l'anglais) :

1. Le lecteur pourra consulter Jean-Louis Locoche, Le principe de la technologie RAID, ADNAVIGO, IRS, <http://www.locoche.net/pdf/raid.pdf> pour une description complète des différents types de RAID. Le niveau RAID 6 a été ajouté aux niveaux définis. Il définit l'utilisation de deux fonctions de codage d'erreur, et donc le stockage sur deux disques dédiés. Ce niveau permet ainsi d'assurer la redondance en cas d'avarie simultanée de deux disques. Cela signifie qu'il faut au moins 4 disques pour mettre en œuvre un système RAID-6.



« Certains fichiers sont chiffrés. Pour acheter le déchiffreur, envoyez un e-mail à l'adresse suivante : n781567@yahoo.com avec l'objet suivant : PGPcoder 000000000032 »

Les données sont donc indisponibles tant que le propriétaire des données n'a pas récupéré l'outil de déchiffrement. La seule parade possible est donc une véritable politique de sauvegarde des données, en amont.

11.5 LA PROTECTION DU CANAL DE TRANSMISSION

La protection des données en elle-même ne suffit pas. Il est possible d'obtenir de l'information malgré l'utilisation de chiffrement. C'est pendant le premier conflit mondial que le problème a été réellement identifié. A l'époque, comme dans tout conflit, les communications sont chiffrées. Mais très vite, les spécialistes militaires du renseignement se sont aperçus qu'il était possible de « faire parler » un trafic chiffré. Si vous interceptez quelques messages chiffrés par jour, le plus souvent à heure relativement fixe, vous en concluez qu'il s'agit d'un échange de données de routine, ce que la taille du message peut également corroborer. Mais si le trafic vient graduellement à augmenter, passant de quelques messages à quelques dizaines, même le chiffrement ne peut cacher le fait qu'une opération se prépare. Des techniques d'analyse de trafic et localisation par radiogoniométrie permettent même d'identifier émetteurs et destinataires (quand ils répondent).

En résumé, malgré le chiffrement, l'adversaire parvient à collecter une quantité relativement importante d'informations sensibles. Pourquoi ? La raison tient au fait que le chiffrement ne protège que les informations elles-mêmes. On parle alors d'aspect COMSEC (Communication Security). En revanche, l'existence d'une communication — autrement dit l'existence d'un canal de transmission — n'est pas dissimulée. L'aspect dit TRANSEC (Transmission Security) n'est pas assuré.

Parmi de nombreuses techniques possibles, la plus connues est ce que l'on appelle la *séganographie* (du grec *stegein* « couvrir » et *graphos* « écriture »). Cet ensemble de techniques assure à la fois les aspects COMSEC et TRANSEC. L'idée est de cacher la communication ET le canal de transmission. L'adversaire ne se doute donc même pas de l'existence d'un échange d'informations. Des techniques comme les encres dites invisibles sont des procédés de stéganographie très anciens.

Un autre exemple retenu par l'histoire est la fameuse lettre de Georges Sand et de la stéganographie dite linguistique¹. Voulant obtenir les faveurs d'Alfred de Musset, bel esprit qui n'entendait pas succomber de manière triviale, Georges Sand lui envoya la lettre suivante :

1. Des auteurs connus comme Boccace, Corneille ou Arthur Rimbaud ont caché dans leur œuvre littéraire des messages cachés.



Je suis très émue de vous dire que j'ai
bien compris, l'autre jour, que vous avez
toujours une envie folle de me faire
danser. Je garde un souvenir de votre
baiser et je voudrais que ce soit
là une preuve que je puisse être aimée
par vous. Je suis prête à vous montrer mon
affection toute désintéressée et sans cal-
cul. Si vous voulez me voir ainsi
dévoiler, sans aucun artifice, mon âme
toute nue, daignez donc me faire une visite.
Et nous causerons en amis et en chemin.
Je vous prouverai que je suis la femme
sincère, capable de vous offrir l'affection
la plus profonde et la plus étroite
amitié, en un mot, la meilleure amie
que vous puissiez rêver. Puisque votre
âme est libre, alors que l'abandon où je
vis est bien long, bien dur, et bien souvent
pénible, ami très cher, j'ai le cœur
gros, accourez vite et venez me le
faire oublier. A l'amour, je veux me sou-
mettre.

Cette lettre en tant que telle n'est qu'une lettre classique rédigée dans le style romantique de l'époque. En revanche, celui qui connaît le procédé, lira une ligne sur deux, accédant à un texte d'une autre nature.

La stéganographie consiste donc à prendre un support anodin — dont l'échange entre deux personnes ne déclenche pas de soupçon — et à dissimuler une information qui, elle est secrète. De nos jours, il existe des systèmes très complexes, matériels ou logiciels, permettant, avec des supports numériques de faire très efficacement de la stéganographie. Des images, des vidéos, des fichiers MP3, des programmes exécutable constituent d'excellents supports — appelés stégano-media — dans lesquels cacher un message secret.. Il existe de nos jours des suites logiciels permettant selon le même principe de cacher des partitions de disques durs entièrement.



Le logiciel le plus célèbre est probablement le logiciel Outguess qui est capable de dissimuler des informations dans des images JPEG. Ce qui est plus intéressant tient au fait que le stégano-medium peut être d'une taille inférieure après la

dissimulation de l'information, ceci grâce à des caractéristiques liées au format JPEG.



Figure 11-4 — L'image de droite (le champ de bombardiers) est cachée dans l'image de gauche, grâce au logiciel Outguess.

Le principe général de ces techniques est assez simple. La dissimulation d'un message secret dans un stégano-medium se fait toujours en deux étapes :

- Identification de données redondantes dans le stégano-medium. Quel que soit ce dernier, il y a toujours des données concernant une information excédentaire. Pour une encre invisible, ce sont les zones du papier qui ne sont pas utilisées. Dans une image, les couleurs sont stockées sur 24 ou 32 bits, soit potentiellement 16 millions ou 4 milliards de couleurs différentes. Mais qui est capable de discerner autant de couleurs ? Personne. Les formats graphiques codent donc beaucoup plus d'information que notre œil est capable d'en identifier. Pour un fichier MP3, c'est la même chose. Notre oreille discerne des sons dans une gamme de fréquences plus limitée que celle possible pour la plupart des formats sonores.
- La seconde étape consiste alors à choisir au hasard un sous-ensemble de ces données redondantes et à y insérer le message. Comme les données éventuellement¹ modifiées sont redondantes — c'est-à-dire non essentielles à la perception —, le support une fois le message secret dissimulé semblera identique à la perception. Bien sûr, au niveau de la statistique des informations redondantes, certains changements et modifications sont intervenus mais un bon système sera capable de les rendre quasi-indétectables.

1. Eventuellement, car si je souhaite cacher la valeur 1 dans un bit redondant dans l'image qui est déjà à 1, je dissimule cette valeur 1 sans modifier ce bit.

La stéganographie, de nos jours, si elle représente une technique intéressante de protection d'un canal de transmission, pose d'insolubles problèmes aux spécialistes lorsqu'elle est utilisée par des terroristes ou des criminels. Ainsi, la préparation des attentats du 11 septembre a-t-elle été, semble-t-il, préparée via des informations dissimulées dans des images pornographiques¹. Criminels et autres malfrats commencent à découvrir tout le potentiel de la stéganographie. Or, dans un cadre judiciaire, dissimuler le canal de transmission, c'est équivalent à empêcher de constater un crime ou un délit.

Si des outils existent, permettant dans certains cas de détecter des informations stéganographiées, ces outils deviennent très vite dépassés par la masse de support qu'il faudrait traiter par jour. Même un réseau comme Echelon, ne peut analyser — sinon en plusieurs mois — les millions d'images échangées ou présentes chaque jour via le seul réseau Internet.

11.6 LE CHIFFREMENT DES DONNÉES DANS LA PRATIQUE

Bien que les technologies existent et pour un coût minime, il existe beaucoup de données confidentielles non protégées. En juin 2006, plus de 75 millions de sites sont recensés sur la planète Internet (source : www.netcraft.com) avec une progression soutenue de 15 millions de nouveaux sites par an². Ainsi, les évaluations estiment à plusieurs méga-octets (ou peut être giga-octets) les données ayant un caractère confidentiel qui sont présentes sur ces sites Internet.

Selon une analyste du cabinet Gartner, citée par ITNews, un vol massif de données revient à 90 dollars par employé touché. Un coût qui peut vite devenir un gouffre pour des entreprises comptant des milliers d'employés. Or. Une protection des données revient moins cher. Le simple fait de protéger des données dudit client par chiffrement - et donc écarter pratiquement tout risque de divulgation après intrusion -, demanderait un investissement de 6 dollars par compte ! Une formule associant moyen de chiffrement, HIDS et audit ne dépasserait pas les 16 dollars ! On peut ne rien faire du tout et fonder une politique sur la discrétion ce qui ne coute rien. C'est la solution adoptée par l'armée américaine qui pensait réaliser une économie de 425 millions de dollars. L'affaire du fichier disparu³ des 26,5 millions d'anciens combattants de l'armée US a prouvé le contraire, comme les vols d'un portable de l'armée française en Côte d'Ivoire en 2005 ou des disques durs contenant des données Secret Défense de l'armée américaine en Afghanistan en 2006. Les journaux américains ont

1. <http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm>. L'usage d'images pornographiques est en soi une forme de stéganographie (qui soupçonnerait des intégristes musulmans de passer par ce type d'images).
2. La Sécurisation des bases de données pour éviter de divulguer les informations privées sur Internet, juin 2006.
3. Source Magazine CSO, du 07/06/2006.



récemment fait état de la compromission de ce fichier, après une intrusion sur leurs réseaux. Avant intrusion, on appelle ça de la « gestion de risque ». Après intrusion, une « déplorable éventualité statistiquement improbable ». D'un point de vue froidement actuariel, en données brutes, la « perte » théorique de 90 dollars par compte multipliée par les 26,5 millions de victimes potentielles fait monter les préjudices à 2,4 milliards de dollars. Ce chiffre est tellement astronomique, que tout gestionnaire préférera mettre en doute la méthode d'estimation et d'analyse... Donc, en attendant, « on » ne chiffre pas. Pas plus aux Etats-Unis qu'en France, d'ailleurs.

Et pourtant, les solutions commerciales efficaces — pour des données sensibles uniquement — et bon marché existent. Les moyens de chiffrement sont désormais libres depuis la récente loi sur l'économie numérique de juin 2004. Mais il convient d'être prudent. Les logiciels de chiffrement sont très nombreux, mais il convient de se méfier. Beaucoup utilisent des algorithmes élémentaires. D'autres mettent en œuvre des algorithmes réputés comme solides, mais les implémentent d'une manière si catastrophique qu'ils dégradent la sécurité finale des algorithmes. D'autres ne publient pas les algorithmes qu'ils utilisent, ce qui ne permet pas de savoir s'ils ne contiennent pas une « porte dérobée » par laquelle il serait facile d'entrer ou des faiblesses permettant un décryptement plus facile (lire également le chapitre 15). Pour une protection réellement efficace, s'agissant de données sensibles uniquement, mieux vaut se tourner vers des solutions utilisant les algorithmes de chiffrement comme GOST, IDEA, RC5, Blowfish ou l'AES, et qui sont réputés de qualité.

Au lieu de chiffrer fichier par fichier — ce qui n'est guère pratique mais néanmoins possible pour un chiffrement limité — beaucoup de produits créent des disques logiques dans lesquels les données sont transférées comme sur une partition standard. Le chiffrement/déchiffrement s'effectue à la volée de manière transparente et sans délai notable. En début de session, un mot de passe est requis pour ouvrir le disque. Certains d'entre eux proposent également des fonctionnalités de stéganographie, permettant ainsi de dissimuler l'existence même de partitions. Citons les principaux :

- Le plus célèbre reste le logiciel PGP (Pretty Good Privacy). Produit phare des années 90 de la communauté, il a acquis la maturité commerciale et propose outre une interface graphique simple mais ergonomique, la plupart des fonctionnalités attendues : chiffrement du courrier électronique à la volée, chiffrement de fichiers, intégrité, effacement sécurisé...
- DriveCrypt de SecurStar. Si son interface est plus austère que celle de PGP, il offre en revanche beaucoup plus de possibilités. Le choix des algorithmes de chiffrement est plus large : du simple DES 56 bits aux très puissants triple AES 768 bits ou triple BlowFish 1344 bits. Une autre fonction très intéressante de ce logiciel permet par exemple à tous les membres d'une équipe d'avoir leurs disques chiffrés avec leurs propres mots de passe, tout en gardant la possibilité pour le responsable d'avoir un mot de passe maître capable d'ouvrir tous les disques. Ainsi, si un utilisateur est absent, ou a quitté la société, il sera toujours possible de récupérer les données de son disque (aspect important de disponibilité des données). Enfin, DriveCrypt propose des fonctionnalités de



stéganographie et permet avec la fonction dénommée « disques invisibles » de leurrer d'éventuels agresseurs qui voudraient forcer l'utilisateur à livrer son mot de passe. Deux mots de passe sont en effet attribués à un même disque. Le premier l'ouvre sur des données « banales » dont la compromission ne porte pas à conséquence et le deuxième sur les données vraiment confidentielles à protéger. Lors d'une éventuelle agression, il suffira de donner le mauvais mot de masse. De plus, la totalité de l'espace libre du disque est occupée par des données aléatoires. Il est donc impossible de savoir si un disque contient ou non, un disque invisible (aspect TRANSEC).

A côté des solutions logicielles, commencent à apparaître pour le grand public et les entreprises, des solutions de chiffrement matérielles. Ces solutions semblent en particulier répondre aux préconisations d'organismes officiels en matière de sécurité informatique. A titre d'exemple, en mars 2006, Interpol demande à ce que les PC vendus soit systématiquement pourvu de systèmes de sécurité, incluant notamment le chiffrement des données. Avec le chiffrement matériel, les données sont chiffrées et déchiffrées à la volée, par le processeur, de manière totalement transparente. Pour le moment, les cibles de cette nouvelle technologie sont principalement les téléphones, assistants personnels ou ordinateurs portables des sociétés, terminaux qui contiennent des données de plus en plus confidentielles (650 millions de mobiles, au sens large du terme, sont vendus chaque année). Des technologies comme Secure Blue d'IBM ou la solution TPM (Trusted Platform Module) du Trusted Computing Group (réunissant les grands éditeurs et constructeurs comme Intel, AMD et Microsoft) commencent à investir le marché. Malgré d'indéniables avantages, ces solutions ne feront pas disparaître pour autant les solutions logicielles. Car si la rapidité de chiffrement et le niveau de sécurité militent très nettement en faveur des solutions matérielles, ces dernières ne sont pas exemptes d'inconvénients :

- Problème de la confiance : comment faire totalement confiance à un système difficile à évaluer et à auditer. De tels systèmes, mis en place par des constructeurs non nationaux, mettront en œuvre du chiffrement difficilement maîtrisable ;
- En cas de faille de conception ou d'implémentation, si corriger un logiciel ou carrément le remplacer est relativement facile, en revanche pour le matériel c'est économiquement et logistiquement ingérable.

Rappelons enfin que ces produits et dispositifs matériels sont strictement interdits d'usage, en France, pour le chiffrement de données relevant du secret de défense. Un industriel qui utiliserait des logiciels dans ce cas risquerait des peines de prison et de lourdes amendes. Il doit pour cela utiliser des logiciels nationaux validés par le SGDN (Secrétariat Général de la Défense Nationale) et la DCSSI (Direction Centrale de Sécurité des Systèmes d'Information). Notons que les autres pays ont adopté le même principe. Ainsi, aux Etats-Unis, le système AES est interdit d'usage s'agissant de données sensibles ou critiques (voir document fédéral FIPS 196).



En résumé

La protection des données est un aspect essentiel dans la sécurité des systèmes d'information. Trop souvent, les politiques de sécurité se polarisent sur la protection des systèmes et éventuellement des données traitantes. Des affaires de compromission de données lors de vols ou de pertes de portables rappellent chaque fois que la ressource ultime devant être protégée est l'information elle-même. Mais il faut également se rappeler que chiffrement, intégrité et disponibilité doivent se placer dans un contexte de sécurité informatique. A quoi sert le chiffrement si le mot de passe protégeant la clef secrète est trop faible, facilement récupérable ou si un virus ou un ver parvient à le dérober ! Encore une fois, la sécurité informatique est un tout qui doit être monolithique. Toute faiblesse dans le dispositif général fragilisera à terme l'ensemble. La difficulté du métier réside précisément dans la vision globale de la sécurité.



La pédophilie sur Internet

Aujourd'hui, l'informatique est entrée dans les mœurs. La moitié des foyers disposent d'un ordinateur et les abonnés à l'Internet à haut débit étaient plus de dix millions au printemps 2006. Si les seniors s'intéressent de plus en plus à cet univers ce sont nos enfants les plus accros. Ils appartiennent à la génération née avec une souris et un clavier dans les mains ! Une enquête réalisée, il y a deux ans, par l'Observatoire d'Ipsos (entretiens auprès de 2203 enfants et de leurs mères) indiquait que 30 % des 6-8 ans utilisent déjà le Web. Vers 13-14 ans, ils sont 80 % à surfer sur la toile. Une autre étude, menée par le CREDOC (Centre de Recherche pour l'Etude et l'Observation des Conditions de vie) en décembre 2004, indique que 57 % des jeunes de moins de 17 ans utilisent les « chats » et ils sont 62 % à penser qu'Internet est un bon outil pour se faire des amis.

Une naïveté toute naturelle mais qui peut avoir des conséquences dramatiques.

Sur Internet on peut côtoyer le meilleur et le pire. Des prédateurs rôdent. Les pédophiles¹ ou des escrocs tentent de rencontrer des mineurs ou d'obtenir des numéros de cartes bancaires. Le cyberspace attire des réseaux crapuleux et charrie des milliers de contenus illicites. D'après une étude menée par l'association Le Bouclier, 261 653 "sites pédophiles" avaient été répertoriés en 2002, contre 4 300 seulement en 1996.

Grace à la coopération internationale, de nombreux réseaux tombent dans les filets des policiers. En juin 2006, neuf Turcs et un Américain ont été arrêtés en Turquie². Les suspects, dont un professeur de lycée, avaient contacté une trentaine de mineurs sur des forums de discussions et les avaient abusés sexuellement. Les photos prises lors de ces abus, ainsi que des enregistrements vidéo, avaient ensuite été vendus via le net.

1. Les professionnels de la justice critiquent, pour beaucoup, le terme même de pédophile, ce dernier introduisant étymologiquement une confusion. Beaucoup de magistrats préfèrent parler de pédocriminel. Nous conserverons cependant le premier terme, plus connu du grand public.
2. Dépêche AFP du 13/06/2006.



Le même mois, soixante-sept utilisateurs présumés de pornographie infantile sur le web ont été interpellés lors d'une opération coordonnée par Europol¹. Dix personnes ont été arrêtées en Espagne, sept en Belgique, trente-huit en France, trois aux Pays-Bas et neuf en Slovaquie. Selon un communiqué du ministère de l'Intérieur espagnol, les suspects « obtenaient des images de pornographie infantile à travers un complexe et lent système de téléchargement qui incluait l'utilisation de programmes complexes de chiffrement. Les personnes interpellées en Espagne avaient de bonnes connaissances en informatique et un niveau culturel élevé ».

Quelques semaines plus tôt, un réseau de pédophiles est démantelé en Pologne². Dix personnes ont été mises sous les verrous. Mais d'autres interpellations devaient avoir lieu car les informations sur les activités de ce groupe ont été transmises à 70 autres pays, via Interpol. « Une cinquantaine de disques durs ont été saisis. Ils contiennent plus de 300 000 photos et 3000 films pornographiques » a indiqué la police polonaise. Le groupe avait créé un forum internet d'échange de contenus pornographiques et une vidéothèque virtuelle. Pour y accéder, il fallait autoriser l'accès à sa propre collection.

12.1 LA TRAQUE POLICIÈRE

Ces trois exemples montrent que la pédophilie sur l'Internet est un fléau qui touche de nombreux pays. Face à ces menaces, les pouvoirs publics ont créé des entités spécialisées. Une veille des contenus illicites véhiculés sur Internet a été mise en œuvre au Service technique de recherche judiciaire et de documentation de la gendarmerie (STRJD) ou au sein de la police nationale. La première grande opération, intitulée « Forum 51 », a été lancée par la Gendarmerie nationale en juin 2001. Elle faisait suite à plus d'un an d'enquête sur certains canaux IRC (Internet Relay Chat), et a donné lieu à 75 interpellations.

Depuis, la pression des pouvoirs publics s'est accentuée grâce à des moyens renforcés. La Brigade de protection des mineurs (une des six brigades centrales de la direction de la Police judiciaire de Paris) traque ces réseaux depuis la fin des années 90. Mais depuis 2003, elle s'appuie sur les compétences d'un groupe d'enquête spécialisé. Le Groupe Internet mène de bout en bout des investigations portant sur des faits de pédophilie ayant comme support ou moyen le réseau internet.

Son activité s'articule autour de deux axes principaux :

- La lutte contre les trafics d'images pédophiles : le nombre d'images et de vidéos pédopornographiques disponibles sur Internet augmente de manière exponentielle chaque année. Selon les estimations, Internet en hébergerait entre 800 000 et un million³. Plus de 260 000 sites contenant de la pédopornographie ont été recensés en mars 2005.

1. Dépêche AFP du 06/06/2006.

2. Dépêche AFP du 23.05.2006.



- La recherche des « prédateurs » du Net : selon des sources policières, les enfants sont régulièrement sollicités lors de ces discussions par des adultes mal intentionnés.

Le Groupe Internet a initié plusieurs affaires. La première année, il a traité 96 affaires. L'année suivante, leur nombre est passé à plus de 300. La plus connue est CAUSSADE. Elle a abouti à l'interpellation d'un homme ayant prostitué de nombreuses mineures « recrutées » sur des sites de conversation en direct (*chats*).

