La CyberCriminalité

Les acteurs, les infractions,

Cas concret et retour d'expérience

Par Vincent Lemoine

Chef du Groupe Cybercriminalité de la B.R Nanterre

Expert non inscrit

Plan de l'intervention

I) Définition.

II) Les Acteurs.

III) Les atteintes aux personnes.

IV) Les atteintes aux biens.

V) Cas concret : une affaire de Phishing.

VI) Retour d'expérience en entreprise.

I) Définition

- ***La cybercriminalité ne défini pas à elle seule une infraction, mais un ensemble d'atteintes aux biens ou aux personnes commises via l'utilisation des nouvelles technologies.***

- ***Par nouvelles technologies, on entend tout mode de communication, à savoir l'Internet mais également la téléphonie mobile, peut importe le protocole utilisé.***

- ***Cette notion de cybercriminalité peut concerner les infractions relatives au contenu qu'il s'agisse de textes (insultes, propos négationniste ou xénophobes) ou d'images (fichiers pédo – pornographique).***

- ***Elle peut concerner également les atteintes à la propriété intellectuelle, qui constitue un véritable fléau pour l'économie.***

- ***Parfois, l'utilisation directe des NTICS qui peut constituer à elle seule une infraction (Ex : Loi 1978, 1988).***

Distinctions entre les Infractions

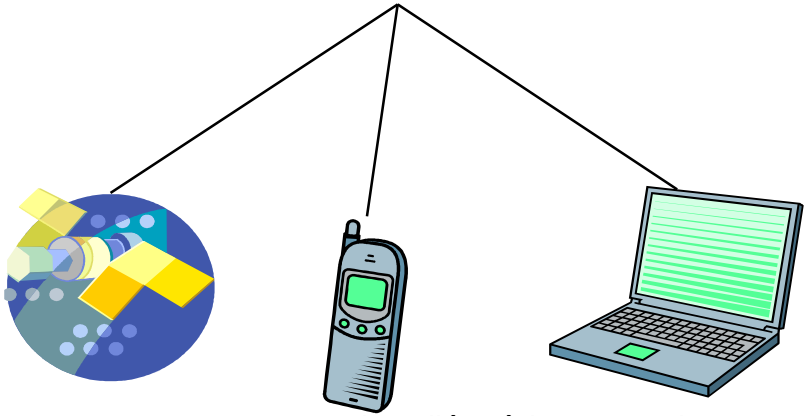
Cybercriminalité

Infractions pour lesquelles les Technologies de l'Information et de la Communication sont l'objet même du délit

Infractions pour lesquelles l'Internet est le moyen de commission ou la facilite

Caractéristiques : nature des technologies utilisées

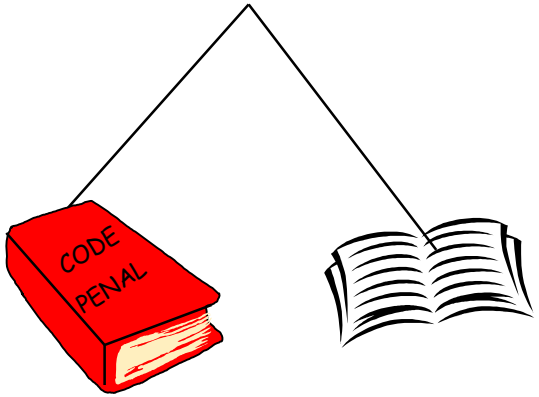
Caractéristiques : criminalité de droit commun, de nature juridique traditionnelle



Infractions liées à la télécommunication

Infractions liées à la téléphonie cellulaire

Infractions informatiques



Infractions prévues par le code pénal

Infractions prévues par des textes spécifiques

Les incriminations relatives à la cybercriminalité ne sont pas uniquement inclues dans le Code Pénal, mais suivant leur nature dans différentes codes, notamment en matière :

- ***d'escroqueries via les moyens de paiements (cartes bancaires, faux chèques, etc.), dans le Code Monétaire et Financier.***

- ***de presse, d'expression, de publication dans La loi du 29 juillet 1881 relative à la liberté de la presse.***

- ***contrefaçon d'œuvres de l'esprit, de brevets, de marques dans le Code de la Propriété Intellectuelle.***

Par contre les incriminations relatives aux dites CNIL et GODFRAIN ont été insérées dans le Code de Pénal.

Comme le décrivait le site du parlement européen en octobre 2005, la lutte efficace contre la cybercriminalité requiert l'utilisation de techniques d'enquête nouvelles et la surveillance générale d'Internet.

- ***Cependant, ces nouvelles méthodes d'investigations et de contrôles des systèmes d'information se révèlent être attentatoires aux droits fondamentaux, en particulier au droit à l'anonymat et à la liberté d'expression. Des règles très strictes sont imposées aux services spécialisés pour l'exercice de la Police Judiciaire.***

- ***A titre d'exemple, il est interdit aux services de Police et de Gendarmerie de réaliser des provocations en matière de faits liés à la cybercriminalité.***

- ***La loi a été modifiée le 05 mars 2007 pour permettre aux enquêteurs comme en matière de stupéfiants de réaliser des infiltrations et des échanges de fichiers illicites. Cependant le décret d'application n'est pas encore paru.***

- ***Le 14.02.2008 Michèle Alliot Marie a annoncé un Plan de Lutte contre la Cybercriminalité. Celui prévoit un renforcement des moyens techniques et humains, ainsi que de nouvelles incriminations (usurpation d'identité dans la LOPSI II).***

- ***Il sera également permis aux enquêteurs de réaliser des perquisitions dans certains états sans aviser les autorités locales au niveau de l'Union Européenne.***

- ***Mais cela semble insuffisant, car actuellement la plupart des faits délictueux sont commis à partir d'adresses de types Webmails (Gmail, Yahoo, Hotmail, etc).***

- ***Elles sont crées à l'étranger et il n'est pas possible de perquisitionner en direct sur ces BAL pour des questions de droit. Le droit applicable est celui d'implantation du serveur.***

- ***Loi de 1978***
- ***Loi de 1988***
- ***Convention Européenne sur la Cybercriminalité* signée et ratifiée par la France à BUDAPEST le 23.11.2001**
- ***L.S.Q* (Loi relative à la Sécurité Intérieure) 11/01**
- ***L.O.P.S.I* (loi pour la sécurité Intérieure). 08/02**
- ***L.C.E.N* (loi dans la confiance dans l'économie numérique) 06/04**
- ***L.C.T* (loi contre le terrorisme) 12/05**
- ***Loi relative à la Prévention de la déliquance des Mineurs* 02/07**
- **Et prochainement la *L.O.P.S.I II***

II) Les Acteurs

- ***L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, créé en 2000, et rattaché à la D.C.P.J.***

- ***Les enquêteurs spécialisés, de la Police : E.S.C.I (Enquêteurs Spécialisés en Criminalité en Informatique). Ils sont environs 170 en France affectés en D.I.P.J, D.R.P.J, B.E.F.T.I, B.PM 75, ainsi qu'en Sécurité Publique.***
  (Ex : Sûreté Départementale d'Amiens et de Melun).

