Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 26 nov. 2009

"Appréhender les menaces
quand les risques sont exacerbés en période de crise"

Puis, la crise avait fini par les atteindre directement. L'un perdit son emploi ...
un autre claquait des dents et touchait du bois (Marcel AYME, Maison basse, p. 169).

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 26 nov. 2009

Table ronde

sur les menaces externes amplifiées par la crise

Email : rene.eckhardt@wanadoo.fr
Web : www.euro-regio-club.com

Animée par René ECKHARDT

Président de l'EURO REGIO CLUB de Srasbourg et du Rhin Supérieur
Fondateur du Cercle des DirCom du grand Est
Chef d'escadron (RC) de la gendarmerie nationale

La sophistication des attaques et son évolution

Email : ch.ambrosini@gmail.com
Web : www.cybercrime.ch

par M Christian AMBROSINI

Monitoring Specialist KOBIK/SCOCI EJPD/ DFJP fedpol
Police judiciaire fédérale / Bundeskriminalpolizei
Service de coordination criminalité sur internet / Koordinationsstelle Internet Kriminalität

Evolution des attaques par "phishing"

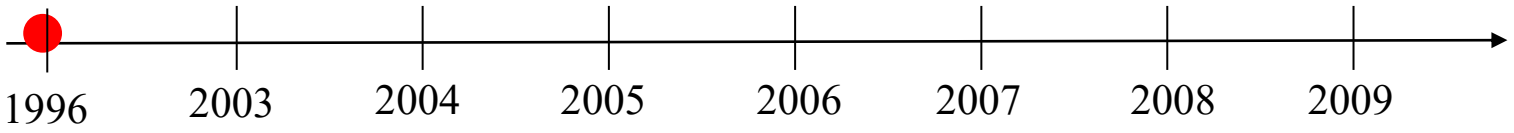
Evolution du "phishing"

Le "phishing", filoutage ou hameçonnage est une technique trompeuse visant à obtenir des renseignements personnels en abusant les détenteurs.

Premières tentatives de "phishing" décrites contre des groupes Usenet de America Online

"Phishing" dirigé contre des banques, principalement aux Etats Unis, où les banques emploient le contrôle d'accès fondé sur un login et un mot de passe.

Premier cas de "phishing" à l'encontre une banque suisse.

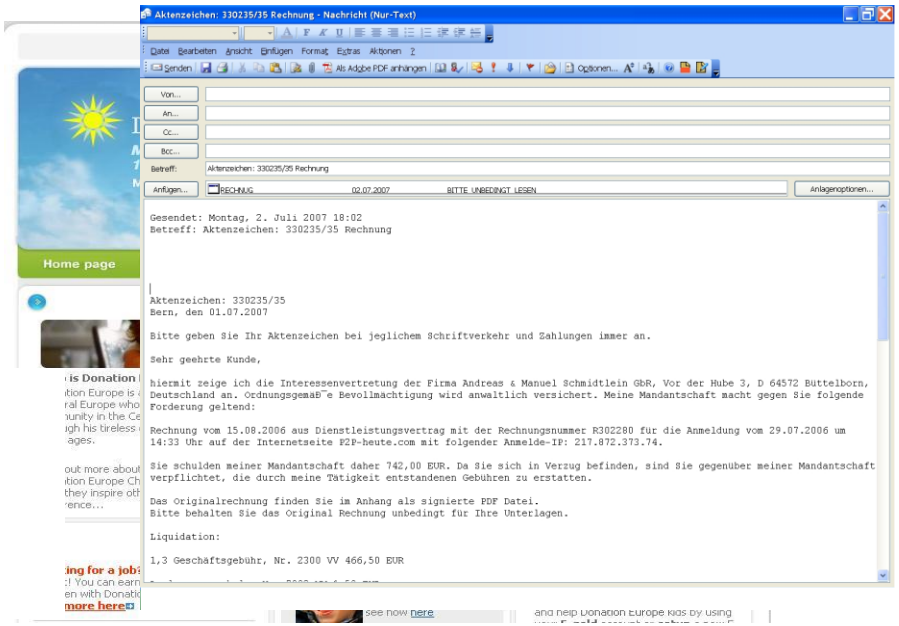


Evolution des modes d'attaques

- Avertissements notifiés

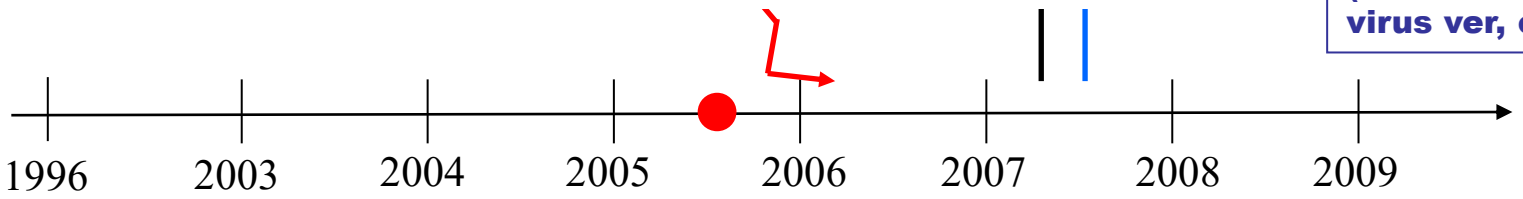
MELANI avertit le secteur financier suisse d'un changement de mode opératoire basé sur des attaques utilisant des logiciels malveillants.

