

Cyberguerre et cyberdéfense

23.03.2015

Gérard Peliks

LTC Réserve Citoyenne de Cyberdéfense DGGN

gerard.peliks@noos.fr

Expert Sécurité



Cyberguerre et cyberdéfense

–Les dangers du cyberspace

- Des attaques sur les organisations
- Vivre avec les menaces, mais réagir



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

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

En 2003 : 40 minutes

En 2004 : 20 minutes



Selon le SANS Institute
www.sans.org

Aujourd'hui : 3 minutes

Gérard Peliks

3/ 47

Exemples de pertes dues aux attaques

- Coût moyen suite à une cyberattaque, en 2014, en France ?

561 000 €

En 2013, 280 000 € (+200% d'augmentation)

Source :



- Coût d'une panne majeure des systèmes d'information en Europe ?

250 milliards de dollars

Source : The logo for the Computer Security Institute, featuring the letters "CSI" in a stylized font with "COMPUTER SECURITY INSTITUTE" underneath.

*Une telle panne a une probabilité de 10 à 20% de se produire dans les 10 prochaines années
Imaginez : Plus d'électricité, plus de transports...*

- Coût mondial estimé du cybercrime en 2014 ?

Environ 600 milliards de dollars

Source : *Forum international sur la communication commerciale*
Sept. 2014

Gérard Peliks

4/ 47

Attaques sur les 3 couches du cyberespace

Couche de la signification

Couche des logiciels

Couche des infrastructures

Gérard Peliks

5/ 47

La disponibilité de l'Information tient parfois à un fil...



Source : iTespresso.fr

Vélizy, mai 2011



Source : iTespresso.fr



matelsom : 250.000 euros de perte, 120 personnes au chômage technique

6/ 47

Attaques sur les 3 couches du cyberespace

Couche de la signification

Couche des logiciels

Couche des infrastructures

Gérard Peliks

7 / 47

Failles d'aujourd'hui : Heartbleed

Le 08 Avril 2014

Des chercheurs alertent sur une faille critique dans OpenSSL



La menace Heartbleed touche plusieurs versions d'OpenSSL

Les experts en sécurité informatique conseillent aux administrateurs de corriger une faille critique dans OpenSSL, une bibliothèque Open Source de protocoles de chiffrement qui est utilisé par un grand nombre de sites web.

Plusieurs spécialistes de la sécurité ont alerté les administrateurs des sites web afin qu'ils corrigent une faille importante dans OpenSSL. Cette vulnérabilité est surnommée « Heartbleed » et se trouve dans plusieurs versions d'OpenSSL, une bibliothèque Open Source de chiffrement pour communiquer en SSL (Secure Socket Layer) ou TLS (Transport Security Layer). La plupart des sites utilise ce système de chiffrement caractérisé par la présence dans les navigateurs du symbole du cadenas. La faille a été découverte en décembre 2011, mais elle vient d'être corrigée par la version 1.0.1g d'OpenSSL publiée hier. Selon un site spécialement mis en place