- ***Le S.T.R.J.D, regroupant le Département de Lutte contre la Cybercriminalité et le Centre d'Analyse des Images Pédopornographiques regroupant une vingtaine d'enquêteurs.***

- ***L'institut de Recherches Criminelles de la Gendarmerie Nationale, notamment le département I.N.L, apportant un concours technique aux enquêteurs, et réalisant des missions d'expertises au profit des Magistrats, soit une quinzaine de personnes disposant pour la plupart de Mastères Techniques (informatique, Télécom).***

- ***170 enquêteurs N-TECH (Nouvelles Technologies), affectés dans des Offices Centraux (O.C.L.C.T.I.C, O.C.L.T.I, O.CL.D.I), en Sections ou Brigades de Recherches, ainsi qu'en Brigade Départementale de Renseignements et d'Investigations Judiciaires au sein des Cellules d'Investigations Criminelles.***

- ***Outre ces enquêteurs, certains services de Police (DST, OCRVP), des Douanes, des Impôts, de la DGCCRF disposent d'enquêteurs spécialisés dans les Nouvelles Technologies.***

- ***Les orientations à venir ?***

  Création au niveau local de correspondants N-TECHS dans les régions en France, dont 32 en Ile de France. Il s'ajouteront au 8 C-NTECH existants sur les Hauts de Seine et les 2 réservistes qui apportent leurs concours à notre groupe.

- ***Le même dispositif devrait apparaître au niveau des services de Police.***

- ***Pour simplifier l'appréhension des faits liés à la cybercriminalité, de nouveaux dispositifs destinés à faciliter le travail des enquêteurs été mis en place :***

  - Plateforme PHAROS.

  (Elle est gérée au niveau de l'O.C.L.C.T.I.C par une équipe mixte composé de Policiers et de Gendarmes.

  Cette année plus de 14 000 signalements ont été reçus et traités donnant lieu à 1200 dossiers, dont 200 en France)

  ce type de plateforme est envisagé au niveau de l'U.E.

  - Système de Pré Plainte. (en expérimentation)

  destiné à simplifier les démarches des victimes.

- ***Ces systèmes vont faciliter les signalements et les plaintes en mettant des dispositifs automatisés et sécurisés et permettre des rapprochements plus précis.***

- ***L'ensemble des enquêteurs sont formés en Interne :***

  - pour la police par l'O.C.L.C.T.I.C,
  - pour la Gendarmerie par l'I.R.C.G.N, ainsi que par le C.N.F.P.J.

- ***La formation au niveau de la gendarmerie, débouche sur des formations diplomates dans le cadre d'un DU en criminalistique et d'un Master en SSI à TROYES depuis 2005***

- ***La ministre de l'Intérieur envisage une formation diplômante identique pour les enquêteurs de la Police avec des partenariats avec le monde professionnel plus étroits.***

- ***La plupart des enquêteurs formés possèdent également outre cette compétence technique une compétence judiciaire, s'agissant de la qualité d'O.P.J.***

L'ensemble des enquêteurs reçoivent une formation adaptée :

- ***Informatique (Windows, Mac, Linux)***
- ***Réseaux Informatique & Gsm,***
- ***Droit des Nouvelles Technologies,***
- ***Sur les techniques d'investigations techniques,***
- ***Formation sur les logiciels Forensics, la récupération des données,***
- ***Etude d'un système ou d'un phénomène particulier dans le cadre de la préparation de leur mémoire.***

Il reçoivent des équipements adaptés à l'issue de leur cursus notamment une station d'analyse équipée :

- ***Des outils Forensics tels que Ilook, Encase, Forensics Toolkit pour l'analyse des supports numériques qui permettent d'effectuer des recherches sur les fichiers présents et effacés, ainsi dans les « Free Space, Slack Space ».***

- ***Des utilitaires développés au sein de la Gendarmerie, par l'Institut de Recherche Criminelle tels que :***

  - Sim Analyst (Carte Sim),
  - Reset Analyst (Identifier la nature d'une carte à puce),
  - Cb Analyst (Analyse carte Bancaire et Yes card)
  - Wifi Analyst

- ***Un Cd Bootable destiné à la recherche automatique de signatures des fichiers connus en matière de Pédo – pornographie (+ 1 000 000 de signatures).***

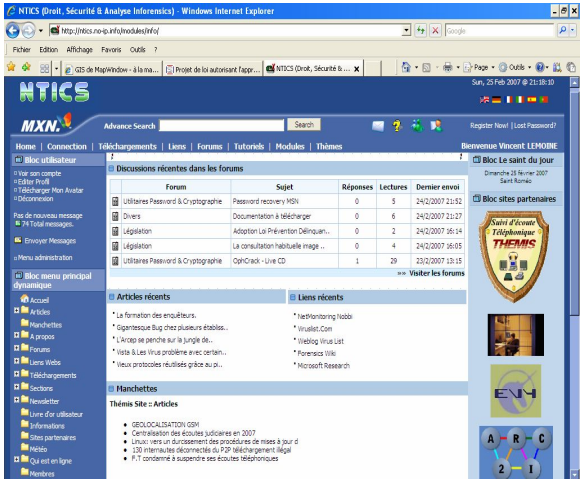
- ***Chaque année, sous l'égide de l'OCLCTIC, et du B.P.J de la Direction Générale de la Gendarmerie Nationale, des séminaires sont organisés pour permettre aux enquêteurs spécialisés, de parfaire leurs formations, d'échanger leurs expériences, et de nouer des contacts qui se révèleront très utiles sur le terrain.***

- ***L'avant dernier est intervenu courant janvier 2007, à l'Ecole Polytechnique de Palaiseau, ou nombre d'Intervenants se sont succédés durant deux jours (le CELAR de la D.G.A, l'Ecole Polytechnique, des Acteurs en matière de Nouvelles Technologies).***

- ***Le dernier a été organisé en novembre 2008 à l'école de Police de PERIGUEUX, il a regroupé une centaine d'enquêteurs.***

Une formidable entraide au niveau technique existe a l'échelle international, par l'intermédiaire d'initiatives personnelles au profit des enquêteurs spécialisés (France, Belgique et Suisse, Canada, Brésil, etc), notamment au travers de sites Internet tels que N.T.I.C.S et 4.N.6.S .