Des réseaux de milliers de personnes

En 2001, l'opération Candyman a mis au jour, à l'initiative du FBI américain, trois groupes de discussion et d'échanges de fichiers basés sur le web et comptant 6 700 membres. Cette enquête a donné lieu à plus d'une centaine d'arrestations. Engagée dès 1999, et étendue à un niveau international en 2001, l'opération Avalanche a permis de faire cesser les opérations de la société Landslide Productions, basée à Fort Worth au Texas, qui diffusait sur plusieurs sites payants des images pédopornographiques importées notamment de Russie et d'Indonésie, et de saisir les coordonnées de 250 000 clients de cette société, localisés dans 37 états américains et 60 pays différents.

Suite de l'opération Avalanche en Grande-Bretagne, l'opération Ore a conduit à l'interpellation, en janvier 2003, de 1 600 suspects sur le seul territoire britannique. Source : Forum des droits sur l'Internet. Janvier 2005.

De son côté, la Gendarmerie nationale surveille ses réseaux depuis 1998. Elle dispose, entre autres, de plus de 120 personnels « NTECH » (nouvelles technologies) spécifiquement formés aux techniques d'enquête propres aux infractions liées à cette problématique. Depuis 1992, le département informatique-électronique (INL) de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) apporte un soutien technique (expertises, surveillance, interceptions) aux différents services de gendarmerie.

12.1.1 Des programmes spécifiques

Les enquêteurs spécialisés de la Police et de la Gendarmerie nationale sont aidés par des programmes et des banques de données. Créé en 2001, par le capitaine Lesobre de l'INL, le logiciel Marina (Moyen Automatique de Recherche d'Images Non Autorisées) dispose de plus de 600 000 signatures d'actes de pédophilie. Il suffit de l'exécuter sur l'ordinateur d'un suspect pour que le robot récupère images, vidéos, e-mails...

Mis en place en 1998 par l'INL, SimAnalyst est un logiciel qui permet de lire le contenu d'une carte SIM et donc de connaître la dernière zone géographique où le téléphone était allumé. Enfin, la Gendarmerie a aussi développé les logiciels Log IRC

3. La diffusion d'images pédopornographiques sur l'internet reste toutefois sans commune mesure avec celle de pornographie adulte.



— pour surveiller de manière automatisée les groupes de discussion sur Internet — et Log P2P pour surveiller les réseaux d'échanges de fichiers.

La Gendarmerie nationale dispose aussi d'une base de données qui permet de regrouper des informations sur les auteurs, les victimes et les lieux utilisés. Cette base est alimentée depuis 2003 par le Centre national d'images pédopornographiques (CNAIP) qui fonctionne en collaboration avec la Police nationale. Cette banque de données contient plus de 480 000 photographies de nature pédopornographique. « Ce système permet de sauver une dizaine d'enfants par an », selon le capitaine de Gendarmerie Eric Freyssinet, Chef du Département Electronique Informatique de l'IRCGN.

12.2 LES LOGICIELS DE FILTRAGE

Les autorités interviennent en aval. Mais pour réduire les risques il est indispensable que les parents soient sensibilisés et mettent en place des solutions en amont. Face à cette situation délétère, beaucoup semblent démunis. Il est vrai que les informations pratiques sur ce sujet font encore cruellement défaut. Ce n'est plus le cas depuis octobre 2006 avec la première version du site officiel Confiance (www.internetsans-crainte.fr), un plan français d'action de sensibilisation aux enjeux et aux risques d'Internet pour les enfants, jusqu'en 2007. Les premiers outils de sensibilisation (posters, guide et CD/DVD) sont diffusés.

En attendant que ce programme ne monte en puissance, les parents doivent installer sur leur ordinateur un logiciel de contrôle parental. Très peu le font. En juin 2005, seulement 15 % des foyers disposaient d'un tel programme !

Son rôle consiste à filtrer les contenus et à bloquer certaines activités préalablement interdites (envois de pièces jointes par e-mail, utilisation d'un logiciel de messagerie instantanée...). Plus facile à dire qu'à faire ! Ces programmes doivent résoudre un sérieux casse-tête. S'ils effectuent un contrôle très strict, ils risquent de bloquer des sites au contenu inoffensif (un site sur la santé contient nécessairement les mots sexe, sein, testicule...). À l'inverse, si leur filtrage est trop limité ils vont laisser passer des horreurs ! Pour résoudre ce dilemme, ces logiciels n'utilisent pas tous sur les mêmes procédés. Certains se contentent du filtrage des sites X, d'autres assurent aussi le blocage et le filtrage d'autres services comme les forums de discussion, les messageries instantanées et les transferts de fichiers.

Pour le filtrage du contenu, les logiciels s'appuient sur une liste noire d'adresses URL. Pour qu'elle soit efficace, il faut que l'éditeur l'enrichisse continuellement et que le consommateur fasse régulièrement des mises à jour. Les sites pédophiles ou pornographiques changent en effet assez souvent d'intitulés ou d'adresses. L'analyse du contenu se fonde aussi sur une liste de mots à exclure. Dès que l'un d'entre eux est repéré par le logiciel, ce dernier peut immédiatement bloquer l'accès au forum ou empêcher l'affichage du message ou du terme en question. Mais là aussi, cette liste



doit être régulièrement mise à jour. Les parents peuvent également y ajouter des nouveaux mots-clés.

Les limites des filtres ICRA et Safesurf

Les navigateurs (Internet explorer, Netscape, Mozilla...) disposent d'une fonction de filtrage des contenus, mais elle n'est pas efficace. La technologie utilisée est basée sur des codes insérés volontairement par les concepteurs de pages web, ceux qu'on appelle les webmasters. Ce procédé s'appuie sur deux filtres. ICRA (Internet Content Rating Association) et Safeguard. Mais leur installation conduit à exclure plus de 99 % des sites web français comme l'a constaté 60 Millions de consommateurs dans son numéro de mai 2004. Ce résultat n'est pas vraiment surprenant car la majorité des sites ne tiennent pas compte de cette codification. On se demande alors pourquoi ils existent encore. Faire référence à ces deux filtres n'offre donc aucune garantie en matière de protection.

Pour affiner les filtres, la plupart des logiciels disposent d'un journal de bord dans lequel sont consignées toutes les alertes. C'est un bon moyen de repérer des sites ou des mots qui n'auraient pas été exclus ou au contraire de constater des fausses alertes engendrées par un filtrage trop pointu.

Ces logiciels ne présentent pas pour autant la solution idéale. Dans son numéro daté de mai 2004, 60 Millions de consommateurs en a testé quinze, en collaboration avec la Délégation interministérielle à la famille (DIF), la Direction du développement des médias (DDM) et la Délégation aux usages de l'internet (DUI). Les plus efficaces sont le logiciel de contrôle parental inclus dans les packs de sécurité (anti-virus, antispams, pare-feu...) « McAfee Internet Security Suite » (75 €) et « Norton Internet Security » (90 €). La sécurité de nos enfants n'est donc pas donnée... Tous les autres logiciels manquent d'efficacité ou sont compliqués à configurer.

Si vous ne voulez pas investir dans un tel logiciel vous pouvez opter pour un gratuit : LogProtect (www.logprotect.net). Ce logiciel en français (pour PC mais pas pour Mac) ne répond qu'à un seul type de problème mais il le fait très bien : il empêche vos enfants de transmettre sur Internet des informations sensibles (nom de famille, adresse, téléphone, nom et adresse de l'école, etc.). Il suffit de compléter un formulaire regroupant ces éléments à ne pas transmettre pour qu'il les bloque dès qu'ils sont tapés avec le clavier. En plus des informations personnelles, il est également possible d'établir une liste de mots. Lorsque ces données sont bloquées un message d'avertissement, qui peut être personnalisé, est affiché à l'écran. Il indique à l'enfant que ce qu'il est en train de faire peut être dangereux pour sa sécurité. Au bout du troisième avertissement il est possible de couper la connexion.

Comme d'autres logiciels de contrôle parental, celui-ci est protégé par un mot de passe (qui doit être changé régulièrement) qui est demandé à chaque modification de la configuration du logiciel ou pour arrêter le système de protection.



12.2.1 Des fournisseurs d'accès laxistes ?

Concernés aussi par ce problème, les FAI ont mis en place différentes parades mais qui n'ont pas vraiment montré leur efficacité. De nombreux spécialistes estiment d'ailleurs qu'ils font preuve d'un manque de volonté. Il est vrai que la loi du 21 juin 2004 pour la confiance dans l'économie numérique n'est pas très pénalisante. Son article 9 prévoit que « les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne » c'est-à-dire en premier lieu, les fournisseurs d'accès à l'internet (FAI), ne peuvent voir leur responsabilité civile ou pénale engagée que dans les cas où :

- ils sont à l'origine de la demande de transmission litigieuse ;
- ils sélectionnent ou modifient les contenus faisant l'objet de la transmission.

Le législateur affirme également que les prestataires techniques ne sont soumis à aucune obligation générale de surveillance des informations qu'ils transmettent ou qu'ils stockent, mais que le juge conserve la possibilité d'imposer une telle mesure de surveillance, ciblée et temporaire (art. 6-I-7°). Cette loi oblige néanmoins les prestataires français d'hébergement, d'une part, à « informer promptement les autorités publiques compétentes de toutes les activités illicites mentionnées à l'alinéa précédent [ayant trait, notamment, à la pédopornographie] qui leurs seraient signalées et qu'exerceraient les destinataires de leurs services ».

L'AFA (Association des fournisseurs d'accès) a néanmoins lancé en février 2005 le label « Net+sûr ». Son cahier des charges comporte les obligations suivantes pour les fournisseurs d'accès membres de l'AFA :

- proposer un outil de contrôle parental,
- donner accès à des informations destinées à mieux protéger les enfants,
- donner accès en un seul clic à un formulaire de signalement des abus,
- traiter les signalements de contenus pédopornographiques ou incitant à la haine raciale...

L'AFA respecte aussi la loi sur la confiance en l'économie numérique (LCEN) votée le 22 juin 2004. La LCEN a repris une disposition datant de 1996 selon laquelle chaque FAI doit proposer à ses abonnés un logiciel de contrôle parental.... contre quelques euros (ou dans un forfait sécurité incluant un antivirus).

En novembre 2005, cette association s'engageait auprès du ministre délégué à la Famille, Philippe Bas, à mettre gratuitement à disposition de ses clients ce type de logiciel. Deux mois après la date limite fixée par le ministre (le 31 mars 2006), E-enfance¹ a fait le point en les testant². Son verdict est sans appel : « Ces logiciels

1. Cette association a pour ambition d'aider les enfants à tirer le meilleur parti des nouvelles technologies, en collaboration avec la Délégation aux usages de l'Internet et le ministère en charge de la Famille.

2. www.e-enfance.org



doivent fortement s'améliorer. La qualité des sites proposés (liste blanche) est insuffisante pour la plupart des FAI (Alice, Club, Free, Numéricable). »

Parmi tous ces logiciels testés, seul celui proposé par AOL tire son épingle du jeu. Il bloque plus de 90 % des sites contenant du sexe, de la violence et ceux vantant les drogues ou proposant des jeux interdits aux moins de 18 ans. Celui d'Orange (ex-Wanadoo) s'en sort aussi convenablement. Les autres logiciels souffrent en revanche de plus grosses lacunes. Les listes blanches fonctionnent mal et le filtrage est généralement insuffisant, notamment pour ce qui est des sites prônant la haine ou la violence, contre lesquels une analyse sémantique est nécessaire. D'autres sont de vraies passoires. Celui de Club-Internet ne bloque que 37 % des jeux interdits aux moins de 18 ans et 17 % des sites contenant des propos haineux ou violents (comme celui d'Alice, d'ailleurs). Mais le bonnet d'âne revient à Free (qui n'est pas membre de l'AFA). Son logiciel est jugé par E-enfance comme « compliqué pour les parents » et « désastreux pour les enfants ». Non seulement il filtre mal les sites indésirables, mais il est en outre le plus difficile à utiliser. A signaler que Neuf-Cegetel et Téléré 2 ne proposaient toujours aucune solution gratuite à leurs abonnés au moment de ce comparatif (leurs logiciels étaient payants mais leur performance n'était pas meilleure d'après l'association !).

Basée sur l'intelligence artificielle, une nouvelle gamme de logiciels pourrait permettre d'améliorer sensiblement les performances du filtrage des fournisseurs. Développés par la start-up française Adamentium, les logiciels LiveMark atteignent un taux de réussite de filtrage de 98 % selon ses concepteurs. ! Issu des pôles d'incubation de l'Ecole des mines d'Alès et de la région Languedoc-Roussillon, Adamentium espère intéresser l'Education nationale, les fournisseurs d'accès à internet (FAI) ou les opérateurs de téléphonie mobile. Développé en collaboration avec le centre de recherche de l'Ecole des mines d'Alès (LGI2P), LiveMark ne fonctionne pas avec des listes noires ou blanches comme les logiciels de filtrage des FAI, mais à partir d'une analyse sémantique du texte, des images et même du contexte. Cette nouvelle génération de logiciels permet de refuser l'accès à toutes les pages indésirables disponibles sur l'ensemble du Web. De plus, elle n'a pas tendance à bloquer les contenus pédagogiques, comme par exemple ceux d'éducation sexuelle.

Les performances nouvelles de cette technologie de pointe ont permis à Adamentium de recevoir en 2004 le label Oppidum, du ministère de l'Economie, des finances et de l'industrie, dans la catégorie « Outils de filtrage pour le contrôle parental ». Les qualités de filtrage de LiveMark sont conseillées par le ministère de l'Éducation nationale (accord cadre) pour sécuriser l'Internet dans les écoles.

Rappelons enfin l'obligation de dénoncer au procureur de la République sous peine de deux ans de prison tout acte mettant en danger les mineurs. Des parents qui découvrent un site lié à la pédophilie ont donc obligation de le dénoncer.



En résumé

Malgré de beaux discours et une offre de plus en plus importante de logiciels de sécurité (et notamment de filtrage), la situation n'a pas beaucoup évolué. Les parents, et leurs enfants, sont peut-être un peu mieux sensibilisés. Mais ils restent néanmoins démunis face à ce terrible danger que représente la pédophilie sur l'Internet. Heureusement, la police et la Gendarmerie nationale disposent de spécialistes aux compétences reconnues. Ils sont cependant en nombre trop faible.



13

Banques en ligne : une sécurité limitée

Attendre patiemment son tour au guichet de sa banque n'est plus qu'un (mauvais) souvenir pour un internaute européen sur deux. Publiée en mai 2006, une étude de Forrester Research montre que près de la moitié des internautes utilisent les services en ligne de leur banque. Cette proportion varie selon les pays. Les Suédois (72 %) sont ceux qui utilisent le plus ce service, suivis des Allemands (56 %), des Français (55 %) et des Britanniques (52 %). Les Italiens ne sont que 31 % à gérer leurs comptes depuis leur ordinateur.

Les différentes affaires de « hold-up numérique » ou d'escroquerie financière ne vont peut-être pas inciter nos voisins transalpins à franchir le pas. Début 2006, la police française a démantelé un réseau franco-russe de malfaiteurs qui auraient réussi à pénétrer les comptes bancaires en ligne d'une soixantaine de leurs compatriotes et à y retirer 200 000 euros. Selon l'Agence France Presse, qui cite une source judiciaire, les pirates avaient créé une société fictive aux Etats-Unis, qui proposait à des intermédiaires français — baptisés « mulets » par les enquêteurs — de recevoir sur leur compte personnel l'argent détourné grâce à un virus tapis dans la mémoire de l'ordinateur des victimes. Les « mulets » percevaient une commission de 1 % à 5 %. Des intermédiaires, résidant en Allemagne ou en Espagne renvoyaient ensuite le butin vers la tête du réseau, des membres de la mafia russe.

Ce n'est pas la première fois que ce genre d'escroquerie est mise en place dans l'Hexagone. En 2005, l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication) a arrêté six personnes soupçonnées d'avoir effectué des virements frauduleux après avoir accédé aux comptes de clients d'Axa Banque. « Des « mules » détournaient l'argent sur leur compte avant de le transférer — via Western Union — sur un compte en

Ukraine, moyennant une commission de 10 % », raconte Marie Lajus, adjointe au chef de cet office¹.

Parallèlement à ces affaires, il y a aussi les braquages virtuels. En 1999, une équipe de pirates russes a détourné 40 millions de dollars de la banque américaine Citibank, en pénétrant dans ses systèmes informatiques. Il y a quelques années, un Chinois habitant à Singapour a détourné environ 36 000 euros dans 21 comptes de la DBS Bank. En moins d'une heure, il a réalisé des virements de 200 à 4.999 dollars singapouriens (les transferts de fonds en ligne chez DBS étant plafonnés à 5.000 dollars singapouriens par jour).

13.1 UN MANQUE DE VOLONTÉ

Certaines banques font preuve d'une certaine légèreté en matière de sécurité informatique. C'est le constat de la CNIL qui a étudié dix sites de banques françaises. « Trop souvent, seul l'identifiant et un mot de passe, inférieur à 7 caractères, sont demandés pour accéder aux comptes. Une fois sur deux, les coordonnées sont mémorisées par l'ordinateur. Plus grave, quatre sites de banque en ligne ne sont pas en transaction sécurisée HTTPS lorsque le client tape ses codes », constate le mensuel *60 millions de consommateurs* dans son édition de janvier 2006.

Pire, sur le site de la Banque postale on peut même consulter un certain type de comptes (pour des raisons de sécurité nous taillons son intitulé) sans avoir besoin de taper un mot de passe. Il suffit d'entrer son numéro de compte et de choisir, dans la courte liste fournie, son centre financier. Deux informations faciles à obtenir, par exemple sur les relevés d'identité bancaire ou sur les chèques.

Ces failles expliquent, en partie, l'augmentation du nombre d'attaques visant ces sites. En juin 2006, l'Association Européenne de Management & Marketing Financiers (EFMA) annonce que « 78 % des établissements ont subi des intrusions dans leur système dans les 12 derniers mois, d'après une enquête² réalisée auprès des 150 premières institutions financières mondiales ». On apprend aussi qu'un « établissement sur deux a subi au moins une attaque venant de l'intérieur ».

Le phishing et le pharming sont les deux principales techniques utilisées, suivies des logiciels espions. Face à cette délinquance, « 58 % des banques agissent pour empêcher les vols d'identité bancaire, et presque toutes investissent dans des pare-feux. Mais la formation adéquate du personnel ne suit pas, dans deux établissements sur trois. » Selon l'étude, le coût des « défaillances dans la sécurité bancaire avoisine le million de dollars ».

Il est difficile d'obtenir des informations plus détaillées, surtout en France où les milieux financiers, entre autres, ont le culte du secret. Les statistiques sont moins opaques outre-manche. Le montant des fraudes sur les sites de banque en ligne bri-

1. L'Expansion, nov. 2005.

2. Rapport mondial annuel sur la sécurité « Global Security Survey » du cabinet Deloitte.



tanniques auraient représenté environ 23 millions de livres au premier semestre 2005, selon l'association britannique des paiements (APACS). Soit 8 millions de plus qu'en 2004. Plus sensibilisés que d'autres établissements, les banques anglaises se sont concertées pour réagir et l'APACS a commencé à travailler avec d'autres pays déjà victimes d'attaques tels que les États-Unis et l'Australie. L'association a aussi créé un site web (www.banksafeonline.org.uk,) pour alerter les internautes sur les attaques et expliquer les règles de conduite à adopter sur Internet. En France, la sensibilisation est assez limitée.

Lorsqu'on se rend sur le site Les clés de la banque (www.lesclesdelabanque.com), édité par la Fédération bancaire française, on découvre une rubrique « Se protéger ». Fausse piste puisqu'il s'agit de la protection des biens et des personnes et donc de... contrats d'assurance à souscrire auprès de son banquier ! Il faut aller dans la rubrique Mini-guides pour y repérer un document consacré à la « sécurité des opérations bancaires ». Après des informations concernant les chèquiers et le vol de code d'une carte bancaire, on trouve un paragraphe assez long dédié aux opérations à distance. On y donne quelques conseils pour ne pas être victime de phishing, sur la manière de se protéger avec un antivirus et un pare-feu, etc.

Proposé par BNP Paribas, le site Espace sécurité (www.espace securite.bnpparibas.com/) est plus détaillé et pratique. On y parle bien sûr de phishing mais aussi comment créer et protéger un bon mot de passe, comment ne pas tomber dans le piège des spams, bien acheter sur internet, de logiciels de sécurité et des aspects juridiques. Des liens vers des sites spécialisés sont aussi signalés. L'initiative du groupe BNP Paribas est donc à saluer. Mais elle est l'exception qui confirme la règle. Plusieurs raisons expliquent cette timide volonté de sensibilisation. Pour maître Eric Barbry, directeur du département nouvelles technologies au cabinet d'avocats Alain Bensoussan, « les banques ont mis en place un système pervers qui marche très bien pour elles : elles se trouvent entre l'internaute et le site marchand. La loi dit en substance : le client a toujours raison. Dans tous les contrats de vente en ligne qu'ils ont passés avec les sites marchands, les établissements bancaires ont indiqué qu'en cas de contestation de l'acheteur c'est le site de commerce électronique qui rembourse la banque qui, ensuite, va ensuite rembourser le client. On déporte la responsabilité sur le vendeur qui n'a pas trop de recours : une assurance, des prêts à long terme afin de couvrir son risque... »

« Ce sont pourtant les banques qui doivent se protéger, estime **Hervé Schauer**, expert en sécurité informatique. On peut difficilement demander à l'utilisateur de se rendre compte qu'il se fait berner. Les banques, comme tous les développeurs de services en ligne, doivent partir du postulat que le PC de leurs clients est infecté par quantité de logiciels malveillants comme les spywares ».

De son côté, Jean-Luc Jacob, responsable de la direction des nouveaux médias du Crédit Mutuel Nord Europe précise que « nous faisons réaliser par une société externe un audit des applications et des services destinés au client et faisons procéder à une vérification de l'intégrité de l'ensemble de nos systèmes de sécurité. Par ailleurs, des tests d'intrusion sont menés par une équipe interne d'experts, épaulée par des correspondants sécurité présents au niveau régional ».



13.2 LES PARADES (OFFICIELLES) DES BANQUES

Pour de nombreux experts indépendants, il existe des solutions assez simples permettant de limiter les risques. D'autres parades plus compliquées n'apporteraient pas nécessairement beaucoup plus de protection pour le grand public ou des PME ; elles permettraient surtout aux vendeurs de solutions informatiques d'augmenter leur chiffre d'affaires !

