Honeypot : un pot-pourri...juridique

Marie Barel

Juriste, spécialiste en droit
des technologies de l'information et de la communication
et sécurité de l'information
marie.barel@legalis.net

Résumé Les systèmes pot de miel, qui continuent de se développer dans le domaine de la recherche, connaissent un regain d'intérêt auprès des responsables de systèmes d'information qui souhaitent optimiser les outils en place (IDS par exemple) ou justifier l'augmentation des budgets alloués à la sécurité auprès des directions générales. Certains freins demeurent néanmoins, et en particulier les incertitudes liées aux risques juridiques. Dans cet article, nous tenterons donc d'évaluer ces risques, de façon à ce que les responsables de projet honeypot puissent ensuite définir un déploiement légalement maîtrisé.

1 Introduction

Janvier 2004.- Les prévisions des analystes américains indiquent un pis aller en matière de délinquance informatique et de cyber-terrorisme et les experts s'alarment de la sophistication croissante des crimes informatiques. Pour tenter de cerner cette menace de l'intérieur et pouvoir étudier la faune de ces cyber-pirates, la communauté des experts en sécurité informatique continue de déployer un nouveau[1] concept : celui des *honeypots* ou, dans sa traduction française, de (systèmes) " pots de miel "...

[1] En réalité, le concept de honeypot n'est pas si nouveau que cela... Petit rappel historique : Cliff Stoll rapporte dans son livre [1] les premiers balbutiements du concept de honeypot, lorsque dans le cadre d'une investigation qu'il menait à l'Université de Berkeley (en 1986), celui-ci a été amené à alimenter un pirate en fausses informations, de façon à garder l'intrus en ligne suffisamment longtemps pour réussir à le localiser et finalement le faire appréhender par les forces de police. Ainsi l'idée de pot de miel ou *honeypot* naît, dans sa première appréhension, dès le milieu des années 1980 ; puis le concept devient plus sophistiqué, faisant l'objet de véritables études et donnant lieu au développement d'outils spécifiques et également de projets complexes parmi lesquels le Honeynet Project, dirigé notamment par Lance Spitzner, le maître à penser du domaine [5].

Un concept " pot-pourri ", emprunt des différentes techniques anti-intrusion [4] qui forment l'état de l'art actuel, et qui consiste, d'une manière générique, à mettre en place des systèmes volontairement vulnérables, c'est-à-dire conçus pour être scannés, attaqués et compromis, dans le but soit d'observer les comportements et de connaître les outils et les méthodes d'attaque des pirates (honeypot de recherche), soit de contribuer directement à la politique de sécurité d'une organisation (honeypot de production). Un concept, haut en couleurs, à la pointe de la lutte contre la criminalité informatique mais qui se révèle rapidement lui-même en proie à de sérieux questionnements juridiques.

L'ambition, simple, du présent article est de fournir à la communauté des ingénieurs et experts en sécurité informatique, un document introductif et un panorama des risques juridiques à envisager lors du déploiement de systèmes " pots de miel ".

2 Honeypots, le " piège à pirates " : mythes et réalité

Le terme de honeypot ou, en français, de système " pot de miel " recèle une suggestivité très forte, véhiculant l'idée que ces systèmes consistent en premier lieu à attirer et piéger les pirates informatiques par la ruse. Or, une telle définition suggère très vite que l'on se situe sur un terrain très proche de la provocation aux crimes et aux délits.

Cette association d'idée explique sans doute en partie le faible taux d'utilisation des *honeypots* dans les environnements de production, l'incertitude quant aux risques juridiques relatifs à ce mécanisme de sécurité tendant ainsi à freiner les organisations dans leur adoption. En effet, force est de constater l'ancienneté du concept[2], lequel connaît aujourd'hui un regain d'intérêt grâce en particulier aux efforts méritoires de Lance Spitzner [3], l'un des fondateurs du très médiatique " projet Honeynet[3] ". Pourtant, cette image de " piège à pirates " assimilée à de la provocation s'avère rapidement une idée trompeuse.

2.1 Principe de fonctionnement

Pour s'en convaincre, il suffit de rappeler le principe de fonctionnement des *honeypots*, seule variable commune à l'ensemble des outils classés dans cette catégorie.

Les *honeypots* sont des systèmes de sécurité qui n'ont aucune valeur de production. Dès lors, aucun utilisateur ni aucune autre ressource ne devrait en principe avoir à communiquer avec lui. L'activité ou le trafic attendu sur le *honeypot*

[2] Cf. *Supra*, note 1.

[3] Projet né en juin 2000, regroupant des professionnels de la sécurité informatique, et consistant dans le déploiement de " réseaux à pirater " en différents endroits de la planète et dont l'objectif est essentiellement pédagogique (apprendre les techniques, stratégies et motivations des pirates informatiques pour mieux sen défendre et partager cette information). Site web : `http://www.honeynet.org`

étant nul à la base, on en déduit a contrario que **toute activité enregistrée par cette ressource est suspecte par nature**.

Ainsi, tout trafic, tout flux de données envoyé à un *honeypot* est probablement un test, un scan ou une attaque. Tout trafic initié par un *honeypot* doit être interprété comme une probable compromission du système et signifie que l'attaquant est en train d'effectuer des connexions par rebond.

Généralement, un *honeypot* se comporte telle une **boîte noire**, enregistrant *passivement* toute l'activité et tout le trafic qui passe par lui, sur la base du principe de fonctionnement précédent.

L'ensemble de ces critères va se révéler déterminant dans la définition de l'impact juridique en matière de *honeypots*.

2.2 Impact sur le plan juridique

De la provocation aux crimes et aux délits On peut s'interroger sur la réalité de la provocation suggérée et l'applicabilité au responsable d'un système *honeypot* du chef de complicité prévu sous l'incrimination de " provocation aux crimes et délits ", tel que défini à l'article 23 de la loi du 29 juillet 1881 sur la liberté de la presse[4] :

> " Seront punis comme complices d'une action qualifiée crime ou délit ceux qui, soit par des discours, cris ou menaces proférés dans des lieux ou réunions publics, soit par des écrits, imprimés, dessins, gravures, peintures, emblèmes, images ou tout autre support de l'écrit, de la parole ou de l'image vendus ou distribués, mis en vente ou exposés dans des lieux ou réunions publics, soit par des placards ou des affiches exposées au regard du public, soit par tout moyen de communication audiovisuelle, auront directement provoqué l'auteur ou les auteurs à commettre ladite action, si la provocation a été suivie d'effet.
>
> Cette disposition sera également applicable lorsque la provocation n'aura été suivie que d'une tentative de crime prévue par (l'article 121-5 du code pénal). "

Au-delà de la question du support utilisé[5], c'est la constatation de l'élément constitutif principal de l'infraction visée, à savoir la publicité, qui suscite le plus d'interrogations : en effet, en quoi la construction des *honeypots, " systèmes conçus pour être scannés, attaqués et compromis "* [3], constitue-t-elle une provocation *directe* aux pirates ? Ceux-ci font-ils l'objet d'une publicité à destination de la communauté *underground* ? Les responsables de systèmes honeypots mettent-ils celle-ci au défi à travers les canaux IRC ? Ou encore, ont-ils fait des déclarations sur le web susceptibles de déclencher les hostilités ?... A l'évidence, cet élément de publicité fait défaut, et l'on peut même affirmer qu'elle serait tout

[4] Nous névoquerons pas ici la question de la provocation policière, en principe interdite en droit pénal français sauf certains domaines spécifiques (stupéfiants), mais très usitée dans d'autres espaces juridictionnels (notamment aux USA).

[5] Dont l'article 23 précité donne la liste limitative (la loi pénale, rappelons-le, étant par ailleurs d'interprétation stricte : article 111-4 du Code Pénal).

à fait antinomique avec les systèmes *honeypots*, leur succès reposant en premier lieu sur la furtivité du système !

En définitive, les attaquants n'ont nul besoin qu'on les aide à trouver les *honeypots* et ils programment, de leur propre initiative, des scans et des attaques que le système se borne *généralement* à enregistrer, sans les avoir préalablement attirés par quelque ruse (fausse information par exemple) pour mieux les piéger.

Autre illustration de cette illusion de la provocation à travers les *honeypots*, la faible valeur ajoutée des systèmes " pot de miel " au service des techniques de déception et de dissuasion.

Ces techniques consistent à augmenter virtuellement le ratio coût/effort nécessaire à une intrusion afin de détourner l'intérêt de l'attaquant. Ainsi, la dissuasion encourage un cyber-criminel à s'intéresser à d'autres systèmes promettant plus de bénéfices à moindre coût. C'est l'application du principe " le jeu en vaut la chandelle " ... Aujourd'hui, l'efficacité de cette stratégie anti-intrusion est remise en cause dans un environnement moderne où la majorité des pirates sont aujourd'hui animés par le " easy kill " et une " shotgun approach ".

En effet, les attaquants perdent rarement de temps à analyser les systèmes qu'ils visent, leur but étant de toucher le maximum de machines ou de voir simplement à quoi ils accèdent avant de recommencer. Pire encore, la plupart des attaques ne sont pas exécutées en direct par les pirates, mais bien de façon programmée par des outils automatisant les attaques (comme les vers par exemple). Seule exception notable, les attaquants aux " cibles choisies " par opposition aux " attaques par cible d'opportunité " susvisées, et qui concernent les rares pirates de haut vol, plus impliqués dans des actions proches de l'espionnage et du contre-espionnage industriel ou du sabotage[6]... Cas extrêmes s'il en est, qui ne font pas partie de notre champ d'étude dans le cadre du présent article.