Plus récemment par la création d'association comme l'A.F.S.I.N. (Association Francophone des Spécialistes de l'Investigation Numérique), ou le Club Corsaire.



III) Les Atteintes Aux Personnes

- ***Elles sont diverses et variées :***
- ***Loi de 1881 (diffamation).***
- ***Détournements de Correspondances, Interceptions.***
- ***Menaces de Mort, racket, Chantage.***
- ***Atteintes à la Représentation de la personne.***
- ***Les infractions dites « Informatique et Libertés »***

- ***Mais surtout, la pédophilie, qui pourrait être décrite comme étant « l'attirance sexuelle d'un adulte envers des mineurs », Une série d'infraction spécifique ont été créées :***

  - Corruption de mineurs (Art. 227-22 du Code Pénal).

  - Enregistrement, diffusion, détention de l'image ou de la représentation d'un mineur à caractère pornographique (Art. 227-23 du Code Pénal)

  - La simple visualisation qui n'était pas sanctionnable auparavant, va l'est devenu depuis mars 2007.

- ***En outre, de ces infractions peuvent découler, notamment des faits :***

  - d'atteintes sexuelles,
  - d'agressions sexuelles,
  - voire de viol.

Mais également des infractions très variées :

- Provocation au suicide, ou mise à disposition d'information pouvant permettre de le faciliter. (223-13 du Code Pénal)

- Provocation à la consommation de substances nocives, telles que :
- l'alcool, (Art. 227-19 du Code Pénal).
- les stupéfiants. (Art. 227-18 du Code Pénal).

- La diffusion de messages à caractère violent, ou permettant la fabrication d'informations relatives à la fabrication d'explosif. (Art. 227-24 du Code Pénal).

- L'outrage à personne dépositaire de l'autorité publique. (Art. 433-5 du Code Pénal).

- Les propos diffamatoires sur des sites Internet, ou d'informations très ciblées destinées à nuire à un tiers.

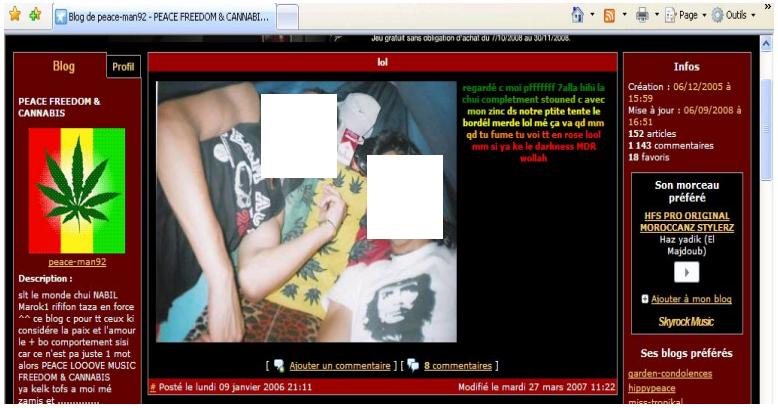
- ***Menaces d'atteintes à l'intégrité de la personne (viol) laissé sur un blog par des collégiennes de 12 ans, à l'encontre de l'un de leur camarade pour un problème de place en classe de physique. (menace).***

- ***Création d'un blog, pour menacer de mort, une jeune fille suite à une affaire sentimentale. (menace).***

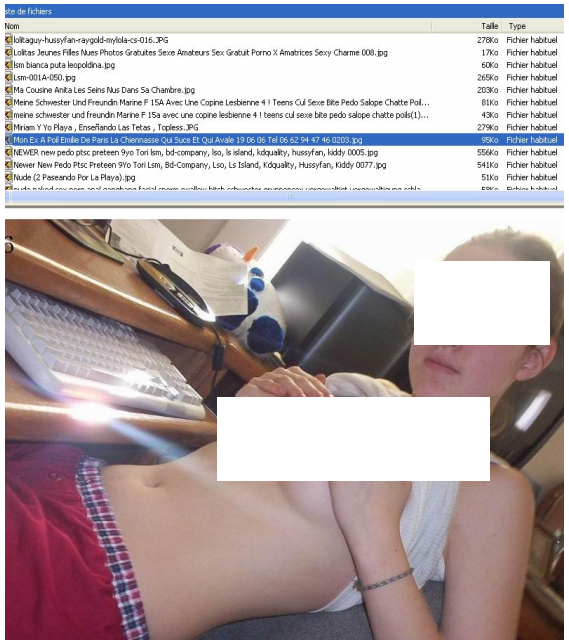
- ***Chantage pour obtenir des faveurs de nature sexuelles, réalisée via la captation à son issue de l'image de la victime lors d'une visio conférence. Transmission sur les réseaux Peer to Peer de l'image de son ex partenaire nue avec ses coordonnés postaux ou téléphonique. (chantage)***

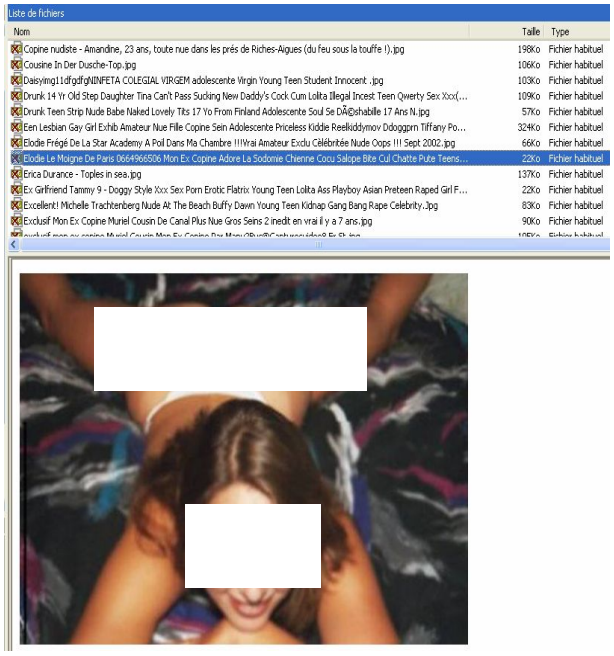
- ***Faux Casting de Mode, en se faisant passer pour un photographe de mode pour obtenir des images dénudées de tierces personnes qu'il a préalablement choisi sur Internet, au travers de Blog (abus de confiance).***

Quelques exemples en photos



Quelques exemples en photos





Il peut s'agir également de photos avec des renseignements d'adresse, Numéro de téléphone, coordonnés employeurs, etc..

