CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

# Panorama de la cybercriminalité année 2012

## Rencontres techniques de la CNEJITA

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

# Le CLUSIF : agir pour la sécurité de l'information

Association **sans but lucratif** (création au début des années 80)

> 600 membres (pour 50% fournisseurs et prestataires de produits et/ou services, pour 50% RSSI, DSI, FSSI, managers…)

**Partage de l'information**

Echanges homologues-experts, savoir-faire collectif, fonds documentaire

**Valoriser son positionnement**

Retours d'expérience, visibilité créée,

Annuaires (Formations, Membres Offreurs)

**Anticiper les tendances**

Le « réseau », faire connaître ses attentes auprès des offreurs

**Promouvoir la sécurité**


***Logo pour vos actions commerciales, votre site web***

**Adhérer…**

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

# Groupes de travail en progression

## Les groupes actifs en 2012

- Codes malveillants : malware
- Evaluation Financière des Incidents de Sécurité - EFIS
- Fiches de sécurité pour la micro-informatique
- Gestion de clés cryptographiques
- Incidents de sécurité et l'ISO/IEC 27035
- MEHARI Pro
- Menaces Informatiques et Pratiques de Sécurité en France (Edition 2012)
- Panorama de la cybercriminalité
- PCI-DSS
- Sécurité des Applications Web : Défense en profondeur des applications Web
- Sécurité des Outils de Communication

… et Espaces dédiés

## Espaces de travail actifs en 2012

- Espace Menaces
- Espace Méthodes
- Espace RSSI

RSS/docs CLUSIF
RSS/actus CLUSIF
RSS/actus CLUSIR
RSS/Call For Paper

*Surveillez les flux RSS, le facebook.com/clusif, linkedIn, twitter…*

# Sélection des événements médias

Illustration

- d'une émergence,
- d'une tendance,
- d'un volume d'incidents.

Cas particuliers:

- impact ou enjeux,
- cas d'école.


Depuis 2009, élargissement au risque numérique (événements accidentels, faits de société).

# Contributions au Panorama 2012

Sélection réalisée par un groupe de travail pluriel issu du privé et de l'administration:

- Accenture
- BSSI
- CEIS
- CERT Devoteam
- CERT-IST
- CERT LEXSI
- Hervé Schauer Consultants
- IBM France
- McAfee Labs
- Orange Labs
- Solucom
- Verizon
- Direction Centrale de la Police Judiciaire \ OCLCTIC
- Gendarmerie Nationale \ STRJD
- Ministère des Affaires Sociales
- Sûreté du Québec

*Le choix des sujets et les propos tenus n'engagent pas les entreprises et organismes ayant participé au groupe de travail*

# Agenda du Panorama 2012

- 5 sujets en bref
  - 2012, ni la fin du monde, ni la fin des accidents…
  - Etat: quelle doctrine pour les cyber-conflits ?
  - Les attaques ciblées: une autopsie de l'année 2012
  - Hack As A Service - Les offres pros enfin accessibles à tous…
  - Les Botnet à toutes les sauces
- Mobilité, la ruée vers l'or version 3G

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

# 2012, ni la fin du monde, ni la fin des accidents…

accidentel

| | |
|---|---|
| Windows Azure | *Interruption de service sur le Cloud au niveau mondial* |
| **Knight Capital** | *Bug logiciel, **perte de 440 Millions de dollars** en quelques minutes* |
| Royal Bank of Scotland | *Incident informatique, des millions de cartes bancaires inopérantes* |
| Orange | *Panne logicielle, **plusieurs millions d'abonnés mobiles privés de communication*** |
| Inde | *Panne d'électricité, **670 millions d'indiens privés d'électricité*** |
| **Amazon** | ***Pannes multiples dans le Cloud**, perturbation des services associés* |
| France Telecom | *Rupture de fibre, **70 000 clients privés de communications*** |
| Canton de Vaud, Suisse | *Bug informatique, perturbation des élections fédérales* |
| Google | *Panne informatique, perturbation des services associés* |
| France Telecom | *Incendie sur un pont à Rouen, fonte de câbles, coupure de certaines communications* |
| Etat de New York | *Tempête Sandy* |
| Ville de Moscou | *Rupture de câble, perturbation dans le contrôle des satellites civils* |

# Knight Capital - Que s'est-il passé ?

accidente!

