La Cybercriminalité

Vulnérabilités, cybermenaces et attaques sur l'information numérique

2016
Gérard Peliks
gerard.peliks@noos.fr
président de l'association CyberEdu

Durée de vie de votre PC non protégé ?

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

3 minutes !

Selon le SANS Institute
www.sans.org

Exemples de pertes dues aux attaques

- **Coût moyen suite à une cyberattaque, en 2015, en France ?**
  - Une attaque majeure en France tous les 15 jours (source ANSSI)

    773 000 euros… €

    NTT Communications | NTT Com Security

    Enquête sur plus de 1000 entreprises, plus de 100 en France

    En 2014, 561 000 €
- **Coût d'une panne majeure des SI en Europe ?**

  250 milliards de dollars CSI COMPUTER SECURITY INSTITUTE

  Imaginez : Plus d'électricité, plus de transports…
- **Coût annuel du cybercrime ?**

  Environ 600 milliards de dollars

Attaques sur les 3 couches du cyberespace

Couche de la signification

Couche des logiciels

Couche des infrastructures

Les 263 câbles sous-marins

Plus d'Internet en Algérie, fin octobre 2015

Attaques sur les 3 couches du cyberespace

Couche de la signification

Couche des logiciels

Couche des infrastructures

Failles Pegasus sur IoS

3 vulnérabilités 0days

Source : NSO août 2016

Attaques sur les 3 couches du cyberespace

Couche de la signification

Couche des logiciels

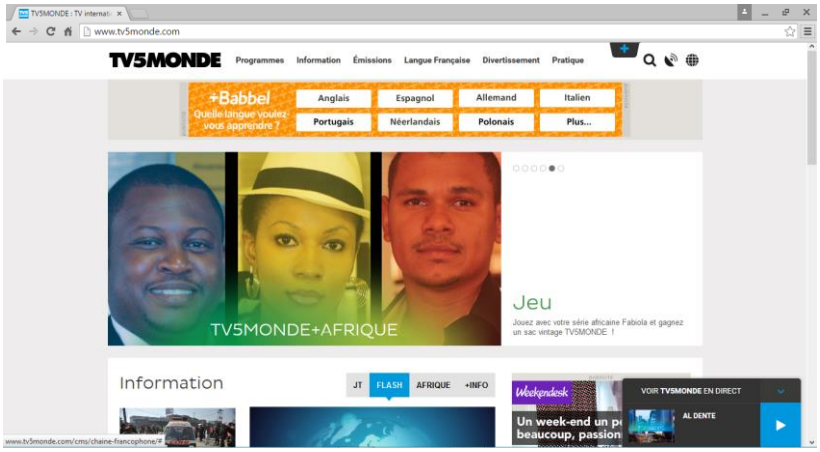
Couche des infrastructures

Attaque sur TV5 Monde : Les émissions

Mercredi 8 avril 2015

TV5 Monde, chaîne internationale francophone, qui émet dans 200 pays et territoires dans le monde, 290 millions de foyers connectés

Attaque sur TV5 Monde



Attaque sur TV5 Monde : Le web

« Au nom d'Allah le tout Clément, le très Miséricordieux, le CyberCaliphate continue à mener son cyberjihad contre les ennemis de l'Etat islamique »

Attaque sur TV5 Monde : Facebook

vidéos de propagandes

CV et cartes d'identités de militaires français impliqués dans les opérations contre l'Etat islamique

« *Nous ne sommes plus en état d'émettre aucune de nos chaînes. Nos sites et nos réseaux sociaux ne sont plus sous notre contrôle et ils affichent tous des revendications de l'Etat islamique* » *Yves Bigot*