En définitive, il est très difficile de voir comment les *honeypots* répondent à l'exigence de publicité requise dans l'incrimination de " provocation aux crimes et aux délits " ni comment la conception volontairement vulnérable des ressources *honeypot* peut constituer en elle-même une incitation dans l'intention criminelle[7] des attaquants.

[6] Dans ce cadre exceptionnel, les *honeypots* pourraient servir efficacement des objectifs de déception et de dissuasion. Ainsi, s'agissant d'organisations titulaires d'informations à forte valeur ajoutée, dans des domaines de recherche sensible (tel que le nucléaire) et/ou les ressources sont classifiées ou soumises à contrôle, l'attaquant qui construit son approche à partir d'un objectif pré-déterminé, pourra être impacté par ces techniques. Par exemple, on pourra construire un *honeypot* de façon à tromper et divertir l'attaquant, tout en prévenant des attaques contre les données de production réelles ; dans ce cas de figure, on pourrait créer un serveur de fichiers jouant le rôle de registre central pour des documents classifiés " secret défense ", mais au lieu dy placer de la documentation valide, ce sont des fausses informations (*fake data*) qui seraient créées et déposées sur le registre du *honeypot*. Ainsi, l'attaquant pensera par exemple avoir obtenu les plans d'un cœur de réacteur dernière génération, alors qu'il met en oeuvre les procédés qu'il a volés, il n'obtiendra aucun résultat utile.

[7] Au sens de l'article 121-3 du code pénal : " Il n'y a point de crime ou de délit sans intention de le commettre (...) ".

Pour d'autres[8], c'est la nécessité d'une provocation " *suivie d'effet* " (ou à tout le moins d'une tentative) qui fait " structurellement défaut " et conduit à rejeter la provocation aux crimes et délits : " *il ne peut y avoir d'atteinte à un système de traitement automatisé de données au sens pénal, si le maître du système est d'accord pour qu'une telle atteinte soit réalisée. Ce qui semble bien le cas lorsqu'il met à la disposition du public un système destiné à faire l'objet d'une intrusion. On ne serait ici donc que dans un cas d'application classique de la théorie des faits justificatifs chère au droit pénal : le consentement de la victime a, en l'espèce, la libre disposition de l'intérêt protégé par la loi pénale et s'érige comme une condition de réalisation de l'infraction.* "

Du droit à mettre du miel dans le pot ? Il est important en effet de considérer l'idée suivant laquelle la mise en place de systèmes volontairement vulnérables constituerait à la fois une forme de consentement implicite de la victime (le responsable du système) et une négligence coupable, faisant l'un et l'autre obstacle à la possibilité même de poursuivre les attaquants pour atteinte au système.

Un consentement implicite de la victime ? Suivant nos développements précédents, nous avons déjà souligné comment, conformément à leur principe commun de fonctionnement, les *honeypots* permettent simplement, grâce à un " effet microscope[9] " et une réduction drastique du niveau de bruit, de mieux capter, sans provocation, une activité non autorisée et illicite. Ce faisant, la vocation de ces ressources à être scannées, attaquées ou compromises ne permet pas pour autant de présumer systématiquement d'une forme de consentement implicite du responsable de *honeypot* et il nous faut relativiser cette première affirmation.

En effet, une telle admission générale du fait justificatif de consentement de la victime peut facilement apparaître comme une évidence. Ce faisant, la simplicité du raisonnement conduit à ignorer les réalités techniques propres à la distinction entre *honeypots* de recherche et *honeypots* de production.

Cette distinction est celle proposée par Marty Roesch[10] face à la diversité de formes et d'outils et l'absence de concept unitaire pour définir les *honeypots*. Selon cette " classification ", les *honeypots* de recherche visent uniquement à la connaissance[11], tandis que **les *honeypots* de production sont conçus**

[8] Voir notamment Thiébaut Devergranne : *Du droit dans le pot, quelques réflexions juridiques autour des "* honeypots *"* - MISC 8, pp.34-35 (consultable sur : `http://hstd.net/honeypots.pdf`).

[9] Seule l'activité dirigée contre les *honeypots* est enregistrée, à l'exception de toute intrusion sur d'autres ressources du système de production, ce qui constitue dans le même temps, l'un des principaux avantages (meilleure gestion des faux positifs et faux négatifs) et inconvénients (champ de vision réduit) de ces ressources.

[10] Le développeur du logiciel SNORT.

[11] considérant, suivant le conseil du chinois Sun Zu dans son ouvrage " L'art de la guerre ", daté du IVème siècle avant J.-C , qu'il faut s'efforcer " *de vaincre par la ruse, sans livrer combat. Les grands stratèges remportent le succès en découvrant le*

moins pour apprendre que pour protéger une organisation spécifique et apporter une valeur ajoutée à sa politique de sécurité :

- soit dans une optique de prévention, par exemple en faisant croire à un pirate qu'il a réussi à accéder aux ressources système alors qu'il a été dirigé dans un environnement préparé et contrôlé[12] - Cf [**?**] : techniques de déflection, de déception et de dissuasion ;
- soit dans une optique de détection d'intrusion, par exemple pour augmenter les performances des NIDS (*Network Intrusion Detection System*) notamment dans la recherche de nouvelles attaques ou vulnérabilités[13] ;
- soit dans une optique de réponse aux incidents en organisant par exemple la pré-constitution des preuves de l'intrusion[14].

Dès lors, parce que les *honeypots* de production ne remplacent pas les autres mécanismes de sécurité (*firewall* et IDS par exemple) et s'inscrivent à part entière dans la politique globale de sécurité, conclure *d'emblée* au consentement de la victime serait selon nous antinomique avec les objectifs possiblement assignés à ces ressources (notamment en fonction de leur place dans l'architecture du réseau d'entreprise), objectifs où la volonté est moins ici d'être attaqué (sondé ou compromis) pour observer mieux et plus que de seulement *faciliter la captation pour mieux protéger*[15]. A l'inverse, il nous semble effectivement que les *honeypots* de recherche, qui ne participent qu'indirectement à la sécurité[16], impliquent bien le consentement du responsable de projet : en effet, la valeur ajoutée de ce type de *honeypot* augmentant à l'aune du nombre de scans, d'attaques ou de compromissions dont ils sont l'objet, on peut raisonnablement penser qu'ils les appellera de ses propres voeux.

---

jeu caché de leurs adversaires, en déjouant leurs plans [...] ". Extrait de l'article de Fabrice Deblock, " *on nattrape pas les pirates avec du vinaigre, mais avec du miel !* " - JDNet, 26 novembre 2003 : `http://solutions.journaldunet.com/0311/031126_honeypots.shtml`

[12] Par exemple le système *Bait and Switch* qui joue le rôle de passerelle entre l'extérieur et le réseau interne à protéger, permet, après " isolement " du trafic suspicieux, de demander la redirection de ce trafic vers un miroir " pot de miel ", qui simule l'environnement de production.

[13] Par exemple, les *honeypots* sont peu sensibles aux faux négatifs car ils ne fonctionnent pas, à la différence des NIDS, à partir d'une base de données de signatures, mais sur la simple observation du trafic et de lactivité enregistrée. Dès lors, un *honeypot* pourra détecter un exploit lancé avec ADMmutate, alors que le NIDS en place sera leurré...

[14] Cf infra, section 3 : au sujet des markers dans la dernière version du logiciel Specter.

[15] Il semble bien que cette opinion soit partagée par quelques uns. En effet, si l'on admettait qu'il a fait justificatif de la victime et qu'en tout état de cause, les intrusions sur les honeypots ne peuvent être poursuivies judiciairement, qu'elle serait l'utilité de développer des fonctionnalités comme les markers offerts dans le logiciel SPECTER (version 7) Cf infra section 3 et dont l'objectif est d'aménager des preuves de l'intrusion ?

[16] Par exemple le projet Honeynet avait permis en janvier 2002 de découvrir l'exploit *dtscp*. Pour plus dinformations : `http://www.honeynet.org`

Une négligence coupable ? Une autre idée répandue est de considérer comme une négligence coupable le fait de, volontairement, laisser des vulnérabilités et " autoriser " ainsi les attaquants à s'introduire sur le système. Partant, la poursuite de l'attaquant sous le chef d'accès ou de maintien frauduleux (article 323-1 du Code pénal) deviendrait impossible.

En ce sens, force est de rappeler que le Sénat lui-même, au cours des travaux préparatoires relatifs à la loi dite Godfrain, avait souligné qu'une exigence de protection du système pour que l'infraction d'accès frauduleux à un système informatique soit constituée lui paraissait raisonnable, " *le droit pénal ne devant pas compenser l'insuffisance ou la défaillance des mesures de sécurité* " ... et plus encore ajouteraient-ils peut-être aujourd'hui, lorsque cette vulnérabilité du système est délibérée et organisée !

Cependant, l'Assemblée nationale[17] a jugée excessive cette position du Sénat, et la jurisprudence ou les textes ultérieurs ont pris la même position : **la protection du système n'est pas une condition de l'incrimination**.

Ainsi, la Cour d'appel de Paris dans un arrêt du 5 avril 1994 a posé le principe que : " *pour être punissable, cet accès ou ce maintien doit être fait sans droit et en pleine connaissance de cause, étant précisé à cet égard qu'il n'est pas nécessaire pour que l'infraction existe, que l'accès soit limité par un dispositif de protection [...]* ". Ainsi l'accès tombe sous le coup de l'article 323-1 du Code pénal dès lors qu'il est le fait d'une personne qui n'a pas le droit d'accéder au système et la barrière technique n'est pas indispensable au jeu de l'interdiction[18].

