DATAPROTECT

La menace de la cybercriminalité

Ali EL AZZOUZI, PCI QSA, Lead Auditor ISO 27001, CISA, ITIL

Président du chapitre marocain de l'AILCC

27 Juillet 2010

Agenda

- Démystification de la cybercriminalité
- Les multiples visages de la cybercriminalité
- L'écosystème de la cybercriminalité
- Les ripostes juridiques
- Vers la confiance numérique
- Conclusion
- Questions

1. DEMYSTIFICATION DE LA CYBERCRIMINALITE

1. Démystification de la cybercriminalité

La cybercriminalité est une activité en pleine croissance

- **Quelques caractéristiques**
  - L'arrivé du Web 2.0 (réseaux sociaux sont devenus les vecteurs privilégiés de la propagation des programmes malveillants)
  - L'augmentation des serveurs clandestins (fournisseurs bulletproof)
  - Paradis cybercriminel
  - La marasme économique actuel favorise le basculement vers les activités déviantes sur le cyberespace (1 poste informatique pour 10 ingénieurs en Russie par exemple)
  - Cybercriminel de dimanche

1. Démystification de la cybercriminalité

La cybercriminalité est une activité extrêmement rentable

- **Quelques caractéristiques**
  - 1 000 Milliards de dollars selon McAfee en 2008
  - Janvier 2007 – Des pirates russes, avec l'aide d'intermédiaires suédois, auraient détourné 800 000 euros de la banque suédoise Nordea.
  - Février 2007 – La police brésilienne arrête 41 pirates pour avoir utilisé un cheval de Troie pour voler les accès à des comptes bancaires et détourner 4,74 millions de dollars.
  - Avril 2007 – Une escroquerie a coûté, en 6 ans, 2 milliards de $ à l'Equity Funding Insurance : une vingtaine d'ingénieurs et de cadres avaient introduit dans le SI de la firme 64 000 clients fictifs
  - 2007, c'est aussi des dossiers d'espionnage par des employés, comme les vols de secrets de fabrique chez DuPont (condamnation à 18 mois de prison et une amende contre l'ancien chercheur reconnu coupable) ou chez Duracell (copie et téléchargement de documents sur les piles AA)

1. Démystification de la cybercriminalité

La cybercriminalité est une activité facile

- **Quelques caractéristiques**
  - Activité facile
    - La compétence n'est pas un pré-requis pour lancer les opérations cybercriminelles (vulgarisation des modes opératoires sur Internet)
    - Location des réseaux Botnets
    - Blanchiment d'argent via les canaux de jeux de paris en ligne et les sites de l'enchère en ligne
    - Recours aux « mules »

1. Démystification de la cybercriminalité

La cybercriminalité est une activité à faible risque

- **Quelques caractéristiques**
  - Activité à faible risque
    - L'internet est parfaitement adapté à l'activité frauduleuse
    - Anonymat
    - Peu de barrières à l'entrée
    - Difficulté d'application de la loi à des juridictions multiples
    - Emergence de paradis cybercriminels
    - Mode d'hébergement en Bulletproof

1. Démystification de la cybercriminalité

La cybercriminalité est une activité organisée

- **Quelques caractéristiques**
  - Une étude conjointe entre le CERT et le FBI démontre que dans **81% des incidents recensés** dans les entreprises, les attaquants avaient planifié leur action à l'avance
  - Travail d'équipe qui exige une spécialisation à outrance
  - Par exemple les chevaux de troie sont conçus par des développeurs de logiciels, qui en général n'exploitent plus par eux-mêmes leurs créations.
  - Ces développeurs vendent leurs créations comme de véritables produits, packagés avec une documentation utilisateur dans la langue de leurs clients. Certains groupes proposent même un support client 24/24 et offrent même une garantie de non détection du malware par les anti-virus

2. LES MULTIPLES VISAGES DE LA CYBERCRIMINALITE

2. Les multiples visages de la cybercriminalité

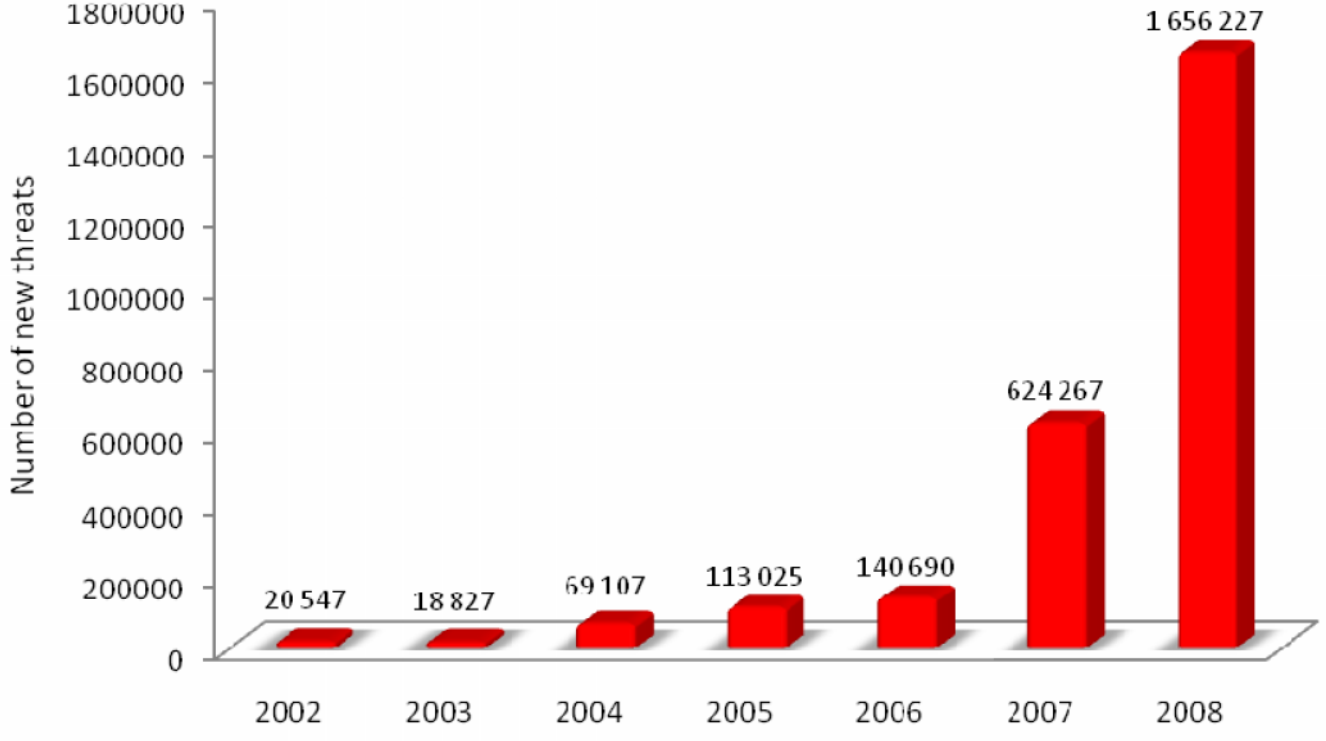
L'ordinateur comme moyen ou cible d'attaques cybercriminelles