Attaque sur TV5 Monde : Le web

Attaque sur TV5 Monde : Les conséquences

- Après huit heures d'interruption, les programmes de TV5 Monde ont finalement pu être rétablis le lendemain, à 5 heures du matin
- Trois mois et demi après, les 400 salariés de TV5 Monde ne pouvaient toujours pas travailler normalement
  - Pas de Wi-Fi, pas d'Internet
  - Obligation de construire une nouvelle architecture de diffusion
- Coût de l'attaque :
  - 4,6 millions d'euros pour l'année 2015
  - 3,1 millions d'euros pour l'année 2016
  - 2,5 millions d'euros par an à partir de 2017
- Les revenus publicitaires se sont effondrés

TV5MONDE

Attaque sur TV5 Monde : L'attaque

- **Première phase : Ingénierie sociale**
  - Repérage et cartographie » du SI et du personnel de TV5 Monde
- **Deuxième phase en janvier 2015 : un e-mail contaminé**
  - Envoi d'un e-mail, adressé aux journalistes de TV5 Monde
  - Un cheval de Troie pénètre dans le système de la chaîne
  - La partie « métier » et la partie bureautique, sont non compartimentées et ouvertes sur l'extérieur via Internet
- **Troisième phase en avril : l'attaque finale**
  - Attaque sur les serveurs et les réseaux sociaux
  - Attaque sur les multiplexeurs, encodeurs, switchs : signal audiovisuel coupé. Infrastructures principale et de secours neutralisées d'un seul coup

Attaque sur TV5 Monde : Qui ?

- **Cybercalifate ? Daesh ??? (pas de revendications)**
- **Piste de 10 hackers russes avancée : APT28**
- **Commanditaire ?**
  - Kremlin ?
  - Etat Islamique ?
  - ???

APT 28 !

?

?

Attaque sur TV5 Monde : Contre-mesures

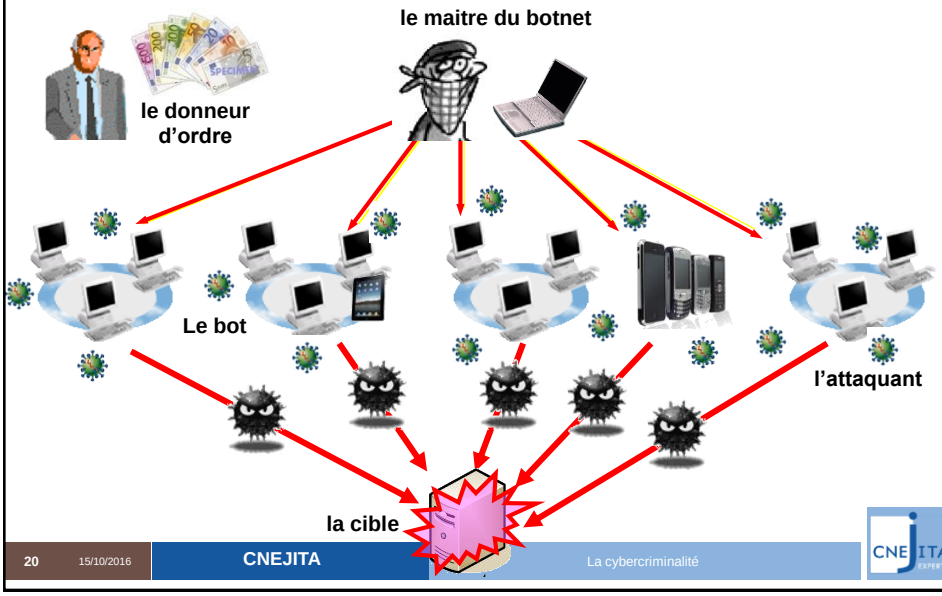
- **Treize ingénieurs de l'ANSSI à la rescousse**
- **Remise en état du site en moins de 20 heures**
- **Nouvelle architecture de diffusion construite**
- **Mots de passe plus complexes, modifiés fréquemment**
- **Aide d'une société d'experts**
- **Sécurité du système d'Information renforcée**