Par analogie, Christian Le Stanc considère de la même façon que : " *il n'est pas licite de pénétrer chez autrui sans autorisation et que, notamment, l'infraction de violation de domicile peut être constituée sans qu'il faille avoir égard à la hauteur du mur d'enceinte ou à la résistance de la serrure* ". Quid en l'absence même de toute protection ? Le fait de ne pas fermer sa porte à clé, voire même de laisser la porte ouverte (idée plus proche encore, pour certains, du concept de *honeypot*, constitue-t-il une négligence coupable de la victime l'empêchant d'engager des poursuites contre un intrus ?

La Commission européenne, dans une proposition de décision-cadre relative aux attaques visant des systèmes d'information[19], nous donne une réponse à cet égard : " *la Commission ne souhaite nullement mettre en cause l'importance qu'elle attache à l'utilisation de mesures techniques efficaces pour protéger les systèmes d'information. Le fait est néanmoins qu'une grande partie des utilisateurs s'exposent malheureusement à des attaques faute d'une protection technique adéquate (voire même de toute protection). En vue de prévenir les attaques contre ces utilisateurs, le droit pénal doit couvrir l'accès non autorisé à leurs systèmes, même si ces systèmes ne bénéficient pas d'une protection technique appropriée.*

[17] Jérôme Dupré, *Pour un droit de la sécurité économique de l'entreprise* - Thèse 2000, Université de Nice-Sophia Antipolis, n°346

[18] Valérie Sédallian, " *Légiférer sur la sécurité informatique : la quadrature du cercle ?* " - 2003, `Juriscom.net`

[19] Com/2002/0173 (Final) - JOCE du 27 août 2002

C'est pour cela (...) qu'il n'est pas nécessaire que des mesures de sécurité aient dû être déjouées ".

Dans l'affaire Kitetoa/Tati[20], le tribunal correctionnel de Paris dans sa décision du 13 décembre 2002[21] a condamné l'animateur du site Kitetoa.com pour accès frauduleux à des données qui n'étaient pas du tout sécurisées (absence de mot de passe ou de restriction d'accès). Par ce jugement, le tribunal rappelle aussi, de manière classique, que la **motivation de l'auteur** (amélioration de la sécurité des systèmes[22], critique des choix de la direction informatique[23], démarche de recherche scientifique[24] e.g.) *ne supprime pas l'intention frauduleuse.*

Finalement, c'est seulement suite à un appel introduit par le Parquet général que le webmestre a été relaxé par décision du 30 octobre 2002 de la Cour d'appel de Paris[25], décision fondée sur l'accès " par des moyens informatiques réguliers " (simple URL sur Internet). Cette dernière décision, qui fait suite à une démarche peu courante du Parquet, ne doit pas cependant être interprétée comme un revirement de la jurisprudence précitée et demeure un cas d'espèce aux circonstances particulières ; en l'occurrence, les données accédées étant des données personnelles, elles étaient soumises à une obligation de sécurité, ce qui justifie que, dès le jugement de première instance, la constitution de partie civile de la société Tati ait été rejetée par le tribunal au motif que " *celle-ci ne saurait se prévaloir de ses propres carences et négligences pour arguer d'un prétendu préjudice*[26] ".

En dernier lieu, il convient de souligner que, si le niveau de protection du système n'est pas une condition de l'incrimination d'accès ou de maintien frauduleux, l'insuffisance des moyens de sécurité mis en oeuvre fait courir au responsable du système des risques connexes non négligeables. Il s'agit en particulier des :

[20] Rappelons en quelques mots les faits de l'espèce : en 1999, l'animateur du site Kitetoa.com signale à l'hébergeur du site des magasins Tati une faille de sécurité permettant d'accéder au contenu des bases de données clients du serveur grâce à un simple navigateur. Constatant près d'un an après que les failles détectées et signalées existaient toujours, il décide de publier sur son site un article relatant cette faille de sécurité. L'information était ensuite reprise dans un magazine spécialisé, ce qui détermina la société Tati à poursuivre l'animateur du site pour accès frauduleux dans un système informatisé.

[21] *Revue Communication Commerce électronique*, mai 2002, p.31, note Grynbaum

[22] Au sujet du dirigeant d'une société de sécurité informatique américaine ayant révélé l'existence de failles dans les systèmes informatiques de l'armée : `http://www.transfert.net/a9371`

[23] Cass.Soc., 1er octobre 2002, Gaz.pal. 20 avril 2003, p.33, note Tessalonikos.

[24] Voir affaire Serge H./ GIE Cartes bancaires, TGI Paris, 25 février 2000 - *Revue Communication Commerce électronique*, mars 2001 ; Voir dépêche AFP du 27 septembre 2002 au sujet de l'intervention policière ayant conduit à l'annulation d'une conférence de presse devant porter sur une vulnérabilité facilement exploitable (sans connaissance complexe ni moyen matériel sophistiqué) de sites bancaires (affaire *Hackervoice*).

[25] *Revue Communication Commerce électronique*, anvier 2003, p.30, note Grynbaum.

[26] *Nemo auditur propriam turpitudinem allegans* (nul ne peut alléguer de sa propre turpitude) est un adage issu du droit romain et appliqué en droit civil.

- recours de la tierce victime :
  - victime collatérale par rebond (ce cas sera abordé dans la section 3 du présent article) ;
  - " personne concernée " (au sens de la Directive 95/46), sur le fondement de l'obligation de sécurité de l'article 29 de la loi " Informatique et libertés " du 6 janvier 1978 (Cf *infra*, section 2) ;
- risque en matière d'assurance : perte du droit à indemnisation.

Ces enjeux et ces risques devront être anticipés et pris en considération dès la phase de conception par le responsable d'un projet *honeypot*, en particulier lorsqu'il définira les spécifications techniques en matière d'étanchéité des systèmes et de contrôle des données.

De la même façon, la conception d'un *honeypot* pourra être modulé en fonction des limitations juridiques applicables en matière de protection des données personnelles (ou, dans un sens plus large encore, de " *privacy* ").

3 " *Honeypots, tracking hackers* " : quelles limites à la capture des données et à la surveillance de l'activité des attaquants ?

Comme indiqué précédemment (cf section 1, *Principe de fonctionnement*), le trafic capté par les *honeypots* est à la fois réduit (effet microscope) et suspect par nature. Les fichiers des enregistrements d'évènements (fichiers de logs) sont donc peu volumineux et il est plus aisé d'identifier une activité malveillante. En fonction de la nature des données collectées, on pourra ainsi retracer précisément les flux échangés :

- provenance,
- activité,
- date,
- durée,
- volume ... et parfois même,
- le contenu des données échangées (*keystrokes*, messages IRC par exemple).

Cependant, la capture de ces données oblige à se poser en droit plusieurs questions :

1. quelle est la nature des données collectées et le régime juridique applicable ? (applicabilité de la législation sur la protection des données à caractère personnel)

2. quelles sont les limites à la licéité de la surveillance de l'activité de l'intrus (problématique des " attaquants internes ") et des moyens utilisés pour capter ces données (keystrokes, interception de *chat*) ?

3.1 Collecte de données et nature juridique : impact de la législation sur la protection des données à caractère personnel

L'analyse post-mortem (ou *forensic*) des données capturées par le *honeypot* est une " tâche longue et rude[27] ". En effet, si les fichiers de journalisation ne sont pas (en principe ![28]) aussi volumineux que ceux produits par les IDS, il faut une certaine expérience et des compétences techniques (pré-requis minimum en SSI, administration systèmes et réseaux, supervision réseau, bagage technique applicatif) pour pouvoir reconstruire les échanges, mettre en évidence les interactions et interpréter à travers les activités et les données techniques recueillies les motivations des intrus.

Du point de vue du droit, il convient surtout d'examiner la nature des données enregistrées, analysées et conservées afin de déterminer si celles-ci tombent ou non sous le coup de la législation sur la protection des données personnelles et quelles sont, dans ce cas, les contraintes juridiques à respecter.

Nature juridique des données collectées : à propos des données " indirectement identifiantes " En réalité, les niveaux d'informations collectées sont très variables d'un *honeypot* à l'autre et il serait difficile dans le cadre du présent article d'en dresser une liste exhaustive. On peut simplement rappeler que les données communément recueillies, à savoir les données de connexion relatives au trafic à destination ou en sortie du honeypot, vont permettre d'obtenir des renseignements sur :

- l'architecture et les ressources de la machine (techniques de *fingerprinting* passif avec Disco, PoF... permettant par exemple de déterminer le type d'OS) et les méthodes utilisées par l'attaquant (ports scannés, *exploits* lancés, *rootkit* et *backdoors* utilisés...) ;
- ...
- la provenance de l'attaque[29] : nom de domaine (.fr, .nl, .au...), adresse IP, " signature " (communauté de pirates : " Iranian Hackers " dans l'attaque contre le site ODEBI e.g.)...

[27] Interview de Fred Arbogast et Alexandre Dulaunoy, professionnels luxembourgeois de la sécurité informatique, à l'origine du projet *honeylux* (`http://www.honeylux.org.lu`) - Zataz Magazine, avril 2004

[28] Ce nest pas toujours le cas et Lance Spitzner [3], dans le chapitre 8 de son ouvrage, (chapitre) consacré au démon *honeyd* développé et maintenu par Niels Provos (`http://www.citi.umich.edu/u/provos/honeyd/`), souligne les défauts de ce programme quant à la gestion des traces obtenues, l'absence duniformisation de leur exploitation (formats notamment) et les " milliers de lignes de logs " que certains évènements peuvent rapidement générer, comme l'indique quelques tests menés par la team *rstack* [5], page 52.

[29] Encore que cette donnée puisse être sensiblement faussée. Par exemple, la provenance de l'attaque " révélée " par une adresse IP correspond très souvent à un groupe dadresses IP détenus par un ISP, ce qui ne garantit en rien la localisation de l'attaquant lui-même, surtout s'il utilise par ailleurs des techniques de rebond pour dissimuler la provenance réelle de l'attaque.