- **L'atteinte à la confidentialité / l'attaque virale**
  - La plupart des virus ou de codes malveillants sont destinés à la récupération des données confidentielles (Numéro de cartes de crédit, mots de passes, email, données personnelles, etc…
  - Selon Symantec, **24% des demandes des « clients** » des pirates porteraient en effet sur des informations détaillées relatives à des **cartes de crédit**, et **18% sur des informations relatives à des comptes bancaires.**
  - Le nombre de virus a progressé **de 165% entre 2007 et 2008**. Plus de 1,6 million de nouveaux programmes malveillants ont été détectés au cours de la seule année 2008. Depuis sa création, Symantec **a recensé 2,6 millions de virus**. Ceux apparus en 2008 représentent donc **60% de l'ensemble de ces codes malveillants**

2. Les multiples visages de la cybercriminalité

L'ordinateur comme moyen ou cible d'attaques cybercriminelles

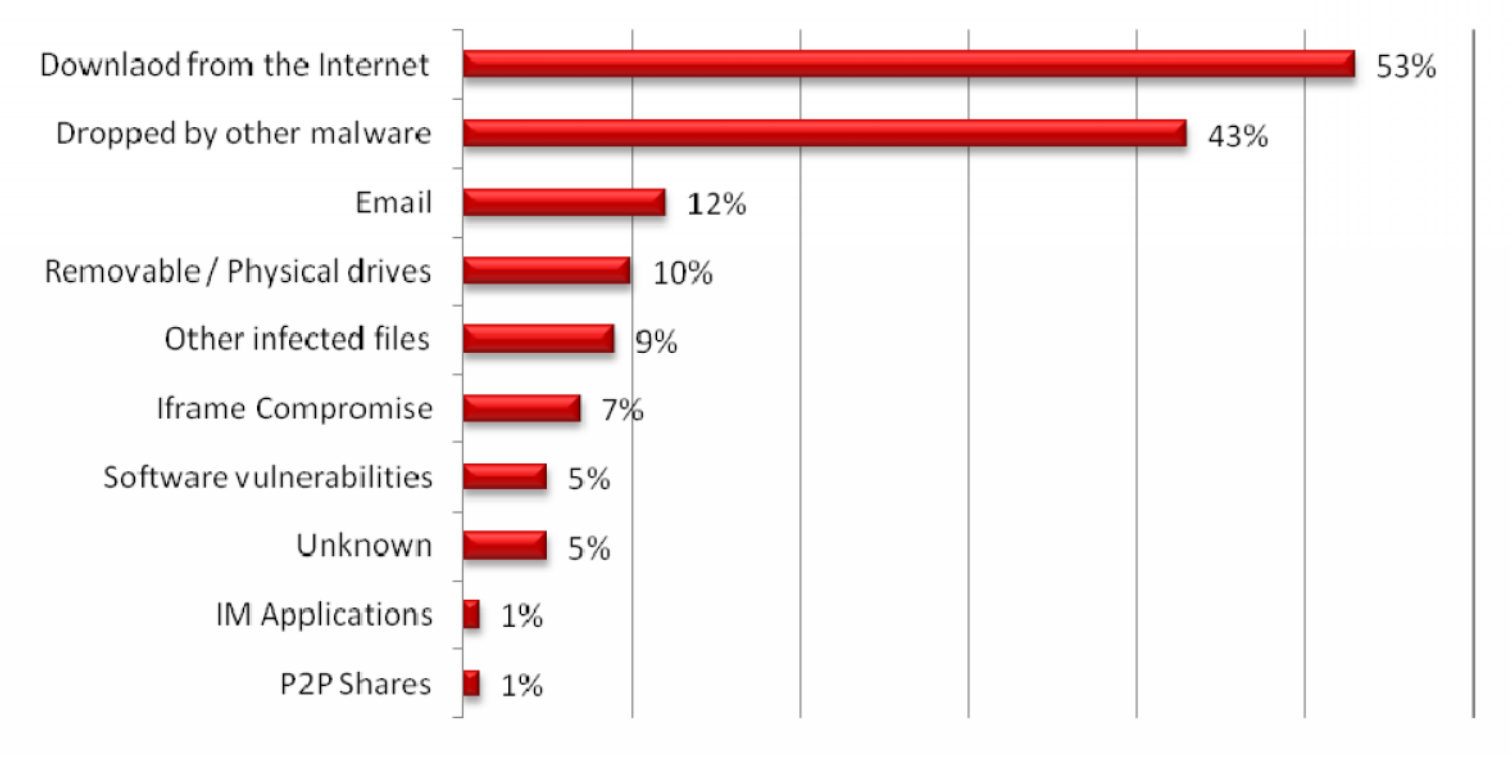
- L'atteinte à la confidentialité / l'attaque virale



2. Les multiples visages de la cybercriminalité

L'ordinateur comme moyen ou cible d'attaques cybercriminelles

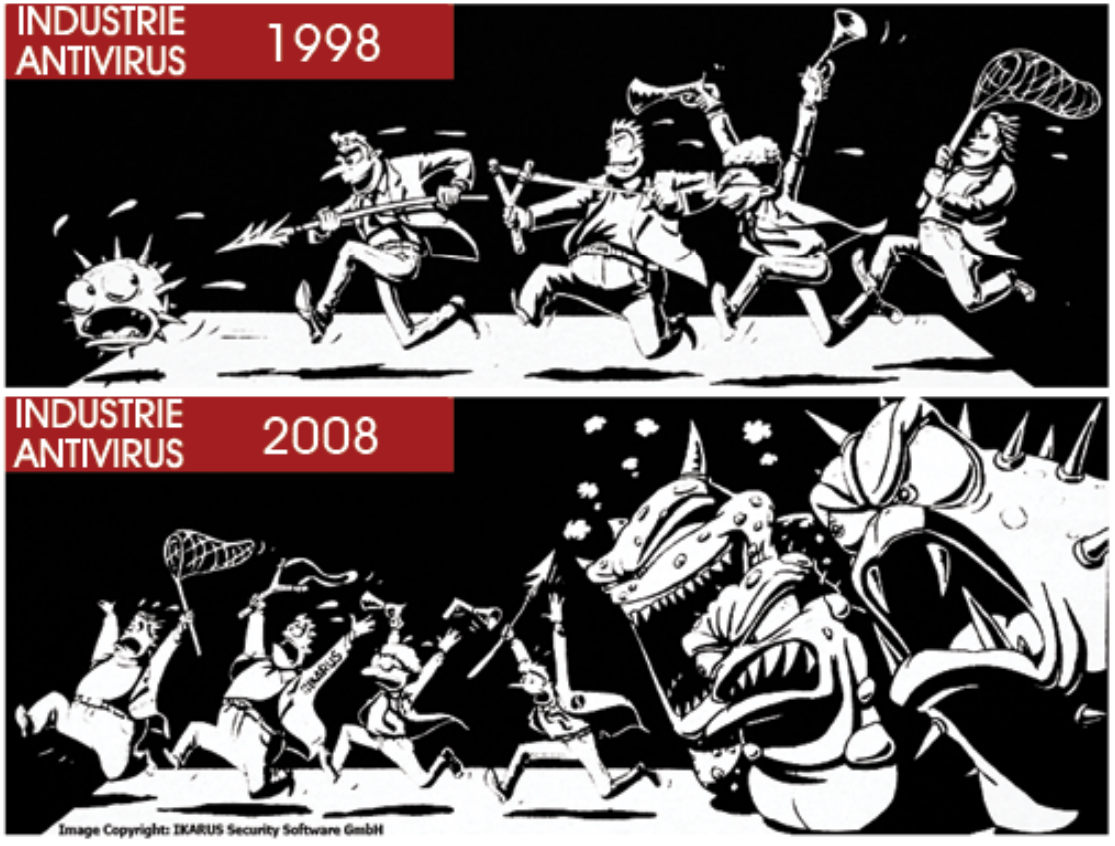
- **L'atteinte à la confidentialité / l'attaque virale**



