CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Panorama de la cybercriminalité année 2010

Paris, 12 janvier 2011

Evénement organisé en partenariat avec :

Orange Business Services **TelecityGroup**

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)

ADHÉRENT CLUSIF 2011

Logo pour vos actions commerciales, votre site web

Anticiper les tendances

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

Promouvoir la sécurité

Adhérer…

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Groupes de travail en progression

Les groupes actifs en 2011

- DDoS
- Documentation de MEHARI™
- Fiches de sécurité pour la micro-informatique
- Gestion de clés cryptographiques
- Gestion des incidents
- Guide d'audit de sécurité physique
- Panorama de la cybercriminalité
- PCI-DSS
- Principes, mécanismes et bases de connaissances de Méhari
- Sécurité des Applications Web - Suite
- Sécurité des Outils de Communication
- Série 27000 / Métriques
- Virtualisation et Sécurité

… et des Espaces dédiés

Espaces de travail actifs en 2011

- Espace Méthodes
- Espace Menaces
- Espace RSSI

Nouveaux GT en annonce, surveillez les flux RSS... RSS/actus CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Une collaboration à l'international, des actions en région

CLUSIF

CLUSIB BELCLIV

CLUSIL

CLUSIS

CLUSIQ

Clusit

CLUSI-BF
Club de Sécurité des Systèmes d'Information du Burkina Faso

CLUSI Côte d'Ivoire

Boite Postale 2409 Abidjan 25

Contact : M. KOUAKOU Clauba Jean de la Croix (Président)
Tel/Fax : (00225) 22 42 42 66
Secrétariat : contact@clusici.org
Web : http://www.clusici.org/.

Club de la Sécurité de l'Information Région Tahiti
Adresse physique : Immeuble SALMON Faa'a Pamatai - Tahiti - Polynésie Française
Adresse postale : B.P. 60123 - Hotuarea - 98704 Faa'a - Tahiti - Polynésie Française
Contact : Matthieu DRUILHE, clusir.tahiti@gmail.com, téléphone : +689 79 82 27
Site web : http://www.clusif.asso.fr/clusir-tahiti/

Club de la Sécurité des Systèmes d'Information du Languedoc-Roussillon
954, avenue Jean Mermoz
34000 MONTPELLIER
Contact : Christian FERRAND
Site web : www.clusirlr.info

Club de la Sécurité des Systèmes d'Information de la Région Midi Pyrénées
S/C INSA
Département de Génie Electrique et Informatique
135, Avenue de Rangueil
31077 TOULOUSE CEDEX 04
Contact : Laurent PELUD
Site web : www.clusir-mp.asso.fr

Club de la Sécurité des Systèmes d'Information de la Région Est
16, rue de Pont-à-Mousson
57000 METZ
Contact : Thierry RAMARD
Site web : www.clusir-est.fr

Club de la Sécurité des Systèmes d'Information de la Région Provence-Alpes-Côte-d'Azur
500, rue de Paradis
13008 MARSEILLE
Contact : Claude LELOUSTRE
Site web : http://www.clusif.fr/clusir-paca/

Club de la Sécurité des Systèmes d'Information de la Région Rhône-Alpes
SITIV
Passage de l'Avenir
69200 VENISSIEUX
Contact : Yannick BOUCHET
Site web : www.clusir-rha.fr

Club de la Sécurité des Systèmes d'Information de la Région Nord Pas de Calais Picardie
1862, avenue Général De Gaulle
59910 BONDUES
Contact : Gérard MOLINES
Site web : http://www.clusif.fr/clusir-npp/

Club de la Sécurité de l'Information de Poitou-Charentes
Technopole Venise Verte
Rue Euclide
BP 8421
79024 NIORT cedex 9
Contact : Sébastien Gioria
Site web : http://www.clusir-poi.fr/

Club de la Sécurité de l'Information Région Aquitaine
s/c Philippe Marty (Vice-Président)
51 rue Manon Cormier
33000 Bordeaux
Contact : Marc Ferrigno

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 2010

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
- Hervé Schauer Consultants
- McAfee Labs
- LEXSI
- Orange Labs, Networks and Carriers
- SNCF
- Telindus France
- Bundeskriminalamt (Office fédéral de police criminelle), Unité SO 43 (National High Tech Crime Unit)
- 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

Interventions, Panorama 2010 (1/2)

- Stuxnet : les mystères d'une cyber-attaque industrielle

M. Jean-Michel DOAN

✉ Analyste Cybercriminalité – LEXSI
jdoan@lexsi.com

- [Evocation] Automobile, les OS embarqués

M. Jean-Michel DOAN

✉ Analyste Cybercriminalité – LEXSI
jdoan@lexsi.com

- Hacktivisme : entre criminalité et militantisme

M. François PAGET

✉ Chercheur de menaces – McAfee Labs
Francois_Paget@avertlabs.com

Interventions, Panorama 2010 (2/2)

- Le crime est de plus en plus mobile…

  M. Eric FREYSSINET

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

- Botnets : la lutte s'intensifie

  M. Pierre CARON

  ✉ Expert Sécurité – Orange Labs, Networks and Carriers
  pierre.caron@orange-ftgroup.com

- [Evocations] Bugs, IPV6, jeux en ligne

  M. Hervé SCHAUER

  ✉ Consultant – Hervé Schauer Consultants
  Herve.Schauer@hsc.fr

Agenda, Panorama 2010

- **Stuxnet : les mystères d'une cyber-attaque industrielle**
- **[Evocation] Automobile, les OS embarqués**
- Hacktivisme : entre criminalité et militantisme
- Le crime est de plus en plus mobile…
- Botnets : la lutte s'intensifie
- [Evocations]Bugs, IPV6, jeux en ligne…

Un malware intriguant

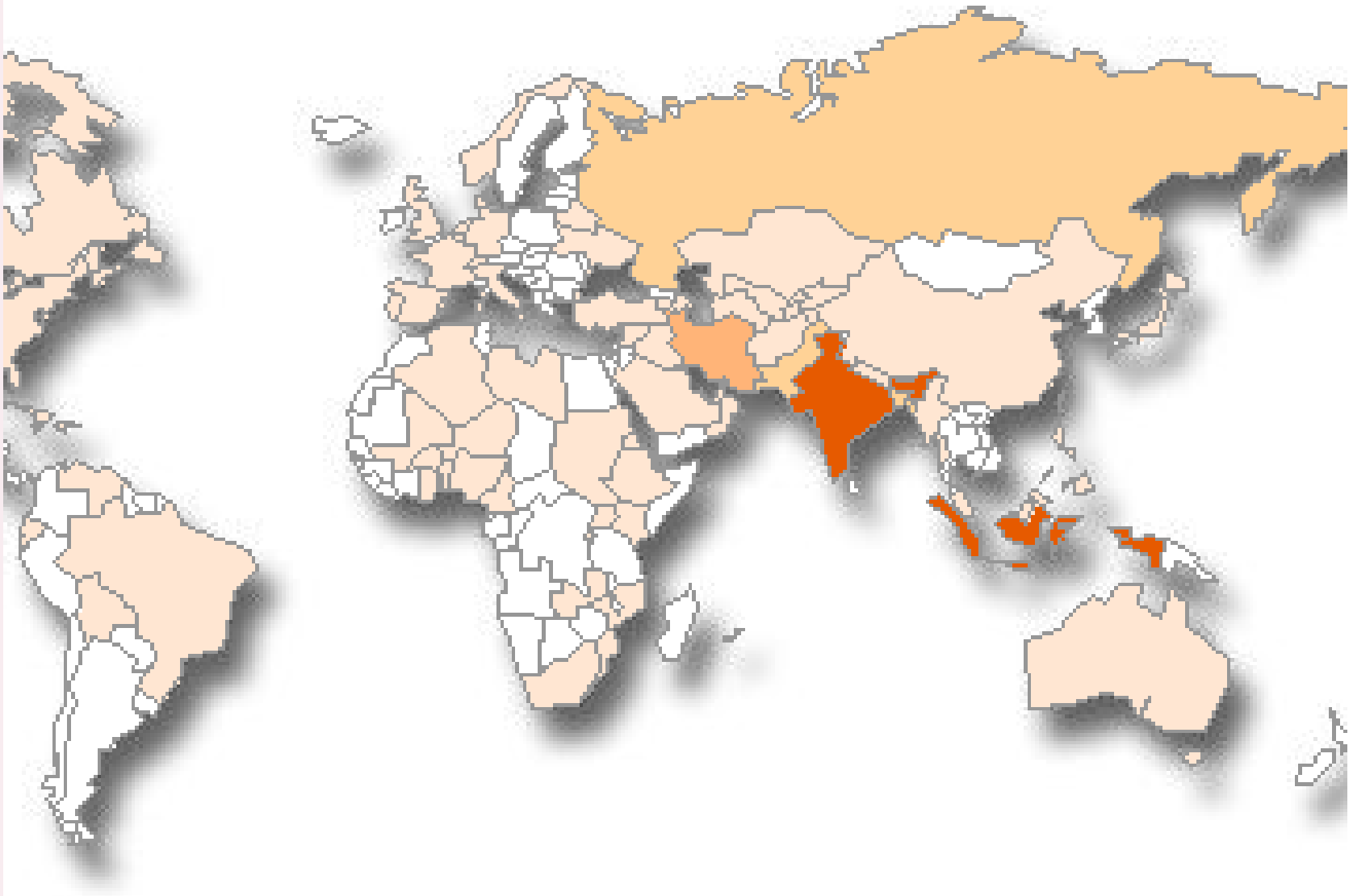
En juin 2010, un petit éditeur antivirus biélorusse découvre une nouvelle menace :

- Dispose de moyens de furtivité impressionnants
- Dispersion géographique étonnante
- Semble cibler les infrastructures industrielles Siemens

Six mois plus tard…

-> une arme pour une opération de sabotage ciblée

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS



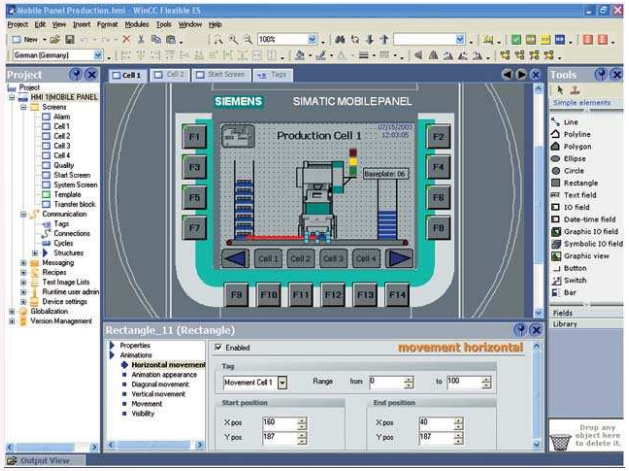
D'importants moyens mis en oeuvre

Propagation locale :

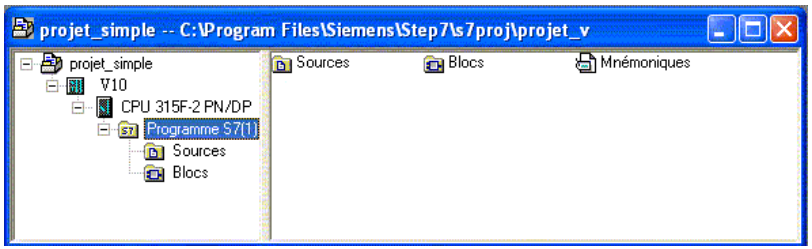
Périphérique stockage amovibles

Imprimantes partagées

Dossiers partagées



Bases de données WinCC (Siemens)



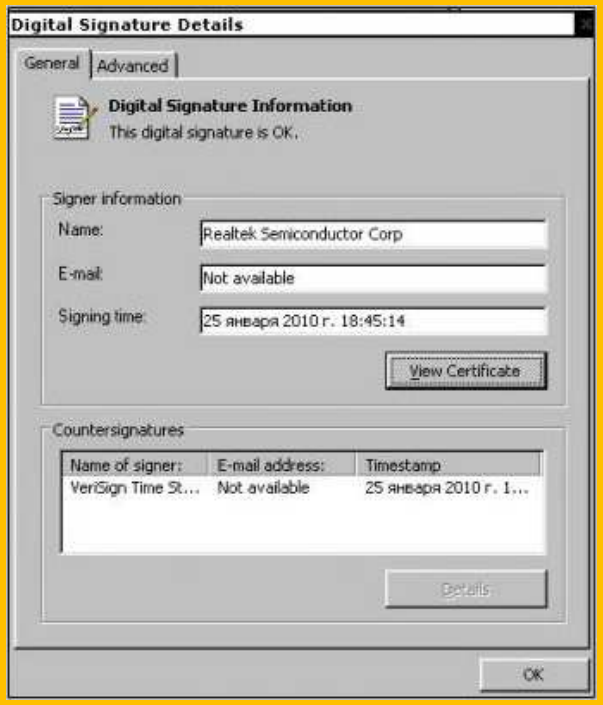
Projets Step7 (Siemens)

D'importants moyens mis en oeuvre

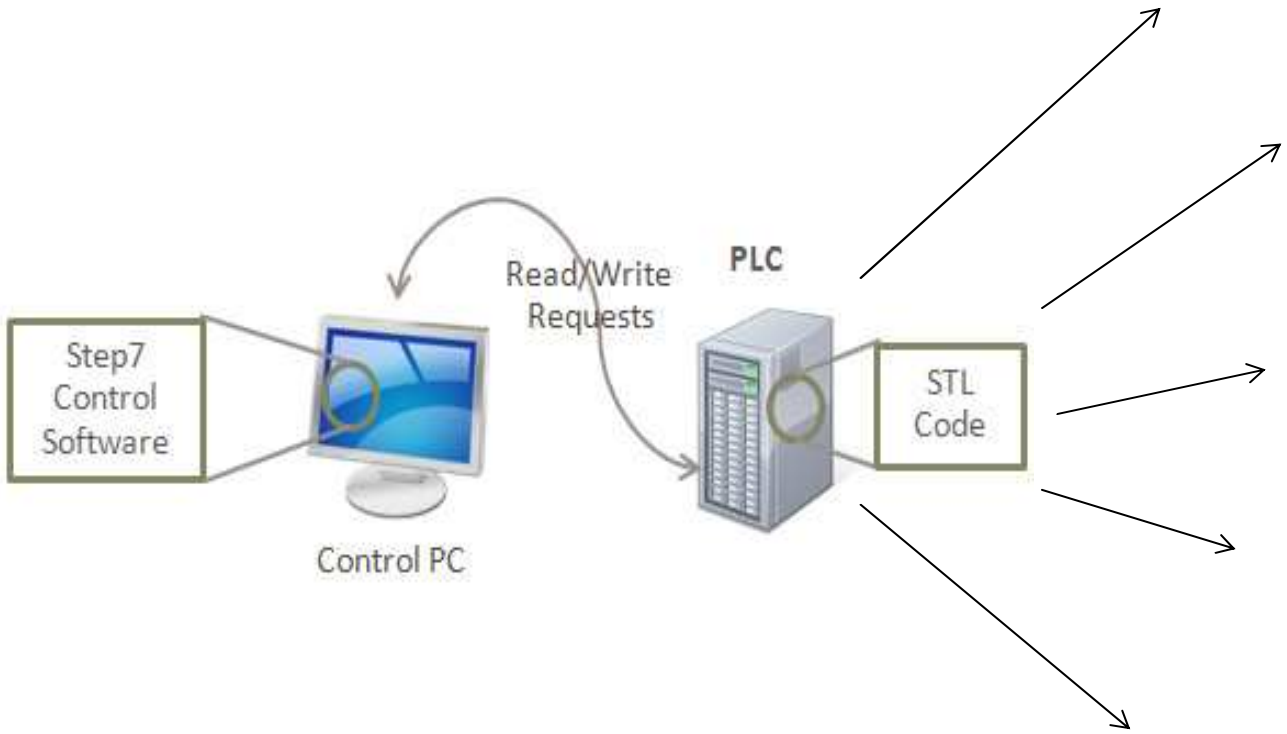
Quatre vulnérabilités non patchées dont trois 0-day

D'importants moyens mis en oeuvre

Utilisation de clés privées volées



L'objectif final :



Une opération de sabotage ciblée

Modifier le comportement d'un processus industriel donné

Pas n'importe lequel !