– l'identification de l'attaquant : adresse e-mail, site web personnel, fonction Whois...

Ce sont les deux derniers niveaux d'information qui vont nous intéresser dans le cadre de notre approche juridique des *honeypots*. En effet, force est de rappeler que les " données à caractère personnel " sont l'objet d'une législation protectrice très étoffée, au sujet de laquelle certains parlent même aujourd'hui d'un véritable " harcèlement textuel "...

Par " donnée à caractère personnel ", on entend au sens de la directive 95/46/CE[30] (ci-après " la Directive ") :

> *toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement* **ou indirectement**, *notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou socialei.*

D'autre part, le considérant 26 de la Directive précise que :

> " *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne ; (...)* "

S'il ne fait pas de doute que l'adresse e-mail ou les données collectées sur un site web personnel (rubrique " contact ", photos...) entrent bien dans la catégorie des " données à caractère personnel[31] ", la question ferait toujours débat pour certains s'agissant de l'adresse IP[32] et a fortiori, de l'URL et du nom de domaine.

Or, la directive 2002/58/CE[33] dispose en son article 6, qu'eu égard aux risques pour la vie privée des abonnés aux FAI[34] et des utilisateurs de services

[30] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données - JOCE n° L 281 du 23/11/1995 p. 0031 - 0050 : `http://europa.eu.int/eur-lex/fr/lif/reg/fr_register_133099.html`

[31] Notez que dans le cadre de la législation française (loi n°78-1 " Informatique et Libertés ", toujours en vigueur jusqu'à la transposition – imminente – des directives communautaires), on parle encore d' " informations (directement ou indirectement) nominatives "...

[32] Lire Sophie Lalande, *L'adresse IP de votre ordinateur : une donnée personnelle relevant du régime communautaire de protection ?* (décembre 2003) Consultable sur : `http://www.clic-droit.com/`

[33] Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Directive dite " Vie privée et communications électroniques ") - JOCE n° L 201 du 31/07/2002 p.37 et s : `http://europa.eu.int/eur-lex/fr/`

[34] En effet, on peut rappeler que, pour obtenir une connexion, on sait que les FAI, pour des raisons de sécurité, ont coutume de consigner dans un fichier la date,

à valeur ajoutée, " les données relatives au trafic[35] (...) doivent être effacées ou rendues *anonymes* lorsqu'elles ne sont plus nécessaires à la transmission d'une communication (...) ". Dans la pratique également, la CNIL, notamment par ses recommandations dans son Rapport sur la cybersurveillance des salariés sur les lieux de travail[36], semble elle aussi considérer d'emblée que les " données de connexion " (type adresse IP ou URL donc) sont des données couvertes par le régime de la protection des données personnelles.

Prenant acte de cette qualification implicite[37], il nous faut encore déterminer quel est l'impact de l'applicabilité de la législation sur la protection des données à caractère personnel en matière de *honeypot*.

Conséquences de l'application de la législation sur les données à caractère personnel De manière générale, tout traitement[38] appliqué à des

l'heure, la durée de la connexion, l'adresse du site Internet consulté ou de la page du site demandée, la taille des messages ainsi que l'adresse IP de l'utilisateur. Ces *logs* sont notamment conservés à des fins utiles pour la répression de la criminalité informatique, conformément à l'exception offerte par la directive 2002 (article 15, paragraphe 1). La Loi sur la Sécurité Quotidienne (LSQ) loi n°2001-1062 du 15 novembre 2001 ; JO n°266 du 16 novembre 2001, page 18215 imposa à cet égard une durée de conservation des données de connexion d'un an minimum.

[35] Données définies à larticle 2 b) de la directive 2002, comme " *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation* ". Ainsi de l'adresse IP...

[36] 2ème rapport publié en février 2002 et réédité en mars 2004. Voir : `http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf`

[37] Notre opinion étant la suivante : si la critique consistant à dire que l'adresse IP ne permet d'identifier concrètement qu'une *machine* et non une *personne physique* (telle que visée par la Directive dans son article 1er " Objet de la directive ") - cf dans le même sens, S. Lalande dans le paragraphe intitulé " limites de la théorie ", *op.cit.*- , on doit considérer néanmoins que l'interrogation de la base de données Whois, combinée selon le cas avec une requête DNS de résolution inverse, est un moyen raisonnable (au sens du Considérant 26 cité dans nos développements) pour permettre d'identifier *indirectement* l'intrus...Bien sûr, les données ainsi recueillies ne constitueraient qu'un simple commencement de preuve quant à l'identité de l'internaute, qu'il faudra par la suite, en cas de poursuites judiciaires, recouper et vérifier (risques d'usurpation d'identité, d'utilisation de techniques de rebond, caractère mensonger des déclarations d'identité effectuées auprès des FAI ou des organismes gestionnaires des noms de domaine). En définitive donc, on peut simplement regretter que de " données permettant *indirectement* d'identifier une personne ", nous soyons amenés à appliquer la législation sur la protection des données à caractère personnel à des *data* qui sont seulement " *potentiellement* identifiantes ", ce qui ne recouvre pas selon nous les mêmes réalités.

[38] C'est-à-dire " toute opération ou ensemble d'opérations (...) telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion,

données à caractère personnel emporte application des principes généraux de la Directive, à savoir :

- principes de nécessité et de finalité du traitement,
- loyauté et transparence de la collecte vis-à-vis des personnes concernées et enfin,
- proportionnalité des moyens avec les objectifs[39].

Corollaire de l'ensemble de ces principes, une déclaration à la CNIL[40] du ou des fichiers de *logs* enregistrés et conservés dans le cadre du *honeypot* peut s'avérer nécessaire.

A l'occasion de son rapport sur la cybersurveillance sur les lieux de travail (cf supra, note 36), la CNIL indique en effet que : " *les fichiers de journalisation (des connexions destinés à identifier et enregistrer toues les connexions ou tentatives de connexion à système automatisé d'informations) n'ont pas,* **en tant que tels***, à faire l'objet des formalités préalables auprès de la CNIL* ". Ils le doivent seulement dans deux cas :

1. lorsqu'ils sont associés à un " traitement automatisé d'informations nominatives " afin de garantir ou de renforcer le niveau de sécurité de ce dernier ; dans ce cas, il devra être porté à la connaissance de la CNIL dans le cadre des mesures de sécurité entourant le fonctionnement du traitement principal ;
2. lorsque les différents journaux (systèmes et applicatifs) font l'objet d'une analyse mise en oeuvre par un logiciel permettant de collecter des informations individuelles poste par poste pour contrôler l'activité des utilisateurs.

En l'occurrence, les analyses *post-mortem* des données de connexion capturées par les *honeypots* de recherche donnent lieu simplement à des analyses statistiques globales (fréquence et moment des attaques, origine géographique, type de ports et machines attaqués...[41]) ou à des analyses comportementales (au sens méthodologique), par ailleurs généralement " anonymisées "[42]. Certains considèrent néanmoins que la directive est même applicable aux données anonymes lorsque les moyens matériels et techniques existent aux fins d'identifier les personnes concernées, alors même qu'ils ne sont pas utilisés car l'identification n'est pas nécessaire à l'activité poursuivie[43]. Dans un sens convergent, on

ainsi que le verrouillage, l'effacement ou la destruction " (article 2 " définitions " de la Directive).

[39] our plus dinformations concernant la signification de ces principes, se reporter au site de la CNIL : `http://www.cnil.fr`

[40] Rappelons que le présent article se place exclusivement sous l'angle de droit français.

[41] *Honeypots : observation platforms*, rapport d'expérimentation (20003-2004) d'Eurocom ; présenté dans le cadre du groupe de travail " SUR " organisé par l'OSSIR `http://www.ossir.org`

[42] Exemple des " honey plots " relatés dans le rapport Sombria *A walk through " Sombria " : a network surveillance system* (May - July 2003), SNS, (c) 2003, LAC Co., Ltd. all rights reserved : `http://www.net-security.org/dl/articles/smbr_1.pdf`

[43] Voir M-H Boulanger, C. de Terwangne, T. Léonard, S. Louveaux, D. Moreau, Y. Poullet, *La protection des données à caractère personnel en droit communautaire*, ERA, volume 27, 2000

citera le considérant 26 de la Directive qui stipule *in fine* que : " *les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable.* "

S'agissant des analyses menées dans le cadre de *honeypots* de production, celles-ci peuvent vraisemblablement entrer dans le cas de figure numéro 2, l'un des objectifs étant potentiellement d'identifier des " attaquants internes ", impliquant dès lors le rapprochement des adresses IP avec les postes des utilisateurs concernés...

Dans tous les cas, force est de recommander ici l'application du principe de précaution : mieux vaut en effet solliciter un avis de la CNIL en cas de doute[44] ou même déclarer inutilement le traitement effectué que d'encourir les peines d'amende et d'emprisonnement prévues en cas de non-respect des formalités préalables (article 226-16 du code pénal) !

En dernier lieu, on rappellera que l'application du régime de la protection des données personnelles impliquera également la mise en oeuvre de mesures de sécurité pour protéger les informations collectées et analysées :

La Directive (articles 16 et 17), de même que la loi française 78-17 dite " Informatique et Libertés " imposent au responsable du traitement une obligation de sécurité et de confidentialité, qui se traduit dans le code pénal par l'infraction prévue à l'article 226-17 : " *le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 2 000 000 F d'amende* ". En pratique, comme l'a illustré l'affaire *Kitetoa* (Cf op.cit., section 1), le Ministère public a recherché de préférence la responsabilité du délinquant informatique, sans poursuivre la société " victime " elle-même coupable de manquement à l'obligation de sécurité. Cependant, les carences dans le respect de cette obligation par le responsable d'un *honeypot* pourront le cas échéant, comme dans cette même affaire, lui faire perdre son droit à poursuivre (en l'espèce, rejet de la constitution de partie civile de la société *Tati*).

