CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

Panorama de la cybercriminalité année 2011

Paris, 11 janvier 2012

Evénement organisé en partenariat avec :

Orange Business Services **TelecityGroup**

orange Business Services

TelecityGroup
Where content meets connectivity

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

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

… et des Espaces dédiés

Espaces de travail actifs en 2011

- Espace Méthodes
- Espace Menaces
- Espace RSSI

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

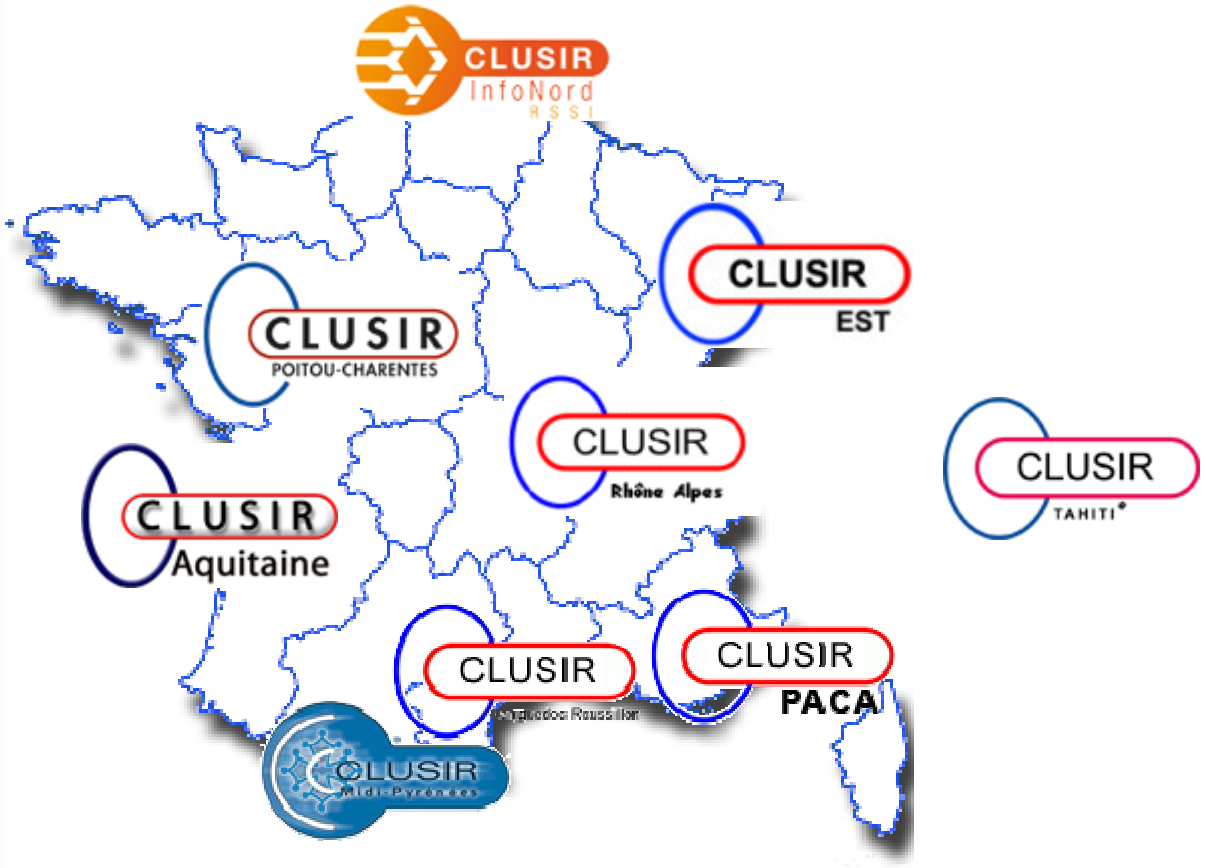
Nouveaux GT en annonce, surveillez les flux RSS...

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Une collaboration à l'international…

Des créations en cours : Ethiopie, pays du Maghreb…

Des actions en région…



Lancement imminent : CLUSIR 974 (Réunion)…

Objectifs du panorama

Apprécier l'émergence de nouveaux risques et les tendances de risques déjà connus

Relativiser ou mettre en perspective des incidents qui ont défrayé la chronique

Englober la criminalité haute technologie, comme des atteintes plus « rustiques »

Depuis 2009, élargissement au risque numérique

- Evénements accidentels 

- Faits de société et comportements pouvant induire / aggraver des actions cybercriminelles 

Sélection des événements médias

Illustration

d'une émergence,

d'une tendance,

d'un volume d'incidents.

Cas particulier

Impact ou enjeux,

Cas d'école.

Contributions au Panorama 2011

Sélection réalisée par un groupe de travail pluriel : assureur, journaliste, officier de gendarmerie et police, offreur de biens et de services, RSSI…

- Best Practices-SI
- CEIS
- Hervé Schauer Consultants
- DEVOTEAM\CERT
- McAfee Labs
- LEXSI
- Orange
- SNCF
- Solucom

- Bundeskriminalamt, Unité SO 43 -117
  (National High Tech Crime Unit)
- Direction Centrale de la Police Judiciaire \ OCLCTIC
- Gendarmerie Nationale \ STRJD
- Ministère des Affaires Sociales
- Police Judiciaire Fédérale de Belgique\Federal Computer Crime Unit
- Sûreté du Québec

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

Interventions, Panorama 2011 (1/3)

- Cybercrime : infos et intox 2011

  M. Olivier CALEFF

  ✉ Responsable du CERT DEVOTEAM
  Olivier.Caleff@devoteam.com

- Moyens de paiement : innovations… dans la fraude

  M. Pierre CARON

  ✉ Expert sécurité – ORANGE
  pierre.caron@orange.com

- La mobilité : les menaces se précisent

  M. Pierre CARON

  ✉ Expert sécurité – ORANGE
  pierre.caron@orange.com

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Interventions, Panorama 2011 (2/3)

- Confiance sur Internet : les autorités de certification compromises

M. Gérôme BILLOIS

✉ Manager Sécurité et Risk Management - SOLUCOM

Gerome.BILLOIS@solucom.fr

- Ruptures de service : les accidents aussi !

M Gérôme BILLOIS

✉ Manager Sécurité et Risk Management – SOLUCOM

Gerome.BILLOIS@solucom.fr

- L'Hacktivisme en 2011 : entre enfantillage et conscience politique

M. François PAGET

✉ Chercheur de Menaces – McAfee Labs

Francois_Paget@McAfee.com

Interventions, Panorama 2011 (3/3)

- Evénements judicaires et débats juridiques

  M. Eric FREYSSINET

  ✉ Chef de la division de lutte contre la cybercriminalité – Gendarmerie Nationale \STRJD
  eric.freyssinet@gendarmerie.interieur.gouv.fr

- Hacking dans le biomédical

  M. Eric GROSPEILLER

  ✉ FSSI – Ministère du Travail, de l'Emploi et de la Santé
  Eric.GROSPEILLER@sante.gouv.fr

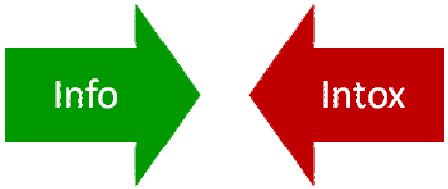
- SCADA, services de secours, systèmes d'armes : tous ciblés

  M. Eric GROSPEILLER

  ✉ FSSI – Ministère du Travail, de l'Emploi et de la Santé
  Eric.GROSPEILLER@sante.gouv.fr

Agenda du Panorama 2011

- Cybercrime : infos et intox 2011
- Moyens de paiement : innovations… dans la fraude
- La mobilité : les menaces se précisent
- Confiance sur Internet : les autorités de certification compromises
- Ruptures de service : les accidents aussi !
- L'Hacktivisme en 2011 : entre enfantillage et conscience politique
- Evénements judicaires et débats juridiques
- Hacking dans le biomédical
- SCADA, services de secours, systèmes d'armes : tous ciblés



en 2011

Olivier CALEFF

Responsable du CERT DEVOTEAM

Que s'est il passé en 2011 ?

Cette conférence de 2h30 sera l'occasion de présenter certains sujets d'actualité très médiatisés mais aussi des thèmes qui ne font pas encore de buzz mais qui ont un enracinement profond et que le CLUSIF souhaite exposer.

Il s'est passé plein de choses, mais il s'en est dit encore plus !

Que s'est il passé **de grave** en 2011 ?

Plein de choses, mais il s'en est dit bien plus !

Et de ***vraiment*** grave ?

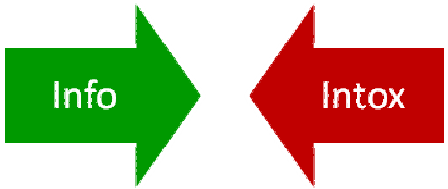
Les vraies questions :

- Comment évaluer la **pertinence** d'une information ?
- Comment estimer son **impact** sur le moment ?
- Comment estimer son impact à **long terme** ?

Essayons de remettre tout cela en perspective

Chronologie :

- Il se produit un événement « sécurité »
- Quelqu'un en parle quelque part
- L'information est reprise, relayée …
  commentée, déformée …
  extrapolée, mise hors contexte



Des attaques contre des Institutions et contre des grands comptes

Profondes brèches de sécurité

- Epsilon (mars), Sony (juin)

Mise en péril de fondamentaux

- Comodo et RSA (mars)
- DigiNotar (août), KPN (novembre)

Sur une longue période

- Bercy (annonce en mars)
- AREVA (annonce en septembre)

En réponse à ces attaques

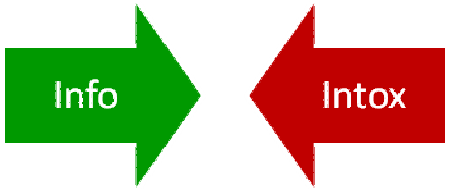
Une **communication officielle** pas toujours réussie

Une volonté de communiquer mais **limitée**

Un dépôt de plainte **pour la forme**

Beaucoup de buzz, mais pas pour rien cette fois ?

- La forme pour masquer le fond ?
- Une information qui « fuite » volontairement ?



Un gestion de crise **(in)adaptée**

Et un vrai travail de fond en réponse

Poursuite de l'industrialisation des attaques

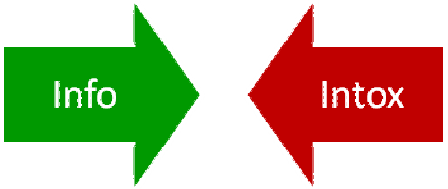
Délocalisation complète des attaques et des traitements

- Un « flash mob » malveillant fortement mobilisateur
- Une réactivité très rapide

Comme pour le Déni de Service

- Un rapport de force en faveur des attaquants
- Des ressources peu onéreuses

Enfin l'année des malwares sur mobiles ?



Les botnets de téléphones mobiles

- Une réalité asiatique qui va s'étendre

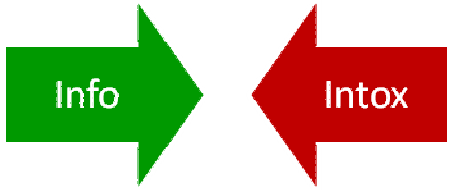
Les outils de DDoS sur mobile

- LOIC (Low Orbit Ion Cannon)

Les centaines d'applications malveillantes sur mobiles

- Les "solutions" apparaissent

Le cas de Carrier IQ



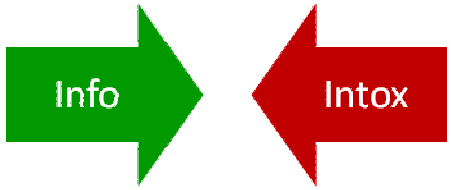
Découverte de Trevor Eckhart en novembre 2011

- Android
- Dénégations de la société
- Comment prouver ?
  - Le reverse engineering est il autorisé ?

FUD – Fear, Uncertainty and Doubt

Ce qui caractérise la communication de certains …

- Etudes empreintes de catastrophisme
  - *"la cybercriminalité dépasse le trafic de drogues"*
- Buzz sur-amplifié



Décalage certain entre :

- Des découvertes
- Les interprétations qui en sont faites

Exemples de décalages

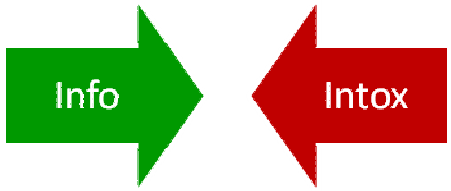
Stuxnet, SCADA et toute l'informatique industrielle

La mobilité et les mouchards

Mais aussi les systèmes de surveillance

- sur Internet
- sur "téléphones" portables

Ou les possibilités offertes de l'Internet des objets

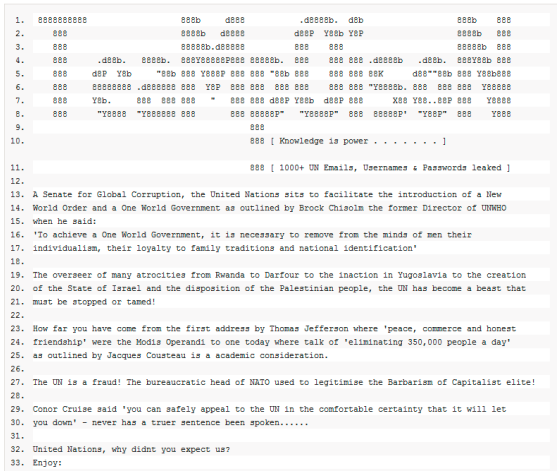


Sans oublier les bons vieux cookies

Modes de diffusion de l'information

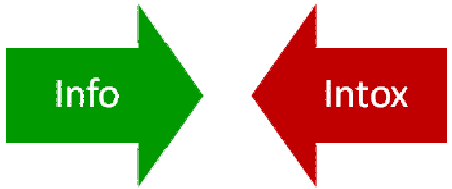
2011 - l'année des sites de copie

- PasteBin
- DropBox
- PasteHTML
- MegaUpload



```
888888888                888b     d888          .d8888b.  d8b                 888b    888
  888                    8888b   d8888         d88P  Y88b Y8P                 8888b   888
  888                    88888b.d88888         888    888                     88888b  888
  888     .d88b.  8888b.  888Y88888P888 88888b.  888    888 888 .d8888b   .d88b.  888Y88b 888
  888    d8P  Y8b     "88b 888 Y8888P 888 888 "88b 888    888 888 88K      d88""88b 888 Y88b888
  888    88888888 .d888888 888  Y8P  888 888  888 888    888 888 888 "Y8888b. 888  888 888  Y8888
  888    Y8b.     888  888 888   "   888 888 d88P Y88b  d88P 888      X88 Y88..88P 888   Y888
  888     "Y8888  "Y888888 888       888 88888P"   "Y8888P"  888  88888P' "Y88P"  888    Y888
                                                   888
                                                   888 [ Knowledge is power . . . . . ]

                                                   888 [ 1000+ UN Emails, Usernames & Passwords leaked ]

A Senate for Global Corruption, the United Nations sits to facilitate the introduction of a New
World Order and a One World Government as outlined by Brock Chisolm the former Director of UNWHO
when he said:
'To achieve a One World Government, it is necessary to remove from the minds of men their
individualism, their loyalty to family traditions and national identification'

The overseer of many atrocities from Rwanda to Darfour to the inaction in Yugoslavia to the creation
of the State of Israel and the disposition of the Palestinian people, the UN has become a beast that
must be stopped or tamed!

How far you have come from the first address by Thomas Jefferson where 'peace, commerce and honest
friendship' were the Modis Operandi to one today where talk of 'eliminating 350,000 people a day'
as outlined by Jacques Cousteau is a academic consideration.

The UN is a fraud! The bureaucratic head of NATO used to legitimise the Barbarism of Capitalist elite!

Conor Cruise said 'you can safely appeal to the UN in the comfortable certainty that it will let
you down' - never has a truer sentence been spoken.....

United Nations, why didnt you expect us?
Enjoy:
```

Qui vérifie la légitimité des données publiées ?