Le principe du trading haute fréquence : acheter au moins cher et vendre au plus offrant toutes les microsecondes pour dégager une faible marge de très nombreuses fois

6 aout 2012 - Knight déploie une version de test de son logiciel de trading; version développée rapidement

La version s'emballe: de multiples erreurs dont un algorithme qui achetait au plus cher et revendait au moins cher engendre des moins-value



En 45 minutes : 4,5 milliards de dollars d'actions achetées, des cours d'action modifiés à + de 150%

Au final 440 Millions de dollars sont perdus pour Knight Capital. La société frôle la Banqueroute

**Nous pensons aux catastrophes mais rarement au bug…**

# Etats: quelle doctrine pour les cyberconflits ?

- Certains Etats (Iran, Japon, Turquie…) ne cachent pas leur objectif de créer des unités offensives. Israël considère le cyberespace comme un champ de bataille à part entière.
- D'autres affirment se doter d'importantes capacités défensives (Brésil, Corée du Sud…).
- Pour le Royaume-Uni, le droit des conflits armés s'applique nécessairement aux opérations dans le cyberespace. Reste à déterminer ce qu'est une réponse proportionnée en cas de cyberattaque.
- Les Etats-Unis affichent l'attitude la plus décomplexée en ce domaine. Ils disent se réserver le droit de riposter en cas de « menace imminente » même si aucune perte humaine n'est constatée. C'est une sorte de légitime défense préventive.
- L'Inde ouvre son école de cyberguerre.
- La France recrute et crée une réserve opérationnelle et citoyenne.

# Etats: quelle doctrine pour les cyberconflits ?

- Publication importante : Draft du Manuel de Tallinn qui réunit les contributions d'experts australiens, britanniques, américains, canadiens et néerlandais.
- Droit existant: Article 461-28 du code pénal, qui découle de la cours pénale internationale. Il devrait s'appliquer aux cyberattaques :

*"Est puni de vingt ans de réclusion criminelle le fait de lancer une attaque délibérée en sachant qu'elle causera incidemment :*

1) *Des dommages aux biens de caractère civil, qui seraient manifestement disproportionnés par rapport à l'avantage militaire concret et direct attendu de l'ensemble de l'attaque ;*
2) *Des dommages étendus, durables et graves à l'environnement naturel, qui seraient manifestement disproportionnés par rapport à l'avantage militaire concret et direct attendu de l'ensemble de l'attaque."*

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

# Attaques ciblées: autopsie pour l'année 2012
# Qu'ont toutes ces attaques en commun ?

Attribuer une attaque :
est-ce vraiment possible ?

- Une origine commune ?
- Une cible de même nature ?
- Un mode opératoire commun ?
- Des moyens techniques similaires ?
- Des objectifs proches ?
- Des contre-mesures convergentes ?
- Un traitement médiatique particulier ?
- Des conséquences communes ?

# Attaques ciblées: autopsie pour l'année 2012
## Qu'ont toutes ces attaques en commun ?

Une origine commune ? ✗

Attribution chancelante: le commanditaire n'est jamais tout à fait certain

Une cible de même nature ? ✗

Un seul point commun : une corrélation entre ces attaques et des tensions préexistantes (géopolitiques, économiques, militaires, sociétales…)

Un mode opératoire commun ? ✗

Lister les modes opératoires observés reviendrait à écrire un livre sur la sécurité

Des moyens techniques similaires ? ✗

La maturité technique est aléatoire (du plus simpliste au plus sophistiqué)

# Attaques ciblées: autopsie pour l'année 2012
## Qu'ont toutes ces attaques en commun ?

Des objectifs proches ? ✗

Des codes hautement polyvalents dont l'action réelle est difficile à cerner

Des contre-mesures convergentes ? ✗

Chaque attaque laisse présager une contre-mesure différente (retour aux fondamentaux ou innovations)

