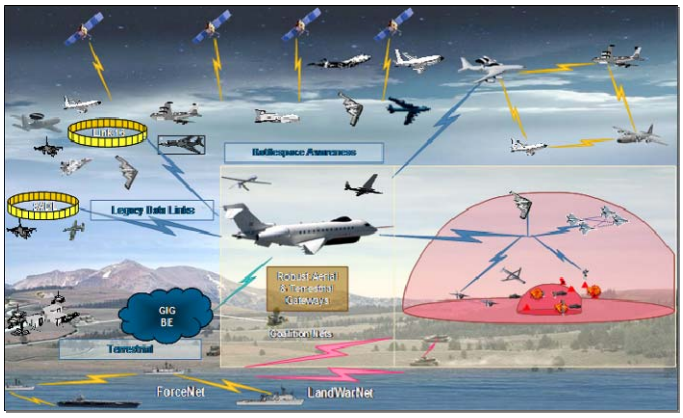
Cyberguerre et cybercriminalité

Gérard Peliks
CyberSecurity Solutions Customer Centre
CASSIDIAN, an EADS company
gerard.peliks@cassidian.com

31 mars 2011

AAEisep

Le cyberespace et la cyber dominance

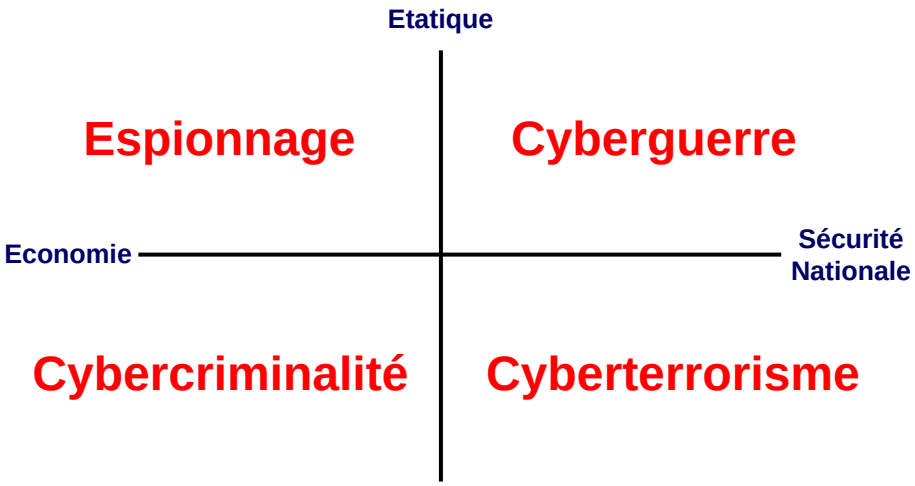


Un des défis les plus sérieux pour l'économie et la sécurité nationale auquel la nation fait face

Barack Obama

AAEisep

Les acteurs de l'insécurité



AAE isep

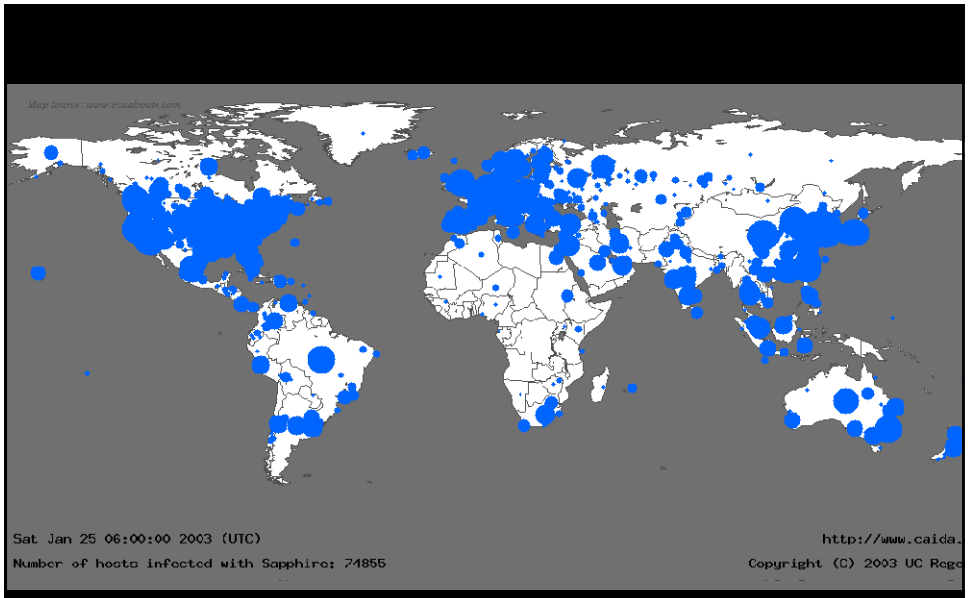
3

La cybercriminalité

- **Le cyberespace, une autre dimension**
- La cyberguerre, la menace du 21eme siècle
- La cybercriminalité
  - Les modèles économiques
    - du Phishing
    - des Botnets
- La cybersécurité

AAE isep

4



Des dizaines de milliers de serveurs dans le monde infectés en 10 minutes !

ver blaster

```
while (*pwszTemp != L'\\')
        *pwszServerName++ = *pwszTemp++;
```

Quelle est la durée de vie de votre PC non protégé ?

- Durée de vie d'un PC sous Windows, directement connecté à l'internet
  - sans antivirus à jour
  - sans firewall personnel

  En 2003 : 40 minutes
  En 2004 : 20 minutes

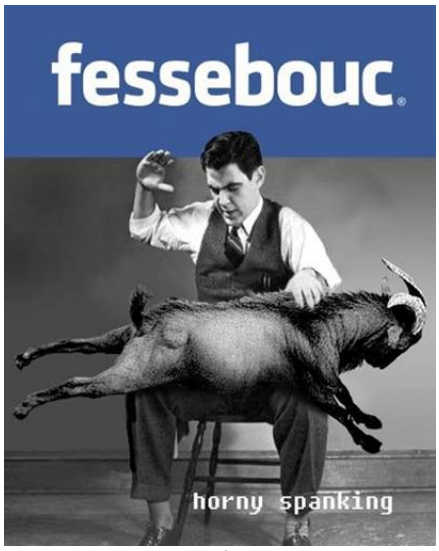
Selon le SANS Institute
www.sans.org

En 2011 : 3 minutes

AAEisep

6

Attention à Facebook !



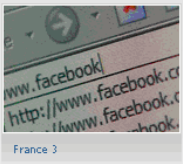
AAE isep

7

Publié le 20/05/2010 | 11:41

Licenciements pour un échange privé sur Facebook

Par AFP/Emmanuèle Bailly



France 3

Trois salariés de chez Alten licenciés pour des propos tenus sur Facebook

Deux ex-salariés du groupe Alten contestaient leurs licenciements, ce matin, devant le conseil des prud'hommes de Boulogne-Billancourt (Hauts-de-Seine).