TV5MONDE

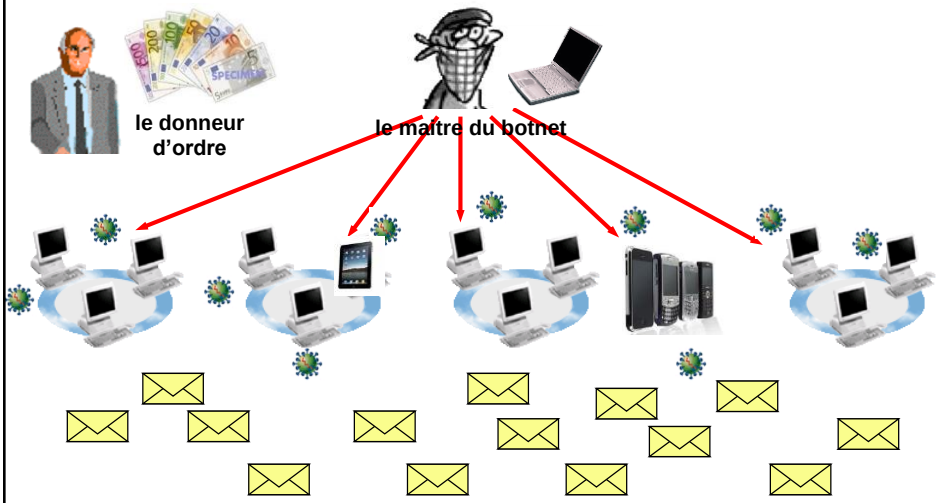
Quelques attaques

- **Estonie 2007 : Les botnets**
- Iran 2010 : Les scada
- Bercy 2011 : Les APT
- Flame 2012 : Le cyber espionnage
- Elysée 2012 : La réaction de la France
- Shamoon 2012 : La destruction
- 2014 / 2015 : Vols d'identités numériques
- Le phishing
- 2015 : La fraude au président
- 2016 : Les cryptovirus

Les botnets : attaques en dénis de services



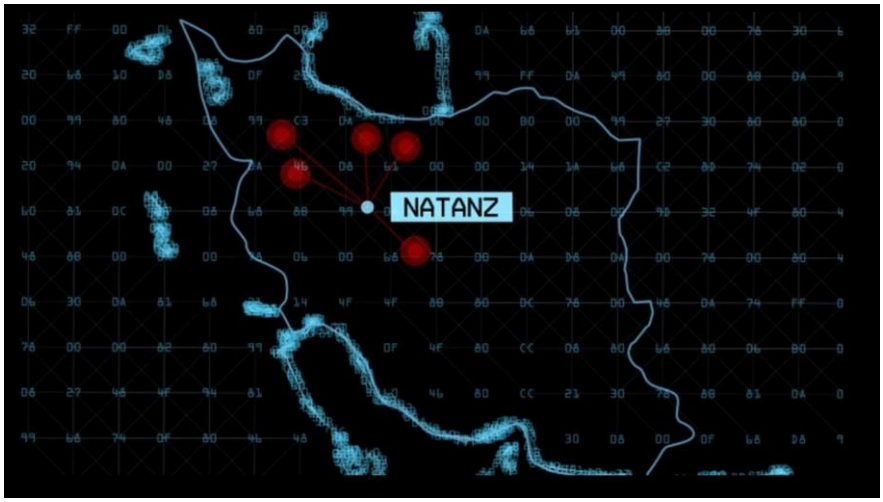
Botnet pour SPAM…



Quelques attaques

- Estonie 2007 : Les botnets
- **Iran 2010 : Les scada**
- Bercy 2011 : Les APT
- Flame 2012 : Le cyber espionnage
- Elysée 2012 : La réaction de la France
- Shamoon 2012 : La destruction
- 2014 / 2015 : Vols d'identités numériques
- Le phishing
- 2015 : La fraude au président
- 2016 : Les cryptovirus