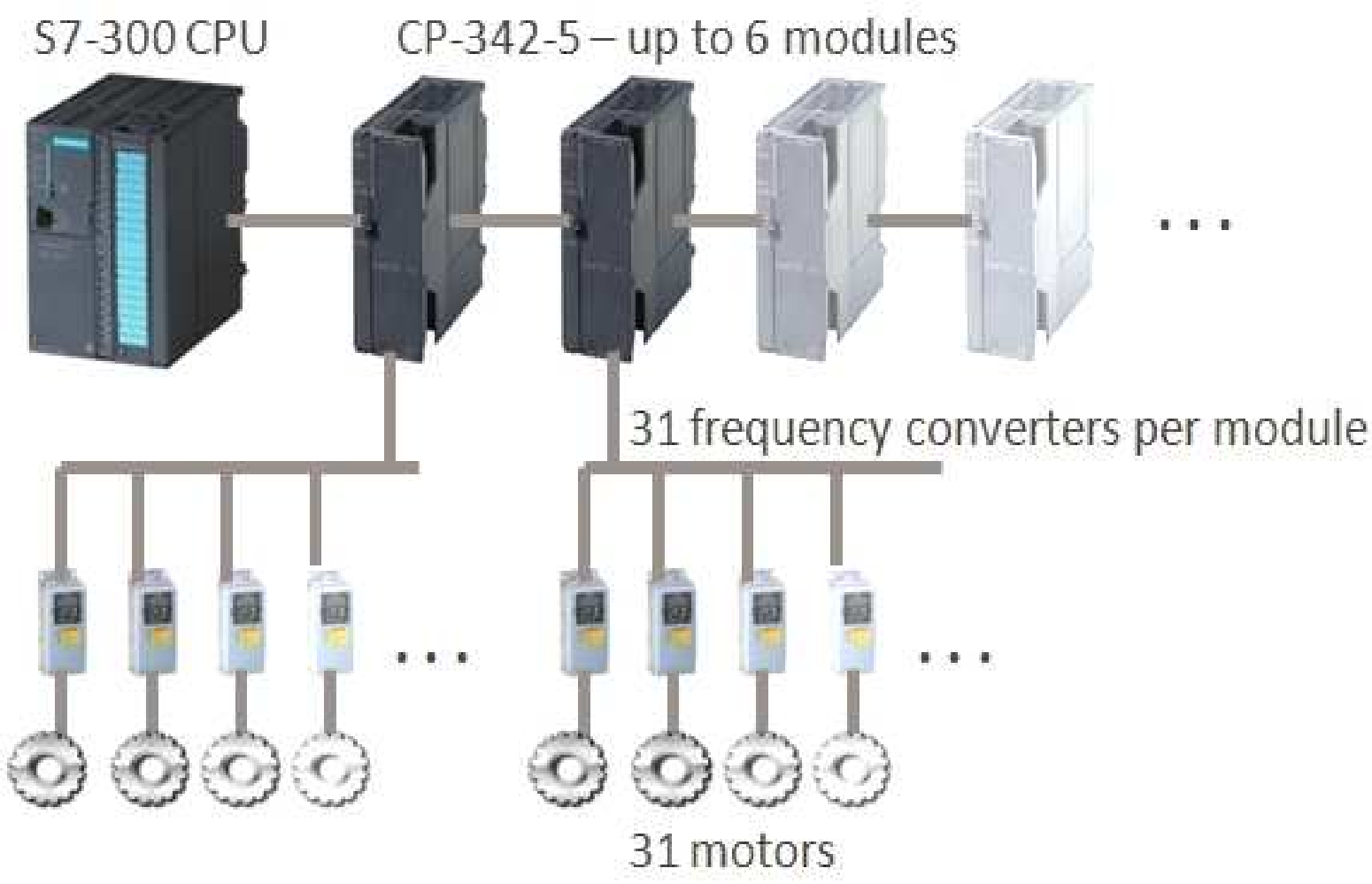
-> Contrôleurs Siemens Simatic **S7-315** ou **S7-417**

uniquement si :

connectés à plusieurs modules de communication **Profibus**

au moins **33** convertisseurs de fréquence **Vacon** ou **Farao Paya** opérant entre **807 et 1210 Hz**

Une opération de sabotage ciblée



Une opération de sabotage discrète

- L'attaque ne se déclenche que tous les 27 jours
- Les processus modifiés sont masqués
- Les systèmes d'alerte sont désactivés

Quelles conséquences ?

Médiatisation

- C'est la première fois qu'une cyberattaque industrielle est rendue publique
- Le mode de propagation laissait penser que toutes les systèmes Siemens étaient ciblés
- «*les infrastructures critiques vulnérables aux cyberattaques ?*»

Mais rien n'a été révélé…

Hypothèses

Quelques indices dans le programmes…

Fausses pistes ? Mauvaises interprétations ?

Ex : Myrtus. Myrte ou MY Remote Terminal Units ?

Cible évoquées	Auteurs évoqués
Iran	Israël, pays occidentaux
Iran	Chine
Inde	Chine
Siemens	?
Chine	USA
…	…

L'Iran : la cible la plus évoquée

Site d'enrichissement d'Uranium de Natanz

Convergences techniques	Inconnues
Cascades de 164 centrifugeuses	Equipements ciblés
Vitesse de rotation des centrifugeuses	Iran dément que Stuxnet a eu un effet
Modifications induites par Stuxnet compatibles avec un endommagement des centrifuges	
USA, Israël, Iran admettent que Natanz est une cible de cyberattaques	

Une guerre de l'information ?

La cible peut être différente ou multiple

On ne sait pas si l'objectif a été atteint

L'objectif peut être plus complexe

Bilan

Stuxnet matérialise les cyberattaques contre les procédés industriels et les infrastructures critiques

Stuxnet sera probablement ré-exploité. Par qui ? Contre qui ?

Les systèmes SCADA ont besoin d'être **précis et performants** et tolèrent difficilement une couche de sécurité supplémentaire

Leur sécurité **reposait sur leur spécificité** et leur **isolation**, mais ils sont de plus en plus connectés vers l'extérieur

Webographie

Analyse technique :

- http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=43876783&caller=view
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf
- http://www.langner.com/en/blog/
- http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Guerre de l'information :

- Stuxnet : Interprétation, Daniel Ventre. MISC 53, Jan/Fev 2011 http://owni.fr/2010/09/29/stuxnet-ou-le-mythe-de-la-cyberguerre-mondiale/
- http://www.f-secure.com/weblog/archives/00002040.html

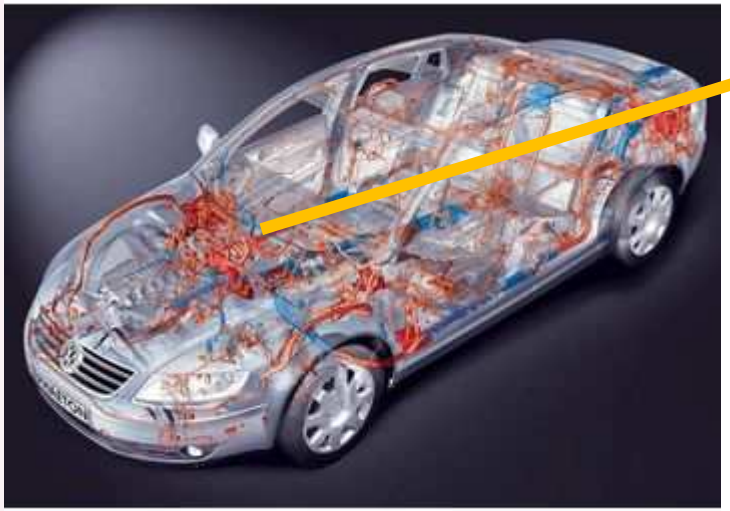
Sécurité des SCADA

- http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/weiss.html

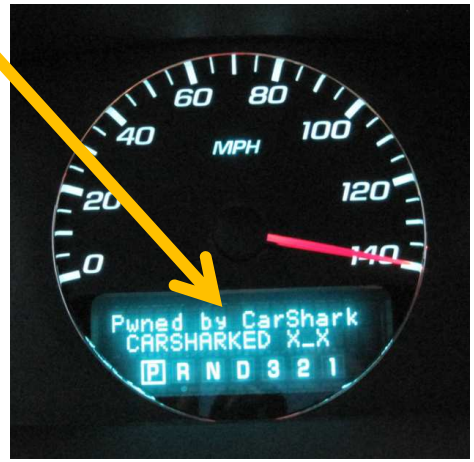
Evocation : les OS embarqués

De plus en plus d'équipements intègrent des systèmes de contrôle :

- Compteur électriques intelligents (*smartgrid*)
- Automobiles



E.C.U.



Agenda, Panorama 2010

- Stuxnet : les mystères d'une cyber-attaque industrielle
- [Evocation] Automobile, les OS embarqués
- **Hacktivisme : entre criminalité et militantisme**
- Le crime est de plus en plus mobile…
- Botnets : la lutte s'intensifie
- [Evocations]Bugs, IPV6, jeux en ligne…

Définitions

Activisme

Engagement politique privilégiant l'action directe

- Greenpeace contre la pêche à la baleine
- Perturbation sur le parcours de la flamme olympique

Hacktivisme

- Contraction de hacker et d'activisme
- Terme créé en 1996
- Phénomène existant depuis plus de quinze ans
- Forte prise de conscience à l'occasion des attaques par déni de service distribué (DDoS) lancées en 2007 contre l'Estonie

L'Hacktivisme avant 2010

Exemples

Patriotes chinois : les médias occidentaux font état de groupes composés de plus de 300 000 membres. Ils s'attaquent sans relâche aux nombreux sites « pro-Tibet »

Nationalistes russes : en synchronisme avec les opérations militaires et avec l'aide d'organisations cybercriminelles, l'Estonie (mars-mai 2007) puis la Géorgie (aout 2008) sont victimes de cyber-attaques

Pro-israéliens et pro-palestiniens s'affrontent aussi sur le Net. Les uns à l'aide d'un botnet de volontaires, les autres par la technique du défiguration

L'Hacktivisme en 2010

Pas un mois sans une protestation virtuelle

Janvier – Turquie : pour une reconnaissance de l'homosexualité

Février – Lettonie : pour dénoncer la corruption

Mars – Vietnam : pour faire taire l'opposition

Avril – Etats-Unis : pour une université ouverte aux défavorisés

Mai – France : rencontres « Pas Sage en Seine »

Juin – Israël : pour soutenir la cause palestinienne

Juillet – France : pour soutenir le peuple haïtien

Aout – Philippines : pour venger la mort des otages chinois tués à Manille

Septembre – Opération Payback : « pour un Internet libre »

Octobre – Papouasie : pour faire taire les ONG

Novembre – Tibet : pour faire taire la presse soutenant la diaspora tibétaine

Décembre – Opération Payback (suite), opération Leakspin : pour soutenir WikiLeaks

L'Hacktivisme en 2010 (exemple)

Conflit israélo-palestinien

Voyage numérique pour la Flottille de la Liberté

- Alors que les organisateurs du convoi utilisent Facebook, Twitter, YouTube et Flickr pour donner de leurs nouvelles, des sympathisants palestiniens s'en prennent aux sites israéliens, alors que d'autres piratent des comptes Facebook pour protester contre l'assaut des forces israéliennes

L'Hacktivisme en 2010 (exemple)

France: Désinformation - Typosquatting

A l'occasion du 14 juillet, un groupe de pirates détourne le site internet du ministère des Affaires étrangères. On y voit un porte parole officiel du Ministère annonçant le remboursement par la France des 21 milliards de dollars (17 milliards d'Euros) que nous avait versés Haïti entre 1825 et 1947

www[.]diplomatiegov.fr

Faux

Vrai

www[.]diplomatie.gouv.fr

L'Hacktivisme en 2010 (exemple)

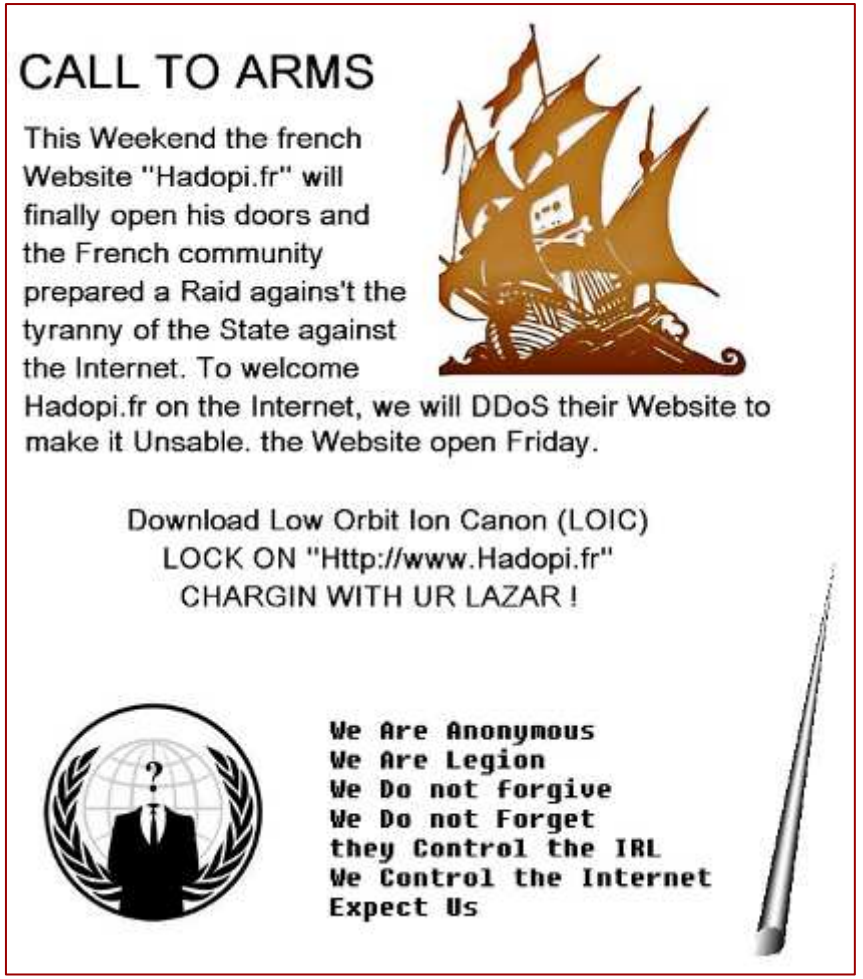
Opération Payback

Septembre 2010 :

Le groupe Anonymous lance des attaques concertées en déni de service distribué (DDoS) contre différents sites web liés aux ayants droit américains et britanniques

Il réagit à l'annonce faite par la société indienne AiPlex qui se vante d'avoir mené – à la demande des majors - des attaques DDoS à l'encontre de différents sites de téléchargement illégaux, dont l'emblématique The Pirate Bay

Le groupe Anonymous menace aussi le site de l'Hadopi et les ayants droit français



L'Hacktivisme en 2010

Vers une première forme de cyber-guerre ?

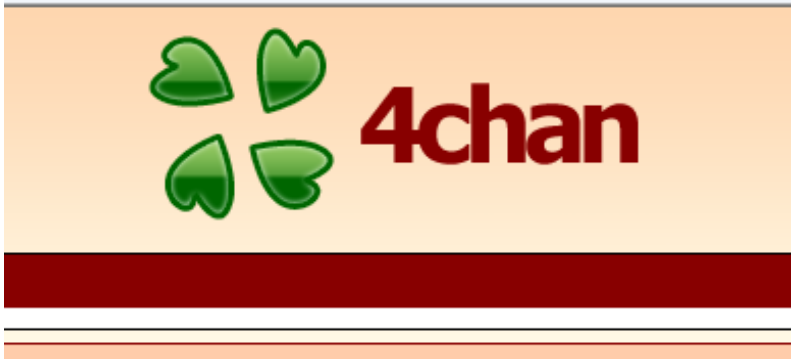
Sous couvert d'hacktivisme attribué à des individus militants, ne voit-on pas aussi apparaître une première forme de cyber-guerre menée en fait par les états ?

