La cybercriminalité et l'expertise judiciaire

Michel Villard (70),
expert près la cour administrative d'appel de Paris,
http://villard-expert.fr

Le contexte

Définition

La "cybercriminalité" désigne l'ensemble des infractions pénales susceptibles d'être commises sur les réseaux de télécommunications en général et notamment sur le réseau Internet.

La cybercriminalité correspond à deux catégories d'infractions pénales :
• les infractions où l'informatique est l'objet même du crime ou du délit ;
• les infractions pénales "classiques" commises au moyen d'Internet, notamment :
– les infractions relatives aux atteintes à la dignité humaine,
– les infractions au Code de la propriété intellectuelle (art. L335-1 à 4 du CPI),
– les infractions à la loi sur la presse (loi du 29 juillet 1881),
– les infractions contre les biens.

Les textes législatifs récents

La loi "informatique et libertés" du 6 janvier 1978 (art. 226-16 à 24 du Code pénal (CP) relative à l'informatique, aux fichiers et aux libertés vise notamment à combattre la création de fichiers nominatifs clandestins et réprime plusieurs infractions portant atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques.

La loi du 5 janvier 1988 dite "loi Godfrain" (art. 323-1 à 7 du CP) incrimine les accès et le maintien frauduleux dans un système de traitement automatisé de données, les modifications et les altérations de données.

L'article 40 de la loi sur la sécurité quotidienne du 16 novembre 2001 insère deux articles après le L. 163-4 du Code monétaire et financier, sur le fait de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés pour contrefaire des cartes.

La loi pour la confiance dans l'économie numérique (n° 2004-575 du 21 juin 2004) définit notamment les obligations générales des prestataires techniques de l'Internet (fournisseurs d'accès et hébergeurs) en matière de conservation des données d'identification des auteurs de contenus ainsi que l'absence de leur obligation générale de surveiller les contenus stockés ou transmis.

Le projet de convention européenne sur la cybercriminalité du 23 novembre 2001, adopté par le Conseil de l'Europe le 8 novembre 2004, doit devenir le premier document international contraignant dans le domaine d'Internet.

Les États-Unis, le Japon et le Canada, qui ne sont pas membres du Conseil de l'Europe mais bénéficient du statut d'observateur auprès de l'organisation, seront également invités à signer et à ratifier ce texte, à la rédaction duquel ils ont été associés.

La Convention entrera en vigueur dès que cinq États, dont au moins trois du Conseil de l'Europe, l'auront ratifiée.

Ce traité, qui a suscité pas moins de 27 versions en quatre années d'élaboration, vise à l'adoption d'une "*politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale*".

Il enjoint les États à poursuivre pénalement un certain nombre d'infractions relatives à l'usage des réseaux, telles que les accès illégaux, la falsification de données, la diffusion de virus ou les atteintes à la propriété intellectuelle, mais également aux contenus lorsqu'il s'agit de pornographie enfantine.

Il fixe également aux fournisseurs d'accès des règles pour la conservation et le stockage des données afin de permettre un contrôle éventuel, par les autorités compétentes, des opérations et des messages informatiques susceptibles de constituer des délits.

L'expertise informatique en cybercriminalité

En procédure pénale, le policier, le magistrat et l'expert travaillent en équipe. Avant tout, les objectifs et la méthode doivent être clairement définis.

La conservation des preuves informatiques

Il est prioritaire de conserver la preuve qui peut exister sur le support de stockage original (disque dur interne

ou externe, clé USB, disquette, CD, DVD, etc.).

En effet, un démarrage d'ordinateur ou un simple accès en lecture va modifier des fichiers sur le disque.

C'est pourquoi il faut réaliser une copie parfaite du support original avec un dispositif de blocage en écriture, et les investigations seront réalisées sur cette copie.

Si l'original doit être laissé sur les lieux de la perquisition, deux copies sont nécessaires.

La recherche de preuves sur supports informatiques

Le travail de l'expert est alors de déterminer si le support contient des données frauduleuses. Une première difficulté est d'isoler l'information pertinente.

La recherche de preuve doit être faite à l'aide d'un logiciel d'investigation [1] spécialisé de type EasyRecovery, EnCase, Forensic Toolkit, X-Ways Forensics ou équivalent.

D'abord, il est important de noter les dates précises (création, dernière modification, dernier accès, dernière impression), même si la date sur un système informatique n'est qu'un indice et ne peut pas être une preuve.

Parfois, des incohérences sont détectées sur les dates, par exemple une date d'impression antérieure à la date de création.