Gérard Peliks

8 / 47

Attaques sur les 3 couches du cyberespace

Couche de la signification

Couche des logiciels

Couche des infrastructures

Gérard Peliks

9/ 47

Un répertoire de Web défacés : www.zone-h.org/archive

 zone-h unrestricted information								
Time	Notifier	H	M	R	L	★ Domain	OS	View
12:00	/Newbie4rt_ID					www.m-mehdizade.ir/Jamvan.php	Linux	mirror
11:56	KuroiSH					jakprogramovat.cz/xmlrpc.php	Linux	mirror
11:54	w4l3xzV3					teamche.com/w.htm	Linux	mirror
11:54	Nitro Gin					ad-airway.fr/index.php	Linux	mirror
11:53	Laakel En Person	H	M			www.claire-pichon-avocat.com	Linux	mirror
11:52	w4l3xzV3					simavis.nl/w.htm	Linux	mirror
11:51	Laakel En Person	H	M			cogipro.com	Linux	mirror
11:50	w4l3xzV3					keepingfamilies together.net/w.htm	Linux	mirror
11:48	Laakel En Person	H				azulicreation.fr	Linux	mirror
11:47	NetDefacer		R			projectcentral.astleygilbert.c...	Win 2000	mirror
11:47	ZeynnymouZ	H	M			perlengkapankostjoga.com	Linux	mirror
11:46	NetDefacer		R			areaclienti.voicevolution.it/b...	Win 2000	mirror
11:44	Dr.T3rr0r	H	M	R		www.protechbuildingproducts.co.za	Linux	mirror
11:44	Dr.T3rr0r	H	M			www.procurementsystem.co.za	Linux	mirror
11:44	Dr.T3rr0r	H	M			www.partyemporium.co.za	Linux	mirror
11:44	Dr.T3rr0r	H	M			www.reddental.co.za	Linux	mirror
11:44	Dr.T3rr0r	H	M			itsupportnelspruit.co.za	Linux	mirror
11:44	Dr.T3rr0r	H	M			www.interiordesignerscapetown....	Linux	mirror
11:44	Dr.T3rr0r	H	M			www.ppmconsultants.co.za	Linux	mirror
11:43	ZeynnymouZ	H	M			produkisprejogja.com	Linux	mirror
11:35	w4l3xzV3		R			interlaw.org/w.htm	Linux	mirror
11:32	w4l3xzV3					dvelopit.co.nz/w.htm	Linux	mirror
11:32	w4l3xzV3					ldag.net/w.htm	Linux	mirror
11:31	w4l3xzV3					gregmessel.com/w.htm	Linux	mirror
11:30	w4l3xzV3					eisenberg-allgaeu.de/w.htm	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified anonymously to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might offend contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. [Read more](#)

Plus de xxxx Webs, en France défigurés du 7 au 9 janvier 2015

Hacked by Islamic State

لَا إِلَهَ إِلَّا اللَّهُ



Hacked by Islamic State (ISIS)
We Are Everywhere :)
<http://fb.com/100008945136328>

Gérard Peliks

11/ 47

Faux tweet sur Associated Press (23 avril 2013)

AP The Associated Press @AP

Follow

Breaking: Two Explosions in the White House and Barack Obama is injured

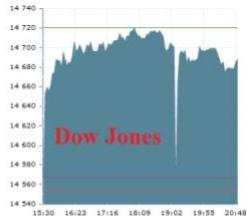
Reply Retweet Favorite More

2,894 RETWEETS

134 FAVORITES



10:07 AM - 23 Apr 13



<http://sea.sy/>

le Dow Jones (DJIA) perd 145 points
136 milliards de dollars de pertes sur l'indice boursier !!!

Gérard Peliks

12/ 47

Cyberguerre et cyberdéfense

- Les dangers du cyberspace
- Des attaques sur les organisations**
- Vivre avec les menaces, mais réagir