IV) Les Atteintes Aux Biens

Il s'agit :

- *d'escroqueries (Art. 313-1 du CP),*
  (Phishing, fausses loteries Coca, Microsoft,
  vente véhicule par Ebay, escroquerie à la nigérienne),
- *d'abus de confiance, (Art 314-1 du CP)*
  (faux casting),
- *De contrefaçons d'œuvres de l'esprit. (Art L.335-2 du C.P.I)*
- *D'intrusions sur les S.T.A.D. (Art 323-1 du CP)*
- *Réalisation de Faux (Art 441-1 du CP et L.163 du CMF)*
  (en matière d'identité ou de banque).
- *Détournement de correspondance. (Art 226-15 du CP)*

- ***Un Internaute passionné de sécurité, à l'aide de tutoriaux trouvés sur Internet, et de softs gratuits exploite les failles de sécurité présents sur des machines distances.***

- ***Il récupère ainsi des documents à caractère personnel, et bloque certains éléments matériels des ordinateurs de ses victimes.***

- ***Quand la victime l'intéresse, il se manifeste via le « NotePad » et propose ses services pour réparer les failles de sécurité sur son ordinateur.***

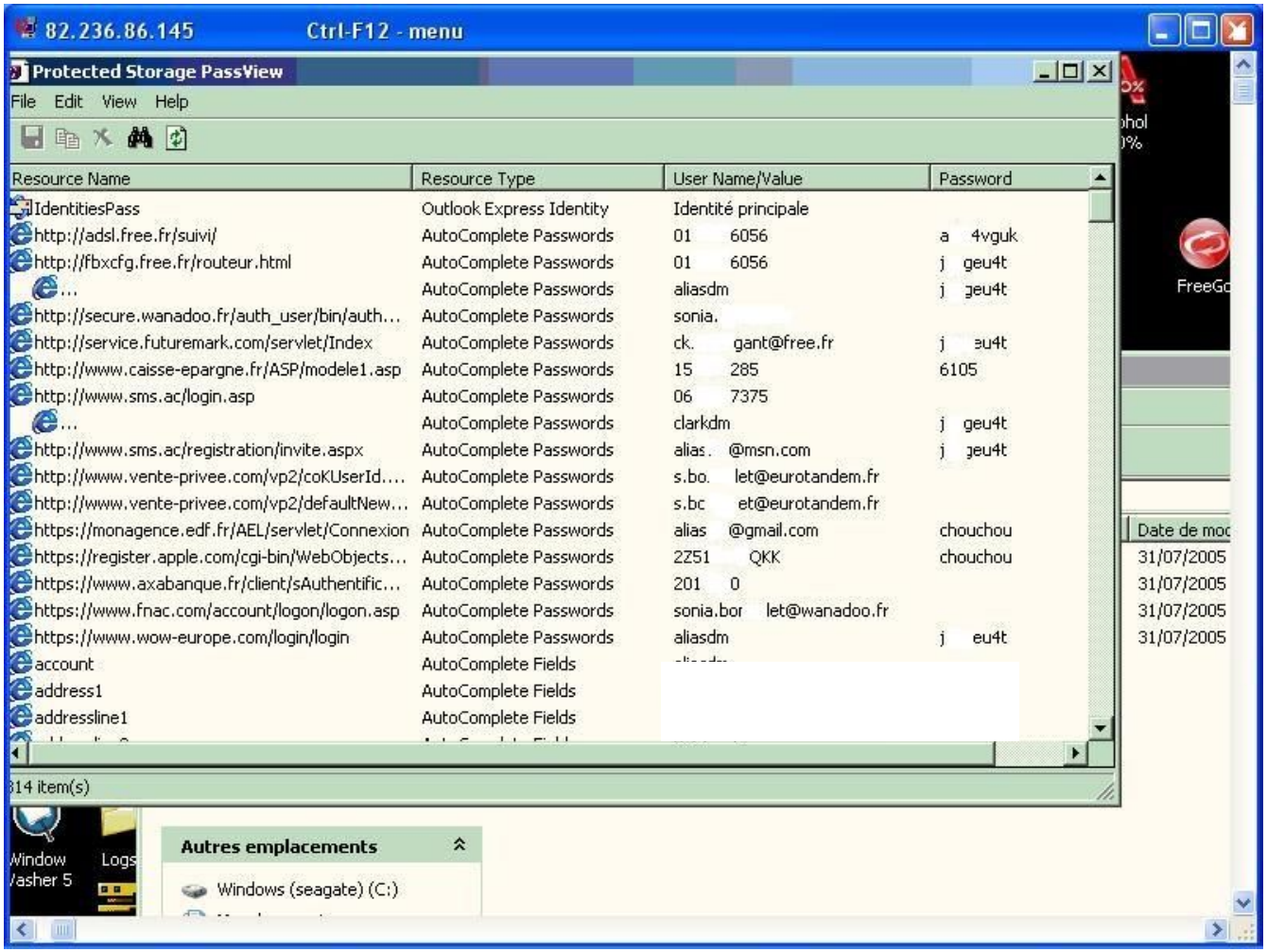
- ***Si la victime refuse son aide, à l'aide des mots de passe qu'il a obtenu sur son ordinateur, il modifie ses annonces de rencontres softs, en annonces à caractère pornographique en communiquant ses vrais coordonnés (propositions de relations sexuelles).***

- ***Les contrefaçons sont mises à disposition, via le réseau Internet, via différents protocoles : P2P (Emule, Kazaa, Morpheus, etc…), ainsi que via des serveurs FTP soient installés par les auteurs eux-mêmes, soient installés sur des serveurs piratés (Stro) de particuliers, de sociétés ou d'universités.)***

- ***Elle est notamment définie en autre, par l'Article L335-2 du Code de la Propriété Intellectuelle :***

- ***Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre reproduction, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit.***