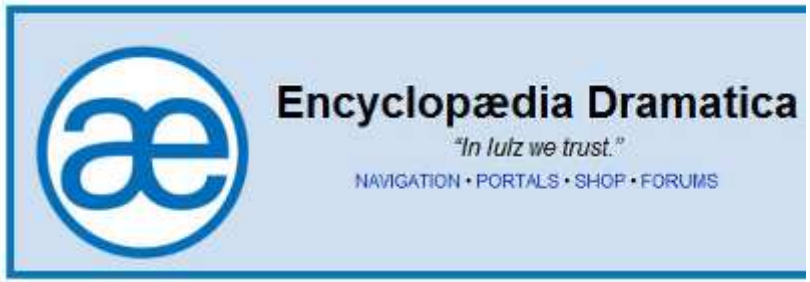
Les soupçons se multiplient :

- 2007/2008 – Estonie, Géorgie
- 2009/2010 - Iranian Cyber Army: Attaques de sites d'opposition,
- Janvier 2010 – Chine, Opération Aurora
- Mars 2010 – Vietnam: Botnet Vulcanbot, blocage de blogueurs,
- Juin 2010 - Stuxnet
- Septembre 2010 - Brigades de Tariq ibn Ziyad / Irak resistance: W32/VBMania@MM
- Octobre 2010 – Vietnam: Botnet Vecebot, blocage de blogueurs
- Décembre 2010 - Indian Cyber Army / Pakistan Cyber Army
- Etc.

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

L'Hacktivisme en 2010 (exemples)

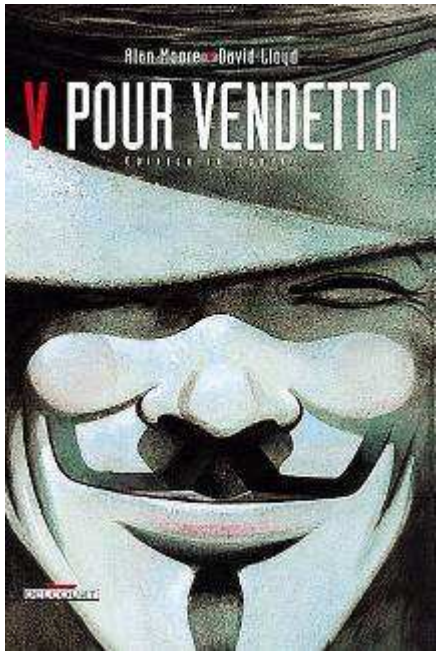




L'Hacktivisme au XXIe siècle (exemple)

De 4chan à Anonymous

- 4Chan :
  - Forums d'images créé en 2003
  - Un des sites les plus fréquentés de l'Internet
  - Le forum le plus populaire se nomme « /b/ »
    - Entre 150 000 et 200 000 messages par jour
    - Pornographie, cadavres mutilés, images scatologiques, appels au meurtre, racisme, homophobie, etc.
    - Liberté d'expression absolue, culte de l'anonymat. On y poste sans pseudonyme (ce qui donne par défaut celui d'Anonymous)
- *Anonymous* est une émanation de /b/
  - 2008 : projet Chanology (attaques informatiques contre l'Église de scientologie)
  - Supporters de l'*Encyclopedia Dramatica*, doublure satirique, voire choquante, de Wikipédia



L'Hacktivisme au XXIe siècle (exemple)

Les « Anonymous » hier…

Ils revendiquent agir contre la censure du Net.

Sans vrai(s) leader(s), ils mobilisent les foules et organisent des actions concertées très diverses :

- Raids sur « Habbo Hotel » : mettre en évidence le manque de personnages noirs
- Youporn Day : intégrer du porno dans des vidéos YouTube d'apparence anodines
- Projet Chanology : tenter d'éliminer la Scientologie du Web
- 2009 Iranian Election Protest: aider et soutenir les opposants iraniens
- Opérations Didgeridie, CyberDyne Solutions & Titstorm: protester contre la censure
- Opération Payback : protester contre les attaques menées à l'encontre des sites de téléchargement (illégal)

… et maintenant…

- Opération Payback (suite) : depuis le 4 décembre 2010, les Anonymous décident de se venger des opposants à WikiLeaks

L'Hacktivisme au XXIe siècle (exemple)

WikiLeaks

Créé en 2006, le site milite pour une transparence planétaire. Il divulgue des documents souvent secrets témoignant d'une réalité sociale, politique et militaire (« Leaks » : fuites en anglais) :

- Corruption en Somalie (2006), au Kenya (2007)
- Affaire Dutroux : mise à disposition de l'intégralité du procès (avril 2009)
- Rapports financiers de la banque Kaupting (juillet 2009)
- « Climategate » : divulgation d'un ensemble de courriels et de fichiers attribués aux responsables du Climatic Research Unit (novembre 2009)
- Bavure lors d'un raid aérien en Iraq en 2007 (avril 2010)
- « Afghan War Diary » (juillet 2010)
- « Iraq War Logs » : (octobre 2010)
- « Cablegate » : télégrammes de la diplomatie américaine (novembre 2010)

L'Hacktivisme au XXIe siècle (exemple)

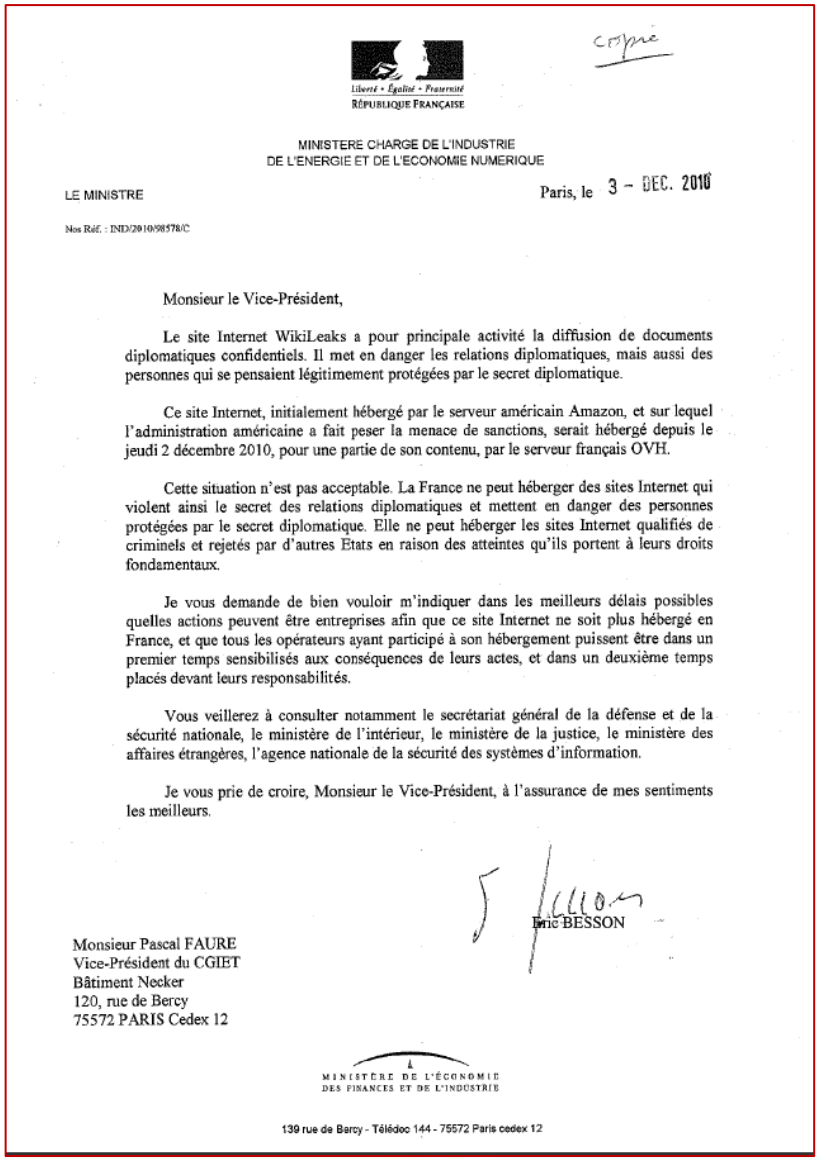
WikiLeaks

- 23 octobre 2010 : Les « Iraq War Logs » sont hébergés par Owni (France)
- 28 novembre 2010 : début de l'opération « Cablegate ». C'est un autre hébergeur français (Octopuce, anciennement Metaconsult) qui héberge l'organisation depuis le 14 novembre
- 28 novembre 2010 : avec son outil XerXes, Jester – « hacktiviste au service du bien » revendique les attaques qui rendent Wikileaks indisponible

L'Hacktivisme au XXIe siècle (exemple)

WikiLeaks

- 29 novembre 2010 : les sous-domaines « warlogs » et « cablegate » quittent Octopuce (France) qui ne peut contrecarrer les attaques DDoS. Le transfert se fait vers Amazon aux Etats-Unis et en Irlande
- 30 novembre 2010 : mandat d'arrêt international à l'encontre de Julian Assange (pour violences sexuelles présumées)
- 1er décembre 2010 : Amazon stoppe l'hébergement après qu'il ait fait l'objet de pressions politiques et commerciales
- 2 décembre 2010 : nouvel hébergement en France chez OVH. EveryDNS stoppe son service de DNS entrainant l'indisponibilité du domaine
- 3 décembre 2010 : Intervention d'Eric Besson. Les sympathisants se mobilisent pour répliquer les données



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

copie

MINISTERE CHARGE DE L'INDUSTRIE
DE L'ENERGIE ET DE L'ECONOMIE NUMERIQUE

LE MINISTRE

Paris, le 3 - DEC. 2010

Nos Réf. : IND/2010/58578/C

Monsieur le Vice-Président,

Le site Internet WikiLeaks a pour principale activité la diffusion de documents diplomatiques confidentiels. Il met en danger les relations diplomatiques, mais aussi des personnes qui se pensaient légitimement protégées par le secret diplomatique.

Ce site Internet, initialement hébergé par le serveur américain Amazon, et sur lequel l'administration américaine a fait peser la menace de sanctions, serait hébergé depuis le jeudi 2 décembre 2010, pour une partie de son contenu, par le serveur français OVH.

Cette situation n'est pas acceptable. La France ne peut héberger des sites Internet qui violent ainsi le secret des relations diplomatiques et mettent en danger des personnes protégées par le secret diplomatique. Elle ne peut héberger les sites Internet qualifiés de criminels et rejetés par d'autres Etats en raison des atteintes qu'ils portent à leurs droits fondamentaux.

Je vous demande de bien vouloir m'indiquer dans les meilleurs délais possibles quelles actions peuvent être entreprises afin que ce site Internet ne soit plus hébergé en France, et que tous les opérateurs ayant participé à son hébergement puissent être dans un premier temps sensibilisés aux conséquences de leurs actes, et dans un deuxième temps placés devant leurs responsabilités.

Vous veillerez à consulter notamment le secrétariat général de la défense et de la sécurité nationale, le ministère de l'intérieur, le ministère de la justice, le ministère des affaires étrangères, l'agence nationale de la sécurité des systèmes d'information.

Je vous prie de croire, Monsieur le Vice-Président, à l'assurance de mes sentiments les meilleurs.

Eric BESSON

Monsieur Pascal FAURE
Vice-Président du CGIET
Bâtiment Necker
120, rue de Bercy
75572 PARIS Cedex 12

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

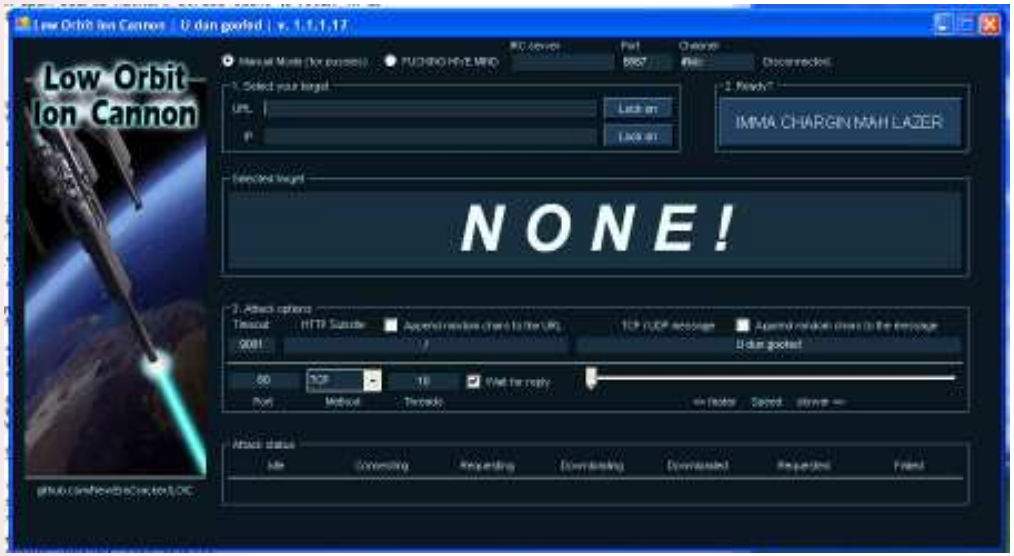
139 rue de Bercy - Télédoc 144 - 75572 Paris cedex 12

L'Hacktivisme au XXI^{ème} siècle (exemple)

WikiLeaks

4 décembre 2010 : le compte Paypal de WikiLeaks est suspendu. Les mesures de sanction financière à l'égard de Julian Assange se poursuivent les jours suivant (PostFinance, Mastercard, Visa International)

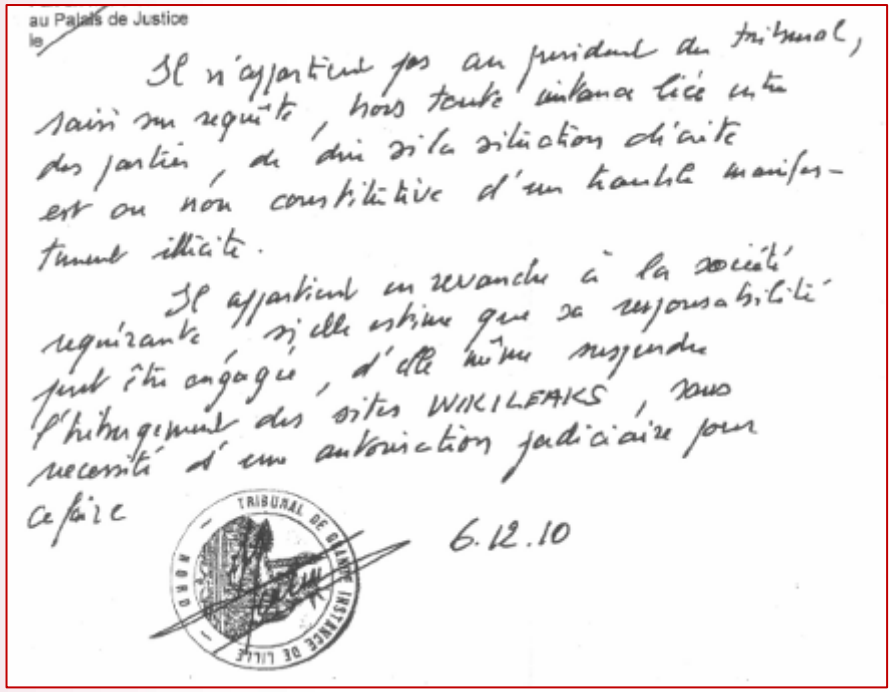
Le groupe Anonymous programme des attaques en déni de service distribué à l'encontre de tous ceux qui s'opposent à Wikileaks. Les volontaires sont invités à télécharger LOIC, qui, avec sa fonction « hive mind » (esprit de ruche) transforme chaque machine équipée en bot volontaire permettant une attaque coordonnée



L'Hacktivisme au XXIe siècle (exemple)

WikiLeaks

- 6 décembre 2010 : la justice française refuse de se prononcer en faveur ou à l'encontre de l'hébergement

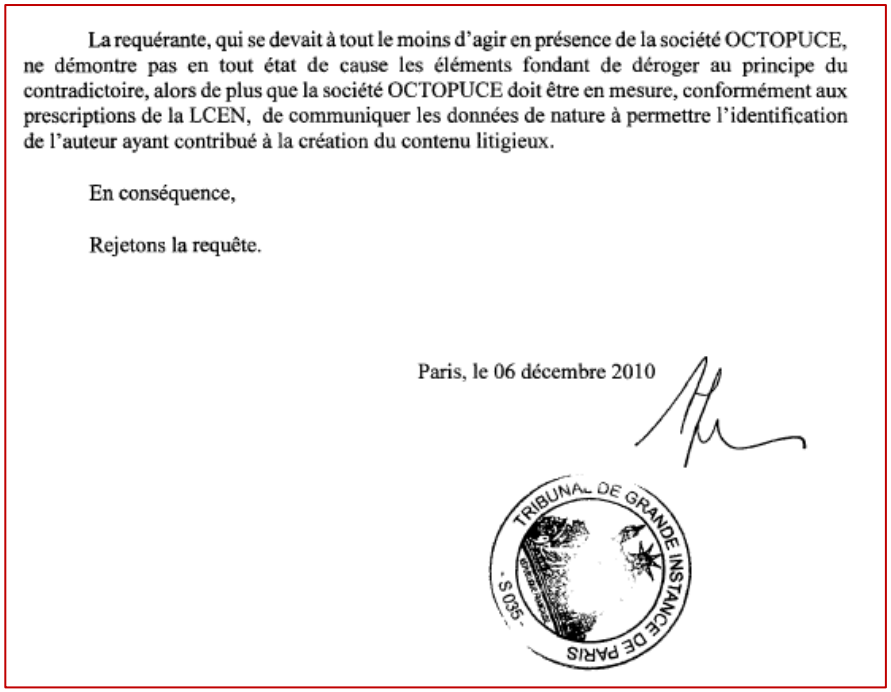


au Palais de Justice
le

Il n'appartient pas au président du tribunal, saisi en requête, hors toute instance liée entre des parties, de dire si la situation alléguée est ou non constitutive d'un trouble manifestement illicite.