« Il faut d'abord que les banques surveillent les connexions de leurs clients, déclare **Hervé Schauer**. Si un client se connecte à son compte depuis Paris et qu'une demi-heure plus tard, il se connecte depuis une autre ville, la banque devrait mettre en attente cette connexion. Un chargé de clientèle doit l'appeler afin de vérifier et valider cette opération. Il peut s'agir en effet du conjoint qui effectue une transaction car il a aussi le mot de passe et une procuration. Il n'y a que American Express qui le fait : si dans la même minute vous achetez deux fois la même chose sur Internet, la société vous appelle. Selon elle, la probabilité des cas où la personne a fait une erreur est plus importante que le piratage et ça leur coûte moins cher de mettre en attente. Si elle n'arrive pas à vous joindre, elle met en attente toutes les opérations faites sur Internet mais ne bloque pas le paiement d'un restaurant par exemple. »

13.2.1 Le pavé numérique

La mise en place par quelques banques françaises du pavé numérique fait partie des solutions simples mais assez efficaces. Ce pavé reproduit les touches à chiffres du clavier d'un ordinateur. Pour taper son mot de passe, il faut donc utiliser la souris pour cliquer sur les bons chiffres. Cette solution évite ainsi qu'un logiciel espion n'enregistre votre mot de passe tapé sur le clavier. Cette parade n'est bien sûr pas la panacée. Il existe des logiciels (**screenloggers**) capables d'enregistrer les mouvements, la position du curseur et les clics de souris ! Mais ils sont moins nombreux que les fameux **keyloggers** chargés d'enregistrer les frappes de clavier et un screenlogger doit être adapté à chaque banque (son coût est donc plus élevé).

Autres écueils : le clavier virtuel a presque toujours la même taille et le même nombre de touches quelle que soit la banque et sa position sur l'écran ne varie pas beaucoup. « Le pavé numérique présente néanmoins un bon équilibre, estime **Hervé Schauer**. Il élimine la plupart des attaques sans imposer de contraintes aux utilisateurs. » Une évolution intéressante pourrait être de considérer des pavés ayant un nombre aléatoire de touches vides, réparties elles-mêmes aléatoirement sur tout le clavier.

13.2.2 L'antivirus de la banque

Beaucoup d'internautes savent qu'il est indispensable d'installer un antivirus sur son ordinateur. Mais tous n'ont pas l'envie ou les moyens de déboursier une trentaine d'euros dans ce genre de logiciel. D'autres ne savent pas lequel acheter. Pour simplifier la vie de ses clients, Barclays a donc décidé de vendre un antivirus. Début 2006,



la banque britannique a décidé de s'associer à l'éditeur finlandais, F-Secure pour commercialiser ses produits (reconnus pour être efficaces). Après l'avoir testé gratuitement pendant un mois, les cinq millions de clients de la banque pourront l'acheter.

La banque a aussi mis en place un astucieux service d'alerte par SMS : dès qu'une transaction est menée sur Internet, un message est envoyé au client pour l'en informer. Un service original pour repérer les tentatives de phishing. Echaudée après avoir été victime d'un cheval de Troie en 2005, la banque anglaise a décidé au printemps 2006 de limiter à 1000 livres (contre 2000 auparavant) le montant des virements par le web à destination de comptes extérieurs à l'établissement.

13.2.3 Les systèmes d'authentification forte

Pour certains, le couple identifiant/mot de passe ou le clavier virtuel ne sont pas efficaces. Il faut employer les grands moyens.

Il existe trois types de solutions :

- l'utilisation d'un code automatique à durée de vie limitée (principe du *token* ou jeton),
- la clé USB qui est capable de stocker des mots de passe chiffrés ou de gérer les certificats électroniques d'accès aux documents,
- et enfin les systèmes de cartes à puce. Une dizaine d'entreprises proposent ce genre de solutions, les plus connues étant RSA et Aladdin Knowledge Systems.

Mais ces parades se heurtent à un terrible dilemme : faut-il mettre en place une protection plus forte au détriment d'un service plus convivial ? Pour l'instant, les systèmes d'authentification forte ont du mal à convaincre. Malgré les injonctions de la Federal Deposit Insurance Corporation, lancées dès 2004, les banques américaines ne se précipitent pas pour renforcer leur sécurité. Elles font pourtant partie des cibles favorites des phishers ! En mars 2006, des chevaux de Troie d'un genre particulier ont été repérés. Ils étaient conçus pour intercepter les codes (TAN) exploités dans le cadre des mécanismes d'authentification forte mis à la disposition des clients de deux établissements allemands, la Postbank et la Deutsche Bank.

Les banques se tournent aujourd'hui vers la signature électronique. Appelée aussi certificat numérique, cette solution est connue de tous les Français qui font leur déclaration de revenus sur le site du ministère de l'Economie et des Finances. Il s'agit en fait d'un petit programme qui permet de sécuriser des transactions de toutes sortes. C'est l'équivalent d'une pièce d'identité électronique qui permet d'être authentifié à chaque connexion.

Après les impôts, ce sont donc les échanges de données entre les clients et leur banque qui ont recours à la signature numérique. Depuis avril 2006, la Deutsche Postbank mise sur cette solution. Produite par TC Trust (premier fournisseur allemand de certificats électroniques créé par des banques), elle fonctionne uniquement avec le logiciel de messagerie Outlook de Microsoft. Lorsque le client veut envoyer un e-mail



certifié, il doit le signer numériquement en cliquant sur le bouton « Sign S/MIME » de la barre d'outils avant de l'envoyer. A l'inverse, pour vérifier qu'un e-mail est bien envoyé par sa banque, il doit vérifier la présence d'un petit cachet rouge dans la boîte de réception. En cliquant dessus, les informations détaillées apparaissent.

Deux organismes français développent une solution basée sur le même principe. Depuis avril 2006, Finaref propose à ses clients de souscrire à une assurance de compte ou de prendre une carte Visa en signant « numériquement » le contrat. Filiale du Crédit agricole, cette société de crédit (5 milliards d'euros d'encours de crédit gérés) a fait appel à Keynectis, un prestataire qui gère aussi les certificats électroniques du site des impôts. « A la différence du site de l'Etat, notre certificat n'est pas lié à un ordinateur ; il s'agit d'un certificat dit « à la volée » qui ne dure que le temps de l'opération en ligne, précise Nicolas Denis, Directeur clientèle et marketing directs de Finaref. Notre client n'est donc pas tenu de signer ses contrats numériquement depuis un seul ordinateur. »

Pour éviter que le document signé par le client ne soit pas modifié par erreur, Finaref a confié la sauvegarde des données à un tiers archiveur (Arkhinéo, filiale de la Caisse des dépôts et consignment). Entre 20 et 30 signatures électroniques étaient enregistrées par jour en mai 2006. Pour l'entreprise, l'objectif à terme est de réaliser une dématérialisation complète du processus. Pour ses clients connus, dont l'identité a été authentifiée, la signature numérique pourrait concerner un avenant de contrat (augmentation de ligne de crédit) ou des contrats complémentaires). « L'étape ultime concernera des clients « non connus » pour une offre préalable de crédit », indique précise Nicolas Denis.

Si cette solution est convaincante elle pourrait être retenue par le Crédit agricole. De son côté, la Banque populaire teste aussi ce genre d'application.

En résumé

Les attaques de *phishing* ont épargné la France par rapport à d'autres pays comme les Etats-Unis, l'Australie et le Brésil. En limitant les possibilités de virements, les établissements financiers français ont limité la casse. Pour l'instant ! Car les escrocs ont de l'imagination et savent contourner les obstacles. Le recours à des réseaux de « mules » démontre que le système bancaire n'est pas infaillible. Cette nouvelle adaptation du célèbre Cheval de Troie devrait inciter les groupes bancaires à redoubler d'efforts et à sensibiliser de façon plus pragmatique leurs clients.



14

Les vigies d'Internet

En 1989, un homme de 22 ans est arrêté après avoir visité les systèmes informatiques de la Direction des Télécoms Réseau National, filiale de France Télécom, ainsi que quelques autres gros systèmes informatiques français (EDF, Aérospatial, CEA, etc.). C'est la première arrestation importante pour la police française. La même année, la Direction de la Surveillance du Territoire (DST) arrête une cinquantaine de hackers français. Les autorités recherchent un individu un peu trop curieux puisqu'il visitait les systèmes informatiques d'importantes entreprises françaises comme Thomson. Des informations récupérées lors d'infiltrations auraient été récupérées par les services secrets allemands...

Depuis, les arrestations font moins souvent la Une des journaux. Une vaste escroquerie a néanmoins été révélée début juillet 2006. Cette affaire concernait le site eBay. Fin juin, la police judiciaire parisienne a arrêté six suspects. La brigade des fraudes aux moyens de paiement (BFMP) a estimé que le préjudice est, en l'état des investigations, de 175 000 euros mais il pourrait dépasser les 300 000 « à terme ». Ce réseau aurait fait 375 victimes dont les numéros de cartes bancaires ont été débités indûment. Certains suspects travaillant à la SNCF et à la RATP auraient donc récupéré toutes les données bancaires lorsque la personne passait à leur guichet... Une fois en possession de ces informations, les présumés escrocs se connectaient sur le site d'enchères et achetaient très rapidement, dans un délai de moins de 36 heures, des appareils électroniques. Et ensuite, ils les revendaient sur le même site !

De nombreuses autres affaires sont en cours mais elles sont traitées de façon plus discrète (de là à imaginer que certains pirates pris sur le fait collaborent avec certaines entités officielles...). Autres raisons de cette absence de publicité : plusieurs accords à l'amiable sont obtenus et enfin les sites Internet sensibles (ceux des administrations et des grandes entreprises) sont mieux protégés. Il y a aussi le fait que les pouvoirs publics français ont mis en place différentes structures spécialisées.

Cette diversité de services est aussi un inconvénient pour les PME ou les particuliers car ils ne savent pas toujours à qui s'adresser... Cette situation pourrait néanmoins évoluer. Comme les autorités britanniques, les pouvoirs publics français envisageraient de mettre en place un site Internet sur lequel tout le monde pourrait signaler un incident informatique.



Figure 14-1 — La sécurité informatique est traitée par de nombreux organismes en France.



14.1.1 La DCSSI

Placée sous l'autorité du Secrétaire général de la Défense nationale, et donc du Premier ministre, la Direction centrale de la sécurité des systèmes d'information (DCSSI) peut être définie comme le rouage essentiel de la sécurité informatique de notre pays. Héritière du Service central de la sécurité des systèmes d'information, elle a été instituée par décret le 31 juillet 2001.

Dirigée par Patrick Pailloux, un polytechnicien de 40 ans, la DCSSI a pour mission de :

- Contribuer à la définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information.
- Assurer la fonction d'autorité nationale de régulation pour la SSI (sécurité des systèmes d'information) en délivrant les agréments, cautions ou certificats pour les systèmes d'information de l'État, les procédés et les produits cryptologiques employés par l'administration et les services publics, et en contrôlant les Centres d'évaluation de la sécurité des technologies de l'information (CESTI).
- Évaluer les menaces pesant sur les systèmes d'information, donner l'alerte, développer les capacités à les contrer et à les prévenir (COSSI)
- Assister les services publics en matière de SSI
- Développer l'expertise scientifique et technique dans le domaine de la SSI, au bénéfice de l'administration et des services publics
- Former et sensibiliser à la SSI (Centre de formation à la sécurité des systèmes d'information — CFSSI). Outre de nombreux stages, d'une durée allant de quelques jours à trois semaines, elle assure la scolarité du Brevet d'Études Supérieures de la Sécurité des Systèmes d'Information (BESSSI), d'une durée de deux ans. Cette formation de très haut niveau, dispensée à des personnels habilités de la fonction publique (essentiellement de la Défense), est la seule formation en France traitant de la SSI opérationnelle.

Selon un parlementaire¹, le budget 2005 du SGDN est de 56,7 M€ avec un effectif de 353 personnes, parmi lesquelles 110, en majorité de formation scientifique et technique, sont affectées à la DCSSI.

La grande force de la DCSSI est de disposer d'un Centre opérationnel de la sécurité des systèmes d'information (COSSI). Installé près des Invalides, à Paris, le COSSI a été créé en octobre 2003 à la suite de la mise en place de Piranet. Ce plan de réaction « en cas d'attaque informatique terroriste d'ampleur » contre l'Etat a été développé comme d'autres plans de réaction à la suite des attentats du 11 septembre 2001.

1. « La sécurité des systèmes d'information : Un enjeu majeur pour la France ». Rapport du Député Pierre Lasbordes. Novembre 2005.



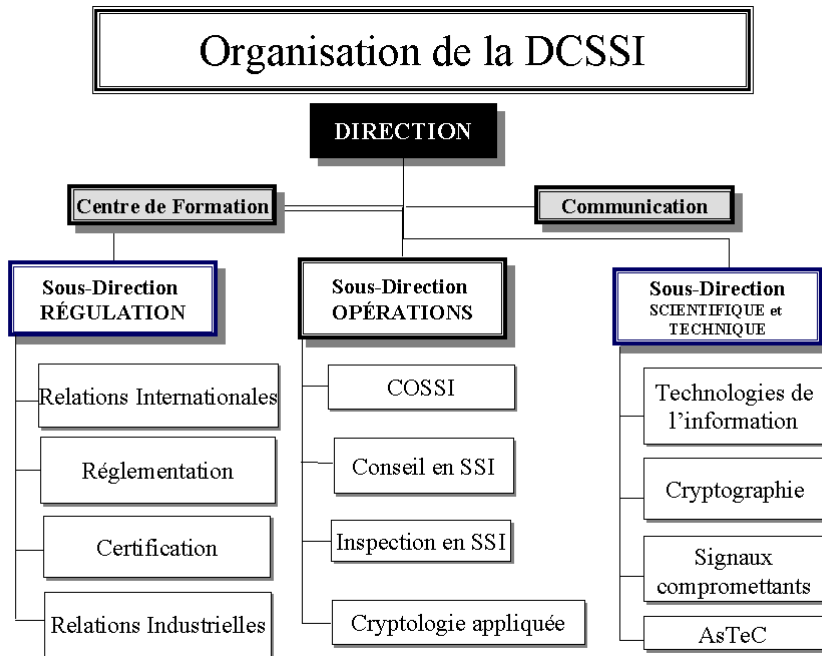


Figure 14-2 – Organisation de la DCSSI.

« C'est le seul centre opérationnel de veille 24h/24, sept jours sur sept, en Europe, rappelle avec fierté Philippe Brandt, chef du COSSI. D'autres pays vont suivre cet exemple. Singapour devait lancer le sien durant l'été 2006 et les Allemands et les Coréens du Sud songent aussi à créer une entité équivalente ».

Composé de vingt-quatre personnes, quasiment toutes ingénieurs en informatique, le COSSI veille sur les réseaux et les systèmes d'information de l'Etat et des services publics. Par exemple, plus de 500 sites Internet officiels sont surveillés toutes les heures. Objectif : vérifier qu'ils n'ont pas été « défigurés » (defacement)¹ ou « testés » en vue d'une attaque programmée.

« Les nuits et week-end, une personne assure la veille et trois autres sont placées en astreinte, précise Philippe Brandt. Mais nous ne les avons encore jamais rappelées en pleine nuit pour l'instant car il n'y a encore jamais eu d'alerte pendant ces créneaux de veille ».

Mais sa mission ne se limite pas à la veille. Officiellement, il est chargé d'assurer la coordination interministérielle des actions de prévention et de protection face

1. Selon différentes sources, il y a environ 2000 actes de *defacement* (modification de la page d'accueil ou de certains éléments écrits ou visuels d'une page) en France par an. Ces attaques ne visent pas uniquement les sites des administrations (voir chapitre 1).

aux attaques sur les systèmes d'information de l'Etat. Il est composé d'une unité de Conduite & Synthèse (CEVECS) et d'une unité technique, le CERTA (centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques). Chacune de ces unités regroupe une dizaine de personnes.

Le COSSI intervient aussi sur deux points : la conduite d'une crise (c'est-à-dire suite à un incident informatique) et la conduite préventive.

Concernant le premier point, il se focalise sur deux aspects : comment l'attaque a-t-elle été techniquement réalisée et quels sont les réseaux susceptibles d'être une cible (et *a fortiori* comment assurer une protection efficace). Le COSSI ne traite donc pas la source à l'origine d'une attaque, cet aspect étant réservé à d'autres services gouvernementaux. La charge de travail est plus importante aujourd'hui car « nous avons de plus en plus d'incidents et des attaques de plus en plus sophistiquées. Il y a toutefois encore très peu d'attaques majeures », constate le responsable du COSSI. Lorsqu'un incident informatique est signalé par un ministère ou une administration, le COSSI lance une expertise technique et répond à trois questions principales :

- s'agit-il d'une attaque majeure ciblant un ministère ?
- s'agit-il d'un incident qui peut toucher d'autres sites gouvernementaux ?
- s'agit-il simplement d'une panne ou d'une mauvaise manipulation ?

« L'important est de hiérarchiser les impacts. Par exemple, le blocage d'une application majeure comme par exemple celle des cartes grises doit être rapidement géré », précise Philippe Brandt.

Lorsque l'origine de l'incident est déterminée, le COSSI travaille avec les autorités compétentes. Les responsables sécurité du ministère concerné effectueront les manipulations nécessaires.

Concernant le second point, c'est-à-dire la prévention, le COSSI aide les ministères à mettre en place des protections et organise des exercices théoriques et réels tous les ans.

Pour anticiper les attaques et l'arrivée de nouveaux codes malveillants, le centre a installé différentes sondes qui attrapent tout ce qui traîne à certains points de la toile. « Nous voyons ainsi en temps réel ce qui se passe », déclare Philippe Brandt. Ces sondes détectent les comportements anormaux et lancent immédiatement une alerte en cas de détection d'un tel comportement.

Toujours à propos d'anticipation, le COSSI informe l'ensemble des ministères dès qu'une vulnérabilité est repérée. Si un *proof-of-concept* (le prototype d'un code malveillant en quelque sorte) est découvert, le centre le récupère afin de tester son impact. Il informe aussitôt les ministères et les autorités par un flash spécial sur le risque potentiel. « Avant on comptait cinq jours entre la découverte d'une vulnérabilité et son exploitation, maintenant c'est quelques jours, voire quelques heures », assure le chef du COSSI.



Le CERTA

Le Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques a été créé en 1999 au moment du présupposé « bug de l'an 2000 ». Il a une mission préventive : repérer les vulnérabilités et les traiter. Chaque jour, ce site (www.certa.ssi.gouv.fr) publie une moyenne de cinq « avis de vulnérabilité » détectés sur des logiciels et accompagnés des moyens de s'en protéger. Plus de 1500 documents (avis, alertes, notes d'information, recommandations) sont disponibles. Une note d'information du Certa liste ainsi les « bons réflexes en cas d'intrusion sur un système d'information ». Une recommandation datant de juin 2005 énumère les moyens de se protéger contre une « attaque ciblée par cheval de Troie ». Autant d'informations qui constituent une référence pour les systèmes et les réseaux publics ou privés.

Le CERTA collabore avec le FIRST¹, le TF-CSIRT², les trois CERT³ français et la dizaine de CERT gouvernementaux d'autres pays.

14.1.2 Le Ministère de l'Intérieur

Il existe plusieurs structures. La plus emblématique est la Direction de la surveillance du territoire. Assurant une veille permanente dans le domaine des TIC, la DST a aussi une activité de prévention qui s'exerce dans quatre domaines : la téléphonie, la criminalité informatique, les satellites et les matériels soumis à une réglementation (art R226 du Code pénal). Elle est donc en relation avec les opérateurs de Télécom et les sociétés de SSI (qui commercialisent des matériels pouvant porter atteinte à la vie privée) et les sociétés de cryptologie. Les informations concernant cette entité étant évidemment très limitées nous présenterons donc les autres structures chargées de la cybercriminalité.

14.1.2.1 L'OCLCTIC

Créé en mai 2000, l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication est une structure à vocation interministérielle (il regroupe donc des policiers et quelques gendarmes) placée au sein de Direction Centrale de la Police Judiciaire (DCPJ). Il lutte contre les auteurs d'infractions liées aux TIC, enquête à la demande de l'autorité judiciaire, centralise et diffuse l'information sur les infractions à l'ensemble des services répressifs (DCPJ, Douanes, Gendarmerie). A noter que la Préfecture de Police de la capitale dispose d'un service similaire, la Brigade d'enquêtes sur les fraudes aux technologies de l'information. Dirigée par le commissaire principal Yves Crespin, la BEFTI (une trentaine de personnes) a un rayon d'action limité à l'Île de France alors que celui de l'OCLCTIC (35 personnes) est national.

1. Forum of Incident Response and Security Teams. www.first.org

2. Task Force - Computer Security Incident Response Teams ou Coordination européenne des organismes de réponses aux incidents de sécurité.

3. Computer Emergency Response Teams (www.cert.org). Il y en a trois : CERT-A (Administration), CERT-IST (entreprises privées) et CERT-RENATER (Enseignement, universités...).



Mais cette « répartition » n'exclut pas l'extension de compétence au niveau national ou international dans les affaires de haute technicité initiées par la BEFTI.

La BEFTI, ex SEFTI devenu Brigade en 2000, dispose de 24 enquêteurs dont 17 travaillent principalement sur les affaires (environ 300 par an) visant l'intégrité des réseaux et non pas, à l'exception de quelques infractions spécifiques, la délinquance véhiculée par Internet. En effet, au sein de la Préfecture de Police de Paris, chaque Brigade de Police Judiciaire dispose de groupes spécialisés dans son domaine de compétence. Par ailleurs, au sein de la BEFTI, un Centre d'Assistances. Il est composé de 7 policiers spécialistes qui d'assistent techniquement (à tous les stades des investigations) toute direction du ressort de la Préfecture de Police ou magistrat qui en ferait la demande. Ce concours correspond généralement à l'exploitation du contenu d'un ordinateur dans un temps limité à la durée d'une opération de Police ou délai d'une garde à vue. Cette nécessité d'assistance suit une courbe exponentielle d'année en année.