Les logiciels d'investigation ont par ailleurs une fonction "histogrammes des dates", sur tous les fichiers ou sur un sous-ensemble de fichiers sélectionnés par un filtre. Une incohérence dans un histogramme de dates est souvent révélatrice d'une falsification de date système.

Suivant la mission définie par le juge d'instruction, l'expert va donc rechercher une preuve ou des indices convergents, par exemple :

- fichiers effacés récupérés, pour les visualiser et les imprimer, et dates d'effacements ;
- adresses URL (Uniform ressource locator) de sites Internet visités et dates des visites ;
- fichiers illicites téléchargés (exemple : vidéos, images à caractère pédophile), comparaison des signatures avec les fichiers téléchargeables du site en ligne, si l'adresse URL est identifiée ;
- échanges de courriels, falsification de dates, identité du véritable émetteur et du chemin suivi par un message reçu (exemple : usurpation d'identité, recherche d'un "corbeau") ;
- mots clés contenus dans des documents ou des courriels (exemple : racisme, contestation de crime contre l'humanité, terrorisme, propos injurieux ou diffamatoires) ;
- traces (adresse IP, date et heure) d'une intrusion par un pirate ;
- comptabilité truquée ;
- données qualifiées de "secrets industriels" (exemple : fichiers de clients, données financières) ;
- piratage de films et de musique ;
- contrefaçon de marque, de modèle, de carte à puce.

La lecture de puces électroniques et de bandes magnétiques

L'expertise en falsification de carte commence par la lecture des données stockées sur la puce ou sur la piste magnétique de la fausse carte saisie par la police.

Il est rappelé qu'une carte bancaire contrefaite (ou YESCARD, qui valide n'importe quel code PIN) permet au malfrat de faire des transactions sur des automates (ex. carburant, billetterie SNCF) et de retirer de l'argent dans des pays étrangers, notamment en Belgique, tant que la transaction n'interroge pas le serveur central du GIE carte bancaire.

À l'aide d'un équipement matériel et logiciel adapté, l'expert va lire le numéro de carte bancaire, le nom du porteur, les dates de validité, et l'historique des transactions récentes.

De manière similaire, sont récupérables, sur la carte SIM d'un téléphone portable, le répertoire, les numéros des appels récents émis et reçus et les SMS conservés.

D'autres exemples de fausses cartes sont la carte Vitale, les cartes d'abonnement aux chaînes TV câblées et les cartes de paiement des grands magasins.

La recherche de traces sur Internet

L'internaute, depuis le navigateur de son ordinateur, accède *via* sa connexion réseau au serveur du fournisseur d'accès, puis chemine d'un serveur A à un serveur B *via* X serveurs.

Il est identifié par une adresse IP, fixe si la connexion est en haut débit mais flottante pour le bas débit.

Par exemple, un pirate Internet pénètre sur la machine d'une entreprise, y laisse des traces (adresse IP et date/heure). Grâce à une réquisition au fournisseur d'accès faite par la police, celui-ci communique le nom et l'adresse du compte titulaire de l'abonnement Internet et également le numéro de téléphone appelant, ce qui permettra de vérifier qu'à l'heure donnée le pirate était bien connecté.

Dans le cas d'un "corbeau" qui envoie un message, la trace se trouve cette fois dans l'en-tête Internet du message reçu. Dès lors, comme dans le cas précédent, on peut remonter à la machine émettrice du message.

Toutefois, la plupart des serveurs de messagerie ne conservent pas le message une fois téléchargé par le destinataire, sauf les serveurs de type Yahoo ou Caramail, et cela tant que l'internaute ne va pas l'effacer.

Dans certains cas, l'utilisateur n'est pas détectable : machine d'un cybercafé, connexion en "*peer-to-peer*" [2].

Enfin, l'expert, grâce à des logiciels spécialisés qui interrogent des annuaires en ligne, peut tracer la route géographique d'une requête vers un serveur Web. Souvent, il constatera que les bases de données à contenus illicites sont déportées à l'étranger. Une astuce consiste alors à demander la saisie de la comptabilité, pour trouver trace de paiements vers l'étranger. n

Pour en savoir plus, se reporter à l'encadré du bas de la page 40.

1. En anglais : *forensic tool*.

2. Sur Internet, "*peer-to-peer*" (point à point) désigne la possibilité de connecter entre eux des ordinateurs pour l'échange de fichiers, sans passer par un serveur centralisé ou par un site Web.