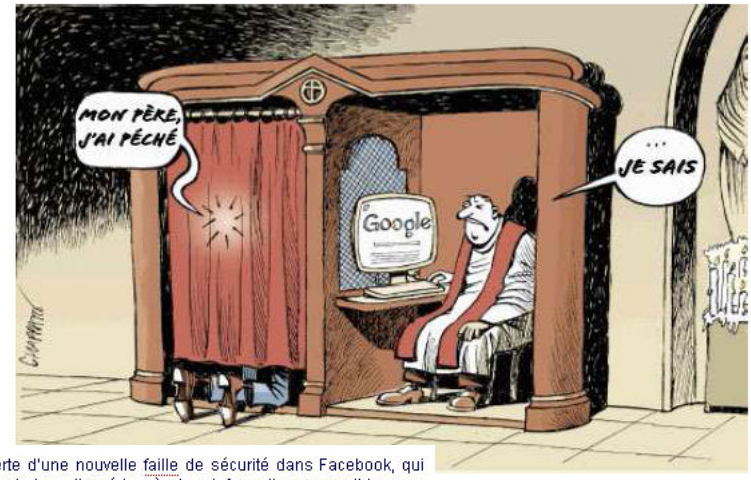
Leur entreprise les a licenciés à la suite de propos critiques tenus sur leur hiérarchie, un samedi soir, sur Facebook.L'affaire, révélée par France Info, remonte à décembre 2008. Connectés depuis leur domicile sur le réseau social Facebook, un samedi soir, les trois salariés de la société d'ingéniérie Alten avaient échangé des propos critiques envers leur hiérarchie et un responsable des ressources humaines.
Lors de ces échanges, l'un des salariés, s'estimant mal considéré par sa direction, avait ironisé sur sa situation en indiquant, sur sa page personnelle, faire partie d'un "club des néfastes".Les deux autres salariées impliquées dans le litige s'en étaient amusés en écrivant: "bienvenue au club". Une autre personne, un "ami" des employés sur Facebook et ayant accès à leur conversation, avait fait une copie des propos tenus et les avait transmis à la direction de l'entreprise.
Quelques semaines plus tard, ils avaient été licenciés pour "incitation à la rébellion"
et "dénigrement de l'entreprise".
Deux d'entre eux avaient alors décidé de porter l'affaire devant les prud'hommes, la troisième ayant accepté une transaction à l'amiable avec l'entreprise.
Le conseil des prud'hommes de Boulogne-Billancourt n'a pas tranché ce matin. Il n'a pas réussi à départager les salariés et employeurs, la moitié des conseillers prenant fait et cause pour l'entreprise, et l'autre pour les employés.
L'affaire est renvoyée et sera jugé par un juge départiteur (professionnel).

AAE isep

8

8

Méfiez-vous des réseaux sociaux



Suite à la découverte d'une nouvelle faille de sécurité dans Facebook, qui permettait à des pirates d'accéder à des informations sensibles sur n'importe lequel des 200 millions de membres du site, Sophos recommande aux utilisateurs d'Internet de ne pas laisser sur ce type de site de données pouvant conduire à des usurpations d'identité.

Source: http://www.rezonance.ch/fs-CH_Rezonance_Reputation_160108-2s.pdf?version_id=1971752

AAE isep

Image tirée de la présentation du CLUSIF

9

Le cyberbullying

- Cyber + bully (brute, tyran)
- Harcèlement virtuel
  - par web (facebook, twitter, blogs), portable, e-mail,
  - discrédit, perturbations, insultes, diffamation …
- Photos compromettantes
- Plusieurs centaines de mails envoyés par jour
- Dépressions, suicides en augmentation

Pour l'attaquant c'est un jeu ou une vengeance
La victime ne peut rien faire sinon ça fait de la pub à l'attaquant

AAE isep

10

La cybercriminalité

- Le cyberespace, une autre dimension
- **La cyberguerre, la menace du 21eme siècle**
- La cybercriminalité
  - Les modèles économiques
    - du Phishing
    - des Botnets
- La cybersécurité

AAE isep

Estonie 2007 : une arme de perturbation massive

Estonie

Une cyberattaque avec un million d'ordinateurs

Au printemps dernier, le réseau internet estonien, très développé, avait été paralysé par des attaques pirates, dont beaucoup provenaient de Russie. L'offensive avait coïncidé avec des émeutes de russophones, mécontents du déplacement d'un monument à la gloire de l'Armée soviétique. Selon Tim Boerner, un expert du Secret Service américain, *"plus d'un million d'ordinateurs dans le monde ont été utilisés pour attaquer l'Estonie au printemps 2007"*.

L'Estonie, une ancienne république de l'URSS qui a rejoint l'UE et l'Otan en 2004, est une **pionnière dans l'utilisation des nouvelles technologies**. Elle est de ce fait encore plus dépendante des réseaux de l'internet. Forte de l'expérience de ces attaques, qui ont en particulier paralysé son réseau bancaire pendant plusieurs jours, l'Estonie a persuadé l'Otan d'ouvrir à Tallinn au printemps un Centre de formation à la cyberdéfense.

Les experts ont aussi souligné que **les particuliers devaient être sensibilisés à ces nouveaux risques**. *"Les gens partout dans le monde doivent comprendre qu'un ordinateur non protégé chez soi peut être utilisé pour une cyber-guerre"*, a affirmé la ministre de la défense estonienne Heli Tiirmaa-Klaar.

AAE isep

Géorgie 2008 : La guerre commence au niveau des réseaux

Cyber-attaques en Georgie

Le conflit entre Russie et Géorgie en Ossétie du Sud a donné lieu il y a un mois à une vaste attaque sur le web : plusieurs sites gouvernementaux géorgiens ont été cybersquattés sans qu'on ait pu déterminer réellement l'origine de cette attaque.

Georgie

Parmi les sites touchés ont trouve celui du ministre de la défense et du ministre des affaires étrangères géorgien. Le site personnel du président Géorgien Mikheil Saakashvili a lui aussi été détourné et mis hors service pendant presque une journée.

Plusieurs serveurs de la Géorgie ont eux dû faire face à l'attaque par déni de service de milliers d'ordinateurs. L'objectif: générer un trafic Internet trop important, susceptible de faire flancher le réseau.

Une attaque de grande ampleur donc. La plus grande à ce jour dans le bloc Est.

Le site personnel du président Géorgien Mikheil Saakashvili a lui aussi été détourné et mis hors service pendant presque une journée. Plusieurs serveurs de la Géorgie

Le bloc Est touché par des cyber-attaques depuis 2 ans

Ce n'est pas la première fois qu'un tel phénomène se produit dans cette région du monde. L'Estonie puis la Lithuanie ont fait l'objet d'attaques de ce type en 2007.