Si les effectifs de la BEFTI ont très sensiblement été renforcés depuis 2 ans (2 à 3 personnes) et ses moyens matériels sont de meilleure qualité, son budget de fonctionnement a été revu à la baisse.

Successeur de la Brigade Centrale de Lutte contre la Criminalité Informatique, l'OCLCTIC est dirigé depuis 2006 par le commissaire principal Fabien Lang, qui succède à Catherine Chambon. Environ 150 dossiers sont traités chaque année. « Nos agents sont avant tout des experts de la procédure pénale », précise-t-elle. Ne trouvant pas toujours sur le marché les logiciels ad hoc, et ne disposant de toute façon pas forcément des budgets pour les acquérir, les policiers de l'informatique se font volontiers développeurs. Des solutions pour traiter, dans des conditions satisfaisantes, les données fournies par les opérateurs télécoms, pour rendre lisibles des images floues sur un film d'une vidéo de contrôle, en passant par les analyses techniques des fréquences du spectre vocal sur une bande-son afin de s'assurer de l'identité de la personne qui parle sur un enregistrement...¹

Des recherches qui coûtent cher

Lorsque la police ou la Gendarmerie demande à un opérateur de téléphonie mobile de localiser un abonné, cette requête est facturée quelques euros. C'est la même chose pour l'Internet. Dans ce cas, il s'agit d'identifier une adresse IP. Selon le site Zataz², ce genre de demande d'information coûtait 12 euros chez Club-Internet, 17 euros chez Noos, 20 euros chez Free, 40 euros chez Orange et 55 euros chez Alice. Ces coûts étant jugés exorbitants par les pouvoirs publics, un accord aurait été trouvé : chaque recherche serait facturée environ 0,99 euro. Chaque requête formulée auprès d'un fournisseur d'accès, interlocuteur incontournable de l'enquêteur, doit faire l'objet d'une autorisation cas par cas de la part d'un magistrat. Cette particularité est un frein certain à un type d'enquête dont la progression ne se conçoit que par voie de réquisition.

1. Magazine 01 Informatique du 02/02/2005.

2. www.zataz.com du 7/06/06.



14.1.3 Le Ministère de la Défense

Ce ministère a plusieurs priorités. Il doit doter l'État d'équipes et de laboratoires capables de satisfaire l'ensemble des besoins gouvernementaux. On peut citer l'Ecole Supérieure et d'Application des Transmissions (ESAT) à Rennes, et en particulier, son laboratoire de cryptologie et de virologie dirigé par l'un des deux auteurs de ce livre. Il doit aussi analyser les menaces étrangères sur les systèmes d'information. Cette fonction est assurée par la Direction générale de la sécurité extérieure (DGSE). De son côté, la Direction de la protection et de la sécurité de la défense (DPSD) assure de son côté une veille sur la sécurité des industries de défense. Les Armées et la DGA (Direction générale de l'armement) possèdent chacune une entité constituée de spécialistes de la SSI, chargée en particulier de procéder aux audits des systèmes d'information dépendant de l'autorité qualifiée correspondante.

En matière de sécurité informatique, la Gendarmerie joue aussi un rôle de premier plan. Dès 1998, elle a créé le département de lutte contre la cybercriminalité au sein du Service technique de recherches judiciaires et de documentation (STRJD). Elle s'appuie aussi sur les compétences de l'Institut de recherche criminelle de la gendarmerie (IRCGN) et des services de la sous direction de la police technique et scientifique de la police judiciaire basés à Ecully.

Créé en 1987, cet institut a reçu de la direction générale de la gendarmerie nationale quatre missions principales :

- Effectuer, à la demande des unités et des magistrats, les examens scientifiques ou les expertises nécessaires à la conduite des enquêtes judiciaires.
- Apporter en cas de besoin aux directeurs d'enquêtes, le soutien nécessaire au bon déroulement des constatations, principalement par la mise à leur disposition de personnel hautement qualifié disposant de matériels adaptés et spécialisés.
- Concourir directement à la formation des techniciens en identification criminelle et à l'information des enquêteurs.
- Poursuivre dans tous les domaines de la criminalistique les recherches nécessaires au développement des matériels et des techniques d'investigation criminelle.

« Nous disposons aussi d'une cellule de veille spécialisée sur la fraude et la veille technologique pour toutes les arnaques sur Internet »¹, ajoute le Capitaine Eric Freyssinet qui dirige le laboratoire de la Gendarmerie Nationale (recherche de la preuve numérique dans les enquêtes de police).

Il existe deux types d'enquêteurs au sein de la Gendarmerie. Il y a tout d'abord quelque 160 enquêteurs qui ont suivi une formation de six semaines. Il y a ensuite des enquêteurs IRCGN. Avec des experts en analyse scientifique des preuves, ils recherchent des traces, récupèrent des données, analysent le fonctionnement de *key-loggers* bancaires et les dispositifs de récupération de caractéristiques de carte bancaire en vue d'une copie.

1. Extrait d'une interview parue dans le numéro 4 de la revue Magsecur.



Ces deux types d'enquêteurs ont d'abord suivi la formation de gendarme « traditionnel » avant d'intégrer les équipes spécialisées en cybercriminalité. D'où un recrutement plus compliqué.

Adresses utiles

La Gendarmerie : il faut contacter le Service Technique de Recherches Judiciaires et de Documentation (STRJD) : judiciaire@gendarmerie.defense.gouv.fr

BEFTI : Son territoire est Paris et la petite couronne. 122, rue du Château des Rentiers. 75013 Paris. Tel : 01 55 75 26 19.

OCLCTIC : cet organisme relève du Ministère de l'Intérieur. 101 rue des Trois Fontanots. 92000 Nanterre. Tel : 01 49 27 49 27.

14.2 LES ORGANISMES ÉTRANGERS

Si le niveau de protection informatique d'un Etat se mesure aux effectifs de ces entités spéciales, alors la France n'est pas bien protégée ! Aux Etats-Unis, la Division Information Assurance de la NSA compte environ 3000 personnes. En Allemagne, le Bundesamt für Sicherheit in der Informationstechnik (BSI) en emploie 450. Enfin, au Royaume-Uni, le Communications Electronics Security Group (CESG) a aussi 450 agents. Rien à voir avec les quelque 110 membres de la DCSSI.

En réalité, ce comparatif n'est pas vraiment significatif des rapports de force entre autorités et escrocs. La France dispose d'une palette très large de services spécialisés et compétents. La différence fondamentale se trouve plutôt au niveau de la sensibilisation des victimes potentielles, qu'il s'agisse de particuliers ou d'entreprises privées et publiques. Plusieurs spécialistes rencontrés estiment en effet que les anglo-saxons sont un peu plus sensibilisés que nos compatriotes.

14.2.1 Les Etats-Unis

Depuis les attentats de septembre 2001, la sécurité est devenue une priorité absolue de la Maison blanche. Cela concerne entre autre les réseaux informatiques et télécoms. Le Federal Bureau of Investigation (F.B.I), les Douanes, l'US Air Force, tous ont mis en place des unités spécialisées dans les technologies de l'information. Un domaine très vaste qui va du piratage de musique ou de vidéo, en passant par la surveillance électronique de nombreux individus ou groupes considérés comme dangereux pour la nation, sans oublier les escroqueries en tous genre qui se multiplient sur le Web.

L'organisme le plus connu (ou plutôt celui qui fait le plus fantasmé...) est la National Security agency (www.nsa.gov). Créée en 1952, la NSA a pour mission de protéger les systèmes d'information des Etats-Unis et d'obtenir des renseignements à partir d'interceptions et des écoutes d'autres pays. C'est donc à la fois une agence de

cryptologie et une agence de renseignements. Elle emploierait quelque 100 000 personnes (voir chapitre 15) pour toute la chaîne de transmission (interception, écoute, décryptement, analyse, traduction...). Son budget n'est pas connu.

L'autre service est le FBI. Les « Fédéraux » ont décroché quelques beaux trophées. Pour démanteler des réseaux illicites, le FBI n'hésite pas à se faire passer pour des pirates. Ce fut le cas en octobre 2005. L'organisme fédéral a mis fin aux agissements d'un important groupe de contrefacteurs de musique connus sous le pseudonyme de 4CHOON. Pour s'échanger leurs chansons, cette bande avait pris le contrôle des serveurs sur lesquels il fallait montrer patte blanche pour y accéder. Le FBI a donc dû se faire passer pour des pirates pour infiltrer ce réseau et mettre la main dessus... Les Fédéraux exploitent aussi les compétences de pirates qu'ils arrêtent. C'est le cas par exemple de Justin Petersen. Arrêté en 1989 pour s'être introduit sur le réseau de TRW, il a été relâché pour aider le FBI à pister et arrêter des pirates.

14.2.2 Le Royaume-Uni

La sécurité informatique revêt un aspect particulier outre-Manche¹. Depuis 2003, le Royaume-Uni s'est doté d'une stratégie nationale qui met l'accent sur le partenariat avec le secteur privé. Le pays a aussi mis l'accent sur l'information des entreprises et des usagers.

Créé en 1999, le National Infrastructure Security Co-ordination Centre s'appuie sur l'UNIRAS (CSIRT gouvernemental) pour fournir aux opérateurs des infrastructures critiques des avis techniques, des informations sur les menaces, les vulnérabilités et les niveaux d'alerte.

Comme les autres Etats, le pays a aussi créé différents organismes spécialisés. Il y a par exemple le Central Sponsor Information Assurance (CSIA) et le Communications and Electronic Security Group (CESG). Ce dernier est l'équivalent de la DCSSI en France.

14.2.3 L'Allemagne

En 2005, le pays a adopté un plan national pour la protection des infrastructures d'information. Il comporte trois objectifs principaux :

- la prévention afin de protéger convenablement les infrastructures ;
- la préparation afin de répondre efficacement en cas d'incidents de sécurité informatique ;
- le maintien et le renforcement des compétences allemandes dans le domaine SSI.

1. Source : « La sécurité des systèmes d'information : Un enjeu majeur pour la France ». Rapport du Député Pierre Lasbordes. Novembre 2005.



Sa mise en oeuvre s'appuie notamment sur le BSI (www.bsi.bund.de), homologue de la DCSSI. Le BSI a aussi créé un standard professionnel en 1993, une « IT Base-line Protection » (les bases de la protection d'un système d'information) remise à jour constamment qui est devenu un standard pour l'industrie. C'est un ensemble de bonnes pratiques qui permettent de sécuriser un système.

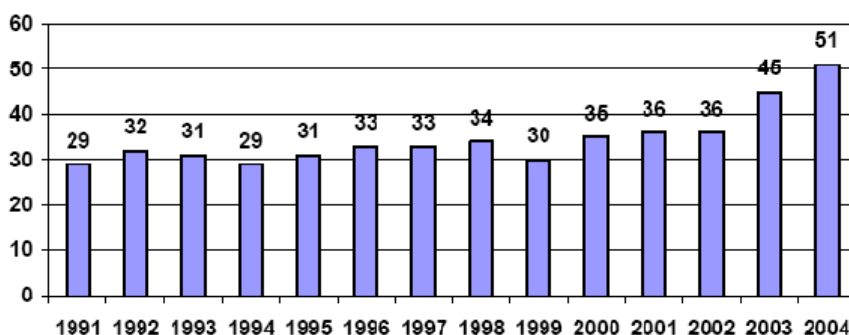


Figure 14-3 — Budget de la BSI.

En résumé

En décembre 1907, Georges Clemenceau dote la France des « Brigades régionales de police mobile », plus connues sous l'expression des « Brigades du tigre ». Pour la première fois, la police dispose de voitures et de moyens (coordination des informations entre la police et la Gendarmerie, dossiers sur les criminels, anthropométrie...) lui permettant de rivaliser avec les bandits. Un siècle plus tard, la France a su s'adapter à l'évolution de la criminalité qui a trouvé avec Internet un nouveau territoire à conquérir. Des ingénieurs en informatique côtoient des policiers et des gendarmes. Les ordinateurs portables ont remplacé les automobiles Renault EK. Mais la donne ne semble pas avoir beaucoup changé : les escrocs ont toujours un (petit) coup d'avance...

Creative Commons BY-NC-ND



Les États qui copient les pirates

Les technologies de l'information et de la communication représentent un formidable potentiel. Mais comme tout potentiel de cette nature, dont la portée est désormais mondiale, la surveillance des États est permanente. Au fond, le cyberspace, dans son acceptation la plus large, est un nouvel espace qu'il convient non seulement de protéger, mais également de contrôler. Or, la notion de contrôle est difficile à définir et à cerner même pour un État : comment s'assurer que les vigiles de cet espace, dont le rôle est de protéger les usagers ou habitants, ne vont pas devenir « corsaires », voire des pirates, pour une raison ou une autre. Là est tout le problème. En particulier, s'il existe un « droit » de la guerre et des conflits armés (la Convention de Genève par exemple), il n'en existe pas de véritable pour le monde virtuel. Résultat : chaque pays, en fonction de sa position plus ou moins dominante sur le sujet, est tenté (quand il ne l'a pas déjà fait...) de définir ses propres règles et de les appliquer.

Le meilleur exemple est sans doute la conception américaine sur le sujet. Etendant la notion de territorialité du géographique au numérique, ce pays considère que toute agression contre un serveur de nom de domaine américain est un acte de guerre comparable à une agression de son territoire national et de ce fait, est libre de prendre toutes les mesures adéquates : « ...les Etats-Unis considèrent toute adresse Internet libellée en .US comme faisant partie du territoire américain et s'autorisent des représailles en cas d'attaques informatiques », révèle le lieutenant-colonel Tarbouriech, de la cellule programme interarmées de l'état-major des Armées¹. Rappelons-nous que le réseau Internet, créé en 1971 sous le nom Arpanet à la demande des militaires du Pentagone, est depuis géré par l'ICAN. Cet organisme américain en contrôle tous les rouages, ce qui n'a pas manqué d'être souligné lors de la dernière conférence internationale

1. *Cyberabordage, Comment combattre les hackers*, Armées d'aujourd'hui, numéro 302, juillet-aout 2005.

sur le sujet à Tunis en 2006. Or, depuis quelques années — et en particulier depuis le 11 septembre 2001 — les conceptions ont changé. Une loi comme le *Patriot Act*, officiellement instituée pour lutter contre le terrorisme, a connu des débordements qui préoccupent actuellement non seulement la justice américaine et la société américaine dans son ensemble mais également le monde entier, puisque les récentes affaires d'écoutes plus ou légales concernaient des ressortissants étrangers, sur leur propre sol national. Mais d'un autre côté, des groupes terroristes comme le Hezbollah ou Al Qaida disposent de capacités et de personnels rompus aux techniques de « cyber-guerre » ou de « cyber-terrorisme ».

Alors nouvel art de la guerre, nouvelle forme de renseignement ou nouvelle « éthique » ? Les pays sont-ils tentés d'utiliser les armes et les moyens des pirates et autres hackers, pour la raison d'État ? Techniquement, cela ne représente aucune difficulté. Entre recruter parmi l'élite universitaire ou embaucher quelques pirates repentis, les États ne sont pas en mal de constituer des équipes importantes et extrêmement compétentes. Le problème se situe avant tout au niveau politique. C'est une question de volonté et de choix qui relève avant tout d'une vision de société. Nous sommes loin de la phrase de Edgar J. Hoover¹ qui affirmait qu'un « gentlemen n'espionne pas la correspondance des autres ». Depuis, le maccarthisme, le Watergate et les débordements sous couvert du *Patriot Act* ont montré que certains États ne reculaient devant aucun moyen, fussent-ils ceux des pirates, pour exercer certaines fonctions régaliennes pour ne pas dire « réganiennes² ». À commencer par les États-Unis, modèle dans bien des domaines. Mais la transparence américaine, presque naïve est peut-être l'arbre qui cache la forêt. Elle permet au moins d'avoir quelques informations, et de là de se faire une idée. Malheureusement, d'autres pays n'ont pas la même attitude et cachent soigneusement toute activité de ce type. Espionnage de ses propres citoyens, guerre économique, espionnage industriel, atteintes médiatique aux personnes, guerre informatique militaire... tout l'attirail des pirates est disponible.

15.1 L'ÉTAT DES FORCES

Il n'existe que très peu d'informations sur l'utilisation de la guerre informatique offensive par les États. Discretion oblige. Encore moins quand les comportements de *hackers* sont le fait de personnels gouvernementaux. Il y a fort à parier que, pour les pays démocratiques du moins, le recours à des mercenaires — des pirates plus ou moins manipulés, des sociétés « de service » spécialisées, leur permet de garder les mains propres. L'état des lieux que nous présentons a privilégié l'exactitude des faits sur l'exhaustivité³.

1. Directeur du FBI de 1924 à 1972.

2. C'est en effet sous le mandat du président Reagan, que le renseignement américain a commencé à passer du renseignement purement stratégique et militaire vers le renseignement économique, incluant l'espionnage de sociétés étrangères.

3. Les données citées ici proviennent, pour la plupart, de deux ouvrages : Eric Filiol, *Les virus informatiques : théorie, pratique et applications*, Springer Verlag 2004 et Cédric Thévenet, *Cyber-terrorisme, mythe ou réalité*, Mastère CESD, Université de Marne-la-Vallée, 2005.



15.1.1 Les Etats-Unis

La philosophie américaine peut être résumée par la phrase du général John Bradley, ancien responsable du Computer Network Attack (CNA) : « ... nous passons plus de temps sur les projets d'attaques informatiques que sur les réseaux de défense parce que beaucoup de personnes — à un niveau très élevé — sont intéressées. » Ainsi, en 2002, George Bush a signé la directive sur la sécurité nationale numéro 16, ordonnant au gouvernement américain de préparer des plans nationaux de lutte électronique offensive contre des ennemis potentiels (ce qui en dit long quand on sait que cette définition est à géométrie variable).

En mars 2005, devant le Sénat américain, l'U.S. Strategic Command (Stratcom) révélait l'existence du Joint Functional Component Command for Network Warfare (JFCCNW). Cette unité composée de hackers, au service de l'armée américaine, a pour mission prioritaire de protéger les réseaux du ministère américain de la Défense, mais également de participer activement au CNA. Au cours de l'audience au Sénat américain, le porte-parole de Stratcom ne laissait aucun doute sur la force de frappe de l'équipe de hackers recrutés par l'armée américaine : « pour des raisons de sécurité, nous ne pouvons donner aucun détail. Toutefois, étant donné la dépendance de plus en plus forte aux réseaux informatiques, toute capacité informatique offensive ou défensive est grandement souhaitable ».

Il est dès lors difficile de dire à quoi peut servir cette force — nouvelle forme de guerre, d'espionnage ou œuvre de basse police — et quelles collaborations elle entretient avec les agences comme la NSA dont les capacités en matière d'interceptions, de décryptement et d'écoutes sont prodigieuses. Il est clair que des laboratoires comme l'IWAR à West Point, le Naval War College à Monterey, des infrastructures comme le réseau RINSE, sont impliqués et qu'il en existe bien d'autres. Enfin, nombreux sont les cas où des pirates repentis ont été et sont « utilisés » par des agences gouvernementales américaines.

Quelques cas de débordements sont déjà connus. Les Etats-Unis les légitiment par la lutte contre le terrorisme. En 2001, les services américains ont largement espionné les flux bancaires internationaux. Le quotidien *Le Monde*¹ révèle que l'Agence centrale de renseignement (CIA) a passé au crible, sous le contrôle du département du Trésor, des dizaines de milliers de transactions financières impliquant des Américains et des étrangers, dans le cadre d'un programme clandestin lancé au lendemain des attentats du 11 septembre 2001 aux Etats-Unis.

En décembre 2005, rapporte le quotidien du soir, « le *New York Times* révélait un programme secret de la National Security Agency (NSA) comprenant, aux Etats-Unis, sans l'aval d'un juge, des interceptions de communications téléphoniques et de messages électroniques de personnes suspectées d'être en relation avec des membres d'Al-Qaïda à l'étranger. En mai, *USA Today* affirmait que la NSA avait aussi collecté auprès de compagnies de téléphone les listes de dizaines de millions d'appels d'Américains ordinaires. »

1. *Le Monde*, 24/6/2006.



Toujours rapporté par *Le Monde*, Michael Hayden — nommé en mai 2005 à la tête de la CIA, après avoir dirigé la NSA de 1999 à 2005 — précisait : « si j'ai mis en place ce programme (d'écoutes téléphoniques) en octobre 2001, c'est parce que ma responsabilité est de défendre la nation et la sécurité de la République. » L'existence du Terrorist Finance Tracking Program (Programme de traque du financement du terrorisme) a été confirmée en juin 2006, par le département du Trésor. Il affirme qu'il est limité à la surveillance des opérations bancaires de personnes soupçonnées de liens avec Al-Qaïda.

Mais un tel programme ne peut pas exister sans la collaboration du réseau de la Society for Worldwide Interbank Financial Telecommunication (Swift), une coopérative interbancaire dont le siège se trouve en Belgique, centre nerveux des transactions financières mondiales par lequel transitent 6 000 milliards de dollars par jour. Elle fournit ses services à 7 800 établissements financiers de plus de 200 pays. Par réquisition administrative, sans l'aval d'un juge, le département du Trésor obtient chaque jour des données de Swift. L'existence de cette surveillance secrète est connue depuis le début par les banques centrales du G10 (Canada, Allemagne, France, Italie, Japon, Pays-Bas, Suède, Suisse, Angleterre, Etats-Unis, ainsi que par la Banque centrale européenne) et les pays alliés des Etats-Unis dans la guerre contre le terrorisme. Mais, comme avec les écoutes clandestines de citoyens américains menées sans l'autorisation de la justice par la National Security Agency (NSA), l'administration Bush semble avoir délibérément contourné les lois protégeant les libertés individuelles. Le journal *Le Monde* révèle également que « le gouvernement avait demandé au *New York Times* de ne pas publier son article, mais le quotidien a refusé. »

15.1.2 La Russie et les anciens pays du bloc communiste

Parler du renseignement des ex-pays de l'Est n'est pas plus facile aujourd'hui qu'hier. Il est cependant clair que ces pays s'intéressent depuis très longtemps aux technologies de l'information. Outre la volonté, ces Etats (en premier la Russie et l'Ukraine) possèdent un extraordinaire vivier de matière grise. Il est à peu près certain qu'à l'heure actuelle ils comptent les meilleurs spécialistes dans les techniques de piratage et de hacking. Et ce genre de savoir-faire ne naît pas spontanément. Que ce soit le KGB (8ème direction principale ou la direction T, par exemple), les services bulgares (suspectés de soutenir une équipe de programmeurs de virus connue sous le nom de *Bulgarian Virus Factory*), roumains (services E, T et D) ou ceux de la Stasi (directions principales III, XIX et XXVI)¹, tous ces pays ont utilisé ces techniques pour espionner l'Occident. Il serait très surprenant que ces activités aient cessé...