Un traitement médiatique particulier ? ✗

Trop de sensationnalisme. C'est préjudiciable au secteur de la sécurité : le contraire de la sensibilisation

Des conséquences communes ? ☺

On se focalise sur des menaces externes. On recherche des boucs émissaires : le BYOD, l'Iran, Huawei, la NSA…

## Hack As A Service

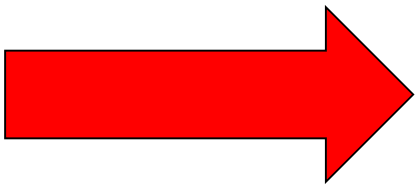
## Les offres pros enfin accessibles à tous…

Les forums tout public ne sont plus privilégiés :

- Perte de temps (trop de « newbies »),
- Manque de confidentialité (trop d'échanges directs, sans garantie sur la qualité du contact),
- Perte d'argent (l'acheteur a tendance à discuter le prix),
- Trop d'arnaqueurs (rippers).

L'offre a évoluée:

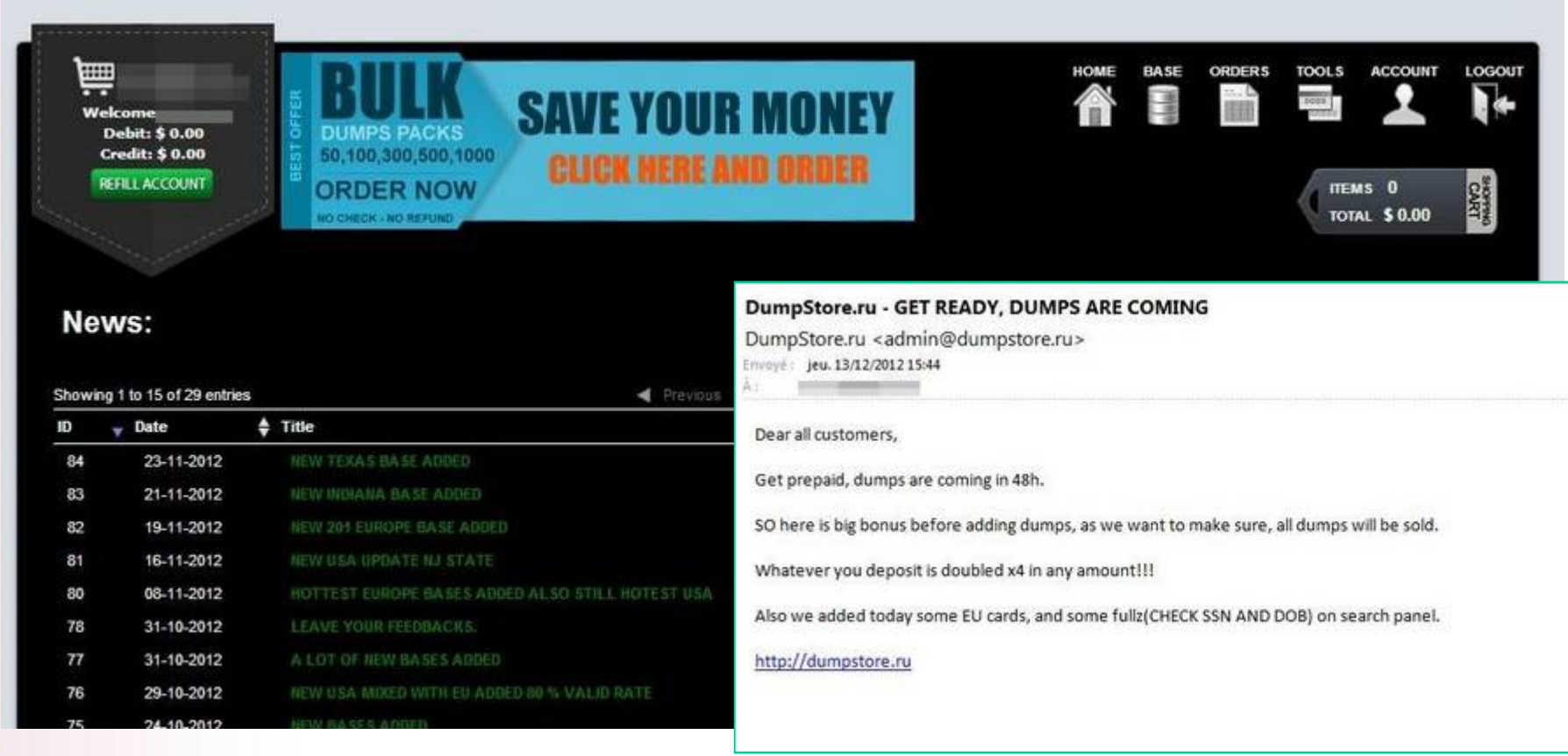
- Espaces privés,
- Forums privés payants,
- Forums privés payants avec parrainage,