MELANI avertit d'un renforcement du recrutement de "mules financières" et par conséquent d'une menace imminante.



D'abord, large diffusion de logiciels malveillants destinés aux services bancaires en ligne, puis l'homme s'implique dans les attaques de navigateur web.

***Un* code malveillant ou "malware" est un programme développé dans le but de nuire (ex. cheval de Troie, virus ver, etc.).**



Panorama des techniques d'attaques

- Evolution du panorama
  - Phishing → Malware
  - Attaques directes → Malware
  - Connaissances informatiques → Crimeware kit
  - Crimeware kit → Crimeware as a Service
  - Connaissances globales → Connaissances spécifiques
  - Anti-debugging, anti-reverse engineering, anti-virtualisation
  - Packers, cryptors, wrappers
  - Malware → compilation de malwares *(ex. Koobface)*

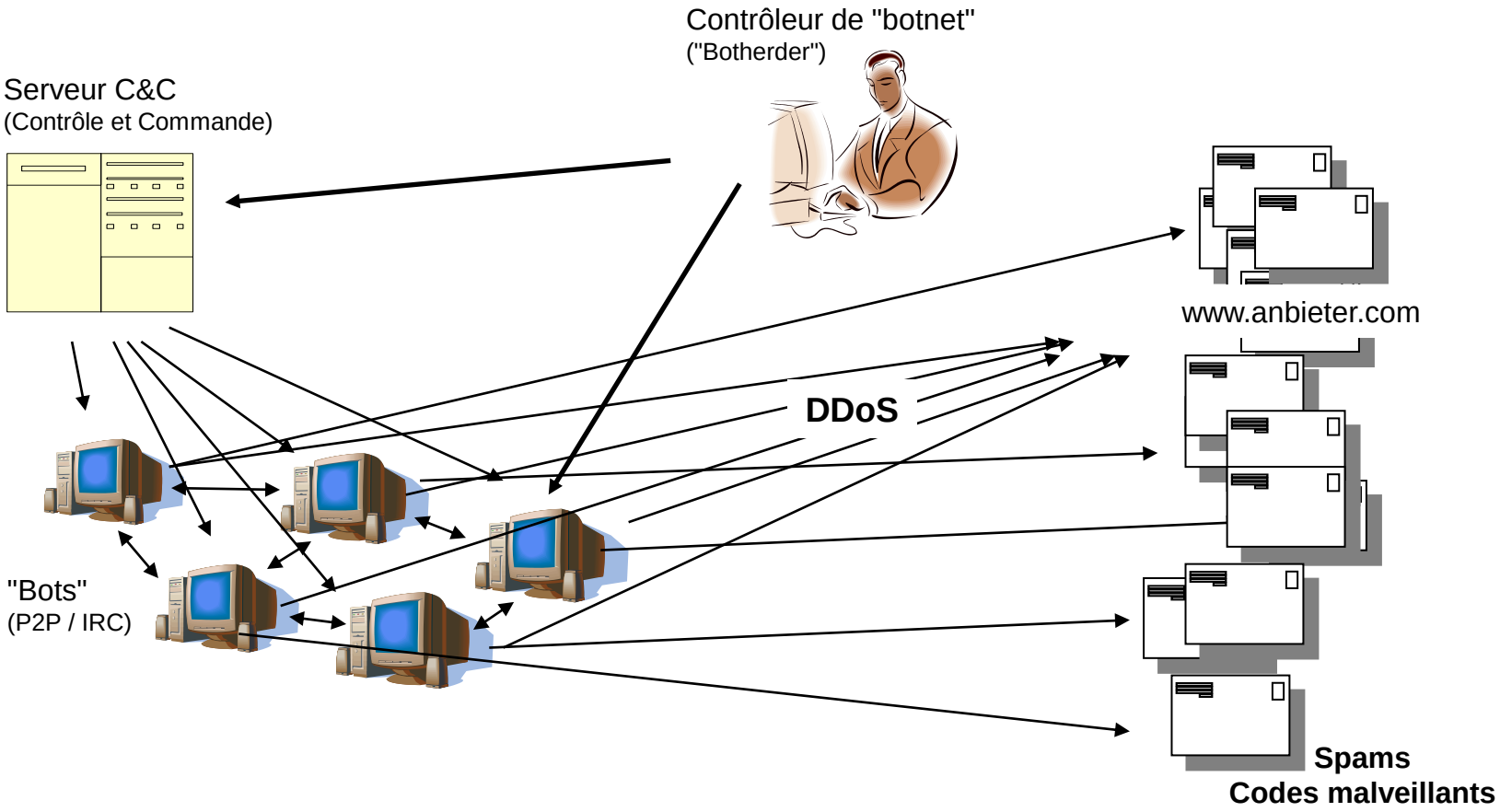
Les réseaux zombies ("botnets")

