D.U. CRIMINALISTIQUE

La CYBERCRIMINALITE

Cybercriminalité : **activité dans laquelle les systèmes et les réseaux informatiques sont une cible, un moyen ou un lieu pour réaliser des activités délictueuses ou criminelles.**

L'informatique est un marché commercial mondial.

En marge du commerce, deux types d'attitude :

Les « Whitehats » : des scientifiques et des passionnés :

- Relèvent les défis technologiques.
- Développent des systèmes et des logiciels libres > Ubuntu, Linux, OpenOffice…..
- Cherchent les failles : Carte Bleue….

Les « Blackhats » évoluent vers les hackers.

Dans les années 90, la cybercriminalité avait un côté artisanal, contestataire et ludique…
Dans les années 2000, elle devient une industrie, source de revenus… : c'est une des formes de délinquance organisée

Quelques termes :

- TIC :Technologies de l'Information et la Communication
- RSSI : Responsable de la Sécurité des Systèmes d'Information
- Hacker : bidouilleur….pirate informatique

LE SPAM :

95% des mails sont des spams…

Les hackers se constituent des réseaux de plusieurs dizaines de milliers d'ordinateurs Zombies : les botnets. *Bot : robot Net :réseaux*
Pour créer ces réseaux, le hacker utilise tous les moyens à sa disposition :

- Envoi de mails piégés, de PowerPoints, sites piratés, etc…
- Il achète des kits de logiciels malveillants (malwares). (au second semestre 2009, 915 197 malwares visant Windows ont été détectés)

Par exemple :

Venue d'Ukraine, une nouvelle boite à outils pirate du nom de Spyeye fait son apparition.
Le kit permet de créer :

- *un cheval de Troie,*
- *un espace web de contrôle et*
- *des options comme un keylogger (qui intercepte les frappes clavier) ;*
- *le remplissage automatique des espaces dédiés aux cartes de crédits.*

*Il est commercialisé entre 350 et 700 euros. (février 2010)*Les hackers sont alors prêts à louer leurs réseaux d'ordinateurs zombis pour envoyer des spams, se livrer à des attaques, etc…

Un ordinateur « zombi » est un ordinateur

- connecté à Internet, mal protégé,
- dans lequel, on a introduit un virus ou un cheval de Troie, et
- qui accomplit des tâches malveillantes, de n'importe quelle nature,
- à l'insu de son propriétaire (silencieusement) et
- sous la direction, à distance, de l'attaquant.
- Et cela, sans perturber le fonctionnement de l'ordinateur.

Le but étant de louer ces ordinateurs zombies, cette « force de travail » à des « commerçants »
On considère que 25% des PC dans le monde sont des ordinateurs zombis.
Le but **premier** est de faire de la publicité à moindre prix : les spammeurs sont donc rémunérés.

Il existe des spams ciblés : les spams pédophiles.

On appelle « spam » l'envoi **massif** de courriers électroniques à des destinataires ne **l'ayant pas sollicité.**
En 2010, chute des tarifs : le zombi est à 10 centimes !!!

A qui envoyer les spams ?

➢Les spammeurs collectent des adresses électroniques sur internet (dans les forums, sur les sites internet, dans les groupes de discussion, etc.)

–grâce à des logiciels, appelés « *robots* », parcourant les différentes pages et stockant au passage dans une base de données toutes les adresses électroniques y figurant.

–Grâce au phishing

➢Il ne reste ensuite au hacker qu':

- à envoyer à chaque adresse mail un message publicitaire : Viagra, médicaments, bijoux, images pédophiles.
- qu'à procéder à des attaques (voir plus loin : **déni de service)**

➢Tarifs 2010: vous pouvez envoyer

- 5 millions d'adresses e-mails pour 140 euros ou encore
- 20 millions d'adresses emails à spammer pour seulement 350 euros

PLAN

I. INFRACTIONS TECHNOLOGIQUES LIEES AUX T.I.C.

1. Atteintes contre les S.T.A.D.

a) Accession ou maintien frauduleux dans un Système Automatique de Traitement de Données (S.T.A.D.)

Article 323-1 Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

b) Suppression, modification de données. Altération de fonctionnement

Article 323-1 Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

c) Entraver ou fausser le fonctionnement d'un S.T.A.D.