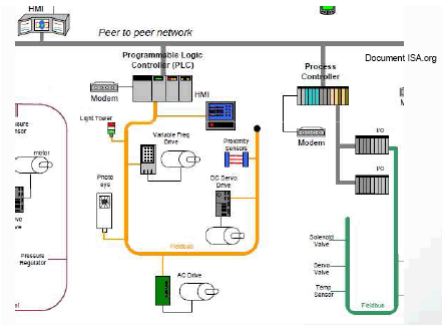
Stuxnet : Les attaques sur les SCADA



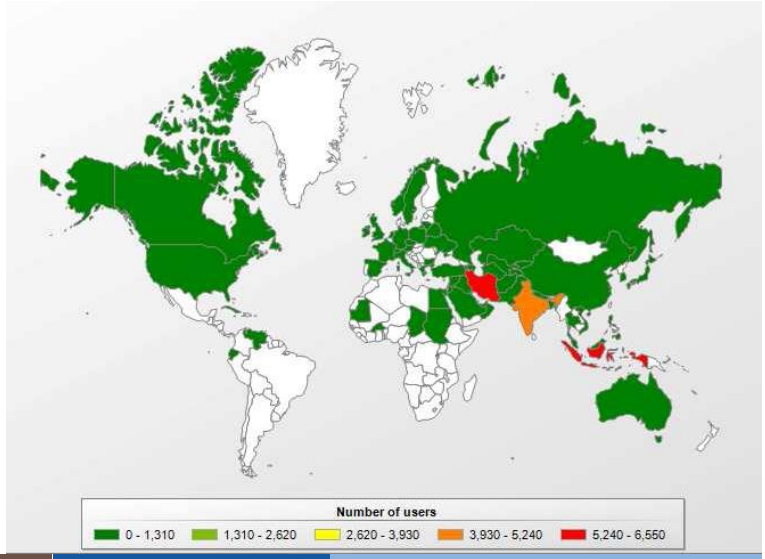
Supervisory Control And Data Acquisition

Stuxnet : Les attaques sur les SCADA

Stuxnet



Stuxnet : Les attaques sur les SCADA



Stuxnet … arrive en France

HACKER OUVERT

LA SOCIÉTÉ AIR LIQUIDE PIRATÉE PAR STUXNET

Le géant français des gaz industriels a été victime du célèbre virus créé pour viser le programme nucléaire iranien.

Stuxnet : Les attaques sur les SCADA

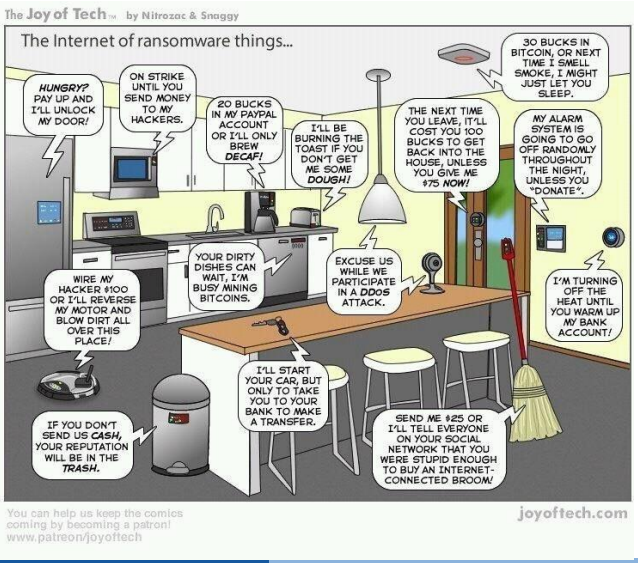
- Coopération USA / Israël (programme Olympic Games)
- 10 000 heures-hommes de développement
- Exploitation de 4 "zero-day attacks"
- Logiciels signés par usurpation (faux certificats...)
- Une erreur dans le sabotage : 100 000 ordinateurs infectés

Et aujourd'hui : **Nitro Zeus**

Autres attaques sur les SCADA

- 2014 : Un haut fourneau endommagé dans une aciérie allemande
- 2015 : Une centrale électrique ukrainienne neutralisée
- 2015 : Une jeep piratée par des hackers

Que nous réserve l'IoT ?