2. Les multiples visages de la cybercriminalité

L’ordinateur comme moyen ou cible d’attaques cybercriminelles

- L’atteinte à la confidentialité / l’attaque virale



2. Les multiples visages de la cybercriminalité

L’ordinateur comme moyen ou cible d’attaques cybercriminelles

- **L’atteinte à la confidentialité / l’attaque virale / Maroc**
  - Une société d’assurance a vu son SI paralysé pendant plus de 2 semaines. Elle était obligée de fonctionner en mode dégradé
  - Une banque a vu son activité interrompu pendant une journée entière, et ce sur l’ensemble du territoire suite à une attaque virale
  - Début du mois de mai 2009 et après avoir changé son mode opératoire, Conficker a infecté plusieurs entreprises privées et organismes publiques au Maroc. Ainsi, plusieurs grandes structures ont vu leurs systèmes d’informations indisponibles pendant plusieurs heures.

2. Les multiples visages de la cybercriminalité

L'ordinateur comme moyen ou cible d'attaques cybercriminelles

- **L'atteinte à la confidentialité / le phishing**
  - Selon Symantec, l'activité de phishing est en hausse de **66% par rapport à 2008**. Ces attaques visaient essentiellement les acteurs du secteur des **services financiers.**
  - **12 % de tous les vols** de données constatés en 2008 concernaient les numéros de carte de crédit.
  - Au Maroc, de nombreux cas ont été apportés:
    - *www.atijariwafabank.com au lieu de www.attijariwafabank.com*
    - *Meditel a découvert en 2007 qu'une tentative de piratage visait ses clients utilisant les cartes téléphoniques pré payées. La technique consistait à envoyer un courriel qui propose d'acheter par cartes bancaires des recharges Meditel à travers le faux site web http://meditel.medi-recharge.ma (site web cloné à partir du site web institutionnel http://www.meditel.ma).*

2. Les multiples visages de la cybercriminalité

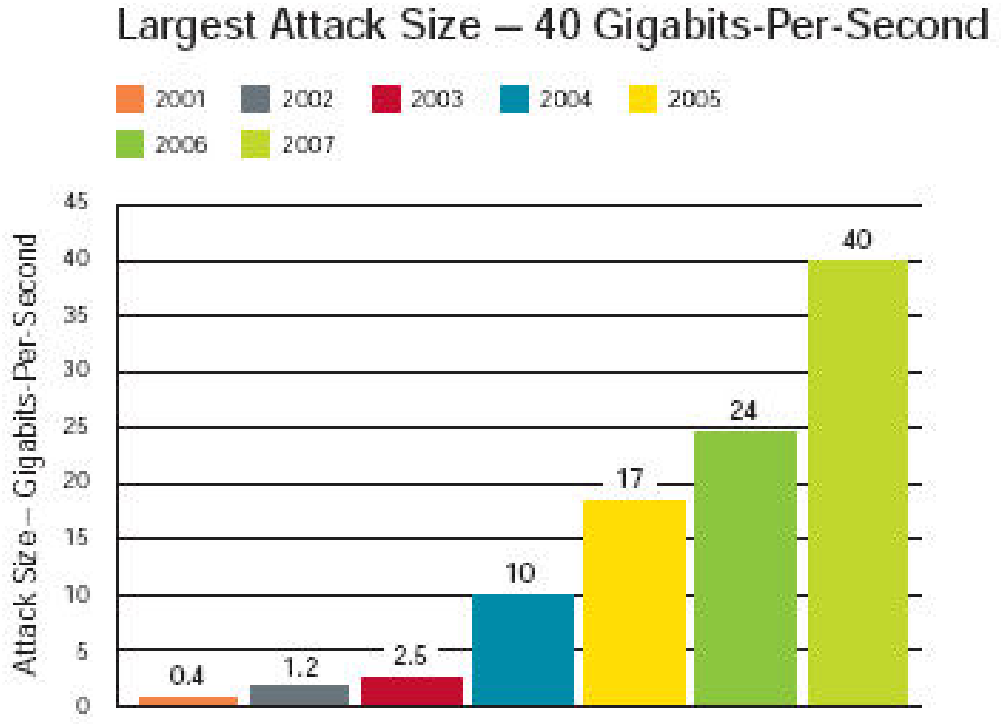
L'ordinateur comme moyen ou cible d'attaques cybercriminelles

- **L'atteinte à la disponibilité/ DoS et DDoS**
  - Selon Verisign, les attaques DDoS croissent plus rapidement que la bande passante allouée à l'internet. Ainsi plus de **190 000 attaques par déni de service distribué ont été organisées en 2008, ce qui aurait rapporté aux cybercriminels plus de 20 millions de dollars**.
  - De nos jours, le moyen le plus couramment utilisé pour lancer des attaques par dénis de services est l'utilisation **des réseaux de zombies**
  - Selon un rapport publié en Novembre 2008 par Arbor Networks, les attaques DDoS ont franchi durant l'année 2008 la barrière **des 40 gigabits par seconde soit 64% de l'échelle des attaques par rapport à l'année 2007**. Peu d'organisations peuvent y faire face.
  - Avec la forte augmentation du nombre d'échanges commerciaux sur l'internet, le nombre de chantages au déni de service est lui aussi en très forte progression.
  - Toute entreprise réalisant un chiffre d'affaire important dans une activité en ligne à fort effet de levier, est potentiellement vulnérable aux attaques par dénis de service.