Il appartient en revanche à la société requérante, si elle estime que sa responsabilité peut être engagée, d'elle même suspendre l'hébergement des sites WIKILEAKS, sous nécessité d'une autorisation judiciaire pour ce faire

6.12.10



La requérante, qui se devait à tout le moins d'agir en présence de la société OCTOPUCE, ne démontre pas en tout état de cause les éléments fondant de déroger au principe du contradictoire, alors de plus que la société OCTOPUCE doit être en mesure, conformément aux prescriptions de la LCEN, de communiquer les données de nature à permettre l'identification de l'auteur ayant contribué à la création du contenu litigieux.

En conséquence,

Rejetons la requête.

Paris, le 06 décembre 2010

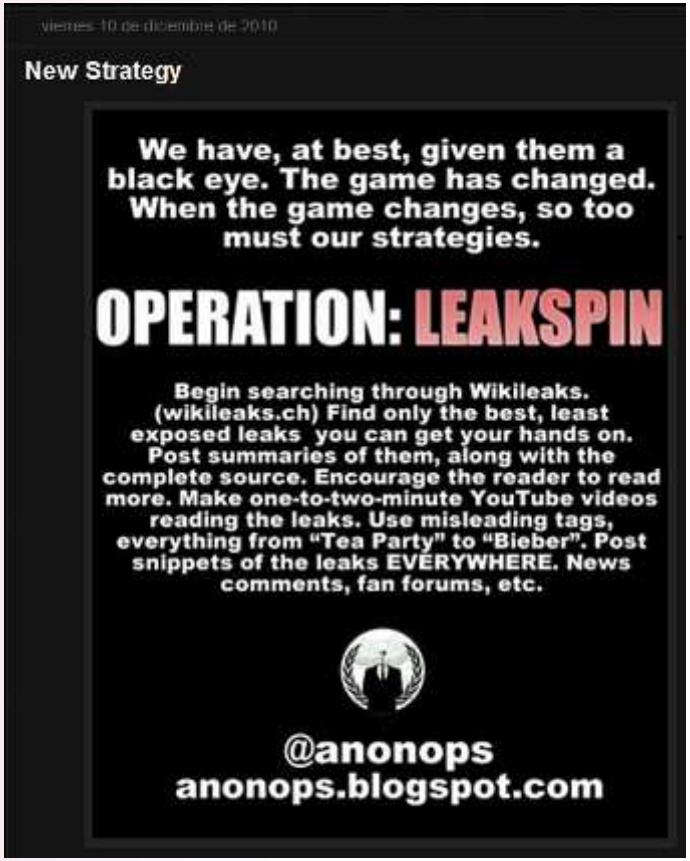
TRIBUNAL DE GRANDE INSTANCE DE PARIS

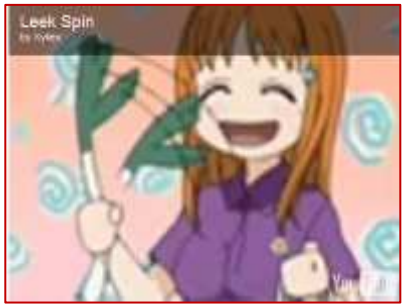
- 7 décembre 2010 : Julian Assange se présente à la police britannique; il est emprisonné à Londres. Julian Assange sera libéré sous caution le 16 décembre

L'Hacktivisme au XXIe siècle (exemple)

WikiLeaks

- 9 décembre 2010 : arrestation en Hollande de « Jeroenz0r ». Ce jeune de 16 ans est accusé d'être le leader et l'administrateur d'un des botnet volontaire (clients LOIC) utilisé à l'encontre de MasterCard, VISA et Paypal





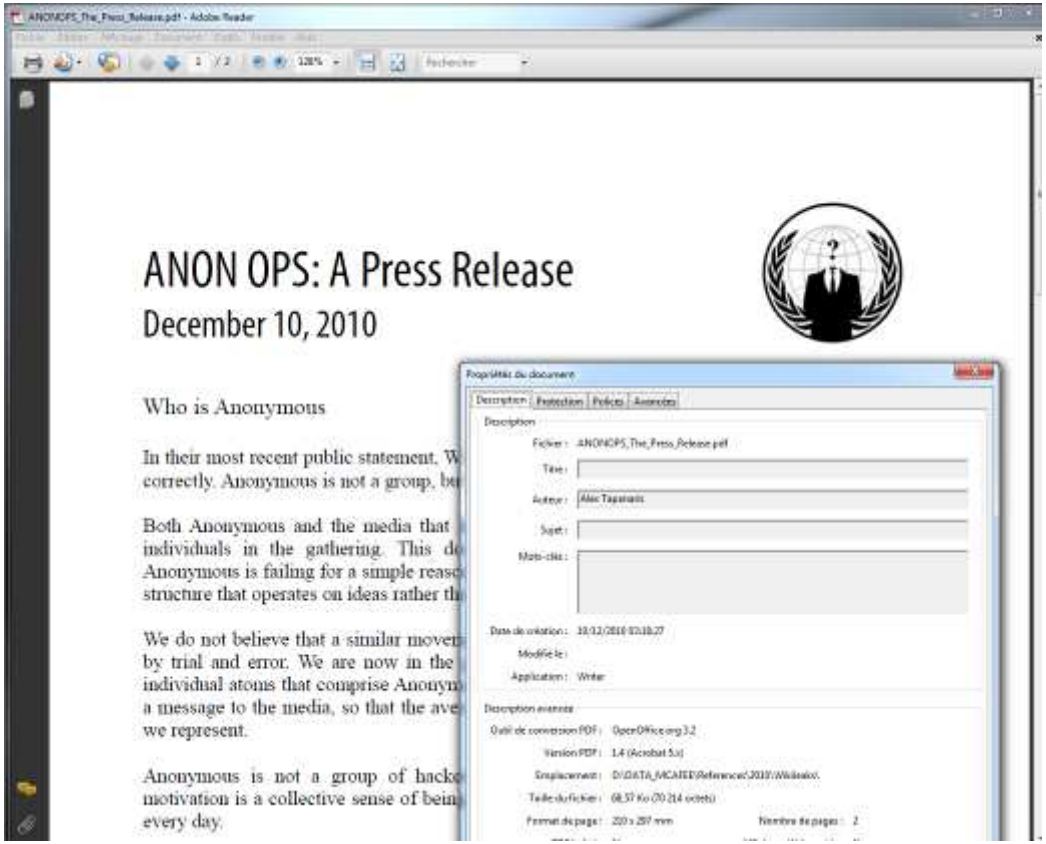
- 10 décembre 2010 : le groupe Anonymous annonce qu'il abandonne les attaques en DDoS avec Loïc (les attaques vont cependant se poursuivre). Il lance l'Opération Leakspin, nom repris d'une animation célèbre circulant parmi les internautes. Les volontaires sont appelés à entreprendre leur propre travail d'enquête sur les câbles diplomatiques pour en publier les plus emblématiques

L'Hacktivisme au XXIe siècle (exemple)

WikiLeaks

- 11 décembre 2010 : arrestation en Hollande d'un autre jeune de 19 ans, utilisateur de LOIC. Celui-ci a été facilement été retrouvé, car, par conception, l'IP de l'attaquant est incluse dans chaque paquet émis par LOIC

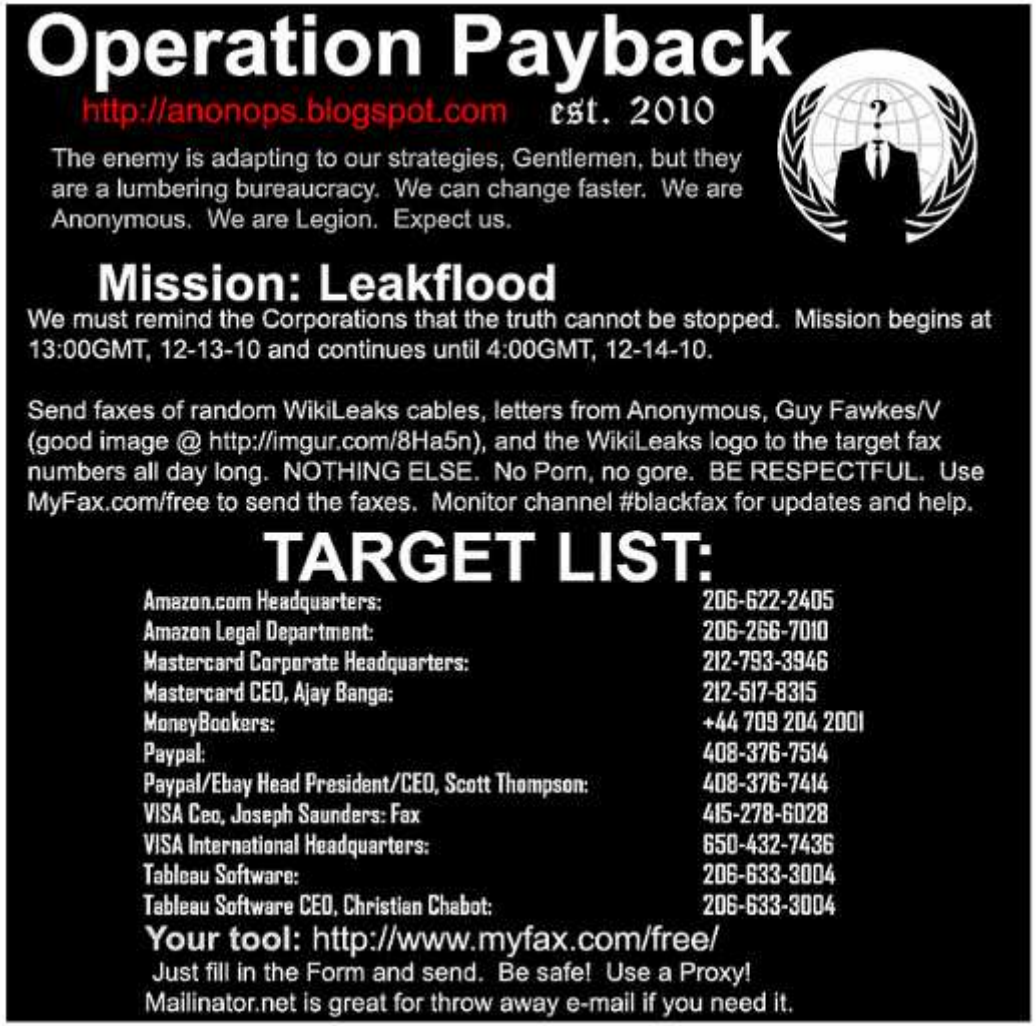
- 13 décembre 2010 : une rumeur fait état de l'arrestation, en Grèce, d'un certain Alex Tapanaris, après que son nom ait été retrouvé au sein d'un communiqué PDF du groupe



L'Hacktivisme au XXIe siècle (exemple)

WikiLeaks

- 13 décembre 2010 : mission Leakflood: envoi massif de fax aux opposants de Wikileaks
- 14 décembre 2010 : Wikileaks.org de nouveau opérationnel. Il est hébergé aux US, depuis le 11 (Silicon Valley Web Hosting) ou il utilise les services DNS de Dynadot. Il n'y a aucun contenu, mais une redirection vers un site miroir hébergé en Russie (mirror.wikileaks.info) auprès d'un hébergeur connu pour sa complaisance avec le cybercrime (Heihachi.net). Ce site miroir n'est d'ailleurs pas listé parmi les sites miroirs officiels sur wikileaks.ch



Operation Payback: Mission: Leakflood [by Anon]

L'Hacktivisme au XXIe siècle (exemple)

WikiLeaks

- 18 décembre 2010 : opération Black Face. En signe de soutien à Wikileaks et à Julian Assange, les internautes sont invités à remplacer la photo de leur profil sur les réseaux sociaux par un fond noir.

- 18 décembre 2010 : opération Paperstorm (distribution de tracts)

L'Hacktivisme au XXIe siècle (exemple)

WikiLeaks

- 27 décembre 2010 : Bank of America est de nouveau la cible d'attaques en DDoS

- Cette attaque est pilotée depuis des canaux IRC eux aussi sous contrôle de groupes cybercriminels russes (toujours Heihachi.net)

L'Hacktivisme au XXIe siècle (exemple)

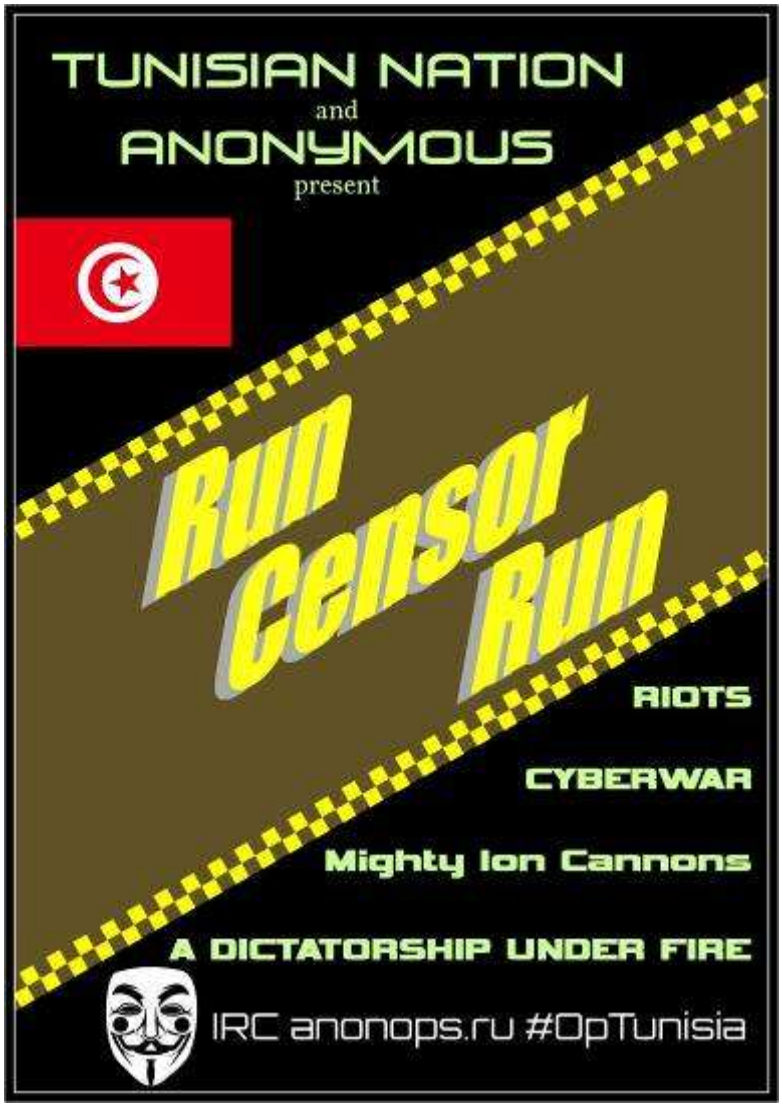
WikiLeaks

Des opérations de tous genres se multiplient. Toutes celles qui proposent des attaques en DDOS sont issues de serveurs sous contrôle d'Heidachi.net :

- 28 décembre 2010 : opération Zimbabwe
- 30 décembre 2010 : opération Tunisia

ATTENTION DANGER!

à suivre…



L'Hacktivisme : entre criminalité et militantisme - Conclusion

D'abord, des questions sans réponses :

Les Anonymous et certains supporters de Wikileaks ont-ils décidé de faire appel à des hébergeurs à l'épreuve des balles ?

Si oui, qui chez eux en est l'instigateur ?