A qui profite le crime … ?

Qui peut tirer partie des info/intox ?

- Les médias, éditeurs, gouvernements, pirates ?
- A quelle vitesse l'information se propage-t-elle ?
- A qui se fier … ?

Comment s'en protéger ?

Evolution depuis 2007 ?

Synthèse

On part d'une information peut-être vraie …

… et on termine avec un buzz planétaire

Vulnérabilité, fuite d'information, découverte, annonce

Sachons analyser et déduire un impact réel

Et si on ne sait pas, fions-nous à ceux qui savent !

Et maintenant, place à de vraies informations qualifiées avec Pierre Caron !

Bonne résolution pour 2012

Soyez *AWARE !*

Si vous réfléchissez avant de cliquer … alors

Ne partez pas d'information "retweetée"

Corrélez les sources

Moyens de paiement : innovations…dans la fraude

Pierre CARON

Expert Sécurité

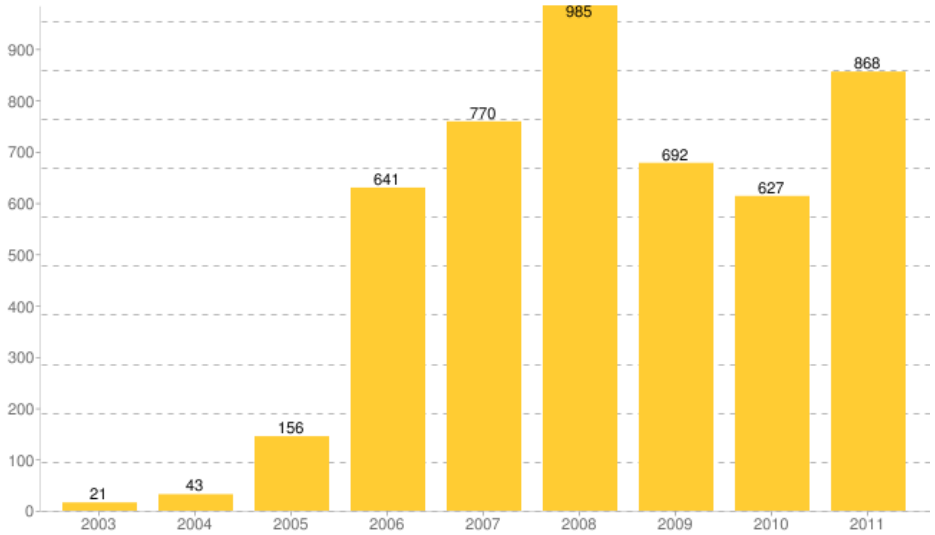
Orange

Fuites d'information : un mauvais cru 2011

Après une accalmie, la tendance repart à la hausse

Cette hausse n'est pas due à un seul méga-contributeur :

-Sony PlayStation Network : 77M
-Sony Online Entertainment : 24,6M
-Tianya : 40M
-SK Communications : 35M
-Steam (Valve, Inc) : 35M
-7k7k : 20M
-Care2 : 17,9M
-Nexon Korea Corp : 13,2M



Recensement des incidents – datalossdb.org

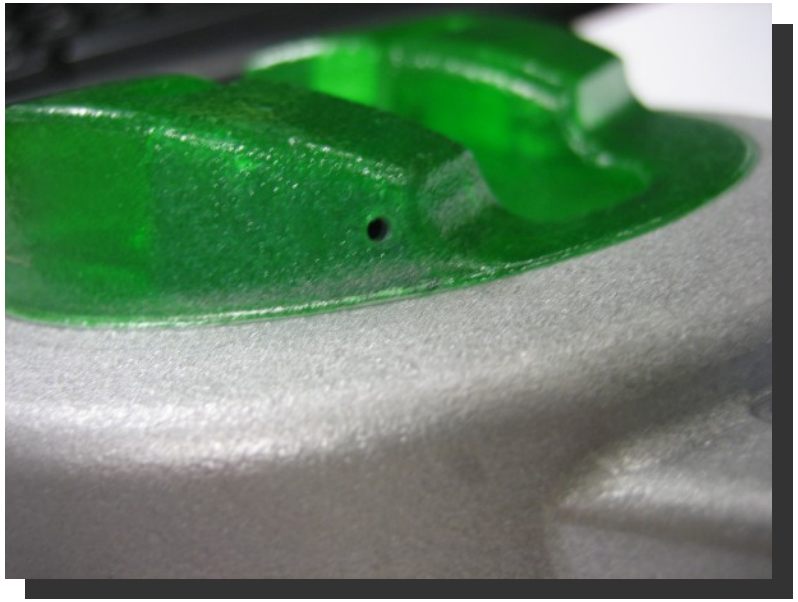
Dans le Top-20 de tous les temps, 8 incidents en 2011 ; L'Asie à l'honneur

Innovation dans le skimming

Identification d'un kit de skimming créé par imprimante 3D

-Haute qualité de fabrication, difficilement décelable

-A part cette innovation, pas réellement de nouveauté



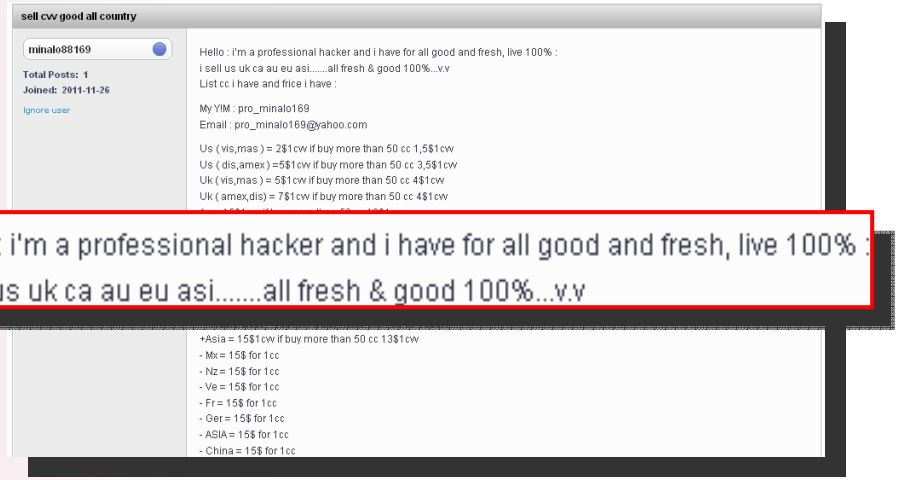
Photographies du kit de skimming – source : Krebsonsecurity.com

Accélération du trafic de cartes bancaires

La vente de cartes bancaires en ligne s'accélère

-Traditionnellement, une négociation directe entre initiés ;

-Désormais, la vente est industrielle et ne nécessite aucune prise de contact préalable



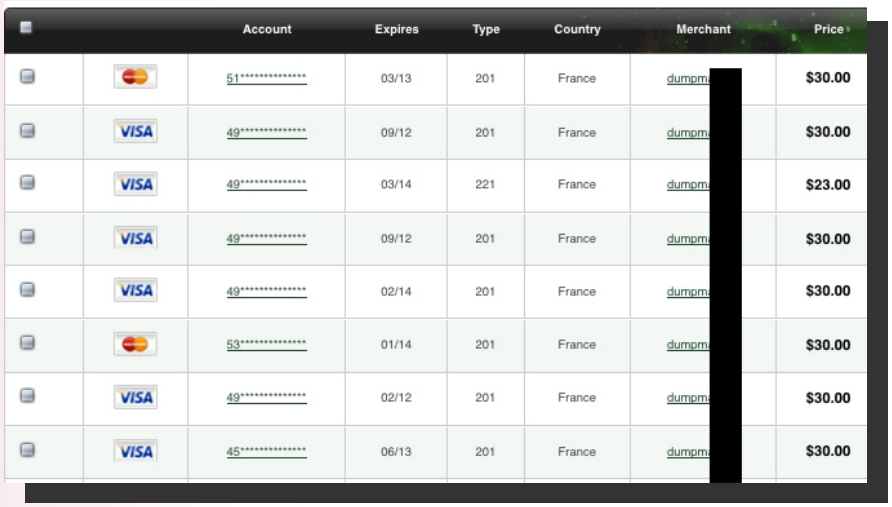
Avant : forums et négociations directes

Maintenant : la place de marché web 2.0

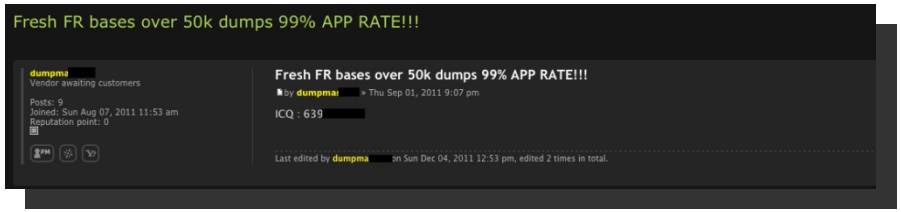
Accélération du trafic de cartes bancaires

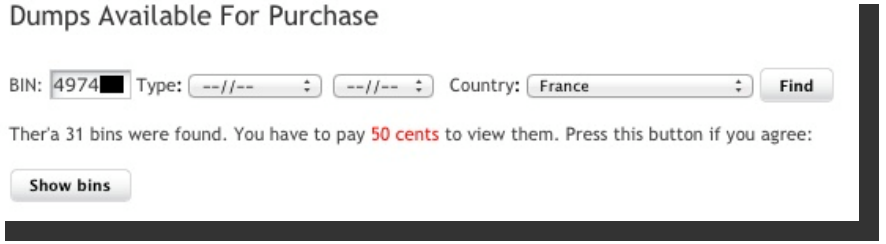
Les CB françaises ne sont pas épargnées

-A tout instant, des centaines d'annonces de vente de CB françaises volées sont disponibles



	Account	Expires	Type	Country	Merchant	Price
	51**********	03/13	201	France	dumpm	$30.00
VISA	49**********	09/12	201	France	dumpm	$30.00
VISA	49**********	03/14	221	France	dumpm	$23.00
VISA	49**********	09/12	201	France	dumpm	$30.00
VISA	49**********	02/14	201	France	dumpm	$30.00
	53**********	01/14	201	France	dumpm	$30.00
VISA	49**********	02/12	201	France	dumpm	$30.00
VISA	45**********	06/13	201	France	dumpm	$30.00





Source des illustrations : Cert XMCO

Accélération du trafic de cartes bancaires

Sophistication croissante des malwares…

-TDL4 : nouveau rootkit et stéganographie

-Zeus : prolifération des variantes depuis la fuite du code source

-Man-in-the-middle en temps réel et multi-canal

…et innovations dans la lutte contre les botnets

-Coreflood, Kelihos : de nouveaux moyens d'action

Accélération du trafic de cartes bancaires

Plusieurs arrestations notables en 2011 :

-octobre : « Opération Swiper » : 111 personnes (dont 86 déjà arrêtées) responsables d'un préjudice de 13 millions USD sur 16 mois

- Diversification des activités : cambriolages, braquages, escroqueries…

-août : 4 arrestations en Ukraine : préjudice potentiel de 20 millions USD

-France : coup de frein sur les plaintes pour fraude à la carte bancaire

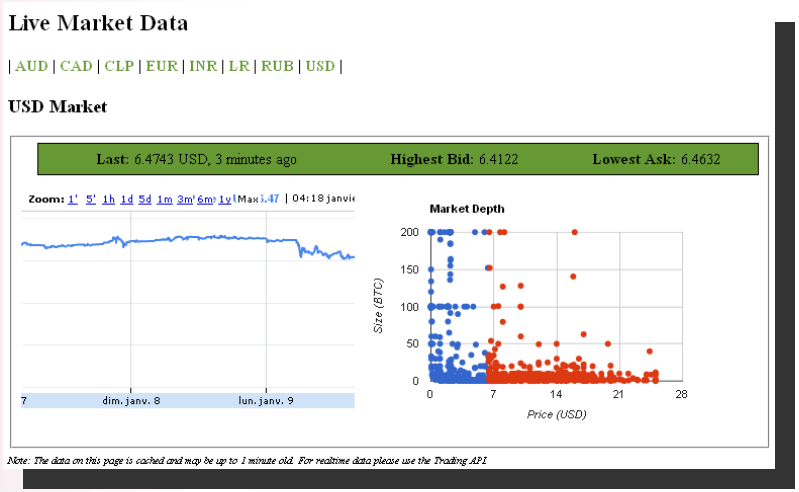
L'émergence de Bitcoin

Bitcoin : une nouvelle monnaie qui fait du bruit

-Principe : monétisation de la puissance de calcul

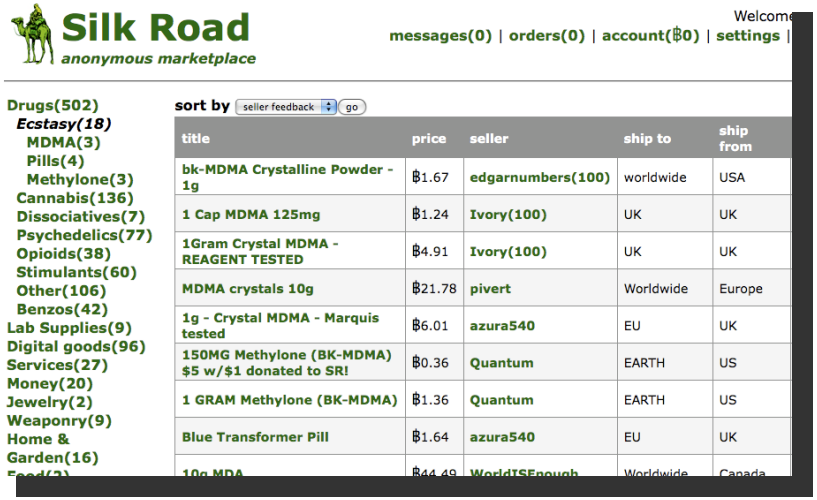
-Les transactions sont enregistrées…mais anonymes

-Menaces : vol de bitcoins, vente de marchandises illégales



Conversion de bitcoins (EUR, USD, RUB…)

Source : www.tradehill.com



Silk Road - Achat/vente de drogues en ligne

Mobilité : les menaces se précisent

Pierre CARON

Expert Sécurité

Orange

Téléphonie et télécommunications

Attaques du chiffrement des communications :

Après le GSM, c'est désormais le GPRS qui est pointé du doigt pour ses failles

- l'année 2011 débute sur la simplification du cassage de A5/1

-récidive en août : Karsten Nohl pointe du doigt les faiblesses du GPRS

- Certains réseaux ne chiffrent pas (GEA/0),
- Beaucoup utilisent un chiffrement faible (GEA/1 et /2)

Téléphonie et télécommunications

Femtocells : nouvelle technologie, nouvelles menaces

-THC dévoile un mode d'emploi du piratage de la femtocell de Vodafone (faille corrigée en 2009)

-Blackhat 2011 : démonstration d'attaques sur des femtocells utilisées en France (faille corrigée)

-Menaces potentielles :

- Ecoute passive des conversations et SMS
- Usurpation d'identité, SMS surtaxés

Les OS mobiles toujours attaqués

La course au jailbreak reste favorable aux pirates

Android devient-il le Windows XP du mobile ?