2. Les multiples visages de la cybercriminalité

L'ordinateur comme moyen ou cible d'attaques cybercriminelles

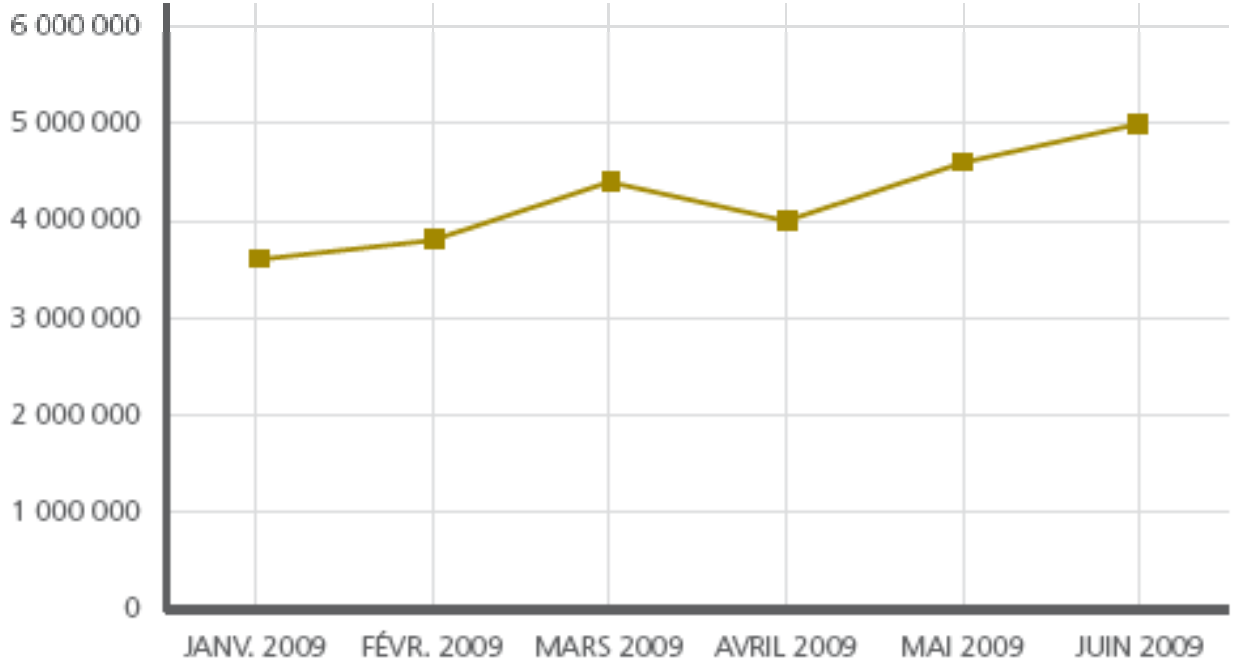
- **L'atteinte à la disponibilité/ DoS et DDoS**



2. Les multiples visages de la cybercriminalité

L'ordinateur comme moyen ou cible d'attaques cybercriminelles

- **L'atteinte à la disponibilité/ DoS et DDoS/ Les botnets**
  - Un botnet est un réseau d'ordinateurs zombies contrôlés à l'insu de leurs propriétaires.
  - Ils sont devenus la principale source de propagation du courrier indésirable, des attaques DDoS et de diffusion de nouveaux virus



2. Les multiples visages de la cybercriminalité

L'ordinateur comme moyen ou cible d'attaques cybercriminelles

- **L'atteinte à la disponibilité/ DoS et DDoS/ Les botnets**
  - Les botnets sont considérés même par certains analystes comme un phénomène géopolitique. Il est important donc, d'examiner la production des ordinateurs zombies par pays.

2eme trimestre 2009

Pays	%
Etats-Unis	15,7
Chine	9,3
Brésil	8,2
Russie	5,6
Allemagne	5,3
Italie	4,0
République de Corée	3,8
Inde	3,2
Royaume Uni	3,0
Espagne	2,6
TOTAL	**60,7**

2. Les multiples visages de la cybercriminalité

L'ordinateur comme moyen ou cible d'attaques cybercriminelles

- **L'atteinte à la disponibilité/ DoS et DDoS/ Les botnets**
  - Le nombre de pourriels en provenance d'un pays par rapport à la quantité globale de pourriels détectés donne une indication du nombre de machines zombies d'un pays par rapport à l'ensemble des machines connectées sur le réseau.

2. Les multiples visages de la cybercriminalité

L'ordinateur comme moyen ou cible d'attaques cybercriminelles

L'atteinte à l'intégrité / Défacement des sites Web

- Le phénomène de défacement des sites web gouvernementaux a atteint un niveau insupportable en 2010. En effet, après plusieurs attaques contre les **sites de la primature, du ministère de l'énergie et de la justice**, la cellule de la lutte contre la cybercriminalité de la Sûreté Nationale a multiplié les coups de filet. Plusieurs groupes ont été arrêtés. Il s'agit notamment du groupe de pirates baptisé « Team Rabat-Salé » connu dans l'univers *Underground* marocain pour ses attaques dirigés contre les sites israéliens et ceux du Polisario.
- Le défacement des sites web est **un acte identitaire à presque tous les pays en voie de développement**
- Certains analystes avancent que les sites marocains constituent un terrain d'entraînement pour les pirates étrangers

2. Les multiples visages de la cybercriminalité

L'ordinateur comme moyen ou cible d'attaques cybercriminelles

- **L'atteinte à l'intégrité / Défacement des sites Web**

Date	Attaquant	Domaine	Système
2009/05/28	Dr.Anach	www.marocainsdumonde.gov.ma/im...	Linux
2009/04/27	Hmei7	www.habous.gov.ma/sidishiker/i...	Win 2003
2009/01/08	GANG hackers ARABS	Docs.justice.gov.ma/ang.txt	Win 2003
2008/11/21	Old.Zone	www.equipementransport.gov.ma/...	Win 2003
2008/11/20	Old.Zone	www.mtpnet.gov.ma/index.htm	Win 2003
2008/09/23	ExSploiters	www.lagencedusud.gov.ma	Win 2003
2008/09/16	NetKiller	www.affaires-generales.gov.ma/...	Win 2000
2008/08/17	mor0ccan nightmares	agadir-indh.gov.ma	Linux
2008/08/17	mor0ccan nightmares	www.essaouira-indh.gov.ma	Linux
2008/08/04	Sm4rT Security Cr3w	www.dapr.gov.ma	Linux
2008/08/02	Handrix	www.invest.gov.ma/all4one.htm	Win 2003
2005/01/18	Fatal Error	www.mhu.gov.ma	Win 2000