Tab. 1. Rappel sur l'obligation de sécurité des données à caractère personnel

[44] Certains considèrent en effet que la directive est même applicable aux données anonymes lorsque les moyens matériels et techniques existent aux fins d'identifier les personnes concernées, alors même qu'ils ne sont pas utilisés car l'identification n'est pas nécessaire à l'activité poursuivie. Voir M-H Boulanger, C. de Terwangne, T. Léonard, S. Louveaux, D. Moreau, Y. Poullet, *La protection des données à caractère personnel en droit communautaire*, ERA, volume 27, 2000. Dans un sens convergent, on citera le considérant 26 de la Directive qui stipule *in fine* : " *que les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable.* "

3.2 Limites à la surveillance de l'activité de l'intrus : problématique des " attaquants internes " et licéité des moyens utilisés pour la captation des données

Parmi les principes de la Directive figure le principe de loyauté et de transparence dans la collecte des informations, lequel suppose en principe le consentement de la personne concernée (article7). Bien sûr, en matière de honeypot, une telle disposition n'a pas de sens. C'est l'article 7 f) (une disposition souvent qualifiée de " fourre-tout ") qui trouvera donc à s'appliquer car la capture des données " *est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement* ", intérêt sur lequel les droits et libertés fondamentaux de la personne concernée (l'attaquant) ne sauraient donc prévaloir. Il existe néanmoins une catégorie d'attaquants qui conservent des droits susceptibles de limiter la capacité et l'étendue de la surveillance.

Les " attaquants internes ", titulaires de droits : des limites du pouvoir de surveillance sur les réseaux d'entreprise La problématique des " attaquants internes " se pose de manière spécifique aux responsables de *honeypots* mis en place dans le cadre d'une organisation (*honeypots* de production). En effet, il ne faut pas perdre de vue le fait que l'intrus peut très bien se révéler être un utilisateur authentifié sur le réseau interne de l'entreprise, mais qui, par malveillance ou excès de zèle, va essayer de dépasser ses droits, sonder le système d'information pour en détecter les failles ou encore installer un quelconque Cheval de Troie...

Dans ce cas, si la mise en œuvre de moyens de surveillance est tout à fait légitime, elle est contrebalancée par certains droits intangibles des utilisateurs (droit au respect de la vie privée, à la liberté d'expression et d'opinion...) qui s'exercent " *même au temps et au lieu de travail*[45] ", et donc y compris sur leur lieu de travail. Dès lors, pour pouvoir utiliser les traces informatiques révélant cette activité fautive du salarié[46], il faudra avoir respecter l'obligation d'information auprès des salariés et de consultation des instances représentatives du personnel préalablement à la mise en place du système pot de miel. A défaut, la " preuve " rapportée devant le tribunal pour justifier un éventuel licenciement serait considérée comme déloyale, conformément à la jurisprudence classique dans ce domaine[47].

Surtout, si l'information des utilisateurs légitimes du réseau de l'entreprise est nécessaire et obligatoire, elle n'est pas en elle-même suffisante.

En effet, la CNIL dans le rapport précédemment visé en matière de cybersurveillance des salariés rappelle qu' " *une déclaration à la CNIL (... n'autorise pas*

[45] Cour de cassation, chambre sociale - 2 octobre 2001 (" arrêt Nikon ") : `http://www.courdecassation.fr/agenda/arrets/arrets/99-42942arr.htm`

[46] Et tous utilisateurs visés par la politique de sécurité et/ou la charte d'utilisation appropriée des moyens informatiques mis à la disposition de l'utilisateur : stagiaires, intérimaires, intervenants externes (sous-traitants...).

[47] CEDH, 27 mai 1997, Halford c/ Royaume-Uni.

(l'organisme) à porter des atteintes à ce que commande le respect de l'intimité de la vie privée et de la liberté personnelle résiduelle du salarié sur son lieu de travail, alors qu'il appartient, en dernière instance, aux juridictions administratives ou judiciaires d'en apprécier la régularité et, compte tenu des circonstances de fait ou de droit de l'espèce, la **proportionnalité**[48]... " Sans doute la mise en œuvre dans le cadre des *honeypots* de moyens de capture en temps réel de discussions en ligne (IRC) ou bien des frappes clavier (*keystrokes*) posera de ce point de vue quelques difficultés, tant au regard des " attaquants internes " qu'au regard des autres attaquants (cf *infra*, " licéité des moyens de surveillance ? ").

Enfin, même dans l'hypothèse où toutes les règles ont été respectées (information préalable des salariés, information des organes représentatifs et justification du contrôle), " l'utilisation des preuves obtenues par la mise en place des dispositifs de surveillance à des fins de sanction doit être maniée avec prudence ", rappelle Me Valérie Sédaillan[49]. En effet, écrit-elle, " les données obtenues peuvent être manipulées, modifiées, effacées, volontairement ou accidentellement (et) la jurisprudence en matière sociale semble donc refuser la recevabilité de la preuve numérique[50] ". Un certain nombre de précautions dans la pré-constitution de la preuve doivent donc être prises pour que les traces enregistrées par le *honeypot* soient le moins possible sujet à caution (cf section 3).

---

[48] Sur ce dernier point, la CNIL s'accorde à dire que, par nature, l'ordinateur peut enregistrer tout ce qui a été fait sur la machine et qu'il constitue ainsi une véritable " boîte noire " des activités de l'utilisateur. Qu'en définitive, " *qu'il s'agisse d'assurer le bon fonctionnement du service informatique, la sécurité numérique de l'entreprise ou le confort de l'usager, ces " traces " sont intrinsèquement liées à la mise à disposition d'une telle technologie. Aussi n'est-ce pas leur existence mais leur traitement à des fins autres que techniques qui doit être proportionné au but recherché* ".

[49] *Internet dans l'entreprise*, article présenté dans le cadre d'un séminaire organisé par Euroforum (janvier 1998). Extrait : " En effet, les données obtenues peuvent être manipulées, modifiées, effacées, volontairement ou accidentellement. La jurisprudence en matière sociale semble donc refuser la recevabilité de la preuve numérique ".

[50] En témoignent deux affaires :

Un arrêt du 4 janvier 1994 de la Cour d'appel d'Aix a refusé de considérer qu'un film vidéo constituait un élément de preuve admissible permettant de démontrer la réalité des fautes invoquées à l'appui d'un licenciement. La Cour a considéré que compte tenu des possibilités de montage et de trucage qu'offre l'évolution des techniques, le document fourni ne présentait pas des garanties suffisantes d'authenticité, d'impartialité et de sincérité concernant tant sa date que son contenu, pour qu'il puisse être considéré comme probant. Peu importe que l'enregistrement ait été réalisé au su des salariés.

Cette décision doit être rapprochée d'une décision en date du 14 mai 1996 de la Cour d'appel de Rouen. Dans cette affaire, après avoir obtenu du salarié le code d'accès personnel à son ordinateur, l'employeur avait fait établir, plus de 24 heures après, en l'absence dudit salarié, un procès-verbal de constat qui avait révélé qu'étaient intégrés sur une disquette, trois logiciels étrangers à l'activité de la société. La Cour a considéré que cette preuve n'était pas recevable en raison des larges possibilités de manipulation du matériel.

Licéité des moyens de surveillance ? : le cas des interception de keystrokes et conversations type IRC. En France, le code pénal prévoit plusieurs incriminations dont la question de l'application aux interceptions de keystrokes et de conversations type IRC peut légitimement être posée. Ainsi des articles 226-1 et 226-15 :

– Article 226-1 (de l'atteinte à la vie privée) :

> " *Est puni d'un an d'emprisonnement et de 300.000 F d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui : i) En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel; ii) ...* "

– Article 226-15 (de l'atteinte au secret des correspondances) :

> " *Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 300.000 F d'amende. Est puni des mêmes peines, le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.* "

Dans l'hypothèse où une poursuite judiciaire est intentée à l'encontre d'un intrus identifié grâce aux traces enregistrées dans le cadre d'un *honeypot*, une " contre-attaque logique " consisterait donc, pour la défense, à invoquer le caractère déloyal des moyens par lesquels la preuve est rapportée[51]. Sans revenir point par point sur les éléments constitutifs de chacune des infractions susvisées, nous souhaitons ici simplement évoquer quelques arguments qui postuleraient ou non en faveur de la licéité des moyens de captation précédemment visés.

Concernant l'interception des commandes clavier (*keystrokes*), il convient de souligner que les données sont échangées non pas avec une personne mais bien avec une machine et que la surveillance du responsable de *honeypot* en tant que propriétaire du système destinataire serait donc légitime (toute activité avec ledit système étant rappelons-le suspecte par nature). Qu'ainsi l'utilisation de *keyloggers* dans le cadre particulier des *honeypots de production* ne peut pas s'apparenter aux logiciels de " prise de main à distance " (permettant le cas échéant aux administrateurs de connaître les frappes clavier des utilisateurs en difficulté), moyens pour lesquels la CNIL recommande (dans le rapport déjà maintes fois cité) la mise en oeuvre de précautions d'utilisation (information et accord préalable de l'intéressé, traçabilité des opérations de maintenance,

[51] Si la preuve est libre en droit français (c'est-à-dire que " les infractions peuvent être rapportées par tout mode de preuve " : article 427 du Code de procédure pénal), la preuve n'en doit pas moins être administrée de manière loyale, compatible avec les droits de la défense. Voir Soyer, J.-C. *Droit pénal et procédure pénale* (12e édition) - BSHS/ Droit -Science politique KJV 7979 S731 2001.

obligation de confidentialité et principe du besoin d'en connaître). Surtout, la réalité technique des échanges (" *sniff* " des pseudo-frappes clavier de l'attaquant à destination de la machine cible) ne permettrait pas de qualifier ceux-ci de " correspondance-privée ", celle-ci étant définie par la jurisprudence comme le fait de destiner un message à une ou plusieurs personnes physiques ou morales individualisées (caractère nominatif) ou déterminées (par leur fonction) et dont la teneur a trait à la sphère privée (le tribunal cite dans sa décision, mais de façon non exhaustive : " l'existence d'un lien les unissant qui peut être familial, amical, associatif, (...) ")[52].