Boutiques en ligne.
Campagnes publicitaires.

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

# Hack As A Service
## Les offres pros enfin accessibles à tous…




J'achète en un clic, je paie en un clic et reçoit ma livraison par mail.

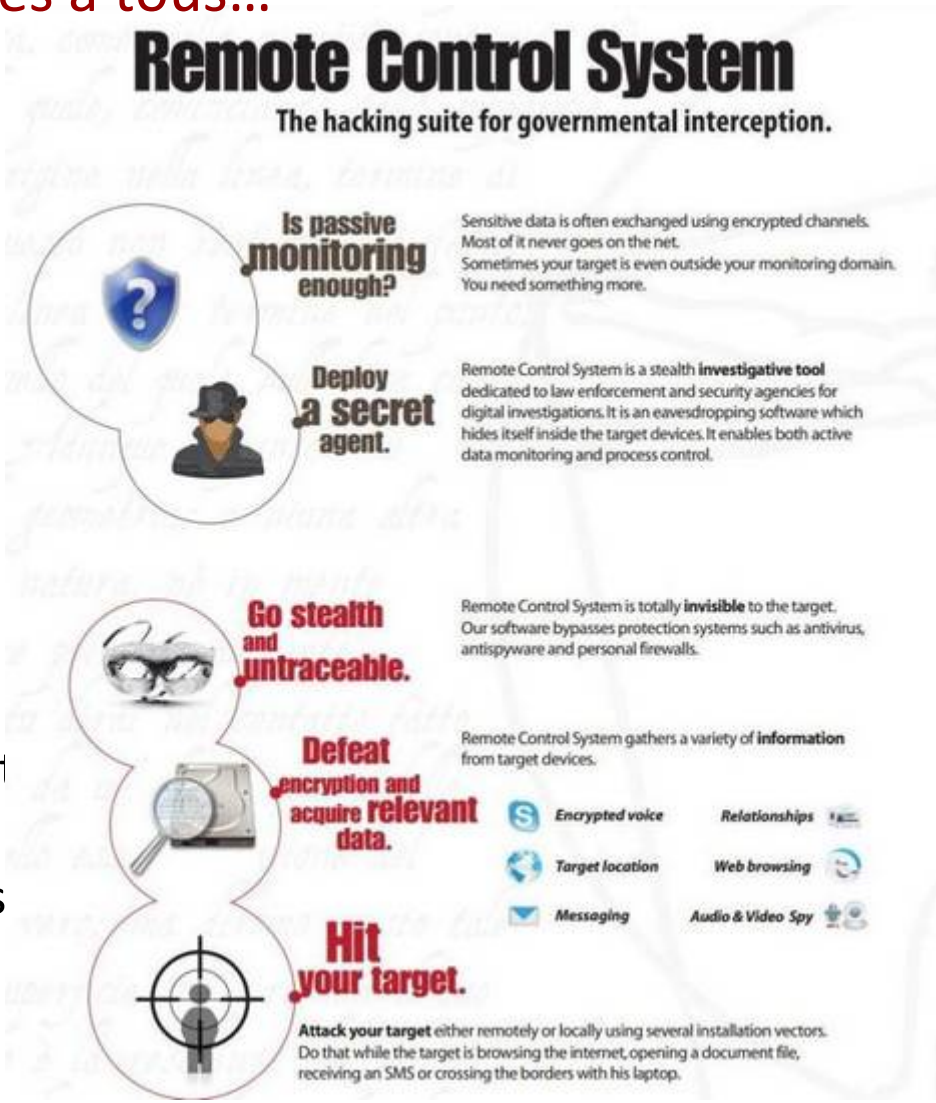
Les promotions me sont annoncées.