2. Les multiples visages de la cybercriminalité

L’ordinateur comme facilitateur d’attaques cybercriminelles

- **L’escroquerie en ligne**
  - L’arnaque nigérienne (SCAM 419)
  - Janvier 2007 : Une femme non identifiée qui prétend être la nièce de l’ambassadeur du Canada à Abidjan arrive à faire croire aux victimes rencontrées sur le Chat de Yahoo qu’elle disposait du pouvoir de les aider à émigrer au Canada. Plusieurs milliers de DHs ont été détournés.
  - Un cyberescroc, originaire de Rabat et qui se faisait passer pour "un Emirati", promettait à ses victimes parmi les femmes rencontrées sur le Web un emploi dans un pays de la péninsule arabique et exigeait des photos personnelles. Une fois les photos reçues, le cyberescroc qui a eu à son actif, une quinzaine d’opérations identiques réclamait des sommes d’argent allant de 2 000 à 2 500 DH sous peine de diffusion des dites photos sur l’internet

2. Les multiples visages de la cybercriminalité

L'ordinateur comme facilitateur d'attaques cybercriminelles

La fraude à la carte bancaire

- Selon le CMI, le nombre de cartes bancaires contrefaites au Maroc est passé de **1.694** cartes en **2.000** à plus de **6.000 en 2008**. **Soit le triple**. En parallèle, le montant des sommes détournées connaît lui aussi une hausse vertigineuse. **De 4,4 millions de dirhams en 2000, ce montant est passé à 20 millions en 2008**
- 2005 : La gendarmerie royale a arrêté 7 personnes soupçonnées d'avoir détourné **4,6 millions de DH** en copiant des cartes bancaires à l'aide de matériel informatique.
- 2008 : Deux employés d'un centre d'appel basé à Casablanca, ont été interpellés par les agents de la brigade centrale de police. Ils ont détourné d'importantes sommes d'argent en utilisant les données de porteur de cartes (nom de titulaire de carte, PAN, date d'expiration, etc…) qu'ils enregistraient lors des conversations téléphoniques avec les clients français et transmettaient par la suite à une complice basée en France qui se chargeait d'acheter des biens sur l'internet et de les revendre après.

2. Les multiples visages de la cybercriminalité

L'ordinateur comme facilitateur d'attaques cybercriminelles

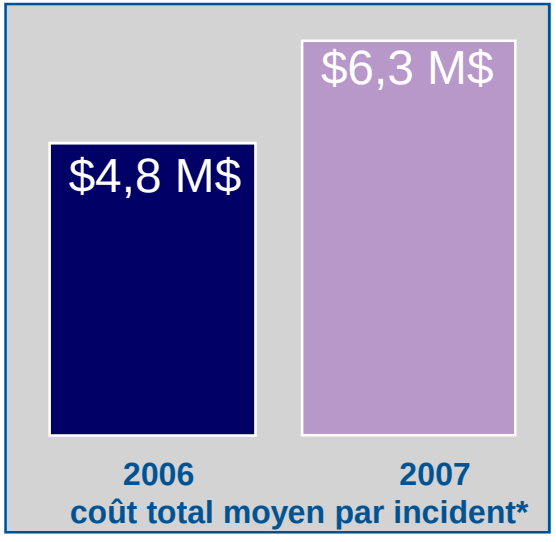
- **La fraude à la carte bancaire**
  - 2009 : Un réseau international spécialisé dans la falsification de cartes bancaires a été démantelé par la police de Casablanca. L'arrestation a eu lieu suite une alerte lancée auprès de la police par le responsable d'un hôtel où avait l'habitude de séjourner l'un des membres du groupe, et ce après avoir découvert, caché dans les gaines, un matériel électronique composé notamment d'un encodeur qui sert à falsifier les cartes bancaires et de plusieurs caméras. Ainsi, **1.400 cartes** falsifiées ont été saisies. Le procédé est le même. Insérer une minuscule caméra et un appareil type **skimmer** dans des guichets automatiques des quartiers aisés de la métropole économique.

.

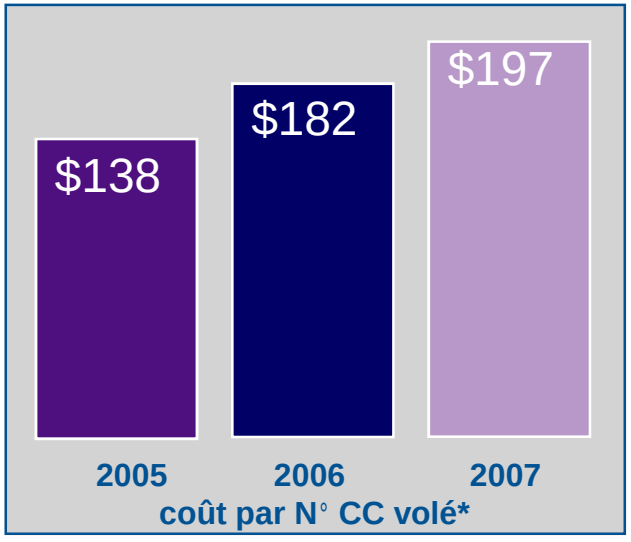
2. Les multiples visages de la cybercriminalité

L'ordinateur comme facilitateur d'attaques cybercriminelles

- Les marques restent très discrètes sur les montants globaux.
  - On parle plutôt de « coût par n° de CC volé » ou « par incident »
    - Coût de la fraude
    - Coût de re-émission des cartes (~20-30 $ par carte)