Quelques attaques

- Estonie 2007 : Les botnets
- Iran 2010 : Les scada
- **Bercy 2011 : Les APT**
- Flame 2012 : Le cyber espionnage
- Elysée 2012 : La réaction de la France
- Shamoon 2012 : La destruction
- 2014 / 2015 : Vols d'identités numériques
- Le phishing
- 2015 : La fraude au président
- 2016 : Les cryptovirus

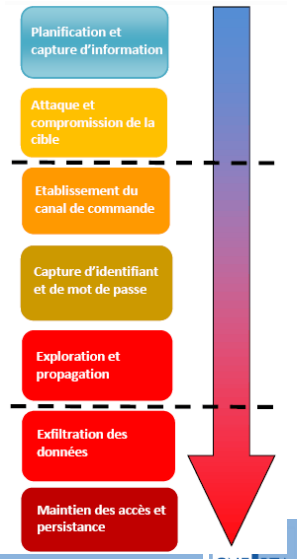
Les attaques par APT (advanced persistent threats)

Les APT, 1/3 de marketing sécurité, 1/3 de gros titres dans la presse, 1/3 de petits mensonges ?

NON !

Une APT est une attaque ciblée qui agit silencieusement et s'installe dans le système d'information cible, avec pour objectif de collecter et corrompre des informations sensibles sur le long terme, plutôt que de réaliser un gain immédiat.

Une APT toutes les 1,5 secondes !



Quelques attaques

- Estonie 2007 : Les botnets
- Iran 2010 : Les scada
- Bercy 2011 : Les APT
- **Flame 2012 : Le cyber espionnage**
- Elysée 2012 : La réaction de la France
- Shamoon 2012 : La destruction
- 2014 / 2015 : Vols d'identités numériques
- Le phishing
- 2015 : La fraude au président
- 2016 : Les cryptovirus

Flame : Le cyber espionnage

- **L'Iran et d'autres pays du Moyen Orient contaminés**
  - Flame arrive avec une mise à jour de Windows
  - C'est un logiciel espion, avec key loggers et screen savers
  - Il contamine les smartphones à proximité, par Bluetooth
  - Il porte une boite à outils de 20 Mo
  - Il est écrit en un langage peu connu : Lua
  - Il s'autodétruit sur commande à distance

Quelques attaques

- Estonie 2007 : Les botnets
- Iran 2010 : Les scada
- Bercy 2011 : Les APT
- Flame 2012 : Le cyber espionnage
- **Elysée 2012 : La réaction de la France**
- Shamoon 2012 : La destruction
- 2014 / 2015 : Vols d'identités numériques
- Le phishing
- 2015 : La fraude au président
- 2016 : Les cryptovirus

Attaque sur l'Elysée, qui est le coupable ?

Source : Linformaticien

Attaque sur l'Elysée, qui est le coupable ?

Source : Lexpress 20//11/2012

Attaque sur l'Elysée, la réaction de la France

Rapport Bockel

ANSSI

218 OIV

LPM

Réserve Citoyenne de Cyberdéfense

Label France Cybersecurity

CyberEdu

Quelques attaques

- Estonie 2007 : Les botnets
- Iran 2010 : Les scada
- Bercy 2011 : Les APT
- Flame 2012 : Le cyber espionnage
- Elysée 2012 : La réaction de la France
- **Shamoon 2012 : La destruction**
- 2014 / 2015 : Vols d'identités numériques
- Le phishing
- 2015 : La fraude au président
- 2016 : Les cryptovirus

Shamoon : Le ver qui détruit

- **Une attaque destructrice**
  - Sur la société Aramco
  - 30 000 ordinateurs détruits en octobre 2012
  - 2 semaines pour rétablir les services informatiques
  - Les installations gazières du Qatar (Rasgaz) touchées