1. La Stasi a notamment été suspectée avec le KGB de manipuler et d'instrumentaliser les membres du fameux Chaos Computer Club de Berlin.



15.1.3 Les deux Corées

Ces deux pays ont depuis les années 90 manifesté leur intérêt pour la cyber-guerre. La Corée du Sud annonçait officiellement, en 2004¹, que sa voisine du nord s'était dotée d'une composante militaire de guerre informatique de 500 hommes. La Corée du Nord, elle, s'équipe, s'entraîne et aurait déjà mené des opérations réelles, notamment contre les réseaux de la Corée du Sud. Selon des responsables américains et sud-coréens, la Corée du Nord entraînerait secrètement une armée de hackers au cyberterrorisme. Pour Cho Kyong-won (agence France-Presse du 7 juin 2003), expert pour la plus importante société sud-coréenne de sécurité informatique, AhnLab, ce n'est pas parce que leur pays est pauvre que ces combattants du cyberspace sont incompetents ou dépassés. « Il se peut qu'ils soient bons », estime-t-il. En 2003, le général Song Young-Geun, qui commande le Département sud-coréen de sécurité de la défense, a averti les autorités de Séoul que leur voisine du nord lâchait dans la nature 100 hackers par an, sans pouvoir cependant en apporter la preuve.

En 2002, le conseiller en technologie pour la Maison Blanche, Richard Clarke, avait révélé à une commission parlementaire américaine que la Corée du Nord, (mais aussi l'Irak et l'Iran, ainsi que la Chine et la Russie), entraînaient des jeunes gens aux subtilités du sabotage informatique. « Qu'il s'agisse d'élaborer des virus informatiques, des missiles ou des bombes nucléaires, il faut les mêmes aptitudes informatiques de base », estime un autre chercheur d'AhnLab, Jung Kwang-Jin. De plus, il semblerait que Kim Jong Il se soit récemment pris de passion pour les ordinateurs. Au cours de ses rares visites à l'extérieur (en Chine et en Russie en 2000), il a visité des laboratoires informatiques et des centres de haute technologie. Dès son retour, il a ouvert des laboratoires dans son pays et rendu l'enseignement de l'informatique obligatoire. « Leur développement en matière de savoir-faire informatique est comparable à celui des pays développés », estime Park Chan-mo, un scientifique sud-coréen qui enseigne à l'université Pohang de sciences et de technologie, qui travaille en collaboration avec la Corée du Nord. Des informations précises sur l'étendue des capacités de la Corée du Nord en matière de diffusion de virus et de pénétration des systèmes informatiques seraient d'une importance stratégique certaine pour les Etats-Unis. La Corée du Sud, qui est l'un des pays les plus informatisés du monde (plus de 70 % des ménages ont un accès à Internet à haut débit), craint aussi pour sa sécurité. En janvier, une infection virale a paralysé le réseau Internet national pendant plusieurs heures.

15.1.4 La Chine et l'Asie

Depuis le début des années 90, la Chine développe ses capacités en cyber-guerre. La doctrine militaire chinoise intègre la cyber-attaque comme une composante de sa stratégie visant à défaire un ennemi mieux équipé ou supérieur en nombre. Lors d'une allocution devant le congrès, le directeur de la CIA, George J. Tenet², a affirmé que la

1. Agence France Presse, 4 octobre 2004.

2. George Tenet, Testimony Before the Senate Committee on Government Affairs, Juin 1998.



Chine cherchait à contourner l'avance technologique de l'armée américaine en utilisant la cyber-guerre comme arme asymétrique. La volonté de la Chine étant de négliger l'obsolescence de ses chars, bateaux et avions et de se concentrer sur les failles technologiques adverses. L'Armée de Libération Populaire a bien compris la dépendance sans cesse croissante des armées modernes vis-à-vis de l'informatique et de leurs besoins permanents de communiquer. À ce titre, une attaque comme celle visant des membres du Parlement britannique (utilisation de la faille WMF) et identifiée comme venant de Chine pourrait très bien entrer dans ce cadre. De même, en 2005, un piratage de grande ampleur, identifié comme venant de Chine a frappé des sites d'information américains sensibles (centre militaires, NASA...).

Un expert en sécurité du SANS Institute a dévoilé de nouvelles informations sur des vols répétés de documents sensibles dont ont été notamment victimes, en 2004, des bases de l'armée américaine ou encore la Nasa. Un commando informatique, baptisé « Titan Rain » composé de vingt Chinois basés dans la province de Guangdong aurait réussi à pénétrer des réseaux informatiques et à s'emparer, entre autres, de documents sensibles. « Ils ont obtenu, depuis l'arsenal Redstone, base de l'aviation militaire et du centre de commandes de missiles, les spécifications d'un système de plans de vol pour les hélicoptères de l'armée, ainsi que le logiciel de planification des vols Falconview 3.2 utilisé par l'armée et l'US Air Force », a indiqué Alan Paller, le directeur du SANS Institute lors d'une réunion au ministère du Commerce et de l'Industrie britannique, à Londres. Ces vols auraient débuté en 2003. Une attaque massive a eu lieu en novembre 2004, rendue publique seulement en 2005. Le quotidien américain *The Washington Post* a rapporté que des sites chinois étaient utilisés pour cibler des réseaux informatiques du ministère de la Défense et d'autres agences américaines.

Selon Alan Paller, durant la nuit du 1er novembre 2004, les pirates ont d'abord exploité des failles dans le poste de commandes du système d'information de l'armée américaine, à Fort Huachuca (Arizona). Ils ont ensuite tiré parti de la même faille dans les ordinateurs de la DISA, un organisme qui administre des portions du réseau Internet entrant dans la composition du réseau militaire, à Arlington, Virginie. Puis, ils s'en sont pris à une installation de la marine américaine à San Diego (Californie). Avant de pénétrer un autre site traitant des questions spatiales et stratégiques à Huntsville (Alabama).

Le magazine *Time* a, lui aussi, relaté l'affaire, indiquant qu'un expert en sécurité américain du ministère de l'Énergie, Shawn Carpenter, avait repéré le manège des Chinois. Les pirates ont laissé des portes d'accès pour pouvoir revenir. Il a réussi à remonter jusqu'à eux, en pénétrant des routeurs en Chine. Il a pu enregistrer des sites ayant été corrompus, et découvert des données volées par les pirates.

Le directeur du SANS Institute estime que le bénéficiaire des données récoltées n'est autre que le gouvernement chinois. « Bien sûr, que c'est le gouvernement. Les gouvernements donneraient tout pour prendre le contrôle des ordinateurs d'autres gouvernements. C'est bien plus efficace que d'effectuer des écoutes téléphoniques. » (Source : AFP du 25 novembre 2005).



Mais les autres pays d'Asie ne sont pas en reste, ne serait-ce que pour contrebalancer l'exemple chinois. La Jemaah Islamiyah recrute en ligne les auteurs de ses futures cyber-attaques. Rohan Gunaratna, président de l'Institute of Defense and Strategic Studies de Singapour — et auteur de plusieurs ouvrages sur Al Qaeda et la Jemaah Islamiyah — met en garde les nations du Sud-est asiatique contre la menace grandissante des cyber-attaques terroristes. L'Inde développe également des capacités dans ce domaine. En 1999, elle se dotait d'un Institut des Technologies de l'Information et les premiers cours étaient donnés sur le campus temporaire de Hyderabad dans le but de former les étudiants aux rudiments de la cyber guerre. En 2002, est née l'université de Défense nationale (National Defense University) dont l'objet est la guerre de l'information et la révolution numérique. Parallèlement, l'Inde a mis au point une stratégie de cyber-guerre incluant l'assistance du secteur privé du logiciel. Le développement de moyens par le gouvernement indien s'expliquerait notamment par les activités offensives du Pakistan dans le domaine numérique. Selon Ankit Fadia, un consultant en sécurité informatique indien, les services de renseignements pakistanais paient des pirates occidentaux entre 500\$ et 10.000\$ pour « défacer » des sites indiens. Les groupes hacktivistes « défacent » selon lui jusqu'à soixante sites par mois. L'Inde s'est donné les moyens d'une réelle politique de développement informatique et a fait en sorte d'intégrer la cyber-guerre dans sa doctrine militaire.

15.1.5 Le Proche et Moyen-Orient

Des pays comme l'Iran, des groupes palestiniens ou pro-palestiniens, et Israël sont également intéressés par la cyber-guerre, même s'il est très difficile d'avoir des informations précises. Selon Cédric Thévenet (voir note de bas de page numéro 4), la tendance à la militarisation et l'isolationnisme économique pousse l'Iran à étudier avec intérêt la piste des armes non conventionnelles, incluant une connaissance avancée des nouvelles technologies. Certains éléments laissent à penser que la nation iranienne a commencé à développer une capacité de cyber-guerre dans le but de compenser les carences de son armée. L'objectif de la politique iranienne est de développer le secteur des technologies de l'information tout en conservant le monopole et le contrôle des accès à Internet. Les moyens consentis par les autorités iraniennes dans le contrôle de l'Internet indiquent une maîtrise des technologies de l'information susceptible d'être utilisée dans des actions de cyber-guerre.

L'utilisation du piratage comme arme dans une stratégie du faible au fort a depuis longtemps été considérée par les différents groupes palestiniens. En juin 2006, des pirates informatiques pro-palestiniens ont mis en panne des centaines de sites Internet israéliens alors que l'armée de l'Etat hébreu lançait une opération d'envergure dans le sud de la Bande de Gaza pour tenter de récupérer un soldat israélien capturé, selon le quotidien *Jerusalem Post*. Quelque 700 sites ont été fermés et leur page d'accueil a été remplacée par le message « piraté par l'équipe du mal des pirates arabes. Vous tuez des Palestiniens, nous tuons des serveurs israéliens ». Selon le *Jerusalem Post*, cette équipe comprendrait six membres et serait apparemment basée au Maroc. Elle aurait commencé à attaquer des sites du gouvernement américain en



2004. Parmi les sites visés figuraient celui de la plus grande banque israélienne, Bank Hapoalim, ainsi que celui d'un hôpital de Haïfa, de BMW Israël, Subaru Israël et Citroën Israël (source AFP du 30 juin 2006).

De façon plus générale, Pierre de Bousquet, patron de la DST, affirme que le risque de cyber-terrorisme est bien réel¹ et qu'il est devenu une préoccupation de l'État français. « Dans ce contexte, affirme-t-il, les entreprises mais également l'Etat semblent vulnérables avec des possibilités de plus en plus réduites de mettre en œuvre des solutions de protection efficaces ». Il estime qu'en 2000 près de 100 % des groupes terroristes islamiques utilisent le web.

Enfin, en ce qui concerne un pays comme Israël, il est difficile de savoir avec précision quel est le niveau d'engagement en matière de cyber-guerre. Dès le début des années 90, des souches virales comme celles de SURIV ont été attribuées aux services du Mossad. L'utilisation de techniques assimilables à du hacking ou du piratage a souvent été citée (en février 1998, l'espionnage de militants islamiques à Berne, par exemple, ou l'élimination de Y. Ayyash après avoir piraté à distance son téléphone portable en 1996). Un ouvrage comme celui de Nima Zamar², ancien membre du Mossad, est révélateur. Cette agent a utilisé le piégeage d'ordinateurs palestiniens et son témoignage indique que ces techniques sont d'un usage courant.

Le niveau scientifique des Israéliens ainsi qu'une diaspora soudée et puissante, assurant complicités et soutien logistique, rend ce type d'attaques assez aisées.

15.1.6 Les autres pays

Les pays européens sont étrangement absents de cet inventaire. Que faut-il en conclure ? Si la France a fait le choix politique d'interdire toute utilisation offensive de l'informatique pour se concentrer sur la défense (voir note de bas de page numéro 1), la situation est peut-être moins claire pour les autres pays, sans qu'il soit possible pour autant d'être plus précis. La lecture de l'ouvrage de Peter Schweizer³ permet de comprendre pourquoi les services allemands (BND) ont dans le cadre du projet Rahab, recruté des hackers à des fins d'espionnage et d'opérations militaires. Le Royaume-Uni quant à lui semble avoir suivi la voie tracée par son allié naturel. A ce titre, la lecture d'un livre écrit par ancien du MI-6, Peter Wright⁴, donne matière à réflexion.

Nous allons maintenant voir, à travers quelques cas très connus sous quelles formes le piratage à la mode étatique peut exister. Les quelques exemples présentés ici sont américains. Mais il ne faudrait pas en conclure que seul ce pays est actif dans ce domaine. Il a indubitablement la part la plus facile : maître du réseau Internet, distri-

1. Mag Secur, Avril 2006.

2. Nima Zamar, « Je devais aussi tuer », Editions Albin Michel, 2003.

3. Peter Schweizer *Friendly Spies : How America's allies are using economic espionage to steal our secrets*, Atlantic Monthly Press, 1993.

4. Peter Wright *The SpyCatcher* Heinemann 1987. Une traduction est parue chez Laffont la même année.



buteur monopolistique de systèmes d'exploitation et de processeurs, artisan de la plupart des normes, une infrastructure mondiale d'espionnage comme Echelon... bref les États-Unis ont tous les moyens d'agir à leur guise.

15.2 LES PROJETS CARNIVORE ET MAGIC LANTERN

Les États-Unis ont multiplié les systèmes de surveillance et d'infiltration et ce bien avant les attentats du 11 septembre, lesquels ont déclenché une véritable hystérie sécuritaire qui a eu son lot de débordements anti-démocratiques, actuellement instruits par la Justice américaine et le Congrès. Nous allons présenter les trois plus médiatisés : les projets Carnivore, le projet Magic Lantern et l'affaire des web bugs de la NSA.

Le projet Carnivore, initié par le FBI, est né en 1997¹ et il est l'aboutissement d'un projet dénommé Omnivore. Il a été rebaptisé DCS1000 en 2001, le terme de Carnivore étant jugé par trop agressif et suggestif. Sorte de cousin du fameux réseau Echelon de la NSA, il s'agit d'une suite logicielle de type *sniffer*. Sa fonction est d'intercepter tout type de trafic sur le protocole IP en provenance des fournisseurs d'accès Internet (FAI). À ce titre, Carnivore est l'équivalent, pour le réseau Internet, des écoutes téléphoniques. Pour fonctionner, une « boîte noire » doit être installée chez les FAI. L'existence de ce projet et de ces « écoutes » n'a été révélée qu'en juillet 2000. Le secret qui l'a entouré n'a pas manqué d'attirer la suspicion des citoyens et journalistes américains à tel point que la justice américaine a dû diligenter des enquêtes. Malheureusement, le FBI n'a jamais collaboré pleinement et près de 50 % de ses fichiers n'ont jamais été communiqués à la justice, malgré de nombreuses injonctions des juges (les documents communiqués sont disponibles sur la page web EPIC Carnivore Page²).

D'un coût total de près de 2 millions de dollars, Carnivore est en fait un ensemble d'outils gérés par une console unique. Initialement, le projet reconstituait en temps réel les pages consultées par les cibles, puis peu à peu le système a accru ses capacités : extension au système Windows (alors qu'il était limité initialement aux systèmes Solaris), gestion de la corruption de données, identification de cibles précises, analyse des protocoles DHCP et Radius, adaptation aux variations brutales des flux du réseau, traitements automatisés des packets interceptés, interception FTP et du courrier électronique. Bref, le produit est devenu une véritable centrale d'espionnage en temps réel des différents trafics sur Internet.

1. Les informations présentées ici sont tirées de documents déclassifiés américains et du rapport officiel du *Electronic Privacy Information Center*, rédigé à la demande du Département de la Justice des États-Unis. L'étude technique a été réalisée par un institut de recherche indépendant : S. P. Smith et al. *Independant Review of The Carnivore System – Final Report*, IITRI CR-030-216, December 2000, IIT Research Institute.
2. <http://www.epic.org/privacy/carnivore/> ; voir également <http://www.akdart.com/carniv.html>



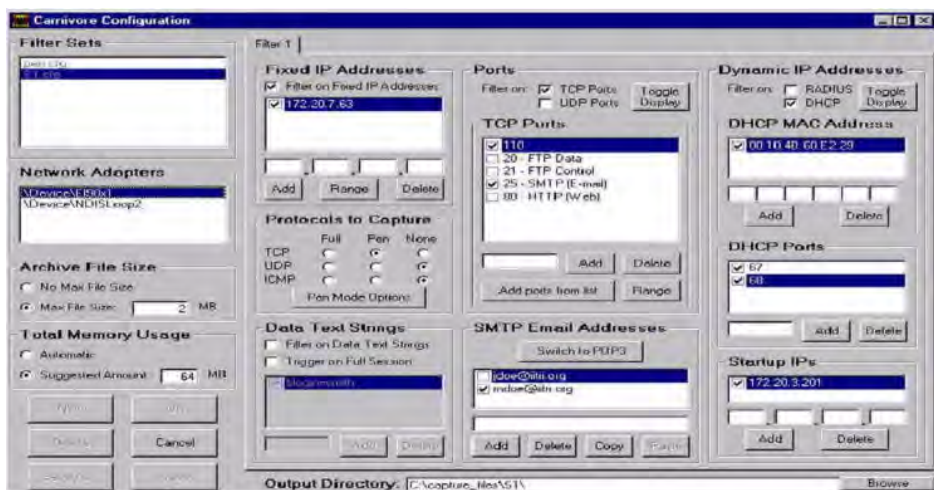


Figure 15.1 — La console de configuration : l’espionnage version internet.

Carnivore provoque toujours des controverses (le système est toujours utilisé sous le nom de DCS 1000) mais il est très difficile, malgré l’abondance de documents officiels, de déterminer comment et dans quel but ce système a été utilisé. Critiqué par le Congrès américain, « inquiet » par la justice, ce projet — très activement soutenu par l’administration Clinton — a soulevé des vagues de protestations dans l’opinion publique américaine, qui craint un usage incontrôlé de cette technologie. Au-delà de ces considérations, le plus désolant est que si l’efficacité de ce projet a pu être établie par la justice américaine, à travers des cas révélés, le projet Carnivore a semble-t-il également connu de graves défaillances, allant jusqu’à interférer avec les enquêtes sur Ben Laden. En effet, l’interception incontrôlée, en mars 2000, suite à une défaillance du logiciel, de cibles non autorisées, a été lamentablement gérée. Pris de panique, les opérateurs ont détruit l’ensemble des enregistrements, lesquels contenaient des preuves d’activités terroristes du réseau Al-Qaïda¹.

Le projet Carnivore présentant des défauts et des limitations (notamment en terme d’usage car les interceptions sont statiques), un second projet plus ambitieux — mais également plus contestable — a été lancé et révélé par le FBI en novembre 2001². Magic Lantern. Il semble être une partie seulement d’un projet plus vaste, dénommé CyberKnight (chevalier du Cyberspace), lui-même constituant une extension « améliorée » du projet Carnivore (version 3.0).

Magic Lantern est en fait un ver espion réalisant de l’interception de clavier. Une fois la machine cible infectée, il est capable d’intercepter tout ce qui est entré au clavier : mot de passe, clef de chiffrement, données... Ces données sont ensuite renvoyées de manière sécurisée vers les analystes du FBI (ou de la NSA éventuelle-

1. FBI memo on « FISA Mistakes » du 5/4/2000. Document déclassifié.

2. Ted Bridis, “FBI develops eavesdropping tools”, Washington Post, 22 novembre 2001.

ment)¹. L'intérêt de cette technologie est d'être mobile et donc de pouvoir gérer dynamiquement les cibles, en plus grand nombre que ne le faisaient les versions initiales du projet Carnivore. Comment est utilisé ce ver à présent ? Nul ne le sait vraiment. Mais le plus inquiétant est la réaction de certains vendeurs de logiciels antivirus face au projet Magic Lantern. Certains d'entre eux auraient modifié leurs produits afin que Magic Lantern ne soit pas détecté. Selon Ted Bridis, du *Washington Post*, au moins une société — Network Associates, éditeur du logiciel McAfee — a contacté le FBI pour lui assurer que Magic Lantern ne serait pas détecté par son antivirus...

Dans cette atmosphère sécuritaire et de peur citoyenne de dévoilements, les révélations de la NSA, le 29 décembre 2005, n'ont certainement pas arrangé la situation. Elles ont contribué à jeter un peu plus de trouble sur la nouvelle politique américaine en matière de sécurité. La NSA utilise depuis quelques mois des cookies et *web bugs* comme mouchards électroniques. Si les cookies s'occupent des pages visités, les web bugs permettent également la surveillance des courriers électroniques. Les cookies sont de petits fichiers textes stockés par votre navigateur Web sur le disque dur, quand vous visitez un site Web. Ils servent (entre autres choses) à enregistrer des informations sur le visiteur ou encore sur son parcours dans le site. Le webmaster peut ainsi reconnaître les habitudes d'un visiteur.

Les *web bug* sont généralement des images GIF transparentes², de la taille d'un pixel, placées dans une page Web ou un courrier électronique au format HTML. Ils s'activent lors du téléchargement de la page et lancent une requête à un serveur distant qui collectera des informations sur l'internaute à son insu. Parmi les informations pouvant être ainsi récupérées, figurent l'adresse IP, le nom et la version du système d'exploitation et du navigateur utilisés, ou même encore la résolution de l'écran de l'internaute. Ces fonctionnalités sont également présentes dans certains documents bureautiques³. Ces dispositifs ont été insérés notamment sur le site web de la Maison Blanche à Washington⁴. Pourtant, l'usage de ces technologies est interdit aux Etats-Unis (loi de 1994).