*Ponemon Institute,



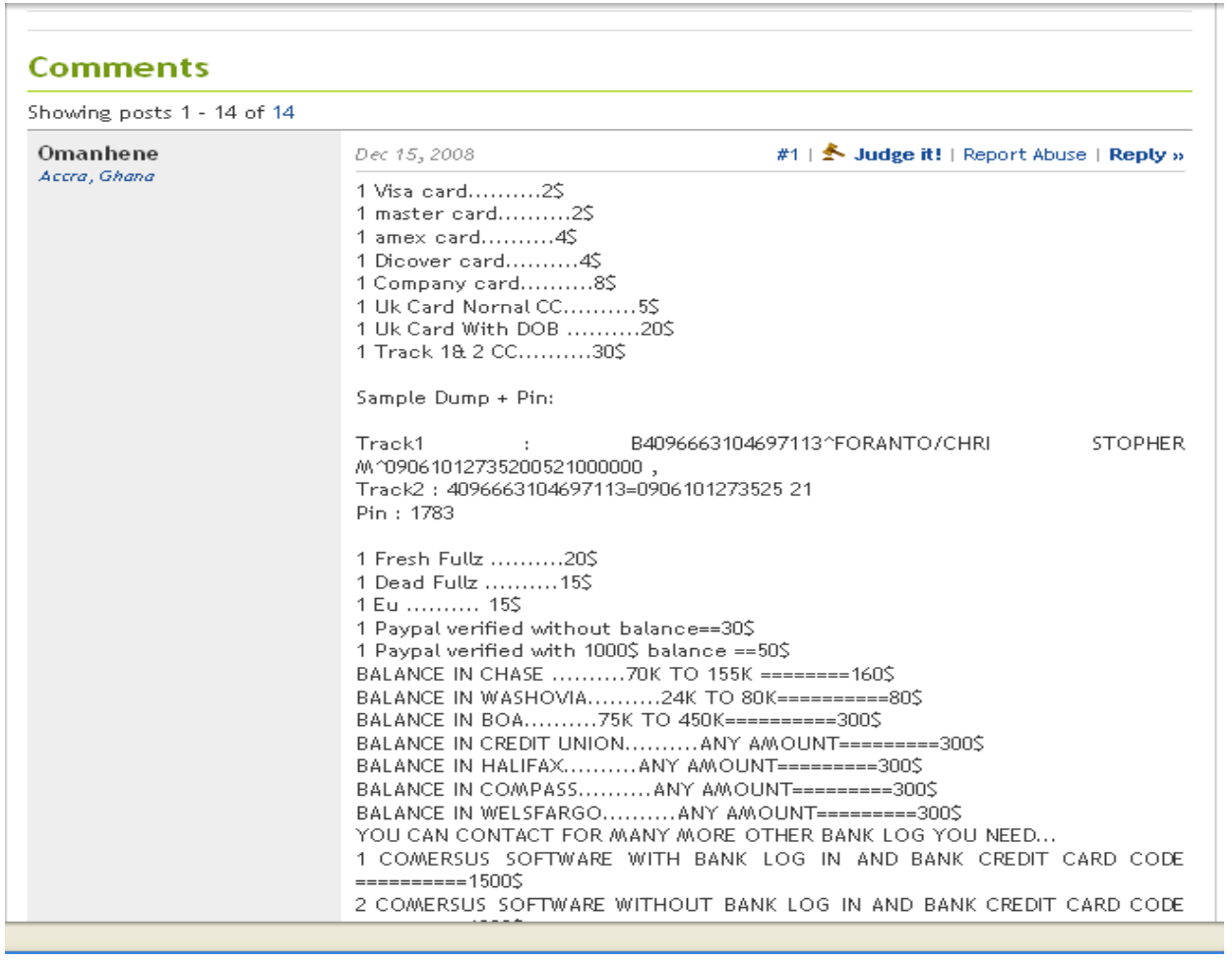
*Ponemon Institute,

- Le « FBI's Financial Report to the Public for 2007 » parle de pertes de 52.6 Milliards $

2. Les multiples visages de la cybercriminalité

L'ordinateur comme facilitateur d'attaques cybercriminelles

La vente des cartes bancaires volées (mot clé :Fullz)



Comments

Showing posts 1 - 14 of 14

Omanhene
Accra, Ghana

Dec 15, 2008 #1 | Judge it! | Report Abuse | **Reply »**

1 Visa card.....2$
1 master card.....2$
1 amex card.....4$
1 Dicover card.....4$
1 Company card.....8$
1 Uk Card Nornal CC.....5$
1 Uk Card With DOB .....20$
1 Track 1& 2 CC.....30$

Sample Dump + Pin:

Track1 : B4096663104697113^FORANTO/CHRI STOPHER M^0906101273520052100000 0 ,
Track2 : 4096663104697113=0906101273525 21
Pin : 1783

1 Fresh Fullz .....20$
1 Dead Fullz .....15$
1 Eu ..... 15$
1 Paypal verified without balance==30$
1 Paypal verified with 1000$ balance ==50$
BALANCE IN CHASE .....70K TO 155K ========160$
BALANCE IN WASHOVIA.....24K TO 80K==========80$
BALANCE IN BOA.....75K TO 450K==========300$
BALANCE IN CREDIT UNION.....ANY AMOUNT=========300$
BALANCE IN HALIFAX.....ANY AMOUNT=========300$
BALANCE IN COMPASS.....ANY AMOUNT=========300$
BALANCE IN WELSFARGO.....ANY AMOUNT=========300$
YOU CAN CONTACT FOR MANY MORE OTHER BANK LOG YOU NEED...
1 COMERSUS SOFTWARE WITH BANK LOG IN AND BANK CREDIT CARD CODE ==========1500$
2 COMERSUS SOFTWARE WITHOUT BANK LOG IN AND BANK CREDIT CARD CODE

2. Les multiples visages de la cybercriminalité

L’ordinateur comme facilitateur d’attaques cybercriminelles

- **Le blanchiment de l’argent**
  - Sur l’internet, en raison notamment de la multiplication des banques en ligne, des casinos virtuels, des sites de paris en ligne et des possibilités de placements boursiers en ligne, les possibilités de blanchiment d’argent sont illimitées
  - Compte tenue de l’implication de la planète toute entière dans la lutte contre le financement du terrorisme international, sous l’impulsion des Etats-Unis, l’argent sale provenant des activités criminelles ne peut plus circuler librement, même dans les paradis fiscaux. Par conséquent, les diverses mafias se sont logiquement tournées vers la Toile pour l’activité de blanchiment de l’argent.
  - Le recours aux casinos en ligne
  - Le recrutement des mules

2. Les multiples visages de la cybercriminalité

L'ordinateur comme facilitateur d'attaques cybercriminelles

- **La pédopornographie en ligne**
  - Grâce à la diffusion des technologies assurant l'anonymat, notamment le chiffrement des courriels et l'utilisation du proxy, il est devenu extrêmement difficiles de surveiller les activités des réseaux pédophiles.
  - La prolifération des contenus pédophiles sur l'internet est telle qu'en 2006, le nombre de sites contenant des images ou des vidéos de pornographie juvénile a dépassé 3000 sites web selon Internet Watch Fondation,
  - Selon un chiffre désormais largement diffusé, un mineur sur cinq a été confronté à des avances sexuelles sur l'internet
  - Selon les résultats d'une enquête réalisée par Center for Media Freedom in the Middle East and North Africa (CMF-MENA) auprès de 106 enfants de la ville de Casablanca, plus des deux tiers des enfants interviewés auraient reçu des offres de voyages, des cadeaux ou des propositions de mariages via l'internet de la part d'inconnus

2. Les multiples visages de la cybercriminalité

L'ordinateur comme facilitateur d'attaques cybercriminelles

La pédopornographie en ligne

- 2005 : Hervé Le Gloannec, un touriste français a été condamné par le tribunal de première instance de Marrakech à 4 ans de prison ferme. Il ne s'était pas contenté d'infliger des sévices sexuels sur des enfants à Marrakech, mais il s'était également adonné à l'exploitation de leur vertu à travers la production et la distribution de films pornographiques utilisant des enfants. Son ordinateur personnel regorgeait de 17.000 photos et 140.000 enregistrements vidéo qu'il envoyait vers des sites pornographiques
- 2005 : Un journaliste belge de l'hebdomadaire « Le Soir » prenait des photos pornographiques des jeunes filles d'Agadir et les publiait sur un site pornographique. Parmi ses victimes, il y avait des prises montrant des filles mineures.
- 2006 : Le directeur du théâtre Mogador à Paris a été condamné par le tribunal de première instance de Marrakech à quatre mois de prison avec sursis après avoir été pris en flagrant délit en train d'abuser sexuellement d'un mineur qu'il a rencontré sur l'internet selon les rapports de police.
- 2006 : Un touriste français a été condamné à 4 ans de prison après avoir été pris en flagrant délit, en train de prendre des photos d'enfants mineurs dans des positions sexuelles. Il possédait dans son appareil photo 117.000 photos pornographiques.