Quelques attaques

- Estonie 2007 : Les botnets
- Iran 2010 : Les scada
- Bercy 2011 : Les APT
- Flame 2012 : Le cyber espionnage
- Elysée 2012 : La réaction de la France
- Shamoon 2012 : La destruction
- **2014 / 2015 : Vols d'identités numériques**
- Le phishing
- 2015 : La fraude au président
- 2016 : Les cryptovirus

Vols d'identités numériques

Target 2014
- Données de 110 millions de clients : coût 252 M$

Orange 2014
- 1.3 millions de e-mails clients volés

JPMorgan 2014
- 80 millions de comptes utilisateurs

OPM 2015
- 4 millions de comptes d'agents fédéraux US

Hello Kitty 2015

Yahoo victime d'un méga vol de données, 200 millions de comptes potentiellement concernés

Quelques attaques

- Estonie 2007 : Les botnets
- Iran 2010 : Les scada
- Bercy 2011 : Les APT
- Flame 2012 : Le cyber espionnage
- Elysée 2012 : La réaction de la France
- Shamoon 2012 : La destruction
- 2014 / 2015 : Vols d'identités numériques
- **Le phishing**
- 2015 : La fraude au président
- 2016 : Les cryptovirus

1 – Le Phishing : l'accroche par e-mail

2 – Le Phishing : la poursuite par le Web

3 – Le Phishing : et pour conclure…

3 – Le Phishing : Si on avait regardé…

IP Information for 41.143.60.21

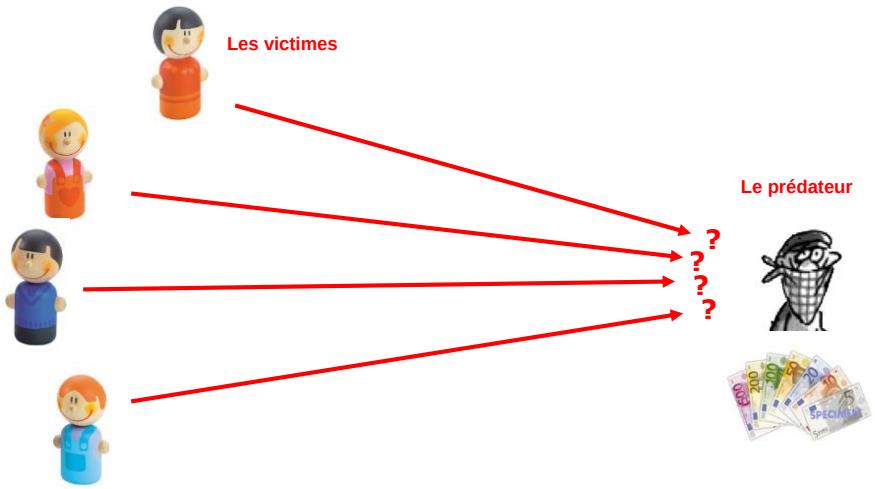
IP Location:	Morocco Rabat Ip Adsl Maroctelecom
ASN:	AS6713
IP Address:	41.143.60.21 W R P D T

```
inetnum:        41.143.0.0 - 41.143.255.255
netname:        IP_ADSL_MarocTelecom
descr:          IP_ADSL_MarocTelecom
country:        MA
admin-c:        SMT1-AFRINIC
tech-c:         DMT1-AFRINIC
status:         ASSIGNED PA
mnt-by:         ONPT-MNT
source:         AFRINIC # Filtered
parent:         41.140.0.0 - 41.143.255.255

person:         SEPFS Maroc Telecom
address:        Service Exploitation des PFS
address:        MAROC TELECOM
address:        Avenue de France AGDAL
address:        Immeuble DR Rabat
e-mail:         nocmt@menara.ma
phone:          +21237686318
nic-hdl:        SMT1-AFRINIC
source:         AFRINIC # Filtered

person:         DEMPFS Maroc Telecom
address:        Division Exploitation et maintenance des PFS
address:        MAROC TELECOM
address:        Avenue de France AGDAL
address:        Immeuble DR Rabat
e-mail:         nocmt@menara.ma
phone:          +21237686318
nic-hdl:        DMT1-AFRINIC
source:         AFRINIC # Filtered
```