- failles permettant de dérober des identifiants (ClientLogin), d'installer des applications sans autorisation, d'accéder à la caméra et au micro…
- Vulnérabilités de l'Android Market : XSS, installation à distance

iOS n'est pas épargné :

- sslsniff : vulnérabilité dans l'implémentation du SSL
- Contournement du code PIN et déverrouillage de l'iPad 2
- Javascript descend en profondeur dans la mémoire d'iOS, et permet de contourner les restrictions d'exécution de code par signature

Malwares et fraude sur mobiles

Les mobiles convoités par les malwares :

-GGTracker : abonnement à des services SMS surtaxés

-LOIC : l'outil de DDoS arrive sur Android

-Android.Arspam : virus propagandiste

A ce jour, aucun malware mobile ne se propage par exploitation de faille OS

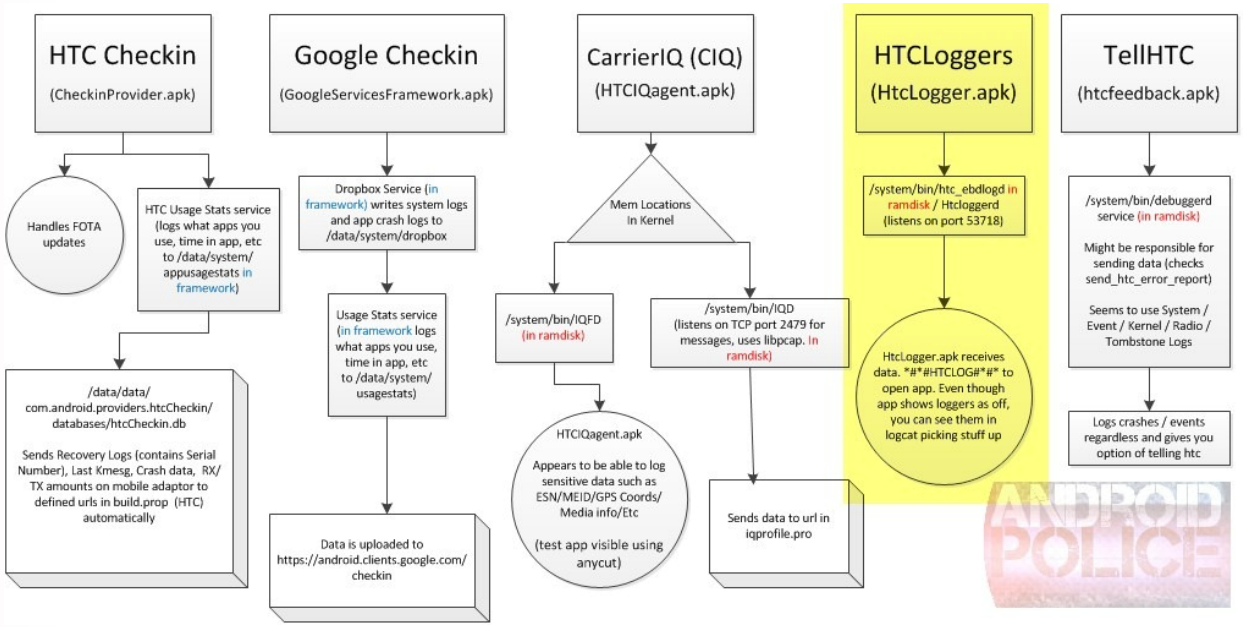
LOIC sur l'Android Market

HTCLoggers, le débogage trop zélé

Un utilitaire de débogage propriétaire présent sur certains téléphones HTC

-Ouvre une autoroute pour les malwares, qui n'ont plus besoin de demander d'autorisation pour accéder à tout le téléphone

-Corrigé rapidement par HTC, mais aucune explication…



Outils de débogage sur Android HTC – androidpolice.com

Carrier IQ, un curieux mélange des genres

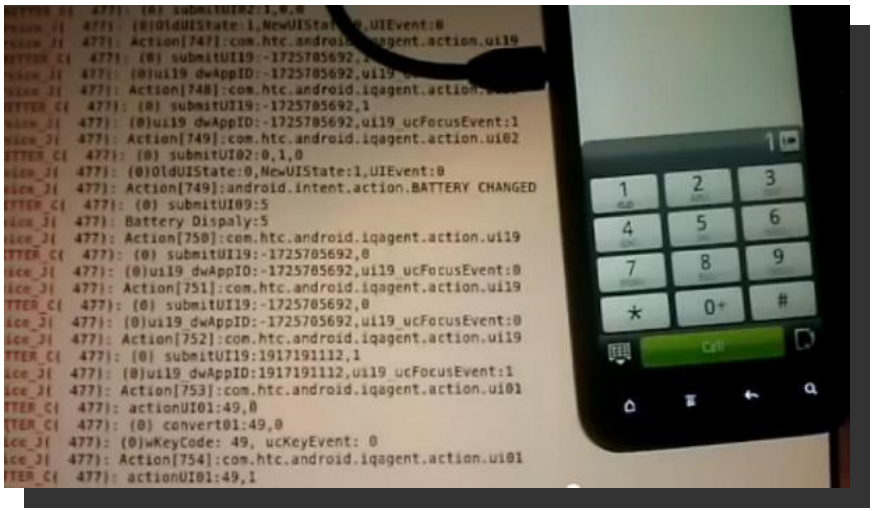
Un « rootkit » pré-installé sur 150 millions de téléphones aux Etats-Unis

-AT&T, Sprint, T-Mobile, HTC, Apple, Samsung, Motorola

-Enregistrement des numéros de téléphone (SMS / voix), géolocalisation, frappes sur le clavier numérique, URLs visités

-Polémiques :

- Capture des frappes clavier ?
- Capture des SMS : un bug ?
- Cas particulier de HTC ?
- Utilisation par le FBI ?



Confiance sur Internet : les autorités de certification compromises

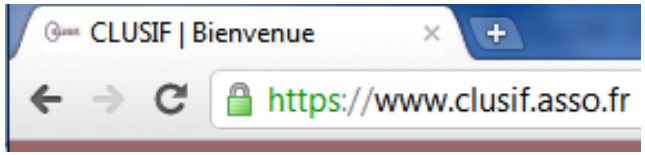
Gérôme BILLOIS

Manager Sécurité & Risk Management

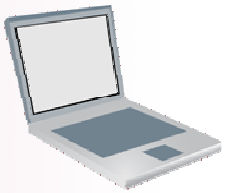
Solucom

La confiance sur Internet…

- Des fondamentaux dans un monde dématérialisé
  - Savoir qui est en face de soi
  - Savoir que les échanges restent confidentiels
- Un marqueur de confiance : le certificat
  - La carte d'identité numérique sur Internet
  - Délivré par une autorité de certification
- Il permet la mise en place
  - Du chiffrement des échanges (https)
  - Et de la vérification d'identité



La confiance sur Internet…

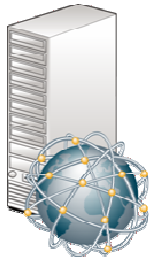


Le navigateur

(et son utilisateur)

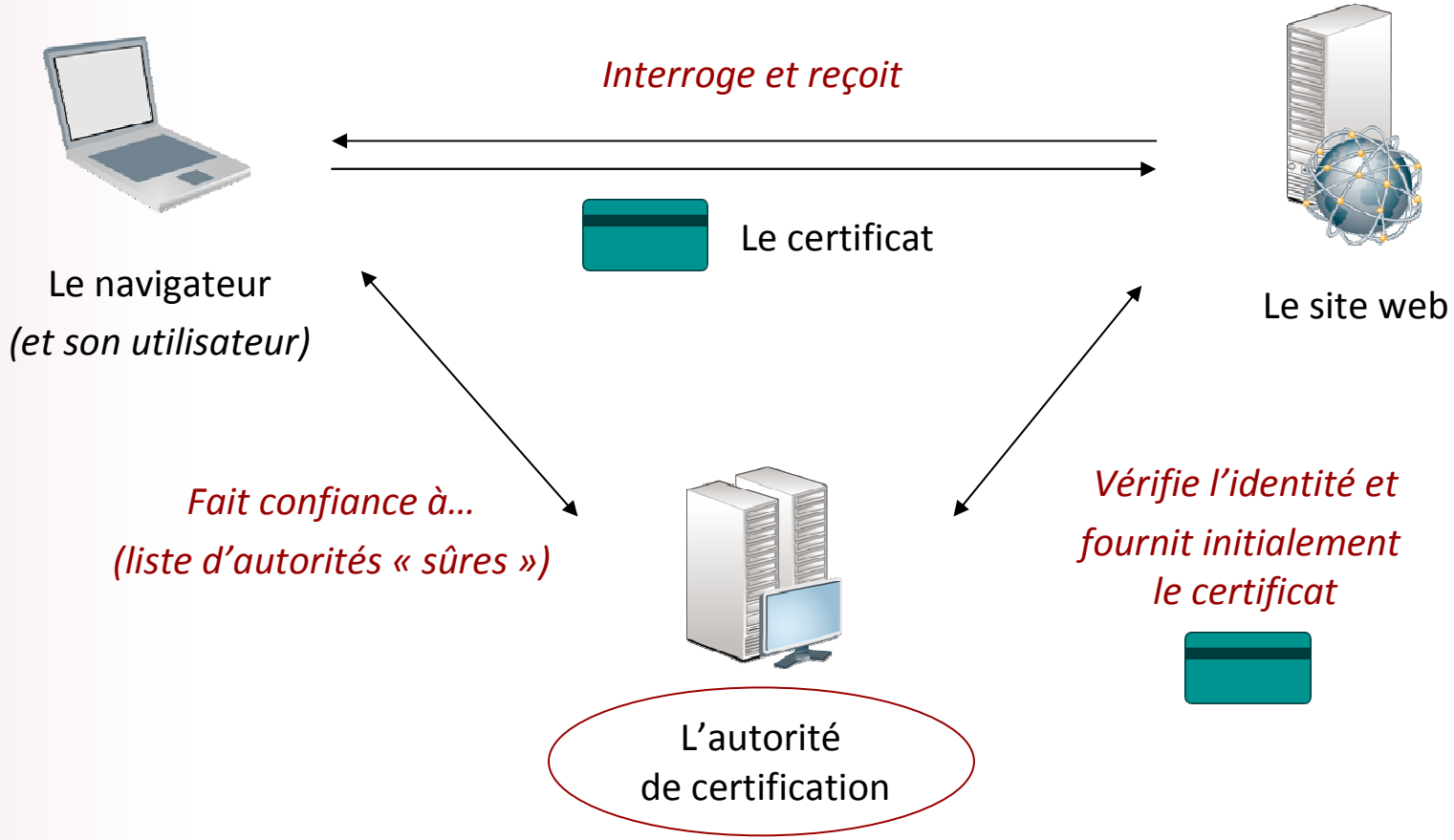
Interroge et reçoit

Le certificat



Le site web

La confiance sur Internet… le principe du **tiers de confiance**



2011 : les autorités de certification au cœur de la tourmente

- Des structures dont la sécurité doit être irréprochable…
- … pour éviter la fabrication de faux certificats
- Mais dont l'année 2011 à montré les limites !

Les risques majeurs : usurpation d'identité et écoute des échanges

Mars 2011 COMODO Creating Trust Online™

Aout 2011 DigiNotar Internet Trust Services

Mais aussi beaucoup d'inquiétudes plus ou moins avérées…

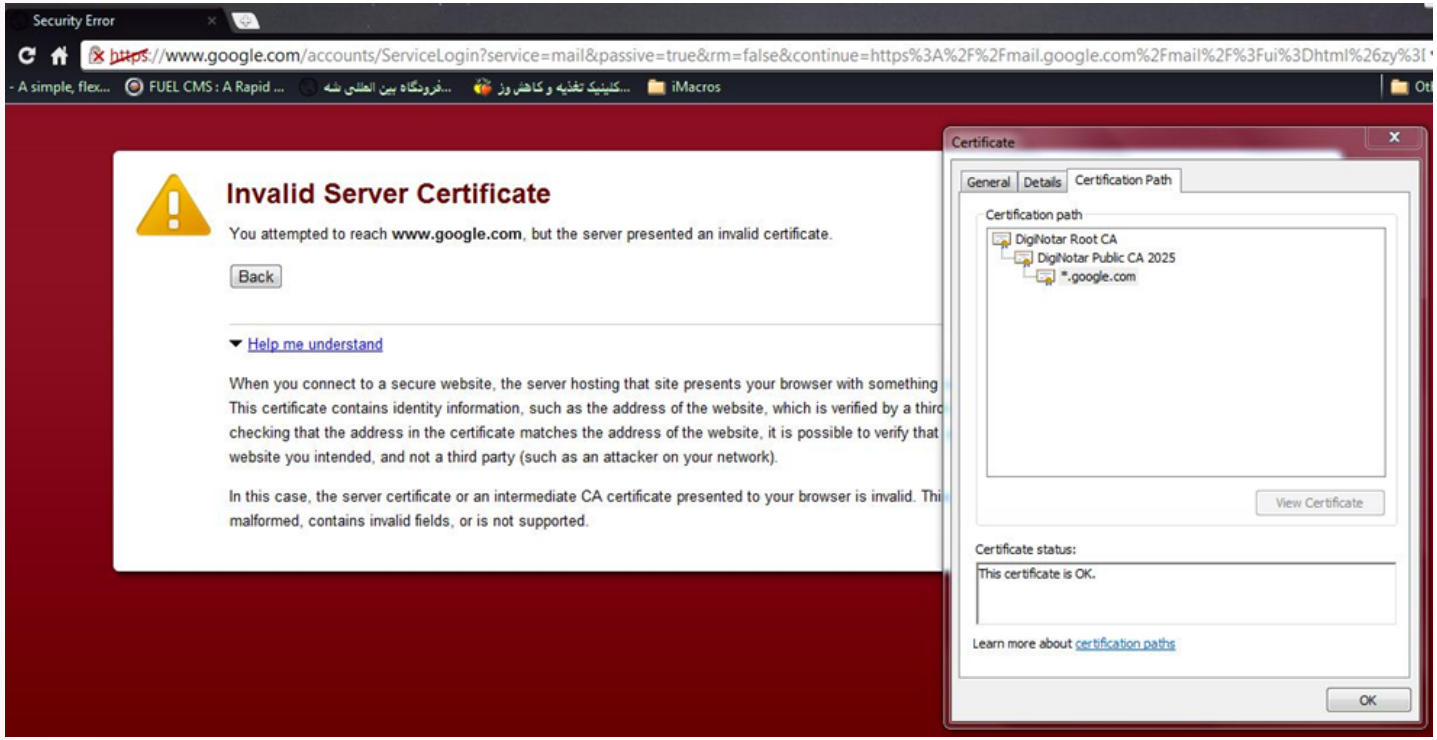
GlobalSign

StartCom SSL SECURED

thawte

L'histoire de Diginotar : la découverte

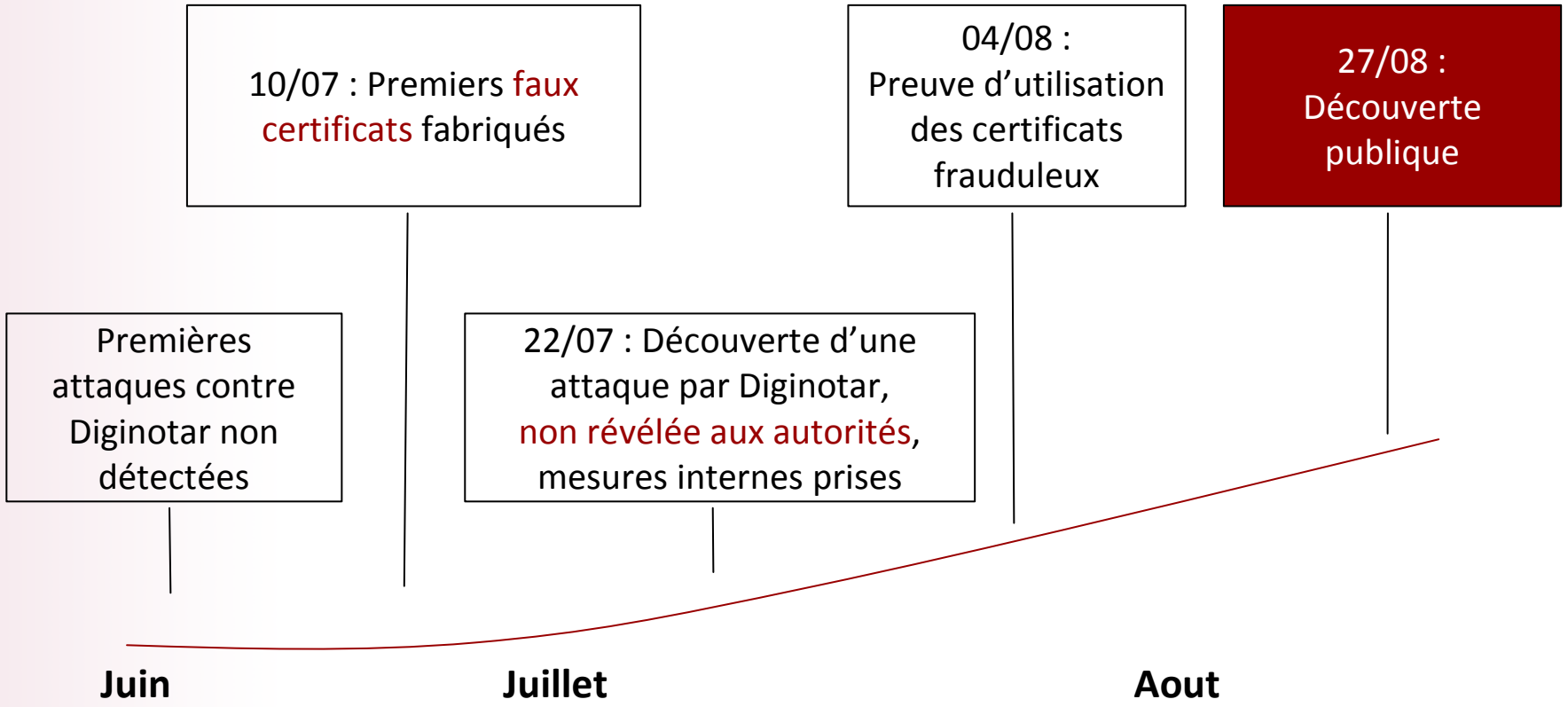
28 août 2011, en Iran, Ali Borhani consulte sa messagerie Gmail…