Intrusion

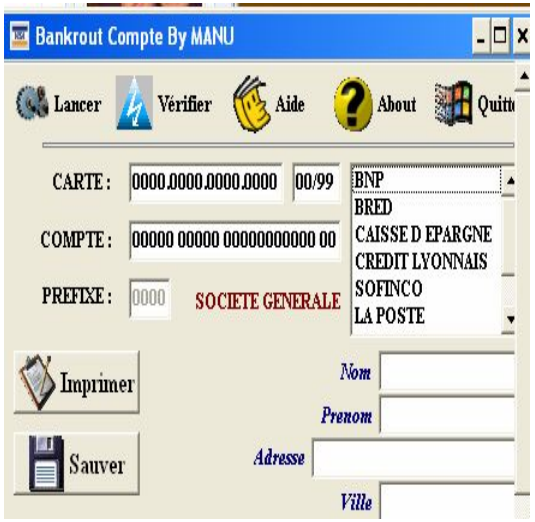

82.236.86.145
Ctrl-F12 - menu
Protected Storage PassView
File Edit View Help
Resource Name | Resource Type | User Name/Value | Password
IdentitiesPass | Outlook Express Identity | Identité principale
http://adsl.free.fr/suivi/ | AutoComplete Passwords | 01 6056 | a 4vguk
http://fbxcfg.free.fr/routeur.html | AutoComplete Passwords | 01 6056 | j geu4t
... | AutoComplete Passwords | aliasdm | j geu4t
http://secure.wanadoo.fr/auth_user/bin/auth... | AutoComplete Passwords | sonia.
http://service.futuremark.com/servlet/Index | AutoComplete Passwords | ck. gant@free.fr | j eu4t
http://www.caisse-epargne.fr/ASP/modele1.asp | AutoComplete Passwords | 15 285 | 6105
http://www.sms.ac/login.asp | AutoComplete Passwords | 06 7375
... | AutoComplete Passwords | clarkdm | j geu4t
http://www.sms.ac/registration/invite.aspx | AutoComplete Passwords | alias. @msn.com | j geu4t
http://www.vente-privee.com/vp2/coKUserId.... | AutoComplete Passwords | s.bo. let@eurotandem.fr
http://www.vente-privee.com/vp2/defaultNew... | AutoComplete Passwords | s.bc et@eurotandem.fr
https://monagence.edf.fr/AEL/servlet/Connexion | AutoComplete Passwords | alias @gmail.com | chouchou
https://register.apple.com/cgi-bin/WebObjects... | AutoComplete Passwords | 2Z51 QKK | chouchou
https://www.axabanque.fr/client/sAuthentific... | AutoComplete Passwords | 201 0
https://www.fnac.com/account/logon/logon.asp | AutoComplete Passwords | sonia.bor let@wanadoo.fr
https://www.wow-europe.com/login/login | AutoComplete Passwords | aliasdm | j eu4t
account | AutoComplete Fields
address1 | AutoComplete Fields
addressline1 | AutoComplete Fields
814 item(s)
Date de mod
31/07/2005
31/07/2005
31/07/2005
31/07/2005
Autres emplacements
Windows (seagate) (C:)

Escroquerie dite Nigérianne

Greetings From Kingsley
Hello Dear
I am Mr Kingsley Tarawally from Seirra leone but residing inIvory Coast in West Africa. It is my desire to contact you on honesty and sincerity to as me in transferring the sum of $ 18,000,000 inherited from my father late Mr. K.S Tarawally, I am motivated in contacting you and hope to gradually build trust, relationship and confidence in you as i get to know you better. So please i want to know if you will be of assistance but first I want to get to know you better. I am willing to offer you 20% of the total amount for your effort input after the successful transfer of this money and investment. Indicate your interest towards assisting me by sending your phone # and address so that i can communicate with you at any time. I will be waiting for your responseThanks Kingsley Tarawally.

Le Carding

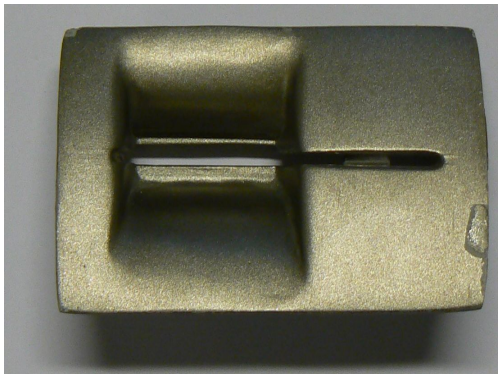

BANQUE POPULAIRE
CCF
BNP
Crédit Mutuel
LA POSTE
CIC
BY MANU
BANQUE SOFINCO
SOCIETE GENERALE
VISA
MasterCard
BANKROUT 1.1

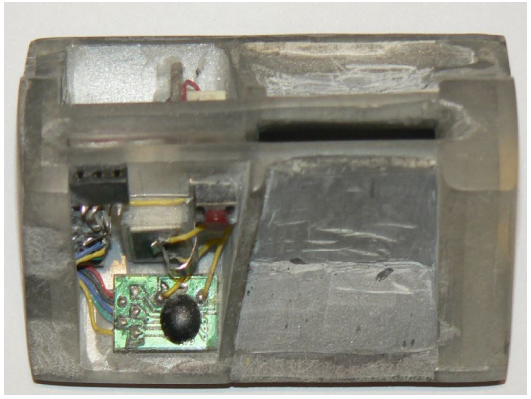

Bankrout Compte By MANU
Lancer
Vérifier
Aide
About
Quitte
CARTE :
0000.0000.0000.0000
00/99
COMPTE :
00000 00000 00000000000 00
PREFIXE :
0000
SOCIETE GENERALE
BNP
BRED
CAISSE D EPARGNE
CREDIT LYONNAIS
SOFINCO
LA POSTE
Imprimer
Sauver
Nom
Prenom
Adresse
Ville


Lhulu
A propos de ...
Retourner au menu principal
Informations :
Numero à 16 chiffres :
4974953817458106
Generer
Nom /Prénom :
MR NIKE LE GIE
Date d'émission :
Mois
Année
Date d'expiration :
Aide ???
No de serie (encarteur) :
4400000
BIN Ref :
F283
?
Code service
101
Code langue :
250
Exposant :
3
Code devise :
250
Chemin de java.exe :
C:\Program Files\JavaSof
Detecter JAVA
Generer un *.hex !!!