Si ces trois cas sont désormais connus, force est de constater que bien des zones d'ombre subsistent, non seulement sur les capacités techniques de ces outils mais surtout sur leur utilisation réelle, et notamment dans ce qui ressemble à des œuvres de basse police et de surveillance de journalistes ou de citoyens « hostiles » à la ligne Bush. D'autre part, cette médiatisation, qui peut surprendre, ne doit pas faire oublier que ces cas sont peut-être les arbres qui cachent la forêt. En concentrant l'attention des médias et du citoyen sur ces cas, ils la détournent d'autres projets du même type.

1. Une description technique de la technologie Magic Lantern, ou du moins de son principe, est décrite dans le chapitre 13 du livre « *Les Virus Informatiques : théorie pratique et applications* », Springer Verlag France, 2004.
2. L'utilisation d'images transparentes permet également l'activation de certains types de virus de manière indétectable. Voir dans Eric Filiol, « *Les virus informatiques : théorie pratique et application* », Springer Verlag France 2004 (pages 106 et suivantes).
3. Lire « *La fuite d'informations dans les documents propriétaires* », Journal de la sécurité informatique MISC, numéro 7, mai 2003, pp. 35—41.
4. Anick Jesdanu, "White House to Investigate Contractor's Web Tracking, Technologies may violate Policy", Associated Press du 30 décembre 2005.



15.3 L'AFFAIRE HANS BUEHLER

Cette affaire¹ éclata en 1995. Elle constitua un véritable cataclysme dans le monde feutré du renseignement, de l'espionnage et des relations internationales. Elle fut en fait juste l'épilogue — et en même temps le révélateur au public — d'une histoire très particulière. Depuis près de 50 ans les services de renseignements américains lisaient à livre ouvert les communications secrètes chiffrées (diplomatiques, militaires, politiques, économiques et commerciales...) de près de 120 pays. Ils y étaient parvenus en s'assurant que le plus important manufacturier de machines à chiffrer — la société Crypto-AG en Suisse — insérait dans les machines vendues à ces pays des dispositifs permettant de briser les codes plus facilement — soit l'algorithme était affaibli soit la clef était dissimulée dans le texte chiffré à l'insu du chiffrer.

Cet espionnage a duré de 1947 à 1992, c'est-à-dire jusqu'au moment où les Iraniens — clients de Crypto AG pour leurs propres besoins en machines à chiffrer — ont commencé à avoir des doutes quant à la sécurité de leurs communications. Des déclarations faites par des politiques dans la presse, mettant en cause l'Iran et ses actions terroristes (enlèvement du journaliste Charles Glass en 1987, attentat contre le vol 103 de la PanAm à Lockerbie, assassinat de Shahpour Bakhtiar en 1991, attentat dans un discothèque à Berlin...) ont très vite incité les Iraniens à penser que leurs communications chiffrées les plus secrètes étaient décryptées par les Occidentaux. De là à soupçonner leur unique fournisseur, Crypto AG, il ni eu qu'un pas.

À l'occasion de son 25^e voyage commercial en Iran, Hans Buehler, le super vendeur de la société suisse, est arrêté sous les charges « d'espionnage pour le compte des services allemands et américains ». Il a été retenu en captivité pendant 9 mois. Les Iraniens ont tenté (en le torturant psychologiquement) de savoir si les machines qui leurs étaient vendues étaient « affaiblies » ou non. Crypto AG négocia avec l'Iran et paya une rançon de un million de dollars (somme payée en collaboration avec la société Siemens dont le nom a également été évoqué dans les collusions avec les services américains) pour la libération de son employé. Cette « affaire » aurait pu s'arrêter là et il n'y aurait jamais eu de scandale. Mais la société licencia dès son retour Hans Buehler et exigea... qu'il rembourse la rançon payée aux Iraniens, sous prétexte d'avoir livré des secrets de la société. Cette attitude provoqua la suspicion et les enquêtes journalistiques. Elle a également effrayé plusieurs salariés. Ces derniers ont alors commencé à parler et à raconter ce qu'ils savaient.

Que révéla cette affaire ? Simplement que les services américains (la NSA) et allemands (le BND) avaient négocié avec la société Crypto-AG pour que toutes les machines à chiffrer vendues à l'étranger soient « affaiblies » afin d'en permettre le

1. Plusieurs sources officielles ont été utilisées ici. Nous en indiquons que les principales. Le lecteur pourra consulter l'article de Wayne Madse, « *Crypto-AG : The NSA's Trojan Whore ?* » (*Crypto-AG, la prostituée de la NSA ?*), *Covert Action Quarterly*, Numéro 63, 1998. L'ouvrage témoignage de Hans Buehler lui même, « *Verschlüsselt - Der Fall Hans Bühler* », écrit par un journaliste Res Strehle, aux éditions Werd Verlag, 1998, ISBN 3-85932-141-2. Enfin, l'article de J. Orlin Grabbe, « *NSA, Crypto AG, and the Iraq-Iran Conflict* », novembre 1997.



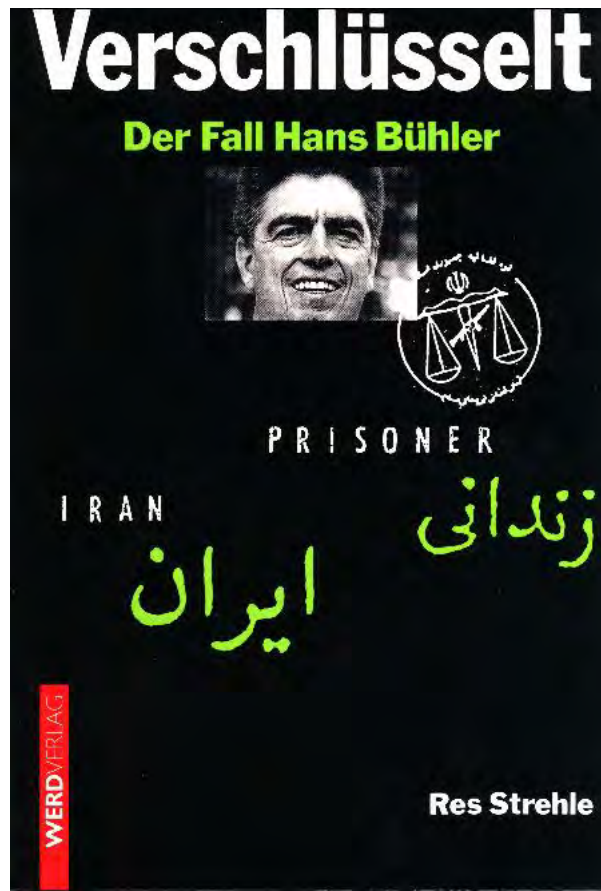


Figure 15.2 — 1 Hans Buehler et le livre témoignage.

décryptement facile, pour quiconque connaissait la faiblesse introduite. Les investigations prouvèrent que, depuis des années, des employés de la société avaient des preuves de ces manipulations et les avaient transmises aux procureurs suisses... sans suite aucune.

La société crypto AG tenta de museler Hans Buehler, les divers témoins et les journalistes en engageant un procès. En vain. Même si des pressions établies de la NSA et du BND se sont arrangées pour que les éléments du dossier les plus « chauds » restent à jamais secrets. Le mal était fait. Les clients de Crypto AG (Saddam Hussein, le Vatican, la plupart des pays d'Amérique Latine...) ne firent plus confiance aux machines de Crypto AG, société suisse dont la neutralité affichée avait été le meilleur des messages marketing. Autre révélation : cette soi-disant neutralité n'existait plus depuis 1956. Un document publié en 1995 par le Public Records Office anglais prouvait que la Suisse et l'OTAN avait conclu un accord secret selon lequel la Suisse serait neutre en temps de paix mais rallierait l'OTAN en cas de guerre¹. D'autres documents américains ont également établi l'importance de la Suisse, notamment en ce qui concerne « la fourniture de matériel de précision et autres matériels nécessaires à la sécurité nationale américaine² ». Les recherches ont montré que des sociétés tierces auraient été impliquées dans les modifications des machines à chiffrer : Siemens en Allemagne. Gretag en Suisse, Transvertex et Ericsson en Suède, Nokia en Finlande...

Plus grave — et ce fut là peut être le volet le plus délicat de cette affaire — il semblerait que les informations techniques de décryptement connues de la NSA aient été partagées avec les Israéliens et que le contenu des communications secrètes iraniennes — une fois décrypté — aient été communiqué à l'Irak en soutien à sa guerre contre l'Iran (lire l'article de J. Orlin Grabbe).

Cette affaire qui illustre ce qu'un Etat en situation de force peut faire n'est pas surprenante. Ce qui l'est plus, c'est que le secret ait pu être préservé si longtemps. Alors que le contrôle de la cryptographie est une chose compréhensible³ au même type que le contrôle des armements⁴, le contrôle à la mode NSA « n'est plus très éloigné » des techniques de chevaux de Troie des pirates. C'est précisément parce que la cryptologie n'était pas contrôlée que l'Allemagne nazie a pu acquérir la machine Enigma, alors en vente libre.

Précisons que la France ne figurait pas au nombre des clients de la fameuse société suisse. Sur décision du Général de Gaulle à la fin des années 1950, les moyens de chiffrements français sont exclusivement conçus et réalisés par la France. Une décision avisée...

1. Document référencé Prem11/1224, du 10 février 1956, rédigé par le Maréchal Montgomery (alors commandant adjoint de l'OTAN) et le ministre suisse de la défense Paul Chaudet.
2. Directive pour la sécurité nationale préparée pour le président Harry Truman.
3. C'est précisément parce que la cryptologie n'était pas contrôlée que l'Allemagne nazie a pu acquérir la machine Enigma, alors en vente libre.
4. Rappelons que jusqu'en 2000, en France, comme dans beaucoup de pays, les moyens de cryptologie étaient assimilés à des armes de guerre. Ils le sont toujours s'agissant de produits exportés.



En résumé

Ces quelques exemples montrent tout l'intérêt des techniques de piratage pour les Etats qui les emploient ou du moins s'y « intéressent ». Une certaine transparence américaine a permis à travers ces quelques cas d'imaginer ce que peut être le « côté obscur ». Mais d'autres pays ne communiquent pas sur le sujet alors qu'il est maintenant avéré qu'ils disposent d'entités de LIO (Lutte Informatique Offensive) ou assimilées (ce qui est de toute logique). Outre les pays cités dans ce chapitre, d'autres sont très probablement dotés de telles structures et ne le disent pas.

Tous ces pays ont compris l'immense potentiel que constitue le champ numérique. Et les entreprises privées également. Elles se lancent dans la production et la fourniture de logiciels « adaptés ». Ainsi, le meilleur outil de désassemblage au monde, IDA Pro, n'est disponible que pour les agences gouvernementales et le logiciel DIRT, vendu aux seuls militaires et policiers, par la société Codex Data Systems, permet de disposer de véritables outils dignes des meilleurs pirates. Ces sociétés sont en quelques sortes les marchands d'armes de demain. Les champs de bataille sont désormais les réseaux et chacun d'entre nous, que ce soit au niveau professionnel ou personnel, est une cible potentielle. Dans ce domaine, il n'y a pas vraiment de temps de paix.

Le plus préoccupant est la facilité avec laquelle une société démocratique pourrait basculer dans la pire des dictatures et sans que personne ne s'en rende compte. De la lutte contre les criminels et les terroristes à la surveillance du citoyen, laquelle peut prêter à tous les débordements, la frontière est mince. Les outils sont en place et nous entourent.

Orwell était peut-être un visionnaire.

Creative Commons BY-NC-ND



16

La législation face à la cybercriminalité

« A l'instar des paradis fiscaux, il existe maintenant des paradis numériques où un malfaiteur peut agir ou héberger des serveurs et des contenus illicites en toute impunité », constate dans la revue *Information & Systèmes* (février 2006) Solange Ghernaouti Hélie, professeur à l'Ecole des HEC de l'Université de Lausanne et directrice de l'Institut d'informatique et Organisation.

Ce constat n'est pas une surprise. Tout au long de ce livre nous avons montré comment et pourquoi les cybercriminels s'étaient adaptés à l'évolution technologique de la société. Cette évolution des mœurs a donc obligé les pouvoirs publics à renforcer son dispositif répressif. Certains seraient tentés de dire que la justice a un train de retard. Ce n'est plus le cas.

Jusqu'au milieu des années 80, la France ne disposait que de deux textes : la Loi informatique et libertés (1978) et la Loi sur la protection du droit d'auteur (1985). Il faut attendre 1988, avec l'adoption de la fameuse Loi Godfrain (relative à la fraude informatique) pour que l'Hexagone commence à se doter d'un arsenal répressif allant jusqu'au pénal. Il y aura ensuite la loi relative à la sécurité quotidienne (2001), la loi relative à la sécurité intérieure (2003), la loi pour la confiance dans l'économie numérique (2004) et la loi relative aux communications électroniques et aux services de communication audiovisuelle (2004).

Cet arsenal, aussi important soit-il en France, présentait néanmoins quelques failles, concernant principalement le commerce électronique. « Jusqu'à la fin des années 90, tout a été fait pour développer le e-commerce, explique un spécialiste. La sécurité n'était pas une priorité. Cette situation est en train d'évoluer depuis que l'Union Européenne a « décidé » que le commerce électronique était suffisamment mature pour qu'on s'attaque maintenant au cybercrime et aux pratiques anormales de certains cybermarchands ».



D'autres signes témoignent de cette évolution. Des magistrats spécialisés dans le domaine des technologies de l'information ont été désignés dans chacun des Tribunaux de grande instance des cours d'appels de Paris et de Versailles.

Au niveau européen, un texte en gestation depuis quatre et remanié une vingtaine de fois devrait être signé fin 2006 par 43 Etats (cf paragraphe 16.1.1 ci-dessous). Il a pour objet la création d'une politique pénale commune destinée à protéger la société de la criminalité. Ce texte réglemente notamment les atteintes à la propriété intellectuelle, la falsification et les fraudes informatiques. Il fixe également les règles relatives au stockage des données.

Condamnation d'un créateur de virus

Les virus qui paralysent une partie de la planète numérique ne font plus parler d'eux. Cette délinquance est passée de mode. Mais cela n'empêche pas les pouvoirs publics de condamner les auteurs de ces méfaits. En juillet 2005, un jeune Allemand à l'origine du virus Sasser a été condamné à un an et neuf mois de prison avec sursis par la justice de son pays. Âgé de 18 ans, Sven Jaschan était jugé pour sabotage d'ordinateurs, modification de données et perturbation d'activités d'entreprises. Quelque 140 particuliers, administrations et entreprises avaient porté plainte. Un an plus tôt, le jeune homme avait créé ce code qui installait un programme (nommé lsass.exe) qui provoquait des redémarrages intempestifs toutes les 60 secondes, après affichage d'un message d'alerte. Lors de son arrestation, il avait déclaré avoir également été le créateur de Netsky, un autre virus. Source : Journal du net.

16.1 UN ARSENAL JURIDIQUE ADAPTÉ

Pour différents juristes que nous avons rencontrés, la France est un modèle en matière de réglementation. « Les articles 323 1, 2 et 3 de notre Code pénal sont courts mais ils sont efficaces et ils font jurisprudence depuis 1988 », indique maître Eric Barbry, directeur du département nouvelles technologies au cabinet Alain Bensoussan.

Ainsi l'article 25 de la Loi informatique et libertés permet par exemple de condamner quelqu'un qui récupère des données au moyen d'un logiciel espion (*spyware*) ou d'un robot. De son côté, la loi Godfrain permet de condamner une personne utilisant un *keylogger* (enregistrant par exemple les mots de passe tapés sur un ordinateur) ou une application malveillante chargée « d'écouter » et de « récupérer » les flux de données d'un réseau. Cette loi sanctionne aussi l'association de malfaiteurs en matière informatique.



16.1.1 La Convention sur le cybercrime

Le 23 mai 2006, le Journal officiel a publié deux décrets officialisant la Convention sur la cybercriminalité, un texte signé par la France et quarante deux autres Etats à Budapest le 23 novembre 2001. Seul bémol : fin juin 2006, il n'y avait que 14 Etats à avoir ratifié ce texte. La France est le troisième pays en 2006 à l'avoir fait, après l'Ukraine et la Bosnie-Herzégovine.

Cette convention poursuit trois objectifs :

- **Harmoniser les législations des Etats** : la Convention établit des définitions communes de certaines infractions pénales commises par le biais des réseaux informatiques. Ces infractions sont notamment relatives aux contenus, ainsi qu'à toute atteinte à la propriété intellectuelle commise sur Internet.
- **Harmoniser les procédures** : cet objectif vise à améliorer la capacité des services de police à mener en temps réel leurs investigations et à collecter des preuves sur le territoire national avant qu'elles ne disparaissent.
- **Améliorer la coopération internationale** : ce volet concerne notamment l'extradition et l'entraide répressive.

Bien que peu de pays l'aient encore ratifiée, Eric Barbry se montre optimiste : « Ce texte est remarquable par la vitesse à laquelle il a été adopté. Généralement, il faut 10 à 20 ans pour qu'une convention internationale soit signée et ratifiée. C'est le signe qu'on a pris, au niveau international, conscience très vite de la cybercriminalité ». Mais pour ce spécialiste, « c'est aussi le signe que l'Union européenne n'a pas nécessairement pris — contrairement au conseil de l'Europe — la mesure de la cybercriminalité en privilégiant avant tout le développement du commerce électronique ». Son maître-mot est : « *on va ouvrir le marché de l'électronique* ». Le Conseil de l'Europe n'a pas la même vue puisqu'il veut lutter contre le cybercrime ! »

16.2 DES CONDAMNATIONS EXEMPLAIRES

Les arrestations de quelques pirates « historiques » — le plus connu étant Kevin Mitnick — ont fait la une des journaux il y a quelques années. C'était l'époque des pandémies de virus et des intrusions visant surtout à prouver qu'on était compétent. Aujourd'hui, la donne a changé. Il y a deux types de cybercriminalité. La première est réalisée par des bandes organisées. Elles s'appuient notamment sur les compétences de pros de l'informatique. Ces derniers utilisant des méthodes très sophistiquées et donc difficilement détectables. Le second type de cybercriminalité est celui orchestré par Monsieur-tout-le-monde. Aujourd'hui, sur Internet on trouve assez facilement des kits du parfait pirate du dimanche (mais aussi d'autres programmes plus sophistiqués mais plus difficiles à dénicher sur le réseau...). Les cas de figure sont variés. Frustré de ne pas avoir obtenu une promotion qu'il juge évidente, un



employé veut se venger en essayant de s'introduire dans le réseau informatique de son entreprise. Il cherche à y glisser un code malveillant. Insatisfait du comportement commercial de sa banque, un client va vouloir défigurer (appelé *defacement* en anglais) son site. Dernier exemple, le beau-frère qui glisse un *keylogger* dans le PC d'un membre de sa belle famille pour récupérer identifiant et mot de passe afin de faire un virement sur son compte. Tout est possible.

Et ces deux types de cybercriminalité sont en hausse. « Bien sûr, nous avons des outils plus sophistiqués permettant de mieux appréhender ce phénomène et nous sommes plus sensibilisés mais il n'en reste pas moins vrai que cette criminalité augmente depuis un ou deux ans », déclare un membre du Secrétariat général de Défense nationale (SGDN). Malgré tout, il y a peu d'affaires rendues publiques.

La fameuse culture du secret propre à la France (« il ne faut surtout pas dire que nous avons été victime d'une attaque car cela voudrait dire que nous sommes mauvais... ») et l'absence d'un organisme unique (et connu de tous) pour déposer des plaintes liées à la sécurité informatique expliquent en partie ce constat.

De son côté, Eric Barbry indique qu'il y a « beaucoup de procédures — très longues — en cours et il y a aussi beaucoup de transactions, c'est-à-dire des négociations à l'amiable ».

Amende record pour une potion miracle

Le roi du Spam, Stanford Wallace, a été condamné en mai 2006 à payer une amende de quatre millions de dollars. Il était accusé d'avoir infecté des PC à l'aide d'un logiciel publicitaire chargé de... vendre l'antidote ! Sa combine était simple. Il infectait des milliers d'ordinateurs et ensuite contactait ces pauvres internautes en le proposant d'acheter un logiciel soi-disant « désinfectant ». Cet américain n'en est pas à sa première condamnation. Il a déjà été reconnu coupable de fax publicitaires sauvages au début des années 1990 et dix ans plus tard, de spam.

16.2.1 La guerre contre les spammeurs

Apparu il y a deux ou trois ans en France, le *spam* est une plaie. Mais la situation semble moins catastrophique que dans d'autres pays comme les Etats-Unis notamment. Les pouvoirs publics de différents pays ont développé un arsenal juridique, plus ou moins efficace.

Pour endiguer le fléau, l'organisme chargé de la concurrence aux Etats-Unis, la Federal Trade Commission (FTC), a lancé en 2004 l'opération « Spam Zombies ». Soutenue par des organismes équivalents dans plus de vingt pays (pas encore la France) et par le London Action Plan, un groupe d'agences gouvernementales internationales, la FTC souhaite sensibiliser les fournisseurs d'accès Internet à la question. Trois mille d'entre eux ont reçu une lettre détaillant les différentes mesures nécessaires pour faire baisser le nombre des zombies : surveillance du nombre



d'envois par les utilisateurs pour identifier tout changement d'habitude suspect, déconnexion des ordinateurs contaminés (en avertissant leurs propriétaires !), limitation de la bande passante qui leur est allouée, assistance aux abonnés pour désinfecter leur PC, etc.