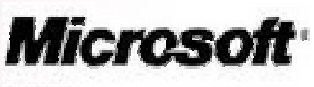
… et découvre un problème avec le certificat utilisé

(grâce à une nouvelle fonctionnalité de Chrome et un œil averti)

L'histoire de Diginotar : la génèse



Et pendant ce temps…. 531 faux certificats fabriqués



…

Mais aussi des certificats génériques

..com et *.*.org

L'histoire de Diginotar : l'amplification

29-30/08 : Notification des CERT

Les principaux navigateurs révoquent certains certificats

31/08 : Le gouvernement néerlandais entre en scène du fait de la compromission possible de nombreux télé-services

03/09 : Le rapport d'investigation montre des lacunes fortes de sécurité

Septembre

04/09 : L'utilisation de services numériques est déconseillé au Pays-Bas : retour au papier !

Demande de délais pour la révocation des certificats pour les Pays Bas

06/09 : Suspicion d'attaques à + grande échelle, l'auteur se dévoile

13/09 : Les grands acteurs ont révoqués les certificats mais il reste des situations difficiles (M2M / téléphones…)

20 septembre, Diginotar dépose le bilan…

Comodohacker : un auteur aux motivations politiques

- Au service de son pays : l'Iran
- Avec un objectif : permettre l'écoute des communications

Lieux d'utilisation des certificats compromis

Une remise en cause des fondamentaux

- Le modèle de tiers de confiance atteint sa limite
  - Une seule autorité défaillante remet en cause la confiance dans le système
  - Il existe plusieurs centaines d'autorités reconnues…
- De nombreuses initiatives d'amélioration
  - Google, IETF, EFF…

En 2011, une nouvelle tendance

- Attaquer les fournisseurs de solution de sécurité…

RSA Google COMODO Creating Trust Online™ DigiNotar Internet Trust Services ….

- … pour fabriquer un double des clés plutôt que de forcer la serrure

A suivre en 2012 !

Références

Les détails sur Diginotar

http://kschang.hubpages.com/hub/What-is-DigiNotar-SSL-Security-Breach-and-how-does-it-affect-you
http://www.networking4all.com/en/ssl+certificates/ssl+news/time-line+for+the+diginotar+hack/
http://www.nrc.nl/nieuws/2011/09/10/onderzoek-nrc-platgaan-computers-rijk-net-afgewend/
http://www.nu.nl/diginotar/2609177/aantal-gemeenten-legt-site-stil-diginotar.html
http://www.f-secure.com/weblog/archives/00002228.html
http://www.eweek.com/c/a/Security/Google-Warns-Iranian-Gmail-Users-After-DigiNotar-Breach-573939/
http://pastebin.com/GkKUhu35
https://blog.torproject.org/files/rogue-certs-2011-09-04.csv

Le cas BEAST

http://www.schneier.com/blog/archives/2011/09/man-in-the-midd_4.html
http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/
http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/page2.html
http://www.bortzmeyer.org/beast-tls.html

Références

De futures solutions

http://www.cabforum.org/Baseline_Requirements_Draft_50.pdf

https://www.eff.org/deeplinks/2011/11/sovereign-keys-proposal-make-https-and-email-more-secure

http://www.links.org/files/CertificateAuthorityTransparencyandAuditability.pdf

L'attaque RSA

http://www.lemagit.fr/article/microsoft-securite-rsa-flash-adobe-gartner-hacking-faille-vol-donnees-hacker/8467/1/hack-rsa-ingenierie-sociale-mails-cibles-faille-zero-day-nouvel-cocktail-detonant-des-hackers/

http://blogs.rsa.com/rivner/anatomy-of-an-attack/

L'attaque COMODO

http://www.scmagazine.com/two-more-comodo-resellers-owned-in-ssl-hack/article/199620/

http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/

Ruptures de service : les accidents aussi !

Gérôme BILLOIS

Manager Sécurité & Risk Management

Solucom

Pendant que la cybercriminalité défraie la chronique…

- Les accidents sont toujours autant présents !
  - Des impacts tout aussi forts
  - Ils touchent à la disponibilité, le fameux « 99,999% »
  - Même sur des services conçus pour assurer la continuité (cloud)
- Une année 2011 riche en évènements
  - Des erreurs humaines comme des évènements naturels
- Aujourd'hui l'analyse de 2 cas emblématiques

Un chantier comme les autres…

accidentel

Le 12 Mai 2011 à Vélizy

Le fameux « coup de pelleteuse »

accidentel

Et voilà ce qu'il reste des fibres optiques…

Des impacts immédiats !

accidentel

- Des opérateurs touchés

- Le site d'un hébergeur dans le noir

- Et des organisations fortement impactées (coupure/bascule PRA)

…

: 250.000 euros de perte, 120 personnes au chômage technique

Des réparations en urgence

accidentel

- Un incident réparé en 8h… grâce aux « soudeurs de fibre »
  - Une équipe de 2 personnes peut ressouder + de 200 fibres en 1 journée

- Mais qui aurait pu être évité grâce à une redondance de collecte
  - A première vue rendue impossible du fait des travaux du tramway…

accidentel

RIM : octobre 2011, une interruption de service majeure

- *Lundi 10* : début de l'incident
  - L'Europe, le Moyen orient et l'Afrique sont touchés sur de nombreux services
- *Mardi 11* : le service est toujours dégradé ou interrompu malgré une communication sur une reprise
- *Mercredi 12* : le problème s'étend aux États-Unis, le CIO prend la main sur la communication
- *Jeudi 13* : communication du fondateur de RIM, retour à la normal
- *Lundi 17* : des applications sont offertes aux utilisateurs en compensation…

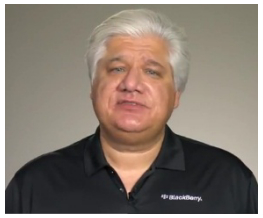
BlackBerryHelp Research In Motion
We're aware many of you are experiencing service delays. Restoring full service is our number 1 priority. rim.com/newsroom/servi... ^PM
14 minutes ago

BlackBerryHelp Research In Motion
Message delays were caused by a core switch failure in RIM's infrastructure. Now being resolved. Sorry for inconvenience. ^PM
18 hours ago

BlackBerryHelp Research In Motion
Some areas have messaging delays and impaired browsing. We're working to restore normal service as quickly as possible. ^PM
21 hours ago

BlackBerryHelp Research In Motion
Some areas have messaging delays and impaired browsing. We're working to restore normal service as quickly as possible. ^PM
11 Oct

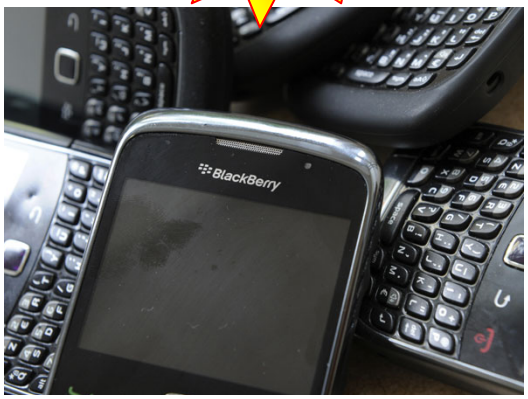
"I apologise for the service outages this week. We've let many of you down. But let me assure you that we're working round the clock to fix this."



Une défaillance en chaîne au cœur de la panne

accidentel

- Un défaillance dans un datacenter à Slough (UK)…
  - Équipement de cœur de réseau défaillant (explication officielle) le secours local aussi
  - … entraîne une réaction en chaîne
  - Saturation des services (8 Go/s de trafic…)
  - Bascule sur le site de secours d'Egham qui crée une corruption de la base de données
  - Des conséquences de premier ordre
  - Des opérateurs qui se désolidarisent
  - Des entreprises touchées dans leur fonctionnement
  - Des clients excédés qui basculent sur d'autres plateformes et menacent d'action en justice
- Des changements en profondeur de l'architecture sont envisagés mais vont prendre du temps



BlackBerry outage this week saw many users switch to an iPhone 4S in frustration, such as Kit Tjia, 22, from west London. Photograph: Georgie Gillard/PA

Les accidents sont une menace réelle…

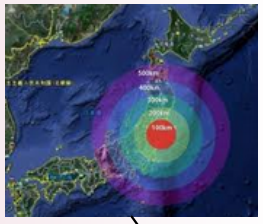
- La disponibilité des SI tient souvent à un fil
  - Ou à une fibre, ou encore à un switch…

- Au cœur de la démarche, évaluer ses risques et se préparer
  - Identifier les services essentiels
  - Choisir les solutions de secours techniques et métiers
  - Tester et maintenir les plans de continuité/reprise
  - Et prévoir la gestion de crise !

➔ *Un exemple de réaction à une crise majeure… Le Japon*

Un exemple de réaction à une crise majeure au Japon

accidentel



Le 11 mars 2011, un tremblement de terre au large du Japon…

… déclenche un tsunami sans précédent…

… qui entraîne un incident nucléaire

et des impacts humains terribles

NTT : Une gestion de crise à la mesure de l'évènement

- 5000 personnes mobilisées

- 2076 téléphones spéciaux gratuits
- 830 téléphones satellitaires
- 400 générateurs d'urgence et 100 sites de chargement de portables gratuits
- Des services de messageries d'urgence utilisés plus de 6 millions de fois

En 18 jours de crise… un rétablissement de premier ordre

accidentel

NTT : Bilan des services interrompus au Japon			
Services et infra. affectés	**13 Mars**	**25 mars**	
Centraux téléphoniques	1,000	72	+92%
Lignes fixes (RTC)	879,500	86,300	+91%
Lignes numériques (ISDN)	118,600	7,900	+93%
Fibre Optique (FTTH)	475,400	23,700	+95%

Accompagné par une mobilisation à l'échelle internationale !

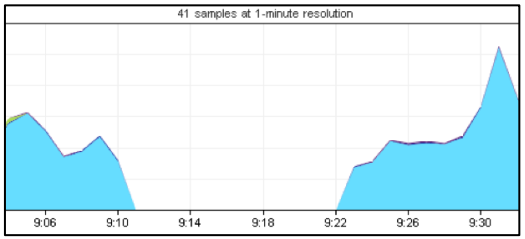
En conclusion

accidentel

- Trois exemples analysés mais il en existe beaucoup d'autres…

L'orage qui a tué le nuage d'Amazon (ou pas…)

Les inondations en Thaïlande



Le bug BGP Juniper qui a fortement perturbé Internet

- Rester humble devant les accidents ! Tester, tester et tester ses plans de continuité/reprise et la gestion de crise…
- Heureusement certaines méthodes utilisées pour couvrir les incidents sont utiles également pour contrer la cybercriminalité !

Références

La fibre de Vélizy et ses déboires…

http://www.itespresso.fr/telecoms-une-rupture-de-fibre-optique-isole-une-partie-de-louest-parisien-42742.html

http://lafibre.info/yvelines/coupure-geante-de-fibre-optique-a-velizy-78/

http://www.leparisien.fr/economie/l-ouest-parisien-prive-de-telephone-et-d-internet-12-05-2011-1446856.php

http://www.zdnet.fr/blogs/infra-net/une-pelleteuse-coupe-le-site-web-du-ministere-de-la-defense-et-beaucoup-d-autres-39760750.htm

https://twitter.com/#%21/_GaLaK_

http://www.prnewswire.co.uk/cgi/news/release?id=316184

NTT et le Japon

http://fr.wikipedia.org/wiki/S%C3%A9isme_de_2011_de_la_c%C3%B4te_Pacifique_du_T%C5%8Dhoku

http://www.ntt.com/business_e/feature/bcp.html

http://www.globalsecuritymag.fr/Comment-NTT-Com-a-fait-face-au,20110331,22909.html

https://itunews.itu.int/Fr/1630-Le-Japon-au-lendemain-du-tremblement-de-terre-et-du-tsunami-.note.aspx

Les évocations finales

http://www.zdnet.fr/actualites/grosse-perturbation-d-internet-causee-par-une-panne-des-routeurs-juniper-39765436.htm

http://www.truedigitalsecurity.com/blog/2011/11/10/juniper-bgp-bug-briefly-takes-down-the-internet/

http://www.datacenterknowledge.com/archives/category/infrastructure/downtime/page/3/

Références

RIM et l'incident d'octobre 2011

http://mashable.com/2011/10/13/blackberry-outage-rim-response/

http://www.rim.com/newsroom/service-update.shtml

http://press.rim.com/release.jsp?id=5214

http://www.huffingtonpost.com/2011/10/11/blackberry-outage-october-2011_n_1005009.html

http://venturebeat.com/2011/10/26/class-action-lawsuit-rim-blackberry/

http://www.bbc.co.uk/news/technology-15474910

http://www.foxnews.com/scitech/2011/10/12/blackberry-says-services-have-improved-after-worldwide-outage/

http://www.guardian.co.uk/technology/2011/oct/14/blackberry-outage-faulty-router-suspected?newsfeed=true

http://www.guardian.co.uk/technology/2011/oct/12/blackberry-outage-executive-apologies

http://www.telco2.net/blog/2011/10/telco_20_news_review_79.html

http://www.guardian.co.uk/business/2011/oct/16/rbs-tries-out-iphone-blackberry-replacement

http://www.telegraph.co.uk/technology/news/8825661/BlackBerry-blackout-how-it-happened.html

http://www.thehindubusinessline.com/industry-and-economy/info-tech/article2534978.ece?ref=wl_industry-and-economy

http://www.silicon.com/technology/mobile/2011/10/12/blackberry-outage-day-three-rim-explains-what-went-wrong-39748071/

L'Hacktivisme en 2011: entre enfantillage et conscience politique

François PAGET

Chercheur de menaces

McAfee Labs

L'Hacktivisme en 2011

- Les 3 aspects de l'hacktivisme en 2011,
- Le monde industriel face à l'hacktivisme
- Les Etats face à l'hacktivisme
- Les criminels face à l'hacktivisme
- L'hacktivisme face à ses contradictions

Face A : Les Anonymous

Ils militent pour un Internet libre.