Email : Roger.morier@fedpol.admin.ch
Web : www.cybercrime.ch

par M Roger MORIER

Monitoring Specialist KOBIK/SCOCI EJPD/ DFJP fedpol
Police judiciaire fédérale / Bundeskriminalpolizei
Service de coordination criminalité sur internet / Koordinationsstelle Internet Kriminalität

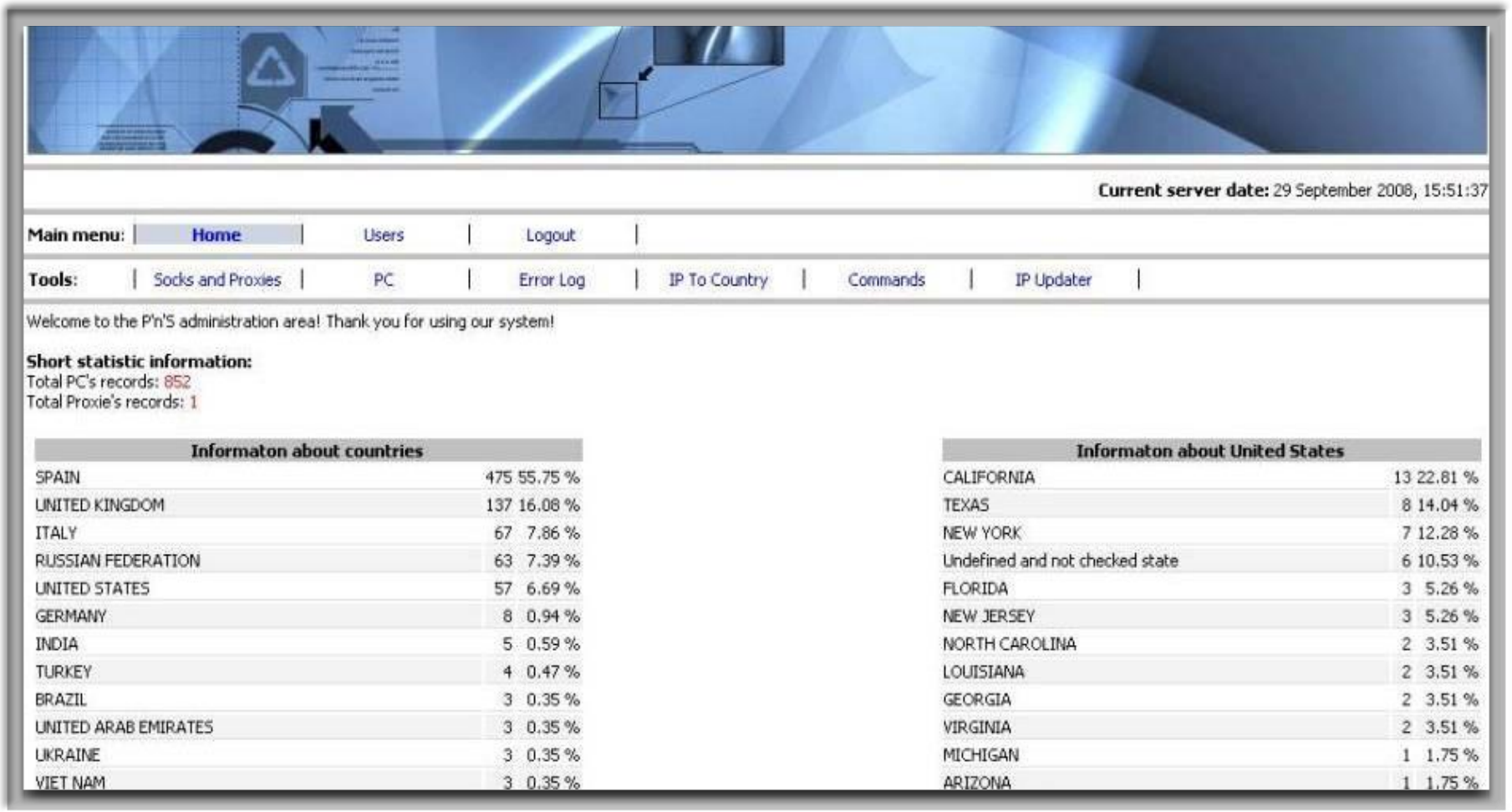
"Botnet" : "the swiss army knife"!



***Un "botnet", ou réseau de robots ("bots") malveillant, est composé de* machines compromises ("zombies"), en nombre pour assurer un camouflage actif et diriger des actions sur une cible déterminée.**

DDoS : Déni de service distribué
Spams : Pourriels

Prise de vue du côté criminel



Current server date: 29 September 2008, 15:51:37

Main menu: Home | Users | Logout

Tools: Socks and Proxies | PC | Error Log | IP To Country | Commands | IP Updater

Welcome to the P'n'S administration area! Thank you for using our system!