2. Les multiples visages de la cybercriminalité

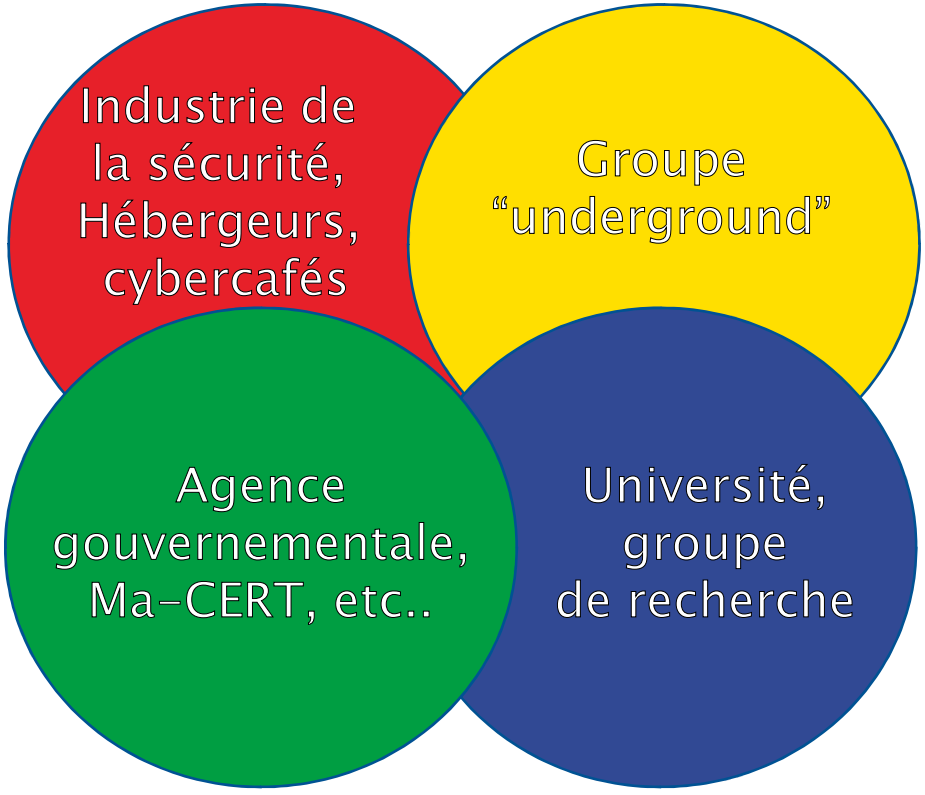
L'ordinateur comme facilitateur d'attaques cybercriminelles

- **Le cyberterrorisme**
  - La cybercriminalité peut donc avoir une dimension terroriste. Selon un rapport de l'Intelligence Advanced Research Projects Activity (IARPA), le cyberterrorisme peut se manifester à plusieurs niveaux. Il en a identifié cinq :

1. **Les communications secrètes**
2. **L'entraînement**
3. **Le transfert et le blanchiment d'argent**
4. **Cyberattaques (cas de l'Estonie, cas de la Géorgie)**
5. **Guerre informationnelle**

3. L'ECOSYSTEME DE LA CYBERCRIMINALITE

3. L'écosystème de la cybercriminalité



3. L’écosystème de la cybercriminalité

L’univers de l’Underground

- **Les acteurs de l’univers de l’underground**
  - Les hackers (Whites Hat, Black hat, etc…)
  - Les crackers
  - Les script kiddies
  - Les hacktivistes
  - Les phreakers, etc…
  - Le basculement est de plus en plus apparent (Ethical Hackers)
  - Vision anglophone (vers la réhabilitation des hackers)

3. L’écosystème de la cybercriminalité

L’univers de l’Underground

- **L’Underground marocain**
  - Il y a certes des hackers réputés, mais nous constatons que l’underground marocain est principalement composés par des scripts kiddies (défaçement des sites web).
  - Le hacktivisme est très présent (exemple des attaques contre Israël lors de la guerre du Gaza, attaques contre le Polisario, etc…)

3. L’écosystème de la cybercriminalité

L’industrie de la sécurité

- **Les éditeurs, constructeurs, cabinets conseil et intégrateurs**
  - Au Maroc, une poignée de constructeurs et éditeurs de solutions de sécurité informatique dont les ventes sont en majorité tirées par les besoins des opérateurs télécoms et du secteur de la banque-finance, se partagent ainsi cette niche de marché. Cisco, Blue Coat Systems, Websense, Kaspersky, Symantec, McAfee, Trend Micro, Juniper Networks, Checkpoint en sont les principaux protagonistes
  - Il n’existe pas une véritable industrie locale en sécurité (Peu d’acteurs locaux). Face à cette situation, il est extrêmement urgent pour le gouvernement marocain d’encourager la naissance d’une industrie locale non seulement pour pouvoir générer de l’emploi hautement qualifié, mais surtout pour ne pas laisser la sécurité d’institutions critiques entre les mains des étrangers.

3. L'écosystème de la cybercriminalité

L'industrie de la sécurité

Les hébergeurs

- Des sociétés commerciales proposent désormais des services d'hébergement dévoués au spamming, au lancement des compagnes de phishing, au stockage des codes malicieux et des données volées, et à l'utilisation des serveurs de commande de botnets.
- Parmi les organisations qui ont le plus fait parler d'elles, nous retenons Russian Business Network, Abdallah Internet Hizmetleri, Atrivo
- C'est le cas de **la société SecureHosting basée au Bahamas** qui a été suspectée d'avoir soutenu RBN en hébergeant certains de leurs serveurs. Le site web de cette société offshore annonce la couleur dans leurs conditions d'utilisation: **« L'internet n'appartient à personne. Ainsi, nous ne pouvons pas nous permettre de surveiller ou de censurer l'internet et nous ne le ferons pas. Nous ne pouvons pas assumer la responsabilité pour des activités de nos clients, qu'il s'agisse de publication d'un contenu offensant ou illégal »**

3. L’écosystème de la cybercriminalité

L’industrie de la sécurité

- **Le cybercafé**
  - Selon l’Agence Nationale de Réglementation des Télécommunications (ANRT), le recours au cybercafé représente un taux d’utilisation de 84% quand il s’agit de connexion internet hors domicile au Maroc
  - Le cybercafé s’est retrouvé à maintes reprises à l’une de l’actualité au Maroc. C’est le cas par exemple de Farid Essebar qui a participé à la création et à la diffusion du vers Zotob en opérant à partir d’un cybercafé basé à Rabat et du Kamikaze qui a perpétré un attentat à l’explosif dans un cybercafé situé à Casablanca lui servant d’un lieu d’échanges et de communications avec les réseaux terroristes