# Hack As A Service
## Les offres pros enfin accessibles à tous…

*… et d'étranges sociétés de sécurité voient le jour…*

*Elles offrent des services pour lesquels on a parfois du mal à cerner les acheteurs potentiels.*

Sous couvert de s'adresser aux gouvernements et à leurs officines, ne sommes-nous pas en droit de nous interroger sur le fait qu'elles pourraient se laisser tenter par d'autres négociations auprès d'acheteurs moins honnêtes ?
Ne dit-on pas que l'argent n'a pas d'odeur ?



# Les Botnet à toutes les sauces
## Acteurs potentiels

Développeurs de logiciels malveillants

Attaquants de sites Web

Gestionnaires de plateformes d'exploits

Traffers

Développeurs/vendeurs de plateformes d'exploits

Spammers

Clients / Collecte des tickets de paiement

Autres botnets utilisés comme mode de distribution

Blanchiment

# Les Botnet à toutes les sauces
## Acteurs potentiels

- Ransomware
  - Les visuels sont souvent copiés d'une famille à l'autre.
  - Certaines versions sont issues de kits à configurer…
  - De nouvelles versions de chaque famille parfois tous les 2 mois.
  - Un site d'information: http://stopransomware.fr/
- Plateformes d'exploit (Blackhole, Nuclear Pack, Sweet Orange, Phoenix, etc.),
- Sality: scan de tout l'IPv4 à la recherche de composants PABX IP (serveurs SIP),
- XDocCrypt/Dorifel: il cible les Pays-Bas,
- Sykipot: il cible les certificats d'identification stockés sur carte à puce,
- Gozi Prinimalka: il mène une campagne massive contre les banques US,
- Carberp: çà continue malgré des arrestations en Russie,
- Nitol, DNS Changer , ZeroAccess, etc.