Pourquoi Wikileaks ne réagit-il pas (dans un sens ou dans l'autre) au sujet du miroir hébergé chez heihachi.net ? Pourquoi n'indique-t-il pas s'il est ou non le propriétaire de wikileaks.org ?

Les campagnes menées par les Anonymous depuis heihachi.net sont elles réellement le fait d'hacktivistes ?

Comme lors d'autres évènements médiatiques (tremblement de terre, décès d'une personnalité publique, etc.), les cybercriminels se serviraient-ils de l'actualité pour mener leurs propres actions (chantage, distribution de malware) ?

L'Hacktivisme: entre criminalité et militantisme - Conclusion

Que retenir ensuite ?

- Wikileaks: des secrets vides ?

  « *La règle selon laquelle les dossiers secrets ne doivent être composés que de nouvelles déjà connues est essentielle à la dynamique des services secrets, et pas seulement en ce siècle. » […]*

  Les révélations « *disent ce que toute personne cultivée sait déjà, » […]. (Umberto Eco),*

- Nous assistons à la montée d'une nouvelle forme d'engagement revendicatif et collectif.
- L'hacktivisme évolue aujourd'hui comme le cybercrime l'a fait hier:
  - L'individu isolé laisse la place à des groupes qui s'organisent,
  - Arrivée de graphistes ➔ pour une meilleure communication,
  - Arrivée de journalistes bénévoles ➔ pour un journalisme participatif fonctionnant comme Wikipédia (le « crowd-journalism »),
  - Arrivée de tacticiens ➔ opération « flood de fax » sur les responsables des sociétés qui ont banni Wikileaks,
- Les Anonymous préfigurent l'arrivée d'un phénomène majeur et de par certains aspects, dangereux.

L'Hacktivisme au XXIe siècle (exemple)

Les « Anonymous »

- Corrupt governments of the world, we are anonymous.
- For some time now, voices have been crying out in unison against the new ACTA laws.
- The gross inadequacies of the new laws being passed internationally have been pointed out repeatedly.
- Our chief complaint is that such measures would restrict people's access to the internet.
- In these modern times access to the internet is fast becoming a basic human right.
- Just like any other basic human right, we believe that it is wrong to infringe upon it.
- To threaten to cut people off from the global consciousness as you have is criminal and abhorrent.
- To move to censor content on the internet based on your own prejudice is at best laughably impossible, at worst, morally reprehensible.
- The unjust restrictions you impose on us will meet with disaster and only strengthen our resolve to disobey and rebel against your tyranny.
- Such actions taken against you, and those you outsource your malignant litigation too, are inevitable, unavoidable and unstoppable.
- We Are Anonymous,
- We Are Legion And Divided By Zero.
- We Do Not Forgive Internet Censorship
- And We Do Not Forget Free Speech.
- We Are Over 9000,
- Expect Us!

- **Gouvernements corrompus de par le monde, nous sommes les Anonymous**
- **Depuis quelques temps déjà, des voix se sont élevées à l'unisson pour dénoncer ACTA.**
- **La grossière inadaptation de ces nouvelles lois qui sont votées partout dans le monde a été dénoncée de façon répétée**
- **Notre principal reproche est que de telles mesures restreindraient l'accès du peuple à internet**
- **Dans ces temps modernes, l'accès à l'internet devient rapidement un droit de l'homme fondamental**
- **Comme tout droit de l'homme fondamental, nous pensons qu'il est mauvais de le violer.**
- **Menacer de couper quelqu'un de la conscience globale comme vous l'avez fait est criminel et abject.**
- **Passer à la censure des contenus sur internet sur la base des seuls préjudices qu'ils pourraient vous causer est au mieux risible, au pire moralement répréhensible.**
- **Les restrictions injustes que vous nous imposez provoqueront un désastre et ne feront que renforcer notre résolution à désobéir et à nous rebeller contre votre tyrannie.**
- **Les actions prises envers vous, ainsi qu'envers ceux avec qui vous faites vos affaires putrides, sont inévitables, nécessaires, et impossibles à stopper.**
- **Nous sommes les Anonymous**
- **Nous sommes légion et divisible par zéro**
- **Nous ne pardonnons pas la censure de l'internet**
- **Nous n'oublions pas la liberté de parole.**
- **Nous sommes plus de 9000**
- **Attendez-vous à nous !**

L'Hacktivisme au XXIe siècle (exemple)

Références

- 4Chan,/b/ et les nouveaux pédophiles
  https://ruedesgarcons.fpc.li/magazine/textes/03/media/ELU03003.pdf
- Les Anonymous, première forme d'intelligence collective ?
  http://fr.readwriteweb.com/2010/12/14/prospective/les-anonymous-premire-forme-dintelligence-collective/
- Attacks by "Anonymous" WikiLeaks Proponents not Anonymous
  http://www.simpleweb.org/reports/loic-report.pdf
- Prix Busiris pour Eric Besson
  http://www.maitre-eolas.fr/post/2010/12/19/Prix-Busiris-pour-Eacute%3Bric-Besson
- Don't Confuse 'Anonymous' With a Russian Gan
  http://blogs.mcafee.com/mcafee-labs/don%e2%80%99t-confuse-anonymous-with-a-russian-gang
- Hackers vengeurs et espions en diligence (par Umberto Eco)
- http://www.liberation.fr/monde/01012305696-hackers-vengeurs-et-espions-en-diligence

Agenda, Panorama 2010

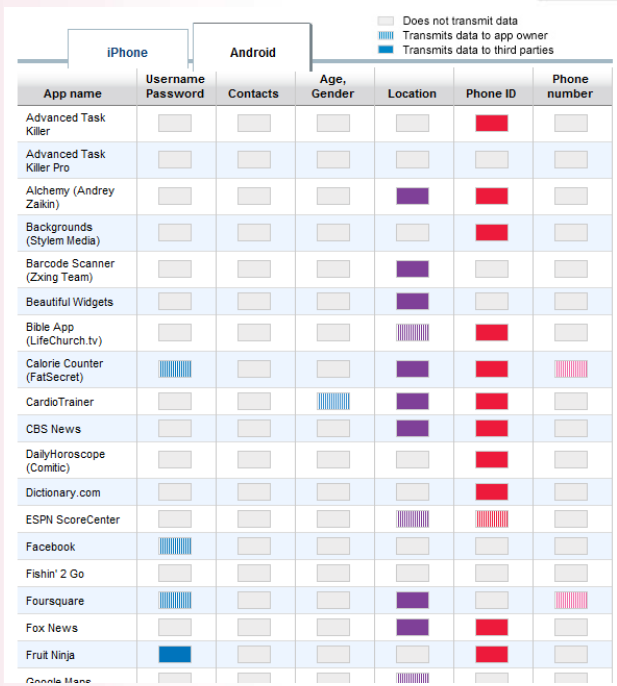
- Stuxnet : les mystères d'une cyber-attaque industrielle
- [Evocation] Automobile, les OS embarqués
- Hacktivisme : entre criminalité et militantisme
- **Le crime est de plus en plus mobile…**
- Botnets : la lutte s'intensifie
- [Evocations]Bugs, IPV6, jeux en ligne…

Plan

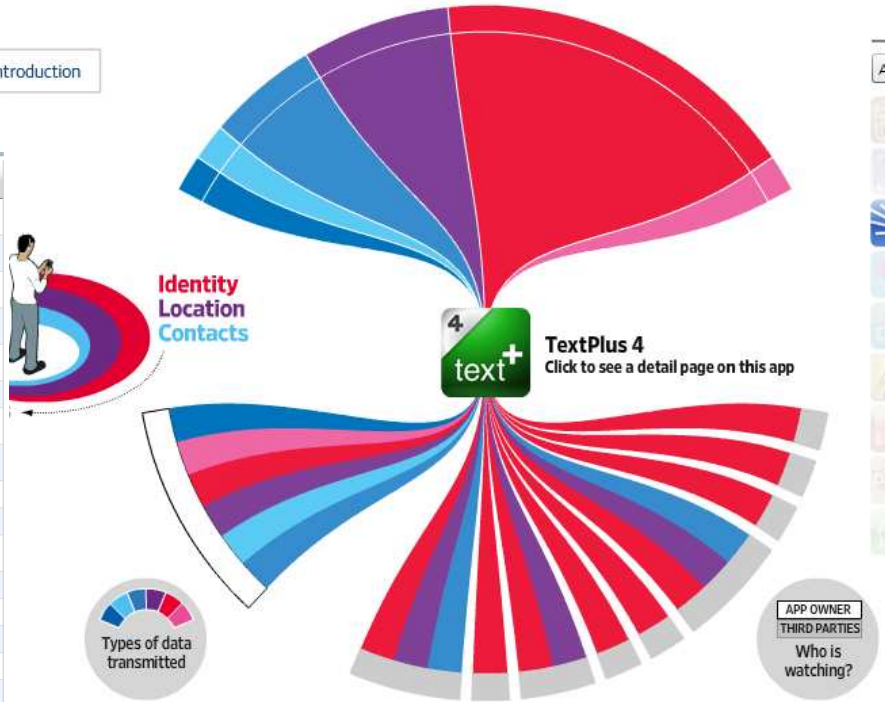
- Des mobiles indiscrets
- Des mobiles vulnérables
- Et de nouvelles attaques contre les mobiles
- Les mobiles entrent dans la danse du botnet

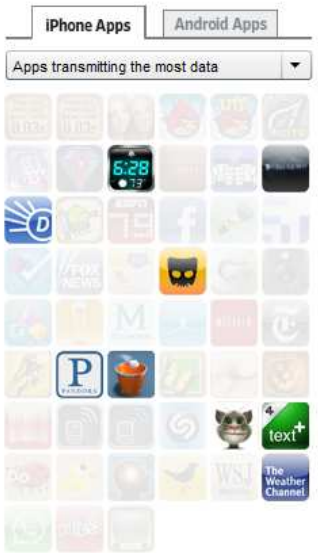
Des mobiles indiscrets (1)

Etude du Wall Street Journal sur 101 applications (12/2010)



App name	Username Password	Contacts	Age, Gender	Location	Phone ID	Phone number
Advanced Task Killer					■	
Advanced Task Killer Pro						
Alchemy (Andrey Zaikin)				■	■	
Backgrounds (Stylem Media)					■	
Barcode Scanner (Zxing Team)				■		
Beautiful Widgets				■		
Bible App (LifeChurch.tv)				■	■	
Calorie Counter (FatSecret)	■			■	■	■
CardioTrainer			■	■	■	
CBS News				■	■	
DailyHoroscope (Comitic)					■	
Dictionary.com					■	
ESPN ScoreCenter				■	■	
Facebook	■					
Fishin' 2 Go						
Foursquare	■			■		■
Fox News				■	■	
Fruit Ninja	■				■	
Google Maps				■		

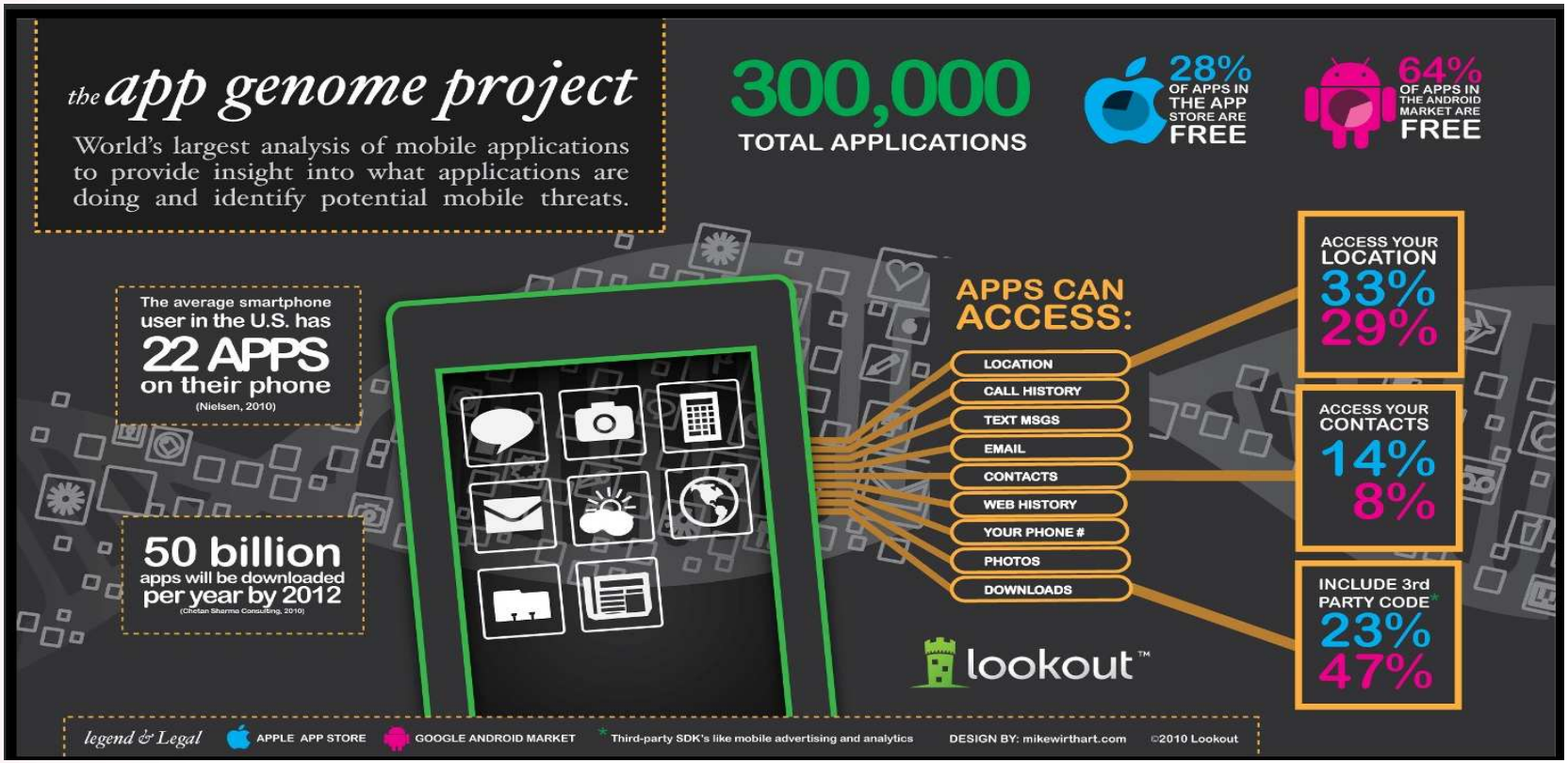




http://blogs.wsj.com/wtk-mobile/

Des mobiles indiscrets (2)

Autre étude menée par Lookout



Des mobiles indiscrets (3)

Apple poursuivi pour divulgation de données personnelles

Bloomberg

Apple Sued Over Applications Giving Information to Advertisers

January 05, 2011, 8:40 AM EST

By Joel Rosenblatt

Dec. 28 (Bloomberg) -- Apple Inc., making of the iPhone and iPad, was accused in a lawsuit of allowing applications for those devices to transmit users' personal information to advertising networks without customers' consent.

The complaint, which seeks class action, or group, status, was filed on Dec. 23 in federal court in San Jose, California. The suit claims Cupertino, California-based Apple's iPhones and iPads are encoded with identifying devices that allow advertising networks to track what applications users download, how frequently they're used and for how long.

Macworld

Apple hit with privacy class action lawsuit

Wed, 29 Dec 2010

A lawsuit alleges that Apple and associated advertisers are collecting iPhone and iPad user information

Christopher Breen

Apple has been hit by a lawsuit that alleges the company and its partners are surreptitiously collecting personal information from the users of iPhones and iPads.

A lawsuit filed December 23 in San Jose, California on behalf of Los Angeles county's Jonathan Lalo alleges that Apple and select codefendants have violated privacy and federal computer fraud statutes.

Des mobiles indiscrets (4)

Insolite : laissez-nous saisir vos cartes de visite à votre place...

Pourquoi pas, mais qui accède aux données ?

L'indiscrétion légale

BlackBerry / RIM et les interceptions

RIM to allow interceptio
BlackBerry Messenger in

By Manan Kakkar | January 4, 2011, 7:12pm PST

Summary

RIM to offer Indian agencies access to BlackBerry messenger communication with cloud services and NDAS. Corporate email remains unaffected with this and RIM might avert the 31st January deadline for a ban.

Topics

India, Research In

The ongoing RIM vs Security agencies in In
some compromise. RIM was given a 31st Ja
comply with the requests put forth by the s
26/11 terrorist attacks in Mumbai, the pres
to allow access to the communication over
BlackBerry's USP has been secure corporat
for the company to easily cave in. To RIM's
customer interest first.