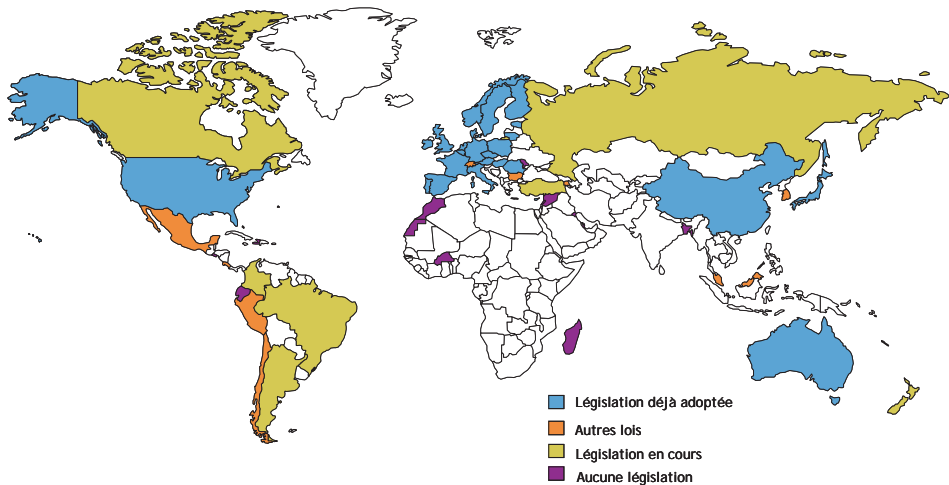


Figure 16-1 — Plusieurs pays ont déjà adopté une législation contre le spam comme l'Australie, les Etats-Unis, l'UE, et le Japon

Pionniers dans ce domaine, les Etats-Unis s'appuient sur la loi CAN Spam (*Controlling the Assault of Non Solicited Pornography and Marketing*), votée en 2003, qui prévoit jusqu'à cinq ans de prison et de lourdes amendes (jusqu'à six millions de dollars) pour le non-respect de ses principes fondamentaux.

Ce dispositif répressif a permis de condamner lourdement quelques spammeurs (mais les Etats-Unis restent malgré tout le premier pays émetteur de spams en avril 2006 juste devant la Chine). En 2003, le FBI a arrêté l'un des plus importants spammeurs au monde en s'appuyant sur cette loi. Pour promouvoir son activité de pharmacie illégale en ligne, cet Américain de 30 ans aurait émis un milliard de courriers indésirables depuis son bureau installé en République dominicaine !

En juin 2006, une cour fédérale du Texas a condamné un trio de spammeurs à une amende et des frais de justice de 10 millions de dollars. Ce groupe de spammeurs est soupçonné d'avoir été l'un des membres du Top 5 des plus gros émetteurs de spams dans le monde. L'un des spammeurs utilisant plus de 200 identités pour envoyer ses millions d'e-mails. Avec ses deux autres complices, il aurait envoyé 25 millions de spams chaque jour en 2004....

Concernant le Vieux continent, le Parlement européen a adopté en juillet 2002 une directive qui pose le consentement préalable du destinataire comme condition à l'envoi de messages. C'est le principe de « *opt-in* » (littéralement « opter pour entrer »). En clair, l'internaute ne doit pas recevoir de courrier commercial sans son

feu vert. Proposé par la Commission européenne en mars 2004, le programme Safer Internet Plus (2005-2008) est doté d'un budget de 45 millions d'euros. Il vise à lutter contre les contenus Internet illicites et préjudiciables. Il couvre également d'autres médias comme les supports vidéo et est explicitement conçu pour combattre le racisme et les communications électroniques commerciales non sollicitées (spam).

En France, la collecte déloyale de données est sanctionnée par l'article 226-18 du Code pénal et dans toute l'Union européenne, depuis la directive 95/46 sur la protection des données. L'article 226-16 du Code pénal précise : « Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de trois ans d'emprisonnement et de 45 000 euros d'amende. »

La première condamnation remonte à mai 2004. Un commerçant du Midi a été condamné à verser 22 000 euros de dommages intérêts et de frais de justice pour non-respect des conditions générales d'utilisation d'AOL et Hotmail. Au printemps 2006¹, la Cour de cassation a confirmé l'amende infligée à la société Alliance Bureautique Service qui a exploité durant quelques mois en 2002 les « logiciels aspirateurs » (Robot Mail et Freeprospec). L'objectif était en effet de collecter sur Internet des adresses de courriers électroniques de personnes physiques afin de leur adresser des messages à caractère publicitaire.

En se référant notamment à l'article 226-18 du Code pénal, lequel interdit et sanctionne toute collecte déloyale ou illicite de données nominatives de personnes physiques, la Cour a donc rejeté le pourvoi d'ABS qui contestait l'arrêt de la Cour d'appel de mai 2005. Cette juridiction l'avait condamné à une amende de 3000 euros pour « délit de collecte de données nominatives aux fins de constituer des fichiers ou des traitements informatiques par un moyen frauduleux, déloyal ou illicite ». Rappelons qu'en décembre 2004, le tribunal correctionnel de Paris avait relaxé ABS. La Cnil (Commission nationale de l'informatique et des libertés) avait demandé au parquet de faire appel de cette décision.

16.2.2 Les phishers sont dans le collimateur

Pour différentes raisons (impossibilité de faire des virements d'un compte de la banque A vers celui de la banque B, comme c'est le cas aux Etats-Unis), le *phishing* ne touche pas beaucoup d'internautes français. Cela ne signifie pas pour autant qu'il n'y ait pas quelques affaires. La plupart impliqueraient... des membres d'une même famille (le frère ou le gendre qui veut escroquer un proche...). Officiellement, il n'y aurait qu'un seul cas de *phishing* national à avoir été condamné. En septembre 2004 à Paris, un étudiant strasbourgeois a été condamné à 1 an de prison avec sursis et à 8500 euros de dommages intérêts pour avoir usurpé l'identité d'une grande banque française.

1. Pour plus de détails sur cette affaire, consultez : www.legalis.net/jurisprudence-decision.php3?id_article=1380



L'amour n'a pas de prix

Les courriers non sollicités inondent nos boîtes aux lettres classiques et nos e-mails. C'est aussi le cas, dans une moindre mesure, de nos téléphones mobiles. Cet harcèlement est aussi condamnable. La société CellCast l'a appris à ses dépens. Début 2006, elle a été condamnée à 50 000 euros d'amende et a aussi dû verser 30 000 euros de dommages intérêts à l'UFC-Que Choisir, qui s'était portée partie civile. Au printemps 2002, des millions de particuliers ont reçu un SMS leur révélant que quelqu'un était secrètement amoureux d'eux... Le message donnait ensuite un numéro de téléphone à rappeler (appel surtaxé : 1,35 euro l'appel, puis 0,34 euro par minute) pour savoir de qui il s'agissait. Si l'utilisateur appelait, il devait alors donner entre un et cinq numéros de téléphone de connaissances qui, selon lui, pouvaient être sous son charme.

D'après l'enquête de la DGCCRF, personne n'était en fait amoureux de qui que ce soit. La société avait loué une base de contacts. Qu'elle continuait d'alimenter en demandant des numéros à ses « victimes ». D'où des poursuites judiciaires engagées pour publicité mensongère et collecte illicite de données nominatives.

Source : 01net.com. 17/01/2006

Les principales condamnations ont lieu aux Etats-Unis, pays qui héberge le plus de sites de *phishing* (voir chapitre 4). En juin 2006¹, un phisher de 23 ans a été condamné à 21 mois de prison ferme assorti d'une amende de 45 565 euros. Entre janvier 2003 et juin 2004, il a envoyé des spams afin de diriger les clients MSN vers son site sur lequel les internautes étaient invités à mettre à jour leurs informations bancaires et leurs numéros de carte de crédit en échange d'une remise de 50 % sur un mois d'abonnement au service MSN. Repéré par Microsoft (à qui appartient ce service de messagerie), l'escroc a été arrêté par le FBI.

16.2.3 Les logiciels espions mis à l'index

Appelés aussi *spywares*, ces programmes malveillants peuvent être extrêmement dangereux. Certains pénètrent dans un ordinateur à l'état dormant et se réveillent soudain quand l'utilisateur de la machine tente d'accéder à un site Internet de banque. Les codes d'accès et les coordonnées de l'utilisateur peuvent ainsi être transférés aux mains d'escrocs, avec toutes les conséquences que l'on peut imaginer. Selon une étude publiée à l'automne 2005 par l'éditeur de sécurité Aladdin Knowledge System², un *spyware* sur six est doté d'un mécanisme de vol d'identité. 60 % des *spywares* se contentent de jouer les espions marketing, notant au passage les habitudes de navigation de l'internaute.

Face à cette menace, les Etats-Unis ont mis en place en 2005 la loi anti *spywares*, le « Spyblock Act » (Software Principles Yielding Better Levels of Consumer

1. www.vnunet.fr. 23.06.2006

2. Magazine CSO. 15/09/2005



Knowledge). Elle vise notamment les entreprises de marketing en ligne qui ne doivent plus rediriger la page d'accueil par défaut du navigateur Web vers un site à vocation marchande. Est également dans la ligne de mire de la proposition de loi, le fait d'empêcher la fermeture d'une fenêtre publicitaire intrusive (pop up), qui ne peut être effective qu'après arrêt du navigateur Web lui-même. Parallèlement à cette loi, l'Etat de l'Utah a adopté une législation spécifique dénommée « Spyware Control Act ». Cette loi ne contient pas seulement l'interdiction d'installer des logiciels espions à l'insu de l'utilisateur, mais pénalise aussi la production de tels logiciels. Tout contrevenant pourra être sanctionné d'une amende pouvant aller jusqu'à 30 000 euros, voire davantage si les dommages sont plus élevés.

Une plainte contre Microsoft

« Le géant Microsoft est poursuivi à cause de son outil anti-piratage Windows Genuine Advantage (WGA) » rapporte le magazine américain *Inquirer* le 30 juin 2006. L'avocat Brian Johnson, de Los Angeles, essaie d'obtenir pour sa plainte le statut de « class-action » (action en justice regroupant plusieurs plaignants). Son argument : l'éditeur n'a pas divulgué suffisamment d'informations sur cet outil quand il a été installé sur les PC à distance, via Windows Update, son système de mise à jour automatique en ligne.

Microsoft n'aurait pas apporté une information claire qui aurait permis aux utilisateurs de choisir librement de l'installer ou pas. Cité par le magazine, un porte-parole de Microsoft a déclaré que cette plainte était « sans fondement » et précise que WGA ne s'installe qu'avec le consentement de l'utilisateur et ne vise qu'à avertir celui-ci de l'absence d'une licence authentifiée.

Travaillant pour le compte du cabinet Kamber & Associés, cet avocat était déjà présent dans le procès qui avait contraint Sony à retirer son logiciel *rootkit* (programme permettant de camoufler des éléments déposés par un pirate ou un éditeur sur une machine).

16.3 L'ÉVOLUTION DE LA LÉGISLATION

Pour Eric Barbry, nous allons « passer d'un droit à la sécurité à une obligation de sécurité. Prenons l'exemple de la jurisprudence Tati¹. Celle-ci dit en substance : « vous ne pouvez pas bénéficier de la protection au titre de la loi Godfrain car vous n'avez pas sécurisé votre réseau ». C'est comme un particulier qui laisse sa maison ouverte et qui ne se fait pas rembourser par son assureur après un cambriolage ». Concernant le réseau informatique, cette évolution ne va pas sans poser de problèmes selon l'avocat du cabinet Bensoussan : « Il y a une différence entre le numérique et la voiture : on sait qu'une voiture qui n'est pas la vôtre ne vous appartient pas ! Or, on ne peut pas toujours faire la différence entre les pages web d'un site Internet et celles

1. www.secuser.com/dossiers/affaire_tati_kitetoa_analyse.htm



d'un réseau interne (Intranet) d'une entreprise. On peut par contre condamner la personne qui s'imisce dans un Intranet où il y a des *tags* ou des annonces qui rappellent qu'on ne peut pas recopier et publier ces documents qui sont protégés par un copyright. Par contre, si les données ne sont pas cryptées ou protégées la personne ne peut pas savoir si ce sont des données privées ! »

Cette évolution permettra aussi de mieux lutter contre l'intelligence économique.

En résumé

Après un temps de retard, les pouvoirs publics ont mis en place tout un arsenal juridique efficace. Les escrocs en tout genre (*spam*, *phishing*, intrusion...) peuvent être condamnés lourdement. La coopération internationale et l'harmonisation des procédures devraient accentuer la pression sur les cyberdélinquants. Les autorités sont donc sensibilisées. Il reste maintenant l'essentiel : informer correctement les entreprises et les particuliers sur les dangers liés à l'informatique afin qu'ils déposent plainte plus facilement et soient surtout plus vigilants.



Creative Commons BY-NC-ND



17

L'avenir de la cyberdélinquance : les prochaines cibles

Comment la cybercriminalité va-t-elle évoluer ? Prendra-t-elle des directions et des formes totalement nouvelles ou bien tout simplement suivre le développement de la technologie ? Cette dernière hypothèse, au vu de l'histoire de la criminalité, semble la plus probable. Au fond, les malfrats numériques n'ont fait qu'adapter des infractions traditionnelles aux nouvelles technologies : du racket, qu'il soit traditionnel ou numérique, reste une tentative d'extorsion. Les buts et motivations restent les mêmes, seuls les moyens changent. C'est ce qui avait guidé le sénateur Godfrain lorsqu'il avait proposé sa fameuse loi de 1988 : adapter l'existant de la criminalité au champ numérique et les quelques nouveautés (association de malfaiteurs informatiques, répression de la tentative...) n'en étaient que du point de vue du juriste et de la procédure. Cette loi, devenue l'article 323 du Code Pénal, est toujours aussi actuelle, près de vingt ans plus tard. Cela tend à confirmer l'hypothèse selon laquelle la cyberdélinquance ne fera que suivre la technologie et ses multiples applications.

Il est cependant possible d'envisager trois ressorts principaux que les cybercriminels de demain pourront exploiter : la mobilité extrême de nos capacités informatiques, leur omniprésence — et en même temps leur invisibilité — et, toujours, ce facteur humain qui, s'il nous protège contre une invasion totale de la technologie, reste un levier extrêmement efficace.

17.1 LA MOBILITÉ

C'est devenu le maître-mot de nos jours. Téléphones mobiles, PC ultra portables, consoles de jeux, PDA et autres organisateurs digitaux, communication sans-fil (Wi-fi, Bluetooth) et plus récemment l'informatique embarquée (dans les voitures par



exemple) envahissent notre espace sans que nous en soyons bien conscients. Combien d'utilisateurs d'un mobile de dernière ou avant-dernière génération savent ou devinent que leur appareil est en réalité un véritable petit ordinateur ?

Les pirates, eux, le savent ! Ils ne s'y sont pas trompés et les attaques fleurissent. Tout ce que l'on connaît en matière d'attaques informatiques pour les ordinateurs traditionnels a été transposé au monde du mobile dans son acception la plus large : virus, vers, dénis de service, *phishing* (voir les chapitres 4 et 5)¹... Tout y est. Et le pire, avec le développement de cette informatique, est à venir. Pour le moment, le nombre de cibles potentielles est relativement limité car les abonnés ne changent pas de mobiles aussi souvent que le souhaiteraient les constructeurs et opérateurs. Mais l'apparition de nouvelles normes de connexion (téléphonie 3,5 et 4G) et ses nouveaux services multimédias et interactifs — pour forcer à la consommation — devraient accentuer le risque.

La planète n'arrête pas de téléphoner ! Au rythme actuel de croissance du marché (22,5 % au deuxième trimestre 2006, 26 % au premier), il devrait se vendre un milliard de téléphones mobiles sur l'année 2006. Le seuil des 2 milliards d'utilisateurs dans le monde a été franchi en décembre 2005 et celui des trois pourrait être atteint vers 2010. En France, les derniers chiffres de l'Arcep indiquaient un taux de pénétration supérieur à 80 % à la fin de juillet 2006 avec plus de 48 millions d'usagers.

Ces quelques chiffres ont de quoi faire saliver bien des escrocs en tout genre. Imaginons que seulement 1 % de ces utilisateurs soient victimes d'une attaque informatique, cela représente quelque 20 millions de victimes ! Mais il est assez difficile d'obtenir des statistiques dans ce domaine. Les constructeurs de téléphones et surtout les opérateurs ne pratiquent pas la transparence : il ne faut pas effrayer le client potentiel. En février 2006, 267 codes malveillants pour smartphones ont été répertoriés. Officiellement, seule une trentaine sont efficaces et seulement cinq seraient réellement actifs. Mais cela correspond-t-il à la réalité ? Des discussions *off* avec des spécialistes du domaine — notamment appartenant aux sociétés de fourniture d'accès — semblent indiquer le contraire, sans qu'il faille céder à la panique. Un virus comme CommWarrior a fait des dégâts qui ne sont pas forcément connus du grand public, avec pour conséquence de la surfacturation de MMS.

Les messages MMS sont des messages à contenu multimédia gérés par les smartphones utilisant le système d'exploitation Symbian ou les téléphones compatibles. Ces messages peuvent contenir toutes sortes de données (images, sons, vidéo, fichier d'installation...). CommWarrior attaque les portables de la série Symbian 60 et se répand via les messages de type MMS ou via le protocole Bluetooth. Dans ce dernier cas, il recherche tous les appareils proches qu'il peut atteindre par ce protocole.

Enfin, le ver envoie des MMS aux contacts présents dans le carnet d'adresses, avec le ver en pièce jointe provoquant ainsi de la surfacturation (quelques dizaines de MMS par minute).

1. Philippe Richard, « Les smartphones, nouvelles cibles des pirates », *Les Echos*, 30 mars 2006, p.31.





Figure 17-1 — Le fichier SIS infecté est alors envoyé (à gauche) et proposé à l'installation. Le nom du fichier est aléatoire (à droite).



Image Copyright © F-Secure Corporation

Figure 17-2 — Fichier SIS infecté.



Les messages incitant la personne à activer le fichier SIS sont nombreux et utilisent tous l'ingénierie sociale. En voici quelques-uns :

3DGame from me. It is FREE ! Security update #12 Significant security update. See www.symbian.com

SymbianOS update OS service pack #1 from Symbian inc.

Happy Birthday! It is present for you! Porno images collection with nice viewer!

Norton AntiVirus Released now for mobile, install it!

L'exemple de CommWarrior est assez exemplaire de ce que font les codes malveillants pour smartphones. Que nous réserve l'avenir ? Voici en résumé quelles sont les évolutions du risque à prévoir¹ :

- La localisation linguistique des messages : pour le moment, l'anglais est la langue la plus utilisée, ce qui limite les possibilités concernant des utilisateurs francophones, mais pour combien de temps ?
- L'explosion des services et protocoles. Voici la chronologie selon les constructeurs :
 - 1990/2000 : Téléphonie et SMS
 - 2000/2003 : Messaging : SMS, WAP, MMS, e-mail
 - 2003/2005 : Systèmes Java ; Symbian ; WinCE
 - 2004/2005 : Multimedia : Camera, Video, Audio
 - 2004/2006 : Bluetooth, Ext Card, USB, WIFI
 - 2005/2007 : 3G : Video-téléphonie / Streaming...

Toutes ces technologies permettent de plus en plus d'applications et donc de plus en plus d'attaques. Gageons que la vidéo-téléphonie, à elle seule, va constituer un formidable potentiel d'attaque (voir le chapitre 5). Le passage au tout IP va également constituer un risque majeur.

- La nature du danger : en effet, la mobilité est tellement pratique qu'elle a investi tous les secteurs, à commencer par celui de la sécurité traditionnelle. Quel médecin, pompier, vigile, personnel de permanence n'a pas désormais d'appareil mobile pour les besoins de sa mission ou de sa permanence ? Cette dépendance vis-à-vis de ces environnements mobiles risque de devenir extrêmement préoccupante, surtout si aucune mesure de gestion de situation dégradée n'est prévue. La dictature de l'ergonomie frappe encore.
- L'interconnexion de tous les systèmes, mobiles ou non, entre eux : en 2006, l'existence d'un code, connu sous le nom de *CrossOver*, a été révélée. Ce code doit son nom au fait qu'il est capable d'infecter un environnement mobile (PDA, smartphone) à partir d'un simple PC. Le virus CardTrp, quant à lui, peut réaliser l'inverse (même s'il s'agit seulement d'une preuve de concept). De par leur nature et leur interaction avec les autres systèmes, les environne-

1. Certaines sont tirées de M. Morvan, « *Quelles menaces pour les téléphones mobiles ?* » Actes de la conférence SSTIC 2005. Disponible sur <http://www.sstic.org/>.



ments mobiles représentent des accès pouvant être utilisés pour pénétrer les systèmes classiques, pourtant protégés par un *firewall*. Mais là, ces périphériques se connectent derrière ces barrières.

- Les problèmes d'atteinte à la vie privée : mobiles, par définition, ces environnements vous suivent partout et renvoient de nombreuses informations sur vous et votre position.

Ce qui vient d'être évoqué ne concerne pas seulement les téléphones mobiles, mais tous les environnements informatiques. Les premiers virus destinés à la console portable de Sony (la PSP) et à celle de Nintendo (la DS) ont été identifiés en 2005 : Trojan.PSP.Brick.a pour la première et Trojan.NDS.Taihen.a pour la seconde. On a beaucoup parlé, cette même année, de virus ayant infecté des ordinateurs de bord de voitures (via une connexion Bluetooth, lors d'opérations de maintenance). Même s'il faut être prudent sur la réalité de ces cas — le manque de transparence des acteurs industriels n'aide pas vraiment —, les données techniques disponibles ne manquent pas ; elles prouvent que techniquement l'infection est réalisable.

17.2 L'INVISIBILITÉ ET L'OMNIPRÉSENCE

En plus d'être mobile, l'informatique devient de nos jours invisible et de fait omniprésente. La domotique est souvent évoquée. Microsoft et d'autres constructeurs y travaillent depuis plusieurs années pour exploiter ce qui est présenté comme l'un des Eldorado des nouvelles technologies. Pour schématiser, la domotique permet de régler le chauffage de son appartement et de fermer les volets à distance (via son téléphone par exemple) ou de commencer à faire rôtir un poulet dans le four (à condition qu'il y soit...). Quelles possibilités seront alors offertes au pirate qui pourra se connecter à votre réfrigérateur en ligne et vous faire livrer quelques dizaines de yaourts. Science-fiction ? Rien n'est moins sûr. Les premiers réfrigérateurs connectables au réseau existent déjà et de grandes enseignes les proposent à leur catalogue. Imaginons qu'un malfrat puisse récupérer des données personnelles via votre frigo ?

Mais dans l'immédiat le risque n'est pas là. Le danger concerne plutôt la RFID (*Radio Frequency Identification*) qui permet d'identifier à distance, sans contact physique ni visuel. Cette technologie, qui date de la seconde guerre mondiale¹ est en train d'envahir notre quotidien. Selon une étude américaine, environ 320 millions de ces puces ont été installées depuis 2002 dont 50 % dans l'industrie, 47 % dans l'automobile et 3 % dans la filière animale. Ce marché devrait progresser de 255 % d'ici à 2010 avec un CA de 2,3 milliards de dollars pour 65 milliards d'étiquettes en 2010.