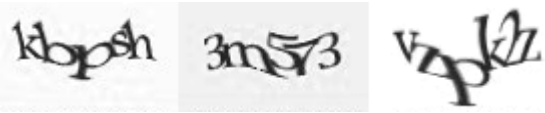
Short statistic information:
Total PC's records: 852
Total Proxie's records: 1

Informaton about countries		
SPAIN	475	55.75 %
UNITED KINGDOM	137	16.08 %
ITALY	67	7.86 %
RUSSIAN FEDERATION	63	7.39 %
UNITED STATES	57	6.69 %
GERMANY	8	0.94 %
INDIA	5	0.59 %
TURKEY	4	0.47 %
BRAZIL	3	0.35 %
UNITED ARAB EMIRATES	3	0.35 %
UKRAINE	3	0.35 %
VIET NAM	3	0.35 %

Informaton about United States		
CALIFORNIA	13	22.81 %
TEXAS	8	14.04 %
NEW YORK	7	12.28 %
Undefined and not checked state	6	10.53 %
FLORIDA	3	5.26 %
NEW JERSEY	3	5.26 %
NORTH CAROLINA	2	3.51 %
LOUISIANA	2	3.51 %
GEORGIA	2	3.51 %
VIRGINIA	2	3.51 %
MICHIGAN	1	1.75 %
ARIZONA	1	1.75 %

Utilisation des "botnets"

- Les "botnets" sont diversement utilisés :
  - Attaques en déni de service distribué *(DDoS)*
  - Spamming
  - Diffusion de codes malveillants
  - Serveurs proxies, reverse proxies et webserver *(nginx)*
  - Relais de trafic en "fast flux"
  - Fraude au clic
  - Craqueur de CAPTCHA



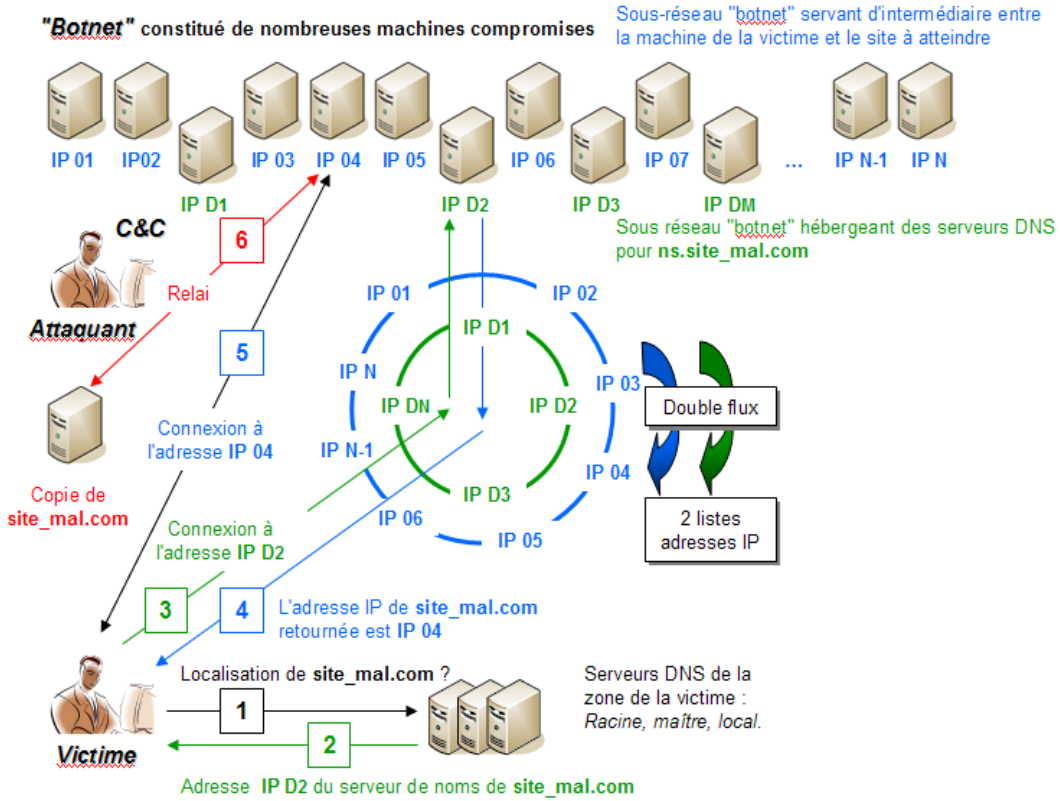
http://en.wikipedia.org/wiki/CAPTCHA

Proxy : Machine ou serveur servant de relai.

CAPTCHA : Pour *Completely Automated Public Turing test to Tell Computers and Humans Apart* ; test utilisé par un ordinateur pour différencier de manière automatisée un utilisateur humain d'un dispositif automatique.

Exemple : "fast flux" en double flux

- Les "botnets" - des relais et plus encore … :
  - "**simple flux**" : Domaine unique, adresses IP de validité < *10 mn* attribuées par roulement par le serveur de noms
  - "**double flux**" : Serveurs de noms disposant d'adresses IP variables



Plusieurs noms de domaine… *le top actuel !*

"Fast flux" désigne une technique de camouflage utilisant les "botnets" comme relais de trafic HTTP et pour simuler les serveurs de noms de domaine et enfin transmettre les adresses IP valides peu de temps.