Il en va différemment selon nous en matière d'interception de conversations *chat*. L'hypothèse considérée ici est celle où l'attaquant utilise le client IRC installé (par lui-même ou non) sur le système pot de miel[53], ce qui donne une position privilégiée au responsable de *honeypot* pour intercepter (on serait tenter immédiatement de dire " pour espionner ") ses messages.

On pressent très vite bien entendu tout l'intérêt scientifique que le contenu de ces échanges peut comporter[54], cependant il faut bien dire que la proportionnalité des moyens mis en œuvre ici (cf *supra*, problématique des " attaquants internes ") est, selon nous, loin d'être une évidence. De plus, on émettra également de sérieux doutes quant à la loyauté de l'administration de la preuve, l'interception de conversations chat pouvant vraisemblablement tomber sous le coup de l'incrimination de violation du secret des correspondances.

En effet, dans ce cas de figure comme dans le précédent, nous écartons d'emblée l'application de l'article 226-1 du code pénal car d'une part, les données concernées (frappe clavier ou messages instantanés) ne sont pas des " paroles " (ou des images telles que visées à l'alinéa 2) et d'autre part, la teneur des échanges est a priori étrangère à " l'intimité de la vie privée "[55].

S'agissant de l'application de l'article 226-15 du code pénal, étant admis que les messages instantanés éventuellement interceptés sont bien une " correspondance émise, reçue ou transmise par la voie de télécommunications " (autrement dit une " correspondance électronique "), il convient néanmoins de s'interroger sur la nature protégeable des messages. En effet, le secret des correspondances

[52] Trib. Corr. Paris, 2 novembre 2000 `http://www.legalis.net/jnet/` (sous " contenus illicites ")

[53] On peut imaginer également que l'attaquant dispose sur sa propre machine d'un client IRC mais qu'il utilise un tunnel VPN à travers le *honeypot* qui devient ainsi le relais des messages...

[54] En effet, dans le cas de communications IRC établies entre les membres d'une même communauté de pirates, on pourrait ainsi recueillir des informations très instructives sur les ressources partagées par les attaquants, informations sur les nouveaux outils et vulnérabilités, résultats de scans massifs préparatoires à de plus importantes offensives, etc.

[55] Bien que la notion d'intimité de la vie privée " ne soit pas définie dans le code et eu égard à la jurisprudence en ce domaine, l'*intimité* de la vie privée concerne plutôt la vie familiale, les murs, le domaine de la santé, etc., et ne s'appliquera pas facilement au domaine du " loisir " informatique que représente pour l'attaquant les activités liées au piratage...

suppose que ces messages n'aient pas un caractère public et que l'on puisse les qualifier, comme le courrier électronique, de " correspondance privée " (Cf *supra* : définition de la correspondance privée). Sur ce point, nous pensons que la notion d' " expectative raisonnable de vie privée ", utilisée notamment par la Cour suprême du Canada, pourrait utilement s'appliquer ici pour déterminer la nature des sessions IRC interceptées. François Blanchette, dans un mémoire intitulé " *L'expectative raisonnable de vie privée et les principaux contextes de communications dans Internet* "[56], rappelle par exemple qu'un canal IRC peut être rendu accessible à tous (on parlera aussi de " forum IRC "), alors que dans d'autres cas, il sera accessible uniquement à des personnes que l'utilisateur connaît ; de plus, il est possible que la communication IRC n'utilise pas les serveurs du réseau IRC mais soit effectué d'ordinateur à ordinateur, entre deux personnes utilisant un logiciel client IRC. Selon le cas (ouvert à tous /fermé à un public préalablement identifié / utilisant ou non un serveur IRC), on pourrait donc présumer du caractère " privé " ou non du message instantané. L'auteur du mémoire précité cite encore de nombreux facteurs qui accroissent ou diminuent l'expectative raisonnable de vie privée en matière de " bavardage-clavier ou clavardage du service IRC ", en particulier l'ouverture ou non d'une fenêtre confidentielle (chiffrement SSL)[57].

En définitive, si la jurisprudence ne nous offre aujourd'hui aucune illustration de l'application de la législation sur la protection des données personnelles en matière de technologies *honeypot*, le risque ici envisagé devra être considéré avec sérieux et dans le strict respect des principes fondamentaux susvisés (proportionnalité, finalité, transparence). *Last but not least...*, il convient maintenant d'aborder la question de la responsabilité.

[56] Mémoire réalisé sous la direction du Professeur Pierre Trudel (Décembre 2001), Maîtrise en Droit (L.L.M.), Faculté de droit de Montréal. Consultable à l'adresse : `http://www.juriscom.net/documents/priv20040203.pdf`

[57] Il opère également une analogie avec les services de communication en temps réel (fonctions de messagerie et de conférence) des anciens babillards électroniques (BBS), présageant pour le même sort pour les messages IRC que dans la décision *United States v/ Charbonneau (979 F Supp. 117, S.D. Ohio 1997, p.1184)*. Selon cette décision, la preuve recueillie par des agents du FBI lors d'une session bavardage-clavier ne bénéficie pas d'une expectative raisonnable de vie privée : " *All of the evidence gathered by the FBI from the chat rooms resulted from the presence of undercover agents, in the rooms. Clearly, when the defendant engaged in chat room conversations, he ran the risk of speaking to an undercover agent. Futhermore, Defendant could not have a reasonable expectation of privacy in the chat rooms. Accordingly, the e-mail sent by the defendant to others in a chat room is not afforded any semblance of privacy* ".

4 Honeypots, entre contrôle et réponse : le “ bras armé ” de la sécurité

Un point souvent discuté[58] en matière de *honeypot* est celui de la responsabilité encourue en cas de dommages causés à un tiers suite à la compromission du système pot de miel. De même a été posée la question de la légalité de certains moyens de réponse qui peuvent être mis en œuvre : fichiers piégés, scans de port en retour par exemple, et pour lesquels l'hypothèse est lancée qu'ils constitueraient eux-mêmes une “ contre-attaque ” punissable au titre des articles 323-1 à 323-3 du code pénal (accès et maintien frauduleux / entrave et faussement du système d'information / introduction, suppression et modification de données).

4.1 Responsabilité du fait de la compromission du système honeypot, un risque avéré mais maîtrisable

Le cas ici envisagé est donc celui où l'attaquant réussit à “ s'échapper ” du pot de miel et à l'utiliser comme rebond pour conduire de nouvelles attaques contre des systèmes étrangers ou, pourquoi pas, d'autres machines du réseau. En réalité, les niveaux de risques sont différents d'un *honeypot* à l'autre ; on oppose classiquement [3] les *honeypots* dits “ à forte interaction ” aux *honeypots* “ **à faible interaction** ”.

Pour ces derniers, le risque potentiel est considéré comme faible car ils ne font pour la plupart que simuler des services sur des machines virtuelles, sans offrir beaucoup de privilèges à l'attaquant. C'est d'ailleurs de cette limitation dans l'interaction que l'attaquant perdra sans doute son intérêt pour le *honeypot*, se mettant en quête de nouvelles cibles.

Par opposition, les *honeypots* de recherche (type *honeynets*), qui sont conçus pour récolter un maximum d'informations, sont classés dans les systèmes dits “ **à forte interaction** ”, car ils offrent de vrais services et un environnement avec lequel l'attaquant va pouvoir interagir après compromission du système, que ce soit en lançant des attaques par rebond, en se servant des machines comme zombie pour réaliser un déni de service, etc.

Le risque est alors important de voir sa responsabilité engagée par un tiers ayant subi des dommages suite à cette compromission, moins sur le plan pénal[59]

[58] Cf les messages postés dans certaines listes de discussion : “ Use a honeypot, Go to Prison ? ” `http://www.securityfocus.com/news/4004` ; “ les pots de miel sont-ils légaux ? ” `http://linuxfr.org/2003/06/16/12887.html`

[59] En effet, “ *nul n'est responsable pénalement que de son propre fait* ” (principe de responsabilité pénale individuelle : article 121-1 du Code pénal). De plus, une action pénale sur le fondement de la complicité par fourniture de moyens (parfois évoquée dans les forums de discussions) nécessiterait de prouver le partage de l'intention criminelle. Autre hypothèse marginale (?), celle où le responsable de *honeypot* qui, pour mieux attirer ses abeilles, aurait mis à leur disposition sur le système différents fichiers ou programmes téléchargeables (MP3, exploits, base de données de virus, etc.) communément disponibles sur Internet dans une page Web consacrée au pira-

mais plutôt par le biais d'une action civile en dommages-intérêts sur le fondement des articles 1382 et suivants du Code civil :

> " *Tout fait de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer* " (article 1382 C.Civ.).