Pour David Betz , enseignant au département d'étude des conflits militaires au King's College de Londres reste mesuré. "*Nous sommes toujours à l'âge de pierre de la cybercriminalité. Ces attaques ne sont pas d'un niveau très élevé mais pourraient très bien s'améliorer au fil des ans. Les Etats-Unis ont déjà créé une unité de cyber-défense, tout comme la Chine, la Russie bien-sûr ainsi que d'autres grandes puissances du globe*".

AAE isep

Iran 2010 : Le ver est dans la centrifugeuse…

Le ver Stuxnet est-il la première cyber-arme ?

Par La rédaction Le 22 septembre 2010 (10:00)
Rubriques : Sécurité Tags : siemens - cyberguerre - iran - scada - stuxnet - nucleaire

Découvert en juillet dernier, le ver Stuxnet ne ressemblait déjà pas à un logiciel malveillant ordinaire, cherchant à récupérer des données aisément monnayables : particulièrement sophistiqué, il vise les logiciels pour infrastructures industrielles automatisées, les Scada. Et tout particulièrement ceux de Siemens. Déjà évoquée alors, la piste du sabotage ne fait plus aucun doute, selon certains experts. Des experts qui verraient bien aujourd'hui, dans Stuxnet, une arme visant spécifiquement l'usine iranienne d'enrichissement d'uranium de Bushehr.

C'est en juillet dernier que Stuxnet a été découvert. Un ver d'un genre inédit : il exploite une faille affectant toutes les versions de Windows pour s'installer sur un ordinateur à l'insertion d'une clé USB, sans passer l'exécution du très classique script autorun.inf, mais en s'appuyant sur les mécanismes de traitement des fichiers liens (.lnk). Stuxnet installe deux pilotes : mrxnet.sys et mrxcls.sys. Tous deux embarquent des fonctions de rootkit pour masquer leurs activités au système d'exploitation. Surtout, ces deux pilotes empruntent la signature numérique de pilotes Realtek.

L'autre spécificité de Stuxnet, c'est de viser spécifiquement les infrastructures industrielles automatisées, à savoir les fameux systèmes Scada utilisés pour le contrôle centralisé des réseaux de distribution électrique ou d'eau potable, par exemple. Selon l'analyste Frank Boldewin, Stuxnet cherche, à son installation, à vérifier la présence, sur la machine qu'il vient d'infecter, des outils Simatic WinCC de Siemens, les outils Scada de l'industriel. S'appuyant sur le mot de passe d'accès aux bases de données de l'outil - défini en dur dans le logiciel et largement diffusé sur Internet, comme l'avaient relevé nos confrères de Wired -, Stuxnet dispose d'un accès complet aux données des infrastructures supervisées avec WinCC.

AAE isep

Iran 2010 : Attaque sur les systèmes SCADA : Stuxnet

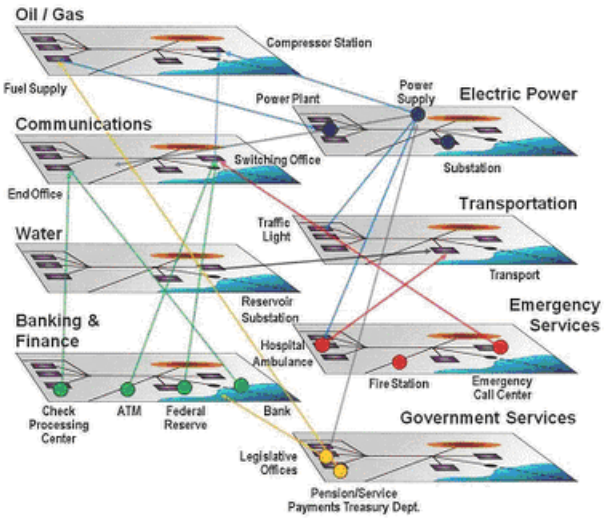
- 10 000 heures-hommes pour l ’écriture de Stuxnet
- 4000 fonctions différentes
- Exploitation de 4 zero-day attacks
- Fonction d’actualisation automatique
- Stuxnet a perturbé la vitesse de rotation des centrifugeuses de Natanz (à partir du 16 novembre 2010)

Pour son potentiel destructeur sur les SCADA, par rapport à un ver classique, Stuxnet fait l’effet d’une mitrailleuse lourde comparée à une arquebuse.

AAE isep

15

Attaques sur les SCADA



AAE isep

16

Le cinquième élément …

Tout comme au XIXème siècle nous avons eu à sécuriser la mer pour la défense de notre pays et sa prospérité,

qu'au XXème siècle, ce fut les cieux qu'il fallut rendre plus sûrs,

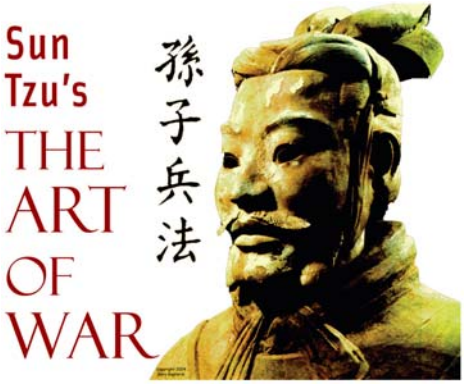
au XXIe siècle, nous prenons place désormais dans le cyberespace ».

Gordon Brown

AAE isep

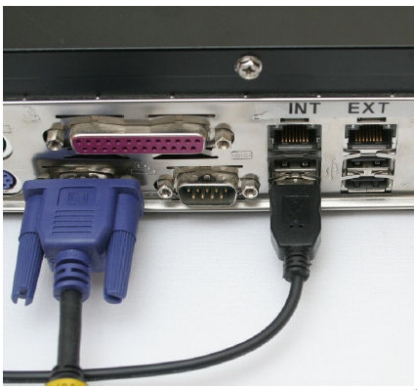
La seule façon …

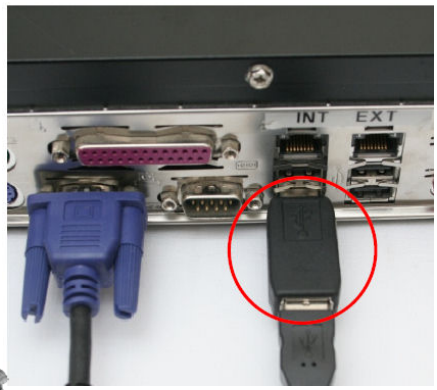
La seule façon de gagner la **cyberguerre**, c'est de l'éviter"



AAE isep

Redoutable : le keylogger USB





Sans

Avec

AAEisep

La cybercriminalité

- Le cyberespace, une autre dimension
- La cyberguerre, la menace du 21eme siècle
- **La cybercriminalité**
  - Les modèles économiques
    - du Phishing
    - des Botnets
- La cybersécurité

AAEisep

Mise en perspective

Si les voitures présentaient les mêmes problèmes que les logiciels …

Plus personne n'oserait rouler avec !!!