Leurs méthodes rappellent la cybercriminalité:

- Attaques en DDoS,
- Piratage,
- Vol et divulgation d'informations personnelles et/ou confidentielles.

Masque de Guy Faykes, emblème des Anonymous

Face A : Les Anonymous

- Une idée et non un groupe structuré,
- Peu de sophistication,
- Beaucoup de dissensions,
- Une véritable motivation politique souvent difficile à établir,
- Un mouvement gangréné par des « script-kiddies »,
- Souvent cantonnés sur le Net.

Le groupe Lulzsec se réclame des Anonymous

Face B : Les Cyber-Indignés

Ils utilisent Internet et les réseaux sociaux:

- Moyen de liaison,
- Propagande,
- Renseignement: collecte et diffusion de données personnelles sur ceux qui les dérangent.

Facebook, Twitter et Youtube ont joué un rôle dans les révolutions arabes

Face B : Les Cyber-Indignés

- Ils militent aussi dans le monde réel (Mouvement des Indignés et des Occupy),
- Ils soutiennent les révolutions arabes,
- Bien moins d'enfantillage,
- Ils cherchent souvent à rester à la limite de la légalité,
- Ils sont rejoints par des Anonymous « canal historique » qui veulent associer l'action sur terrain à celle sur le Net.

Le mouvement « Occupy » a atteint la France en 2011

Face B : Les Cyber-Indignés – 2011, Telecomix et do-ocratie

- Janvier 2011, aide à l'accès au web en Egypte.
- Actions similaires en Lybie (février) et en Syrie (août).
- Cours de cryptographie pour l'ONG Reporters Sans Frontières.

Le groupe Telecomix soutient les révolutions arabes

Face C : Les Cyber-Armées

Elles soutiennent des régimes totalitaires et véhiculent des idées extrémistes:

- Défacements de sites,
- Attaques DDoS sur des blogs de dissidents et des sites qui les dérangent.

Leurs actions ont peu d'impact.

Sigles de quelques cyber-armées

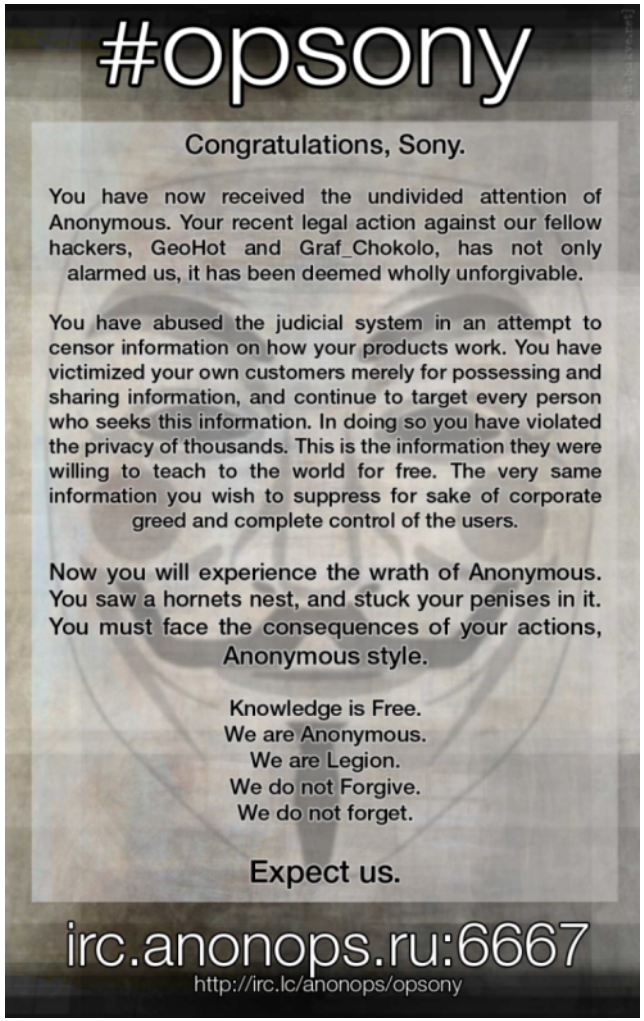
Face C : Les Cyber-Armées - 2011, loi sur les génocides

Le 25 décembre, le site Internet de Valérie Boyer, députée à l'origine de la proposition de loi réprimant la négation des génocides, dont celui des Arméniens, renvoyait automatiquement à un écran noir affichant le drapeau de la Turquie et un message en turc et en anglais s'en prenant au gouvernement français et à la communauté arménienne de France.

Copie d'écran du site de Valérie Boyer

L'entreprise face à l'hacktivisme : le cas de Sony

- Début avril, Anonymous réclame le droit au débridage (jailbreak) de la PS3. Il souhaite aussi l'arrêt des poursuites à l'encontre de Georges Hotz (pseudo GeoHot).
- Entre le 16 avril et le 19 juin, plus de 20 attaques sont référencées. Plus de 100 millions d'individus voient leurs données personnelles détournées.
- Le 23 mai, en pleine période de crise, Sony annonce déjà une enveloppe de $170 million (14 billions de yen) pour répondre aux attaques.

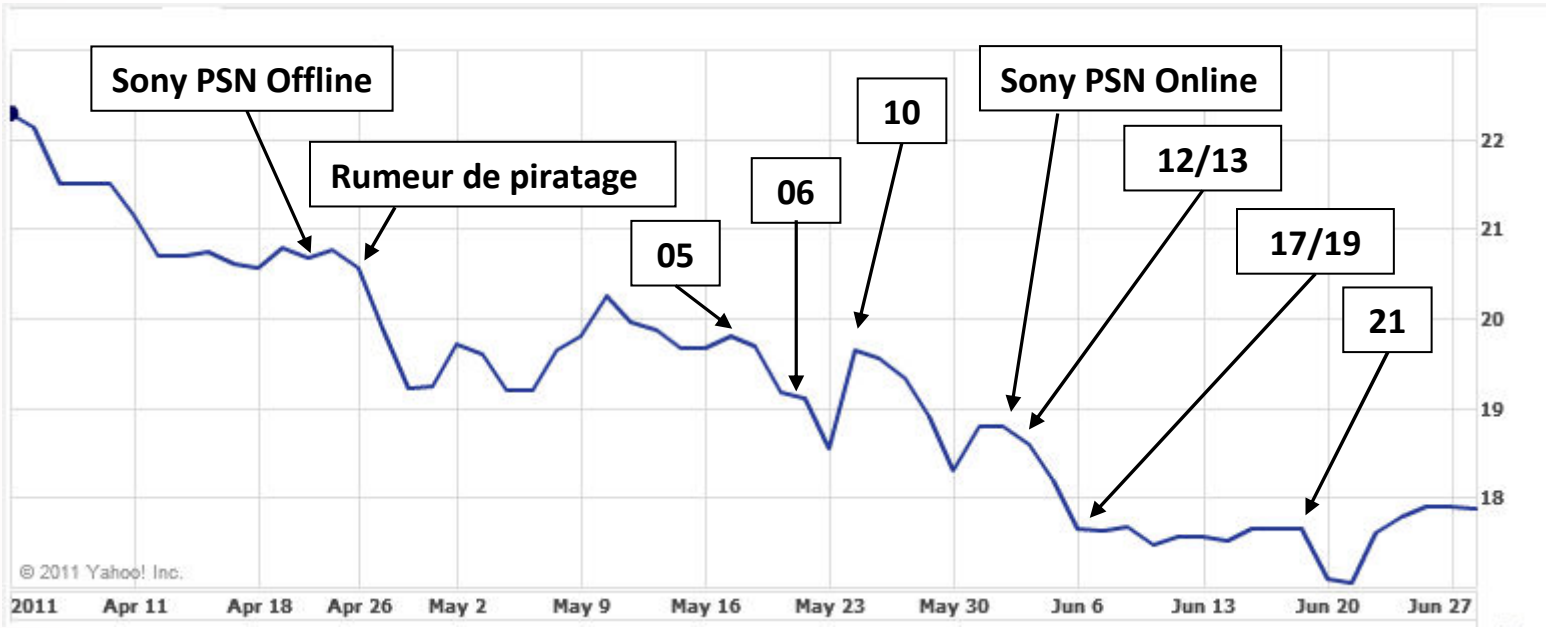


L'un des nombreux messages des Anonymous à Sony

L'entreprise face à l'hacktivisme : le cas de Sony

11 mars 2011 (tremblement de terre & tsunami)

SONY (SON1.MU)

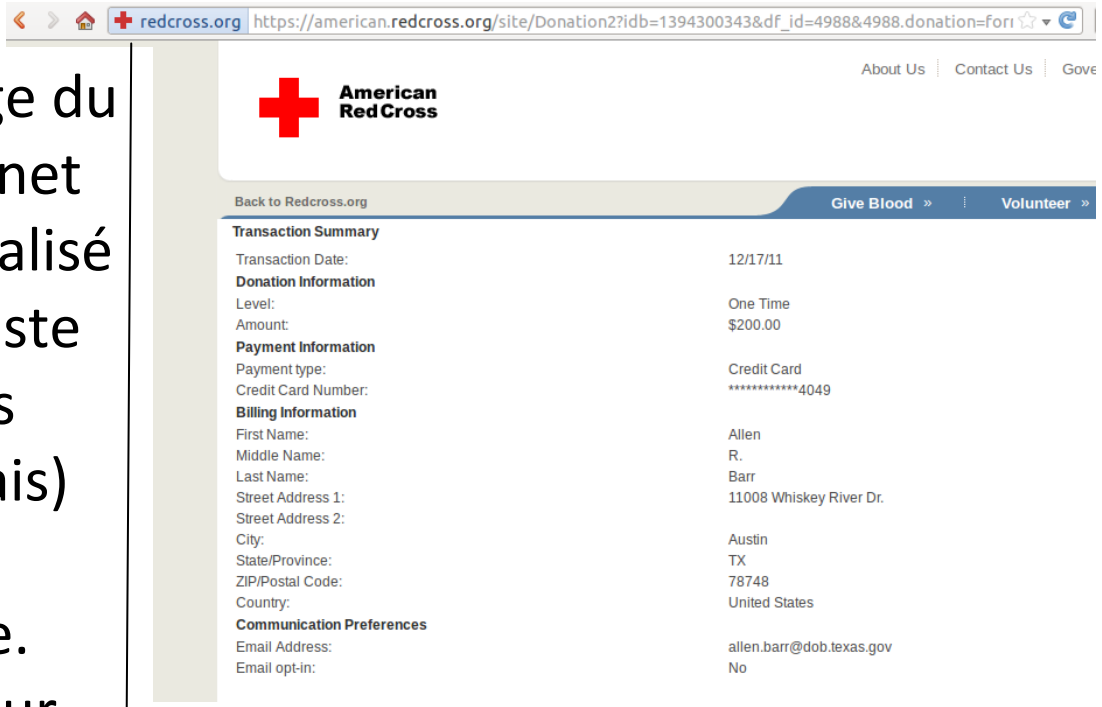


L'entreprise face à l'hacktivisme : le cas de HBGary

- 5 février: le Financial Times révèle qu'Aaron Barr (CEO of HBGary Federal) envisage de fournir au FBI des informations qu'il a collectées sur les Anonymous.
- 6 février: les serveurs HBGary sont piratés. 70000 mails sont diffusés sur le Net.
- 28 février: Le contenu de certains mails contraint Aaron Barr à la démission. Plusieurs gros clients prennent leur distance avec sa société. Une plainte est déposée pour soupçon d'activités illégales.

L'entreprise face à l'hacktivisme : le cas de Stratfor

- 24 décembre: piratage du cabinet Stratfor (cabinet privé américain spécialisé dans la sécurité). La liste de 4000 de ses clients (parmi eux des français) avec coordonnées bancaires est diffusée. Elles sont utilisées pour faire des dons à des ONG.



Pour démontrer leurs réussites, quelques Anonymous diffusent les preuves de versements aux ONG

- Plusieurs canaux accrédités Anonymous démentent la paternité de l'attaque tandis qu'une faction la confirme (Sabu, LulzSec).
- Les ONG deviennent des victimes (frais de chargeback).

L'entreprise face à l'hacktivisme

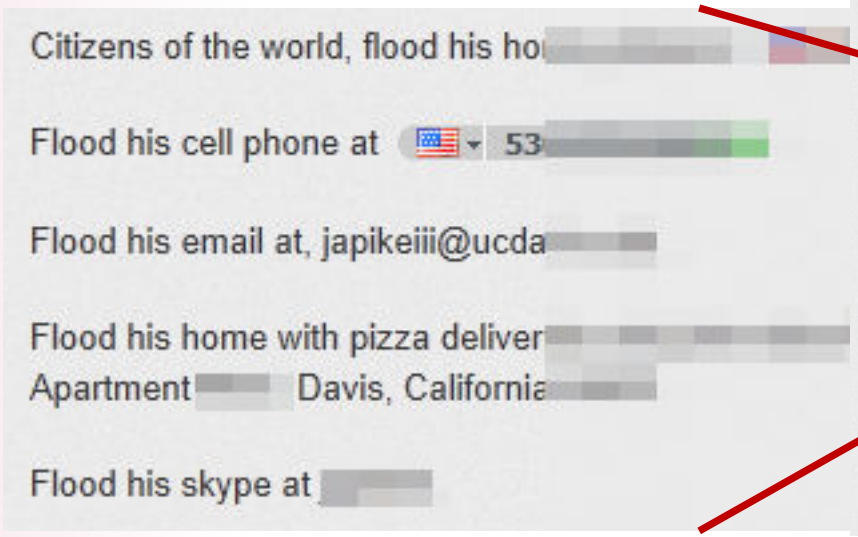
Autres exemples:

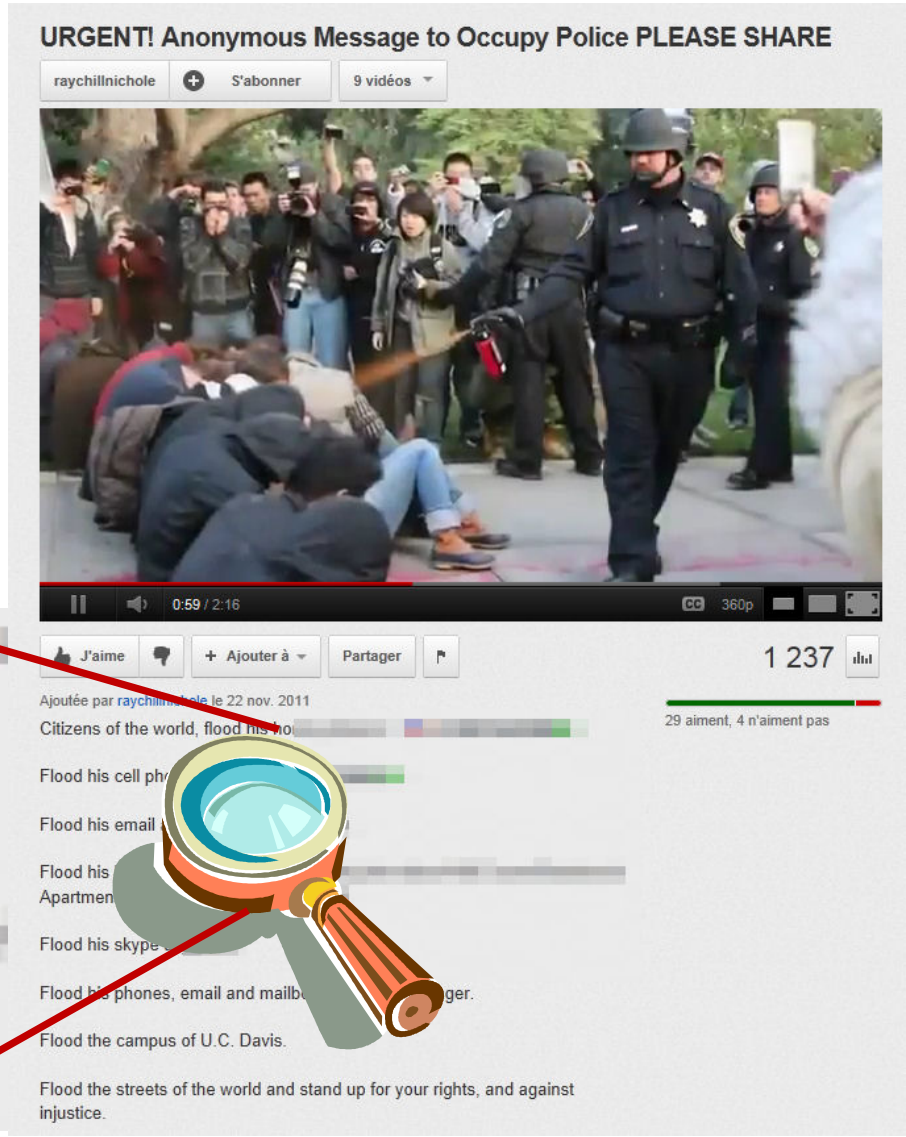
- 14 mars: Bank of America
- 4 avril: EDF
- 29 avril: Fox Broadcasting
- 5 juin: Nitendo
- 8 juin: National Health Service (UK)
- 11 juillet: Booz Allen Hamilton
- 12 juillet: Monsanto
- 29 juillet: ManTech
- 31 décembre: piratage d'une vingtaine d'agences de notations