# Mobilité: la ruée vers l'or version 3G

**Fabien COZIC**

Consultant en cybercriminalité - CERT-LEXSI

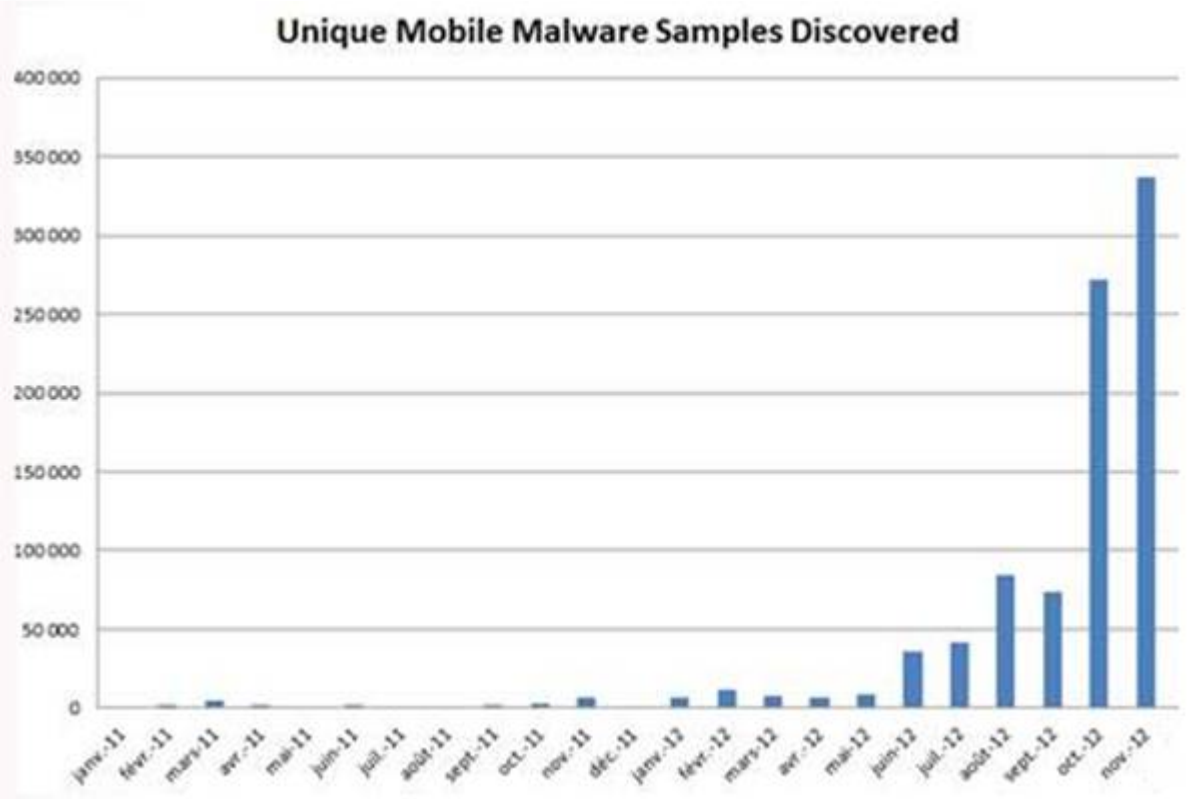
# Agenda

1. Explosion du nombre de malware sur Smartphone
   1. Croissance inédite des logiciels malveillants sur mobile
   2. L'iOS n'est plus épargné
   3. Android reste la plateforme de prédilection des cybercriminels
   4. La R&D de Cybercrime Co. fonctionne à plein
2. A la frontière de la légalité et de la criminalité
   1. La ruée vers les informations personnelles est en cours
   2. Affaire des applications électorales très indiscrètes
   3. Projet « Contextual Awareness » d'Intel
3. Les problématiques de la technologie NFC se font plus pressantes
   1. Vulnérabilité des puces MiFare
   2. Les transactions bancaires par NFC sont insuffisamment sécurisées

**Conclusion**

# 1. Explosion du nombre de malware sur Smartphone

## 1.1 Croissance inédite des logiciels malveillants sur mobile

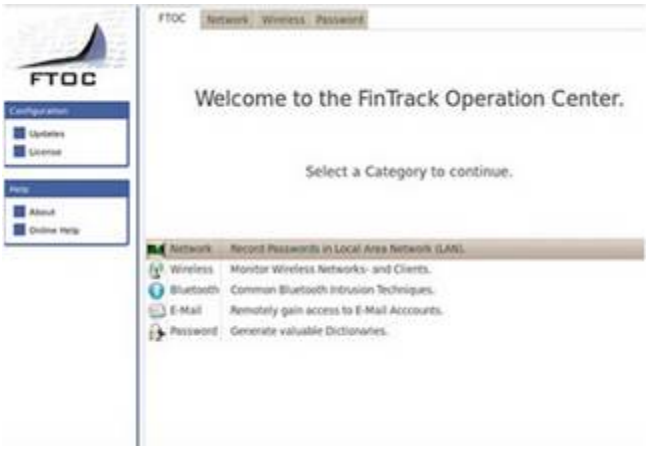



Source FPaget/McAfee Labs

## 1.2 L'iOS n'est plus épargné

Finfisher peut prendre le contrôle d'un Windows Phone, d'un Android, d'un Symbian et d'un iOS

- Possibilité à l'attaquant d'écouter les conversations et de localiser l'appareil
- Installation de l'application via un lien compromis
- La société de sécurité à l'origine du programme dénonce le vol d'une de ses copies de démonstration