AAE isep

21

Mise en perspective

Plus personne n'oserait voler avec !!!

AAE isep

22

Les principaux risques pesant sur l'information

1. Le Web
2. La messagerie
3. Les clés USB

Mais n'oublions pas que le plus gros risque pour votre information et celle de votre organisation, c'est vous !

AAE isep

23

Le coût du cybercrime

Coût estimé de la perte d'un PC portable, en moyenne

49 000 dollars Source : Institut Ponemon

2.1 milliards de dollars au total, pour 86.000 PC de 329 entreprises

- Coût estimé du cybercrime par an

entre 100 et 1000 milliards de dollars

Source : OTAN printemps 2009

Une panne majeure des infrastructures d'information (réseaux téléphoniques, fibres optiques, réseaux d'ordinateurs…) en Europe pourrait avoir un coût global de 250 milliards de dollars (Forum économique mondial)
La probabilité d'une telle panne dans les 10 ans à venir serait de 10 à 20%.

Voir l'enquête : CSI COMPUTER SECURITY INSTITUTE http://gocsi.com/

AAE isep

24

Quelques types de menaces

- La plus médiatisée : **Le virus**
- La plus rusée : **Le ver**
- La plus sournoise : **Le cheval de Troie**

AAEisep

Conficker …

© *Financial Times*

05/02/2009

Les armées attaquées par un virus informatique

"Depuis deux semaines, les réseaux informatiques du ministère de la Défense sont infectés par un virus qui a immobilisé certains systèmes d'armes", comme les Rafale de la Marine, assure IntelligenceOnline. Cette crise *"d'ampleur"* pose de *"sérieuses questions sur la sécurité des réseaux militaires français"*, affirme la lettre confidentielle

Le réseau interne de la Marine, Intramar, a été le premier contaminé par le virus Conflicker [Conficker, selon Microsoft], le 12 janvier. Deux jours plus tard, l'état-major a décidé d'isoler Intramar des autres systèmes d'information, mais certains ordinateurs de la base aérienne de Villacoublay et du 8ème régiment de transmissions auraient été infectés. Les 15 et 16 janvier, les Rafale de la Marine *"sont restés cloués au sol"* faute d'avoir pu *"télécharger leurs paramètres de vol"*. Ils ont, par la suite, utilisés un autre système.

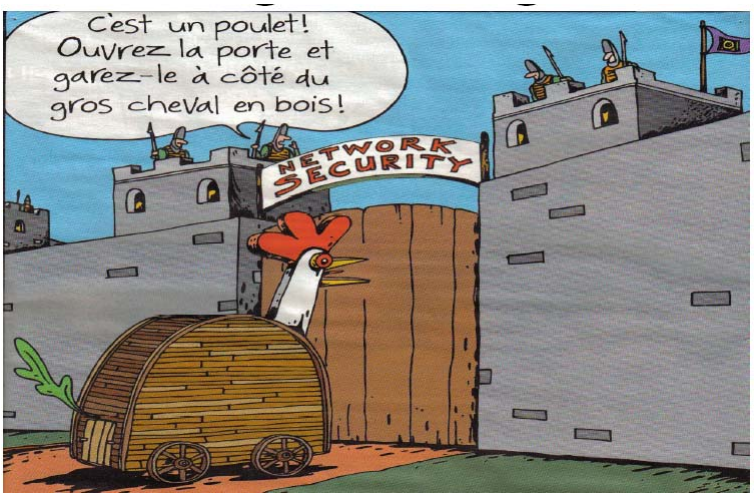
Le virus Conflicter avait pourtant été identifié par Microsoft dès l'automne 2008. En octobre, il avait averti ses clients de la nécessité d'effectuer des mises à jour pour se prémunir. IntelligenceOnline assure qu'***"au sein des armées, ces modifications n'ont pour l'essentiel pas été faites"***. Il a fallu attendre le 16 janvier, *"avec trois mois de retard"*, pour qu'une première intervention ait lieu à l'état-major de la Marine.

"A ce jour, l'état-major et le ministère de la défense ne savent pas combien d'ordinateurs et de systèmes d'informations militaires sont susceptibles d'avoir été contaminés par le virus Conflicker" - un ver informatique qui exploite une faille du service "serveur" de Windows pour se dupliquer. Bonne nouvelle, cependant, *"Conflicker ne permet pas a priori de prendre le contrôle d'un*

secretdefense.blogs.liberation.fr/defense/2009/02/les-armes-attaq.html

AAEisep

Le cheval de Troie



AAEisep

27

Les antivirus en échec

Résultats test antivirus ESIEA

Logiciel antivirus	*Attaque n°1*	*Attaque n°2*	*Attaque n°3*	*Attaque n°4*	*Attaque n°5*	*Attaque n°6*	*Attaque n°7*
Avast (version gratuite)	Echec	Détecté	Echec	Echec	Echec	Echec	Echec
AVG	Echec	Détecté	Echec	Echec	Echec	Echec	Echec
Avira	Echec	Détecté	Echec	Echec	Echec	Echec	Echec
BitDefender	Echec	Détecté	Détecté	Echec	Echec	Echec	Echec
DrWeb	Echec	Détecté	Echec	Echec	Echec	Echec	
F-Secure	Echec	Détecté	Détecté	Echec	Echec	Echec	Echec
GData	Echec	Détecté	Echec	Echec	Détecté*	Echec	Echec
Kasperky	Echec	Détecté	Echec	Echec	Echec	Echec	(1)
McAfee	Echec	Détecté	Echec	Echec	Echec	Echec	Echec
MSE (Microsoft)	Echec	Détecté	Echec	Echec	Echec	Echec	Echec
NOD 32	Echec	Détecté	Echec	Echec	Echec	Echec	Echec
Norton Symantec	Echec	Détecté	Echec	Echec	Echec	Echec	Echec
Safe 'n" Sec	Echec	Détecté	Echec	Echec	Echec	Echec	Echec
Sophos	Echec	Détecté	Echec	Echec	Echec	Echec	(2)
Trend Micro	Echec	Détecté	Echec	Echec	Détecté	Echec	Echec

AAEisep

28

Les facticiels

Dear Microsoft Customer,

Starting 12/11/2009 the 'Conficker' worm began infecting Microsoft customers unusually rapidly. Microsoft has been advised by your Internet provider that your network is infected.

To counteract further spread we advise removing the infection using an antispyware program. We are supplying all effected Windows Users with a free system scan in order to clean any files infected by the virus.

Please install attached file to start the scan. The process takes under a minute and will prevent your files from being compromised. We appreciate your prompt cooperation.