EDF, seconde cible de l'opération GreenRight contre les géants de l'énergie

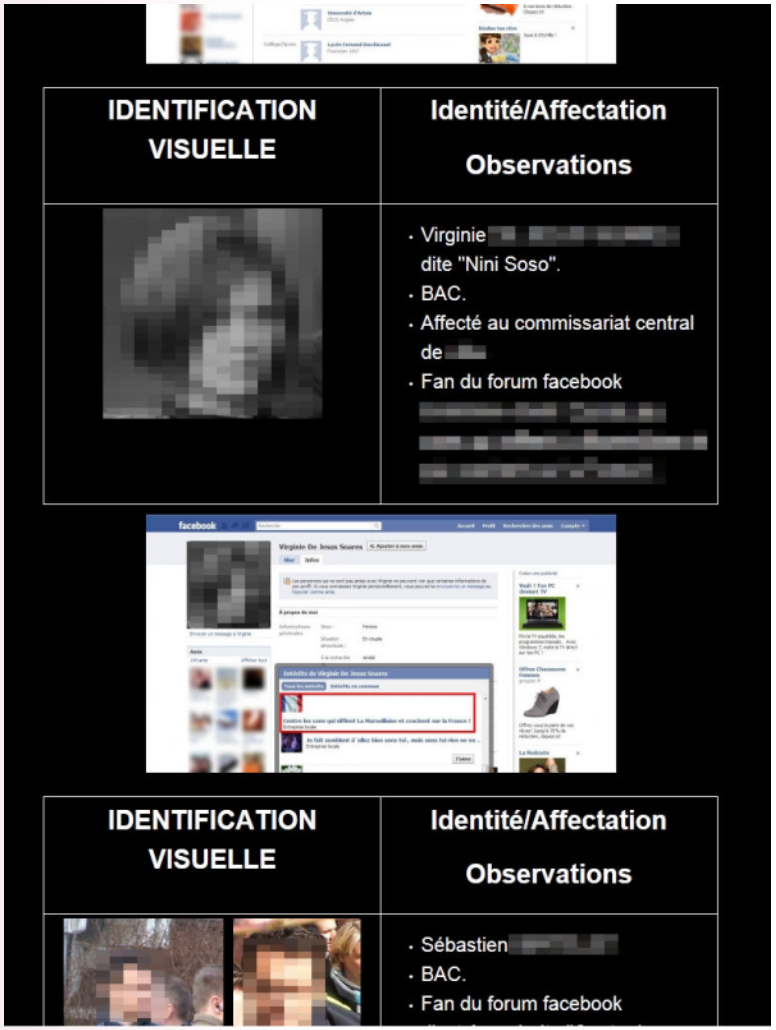
Les forces de police face à l'hacktivisme

Le doxing consiste en la publication de photos, de coordonnées et de données personnelles et familiales en représailles à une action menée par l'individu qui en est la victime.





Les forces de police face à l'hacktivisme



IDENTIFICATION VISUELLE	Identité/Affectation Observations
	• Virginie [redacted] dite "Nini Soso". • BAC. • Affecté au commissariat central de [redacted] • Fan du forum facebook [redacted]

IDENTIFICATION VISUELLE	Identité/Affectation Observations
	• Sébastien [redacted] • BAC. • Fan du forum facebook

maintien de l'ordre de la moindre manifestation à Paris

- Antoine [redacted]
- Commissaire à la tête de la division nationale de lutte contre le hooliganisme.
- Ancien chef de la BAC départementale du Nord.
- Connu pour ses opérations passées et actuelles de maintien de l'ordre musclées.
- Ancien bénévole de la croix rouge française.

Catégorie:
Base Paris

Doxing: le 14 octobre, le tribunal de grande instance de Paris ordonne aux FAI de bloquer l'accès au site copwatchnord-idf (39 copies du site sont aujourd'hui référencées)

Les forces de police face à l'hacktivisme

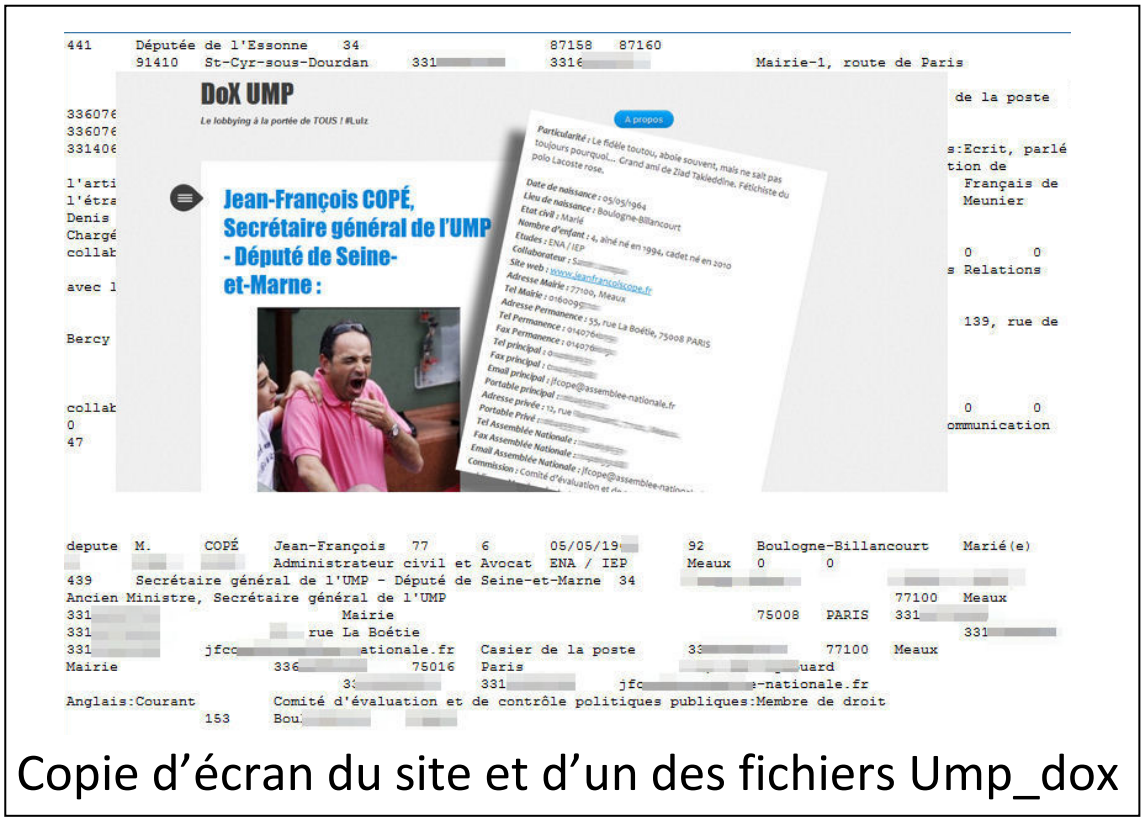
Tout au long de l'année, le collectif Antisec a piraté puis divulgué des données personnelles liées aux forces de l'ordre

Chinga La Migra	Date	Targets
I	24 JUN 2011	Arizona Department of Public Safety (AZDPS)
II	29 JUN 2011	AZDPS
III	1 JUL 2011	Arizona Fraternal Order of Police (AZFOP)
IV	2 SEP 2011	Texas Police Chiefs Association

F**K FBI Friday	Date	Targets
I	5 JUN 2011	Infragard
II	8 JUL 2011	IRCFederal
III	29 JUL 2011	ManTech
IV	19 AUG 2011	Vanguard Defense Industries
V	18 NOV 2011	Freb Baclagan Cybercrime Investigator

Le monde politique face à l'hacktivisme

- 26 octobre: divulgations de données (légèrement) personnelles relatives à Jean François Copé, Christian Estrosi et Eric Ciotti. Création d'un site qui se veut humoristique. Il reprend ces données en les accompagnants de photos détournées.
- 5 novembre, 4 fichiers contenant des données similaires, mais touchant 1331 élus/cadres de la majorité présidentielle sont déposés, à leur tour sur Pastebin.



Copie d'écran du site et d'un des fichiers Ump_dox

Le monde politique face à l'hacktivisme

Autres exemples:

- 23 & 25 janvier: piratage de la page Facebook de Nicolas Sarkozy,
- 13 juin: Sénat Américain
- 3 Juillet: Democratic Party of Orange County, Florida (doxing)
- 26 juillet: redirection de la page elysee.fr
- 29 juillet: Front National (doxing)
- 15 décembre: NDAA (National Defense Authorization Act) mass dox
- Depuis le 25 décembre: réactions face à la proposition de loi réprimant la négation des génocides

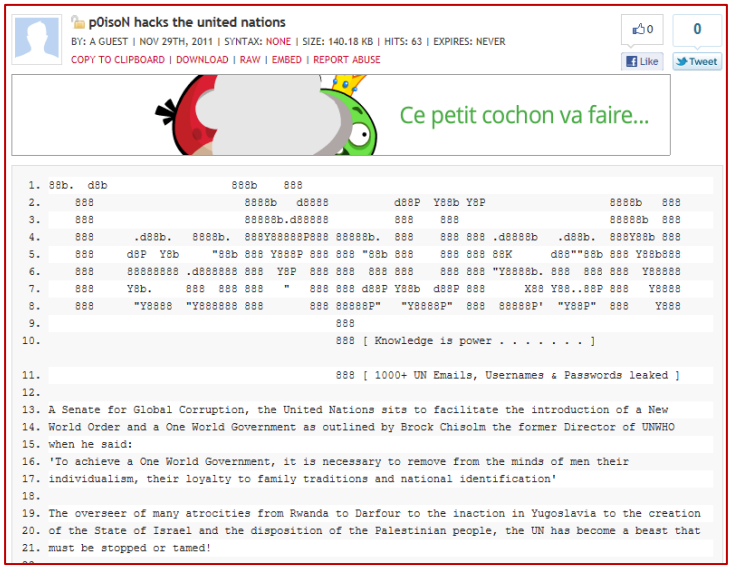
Revendication du dox UMP

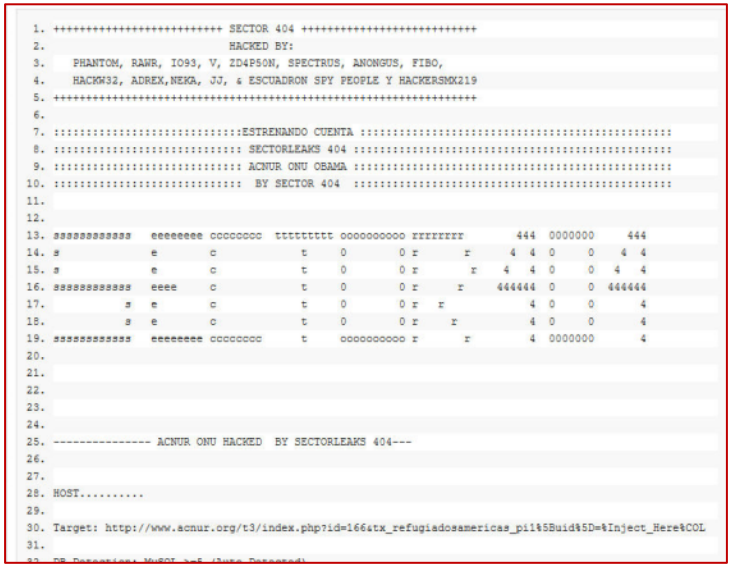
...

Les institutions internationales face à l'hacktivisme

Le 29 novembre, 2 groupes se réclamant des Anonymous divulguent de nombreuses informations en provenance de:

- UNDP/PNUD (Programme des Nations Unies pour le développement),
- OECD/OCDE (Organisation de coopération et de développement économiques),
- UNICEF,
- WHO/OMS (Organisation mondiale de la santé),
- UNHRC/ACNUR (Agence des Nations Unies pour les Réfugiés).





Les criminels face à l'hacktivisme

Campagne #OpCartel

•6 octobre: Soutenu par Barrett Brown, des Anonymous mexicains menacent le cartel « Los Zetas » si l'un des leurs, enlevé dans la ville de Veracruz, n'est pas libéré,

•28 octobre: la page d'accueil du site de l'ancien procureur de Tabasco, Gustavo Rosario Torres est défacée. On peut y lire « Gustavo Rosario est un zeta »,

•3 novembre: l'otage est libéré,

•9 novembre: quatrième assassinat d'activistes par Los Zetas.

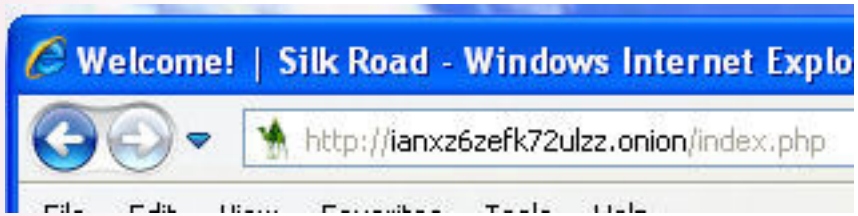
Les Anonymous s'adressent au cartel « Los Zetas »

Les cybercriminels face à l'hacktivisme

Campagne #OpDarknet One

•18 octobre: blocage de sites pédophiles hébergés chez Freedom Hosting. Ceux-ci étaient accessibles sur le « web invisible ». Diffusion des noms/pseudos de 1589 personnes utilisant la plateforme « Lolita City », hébergeur de photos d'abus sexuels sur mineurs.

Logo du site Lolita City



Exemple d'une URL utilisée pour rejoindre le « web invisible », accessible via l'outil d'anonymisation TOR

Les Anonymous face à leurs contradictions

2011 une année de délations

Rappel 2010

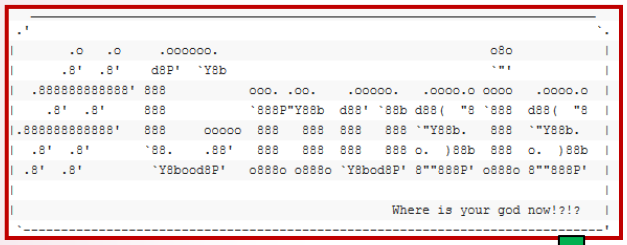
- Juin 2010: le hacker Adrian Lamo dénonce le soldat Bradley Manning
- 30 décembre 2010: Jester (« hacktiviste au service du bien ») divulgue des informations sur des attaquants Paypal.