Du spamming au déni de services

Email : presse@pr-simon.de

par Dr Dieter SIMON

Gérant SIMON Communication (Allemagne) et INTEREUROP (France)
Vice Président de l'Euro Régio Club

Die externen Gefahren

- Vom "Spam" bis zur stillen Eindringen
- Welche Mittel zur Abschirmung

Les phénomènes de filoutage ("phishing")

Email : dvoigt@beck-tiefdruckzylinder.com

par M Dominik VOIGT

Softwareaktualizierung Datenschutz Fa BECK Tiefdruckformen in KIPPENHEIM

Die externen Gefahren

- Welche externen Gefahren durch "Phishing"?
- Welche Mittel um diese Gefahr zu verhindern

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 26 nov. 2009

"Appréhender les menaces
quand les risques sont exacerbés en période de crise"

Puis, la crise avait fini par les atteindre directement. L'un perdit son emploi ...
un autre claquait des dents et touchait du bois (Marcel AYME, Maison basse, p. 169).

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 26 nov. 2009

Table ronde

sur les menaces internes à ne pas négliger

Email : rene.eckhardt@wanadoo.fr
Web : www.euro-regio-club.com

Animée par René ECKHARDT

Président de l'EURO REGIO CLUB de Srasbourg et du Rhin Supérieur
Fondateur du Cercle des DirCom du grand Est
Chef d'escadron (RC) de la gendarmerie nationale

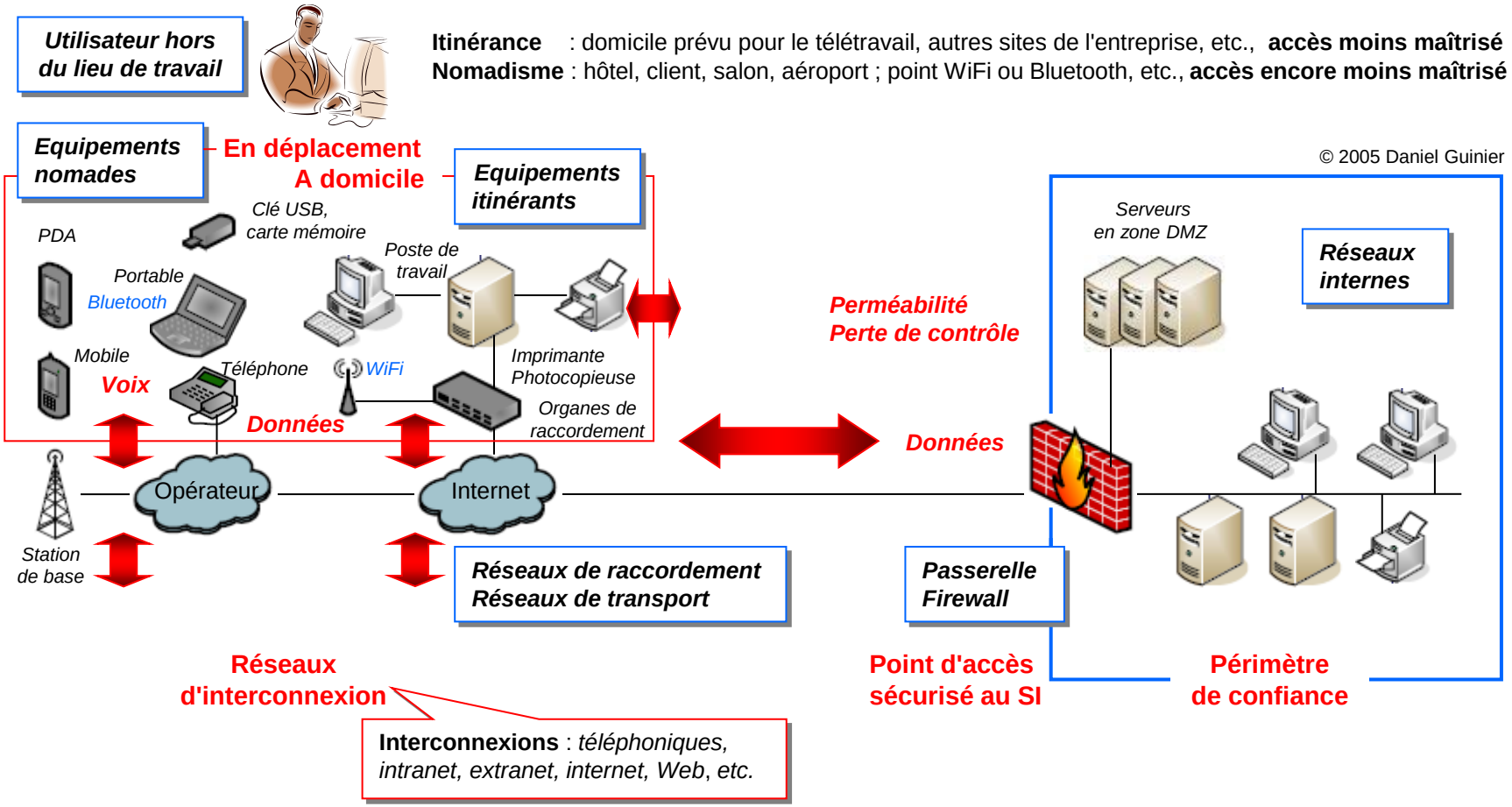
Les menaces liées au nomadisme et aux outils mobiles

Email : charles.gamet@gendarmerie.interieur.gouv.fr
Web : www.defense.gouv.fr/gendarmerie

par le Lieutenant-colonel Charles GAMET

Chef d'Etat Major adjoint Opérations Emploi
Région de Gendarmerie d'Alsace

Schéma global type



Les informations critiques accessibles hors du lieu de travail usuel posent un problème de sécurité du fait de facteurs plus ou moins bien maîtrisés, voire pas du tout.