Regards,

Microsoft Windows Agent #2 (Hollis)
Microsoft Windows Computer Safety Division

Un faux anti-virus vendu 50 dollars rapporte 35 millions de dollars par mois,
selon (selon Panda Security).

AAE isep

29

La troisième guerre mondiale a commencé !!!

9 July 2008 03:58 GMT

World war III has started! US has invaded Iran! Click here to see the firsthand video!

20000 US soldiers in Iran
Iran USA conflict developed into war
More than 10000 Iranians were murdered
Negotiations between USA and Iran ended in War
Occupation of Iran
Plans for Iran attack began
The Iran's Leader Mahmoud Ahmadinejad declared Jihad
The World War III has already begun
The begining of The World War III
The military operation in Iran has begun
The secret war against Iran
Third War in Iran
Third World War has begun
US Army crossed Iran's borders
US Army invaded Iran
US army is about 20 kilometers from Tegeran
US soldiers occupied Iran
USA attacked Iran
USA declares war on Iran

Just now US Army's Delta Force and U.S. Air Force have invaded Iran. Approximately 20000 soldiers crossed the border into Iran and broke down the Iran's Army resistance. The video made by US soldier was received today morning. Click on the video to see first minutes of the beginning of the World War III. God save us

AAE isep

30

Les nouveaux cybercriminels

Ce qui motive les nouveaux hackers
- Ce n'est plus la notoriété
- Ce n'est plus le défi et l'excitation des attaques
- Ce n'est plus de faire ses preuves

• Ce qui motive aujourd'hui le hacker …

C'est le pognon !!!

31

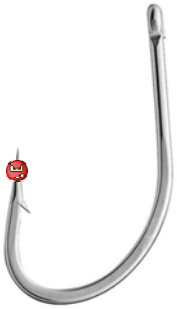
La cybercriminalité

– Le cyberespace, une autre dimension
– La cyberguerre, la menace du 21eme siècle
– La cybercriminalité
  • Les modèles économiques
    – **du Phishing**
    – des Botnets
– La cybersécurité

AAEisep

32

Le phishing (hameçonnage)



PHREAKER **FISHING**

AAEisep

33

1 - L'accroche par e-mail

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DIRECTION GENERALE DES FINANCES PUBLIQUES 05/10/2009

Notification d'impôt - Remboursement

Après les derniers calculs annuels de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement d'impôt de € 178,80.

S'il vous plaît soumettre la demande de remboursement d'impôt et nous permettre de 10 jours ouvrables pour le traitement.

Pour accéder au formulaire pour votre remboursement d'impôt, cliquez

http://adsl-072-156-092-021.sip.asm.bellsouth.net/fr
Cliquez pour suivre le lien

Un remboursement peut être retardé pour diverses raisons. Par exemple la soumission des dossiers non valides ou inscrivez après la date limite.

Le Conciliateur fiscal adjoint

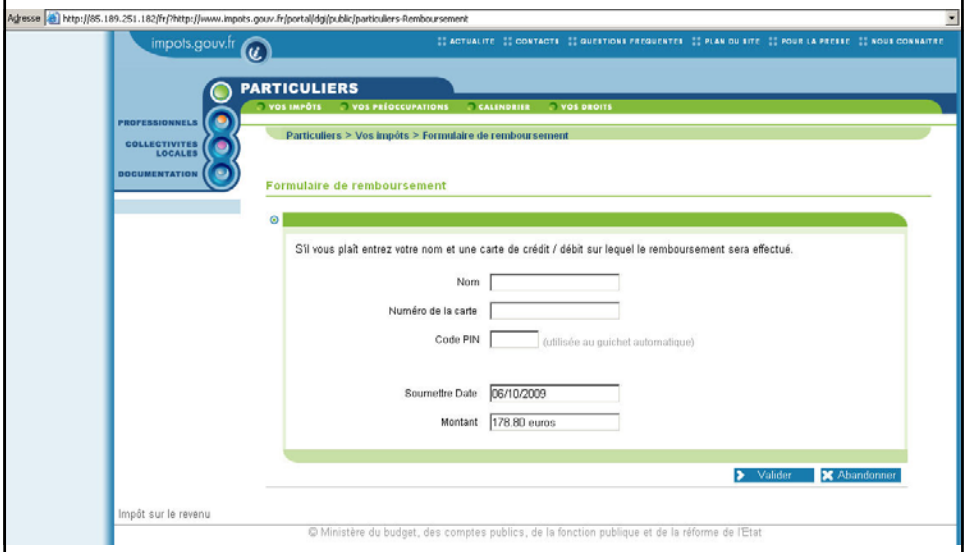
Philippe BERGER

© Ministère du budget, des comptes publics et de la fonction publique

AAEisep

34

2 – La poursuite par le Web



AAEisep

35

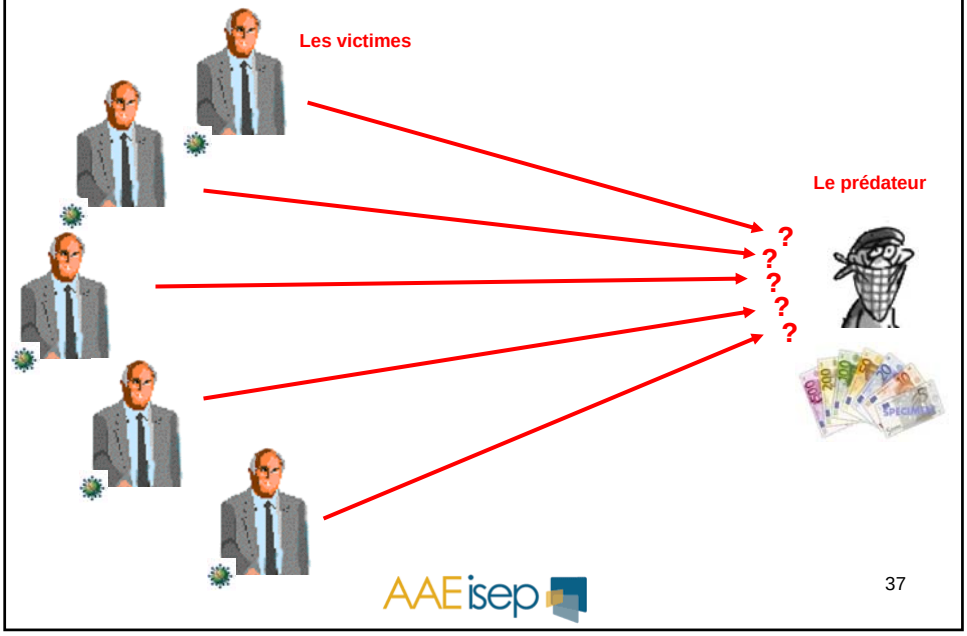
3 – L'arnaque finale

Et encore merci pour vos coordonnées bancaires ! ;-)