2011

- Février 2011: Fichier Aaron Barr/HBGary (plus de 130 noms et pseudos)
- Mars 2011: Fichier Backtrace Security (plus de 80 noms et pseudos)
- Mai 2011:
  - Fichier Ryan (environ 650 adresses IP et pseudos)
  - Dénonciations réciproques (Ryan/ev0)
- Juin/Septembre 2011:
  - Sites délateurs TeaMpOison, Web Ninjas, Jester, Lulzsecexposed, etc.
  - Liste A-Team

CLUSIF

Les Anonymous face à leurs contradictions



BACKTRACE SECURITY

TEAMPOISON

th3j35t3r

@operationunmask
Operation Unmask

2011: la guerre des clans

Les hacktivistes face à leurs contradictions

En 2011, les tentatives d'actions coordonnées entre manifestants et cyber-manifestants ont eu peu d'impact.

DATE (2011)	DANS LA RUE	SUR INTERNET
20 MARS	International Bradley Manning Support Day	Operation Bradical
16 AVRIL	Worldwide sit-in at Sony store	OpSony (1ère attaque)
13/15 AOUT	Sit-in à la Civic Center BART station (BART: San Francisco's Bay Area Rapid Transit)	#operationBART
SEPTEMBRE	Day of Rage (le 17)	Day of Vengeance (le 24)
2 OCTOBRE	Occupy Wall Street	Invade Wall Street
26 OCTOBRE	OccupyOakland	OpUprise

Les hacktivistes face à leurs contradictions

En 2011, les dissensions entre diverses factions Anonymous ont desservi leur cause.

DATE (2011)	ACTIONS DEMENTIES
6 FEVRIER	HBGary
22 AVRIL	Opération Sony
2 OCTOBRE	Invade Wall Street
OCTOBRE	Opération Cartel
5 NOVEMBRE	Opération Facebook
24 DECEMBRE	Attaque Startfor

L'Hacktivisme en 2011 – Références 1/3

- Telecomix, les empêcheurs de censurer en rond.

http://www.rezocitoyen.fr/telecomix-hacker-pour-la-liberte.html

- Telecomix wiki – Egypt/Main Page

http://werebuild.eu/wiki/Egypt/Main_Page

- Telecomix: des hackers pour communiquer librement, une méduse pour traquer les surveillants

http://blog.lesoir.be/geek-politics/2011/12/29/telecomix-des-hackers-pour-communiquer-librement-une-meduse-pour-traquer-les-surveillants/

- Bulletin du Ministère de la Sécurité Intérieure US

http://info.publicintelligence.net/NCCIC-Anonymous.pdf

- Sony Sees $3.2 Billion Loss After Projecting Profit

http://www.npr.org/2011/05/23/136575271/sony-sees-3-2-billion-loss-after-projecting-profit

- A concise history of recent Sony hacks

http://attrition.org/security/rants/sony_aka_sownage.html

- Cyberactivists warned of arrest (l'origine de l'affaire HBGary)

http://www.ft.com/intl/cms/s/0/87dc140e-3099-11e0-9de3-00144feabdc0.html

- HBGary Hearts Apple

http://www.forbes.com/sites/seanlawson/2011/02/22/hbgary-hearts-apple/

L'Hacktivisme en 2011 – Références 2/3

- Anonymous Denies Hacking Stratfor

http://www.talkleft.com/story/2011/12/25/124727/35

- Les hackers d'Anonymous lancent l'opération « Green Rights »

http://www.ecologie.tv/politique/les-hackers-d-anonymous-lancent-l-operation-green-rights-19072011-3180.html

- November 18, 2011 UC Davis Police Response to Occupy UC Davis

http://daviswiki.org/November_18,_2011_UC_Davis_Police_Response_to_Occupy_UC_Davis

- Quelques vidéos de Radio Libertaire

http://www.rezocitoyen.fr/rezo.php?page=video_telecomix

- Copwatch – jugement rendu le 14 octobre 2011

http://www.economie.gouv.fr/files/files/directions_services/daj/publications/lettre-daj/2011/lettre108/tgi_paris_copwatch.pdf

- Données persos : le piratage a visé le groupe UMP à l'Assemblée

http://www.rue89.com/2011/11/08/les-donnees-personnelles-dun-millier-de-cadres-ump-piratees-226342

- Campagne #opCartel

http://sergeadam.blogspot.com/2011/11/une-victoire-danonymus-contre-le-cartel.html

L'Hacktivisme en 2011 – Références 3/3

- Anonymous collects, publishes IP addresses of alleged pedophiles

http://arstechnica.com/business/news/2011/11/anonymous-collects-publishes-ip-addresses-of-alleged-pedophiles.ars

- The Rise and Fall of Anonymous

http://blogs.mcafee.com/mcafee-labs/the-rise-and-fall-of-anonymous

- Frédéric Bardeau, Co-auteur de « Anonymous : peuvent-ils changer le monde ? »

http://www.france24.com/fr/20111229-entretien-frederic-bardeau-co-auteur-anonymous-peuvent-ils-changer-le-monde

- Anonymous entrerait-il en phase de dissolution ?

http://www.fluctuat.net/blog/30929-Anonymous-entrerait-il-en-phase-de-dissolution-

- Anonymous prévoit de détruire Facebook le 5 novembre prochain

http://www.zonebourse.com/barons-bourse/Mark-Zuckerberg-171/actualites/Anonymous-prevoit-de-detruire-Facebook-le-5-novembre-prochain--13753673/

- Antisec is not Anonymous

http://www.chronicle.su/editorial/antisec-is-not-anonymous/

Evénements judiciaires et débats juridiques

Lieutenant-colonel Éric FREYSSINET

Chef de la division de lutte contre la cybercriminalité

Pôle judiciaire de la gendarmerie nationale

Plan de l'intervention

- Le rapport de l'ONDRP
- Retour sur les évolutions juridiques 2011 et à venir
- Données personnelles, données confidentielles
- Le rançongiciel « gendarmerie »

Rapport de l'ONDRP 2011 – Dossier Cybercriminalité

Un centre européen de lutte contre le cybercrime en 2013. A Europol ?

Le Point.fr

24h d'info · Flux RSS · Mobile · Newsletters · Sommaire · Abonnement · Édition digitale · Nos publications · Météo · Bourse · Jeux-Concours

ACTUALITÉ | Débattre | POLITIQUE | ÉCONOMIE | TECH & NET | SANTÉ | CULTURE | ART DE VIVRE

Tech & Net | Guide du numérique | Jeux vidéo | Planète Appli

ACTUALITÉ › Tech & Net RSS

Le Point.fr - Publié le 23/11/2011 à 11:13

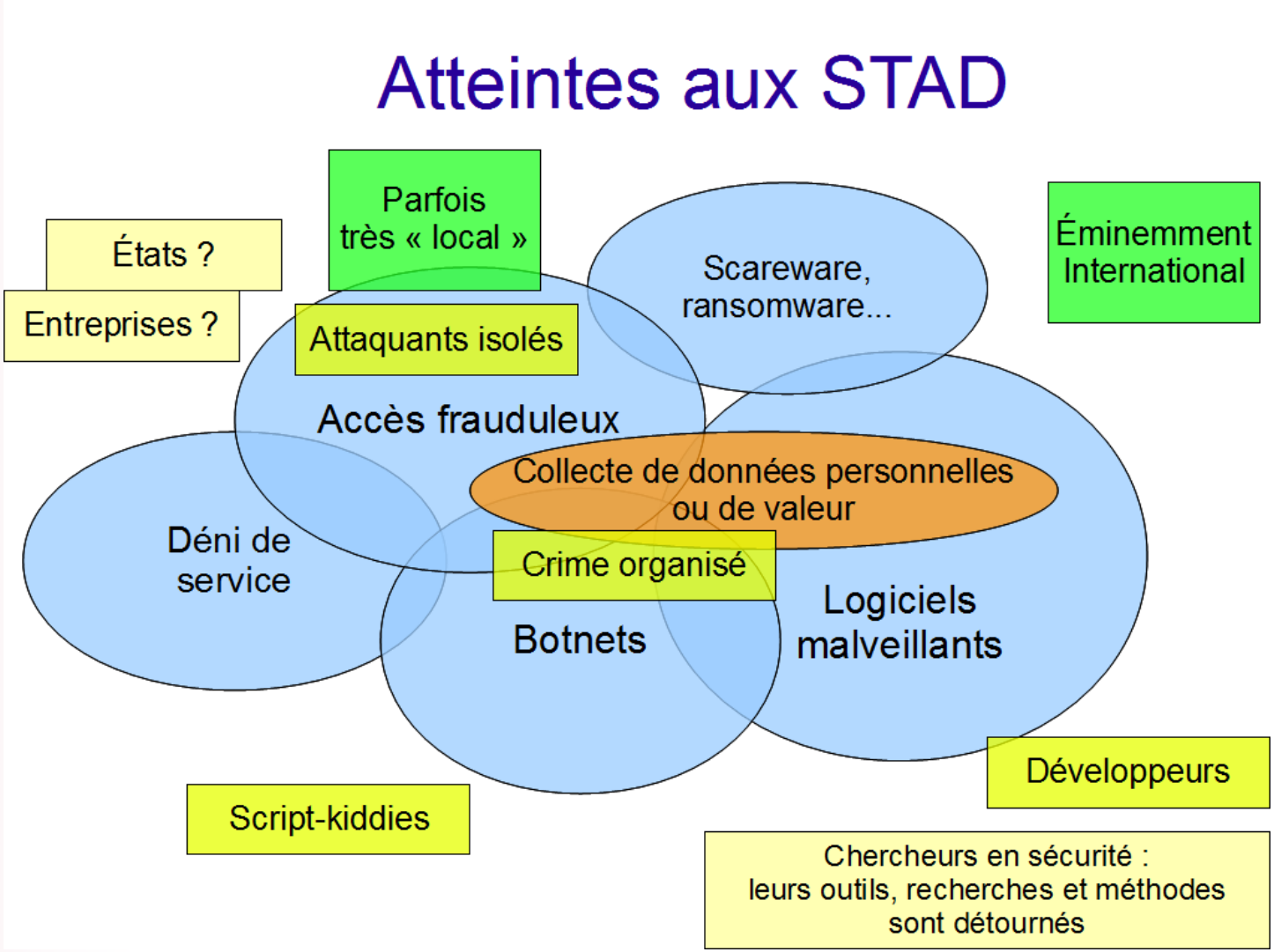
Internet : plus de 33 000 infractions constatées en 2010

Selon une étude officielle, l'ampleur de la cybercriminalité est évaluée à 1,7 milliard d'euros l'année dernière.

80 % de la cybercriminalité commise en France concerne des cas d'escroquerie. © Witt / Sipa

Une première étude chiffrée « officielle » en France

Rapport ONDRP – Profils des cybercriminels



Nouveaux textes

- LOPPSI 2
  - Blocage des sites pédopornographiques
  - Usurpation d'identité
  - Dispositifs de captation de données
- Directives européennes
  - Protection des mineurs 2011/92/UE
  - Attaques contre les systèmes informatiques (à venir)
- Obligation de notification des incidents de sécurité
  - Concerne pour l'instant les fournisseurs de services de communication électronique accessibles au public

Données personnelles, données confidentielles

- Réseaux sociaux
- Applications mobiles (toujours et encore)
- Données personnelles volées en masse
- Les données confidentielles sont-elles en sécurité ?

Les réseaux sociaux sous surveillance

Friending Facebook
Emil Protalinski

Home / News & Blogs / Friending Facebook

Facebook promises changes following Irish privacy audit

By Emil Protalinski | December 21, 2011, 2:15pm PST

Summary: *Ireland's Data Protection Commissioner has completed his three-mo audit of Facebook's activities. Facebook's international headquarters is in Dublin, are affected.*

Facebook today announced that the office of Billy Hawkes, the Irish Data Protection Commissioner (DPC), has completed its privacy audit of the company's practices and policies. The DPC report has concluded Facebook adheres to European data protection principles and complies with Irish law. Nevertheless, Menlo Park has promised to make changes based on recommendations from the DPC.

ZDNet 20th Anniversary

Un bilan complet fait en Irlande

LeMondeInformatique.fr
Toute l'info et les tendances du monde IT

CONFERENCE STRATEGIQUE
Poste de travail : segmenter les usages
Industrialiser l'hétérogénéité

Accueil | Réseau | Mobilité | Sécurité | Stockage | Datacenter | Logiciel | Virtualisation

OS | Internet | Emploi | Business | Dossiers | Entretiens | PME | Vidéos | Newsletters

Toute l'actualité > Sécurité > Données personnelles

Désormais sous surveillance, Facebook a reconnu ses tromperies

Page précédente 1 2 Page suivante

Edition du 30/11/2011 (3 commentaires) Partager

Crédit Photo: D.R

Selon la Federal Trade Commission (FTC) américaine, le site de réseau social aurait trompé les utilisateurs en matière de confidentialité à « de nombreuses occasions ». En conséquence, Facebook va être placé sous surveillance pendant 20 ans.

Facebook a accepté de prendre en compte les accusations de la Federal Trade Commission, qui estime que le réseau social a trompé les utilisateurs « à de nombreuses reprises, » affirmant d'un côté que les informations privées de leurs utilisateurs étaient protégées, alors que, d'un autre, le réseau les a partagé plusieurs fois, comme l'a déclaré la FTC. L'institution américaine a relevé que dans un « certain nombre de situations, » Facebook avait fait, en matière de protection de la vie privée des utilisateurs, des promesses « qu'elle n'avait pas tenu, » a ajouté la FTC dans son communiqué.

Facebook suivrait ses abonnés même déconnectés

Et toujours les applications mobiles

Carrier IQ transmet-il les données personnelles au FBI?

20minutes.fr

CARRIER iQ™

Carrier IQ Updates Statement: Operators Use Carrier IQ Software Only to Diagnose Operational Problems on Networks and Mobile Devices

Mountain View, CA – December 1, 2011 – To clarify misinformation on the functionality of Carrier IQ software, the company is updating its statement from November 23rd, 2011 as follows:

We measure and summarize performance of the device to assist Operators in delivering better service.

- Surtout un problème de maturité et de transparence

Carrier IQ faces federal probe into allegations software tracks cellphone data

By Sari Horwitz, Published: December 14

The Washington Post

Federal investigators are probing allegations that Carrier IQ software found on about 150 million cellphones tracked user activity and sent the information to cellphone companies without informing consumers, according to government officials.

Vols massifs de données personnelles

Data stolen from 35 million South Korean social networking users

by Graham Cluley on July 28, 2011

Contract Worker Steals Personal Data On 9 Million Israelis

Worker created a searchable database in order to sell it to private buyer, officials say

Oct 24, 2011 | 09:50 AM | 0 Comments

Steam Attack Puts Users at Risk of Spear Phishing

Wednesday, November 16, 2011

Contributed By: Josh Shaul

Steam Database Attack Puts Users At Risk Of Spear Phishing Scams

Last week it was announced that attackers gained access to Steam, an online video gaming platform run by parent company, Valve.

According to the information posted on Steam's website, the first phase of this massive attack was the insertion of targeted malicious ads or "malvertising" offering to sell cheat codes for online games to users of the Steam forums.

Initially, the company thought that only its forums had been infiltrated, until late last week when it was announced that its database housing personal information of its 35 MILLION customers had also been compromised.

- A quand une prise de conscience?
- La législation est-elle à la hauteur des enjeux?

Fuites de données sensibles

Fuites au bac S : l'épreuve de maths ne sera pas annulée

Un exercice du sujet de mathématiques avait été révélé lundi soir sur le forum d'un site internet. Les candidats ne seront notés que sur trois exercices au lieu de quatre, a indiqué Luc Chatel, qui annonce le dépôt d'une plainte.