Préconisations essentielles

- Concernant les postes maîtrisés
  - Protection : physique et sauvegarde régulière des données
  - Protection du contenu : antivirus et firewall, chiffrement
  - Contrôle d'accès : au démarrage et après une période d'inactivité
  - Désactivation de la connexion en cours, lors d'une connexion au réseau d'entreprise
- Concernant les postes non maîtrisés
  - Respect strict des règles de bon usage
  - Flux web HTTPS exclusivement
  - Recours à l'authentification forte *(ex. carte à puce)*
  - Echanges en réseau virtuel privé (VPN)
  - Ne pas y sauvegarder de données sensibles en clair

Pour les WAP : Authentification par un secret non stocké, connexion sécurisée. Pour les *PDA : verrouillage à l'arrêt, chiffrement des données, applications sur client léger, synchronisation avec authentification forte,* antivirus, *etc.*

La divulgation d'informations sensibles et personnelles

Retour d'expérience

Email : esand@fmlogistic.fr
Web : www.clusir-est.org

CLUSIR : Club de la Sécurité de l'Information Régional

par M Eric SAND

Directeur de l'Organisation des Systèmes d'Information FM Logistic
CLUSIR-Est

Historique (1)

- 17/09/2007
  - Envoi d'un courrier recommandé avec A/R à un collaborateur pour lui signifier son licenciement avec un préavis qui sera effectué à domicile
- 18/09/2007
  - Le collaborateur n'a pas "encore" reçu le courrier et se rend au travail
  - Réception du courrier par la mère du collaborateur qui le prévient par téléphone.
  - A 12h00 il quitte son travail en n'ayant pas terminé sa journée
- 19/09/2007
  - Décision de l'entreprise de réattribuer son poste de travail. A cette occasion on se rend compte qu'un certain nombre de fichiers de travail et de messages ont été effacés

Historique (2)

- 20/09/2007
  - Appel du service juridique RH au RSSI, les préconisations
- 01/10/2007
  - Intervention de l'huissier et d'un expert judiciaire pour procéder aux constats
- 02/10/2007
  - Remise à l'huissier d'une copie de la messagerie du collaborateur

L'expert a pu orienter l'huissier dans un domaine qui n'est pas directement celui de sa compétence.

Procès verbal d'huissier – page 1

COUT	
PV	250,00
Article 18	6,22
Montant HT	256,22
T.V.A à 19.6%	50,22
Trésor Public	9,15
Montant TTC	315,59

Je soussigné,

Michel DELACOUR, Huissier de Justice associé près le Tribunal de Grande Instance de SENLIS, à la résidence de CREPY EN VALOIS y domicilié, 16 rue Jeanne d'Arc,

Me suis rendu ce jour à 14h 30, sur le site de FM LOGISTIC, rue du Bois de Tillet à CREPY EN VALOIS, où étant, j'ai constaté ce qui suit :

CONSTATATIONS :

Je constate la présence de Madame LEPERCQ Laure, Directrice des Ressources Humaines, et Monsieur BLANCHARD Aurélien.

Monsieur BLANCHARD remet à Madame LEPERCQ une clé USB-32.

A 14h 50, Monsieur BLANCHARD quitte le site FM LOGISTIC.

Après visionnage, en présence de Madame LEPERCQ, nous retrouvons :

Tableau des reprises - (contenu conforme)
Guides processus - documents - procédure travail
Guide bonne pratique
Tableau statistique
Prise rendez-vous
Tableau reprise
Bilan transport - performance et indicateur sur dossier HENKEL, de janvier 2007 à juillet 2007.

Page 1

Historique (3)

- 04/10/2007
  - Constat transmis par l'huissier
- 09/10/2007
  - Envoi d'un courrier recommandé avec A/R
- …/10/2007
  - Restitution de la clé USB
  - Confirmation du collaborateur du fait qu'il ait pris des données appartenant à l'entreprise et tout cela devant huissier

Bilan

- En cas de doute sur l'intégrité d'un collaborateur susceptible de subtiliser des données à l'entreprise, il est indispensable :
  - D'isoler son PC et de ne plus y toucher jusqu'à la venue de l'expert
  - Ou, en mode dégradé, de procéder à une copie des états informatiques en présence d'un huissier certifiant les opérations, qui consigne dans la foulée la copie

- Ce qui a été déclencheur pour la restitution des données :
  - Le contact tél (par le DRH) lui précisant que nous avions entamé une action en justice avec notamment dépôt de plainte....
  - L'envoi d'un courrier AR, lui notifiant notamment : *"nous vous rappelons que nous vous interdisons formellement d'utiliser les données relatives à l'entreprise, sachant que dans le cas contraire, nous serions amenés à demander réparation et à poursuivre notre action entamée en justice"*