AAEisep

36

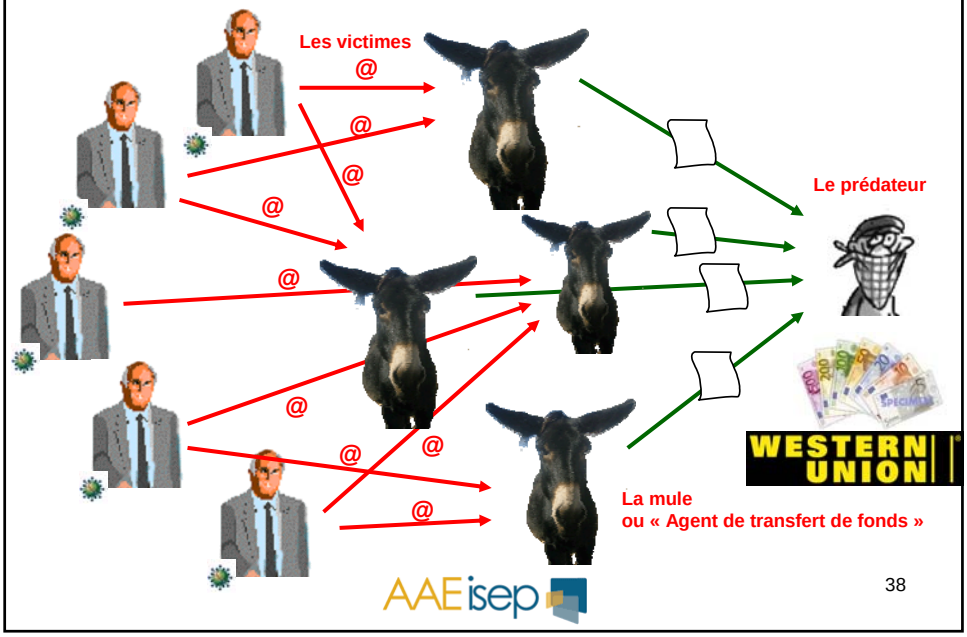
Le modèle économique du Phishing



AAEisep

37

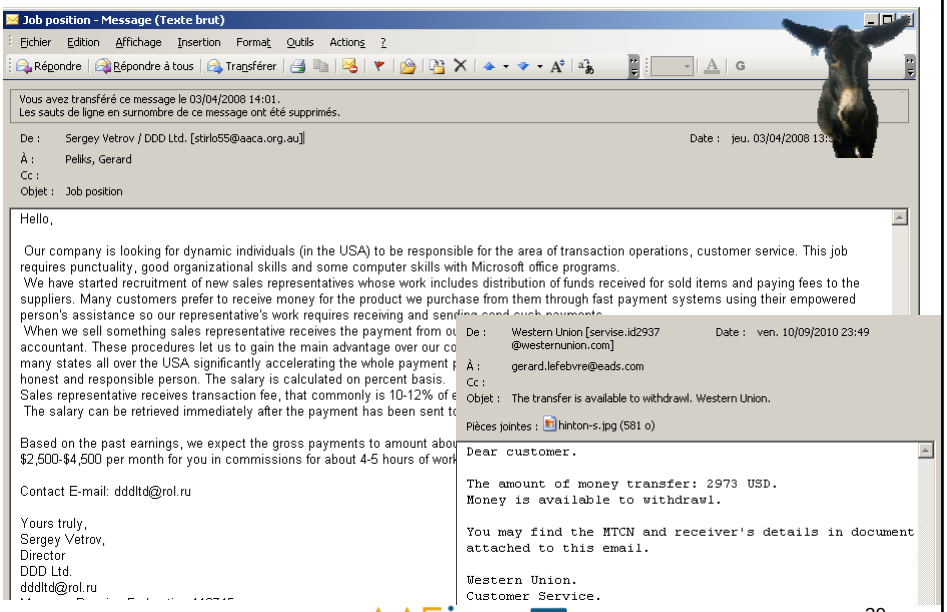
Le modèle économique du Phishing



AAEisep

38

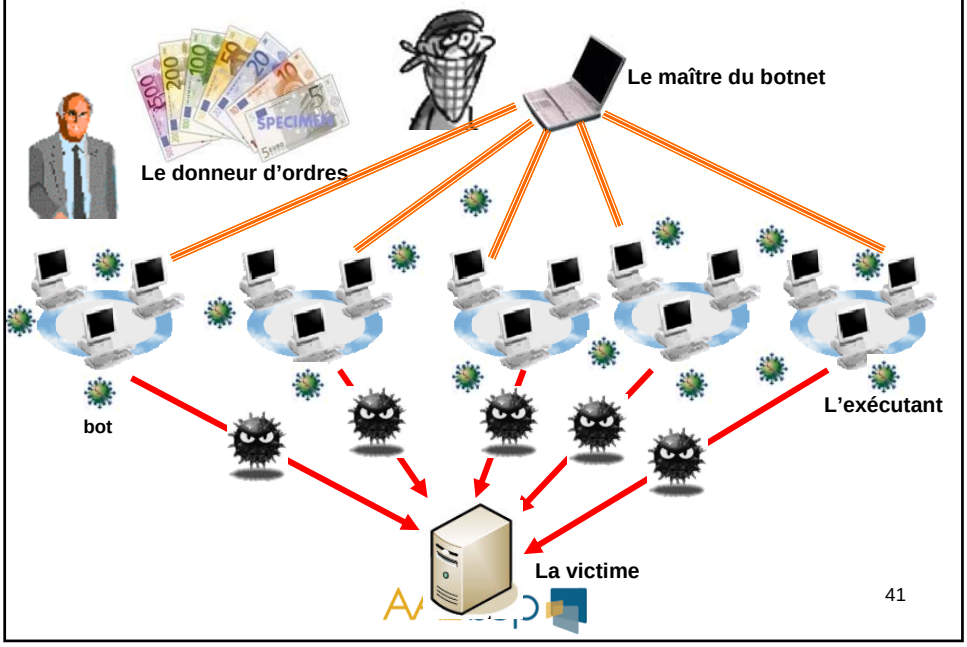
Les mules, un nouveau métier …



La cybercriminalité

- Le cyberespace, une autre dimension
- La cyberguerre, la menace du 21eme siècle
- La cybercriminalité
  - Les modèles économiques
    - du Phishing
    - **des Botnets**
- La cybersécurité

Le botnet



41

Le ransomware qui s'appuie sur des botnets

Vous avez jusqu'à 17 heures, heure locale.

Je vais maintenant lancer une attaque pendant une heure. Celle-ci ne représente qu'un vingtième de la puissance que je peux déployer.

Répondez-moi et je vous communiquerai un numéro de compte sur lequel vous devrez verser immédiatement 7000 €.

Dans l'attente d'une réponse …

42

Petite annonce …

Loue botnet de 15000 PC à la journée.