Par Marion Brunet

- Connaît-on les données à protéger?
- Comment prévenir, réagir?

Hacker cuffed in job interview sting with hotel he blackmailed

Hungarian demanded Marriott job after stealing secrets

By **John Leyden** • **Get more from this author**

Posted in Security, 28th November 2011 16:39 GMT

Free whitepaper – King's College London uses IBM System Networking RackSwitch for HPC

A job-seeking Hungarian hacker has pleaded guilty to breaking into the systems of the Marriott hotel chain before attempting to blackmail his way into an IT job.

Attila Nemeth, 26, sent Trojan-infected emails to Marriott employees late last year, according to his plea agreement, in a move that successfully allowed him to extract confidential and financially sensitive information from the hotel chain's network. He then apparently threatened to reveal this information unless he was given a job maintaining Marriott's systems.

Le rançongiciel « gendarmerie »

Copie d'écran de la dernière version du « rançongiciel »

Références

- Rapport ONDRP 2011 - http://www.inhesj.fr/fichiers/ondrp/rapport_annuel/ra2011/synthese_rapport_2011.pdf
- Textes
  - Obligation de notification des incidents de sécurité http://www.reseaux-telecoms.net/tribunes-experts/lire-notification-des-incidents-de-securite%C2%A0-le-rssi-doit-se-preparer-a-un-changement-en-profondeur-48.html
  - Directive européenne sur la protection des mineurs http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:FR:PDF
- Données personnelles
  - Facebook http://www.zdnet.com/blog/facebook/facebook-promises-changes-following-irish-privacy-audit/6511, http://www.lemondeinformatique.fr/actualites/lire-desormais-sous-surveillance-facebook-a-reconnu-ses-tromperies-46825-page-2.html
  - http://www.darkreading.com/database-security/167901020/security/privacy/231901478/contract-worker-steals-personal-data-on-9-million-israelis.html
  - http://www.infosecisland.com/blogview/18164-Steam-Attack-Puts-Users-at-Risk-of-Spear-Phishing.html
  - http://nakedsecurity.sophos.com/2011/07/28/data-stolen-from-35-million-south-korean-social-networking-users/
  - http://www.theregister.co.uk/2011/11/28/hungarian_hacker_hotel_sting/
  - Carrier IQ: http://www.20minutes.fr/high-tech/842612-carrier-iq-transmet-il-donnees-personnelles-fbi, http://www.carrieriq.com/company/PR.CIQ_Press_Statement_DEC_1_11.pdf , http://www.washingtonpost.com/business/economy/feds-probing-carrier-iq/2011/12/14/gIQA9nCEuO_story.html
- Fuite de données sensibles
  - http://www.lefigaro.fr/actualite-france/2011/06/22/01016-20110622ARTFIG00403-soupcons-de-fuites-avant-l-epreuve-de-maths-du-bac-s.php
- Virus gendarmerie
  - http://blog.crimenumerique.fr/2011/12/17/le-virus-gendarmerie-bilan-de-la-semaine/
  - http://www.malekal.com/2012/01/10/virus-gendarmerie-activite-illicite-demelee/

Hacking dans le biomédical

Eric Grospeiller

Fonctionnaire de Sécurité des Systèmes d'Information

Ministère du Travail, de l'Emploi et de la Santé

Malwares et établissements de santé

En 2009, CONFIKER perturbe des établissements de soins

En 2011, un hôpital près d'Atlanta subit des perturbations importantes…

Les points communs :

Propagation rapide d'un ver

Supervision « faible »

Interconnexion des réseaux

Points d'entrée non maitrisés

Mais aucune perturbation des services aux patients !

A propos des patients…

L'actualité nous rappelle chaque jour les dangers des dispositifs médicaux.

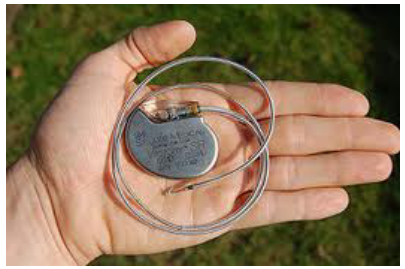
Ces dispositifs sont aussi des dispositifs actifs :

Appareils de surveillance, monitoring, in situ ou à distance,

Pacemaker,

Pompes à insuline,

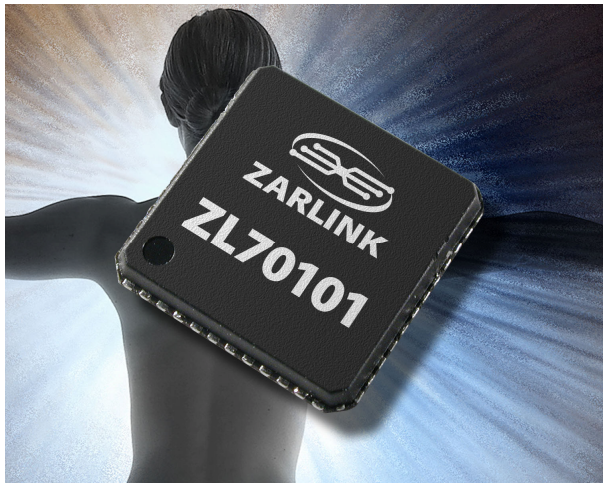
….



Point commun :

Utilisation de technologie sans fil…

- Bluetooth
- Wifi,
- Radio …



Cas des pompes à insuline

Jay Radcliffe à démontré lors de la Black Hat qu'il est possible de prendre le contrôle d'une pompe à insuline.

Il a réussi a modifier les informations pour délivrer une dose mortelle.

Il a intercepté la fréquence de communication propriétaire et l'a retransmise modifiée pour changer le ratio sucre/sang.

Cette démonstration fait suite aux publications de 2008 sur le danger des pacemakers.

Virus et transport d'urgence…

Les centres de communication d'Aucland, Wellington et Christchurch touchés par un virus.

La conséquence de l'incident est l'affectation manuelle des moyens de transport.

Le service touché traite 90% des transports médicalisés, qu'ils soient d'urgence ou non.

Les systèmes touchés sont les systèmes radio et de messages.

Rien ne permet d'affirmer qu'il s'agissait d'une attaque ciblée.

Pour conclure

L'utilisation généralisée d'un nombre limité de systèmes d'information étend la menace à des outils de production qu'il est nécessaire de sécuriser. La frontière des spécificités métier ou production n'est plus une protection.

De manière plus large, la mutualisation est une source de vulnérabilité.

Références

Confiker et établissements de santé

http://www.tomshardware.com/news/Conficker-Worm-Hospital-Equipment,7620.html

http://www.ticsante.com/show.php?page=story&id=495

Atlanta

http://nakedsecurity.sophos.com/2011/12/13/malware-shuts-down-hospital-near-atlanta-georgia/

Pompe à insuline et pacemaker

http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

http://blogs.computerworld.com/18744/black_hat_lethal_hack_and_wireless_attack_on_insulin_pumps_to_kill_people

http://www.secure-medicine.org/icd-study/icd-study.pdf

Appels d'urgence

http://www.stuff.co.nz/waikato-times/news/5953497/Computer-virus-hits-ambulances

http://nakedsecurity.sophos.com/2011/11/14/ambulance-service-disrupted-by-computer-virus-infection/

SCADA, services de secours, systèmes d'armes : tous ciblés

Eric Grospeiller

Fonctionnaire de Sécurité des Systèmes d'Information

Ministère du Travail, de l'Emploi et de la Santé

Les infrastructures de production en première ligne

Inquiétude de l'industrie du pétrole face à l'augmentation des cyber attaques sur leurs infrastructures.

Les conséquences sont économiques, humaines et environnementales :

Vols de données confidentielles ou de recherche,

Prise de contrôle de la distribution,

Destruction de sites ou d'équipements.

En cause, Stuxnet et puis DUQU.

"Everyone can hack today," Shell's Luehmann said. "The number of potential hackers is not a few very skilled people -- it's everyone."

Un succès de la formation et de la vidéo en ligne …

Le traitement d'eau comme cible…

Springfield : destruction d'une pompe de distribution d'eau à la suite d'une prise de contrôle de son système SCADA. La destruction est due au fonctionnement à vide de la pompe.

L'intrus met la main sur les données des clients (identifiants, mots de passe,…) du concepteur de la solution.

Il ne reste plus qu'à rendre visite au client… Qui souvent est accessible pour raison de maintenance.

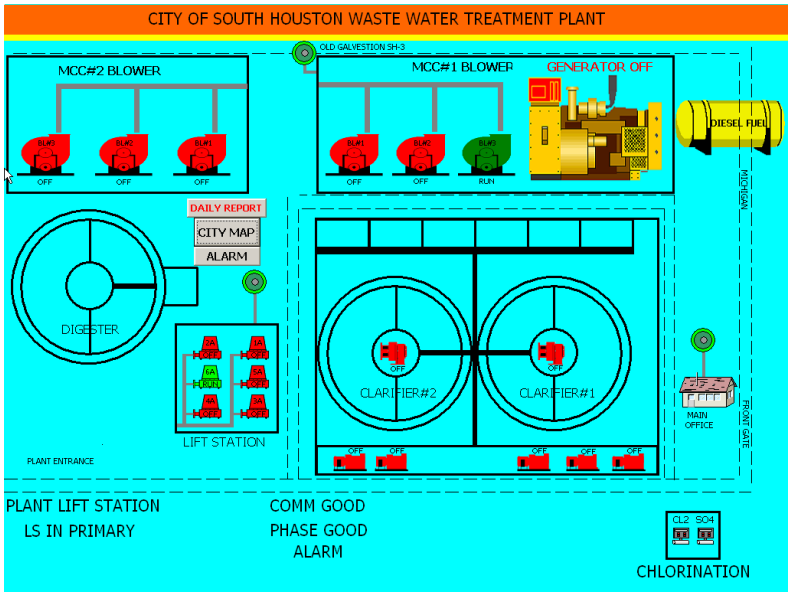
L'adresse IP qui a pu être tracée à conduit vers un pays étranger qui peut n'être qu'un rebond…

L'intrus était présent dans le système depuis 2 mois…

Eau : après Sprinfield, Houston…

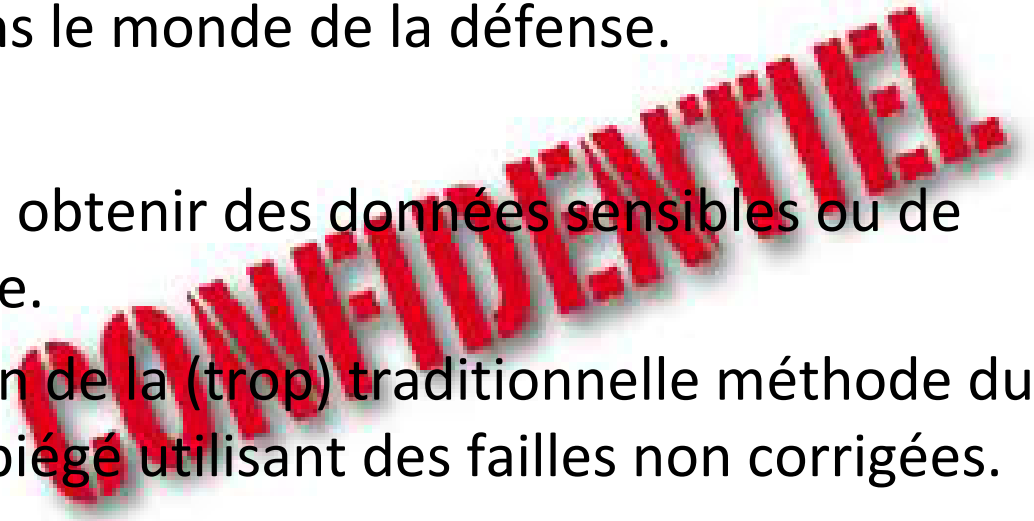
Houston : intrusion dans le système, avec publication de captures d'écran de ce qui semble être le système de supervision de la gestion de l'eau d'une partie de la ville.

L'intrus réagissait aux propos qui minimisaient l'état d'insécurité des installations…



L'industrie chimique et de la défense en ligne de mire…

29 entreprises de l'industrie chimique prises pour cible.
Et 19 dans le monde de la défense.



Objectif : obtenir des données sensibles ou de recherche.

Utilisation de la (trop) traditionnelle méthode du courriel piégé utilisant des failles non corrigées.

L'infection des postes (Poison Ivy or Backdoor.0divy) s'effectue par un clic sur une des pièces jointes.

Infection de drones militaires

Les systèmes de pilotage des drones militaires infectés par un virus.

Les drones Predator et Reaper sont concernés.

Le code malveillant se contente d'enregistrer les actions sans interférer avec les missions (en zone d'opération…). La menace est qualifiée de persistante, mais bénigne…

Les satellites sont (aussi) vulnérables…

Un rapport du Sénat Américain indique qu'en 2007 et 2008, des interférences ont affecté deux satellites.

L'origine malveillante est prise au sérieux.

Ces interférences auraient été permises grâce à une intrusion dans la station de contrôle.

Heureusement, perturbation ne signifie pas accès ! Ce qui permettrait contrôle, dégradation, voire destruction. Les suspects nient toute implication…

Comme les trains…

Le système d'aiguillage serait vulnérable…

Longtemps propriétaires, ces systèmes sont en voie de standardisation à l'initiative d'une groupement d'industriels qui a donné naissance au GSM-R (version sécurisée du GSM).

Sa particularité est d'utiliser des clés de chiffrement stockées sur clés USB… Qu'il faut être capable de gérer en toute sécurité…

Et les serrures sur IP...

Stuxnet appliqué aux serrures sur IP :

Une étude réalisée par 3 chercheurs a montré que les automates de gestion de l'ouverture et de fermeture des portes de prison peuvent être pilotés depuis Internet…

Pour conclure

Toutes les infrastructures connectées sont des cibles potentielles, par ciblage ou effet de bord.

La communication est nécessaire, mais elle peut s'avérer dangereuse et ne règle en aucun cas les vulnérabilités.

Références

Inquiétudes dans le monde du pétrole

http://www.bbc.co.uk/news/technology-16137573

http://af.reuters.com/article/commoditiesNews/idAFL5E7N81C920111212

Drones

http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

http://www.cbsnews.com/stories/2011/10/08/earlyshow/saturday/main20117624.shtml

Eau

http://www.wired.com/threatlevel/2011/11/hackers-destroy-water-pump/

http://www.theregister.co.uk/2011/11/17/water_utility_hacked/

http://www.branchez-vous.com/techno/actualite/2011/11/springfield_eau_pirate_scada.html

http://nakedsecurity.sophos.com/2011/11/18/us-scada-infrastructure-woefully-unprotected/

Industries chimique et de défense :

http://www.theregister.co.uk/2011/10/31/chemical_firms_hacked/

Références

Drones

http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

http://www.cbsnews.com/stories/2011/10/08/earlyshow/saturday/main20117624.shtml

Satellites

http://www.undernews.fr/hacking-hacktivisme/un-satellite-en-orbite-pas-a-l%E2%80%99abri-d%E2%80%99un-piratage.html

Trains

http://www.canada.com/canspell/Hackers+could+shut+down+train+lines/5918784/story.html

http://www.bbc.co.uk/news/technology-16347248

Serrures sur IP

http://www.cnis-mag.com/log-picking-a-la-stuxnet-%E2%80%A6.html

Conclusion

En conclusion, nous aurions aussi aimé évoquer…

- **Veille et qualification de l'information** : une nécessité dans un monde de surinformation
- **Gouvernance de l'Internet**… parfois chaotique
- **Criminalité et jeux en ligne**… hors de France
- **Attaques contre les IPBX** (centraux téléphoniques IP)

Questions aux Intervenants…

Cocktail !..