Les menaces liées à l'utilisation illicite des TIC

Email : esachner@beck-tiefdruckzylinder.com

TIC : Technologies de l'Information et de la communication

par Mme Eva SACHNER

Dipl. Kauffrau
Qualitätsmanagement und Marketing
Fa BECK Tiefdruckformen in KIPPENHEIM

Die internen Gefahren

- Welche Gefahren durch illegale Benutzung der Kommunikation Technologie
- USB Blockierung Wettbewerb in unmittelbarer Umgebung Usw

La fraude financière et les TIC

Etat des lieux, découverte et réponse

Email : karine.beguin@gendarmerie.interieur.gouv.fr
Web : www.defense.gouv.fr/gendarmerie

TIC : Technologies de l'Information et de la communication

par le Capitaine Karine BEGUIN

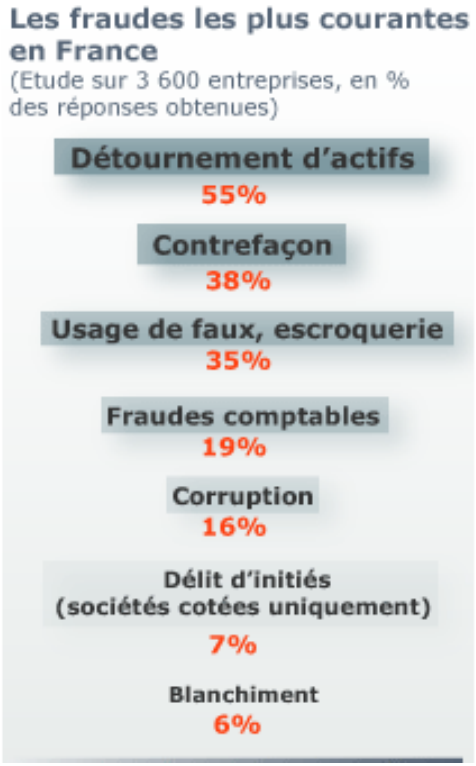
Chef de département CTGN / STRJD
Div. Cybercriminalité / Dép. Surveillance Internet, Gendarmerie nationale

La fraude en entreprise

- Introduction sur la fraude et l'utilisation des TIC

La fraude en entreprise constitue un enjeu et une menace croissante pour les entreprises particulièrement en raison des évolutions technologiques et de la dépendance croissante vis-à-vis des systèmes d'information.

- La fraude en interne
  - Causes
  - Conséquences
  - Nature des fraudes et indicateurs



Etude menée en 2007 sur la fraude dans les entreprises en France et dans le monde.

Découverte de la fraude et réponses

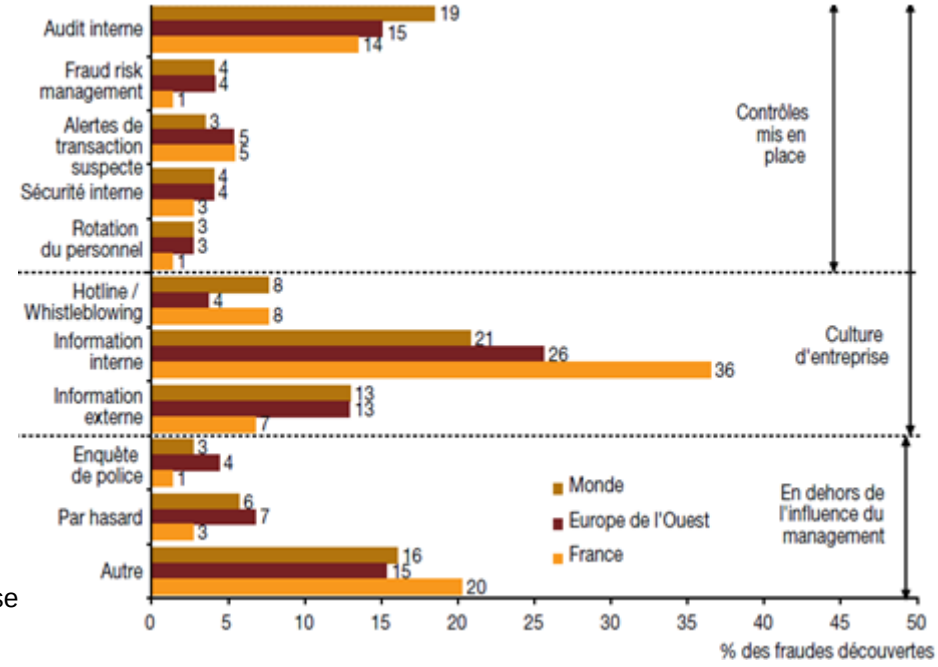
Constats

80% de la fraude serait donc interne mais les entreprises ne souhaitent pas communiquer sur le sujet. Cela s'explique peut être par la superstition, la culpabilité ou tout bonnement une absence totale de maitrise en la matière

La découverte de la fraude

- Détection des fraudes
- Prévention
- Réponse juridique

Méthodes de détection des fraudes



Etude menée en 2007 sur la fraude dans les entreprise en France et dans le monde.

La fraude financière via la comptabilité

Guide pratique du chef d'entreprise face aux risques numériques,
Version du 24/03/09, extrait, p. 17.