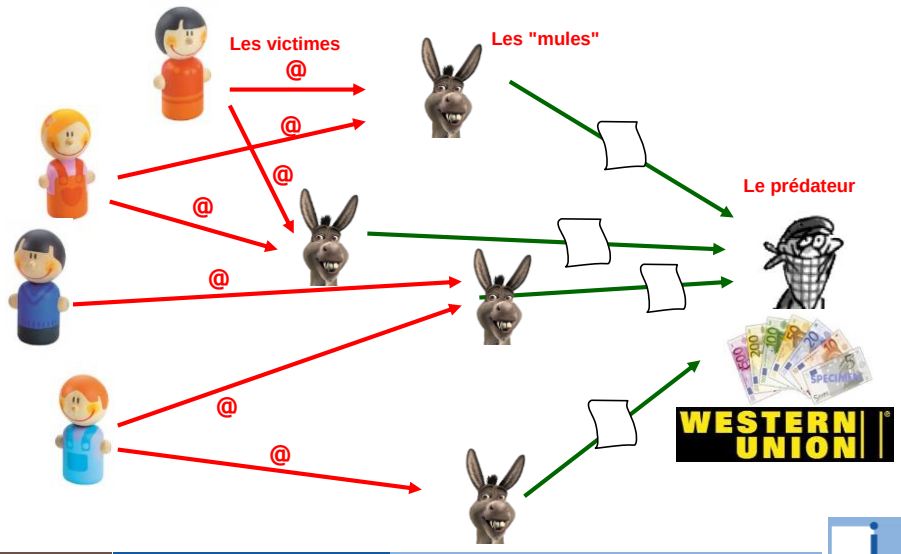
4 - Le Phishing : exploitation des résultats

Vos coordonnées bancaires vont être exploitées par le pirate !

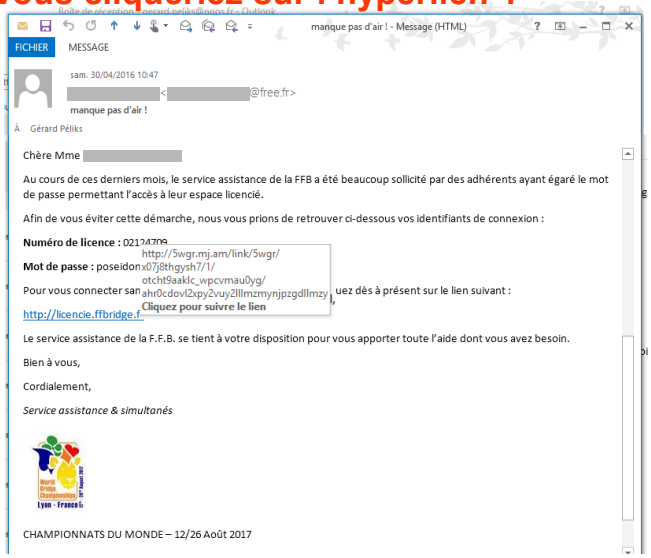
Le Phishing : Le modèle économique



Le Phishing : le modèle économique



Vous cliqueriez sur l'hyperlien ?