# 1.3 Android reste la plateforme de prédilection des cybercriminels

***FakeInst***

***SMSZombie***

***NotCompatible***

Découverte de SpamSoldier sur Android

- Le botnet de spam se sert des appareils infectés pour envoyer des sms surtaxés par vagues de 100 toutes les minutes
- Il dissimule son activité en masquant l'envoi des messages
- Il bloque tous les messages entrants pendant la campagne pour empêcher les opérateurs de prévenir la victime

**Et ce n'en est qu'un parmi d'autres !**

***LuckyCat***

***Android.Bmaster***

***Marketpay***


Message incitant à l'installation de SpamSoldier

# Infiltration courante des plateformes officielles

Infection via applications pour l'installation de jeux populaires (une version gratuite du jeu est installée pour tromper l'utilisateur)

- « Repack » d'applications légitimes sur les marchés officiels, spécialement Android.

- 23 applications du top 500 de Google Play classées comme dangereuses

-Le marché d'applications Android ne dispose pas encore d'un système efficace de vérification -> Google Bouncer est vulnérable (Jon Oberheide & Charlie Miller, Juin 2012)

- La politique de vérification systématique sur l'Apple Store semble porter ses fruits jusqu'à aujourd'hui

# 1.4 La R&D de Cybercrime Co. fonctionne à plein

Infection via QR Code

Infection via drive-by download


Développement des ransomware sur Smartphone

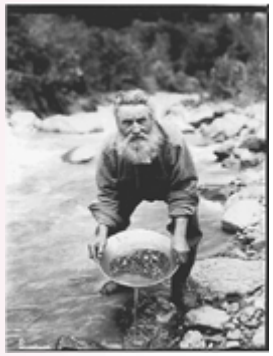
## 2. A la frontière de la légalité et de la criminalité

### 2.1 La ruée vers les informations personnelles est en cours

Le nombre d'Adware visant à recueillir les informations personnelles des utilisateurs d'Android a progressé de 583 % sur trois mois.

30 000

Juin 2012



175 000

septembre 2012

## 2.2 Affaire des applications électorales très indiscrètes Obama / Romney

Application pour fédérer autour du candidat

- Mais aussi récupérer la localisation GPS, information sur l'identification de l'appareil, contenus des cartes SD, accès au carnet d'adresse et même accès aux matériels audios et vidéos

## 2.3 Projet « Contextual Awareness » d'Intel

- Application installée « volontairement » avec un accès total au mobile et à son contenu
- Détection des activités de l'utilisateur du Smartphone
- Recoupement des données environnementales et des données d'utilisation

# 3. Les problématiques de la technologie NFC se font plus pressantes

## 3.1 Vulnérabilité des puces MiFare (Septembre 2012)

- Exploitation via une application Android
- Réécriture des blocs de données (*rewrite*)
- Voyages gratuits et illimités !

## 3.2 Les transactions bancaires par NFC sont insuffisamment sécurisées

- Les standards bancaires ne sont pas prévus pour une utilisation sans fil
  - Probable incompatibilité avec le standard PCI-DSS
- Possibilité de concevoir un appareil pour lire les flux de données lors des phases actives de la puce
  - Pas de chiffrement du container NFC
  - Pas de chiffrement des communications
- Possibilité de pousser un malware sur Android par tag NFC

# Conclusion

- Un cap décisif a été franchi par les cybercriminels: un filon a été découvert et c'est une véritable ruée sur le mobile qui est en cours

- L'absence de définition de règles claires dans la collecte d'informations personnelles même acceptées permet la dérive des pratiques commerciales

- On assiste à l'application stricte des modes opératoires connus sur Internet et employés pour la fraude sur un nouveau terrain de chasse

- L'année 2013 devrait confirmer cette tendance avec une accélération des infections grâce entre autre à l'amélioration des procédés d'ingénierie sociale

# Questions / Réponses

L'intégralité du panorama 2012 du CLUSIF est disponible au téléchargement depuis notre site :
https://www.clusif.asso.fr/index.asp

à la page:
https://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER-CRIMINALITE