In a solution proposed, RIM will allow India
over BlackBerry Messenger with the help o
up Network Data Analysis System (NDAS) i
carriers to intercept Messenger communica
that the NDAS was only for their consumer
their enterprise solutions.

Blackberry et interception des emails : RIM tente de gagner du temps en Inde

voter 0 ecouter email imprimer

Partagez cet article

par **Olivier Chicheportiche**, ZDNet France. Publié le 7 janvier 2011
Tags: BlackBerry, RIM, Sécurité

Sécurité - Le fabricant canadien demande un nouveau délai pour répondre aux exigences "sécuritaires" du pays tout en affirmant qu'il ne fournira pas un accès aux données transmises via le serveur professionnel du Blackberry. Vous avez dit grand écart ?

Le bras de fer entre les autorités indiennes et **RIM**, le fabricant des Blackberry se poursuit. Rappelons que depuis l'été dernier, l'Inde exige un accès aux courriels et à la messagerie instantanée des BlackBerry pour des questions de "sécurité nationale". Faute de quoi, ces services seraient tout simplement bloqués.

Depuis, le canadien tente de trouver une solution permettant à la fois de contenter les objectifs sécuritaires du gouvernement indien et de protéger quelque peu les données confidentielles de ses utilisateurs. Un grand écart particulièrement difficile qui se poursuit aujourd'hui.

Commentez cette actualité

L'actu des sociétés

Acer
Amazon
AMD
Apple
Asus
Bouygues Telecom
Cisco

Après tout, il s'agit d'appliquer la loi

Indiscrétions illégales

Articles 226-1, 226-3 et 226-15 code pénal

Est-ce que je peux espionner ma femme ou mon patron ?

Applications bidon

Ou logiciels commerciaux (extrait vidéo de démo...)

Des mobiles indiscrets

Pour fonctionner les réseaux GSM donnent parfois accès à beaucoup d'information

25th Chaos Communication Congress
Nothing to hide

Locating Mobile Phones using SS7

You are used to your mobile phone number following you around the globe. But the same functionality that makes you reachable worldwide can also be used to track your whereabouts down to city-level – without you ever knowing about it.

This talk will explain what SS7 features are exploited for locating mobile phones, how the returned information has to be interpreted and what you can (and can't) do against being located that way without having to turn off your phone altogether.

Attached files

- Locating Mobile Phones using SS7 (application/pdf - 896.3 KB)

En 2008, Tobias Engel expliquait comment localiser un téléphone mobile au niveau de la ville grâce au protocole SS7 de signalisation

En 2010, Nick DePetrillo et Don Bailey de chez ISEC ont prolongé cette étude et montré qu'ils pouvaient identifier des abonnés et les suivre (Source Boston)

Des mobiles vulnérables (1)

Les protocoles de communication du GSM mis à mal

26C3 - 26C3 1.15

26th Chaos Communication Congress
Here be dragons

GSM: SRSLY?

The worlds most popular radio system has over 3 billion handsets in 212 countries and not even strong encryption. Perhaps due to cold-war era laws, GSM's security hasn't received the scrutiny it deserves given its popularity. This bothered us enough to take a look; the results were surprising.

From the total lack of network to handset authentication, to the "Of course I'll give you my IMSI" message, to the iPhone that *really* wanted to talk to us. It all came as a surprise – stunning to see what $1500 of USRP can do. Add a weak cipher trivially breakable after a few months of distributed table generation and you get the most widely deployed privacy threat on the planet.

Cloning, spoofing, man-in-the-middle, decrypting, sniffing, crashing, DoS'ing, or just plain having fun. If you can work a BitTorrent client and a standard GNU build process then you can do it all, too. Prepare to change the way you look at your cell phone, forever.

Attached files

- GSM - SRSLY? (application/pdf - 664.7 KB)

Links

- Torrent of the video recording for this event in MPEG-4
- Video recording for this event in MPEG-4

SPEAKERS	
	Chris Paget
	Karsten Nohl
SCHEDULE	
Day	Day 1 - 2009-12-27
Room	Saal1
Start time	20:30
Duration	01:00
INFO	
ID	3654
Event type	Lecture
Track	Hacking
Language used for presentation	English
FEEDBACK	
Did you attend this event? Give Feedback	

Chris Paget , Karsten Nohl, CCC 2009

Karsten Nohl, Sylvain Munaut, rebelote au CCC 2010…

27C3 - Version 1.6.2

27th Chaos Communication Congress
We come in peace

Wideband GSM Sniffing

GSM is still the most widely used security technology in the world with a user base of 5 billion and a quickly growing number of critical applications. 26C3's rainbow table attack on GSM's A5/1 encryption convinced many users that GSM calls should be considered unprotected. The network operators, however, have not woken up to ities to be unleashed this year signal processing – will wake

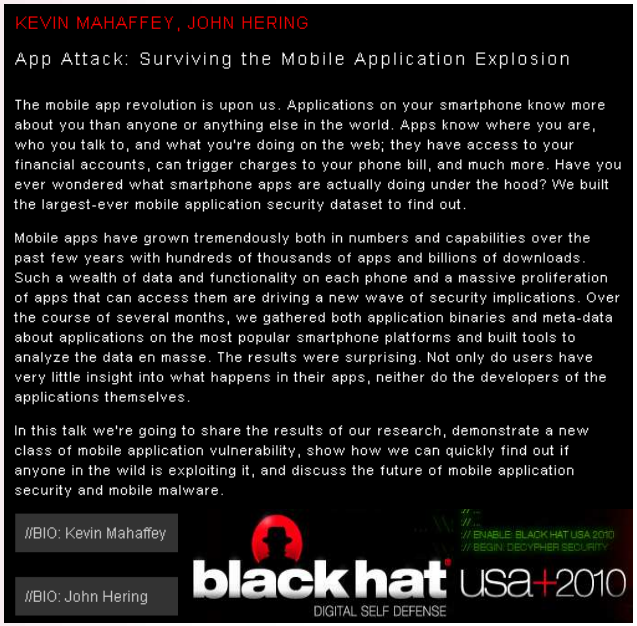
ked in seconds, the complexity of wireless phone e GSM hops over a multitude of channels, a large chunk example with USRPs, and decoded before storage or andwidth task can be achieved with cheap

f - 755.6 KB)

SPEAKERS	
	Karsten Nohl
	Sylvain Munaut
SCHEDULE	
Day	Day 2 - 2010-12-28
Room	Saal 1
Start time	14:00
Duration	01:00
INFO	
ID	4208
Event type	Lecture
Track	Hacking
Language used for presentation	English
FEEDBACK	
Did you attend this event? Give Feedback	

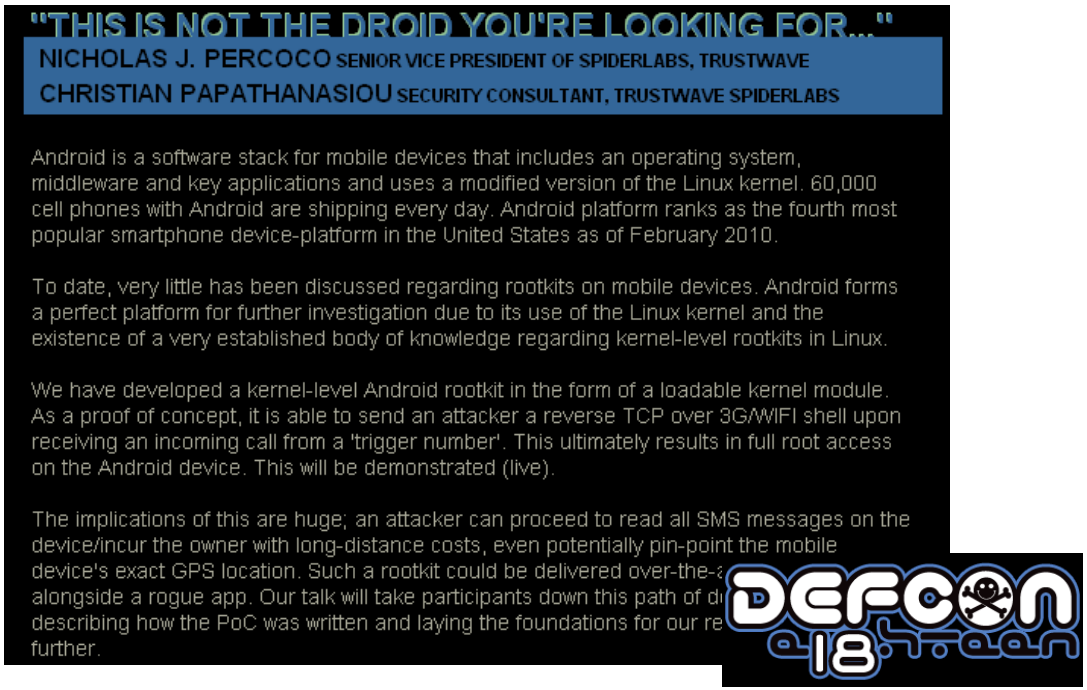
Des mobiles vulnérables (2)

Plusieurs vulnérabilités Android connues en 2010, pas toujours corrigées rapidement, souvent liées aux failles Linux



Présentation de Lookout à BH 2010

Présentation de Trustwave à Defcon 2010



Des mobiles vulnérables (3)

Les téléphones classiques sensibles à des attaques par SMS

27th Chaos Communication Congress

We come in peace

SMS-o-Death

From analyzing to attacking mobile phones on a large scale.

Smart phones, everybody has a smart phone! No! Just about 16% of all mobile phones are smart phones! Feature phones are the most common type of mobile phone in the world. Some time ago we decided to investigate the security of feature phones. In this talk we show how we analyzed feature phones for SMS security issues. We show our results and the kind of attacks that are possible with our bugs.

This talk is about security analysis of a class of mobile phone the so-called "feature phones". We show how we analyzed these type of phones for SMS security issues and what kind of problems to overcome in the process. We show results for the major mobile phone manufacturers in the world. Everyone of them has problems. Finally we show what kind of global scale attacks one can carry out with these kind of bugs. The attacks range from interrupting phone calls, to disconnecting people from the network, and sometimes even bricking phones remotely.

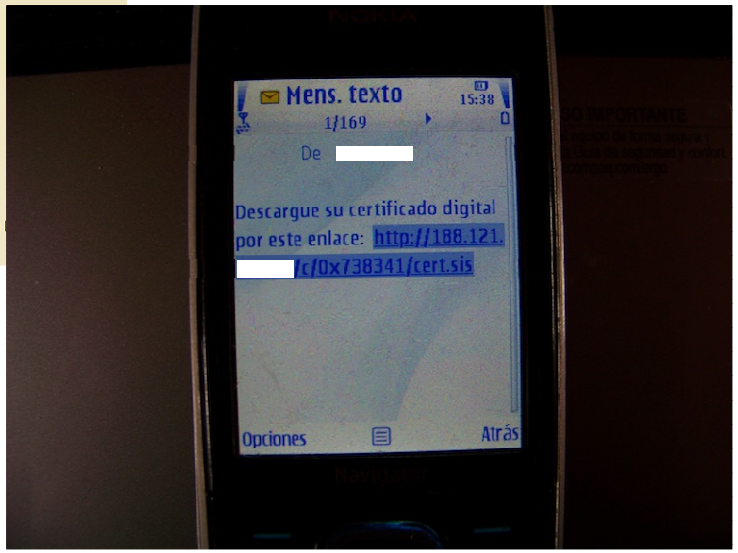
27C3 - Ver

SPEAKERS	
	Collin Mulliner
	Nico Golde
SCHEDULE	
Day	Day 1 - 2010
Room	Saal 1
Start time	17:15
Duration	01:00
INFO	
ID	4060
Event type	Lecture
Track	Hacking
Language used for presentation	English

Des mobiles vulnérables (4)

L'authentification à double facteur par SMS en danger ?

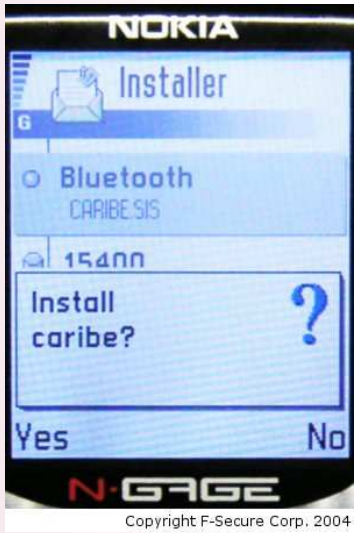
09/2010: S21Sec décrit ZeuS Mitmo



De nouvelles attaques contre les mobiles (1)

2010 : L'année du logiciel malveillant pour mobiles ?

2004: Cabir



Copyright F-Secure Corp. 2004

2006: McAfee sonne l'alarme

L'Expansion.com

RSS | Newsletters | Mobile | Vidéos | Diapos

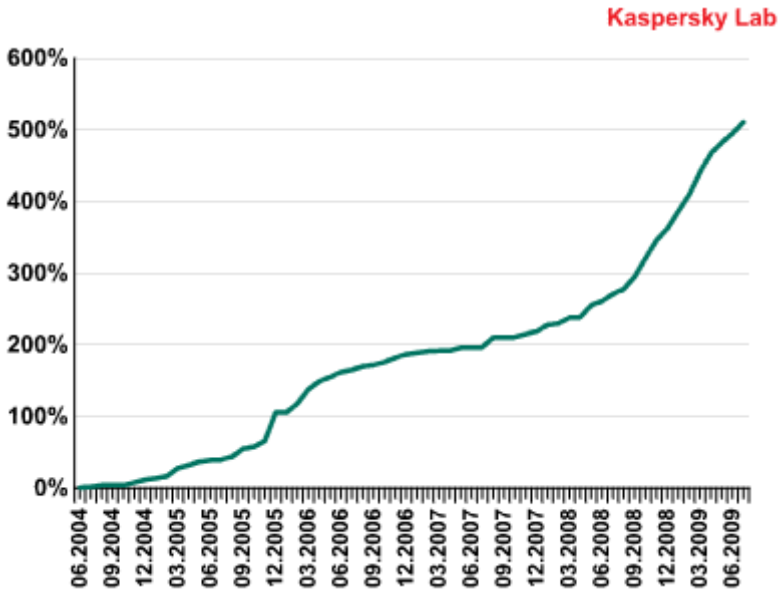
Actualité | Economie | Entreprise | High-Tech | Emploi & Carri

2006 sera l'année des virus mobiles

L'Expansion.com - publié le 20/12/2005 à 17:50

0 commentaire

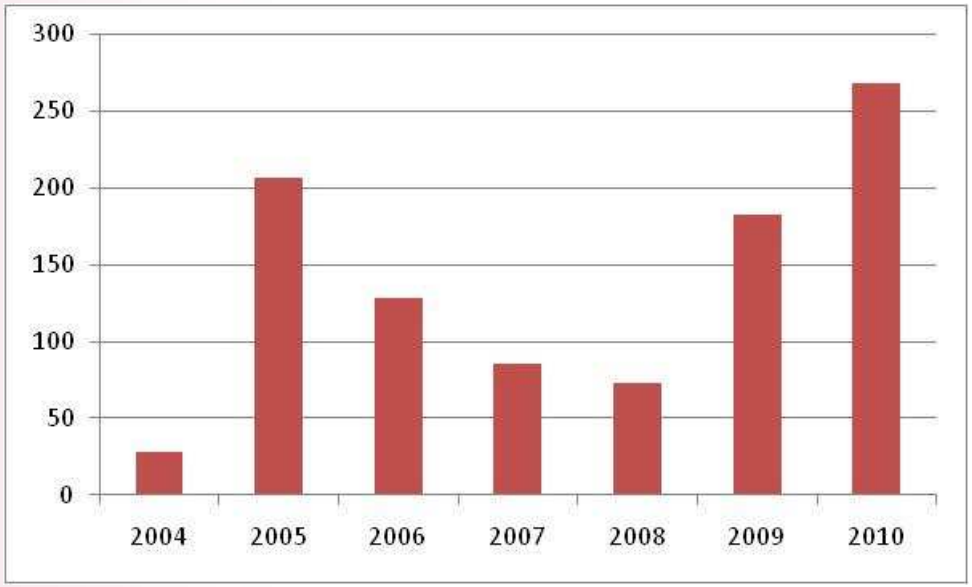
A la veille de chaque nouvelle année, l'éditeur d'antivirus McAfee livre des prévisions sur son marché. En 2006, ses chercheurs du McAfee Avert Labs s'attendent à la prolifération des virus pour téléphones portables. Le nombre de programmes nuisibles créés pour les mobiles devrait ainsi atteindre 726 à la fin 2005, contre 226 fin 2005. Si l'un d'entre eux venait à frapper simultanément plusieurs systèmes d'exploitation mobiles, il pourrait faire jusqu'à 200 millions de victimes portables, contre 10 millions de PC touchés par « I Love You » en 2004, estime McAfee. Qui n'oublie pas de préciser, par ailleurs, que le phishing, les adwares et les spywares seront toujours des menaces importantes pour la sécurité informatique.