Quelques attaques


Estonie 2007 : Les botnets


Iran 2010 : Les scada


Bercy 2011 : Les APT


Flame 2012 : Le cyber espionnage


Elysée 2012 : La réaction de la France


Shamoon 2012 : La destruction


2014 / 2015 : Vols d'identités numériques


Le phishing


2015 : La fraude au président


2016 : Les cryptovirus

La fraude au président

- **Particularité française**
- **Parfaite connaissance de l'entreprise**
- **Cible : En général un comptable**
- **Attaquant : Il se fait passer pour le président**
- **Quand : Souvent juste avant un weekend ou les congés**
- **350 entreprises françaises** attaquées en 2013
  - Géant Vert (Landes) : 17 millions €
  - KPMG : 7,6 millions €
  - Michelin : 1,6 millions €
  - Elysée : 2 millions € (rembousements voyages Air France)
- **350 millions d'euros (évaluation printemps 2015)**

Quelques attaques

- Estonie 2007 : Les botnets
- Iran 2010 : Les scada
- Bercy 2011 : Les APT
- Flame 2012 : Le cyber espionnage
- Elysée 2012 : La réaction de la France
- Shamoon 2012 : La destruction
- 2014 / 2015 : Vols d'identités numériques
- Le phishing
- 2015 : La fraude au président
- **2016 : Les cryptovirus**

Petit clic et grosse claque !

Tiré d'une présentation de la gendarmerie nationale

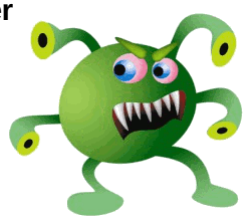
Rançongiciel - Cryptolockers

Cryptolocker : un commissariat de police américain débourse 500$ pour récupérer ses données

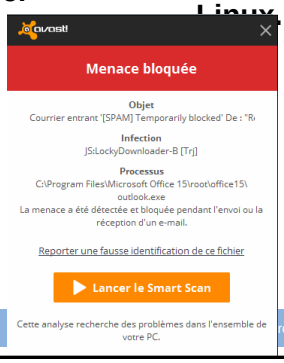
Quelques cryptovirus …

- CryptoWall
- CBT-Locker
- Locky
- TeslaCrypt
- CryptXXX
- ZCryptor
- Petya
- Mischa
- …….

- KeRanger



- Dubbed Linux.Encoder.1



http://map.norsecorp.com/#/

Plate-forme Pharos du Minint

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

internet-signalement.gouv.fr
Portail officiel de signalement des contenus illicites de l'Internet

Signaler

SE RENSEIGNER
Questions et Réponses
Conseils
Conseils aux Jeunes
Conseils aux Parents
Internet Prudent
Protéger son ordinateur
Liens Utiles

Internet est un espace de liberté où chacun peut communiquer et s'épanouir. Les droits de tous doivent y être respectés, pour que la « toile » reste un espace d'échanges et de respect. C'est pourquoi les pouvoirs publics mettent ce portail à votre disposition. En cliquant sur le bouton « SIGNALER », vous pouvez transmettre des signalements de contenus ou de comportements illicites auxquels vous vous seriez retrouvés confrontés au cours de votre utilisation d'Internet.

Signaler >>

Vous trouverez également sur ce site des pages d'information, ainsi que des conseils de spécialistes pour mieux vous protéger et protéger vos proches dans leur utilisation de l'Internet.

ACTUALITÉS

Bulletin d'information sur le virus DRID... - 23 juillet 2015 Qu'est-ce que Dridex ? Dridex est un cheval d...

Le nombre de signalements a augmenté en ... - Vous nous avez adressé 137 456 signalements en 2014. Nous vo...

Faux courriels terroristes / vraies arna... - 2 mai 2014 On signale une recrudescence de pourriels (spams) ...

Le nombre de signalements a augmenté en ... - 03/01/2014 Vous nous avez adressé 123 987 signalements en 201...

Le nombre de signalements augmente - 16/01/2013 Grâce à vous, près de 120 000 contenus

130 000 signalements par an, 400 par jours
38 000 signalements,entre le 7 et le 30 janvier 2015

Les tuiles qui protègent de la pluie ont toutes été posées par beau temps

用瓦盖 *Proverbe chinois*

Merci pour votre attention!

Des questions?

Gérard Peliks
gerard.peliks@noos.fr