> Fiche 2 Comportements à risque

La fraude financière via la comptabilité

- *Le chef-comptable, en poste depuis de nombreuses années, vient d'être mis en arrêt longue durée suite à un accident automobile.*
- *Un intérimaire est embauché d'autant plus rapidement que le bilan doit être clôturé prochainement.*
- *A l'occasion de rapprochements bancaires et stocks, ce remplaçant détecte une différence entre les factures payées à un fournisseur et les livraisons effectives de matériaux.*
- *En collusion avec un employé du fournisseur, le chef-comptable a détourné plusieurs centaines de milliers d'euros en moins de deux ans. Il apparaissait comme consciencieux, extrêmement zélé et d'ailleurs, ne prenait quasiment pas de congés.*
- *Une procédure judiciaire a été lancée mais la récupération des actifs détournés s'avère délicate. Ces derniers ayant été consommés ou investis dans des biens immobiliers dont la liquidation va prendre des mois.*

Impacts judiciaires

Le licenciement du salarié ne peut se faire tant que son contrat se trouve suspendu sauf faute grave ou lourde qui ne pourra être démontrée que par une expertise comptable ou une enquête pénale.
Elles devront déterminer s'il a bénéficié de complicité.
Une procédure d'expertise devra être lancée afin de déterminer le préjudice exact subi par l'entreprise. Des conséquences fiscales sont également envisageables du fait de l'absence de fiabilité des documents comptables.

Définition :
La fraude financière est un acte illicite délibéré, réalisé par des moyens plus ou moins subtils, avec la volonté de tromper dans le but de s'approprier un avantage. Elle peut prendre diverses formes qui nécessitent ou non des complicités, et conduit à un préjudice pour la victime.

Impacts managériaux et humains

Détection délicate a priori car tout le monde se connaissait dans l'entreprise et la suspicion d'une malversation semblait inimaginable. Dès la présomption fondée, le chef d'entreprise doit agir rapidement et discrètement en supposant l'existence de collusions internes.

Préconisations

Mettre en place des contrôles informatiques et des procédures : double ordonnancement, séparation des circuits paiements et achats, limitation de seuils, audit et inventaires apériodiques.

Impacts financiers

Effets multiples : perte des actifs détournés et difficultés à venir pour récupérer les fonds détournés d'autant plus que la PME ne s'était pas assurée contre les fraudes financières.

Impacts sur l'image

Impact sur le sérieux de l'entreprise (rigueur dans les contrôles) et crainte de difficultés financières futures qui pourraient remettre en cause des contrats clients, voire d'autres fournisseurs...

LES POINTS CLES A RETENIR

Les mécanismes de détournements sont le plus souvent très simples à comprendre et parfois stupides de la part du commettant car la détection n'est qu'une affaire de temps (cf fraude dite « en cavalerie* »).
Etudier des scénarios techniquement possibles (c'est à dire sans présumer de la bonne foi des salariés) et mettre en place des indicateurs qui permettront la détection des situations atypiques.

(*) : La fraude financière dite «en cavalerie» peut prendre diverses formes. L'une consiste à créditer artificiellement un compte par des chèques croisés de montants croissants pour maintenir la confiance, ce qui nécessite des complicités successives, sinon de complaisances.

AVIS D'EXPERT :

La traçabilité des activités et des interventions du personnel joue un rôle primordial pour la prévention des fraudes. En effet, les fraudes d'ordre comptable par exemple peuvent entraîner des conséquences désastreuses pour une entreprise tant au niveau financier que pour son image. Pour se prémunir d'éventuelles tentatives de détournement de fonds au travers de manipulations comptables, un traitement électronique de l'ensemble des transactions ainsi que leur archivage est indispensable.

La sécurité des systèmes d'information

Responsabilités associées

Email : cutajar.chantal@wanadoo.fr
Web : www.em-strasbourg.eu/

par Mme Chantal CUTAJAR

Dr. en droit privé et sciences criminelles, Professeur affilié - EM, Université de Strasbourg
Resp. MASTER : Prévention des fraudes et du blanchiment ; Lutte contre la criminalité organisée économique et financière à l'échelle européenne
Directeur du Grasco (Groupe de recherche sur la criminalité organisée)

Les sanctions pénales…

Peu d'effectivité des sanctions

Peu de plaintes

Peines prononcées légères

…En cas d'atteinte au traitement automatisé de données.

Cas jurisprudentiel

- TGI de Paris, 12ème ch, 19 mai 2006

  Ministère public / Clément P., Elypsal, Thomas P.

Entrave au fonctionnement d'un système de traitement automatisé de données.

Etendue de la responsabilité

- CC, 2ème ch. civ., 13 mai 2003, pourvoi n° 01-21423
- CA de Bordeaux, 2ème ch., 10 mars 1993

Conclusion : Seul le ***"bon professionnel"*** peut voir sa responsabilité exonérée

Question : Qu'est-ce qu'un ***"bon professionnel"***

Le "bon professionnel" ?

- 1° - **Nomme** une personne et son suppléant en charge de la responsabilité de la sécurité du système d'information *(le RSSI)*
- 2° - **Forme** son personnel
- 3° - **Rédige** un code de bonne conduite

A défaut…

…son assurance risque de ne pas couvrir les conséquences pécuniaires de sa responsabilité !