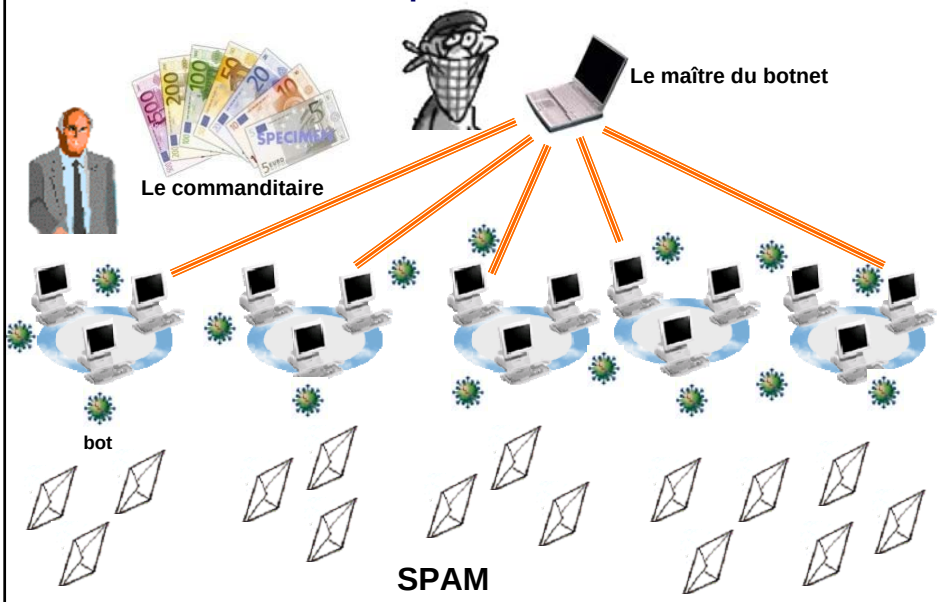
Déni de service garanti !

Satisfait ou remboursé

AAEisep

43

Le modèle économique des botnets



AAEisep

44

200 milliards de spams par jour !!!

200 milliards de spams sont envoyés chaque jour dans le monde

LE MONDE | 09.02.09 | 15h31 • Mis à jour le 10.02.09 | 15h11

Plusieurs études viennent de le confirmer : le spam se porte bien. Les concepteurs d'antivirus Sophos et Symantec ont créé des *"pièges à spams"*, de fausses adresses mails visant à collecter ces courriers électroniques non sollicités envoyés en masse.

Résultat : en 2008, entre 150 et 200 milliards de spams ont été envoyés chaque jour, selon Laurent Heslault, directeur des technologies de sécurité chez Symantec. Cela représente entre 80 % et 90% des mails à destination des particuliers, et même 97 % pour les professionnels, estime Sophos. Le nombre de spams augmente régulièrement, en suivant la courbe croissante des e-mails. Difficile de savoir d'où proviennent ces *"pourriels"*. Seul le dernier expéditeur est facilement identifiable, mais il est dans 95 % des cas l'ultime relais, et non l'origine du spam.

Selon le rapport annuel de la société Sophos, les Etats-Unis restent le plus gros pays émetteur de spams en 2008, malgré une baisse sensible par rapport à 2007 (17,5 %, contre 22,5 % l'année précédente). Le trio de tête est complété par la Russie (7,8 % des envois de spams) et la Turquie (6,9 %). A l'échelle des continents, l'Asie se distingue (36,6 %), devant l'Europe (27,1 %). *"Les principaux émetteurs sont des pays où il y a une masse d'ordinateurs, même s'ils sont bien protégés, ou ceux où ils sont rares, mais très mal protégés"*, explique Michel Lanaspèze, directeur marketing et consultant sécurité chez Sophos.

Un ordinateur peut être infecté en ouvrant une pièce jointe ou en cliquant sur un lien, parfois dissimulé dans une vraie lettre d'informations. Les pirates peuvent ensuite trouver des informations confidentielles ou nous transformer à notre tour en émetteur de spams.

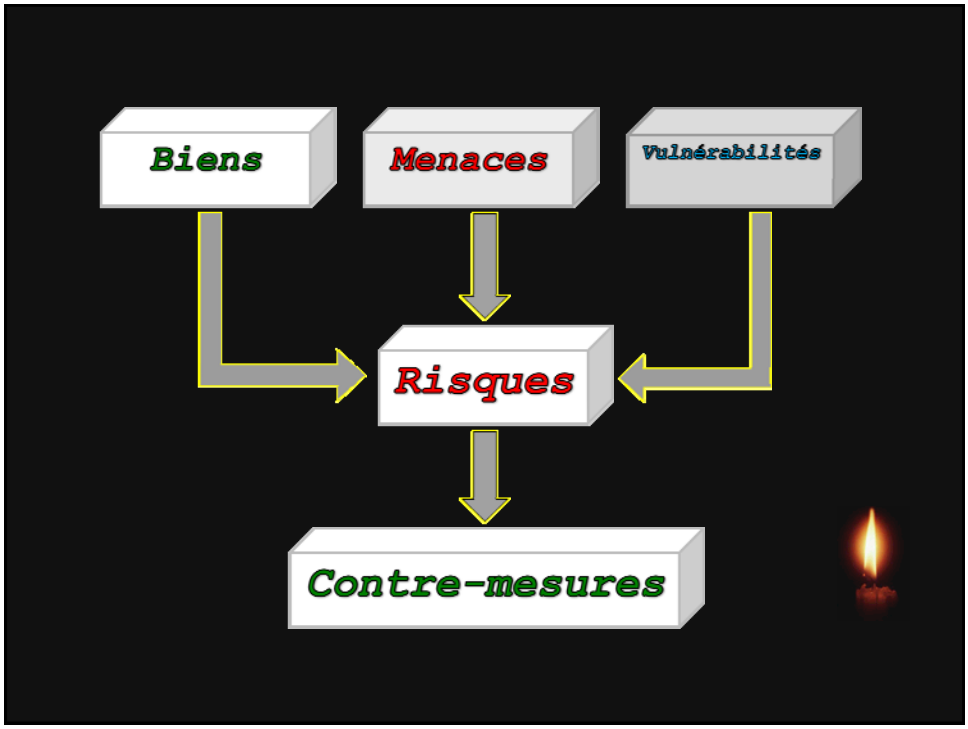
45

La cybercriminalité

- Le cyberespace, une autre dimension
- La cyberguerre, la menace du 21eme siècle
- La cybercriminalité
  - Les modèles économiques
    - du Phishing
    - des Botnets
- **La cybersécurité**

AAE isep

46



La sécurité : le résultat d'un compromis

- La sécurité est un compromis entre
  - Un besoin de protection
  - Le besoin opérationnel qui prime sur la sécurité
  - Les nouvelles technologies : mobiles, cloud, réseaux sociaux …
  - Les ressources financières et les limitations techniques
- La sécurité assure pour les données
  - La disponibilité
  - L'intégrité et l'authenticité
  - La confidentialité
- La sécurité est un process, pas un produit
  - La sécurité, ça se mérite et ça s'apprend