Pour autant, il faudra au demandeur prouver à la fois **la faute** du responsable de *honeypot*, son préjudice et le lien de causalité entre les deux. Sur ce point, des doutes peuvent tout à fait être émis sur l'existence d'une faute, les systèmes pot de miel n'étant pas nécessairement des machines non sécurisées ; bien au contraire, comme nous le verrons un peu plus loin, les *honeypots* doivent être astreints à un contrôle très scrupuleux du trafic vers l'extérieur...

Enfin, il ne faudra pas négliger, à côté du risque de l'action civile en réparation par le tiers, le **risque assurantiel** ; en effet, la mise en place d'un *honeypot*, si elle introduit des risques pour le système d'exploitation assuré, pourrait conduire à exclure les garanties de la police d'assurance en matière de risques informatiques. Il faudra donc valider préalablement les conditions dans lesquelles le *honeypot* pourra être déployé en particulier en environnement de production. A l'occasion du rapprochement avec l'assureur, on fera notamment état des mesures de sécurité mises en œuvre pour prévenir les utilisations malveillantes après compromission.

Des risques maîtrisables : le contrôle des données En effet, la limitation du risque d'action en responsabilité et du risque assurantiel passe au premier chef par la mise en place de mesures de sécurité de nature à permettre la surveillance et la maîtrise des connexions sortantes de l'attaquant. Ainsi, pour éviter la réalisation du risque d'attaque par rebond, plusieurs **solutions techniques** peuvent être adoptées :

---

tage. Dans ce cas, il aurait tout intérêt à n'offrir que des utilitaires seulement *en apparence* efficaces et d'origine non contrefaisante sous peine de tomber sous le coup du futur article 323-3-1 du Code pénal, en voie d'adoption devant le Parlement dans le cadre du projet de loi pour la Confiance dans l'Economie Numérique : " *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* ". [Disposition non définitive, issue du deuxième vote devant le Sénat le 8 avril 2004 : `http://www.senat.fr/dossierleg/pjl02-195.html`]. Là encore, cependant, il faudrait prouver l'intention criminelle du responsable de *honeypot*, ce qui semble improbable eu égard aux objectifs envisagés ici... Surtout, une telle disposition risque de mettre un coup d'arrêt à l'un des principaux objectifs des *honeypots*, à savoir l'étude des outils et méthodes d'attaques. En effet, suite à l'amendement des députés en seconde lecture, les exceptions légales initialement prévues, en particulier celle relative aux " *besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de communications électroniques et des systèmes d'information* ", ont été supprimées au profit de la simple référence au " *motif légitime* ", dont l'appréciation reviendra par conséquent à la seule discrétion du juge.

1. l'interdiction de tout trafic vers l'extérieur : à l'évidence, cette solution, si elle a le mérite de l'efficacité, pêche par manque de furtivité puisque ce comportement sera très vite détecté et considéré comme suspect, poussant ainsi l'attaquant à abandonner son attaque[60] ;
2. la limitation de la bande passante ou du nombre de connexions sortantes (Cf *Netfilter* e.g.). Ainsi, dans l'architecture dite de première génération (GenI) du *Honeynet Project*, les communications sortantes sont limitées dans le temps (typiquement entre 5 et 10 par heure) ;
3. l'analyse des paquets sortants et leur modification à la volée pour les rendre inoffensifs (Cf architecture de seconde génération - GenII, Snort_inline).

Dans tous les cas, ne rien contrôler serait une politique éminemment dangereuse et aussi la pire des défenses en cas d'action judiciaire ; le responsable de *honeypot*, en bon gestionnaire de risques, appréciera donc les mesures de sécurité appropriées en fonction du niveau d'interactivité du système.

4.2 Capacités de réponse et pré-constitution de preuves : le cas de SPECTER

Le mode de preuve des infractions étant libre en droit pénal français[61], la tentation est grande de vouloir organiser et pré-constituer un maximum de preuves des intrusions frauduleuses dont le *honeypot* est le capteur. Pour ce faire, certains outils offrent des fonctionnalités tout à fait intéressantes. Ainsi du logiciel SPECTER qui propose (entre autres) comme action réactive face à une attaque :

- le " scan de port en retour ", ou encore
- dans sa nouvelle version V7, l'insertion de *markers* sur le PC de l'attaquant, issus de fichiers piégés qu'il aura téléchargés sur le *honeypot* [6].

L'option Port Scan S'agissant de l'option de " *Port Scan* " de l'attaquant offerte par SPECTER dans la paramétrage des actions automatiques de renseignements (*Intelligence*), celle-ci permet simplement d'enrichir les logs de la liste de ses services ouverts. Pour autant, selon [5], il s'agit d'une " *fonctionnalité très sensible dans le monde des pots de miel (car) cette réaction peut être considérée comme une contre-attaque* ". Qu'en est-il exactement de la sensibilité de cette fonction et de son caractère potentiellement illicite ?

Comme on le sait, un scan de ports permet d'étudier l'architecture de machines distantes et de déterminer quels sont les ports ouverts, fermés ou filtrés d'un système. Ce faisant, il constitue souvent le préliminaire d'une attaque, car l'attaquant peut ainsi cartographier les failles d'un système ou d'un réseau et éventuellement, lancer automatiquement un *exploit*. Pour autant, comme le rappelle Thiébaut Devergranne dans son article *Le scan de ports est-il licite ?* " [7], cette fonctionnalité n'a rien d'exceptionnel " *puisque c'est le préalable à toute connexion* " et qu' " *il existe des motifs légitimes de multiples connexions aux*

[60] D'où l'" échec " des premiers essais du *Honeynet Project* [2]
[61] Cf *op.cit*, note 52

ports d'un système ". Dès lors, la difficulté provient en réalité de la dérive d'un usage normal du système.

Dans le présent cas de figure, le scan de ports en retour initié par le système *honeypot* pour recueillir de l'information, s'il n'est pas exécuté à des fins malveillantes, pourrait néanmoins revêtir un caractère frauduleux dans le sens où il s'agit d'un acte volontaire, étranger au fonctionnement normal des systèmes en vue d'établir une connexion et non autorisé[62] par le propriétaire de la machine distante[63]. Il faudrait cependant encore que, dans l'hypothèse (particulièrement improbable) d'une poursuite judiciaire pour fait de " scan en retour ", on puisse qualifier ce scan sinon d'accès ou du moins de tentative d'accès frauduleux au système du " premier attaquant ". A cet égard, [7] rappelle à juste titre que, pour être punissable, le scan de ports doit dépasser le stade des actes préparatoires et être au minimum qualifié de commencement d'exécution, ce qui n'est guère envisageable en l'espèce, le scan de port en retour n'étant pas à proprement parler suivi d'effet, c'est-à-dire qu'il donne lieu simplement à la collecte d'informations et en aucun cas, à une exploitation malveillante à l'encontre du système sondé.

Les fichiers traces ou " *markers* " A la différence de l'option précédente, on pourrait soutenir que les markers sont eux " suivis d'effet " car ils agissent comme des virus en répandant, à l'insu de l'attaquant, différentes traces plus ou moins cachées[64] sur son disque dur. Ces traces contiennent tous les éléments du passage de l'attaquant : date, heure, adresses IP du pot de miel et de la machine ayant réalisé l'intrusion.

On perçoit très bien l'intérêt d'une tel procédé de " mouchard virtuel " lorsque l'on est confronté au problème de preuve des tentatives d'intrusion, si l'attaquant *spoofe*[65] sa connexion, qu'il réalise une attaque par rebond ou de façon plus originale, adopte une stratégie défense du type " **Trojan defence** "[66]. Cependant, on peut penser qu'il y a ici un risque de se trouver soi-même

[62] L'hypothèse des tests dintrusion doit en effet être réservée...

[63] Rappel : il ne faut pas confondre ici la motivation (qui peut être légitime) et l'intention frauduleuse - Cf *supra* sous 1.2.2. -. En l'espèce, dans le cadre de l'article 323-1 du Code pénal, l'intention frauduleuse se caractérise par " la connaissance du fait que l'on a agit sans droits ou que l'on était pas autorisé à accéder au système " (Raymond Gassin, *Fraude informatique*, Encycl. Dalloz Droit pénal [Rép. Pén. Dalloz], pages 1-41, n°132 - oct. 1995).

[64] Seule l'exécution d'un contrôle d'intégrité de son disque dur permettrait à l'attaquant de retrouver l'emplacement des *markers*, opération que personne ne veut réaliser en pratique avant et après chaque clic de sa souris ! [6].

[65] C'est-à-dire qu'il se fait passer pour une autre personne : problématique de l'usurpation d'identité et/ou de compte utilisateur...

[66] De plus, on aura peut-être de ce côté de la Manche à affronter également une nouvelle ligne de défense déjà utilisée en Grande-Bretagne et qui se résume dans l'expression suivante : " *Computer did it* ". Deux affaires ont récemment permis dillustrer cette stratégie :

– Juillet 2003, affaire " Julian Green " (UK) : placé en détention provisoire pour détention de 172 photos pédo-pornographiques, un Britannique est finalement

délinquant, non pas sur le fondement de l'accès ou du maintien frauduleux sur un système, mais sur celui de l'introduction frauduleuse de données[67]. En effet, c'est bien l'attaquant lui-même qui télécharge les fichiers piégés sur son propre disque dur (et non le gestionnaire de *honeypot* qui y accède pour y placer les *markers*), mais une fois exécutés, ils insèrent de nouvelles données dissimulées sur le disque de l'attaquant.