La première étape est le remplacement du bon vieux code barre présent sur le moindre article ou bien de consommation. Mais elle promet maintenant une véritable

1. Elle permettait à la Royal Air Force de distinguer les avions alliés des avions ennemis, une sorte d'ancêtre de l'IFF.



révolution dans le monde industriel, médical et de la sécurité. Grâce à un lecteur spécial, le consommateur peut plus facilement repérer son fromage préféré dans le rayon d'un supermarché et de son côté, le chef de ce même rayon peut connaître en temps réel l'évolution de son stock. Cette solution est aussi utilisée par des laboratoires pharmaceutiques. Ils mettent des petites puces communicantes sur les bouteilles de médicaments afin de combattre la contrefaçon et la fraude. Autre application : la protection des documents. Une banque japonaise, la Nagoya Bank, a décidé d'intégrer un système de gestion de documents faisant appel à la RFID. Cette solution lui permet notamment de répertorier et de suivre des milliers de dossiers et savoir si un élément de l'un d'entre eux quitte une pièce ou un bâtiment. Enfin, ces puces pourraient aussi être exploitées pour contrôler l'accès à des lieux ou à des ordinateurs sensibles. Et même des hommes ! Au Mexique, des avocats et des juges se sont fait implanter une puce pour que la police les retrouve plus facilement en cas d'enlèvement.

Une atteinte à la vie privée ?

Comme les Etats-Unis sont en avance sur ce domaine par rapport à l'Europe, la polémique sur ces étiquettes high tech fait rage depuis quelques années. Le principal pourfendeur de cette nouvelle technologie est le Caspian (Consumers Against Supermarket Privacy Invasion And Numbering). Selon cet organisme, ces puces menaceraient la vie privée des consommateurs car elles pourraient permettre aux entreprises ou aux forces de l'ordre de lier chaque produit à l'identité de son acheteur.

Il est vrai que les grands magasins américains et certains industriels n'ont pas faits dans la finesse. Caspian a révélé que le « Carrefour américain », Wal-Mart, avait pratiqué des tests pour le compte de Procter&Gamble. Des puces RFID étaient placées sur des rouges à lèvres de la marque. Dès qu'une cliente se servait en rayon, le fabricant était alerté et pouvait suivre sur un écran d'ordinateur le comportement de la personne grâce à une Webcam du magasin !

Un système RFID est composé essentiellement de trois parties ¹:

- un transpondeur, appelé *tag* ou étiquette, qui est apposé sur les objets à identifier ;
- un lecteur permettant d'interroger ces étiquettes par radiofréquence ;
- un système de traitement de donnée, centralisé ou distribué au niveau de chaque lecteur.

Le facteur de risque est essentiellement lié aux étiquettes, lesquelles peuvent avoir une taille inférieure à celle d'un grain de riz et de ce fait être totalement invisible. Notons qu'une telle étiquette coûte quelques centimes d'euros seulement. Ces étiquettes peuvent être de deux sortes :

1. Gildas Avoine, « RFID et sécurité font-elles bon ménage ? » Actes de la conférence SSTIC 2006, p. 400-409. Disponible sur <http://www.sstic.org>.



- Passives : elles n'ont pas d'alimentation interne et se comportent en fait comme de simples codes barres. Le signal du lecteur induit un courant électrique suffisant pour que l'étiquette puisse émettre les informations qu'elle contient. La plus petite a une taille de 0,15 mm par 0,15 mm et est plus fine qu'une feuille de papier. Leur portée d'émission est de 10 cm à quelques mètres selon la norme.

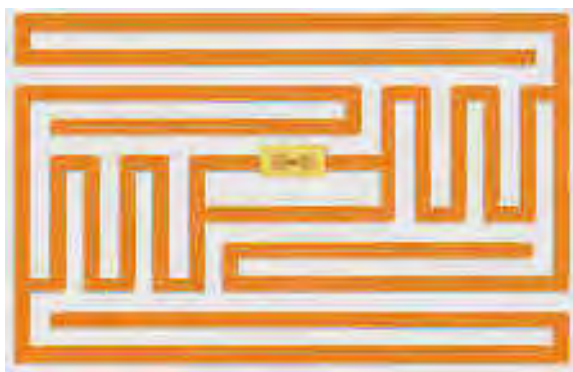


Figure 17-3 – Ces nouvelles étiquettes sont utilisées dans les bibliothèques pour gérer les fonds bibliothécaires et lutter contre le vol.

- Active : elles disposent de leur propre source d'alimentation interne et dispose de fait d'énergie suffisante pour conduire de véritable session de connexion avec un lecteur. Elles contiennent de la mémoire, peuvent émettre sur plusieurs centaines de mètres et leur batterie dispose d'une autonomie de près de dix ans. Elles sont utilisées par exemple pour marquer le bétail et pouvoir le localiser.

Ces tags sont utilisés dans un grand nombre d'applications :

- Moyen de paiement : métros de Moscou, de Londres, de New York, de Hong Kong, système Navigo de la RATP, péages d'autoroutes, remontées mécaniques dans les Alpes...
- Système de traçage des biens et des personnes¹ : codes barres, badges d'accès, cartes bancaires (la carte American Express intègre désormais des tags RFID à haute fréquence), passeports², cartes d'identité (la future carte d'identité française INES), systèmes de surveillance des prisonniers (depuis 2004 dans l'Ohio aux Etats-Unis)...

1. La société Carrefour a signé en février 2006 un contrat avec le fabricant Checkpoint Systems pour équiper ses 179 magasins.

2. Les passeports des citoyens américains intègrent une telle étiquette. Mais la peur de la voir utiliser par des terroristes et ainsi identifier facilement leurs cibles a obligé à modifier le système. Les tags n'émettent pas lorsque le passeport est fermé

- Contrôle à distance : des constructeurs automobiles (Toyota) ou de pneumatiques (Michelin depuis 2003) utilisent des tags FRID pour ce type d'application. Les systèmes antivol moderne fonctionnent ainsi et peuvent bloquer à distance un véhicule volé....

Et de très nombreuses autres applications¹...

Quel est le risque en termes de sécurité attaché à cette technologie ? Il semble quasi-illimité mais il est difficile de se faire une idée précise. En effet, comme pour d'autres technologies « stratégiques », les intérêts de toutes sortes empêchent qu'un débat véritablement ouvert et constructif puisse avoir lieu. Ces risques sont de deux types :

- Ceux liés à la technologie elle-même : pour le moment, seules quelques faiblesses dans les implémentations (faille de type *buffer overflow*), dans les protocoles de chiffrement ont semble-t-il été identifiés... aux dires des constructeurs. Mais la réalité pourrait être toute autre. Ainsi, Annalee Newitz du journal *Wired*² a montré comment en quelques secondes seulement il est possible de modifier le prix des denrées vendues dans certains supermarchés. La journaliste était simplement équipée d'un simple PDA et d'une petite antenne... Il était tout aussi facile de lire puis de cloner le badge permettant d'entrer dans un bâtiment « sécurisé », une chambre d'hôtel ou une voiture bardée d'électronique. Pire, semble-t-il, Annalee Newitz raconte comment Jonathan Westhues, un développeur de 23 ans, a également réussi à cloner la célèbre puce Verichip qu'elle s'était faite implanter dans le bras. Accessoirement, les puces RFID accessibles en écriture étant nombreuses, il serait également possible d'y placer subrepticement des « cookies », à la manière de ceux qu'envoient les sites web, afin de suivre à la trace le trajet des objets ainsi identifiés.

Pour Ari Juels, des laboratoires RSA, spécialisés dans la sécurité informatique, « le monde des RFID ressemble à l'internet à ses débuts » : l'un comme l'autre n'ont pas été sécurisés « par défaut », et ce n'est que des années après que l'on en mesure vraiment les conséquences. On dénombre pourtant d'ores et déjà des dizaines de failles ou d'utilisations détournées des RFID.

Que croire ? L'avis d'Ari Juels est pertinent. Les moyens seuls changent mais notre capacité à plus ou moins bien gérer les choses, à vouloir du profit avant tout restent les mêmes. Seul change également le « champ de bataille » des pirates : avec le RFID, le réseau est maintenant partout, invisible et omniprésent.

En mars 2006, une équipe de l'université d'Amsterdam a annoncé avoir réalisé plusieurs virus pour système RFID³. La nouvelle a jeté un trouble et le consortium

1. La lecture de l'article « Voila ce que nous réserve la biométrie », http://nice.indymedia.org/article.php?id_article=12589 permettra au lecteur de se faire une idée assez précise de l'utilisation à venir de cette technologie. Indymedia, 15/08/2006.
2. « RFID sous-cutanées en avoir ou pas ? » Internet Actu, 6/6/2006.
3. M. Rieback, B. Crispo et A.S. Tanenbaum, « Is your cat infected with a computer virus ? » (« Votre chat est-il infecté par un virus informatique ? »), Conférence IEEE, Pise. Ces résultats ont également été présentés lors de la conférence TCV 2006 à Nancy en mai 2006.



pour la technologie RFID s'est empressé de nier ou au moins d'amoindrir ces résultats. Si ces résultats utilisent des faiblesses supposées dans le système et sont donc « discutables » quant à une efficacité réelle, ils n'en demeurent pas moins importants car ils illustrent le fait que la moindre faille dans le système sera techniquement et immédiatement exploitable. Mais qui pourra contrôler un système devenu invisible et omniprésent ?

Ceux liés à l'utilisation de cette technologie. On ne peut s'empêcher d'avoir une vision orwellienne de ce que sera la société gouvernée par la technologie RFID. Qui pourra empêcher un dirigeant d'entreprise, un gouvernant extrémiste, une dictature... d'en faire un usage que l'on ose imaginer. Avec le RFID, le pirate peut très bien être l'Etat lui-même. Imaginons ce que la technologie RFID a dû permettre de faire depuis que le *Patriot Act* a été voté outre-Atlantique. La traque multicritères des citoyens sera alors possible. Certes, en France, la CNIL veille mais avec une technologie invisible en aura-t-elle la possibilité ?

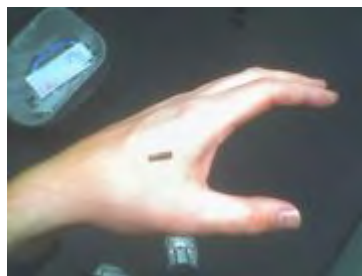
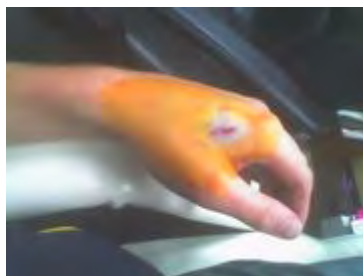


Figure 17-4 — Le pire réside certainement dans tags RFID implantés sous la peau.

Ce qui était jusqu'à présent réservé aux bovins et autres animaux s'appliquera alors aux hommes. Des boîtes de nuit à Rotterdam et à Barcelone proposent à leurs clients VIP — qui trouvent cela « tendance » — de se faire implanter sous la peau un moyen de paiement RFID. Au Mexique, en Australie les personnels de tribunaux ou de banques se font implanter de tels tags à des fins d'identification.

La technologie RFID pose donc un « certain nombre » de problèmes et de questions de société. Mais, cette technologie pourrait bien faire voler en éclat le principe même de sécurité informatique, entre autres choses. Alors que les seules solutions consistent à cloisonner ou à isoler les réseaux et les infrastructures sensibles, qui peut prédire l'effet final d'un tag RFID actif et caché dans un disque dur ou pire dans un processeur. Et pourra-t-on le détecter ? Aujourd'hui, il est très difficile de savoir ce que peut faire réellement un logiciel. Cette incertitude — pour ne pas dire inquiétude — concernera aussi le matériel. Imaginons un tag RFID servant de relais pour émettre des informations capturées dans un ordinateur. Plus besoin de prise réseau.

Ces quelques incursions dans un futur qui se rapproche toujours plus vite ont permis d'entrevoir comment la cyber-criminalité pourrait évoluer. La technologie aidant, les attaques pourront viser potentiellement un nombre toujours plus important de cibles. Verra-t-on un jour un 11 septembre informatique (des vers ayant

infectés des systèmes informatiques embarqués par exemple, pilotés par radiofréquence) ? Qui sait ? Science-fiction pour les uns, champ d'investigation pour les attaquants. « La société devient de plus en plus dépendante des télécommunications. Nous pensons qu'un jour, il y aura des attaques globales, c'est-à-dire classiques et numériques, nous a déclaré un haut responsable de la sécurité informatique de l'Etat. Nous faisons des exercices avec les différents départements ministériels et nous simulons sur papier comment nous pourrions communiquer avec le papier, sans téléphone, ni internet. Ce qui m'inquiète le plus c'est la grosse panne qui paralyserait tout. »

Mais les dénégations de telle ou telle corporations ou lobby n'empêcheront pas les pirates d'agir si la technologie le permet. Les attaques frapperont des gens endormis par des discours lénifiants et rassurants. Comme disait un humoriste : « la dernière phrase que l'on entendra durant l'apocalypse (nucléaire) sera que c'était techniquement impossible ». Le futur de la cyberdélinquance pourrait très bien être celui-là.

Alors faut-il désespérer ? Aucunement. Mais tout cela rappelle que l'humain doit rester le maître en toutes choses. Si l'ingénierie sociale permet à l'attaquant de frapper efficacement, le bon sens, la sagacité, la vigilance et la prudence permettent également à un RSSI de savoir comment organiser et faire évoluer la sécurité des systèmes de sa société. Jean Bodin disait : « Il n'est de richesse que d'hommes ! ».

Et si les personnes les mieux protégées étaient celles que nous considérons avec condescendance comme du « mauvais » côté de la fracture numérique ? Les pays soi-disant « en retard » en matière de technologies de l'information et de communication ne seront-ils pas en fait les mieux protégés et les moins touchés le jour où « la grande panne » tant redoutée par les responsables, surviendra ? Un « Pearl Harbour numérique » ne risquerait-il pas de changer la polarité de la planète et d'inverser les équilibres géostratégiques ? L'avenir le dira.

En résumé

Au fur et à mesure que l'informatique et les technologies numériques s'immiscent, souvent à l'insu des utilisateurs, les risques d'attaques et d'infection en tout genre se multiplient. Les téléphones portables, et de façon plus générale tous les appareils mobiles, et les étiquettes communicantes (RFID) constituent de nouveaux terrains d'investigation pour les pirates. Plus que jamais la vigilance s'impose. Seuls les paranos survivront-ils à ce développement de la cybercriminalité ?



Bibliographie

OUVRAGES ET ARTICLES DE RÉFÉRENCE

MISC Le journal de la sécurité informatique : revue vendue en kiosques et traitant de tous les aspects de la sécurité informatique (techniques, réglementaires, guerre de l'information, droit...). Bimestriel.

Revue La lettre des techniques de l'ingénieur - Sécurité des systèmes d'Information, éditions des Techniques de l'ingénieur : lettre bimestrielle présentant de manière didactique et condensée les aspects techniques et les enjeux en matière de sécurité des SI. Bimestrielle.

Actes des conférences SSTIC (Symposium sur la Sécurité des Technologies de l'Information et des Communications). Conférence nationale annuelle réunissant tous les spécialistes et professionnels de la sécurité informatique francophones. Les articles sont disponibles gratuitement en ligne sur le site <http://www.sstic.org>.

Le hold-up planétaire, de Roberto Di Cosmo et Dominique Nora. Ce texte a été publié par les Éditions Calmann-Lévy et les Éditions 00h00 en 1998. L'éditeur ne souhaitant plus le réimprimer, les auteurs ont récupéré les droits d'auteur sur ce livre. Ils ont décidé de le mettre à disposition de la communauté (sous licence Creative Commons Attribution-NoDerivs-NonCommercial). Il sera toujours disponible sur <http://www.pps.jussieu.fr/~dicosmo/HoldUp/HoldUpPlanetaire.pdf>.

Encyclopédie de la sécurité informatique. Ouvrage collectif sous la direction de Claude Kirchner. Vuibert, 2006.

Protection des systèmes d'information, Qualité et sécurité informatiques, sous la direction de philippe Rosé, Référentiel de 4800 pages + 1 CD-Rom. Mise à jour trimestrielle. Dunod.

Sécurité des Systèmes d'Information. Ouvrage collectif sous la direction de M. Maknavicius-Laurent. Techniques de l'Ingénieur, vol. TI400, 2004. Ouvrage didactique et très complet, accessible à un public non spécialiste.

Sécurité des systèmes d'information. Ouvrage collectif sous la direction de Ludovic Mé, (traité IC2). Lavoisier, 2006.



Les virus informatiques : théorie, pratique et applications de Eric Filiol. Springer Verlag, Collection IRIS, 2004.

Évaluation des logiciels antivirus : quand le marketing s'oppose à la technique de Éric Filiol. MISC – *Le journal de la sécurité informatique*, numéro 21, sept. 2005.

La simulabilité des tests statistiques de Éric Filiol. MISC – *Le journal de la sécurité informatique*, numéro 22, novembre 2005.

Sécurité informatique et réseaux. S. Ghernaoui-Hélie, Dunod, 2006..

Utiliser votre PC en toute sécurité de T. Gérard, Éditions Dunod/Micro Hebdo, 2005.

Halte aux hackers (4e édition) de Mclure, Scambray et Kurtz. OEM/Eyrolles, 2003.

Google Hacking, Mettez vos données sensibles à l'abri des moteurs de recherches. J. Long, Dunod, 2005.

Tout sur la sécurité informatique de J-F. Pillou. Dunod, 2005.

Stratégies anti-hackers, (2^{ème} édition) de Russell. OEM/Eyrolles, 2003.

Secrets et mensonges de B. Schneier. Vuibert, 2001.

Histoire des codes secrets de Singh. Lattès, 1999.

Les protocoles de sécurité d'Internet, S. Natkin, Dunod, 2002



Sites utiles

Sites gouvernementaux

CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques). www.ssi.gouv.fr.

OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication). www.interieur.gouv.fr

Legifrance (service public de la diffusion du droit). www.legifrance.gouv.fr.

Autres sites

CLUSIF (Club de la Sécurité Informatique des systèmes d'information Français). www.clusif.asso.fr.

CNIL (Commission Nationale Informatique et Libertés). www.cnil.fr.

Mag Secur : magazine dédié à la sécurité informatique. www.mag-secur.com/.

Vulnérabilité : site spécialisé dans la sécurité informatique. www.vulnerabilite.com/.

Internet sans crainte. <http://www.internetsanscrainte.fr/>.

Journal du Net. www.journaldunet.com.

01Net, **Silicon** et **Zdnet**. Trois sites dédiés aux nouvelles technologies et à l'informatique. www.01net.com, www.silicon.fr et www.zdnet.fr.

CNRS : site dédié à la sécurité et à la protection du patrimoine scientifique. www.sg.cnrs.fr.

F-Secure et Kaspersky : sites de deux éditeurs de logiciels de sécurité. De nombreuses informations sur les derniers codes malveillants. www.f-secure.fr et www.kaspersky.com/fr.

Les Echos. Quotidien économique avec chaque mercredi le cahier « Echos Innovation ». www.lesechos.fr.

Action innocence. Constituée en novembre 1999, cette organisation non gouvernementale (ONG) à but non lucratif lutte contre les abus sexuels impliquant des enfants sur Internet. www.actioninnocence.org

Internet Mineurs. Site fondé par les ministères de la Justice, de l'Intérieur, de la Défense et de l'Emploi. www.internet-mineurs.gouv.fr



Filtra Info. Créé par Action Innocence, ce site a pour objectif d'évaluer, tous les 6 mois au minimum, les solutions de contrôle parental disponibles sur le marché. www.filtra.info.

Assiste et Zebulon. Deux très bons sites informatiques avec notamment des forums thématiques (dont un dédié à la sécurité) très réactifs et aux réponses pertinentes. Assiste publie aussi une « liste noire », non exhaustive, des logiciels inutiles, voire dangereux car inefficaces. www.zebulon.fr et <http://assiste.free.fr>.



Index

Numériques

3D-Secure 83

A

antivirus 107

Arpanet 175

B

BEFTI 168

blogs 66, 75

Bluetooth 27

bombe logique 65

botnet 5, 58

Brigade de Protection des Mineurs 150

bug de l'an 2000 125

C

Carnivore 183

carte bancaire 77

Carte Vitale 35

cartes de paiement, 34

CERTA 167

cheval de Troie 68

chevaux de Troie 4

ChoicePoint 30

Convention sur la cybercriminalité 193

COSSI 166

Crypto AG 186

cyber-guerre 176

cyber-terrorisme 176

D

DCSSI 165

DDoS 5, 66, 67

défaçage 120

defacement 9

DMZ (zone démilitarisée) 121

DST 168

E

eBay 88

eCarte Bleue 87

eGold 87

EMV 83

F

filtres ICRA et Safesurf 153

Fournisseurs d'accès à Internet 70

G

Google 67

H

hacker 9

hackers 177, 179

Hoax 15

I

ICAN 175

ingénierie sociale 14



K

keylogger 45

L

L'officier de sécurité (ou RSSI) 118

Licorne 31

logiciel de contrôle parental 152

logiciels antisпам 73

Loi Godfrain 191

M

Magic Lantern 183

mass mailing 74

Mastercard 33

messagerie instantanée 46

micro paiement 86

Mots de passe 17

N

NSA 177

O

OCLCTIC 169

ordinateurs portables 32

P

PayPal 86

PC zombies 5

pédophiles 149

phishing 15, 39, 196

proof-of-concept 2

R

racket 65

ROKSO 70

rootkit 198

RSSI 127

S

screenloggers 53

serveur proxy 122

serveur reverse proxy 123

sites d'enchères 88

spam 43, 69, 194

spam nigérian 70

Spamhaus 70

spams 66

spywares 197

SSL 82

T

Ticket Surf 87

tokens 88

V

ver espion 184

vishing 55

VoIP 63

voix sur IP 46

Vol de données 119

vulnérabilités 23

W

web bug 185