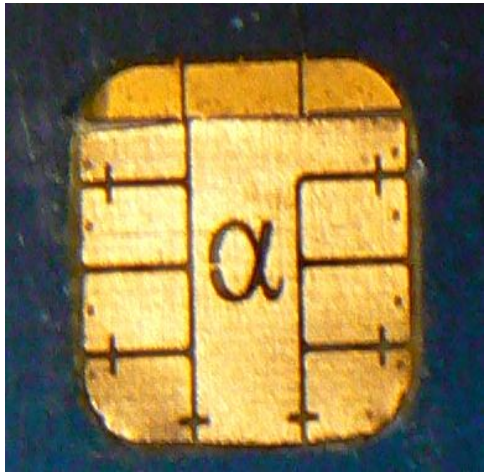

Bankrout Compte By MANU
Lancer
Vérifier
Aide
About
Quitter
CARTE :
4973.9709.4263.1473
11/99
COMPTE :
30003 97105 0426381157 14
PREFIXE :
0000
SOCIETE GENERALE
CAISSE D EPARGNE
CREDIT LYONNAIS
SOFINCO
LA POSTE
SOCIETE GENERALE
Perso
Imprimer
Sauver
Nom
BARD
Prenom
CLEMENT
Adresse
212 Bd Aristide Briand
Ville
Yerres 91330

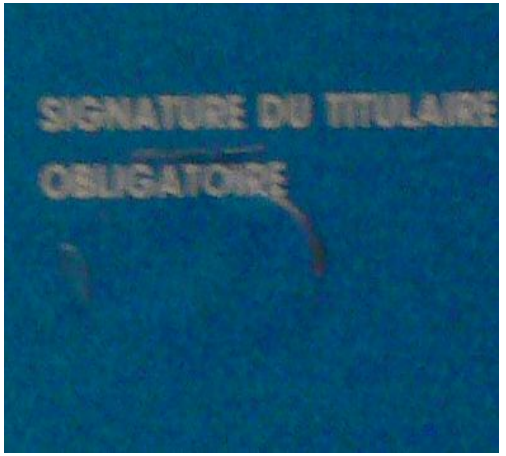
Exemple de Skimmer





Exemple de Fraude C.B





Retour d'Expérience : le Phishing

Depuis le mois de février 2008, la société CarBoat Média qui exploite le site Internet http://www.lacentrale.fr spécialisée dans les petites annonces de véhicules au profit de professionnels et de particuliers est victime de nombreux cas d'escroquerie par Phishing. A ce jour 4 méthodes différentes ont été employées

Les auteurs des faits ont mis dans un premier temps un processus destinés à recueillir les coordonnés de vendeurs de véhicules, pour ceux dont les coordonnés n'apparaissent pas sur le site en envoyant via un formulaire HTML mis a disposition via le site de la centrale, une demande de renseignement pour obtenir l'adresser mail du vendeur en réponse à son mail, ou soit en récupérant les coordonnés des vendeurs qui les mettent sur le site.

A partir des adresses mails collectées, via une fausse adresse mail laissant présumer que l'expéditeur est le site de la centrale, ils adressent plusieurs centaines de mails à des vendeurs pour les inviter à ressaisir leurs identifiants (login et mot de passe), et/ou leur coordonnées bancaires sur un site présentant des similitudes avec le site de la centrale (limages, et logo, animés, logo carte bancaire).

Par ce stratagème, le ou les auteurs des faits collectent des données nominatives qu'ils vont pouvoir ré utiliser de deux manières :

- en se connectant sur le site de la centrale en modifiant le compte pour empêcher que le vendeur du véhicule puisse se connecter sur son annonce, puis il baisse le prix du véhicule pour le rendre très attractif (de plusieurs milliers d'euros) et modifie les coordonnés du vendeur pour mettre les siennes pour être contacté directement par les acheteurs.

Cette opération lui permettra de solliciter une avance, ou le paiement avant la livraison du véhicule.

-En récupérant l'intégralité des données d'une carte bancaire, en l'espèce du numéro, de la date de validité, ainsi que du pictogramme de sécurité.

Ces renseignements permettront de passer des commandes sur Internet. L'ensemble des manipulations sont réalisées de manière très structurée :

- en créant des comptes mails de type Webmails,
- en créant un site avec nom de domaine sur les Iles Tobago & Tuvalu, British India Ocean Territory, (+ sous domaine Roumain).
- les sites sont hébergés pour moitié en Allemagne et aux Etats-Unis grâce à un système de « frame » sur des espaces gratuits.

-des « Proxy » sont utilisés pour anonymiser les IP lors de chacune des manipulations ou via des systèmes de transmission de mails anonymes situés à Hong Kong.

A ce jour des milliers de clients ont été impactés et 10 % de ceux-ci se sont connectés sur les faux sites et on saisis leurs identifiants. Plus d'une centaine d'annonces ont été modifiées par les auteurs. Les faux mails sont généralement adressés le vendredi ou le Week End.

Les adresses emails des potentiels victimes sont collectées, et réutiliser soit immédiatement, soit plus mois après.

Exemple de messages

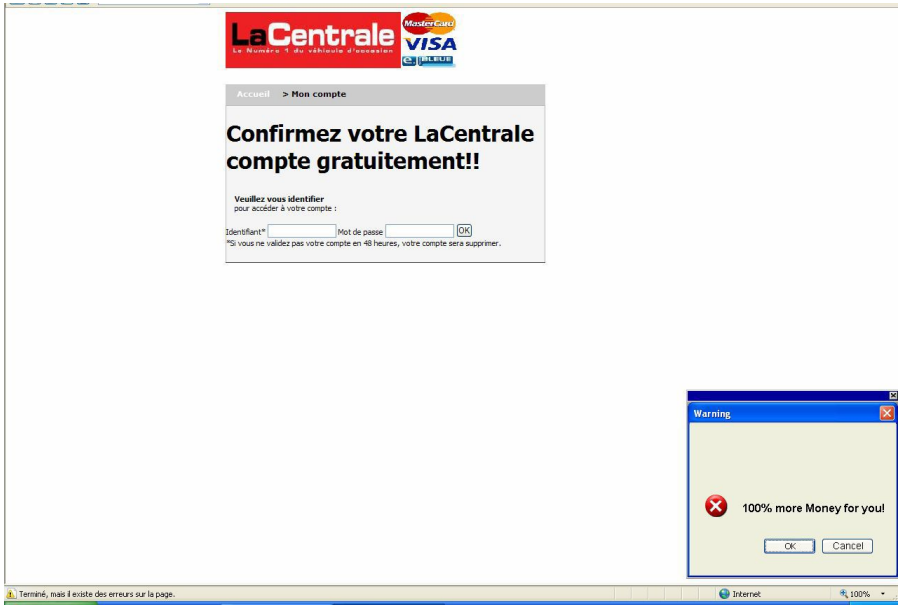
Les vendeurs reçoivent un mail émanant de l'adresse lacentrale@paris.com les invitant à se connecter sur le faux site :

« *Nous avons LaCentrale dans la base de données plus de 40 % les comptes inactifs. Pour garder votre compte actif s'il vous plaît, connectez vous ici (lien vers le faux site). Si vous n'avez pas accès à cette page http://www.lacentrale-confirmation.fr.tt identifian LaCentrale et votre mot de passe la maxime 48 heures votre compte sera supprimé* ».