3. L'écosystème de la cybercriminalité

Les centres de recherche et les acteurs de formation

La recherche

- Par définition, l'industrie de la sécurité de l'information est liée à la recherche et au développement,
- Autre la recherche et le développement dans le domaine de la sécurité de l'information engagée par les industriels, les universités et les armées s'y intéressent aussi de plus prés. D'ailleurs de nombreuses entreprises « Start-Up » ont vu le jour en tant que «Spin-off» dans le milieu universitaire et de l'armée. Le rôle joué par l'université dans l'innovation n'est plus à démonter. Aux Etats-Unis par exemple, plus de 70% de tous les brevets sont basés sur des résultats universitaires
- Au Maroc, l'université est complètement déconnectée de la recherche scientifique à vocation industrielle. Une étude récente, coordonnée par le sociologue Mohamed Cherkaoui précise que plus de 55% des professeurs marocains n'ont jamais publié une seule ligne de leur carrière

3. L'écosystème de la cybercriminalité

Les centres de recherche et les acteurs de formation

- **La formation**
  - L'offre en terme de formation en sécurité est très pauvre
  - Les universités et les écoles des ingénieurs marocaines proposent au mieux quelques cours qui se limitent souvent à des introductions à la sécurité si on excepte le cas de l'Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS) a enrichi récemment son programme de formation pour y inclure désormais une option de sécurité des systèmes d'information
  - Vers la professionnalisation du métier de la sécurité (CISA, CISSP, CEH, PCI QSA, L.A ISO 27001, CISM, etc….)

3. L’écosystème de la cybercriminalité

Les acteurs institutionnels nationaux

- Les acteurs d’investigation (Chiffre noir)
- Les acteurs de la répression
- Les acteurs de veille et de signalement (CERT, ma-CERT, etc…)
- La police
- La gendarmerie

3. L’écosystème de la cybercriminalité

Les acteurs institutionnels internationaux

- Les Nations-Unies
- L’Organisation de Coopération et de Développement Economiques (OCDE)
- L’Union Internationale des Télécommunications (UIT)
- Interpol
- Le conseil de l’Europe
- Europol
- La coopération internationale est l’un des facteurs clés du succès en matière de lutte contre la cybercriminalité.

4. LES RISPOSTES JURIDIQUES

4. Les ripostes juridiques

La loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données

- **Les intrusions**
  - L'accès frauduleux dans un STAD
  - Le maintien frauduleux dans un STAD
- **Les atteintes**
  - Les atteintes au fonctionnement d'un STAD
  - Les atteintes aux données

4. Les ripostes juridiques

La loi n°53-05 relative à l'échange électronique de données juridiques

- **La preuve**
  - La redéfinition de la preuve littérale
  - La consécration de la force probante de l'écrit électronique
- **La signature électronique**
  - La reconnaissance juridique de la signature électronique
  - Les prestataires de service de certification

4. Les ripostes juridiques

La loi n°09-08

- **La nature des données à protéger**
- **Les droits de la personne concernée**
  - Le droit à l'information
  - Le droit d'accès
  - Le droit de rectification
  - Le droit d'opposition
- **Les obligations du responsable du traitement**
  - Déclaration préalable
  - Autorisation préalable
  - Obligation de confidentialité et de sécurité des traitements professionnels

5. VERS LA CONFIANCE NUMERIQUE

5. Vers la confiance numérique au Maroc

Quelques exemples

- Les Etats-Unis inscrivent leur politique de répression contre la cybercriminalité dans le cadre de la protection des intérêts vitaux de la nation américaine;
- En France, la lutte s'inscrit dans une perspective de protection des libertés individuelles et de droits de l'Homme;
- Au Maroc, le programme « Confiance Numérique » qui rentre dans le cadre de la stratégie « Maroc Numeric 2013 », est incontestablement la feuille de route la mieux élaborée à l'heure. Trois initiatives ont été définies:
- Initiative 1 : Mettre à niveau et renforcer le cadre législatif ;
- Initiative 2 : Mettre en place les structures organisationnelles appropriées ;
- Initiative 3 : Promouvoir et sensibiliser les acteurs de la société à la sécurité des systèmes d'information.

5. Vers la confiance numérique au Maroc

Maroc Numeric 2013

- **Mettre à niveau et renforcer le cadre législatif**
  - Protéger les personnes physiques à l'égard des traitements de données à caractère personnel
  - Favoriser la dématérialisation des transactions électroniques
  - Soutenir le développement du commerce électronique
  - *La sécurité lors de la formation du contrat*
  - *La sécurité quant à l'exécution de la prestation*
  - *La sécurité lors du paiement de la transaction*

5. Vers la confiance numérique au Maroc

Maroc Numeric 2013

- **Mise en place des structures organisationnelles appropriées**
  - Le comité de la sécurité des systèmes d'Information (SSI) ;
  - L'organisme ma-CERT ;
  - L'organisme de tiers de confiance ;
  - La commission Nationale de Protection des Données Personnelles (CNDP) ;
  - Les sites de back-up.

5. Vers la confiance numérique au Maroc

Maroc Numeric 2013

- **Promotion d'une culture de sécurité**
  - Mettre en œuvre un programme de sensibilisation et de communication sur la SSI ;
  - Mettre en place des formations sur la SSI à destination des élèves ingénieurs ;
  - Mettre en place des formations à destination des professions juridiques ;
  - Définir une charte des sites marchands.

6. Conclusion

Dure, dure sera la lutte…….

- Le nombre d'internautes marocains, qui n'a pas cessé de croître ces dernières années, continuera de grimper d'une façon exponentielle pour atteindre 12 millions d'internautes en 2012 selon l'ANRT.
- Cette croissance, qui sera tirée notamment par le haut débit et l'internet 3G, couplée à l'anonymat et au faible risque de se faire arrêter, jouera un rôle favorable pour le développement de la cybercriminalité. Ce qui est de nature à encourager l'émergence de nombreuses dérives et l'apparition d'utilisateurs peu scrupuleux.
- La convergence de la criminalité perpétrée dans le monde réel vers la criminalité numérique perpétrée dans le cyberespace sera de plus en plus appréciée par les mafias. Ainsi, le blanchiment d'argent, l'escroquerie, la fraude, le proxénétisme et la pédopornographie trouveront dans le cyberespace un terrain propice à leur développement.
- Face à une cybercriminalité qui sera de plus en plus globale, variée, organisée et rentable, il est particulièrement important pour les pouvoirs publics d'adopter une approche transverse mêlant problématique géopolitique, sociologique, financière et juridique.

MERCI

Blog de Ali EL AZZOUZI http://www.cybercriminalite.ma