AAEisep

48

La protection absolue d'un PC : une fiction …

Seul un ordinateur éteint, enfermé dans un coffre fort et enterré six pieds sous terre dans un endroit tenu secret peut être considéré comme sécurisé, et encore …

Bruce Scheier

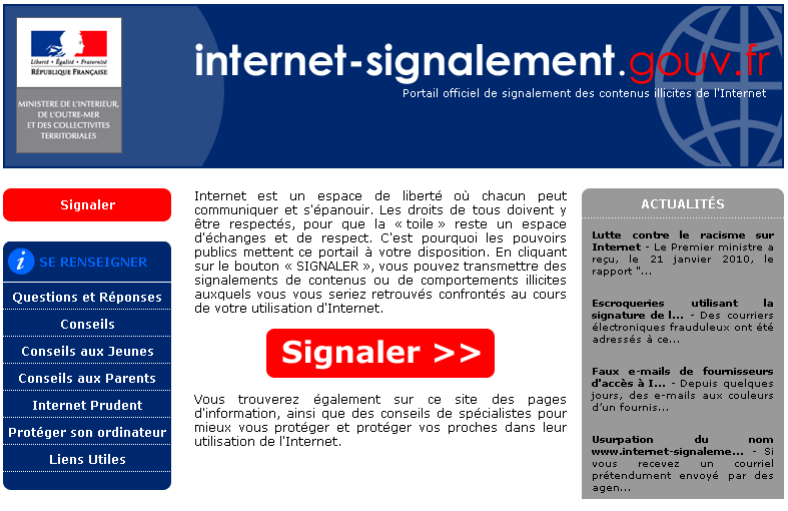
Les entreprises du futur n'auront que deux employés, un homme et un chien. L'homme pour nourrir le chien; le chien pour empêcher l'homme de s'approcher du clavier.

3300 ordinateurs portables sont perdus ou volés dans les 8 plus grands aéroports européens chaque semaine !

AAE isep

49

www.internet-signalement.gouv.fr/

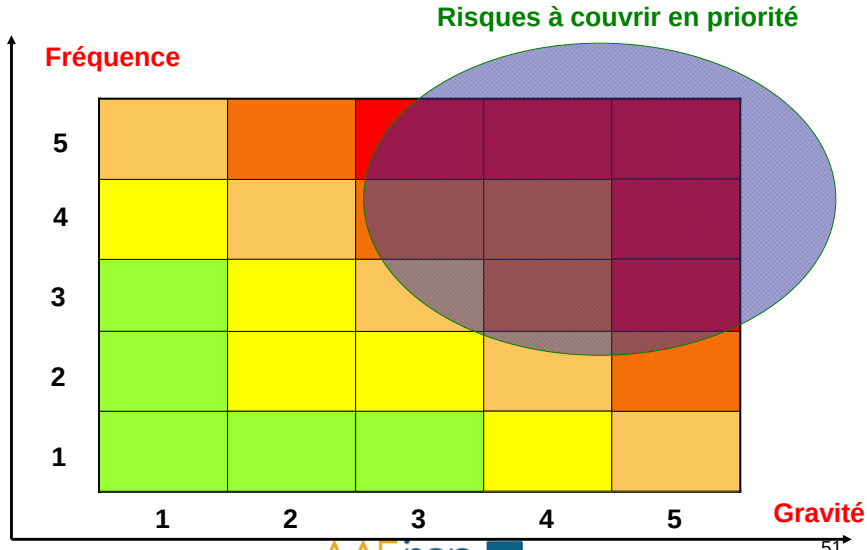


En 2009, collecte de **52 000** signalements
312 ont fait l'objet d'enquêtes nationales
1800 ont été transmises à Europol

AAE isep

50

Cartographie des risques



AAEisep

51

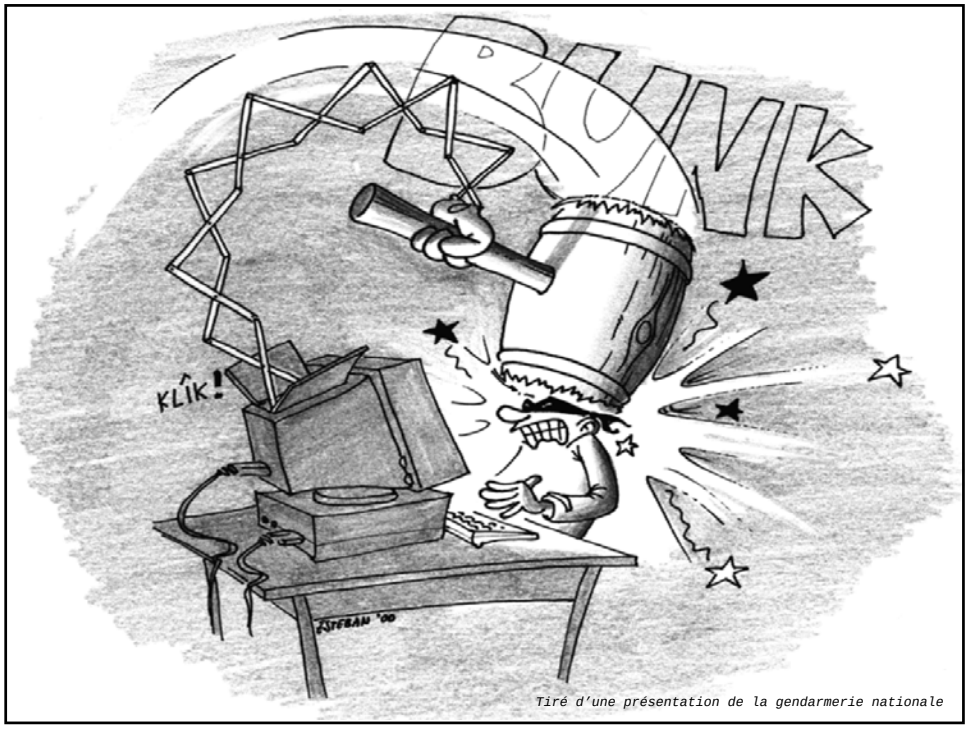
Pourquoi investir dans la sécurité ?

- L'information est une ressource stratégique
- Les menaces portent sur :
  - La confidentialité — **chiffrement**
  - L'intégrité — **hash et chiffrement**
  - L'authenticité — **identification / authentification**
  - La disponibilité — **PCA / PRA**

Outils et expérience !

AAEisep

52



Tiré d'une présentation de la gendarmerie nationale

Questions ?

CASSIDIAN
AN EADS COMPANY

Gérard Peliks
Cyber Security Centre
gerard.peliks@cassidian.com

AAE isep

54