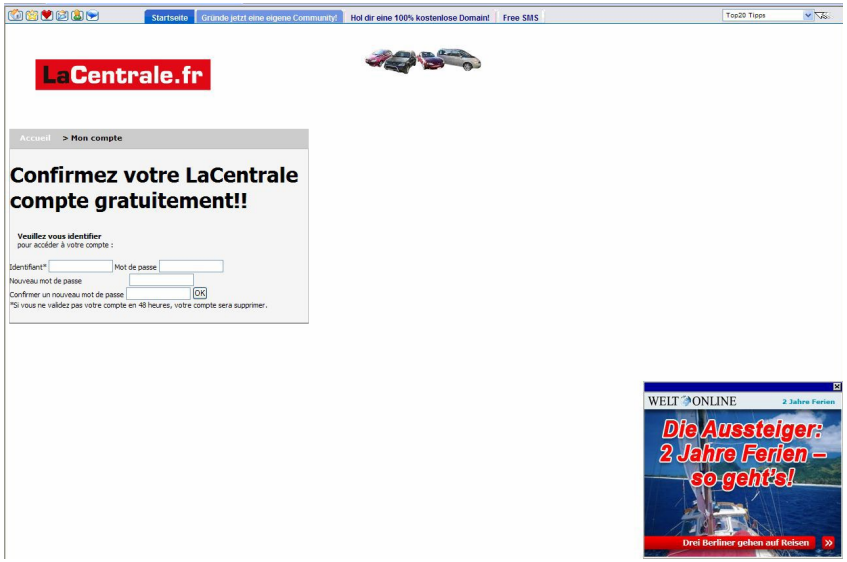
Les vendeurs reçoivent un mail émanant de l'adresse lacentrale@paris.com les invitant à se connecter sur le faux site :

« *Cher client La Centrale, Votre compte a été infiltré sans autorisation par une autre personne, Pour éviter de suspendre votre compte nous vous demandons de réintroduire vos dates. Cliker sur sur le suivant link pour la confirmation d'identité www.lacentrale-alerte.fr.tt Merci !* »

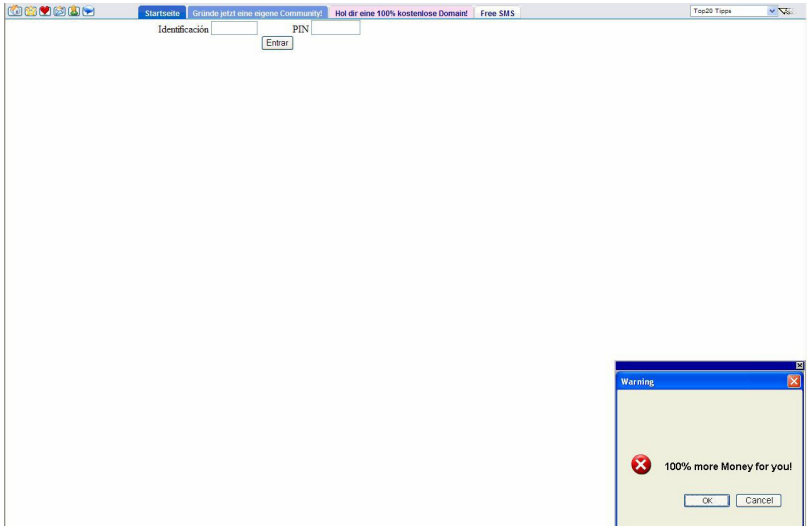
Faux site : **1° faits** (février 2008)



Faux site : 2° faits (avril 2008)



Faux site : **3° faits** (mai 2008)

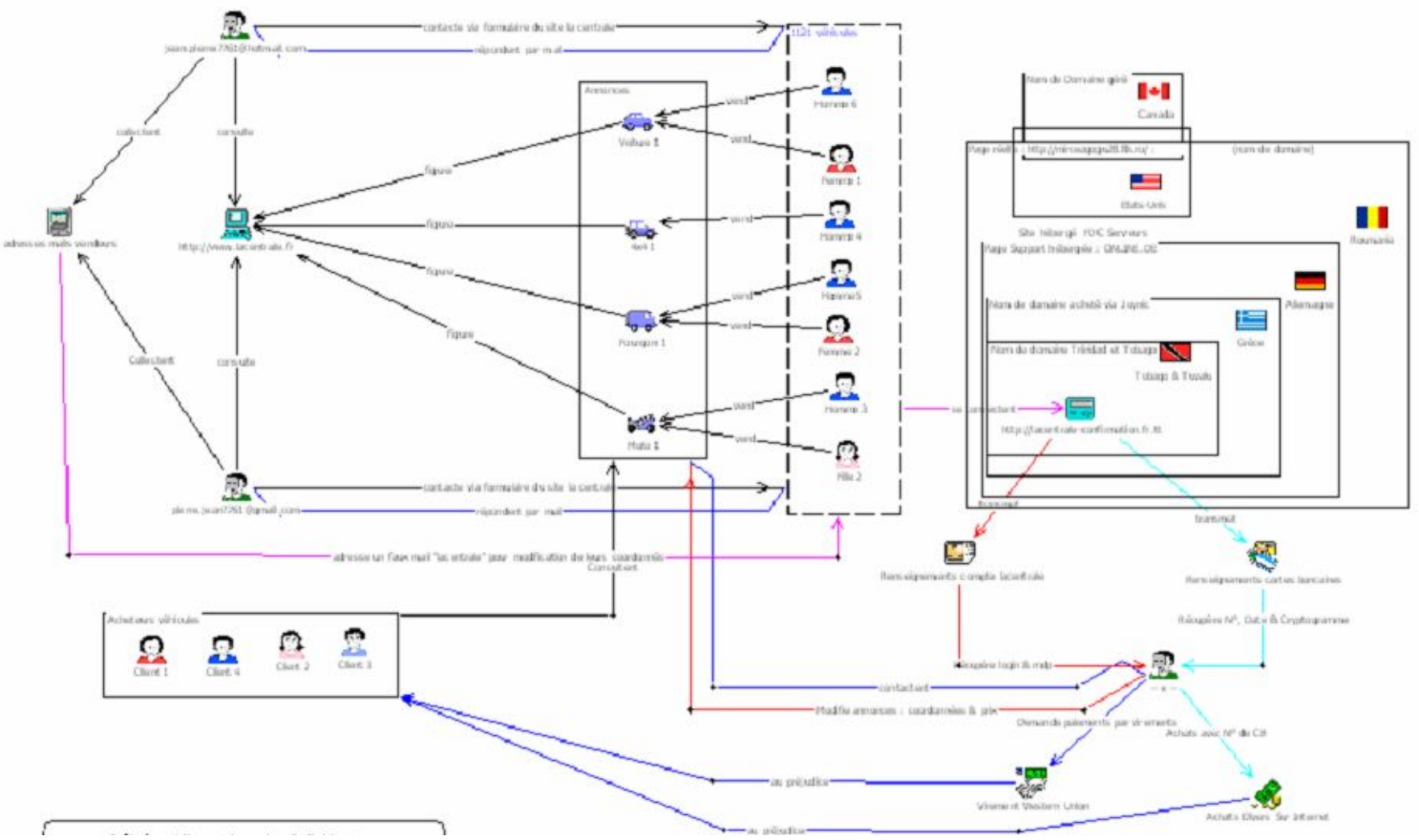


Faux sites : **4° faits** (11 juillet 2008)