" Légitime défense ", rétorquerait-on. Quelle différence par exemple avec les dispositifs anti-vol consistant en la projection d'une encre rouge indélébile sur des billets de banque ou encore des vêtements protégés par ce procédé ? A ceci près qu'en droit pénal français, la légitime défense ne s'applique qu'aux personnes et non à la protection des biens, sauf lorsque l'acte de défense est accompli par la victime " *pour interrompre l'exécution d'un crime ou d'un délit*

acquitté suite au témoignage dun expert qui a identifié onze Chevaux de Troie sur le PC de l'inculpé, ce qui corrobore l'hypothèse soutenue par l'avocat de la défense selon laquelle le téléchargement des fichiers litigieux a pu être effectué sans la connaissance ni la permission de l'utilisateur. Fait suite à une affaire similaire en avril 2003 pour des faits et des circonstances similaires (affaire " Karl Schofield "). Lire : `http://www.sophos.com/virusinfo/articles/porntrojan.html(ManblamesTrojanhorseforchildpornography)`.

– Octobre 2003, affaire " Aaron Caffrey "(UK) : adolescent de 19 ans accusé d'avoir lancé un déni de service qui a fait tombé plusieurs systèmes du port de Houston (Texas) en septembre 2001. Alors qu'une copie du script de l'attaque (qui porte par ailleurs le nom de sa petite amie Internet, Jessica) est saisie sur le disque dur de son PC et qu'aucune preuve de la compromission alléguée pour se défendre n'est révélée par l'expertise des données sur le disque, le jury se laisse convaincre par l'histoire et la personnalité du jeune adolescent qui dit vouloir devenir un professionnel de la sécurité et appartenir à un groupe appelé *Allied Haxor Elite* dont l'objectif déclaré est de mener avec la permission de ses amis des tests d'intrusion sur leurs machines. Ainsi l'adolescent est blanchi alors même qu'aucun indice matériel ne vient cette fois corroborer les allégations du suspect !

  Lire : `http://news.zdnet.co.uk/0,39020330,39117033,00.htm` (" *Expert undermines hackings suspect defence* "); `http://uk.news.yahoo.com/031028/80/ecbh4.html` (" *Hackers defence : the computer did it* "); `http://www.sophos.com/virusinfo/articles/caffrey.html` (" *Teen hacker cleared by jury - blames other hackers for port of Houston attack.* "); `http://news.zdnet.co.uk/internet/security/0,39020375,39117209,00.htm` (" *Trojan defence acquits British teenager* ").

[67] Article 323-3 du code pénal : " *le fait d'introduire frauduleusement des données dans un système de traitement automatisé de données (...) est puni de trois ans d'emprisonnement et de 300.000 F d'amende* ".

"[68]. En l'occurrence, le procédé de fichiers piégés n'est ni exécuté par la victime (le responsable de *honeypot*) ni conforme au but à poursuivre.

" Etat de nécessité ", alors ? Le fait justificatif de l'état de nécessité[69] peut effectivement s'appliquer aux « biens » et il est en fait privilégié par certains[70] pour appuyer la légalité du procédé. Or, une lecture attentive de l'article 122-7 du code pénal montre que celui-ci exige, pour pouvoir justifier de l'état de nécessité, que l'acte de défense ait été " nécessaire à la sauvegarde (...) du bien ", condition qui n'est pas respectée en l'espèce, les fichiers traces tendant non pas à limiter l'étendue des dommages liées à la compromission, mais seulement à pré-constituer les preuves de l'infraction.

En définitive, l'obtention par le procédé des *markers* d'indices de nature à établir la matérialité d'une intrusion frauduleuse risque fort, selon nous, de se trouver contestée au regard du principe de légalité de la preuve et ne devrait pas en tout état de cause être activée dans le cadre des *honeypots* pour lesquels le responsable n'a pas d'emblée, dès l'initiation du projet, inscrit dans ses objectifs la poursuite des attaquants[71] (par exemple pour les *honeypots* de recherche). Pour tenter néanmoins de s'aménager des indices de rattachement fort avec la machine de l'attaquant, il serait possible et surtout légalement admissible de prévoir en lieu et place de ces markers disséminés un procédé similaire par lequel l'attaquant téléchargerait lui-même des fichiers attractifs présents sur le *honeypot* et qui recèleraient simplement (mais toujours à son insu[72]) des signatures, tatouages électroniques ou tout élément passif dont on peut prouver l'origine. Enfin, pour éviter la disparition des preuves et traces informatiques relatives à l'intrusion et permettre que celles-ci soient recevables en justice, on recommandera la mise en œuvre de toutes mesures de sécurité propres à garantir l'intégrité des données enregistrées par les *honeypots* (horodatage, certification

[68] Article 122-5 du code pénal : " Nest pas pénalement responsable la personne qui, devant une atteinte injustifiée *envers elle-même ou autrui*, accomplit, dans le même temps, un acte commandé par la nécessité de la légitime défense d'*elle-même ou d'autrui*, sauf s'il y a disproportion entre les moyens de défense employés et la gravité de l'atteinte.

Nest pas pénalement responsable la personne qui, pour interrompre l'exécution d'un crime ou d'un délit contre un bien, accomplit un acte de défense "

[69] Article 122-7 du code pénal : " Nest pas pénalement responsable la personne qui, face à un danger actuel ou imminent qui menace elle-même, autrui ou un bien, accomplit un *acte nécessaire à la sauvegarde de la personne ou du bien*, sauf s'il y a *disproportion* entre les moyens employés et la gravité de la menace ".

[70] Lire Elisabeth Stella dans l'article consacré au logiciel SPECTER et à la fonctionnalité de *markers* [6] page 8.

[71] Application analogique du principe de stratégie et de négociation contractuelle : " Omit needless words " - RAIFFA Howard, " The art & science of negociation ", éd. Belknap / Harvard University Press, 1982.

[72] Ces éléments pourraient par exemple être dissimulés par le recours à des moyens stéganographiques.

serveur, authentification forte, etc.) ainsi que l'application de mesures conservatoires[73] (constat d'huissier, scellés électroniques, mise sous séquestre, etc.).

5 Conclusion

Les *honeypots* sont un sujet passionnant sur le plan de la prospective juridique. Quant à statuer sur la légalité ou non de ces ressources, on voit bien que la diversité des objectifs et des outils ne permet pas de tirer des enseignements généraux, en particulier lorsque les domaines du droit touchés sont un parent pauvre de la jurisprudence. Dès lors, la seule approche possible est celle de la gestion de risques, avec pour objectif de prévenir au maximum les risques de contentieux, la présente analyse des points sensibles de la construction juridique des *honeypots* permettant simplement de se poser les bonnes questions.

Par exemple, une question fondamentale est de savoir quels sont les objectifs du *honeypot* ? : observer, défendre... et poursuivre ? Ces objectifs doivent être déterminés dès l'origine du projet et documentés dans un document de conception générale et détaillée, incluant le cas échéant une analyse de risques, un plan de sécurité et tous documents permettant de retracer l'historique du projet et les étapes de sécurisation (techniques, organisationnelles, juridiques) qui ont été menées. Bien sûr, la frontière entre *honeypot* de recherche (dont on a dit qu'ils ne permettraient pas la poursuite des attaquants du fait du consentement de la victime[74]) et les *honeypots* de production (qui nécessitent des précautions sur le plan juridique, par exemple s'agissant de la problématique des " attaquants internes "[75]) est à géométrie variable, ce qui implique, encore une fois, une casuistique et une gestion de projet adaptée à ses spécifications techniques...

In fine, le responsable de projet devra définir son niveau de risque acceptable, en fonction notamment de la valeur ajoutée attendue [76], de la nature et de

[73] Ces mesures pourront être décidées notamment sur le fondement de l'article 145 du Nouveau Code de Procédure Civile : " S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé ".

[74] Cf section 1.2.1.

[75] Cf section 2.2

[76] " En matière de *honeypot* de production, on se rendra vite compte par exemple qu'il est fastidieux de dépenser du temps pour regarder des traces de sécurité sur un système non critique, à moins d'avoir déjà terminé d'analyser les traces des vrais systèmes de production à protéger (le *honeypot* n'étant pas, en général, la priorité sur un réseau d'entreprise. " Cf [5], au sujet du démon *Honeyd* développé par Niels Provos pp.43 à 53.

l'étendue des dommages potentiels et de l'" entropie "[77] des scénarios de risque juridique.

Références

1. Cliff Stoll : The Cuckoo's egg : tracking a spy through the Maze of Computer Espionnage (1988) - ISBN 0743411463.
2. The Honeynet Project - `http://www.honeynet.org`
3. Lance Spitzner - *Honeypots : tracking hackers* (2002) - ISBN 0321108957.
4. L. Halme et R. Bauer, *AINT misbehaving : a taxonomy of anti-intrusion techniques* (1995) - `http://www.sans.org/resources/idfaq/aint.php`
5. *Honeypots, le piège à pirates !* - Dossier spécial, MISC Juillet-Août 2003, pp.24-61.
6. Elisabeth Stella et Thierry Martineau, *Specter, un honeypot qui compromet les pirates : techniques et légalité*, article paru dans MISC, Janvier-février 2004, pp.6-9.
7. Thiébaut Devergranne, *Le scan de ports est-il illicite ?* - 31 janvier 2003 `http://hstd.net/scandeports.pdf`
8. Valérie Sédallian, *Légiférer sur la sécurité informatique : la quadrature du cercle* - 2003, Juriscom.net.

[77] Dans la théorie de l'information (définie par Claude Shannon en 1949 - *A Mathematical Theory of Communication*, Bell System Technical Journal, vol.27 n°4 ; *Communication Theory of Secrecy Systems*, Bell System Technical Journal, vol.28 n°4), l'entropie est le nombre qui mesure l'incertitude d'un message en fonction de la quantité d'informations nécessaires pour retrouver le texte en clair en entier. Cf Bruce Schneier, *Cryptographie appliquée* (2nde édition), John Wiley & Sons, Inc., 1996.