2009: Kaspersky confirme la tendance

De nouvelles attaques contre les mobiles (2)

Confirmées en 2010

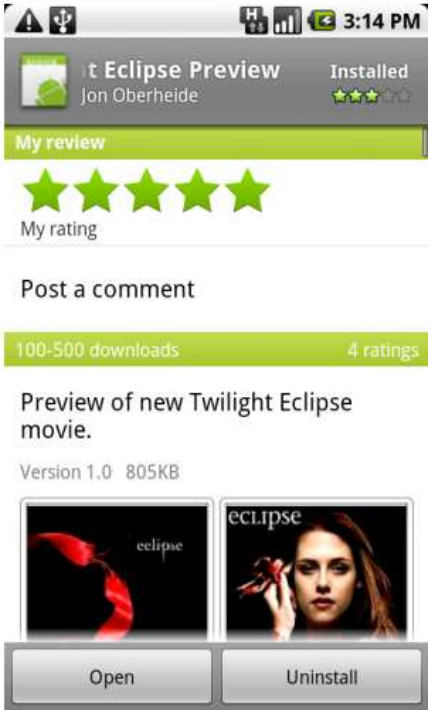


François Paget, McAfee

...Le marché de l'anti-virus pour mobiles est mature

Des botnets de mobiles

Juin 2010 : Jon Oberheide montre à la conférence Summercon qu'on peut créer un botnet à base d'Android



Des botnets de mobiles

Toutes les plateformes sont concernées

Botnet Viruses Target Symbian Smartphones

Nokia, Samsung and Sony Ericsson smartphones are among those running the two Symbian operating systems vulnerable to attack according to NetQin.

By **Mathew J. Schwartz** , InformationWeek
juillet 6, 2010 04:32 PM

New viruses targeting Symbian smartphones have surfaced, according to NetQin, which develops security software for mobile devices.

Two Symbian operating systems are vulnerable: S60 platform 3rd Edition, al S60 5th edition, aka Symbian OS 9.4. The operating systems run a number manufacturers as Nokia, Samsung and Sony Ericsson.

iKee transforme les iPhone jailbreakés en botnet

voter email imprimer Partagez cet article

par **Olivier Chicheportiche**, businessMOBILE.fr. Publié le 23 décembre 2009
Tags: Virus, Apple, iPhone, Sécurité,

Une nouvelle version du ver transforme le smartphone d'Apple en machine zombie afin de détourner des données. Le réseau serait contrôlé depuis la Lituanie.

Il fallait s'y attendre. La multiplication de vers visant les iPhone jailbreakés devait fatalement déboucher sur la constitution d'un réseau de smartphones contrôlables à distance (machines zombies).

La preuve en a été faite par l'institut SRI International Malware Threat Center. Comme on pouvait s'en douter, c'est le ver iKee qui est au centre de l'attaque.

Un réseau de 100 000 smartphones Symbian zombies découvert

voter email imprimer Partagez cet article

par **Guénaël Pépin**, businessMOBILE.fr. Publié le 6 juillet 2010
Tags: Symbian,

Sécurité - L'éditeur de sécurité mobile NetQin a mis au jour un réseau botnet visant les smartphones Symbian S60, se propageant par des jeux à télécharger. 500 plaintes ont déjà été déposées.

Un an après **Sexy Space**, une seconde vague de virus vise les smartphones sous **Symbian** S60 (3.0 et 5.0), l'OS mobile le plus répandu. Les virus ShadowSrv.A, FC.Downsis.A, BIT.N et MapPlug.A ont été identifiés par l'éditeur chinois d'antivirus pour smartphones NetQin, notamment pour l'opérateur China Mobile.

THE LOOKOUT BLOG

DECEMBER 29, 2010

Security Alert: Geinimi, Sophisticated New Android Trojan Found in Wild

By [illegible] 85 Comments

The Threat:

A new Trojan affecting Android devices has recently emerged in China. Dubbed "Geinimi" based on its first known incarnation, this Trojan can compromise a significant amount of personal data on a user's phone and send it to remote servers. The most sophisticated Android malware we've seen to date, Geinimi is also the first Android malware in the wild that displays botnet-like capabilities. Once the malware is installed on a user's phone, it has the potential to receive commands from a remote server that allow the owner of that server to control the phone.

Webographie

- **Vie privée**
  - Etude du WSJ: http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html
  - Lookout, App Genome project: http://blog.mylookout.com/2010/07/introducing-the-app-genome-project/
  - Apple poursuivi: http://www.businessweek.com/news/2011-01-05/apple-sued-over-applications-giving-information-to-advertisers.html, http://www.macworld.co.uk/ipod-itunes/news/index.cfm?newsid=3254729
  - E-contact Pro: http://www.econtact-pro.com/FR/
  - Tobias Engel, CCC 2008: http://events.ccc.de/congress/2008/Fahrplan/events/2997.en.html
  - DePetrillo & Bailey, Avril 2010: http://news.cnet.com/8301-27080_3-20002986-245.html
  - Interceptions RIM/BlackBerry: http://www.zdnet.com/blog/india/rim-to-allow-interception-of-blackberry-messenger-in-india/305, http://www.zdnet.fr/actualites/blackberry-et-interception-des-emails-rim-tente-de-gagner-du-temps-en-inde-39757314.htm
- **De nouvelles attaques contre les mobiles**
  - Cabir (Wikipédia), 2004: http://en.wikipedia.org/wiki/Caribe_(computer_worm)
  - 2006 sera l'année des virus mobiles: http://www.lexpansion.com/high-tech/2006-sera-l-annee-des-virus-mobiles_112527.html
  - Botnets Android PoC, Jon Oberheide: http://jon.oberheide.org/files/summercon10-androidhax-jonoberheide.pdf, http://jon.oberheide.org/blog/2010/06/25/remote-kill-and-install-on-google-android/, http://blogs.forbes.com/firewall/2010/06/21/researcher-builds-mock-botnet-of-twilight-loving-android-users/

Webographie

Des mobiles vulnérables

- Faiblesses du protocole GSM, CCC 2010: https://events.ccc.de/congress/2010/Fahrplan/events/4208.en.html
- ZeuS Mitmo, S21Sec: http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html
- Zeus Mitmo, Fortinet: http://blog.fortinet.com/zeus-in-the-mobile-zitmo-online-bankings-two-factor-authentication-defeated/

Des botnets de mobiles

- Article sur le blog de Damballa: http://blog.damballa.com/?p=739
- Geinimi Android: http://blog.mylookout.com/2010/12/geinimi_trojan/
- Botnets plateforme Symbian: http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=225702440, http://www.businessmobile.fr/actualites/un-reseau-de-100-000-smartphones-symbian-zombies-decouvert-39752955.htm
- Botnet Ikee sur iPhone: http://mtc.sri.com/iPhone/, http://www.businessmobile.fr/actualites/ikee-transforme-les-iphone-jailbreakes-en-botnet-39711783.htm

Agenda, Panorama 2010

- Stuxnet : les mystères d'une cyber-attaque industrielle
- [Evocation] Automobile, les OS embarqués
- Hacktivisme : entre criminalité et militantisme
- Le crime est de plus en plus mobile…
- **Botnets : la lutte s'intensifie**
- [Evocations]Bugs, IPV6, jeux en ligne…

Définition

Botnet : ensemble de machines infectées par un composant malveillant et autonome, le « bot » (ou « robot »). Ces machines agissent de concert sous le contrôle d'une même personne.

Les botnets sont typiquement utilisés pour :

- envoyer du spam
- attaquer et infecter de nouvelles machines
- réaliser des attaques de déni de service distribuées (DDoS)
- diffuser d'autres programmes indésirables sur les machines infectées
- générer de façon abusive des clics sur un lien publicitaire
- capturer de l'information sur les machines compromises
- effectuer des opérations de calcul distribué
- dissimuler l'adresse d'un site frauduleux à travers un système de relais transparents (proxy inversé)

Un même ordinateur peut participer à plusieurs botnets ;

Un malware ne forme pas toujours un botnet.

2010 : une année de continuité...

Les botnets qui ont marqué l'année 2010 :

- Bredolab : cumul de 30 millions d'adresses IP infectées
- Mariposa : cumul de 12,7 millions d'IP infectées
- Conficker fait de la résistance : encore 4,8 millions d'IP infectées à fin 2010
- Les botnets bancaires ont le vent en poupe : Zeus/ Murofet, SpyEye, Carberp
- La cyber-armée iranienne se dote d'un botnet

Sur l'année, 77% du spam provient de botnets

- Les botnets spécialisés dans le spam représentent entre 3,5 et 5,4 millions de machines
- Rustock est responsable à lui seul de 47,5% du spam à fin 2010
- Grum, Cutwail, Maazben, Mega-D, Cimbot, Bobax se partagent les places suivantes du classement

… et de ruptures notables

2010 s'est avérée une année sans précédent en matière de coordination de la **lutte contre les botnets** ; et ce non seulement sur le plan de la coopération des forces de l'ordre, mais aussi en matière de coopération public/privé

2010 a vu apparaître en Chine un malware Android évolué, GeiNiMi, qui forme un botnet de téléphones sous Android

La découverte de StuxNet marque également l'apparition de botnets ne répondant pas au modèle cybercriminel classique

Mariposa : l'effet papillon

Identifié en mai 2009, le botnet est décapité le 3 mars 2010 suite à une action conjointe de la Guardia Civil espagnole, de Panda Security et de Defence Intelligence

- Trois personnes d'origine slovène sont arrêtées en Espagne…puis libérées en raison de failles dans la législation espagnole anti-cybercriminalité
- Le 22 mars, « Netkairo » et « Ostiator » postulent chez Panda Security, mais sans succès. S'ensuivent le 12 avril des menaces verbales contre Panda Security, et la publication d'une vidéo dénigrante
- Le 29 juillet 2010, Iserdo, le créateur du malware, est arrêté en Slovénie

Mariposa : l'effet papillon

Gains estimés : 3.000 Euros / mois, correspondant à la location du botnet à d'autres pirates

Des gains faibles comparativement à ceux générés par d'autres botnets

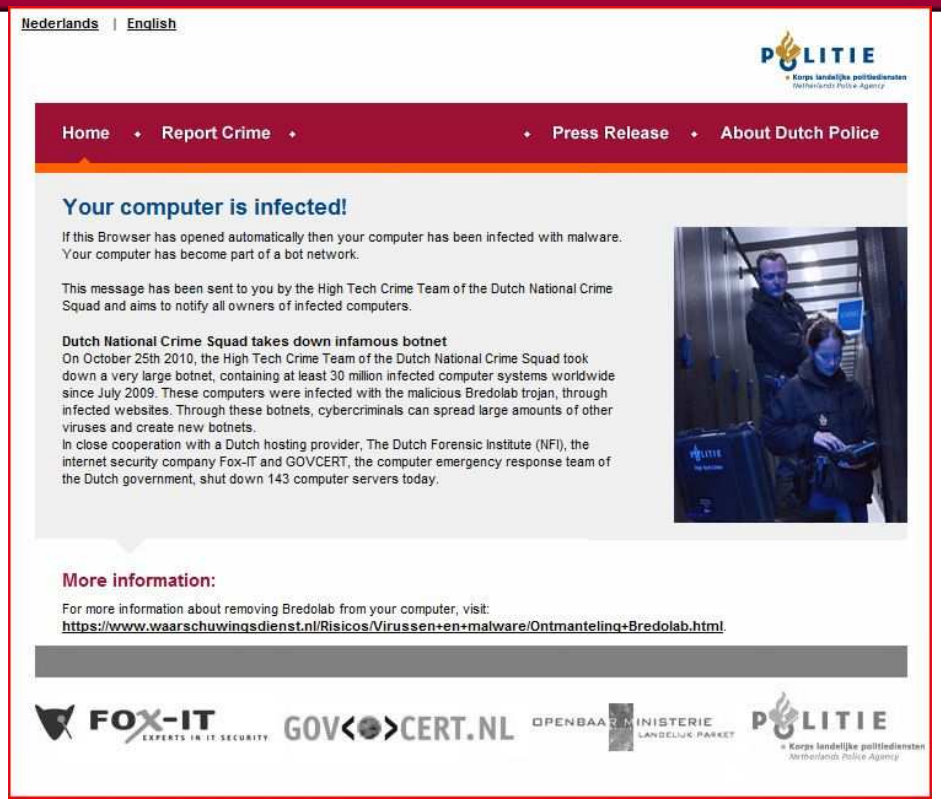
Polémique sur les chiffres : Panda affirme toujours que 13 millions de machines sont infectées, alors qu'il s'agit d'un cumul d'adresses IP sur toute la durée de vie du botnet ; les administrateurs de Mariposa avancent qu'une fourchette de 100.000 à 900.000 machines « seulement » ont participé simultanément au botnet

Problème : le nombre de 13 millions de machines a été repris partout, y compris devant le congrès américain

La fermeture de Bredolab

Le 25 octobre, le Dutch National Crime Squad annonce avoir fermé le botnet Bredolab. Cette opération conjointe a été réalisée en collaboration avec Fox-IT et le CERT gouvernemental néerlandais

- 143 serveurs de contrôle, hébergés chez LeaseWeb, ont été saisis et déconnectés
- L'annonce fait état de 30 millions d'ordinateurs infectés
- Le 26 octobre, Georgiy Avanesov, citoyen russe administrateur de Bredolab, est arrêté en Arménie. Il est soupçonné d'avoir engrangé pas moins de € 100.000 par mois grâce au spam envoyé par son botnet



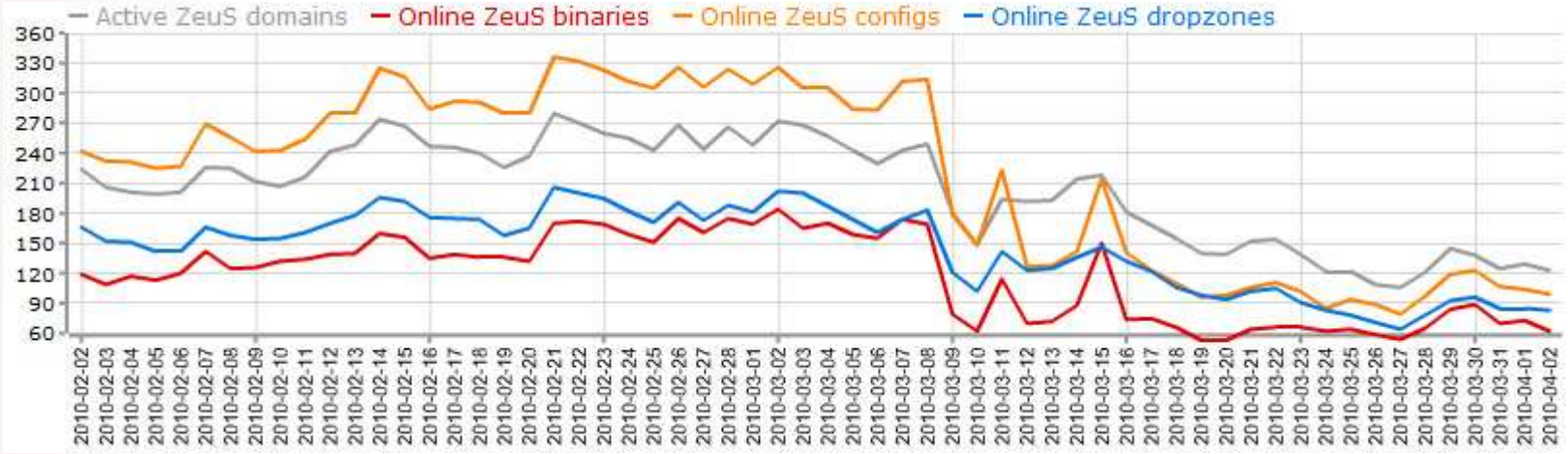
Cette action est toutefois émaillée de polémiques :

la police a utilisé les botnets pour rediriger les victimes de Bredolab vers une page d'information sur le site de la police. Une action dont on peut douter de la légalité

le botnet a partiellement ressuscité quelques jours plus tard

La lutte contre les botnets Zeus

9 mars : l'opérateur kazakh TROYAK (littéralement, « Troyen ») ferme ses portes. Il entraîne dans sa chute la moitié des serveurs de contrôle de Zeus recensés