2° formule :

Faux site : **5° faits** (22 juillet 2008)

Faux sites : **6° faits** (18 août 2008)


contacte via formulaire du site la centrale
répondent par mail
TEST véhicules
Annonces
Voiture 1
Homme 6
Homme 1
Homme 4
Moto 1
Homme 5
Fourgon 1
Femme 2
Homme 3
Moto 1
Fille 2
collectent
consulte
figure
vend
Nom de Domaine géré
Canada
Page visitée : http://mirrorpage28.fr.nr/ (nom de domaine)
Etats-Unis
Site hébergé : FDC Services
Roumanie
Page Support hébergée : GRATUIT
Nom de domaine acheté via 2 sync
Allemagne
Nom du domaine Trinidad et Tobago
Grèce
Tobago & Tuvalu
http://facenfate-confirmation.fr.fr
se connecte
transmet
Renseignements compte bancaire
Renseignements cartes bancaires
Réception N°, Date & Cryptogramme
Réception login & mdp
contactent
Modifie annonces : coordonnées & prix
Demande paiements par virements
Achats avec N° de CB
Virement Western Union
Achats Divers Sur Internet
adresse sur l'axe mail "la centrale" pour modification de leurs coordonnés
Consultent
Achateurs véhicules
Client 1
Client 4
Client 2
Client 3
au préalable
au préalable

Retour d'expériences en entreprise

De nombreux problèmes peuvent se poser lors d'une intervention réalisée par les services de Police dans les entreprises, voici quelques Exemples :

- constatations initiales effectuées par un huissier, qui ne correspondent pas aux besoins des enquêteurs, d'ou la nécessité de refaire celles-ci (perte de temps et d'argent).

- rétention d'informations par la société victime ou par une personne requise, par méconnaissance de la législation (droit de perquisition, réquisition ou de communication).

***- Procédures engagées devant différentes juridictions ou ouvertes sur de multiples infractions non caractérisées. Ce qui oblige les Enquêteurs* à vérifier chacun des faits (*perte de temps*).**

- Délais importants entre la date des faits et le dépôt plainte (problème d'obtention des données légales F.A.I), du fait :
d'une plainte avec constitution de partie civile auprès du Juge.
d'une plainte par un cabinet d'avocat.
(délais de la Justice, plutôt qu'une saisine directe d'un enquêteur).
Le coût est de 0€ pour ce type de saisine pour un résultat identique.

- Mise en place d'une communication dans les médias sans en parler aux enquêteurs ou au magistrat en charge du dossier.
(Violation du secret de l'instruction / destructions preuves).

- Réticence à déposer plainte pour l'image de marque de la société, dans le cas d'une intrusion (préjudice plusieurs centaines de milliers d'euros).
(Manque de confiance dans les services de Police / Gendarmerie).

- ***Les sociétés ne disposent pas toujours d'un service juridique ou de moyens financiers (avocats ou constats d'huissier). Le RSSI ou le DSI doit être en mesure d'identifier rapidement l'enquêteur (NTECH ou ESCI) qui pourra être en mesure de traiter votre problème. (prise de contact préalable)***

- ***La mise en place d'un protocole adapté en cas d'incident, qui ne prend pas seulement en compte le plan de continuité ou de reprise de l'activité, mais les aspects de la preuve indispensable pour les enquêteurs pour optimiser la résolution de l'affaire.***

- ***Formation « Forensics » collecte des données - copies supports dans le respect des Lois et réglements en vigueur.***

- ***Ce type d'action doit être documenté, comme ceux mis en place notamment au sein de RENATER et du CNRS, et remis aux enquêteurs lors du dépôt de plainte.***

Pour gérer ce type de problématique, nous avons essayé de mettre en place en amont des solutions adaptées aux problématiques actuelles :

- ***Création d'une structure au sein de la Gendarmerie pour traiter ce type de dossier, et développement de contacts au sein des sociétés avec les responsables de la sécurité.***

- ***Actions de formations au profit de futur R.S.S.I, notamment au Master 1 et 2 de l'Institut de des Risques Industriels, Assurantiels et Financiers à NIORT depuis 2 ans (Droit des NTICS : droit de perquisition, réquisition, Recueil de la Preuve, Montage Dossier).***

- ***Actions de sensibilisation au sein des entreprises sur les risques liés à la Cybercriminalité.*** (comme aujourd'hui)

Pour conclure

- ***La lutte contre la Cybercriminalité passe impérativement par une meilleure collaboration entre les services publics et les victimes.***

- ***Celles-ci doivent prendre conscience de l'existence d'enquêteur ou de services spécialisés (ex : maillage territorial de la Gendarmerie).***

- ***Pour faciliter ces actions, il est nécessaire de mettre en place une communication au niveau départemental ou régional entre ces acteurs, et non pas une communication axée essentiellement sur des services centraux.***

- ***Les victimes ne doivent pas penser qu'à leur « image », mais entamer des actions pour faire condamner les auteurs.***

- ***En cas d'incident, le recours à un protocole éprouvé s'avère indispensable : (principe de l'action = Réaction)***

- ***je fais quoi ? Comment ? avec qui ?***

Vincent Lemoine

EXPERTISES INFORMATIQUES

Membre de l'Association Francophone des Spécialistes de l'Investigation Numérique.

Master en Droit N.T.S.I & Doctorant

Master en S.S.I

spécialisé en Forensics

80 rue de Sèvres

92100 Boulogne Billancourt

☎ 01 46 05 58 61

🖷 01 48 25 85 22

vincent-lemoine@orange.fr

Des questions ?

Je suis également à la recherche d'entreprises pouvant prendre des stagiaires de l'U.T.T de Troyes et le l'I.R.IA.F de Niort (principalement en Master).

N'hésitez pas à me contacter. Merci de votre attention.