Article 323-2 Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004
Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Extorsion par Déni de Service (saturation d'un site en effectuant des centaines de milliers de demandes au même moment, en utilisant des botnets - voir plus haut) : chantage

d) Introduction, suppression, modification de données

Article 323-3 Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004
Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

e) Fourniture de moyens

Article 323-3-1 Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

f) Groupement de pirates

Article 323-4 Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

2. Traitement de données à caractère personnel

La loi Informatique et Liberté, dès 1978, préservait des déviances informatiques.

Article 1er
« L'informatique doit être au service de chaque citoyen. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »

a) L'ELEMENT MATERIEL:
la mise en œuvre d'un fichier ou d'un logiciel d'exploitation des données à traiter **sans avoir respecté les procédures légales** (déclaration CNIL, etc.).

➢Il s'agit de délits continus,
➢Le délai de prescription part de la date de révélation des faits délictueux.
➢La notion « intentionnelle » a été atténuée, car le législateur a introduit la formule « y compris par négligence »

b) NORMES NON RESPECTEES
- le **non respect des formalités préalables pour constituer un fichier** (terme que pudiquement la loi nomme: traitement automatisé d'informations **nominatives**) est puni de 3 ans d'emprisonnement et 45000 euros d'amende (art. 226-16 CP.).
- **l'absence de précaution dans le stockage des données nominatives** est puni de 5 ans d'emprisonnement et de 300000 euros d'amende (art. 226-17 CP.).

c) COLLECTE DELOYALE
- Le fait de **collecter des données** à caractère personnel **par un moyen frauduleux, déloyal ou illicite** est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende (art. 226-18 CP.)
- **Malgré l'opposition de la personne**, lorsque le traitement répond à des fins de **prospection, notamment commerciale**, ou lorsque cette opposition est fondée sur des motifs légitimes (art. 226-18-1 CP.).
- **Sans accord express de l'intéressé**, il est bien sûr interdit de faire apparaître les **origines raciales, les opinions politiques, philosophiques ou religieuses**, tout comme l'appartenance syndicale ou les **mœurs de personnes** >> puni de 5 ans d'emprisonnement et 300 000 euros d'amende (art. 226-19 CP.).

d) LIMITES
- les articles 226-20, 21 et 22 punissent :
  - la divulgation, (porter ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir). Ex : le STIC
  - le détournement (transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un État n'appartenant pas à la Communauté européenne).
  - la conservation : la durée de conservation des données n'est pas illimitée. Elle doit toujours être précisée.

3. Infractions à la carte bancaire

Loi n°2001-1062 du 15 novembre 2001 relative à la Sécurité Quotidienne Art. 35-39 et 40

- Fabrication, acquisition, détention, cession, offre, mise à disposition d'équipements, instruments, programmes informatiques ou données conçues ou adaptées pour fabriquer des fausses cartes de paiement : punit de 7 ans d'emprisonnement et 750 000 euros d'amende

4. Chiffrement / Cryptage

Article 434-15-2 **Loi n°2001-1062 du 15 novembre 2001 - art. 31 JORF 16 novembre 2001**

- Punit de trois ans d'emprisonnement et de 45 000 euros d'amende,
- Le fait, pour quiconque ayant connaissance de la **convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre,**

Pour décrypter des documents dans un dossier pénal,

- le magistrat saisit
- l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (O.C.L.C.T.I.C.) qui transmet à la
- Direction Centrale du Renseignement Intérieur (D.C.R.I.) qui transmet au
- Centre Technique d'Assistance (C.T.A.)

II. INFRACTIONS TECHNOLOGIQUES FACILITEES PAR LES T.I.C.

Internet apparaît le plus souvent comme un vecteur de multiplication des infractions réalisées au moyen de la technologie (informatique, réseaux, etc.…).