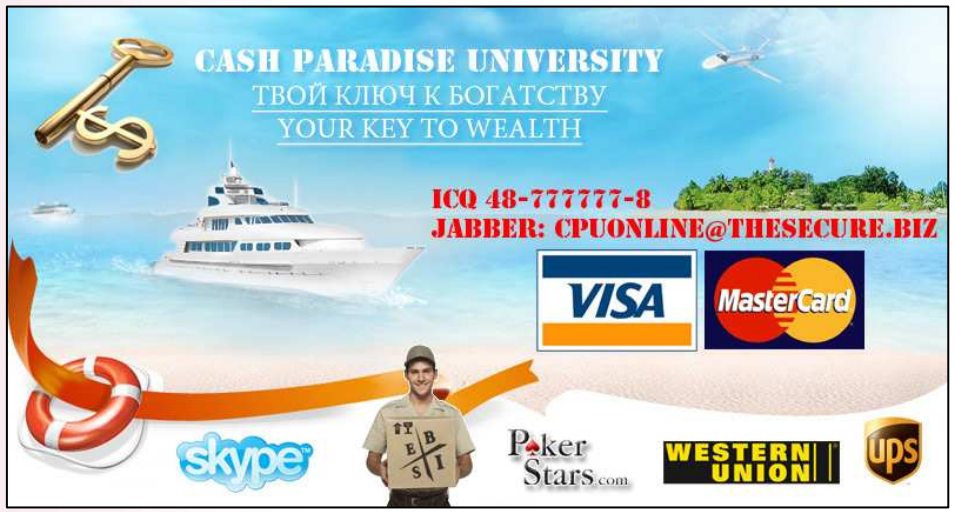


Serveurs de contrôle Zeus actifs entre février et avril 2010

Source : Abuse.ch

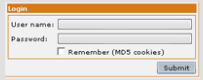
La lutte contre les botnets Zeus

Les criminels s'organisent : apparition d'une offre de formation en ligne pour maîtriser Zeus



[6] Botnet or how to get my own bank accounts. 12-18h - 500$

**for those who passed the basic*
**experienced PC user*



Trojan - virus, programm, that helps you to get your own bank accounts, paypal, credit cards, poker accounts, ebay, admin accounts of shops and so on.

A botnet is a serious thing, it's not Skype carding)) Bank accounts, credit cards, shops, MoneyBookers, Bet office, poker, Ebay, Enroll - all this you get with Bank Trojan, Trojan are all sorts of public nice triple ZeuS, I remember in my memory was limbo and adrenaline and SpyEye, from privat mbo and 76, must always start somewhere in order to get results and not necessarily to invest 15k in a new Zeus of the author, can be found in public for free 1.2 or 1.3, forums often spread builder, that's only 90% of them are infected with other viruses and your admin panel, along with Troy obscured As soon as you let go LOADS.

Material for the work included:

Zeus Trojan (bank trojan). *WE DON'T SELL BUILDER*
Injects Pack (>200 injects)
VPS Hosting for trojan (1 month)
DoubleVPN for security in network

Advice: invest in a triple can be infinitely better to hone a particular topic, of course the most money its auto-transfers:)

Result: Mak Trojan, will go a few thousand loads and get the combat botnet, which You will have your own logs (bank accounts), will introduce the basics of cryptography, where are get loads, also learn to write injections, and be able to earn money on this.

La lutte contre les botnets Zeus

Octobre : arrestation au Royaume-Uni, aux Etats-Unis et en Ukraine de 116 personnes exploitant Zeus. Le montant des gains de ce gang est estimé à 9,4 millions USD

… mais Victor Pleshchuk, cerveau du gang, évite la case « prison », et n'est condamné qu'à 4 ans de probation par la justice russe

Octobre : le créateur de Zeus jette l'éponge et donne le code-source du malware à son rival, l'auteur de Spy Eye

Attention aux effets d'annonce

Sur l'année, le traitement médiatique des botnets laisse globalement à désirer :

- **Des chiffres grossièrement surestimés :** Mariposa, Bredolab, la cyber-armée iranienne, etc.
- **Des botnets imaginaires :** le terme « botnet » a de plus en plus tendance à se substitue à celui de « malware », bien qu'ils désignent des objets différents.
- **Des amalgames** : « le » botnet Zeus
- **Des angles morts** : des botnets dont on ne parle jamais, et d'autres dont on parle tout le temps
- **Des manipulations** : pour vendre, ZoneAlarm se laisse tenter par la tactique de la peur

Coups durs pour d'autres botnets

Lethic : fermeture des serveurs de contrôle par Neustar en janvier ; mais le botnet ressurgit le 11 février. Une nouvelle variante de Lethic est détectée en novembre

Waledac : le 25/02, Microsoft obtient une décision de justice contraignant Verisign à bloquer 277 domaines de contrôle du botnet. Le botnet est décapité

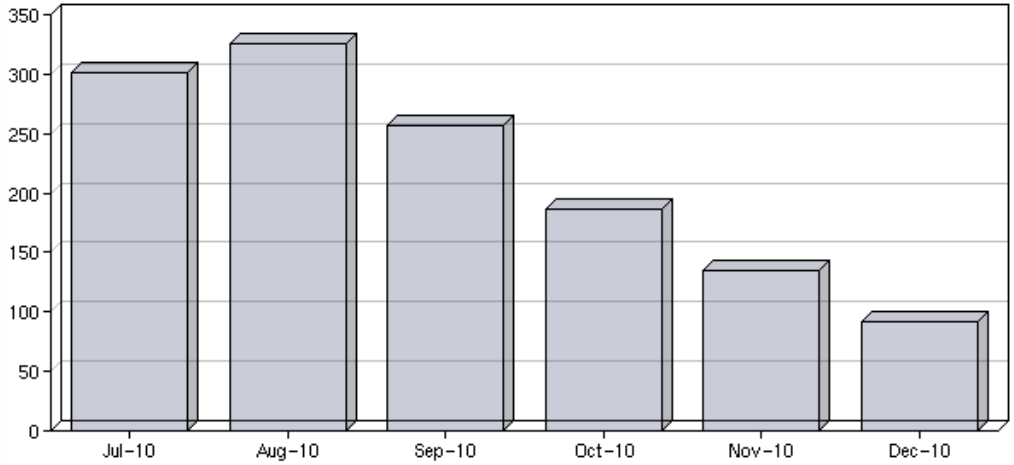
Cutwail/Pushdo : la troisième tentative en août n'est pas plus efficace que les deux premières : le botnet ne reste inactif que pendant deux jours

Mega-D : arrestation en novembre d'Oleg Nikolaenko à Las Vegas, botmaster présumé de 23 ans. Le botnet réduit son activité de 80 %

Depuis mi-2010, le botnet **Avalanche, spécialisé dans le phishing,** n'envoie presque plus de mails

Des effets durables ?

La plupart des observateurs s'accordent pour dire que le volume de spam a globalement diminué sur l'année 2010



Source : Senderbase.org

Volume de spam (milliards) sur la deuxième moitié de l'année 2010

Une baisse accentuée par la fermeture du programme d'affiliation **Spamit** (Canadian Pharmacy, Downloadable Software) au 1er octobre dernier

Les opérateurs s'organisent

Une première européenne :

Au 1er janvier 2010, 14 fournisseurs d'accès néerlandais, représentant 98% du marché de l'accès à Internet grand public du pays, ont mis en place un procédé de filtrage des botnets parmi leurs abonnés

Principales caractéristiques : **notification, mise en quarantaine, assistance technique**

Détection des abonnés infectés depuis de multiples sources, internes et externes ; volonté de partage des informations pertinentes entre opérateurs participant à cet accord

Une initiative qui fait tache d'huile

Australie : l'Australia Internet Industry Association publie son « zombie code », code de bonnes pratiques à destination des FAI, qui promeut le concept de mise en quarantaine ; les FAI volontaires doivent implémenter le zombie code avant décembre 2010. L'IIA milite pour exporter ce code aux Etats-Unis et dans toute la zone Asie-Pacifique

Royaume-Uni : mi-août, Virgin Media annonce que la société préviendra ses abonnés infectés, sur la base des données fournies par des organisations indépendantes, telle que la fondation Shadowserver

Allemagne : le 15 septembre, le pays lance son programme de lutte contre les botnets. Le programme repose sur la notification des infections aux abonnés à Internet

Etats-Unis : Microsoft prend publiquement position pour la mise en place d'un modèle similaire à celui du système de santé publique

Webographie

Observatoire des botnets Zeus et SpyEye :
https://zeustracker.abuse.ch, https://spyeyetracker.abuse.ch

Observatoire des botnets et documentation générale : http://www.shadowserver.org

Microsoft Security Intelligence Report : http://www.microsoft.com/security/sir/threat/

Cartographie des infections selon Panda Security :
http://www.pandasecurity.com/img/enc/infection.htm

Statistiques sur le spam et les malwares selon Cisco : http://www.senderbase.org/

Le blog de Brian Krebs : http://krebsonsecurity.com/

Agenda, Panorama 2010

- Stuxnet : les mystères d'une cyber-attaque industrielle
- [Evocation] Automobile, les OS embarqués
- Hacktivisme : entre criminalité et militantisme
- Le crime est de plus en plus mobile…
- Botnets : la lutte s'intensifie
- **[Evocations]Bugs, IPV6, jeux en ligne…**

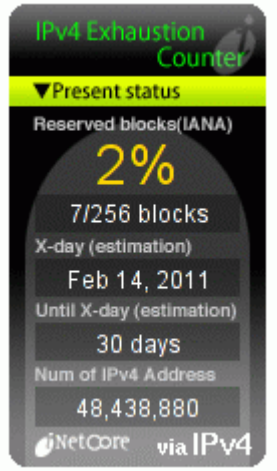
Problèmes de date

- Système informatique bancaire invalide les cartes car se retrouve en 201
- Windows Mobile aussi se retrouve en 2016
- Iphone ne réveille plus

- N'oubliez pas 2038...

IPv6

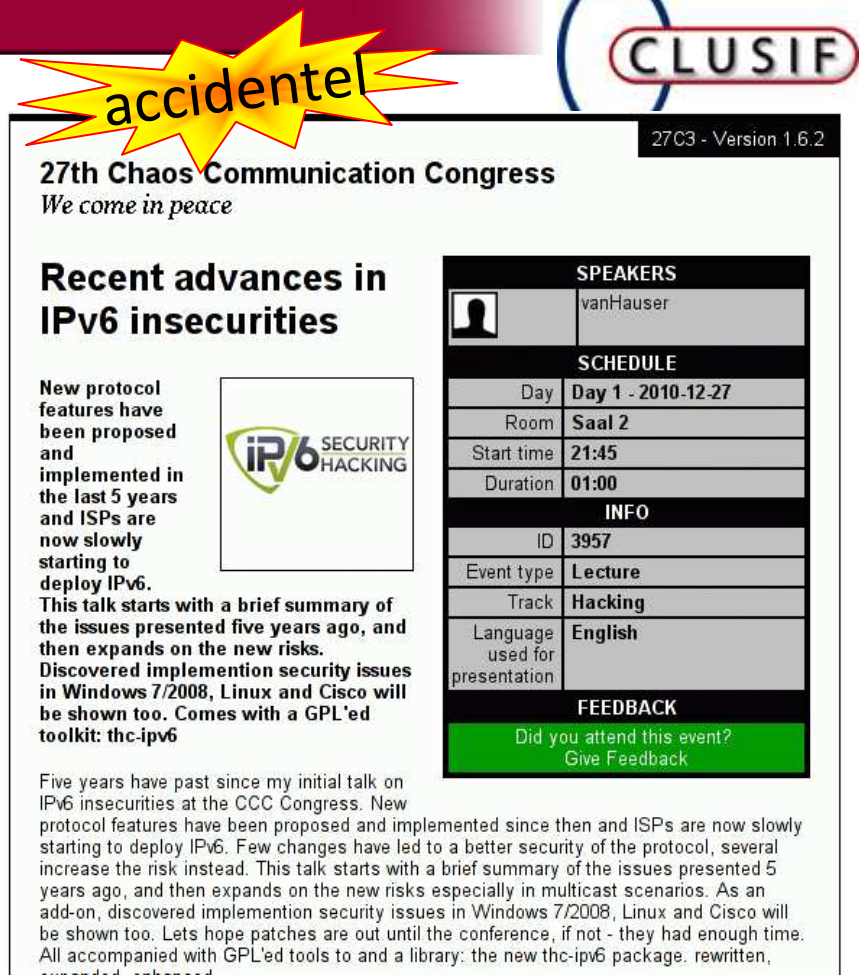
- Fin des adresses IPv4 publiques disponibles coura 2011
  - Difficultés prévues en fin d'année
- Infrastructures prêtes pour IPv6
  - Routeurs, Systèmes d'Exploitations, Google
  - Mais peu d'applications prêtes pour IPv6
- FAI permettent IPv4 et IPv6
- 2011 = début de cohabitation IPv4 / IPv6



IPv6

- Pare-feu de PME-PMI ne protègeront pas toujours en IPv6
- Administrateurs ne sauront pas tous gérer

- Ponts plus exploités depuis des années seront ouverts
- IPv6 maîtrisé par cybercriminels
- Attaques à prévoir



- IPv6 mal conçu
  - Nouveaux problèmes découverts régulièrement

société

Jeux d'argent en ligne

- Opportunité de licences pour petits pays & réserves indiennes
  - Decorrélation géographique entre licence et joueurs
- Immense majorité de sites sans licence du tout
- Escroqueries très nombreuses à l'étranger
  - Automates de jeux, usurpations d'identité, de site, truquage des probabilités, faux intermédiaires, monnaie virtuelle, etc
  - Plus ce qui n'est pas spécifique : vol de n° de cartes, dénis de service, etc.

Jeux d'argent en ligne

- Autorité de Régulation des Jeux en Ligne
  - Protection des consommateurs et populations vulnérables
  - Sécurité et sincérité des opérations de jeux
    - Audit de sécurité front & back-office
    - Contrôle du générateur aléatoire
  - Tracabilité des flux financiers pour lutter contre la fraude et le blanchiment
    - Coffre-fort électronique
  - Fiscalité : prélèvement sur les mises

Jeux d'argent en ligne

- Autorité de Régulation des Jeux en Ligne
  - Cadre régulé de manière exhaustive
  - Pas des bureaucrates
  - Déjà copiée
- Problèmes largement résolus à l'origine
  - Cybercriminalité très difficile en France
  - Peu de cybercriminalité à prévoir

Webographie

Oz bank thinks it's 2016 ! Y2.01K bug invalidates cards
http://www.theregister.co.uk/2010/01/04/bank_queensland/

2016 bug hits Windows phones Y 2.01K spreads
http://www.theregister.co.uk/2010/01/05/windows_mobe_bug/

Webographie

IPv6 Act Now http://www.ipv6actnow.org/info/what-is-ipv4/

273C : Recent advances in IPv6 insecurities
http://events.ccc.de/congress/2010/Fahrplan/events/3957.en.html
http://www.youtube.com/user/kkkwwwaaakkk#p/search/0/c7hq2q4jQYw

Webographie

ARJEL http://www.arjel.fr/-Role-et-missions-.html

Fraud on PartyPoker
http://forumserver.twoplustwo.com/28/internet-poker/fraud-partypoker-533049/

Money laundering with a poker face
http://www.theregister.co.uk/2010/02/05/terror_cybercrime/

Gamer embezzles virtual cash to settle real debts
http://www.theregister.co.uk/2009/07/03/eve_banker_does_a_runner/

En conclusion,
nous aurions aussi aimé évoquer…

- Le **phishing** qui reste une préoccupation majeure avec des variantes (Marché du carbone)…
- La **Chine** : parc informatique très hétérogène, 450 millions d'Internautes… une opportunité pour toutes formes de cybercriminalité
- **Réseaux sociaux et mondes virtuels** : prise de conscience pour certains mais aggravation des conséquences pour d'autres (suicides, ouverture de bureaux de Police virtuels...)
- La **clef USB** : impliquée dans de nombreuses affaires (Stuxnet, attaques ciblées (Pentagone))
  25 % des nouveaux *malwares* sont conçus pour ce périphérique…