1. La pédopornographie

A. Diffusion d'images pornographiques de mineurs sur un réseau

a) art. 227-23 du C.P.
- Fixer, enregistrer, transmettre, rendre disponible, offrir ou diffuser par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter
- Les peines sont aggravées lorsqu'un réseau de télécommunications a été utilisé pour diffuser l'image ou la représentation du mineur à destination d'un public non déterminé.

b) loi n°2002-305 du 04 mars 2002
- sanctionne la détention d'une image ou représentation pornographique d'un mineur;

c) loi n°2004-204 dite Perben 2
a créé la circonstance aggravante de commission en bande organisée de l'infraction d'enregistrement et de transmission d'images pédopornographiques

d) l'offre d'image pédopornographique est également pénalisée

e) **la loi n°2007-293 du 5 mars 2007 réformant la protection de l'enfance** créé une nouvelle infraction, en l'occurrence, le fait de consulter **habituellement** un site de pédopornographie.

Note :

- Apparence d'un mineur suffit, sauf si majorité établie au moment de la captation d'image.
- Représentation virtuelle d'un mineur interdite (loi n°98-468 du17/06/98)
- En matière de diffusion de contenus illicites sur Internet, la possibilité d'y avoir accès en France, suffit à constituer le délit et à attribuer la compétence aux juridictions nationales. De même, si les auteurs résident hors de France. (art 113-2 du C.P.)

- En cas « mise en péril des mineurs », proxénétisme, traite des êtres humains : possibilité d'« infiltration numérique » par des enquêteurs spécialisés – mais pas de provocation / incitation sous peine de nullité.

2. Infractions de presse >>

a) **Diffamation et injures**

En l'occurrence, sur le web, c'est-à-dire sur un site, un blog ou un forum ouvert
Mails et forums « fermés » ne sont pas concernés

b) **Provocation à la discrimination, diffamation et injure raciale**

La Loi Gayssot s'applique également sur le Net

3. Escroqueries

Il n'existe pas en droit pénal français d'incrimination spécifique pour les escroqueries commises via Internet.
L'utilisation du vecteur informatique ne constitue pas non plus une circonstance aggravante de l'escroquerie.

Article 313-1 du CP
L'escroquerie est le fait,

- soit par l'usage d'un faux nom ou
- d'une fausse qualité,
- soit par l'abus d'une qualité vraie,
- soit par l'emploi de manoeuvres frauduleuses,

de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

Escroqueries dans

a) le commerce de biens,
b) l'offre de services et
c) la fausse loterie
d) **La « Nigériane » ou « scam » Technique très ancienne jouant sur l'appât du gain et l'émotion**
    1. **La « prisonnière espagnole » au XVIe siècle.**
    2. **La « lettre de Jérusalem » en France à la fin du XVIIIe et au début du XIXe siècle**

    Ère quasi-industrielle grâce à internet

e) **Le « phishing » ou hameçonnage**

Les escrocs envoient des messages à un maximum d'internautes (les « spams ») en se faisant passer pour une banque, par exemple. Ils invitent les destinataires à mettre à jour leurs comptes bancaires sur Internet en indiquant leur noms et mots de passe. En fait, ils les communiquent aux escrocs qui peuvent alors vider les comptes bancaires.

4. Autres infractions

a) **Contrefaçon / vol ou copie de contenus**

Infractions au Code de la Propriété Intellectuelle

b) **Paris et jeux de hasard en ligne**

Nouveaux textes en 2010 : les jeux sont autorisés sur le territoire français

c) **Diffusion de mode d'emploi et de fabrication armes & de moyens de destruction** Explosifs : TATP

d) **Mise en relation d'un mineur avec un adulte**

e) **Chats, forums, messageries instantané, etc..**

f) **Corruption de mineurs**

III. LES SERVICES DE LUTTE CONTRE LA CYBERCRIMINALITE

1) ANSSI : **L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) créée le 8 juillet 2009 a vocation à protéger les réseaux gouvernementaux et sensibiliser tous les publics aux menaces de l'Internet.**

2) GENDARMERIE
   - **IRCG Rosny sous Bois**
     - **Service de Recherches Judiciaires et de Documentation (S.T.R.J.D.)**
       >> surveillance réseaux
     - **Centre National d'Images Pédopornographiques (C.N.A.I.P.)**
       >> base de données d'images pédophiles

3) L'O.C.L.C.T.I.C.

(Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication)
   - **P.H.A.R.O.S. >> Plate-forme d'Harmonisation d'Analyse, de Recoupement et d'Orientation des Signalements >> depuis 2006**
   - **la plate-forme téléphonique "INFO ESCROQUERIES" 08 11 02 02 17**
     outil d'information et de prévention