Gérard Peliks

13/ 47

Les attaques notables sur les organisations entre 2007 et 2011

 Estonie 2007 : **Les botnets** 

 Iran 2010 : Le ver Stuxnet : Les SCADA

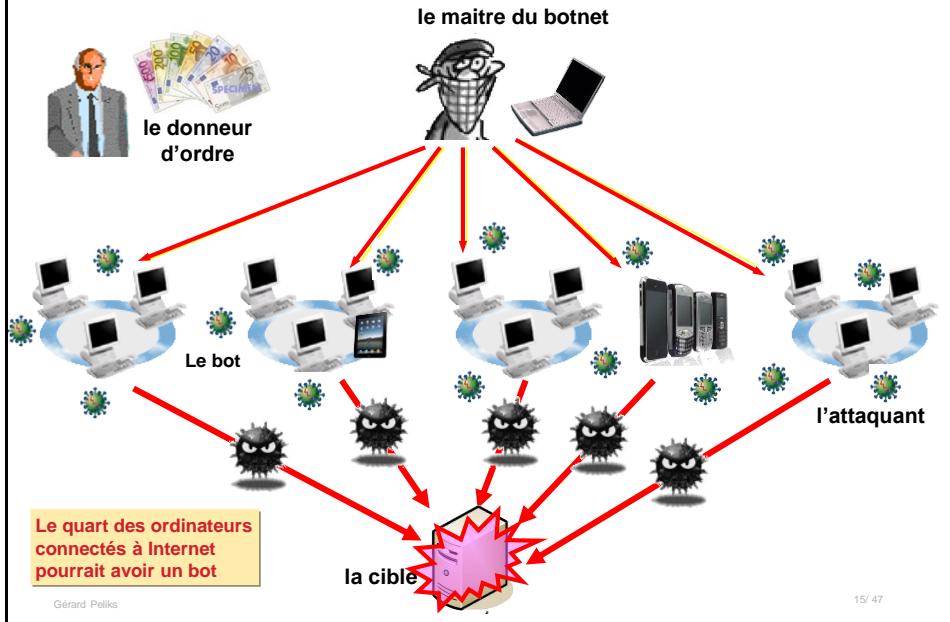


Bercy, Areva, Sony 2011 : Les APT

Gérard Peliks

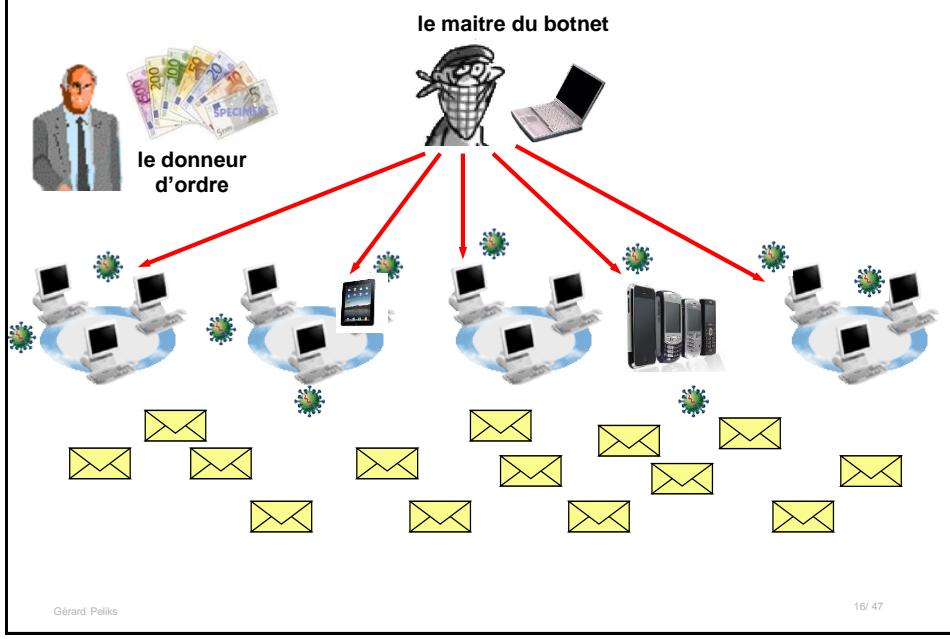
14/ 47

Le botnet : attaques en dénis de services distribués



15/ 47

Le botnet pour spammer



16/ 47

Les attaques notables sur les organisations entre 2007 et 2011

 Estonie 2007 : Les botnets

 Iran 2010 : Le ver Stuxnet : **Les SCADA** 

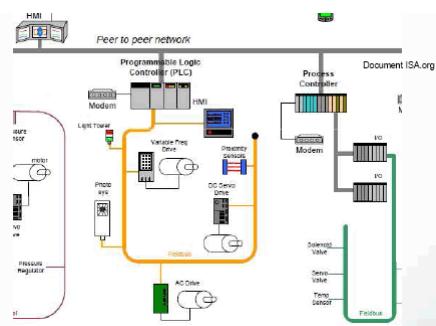


Bercy, Areva, Sony 2011 : Les APT

Gérard Peliks

17/ 47

Stuxnet : Attaques sur les SCADA (*)



(*) Supervisory Control And Data Acquisition

Gérard Peliks

18/ 47



Le ver Stuxnet : Les attaques sur les SCADA

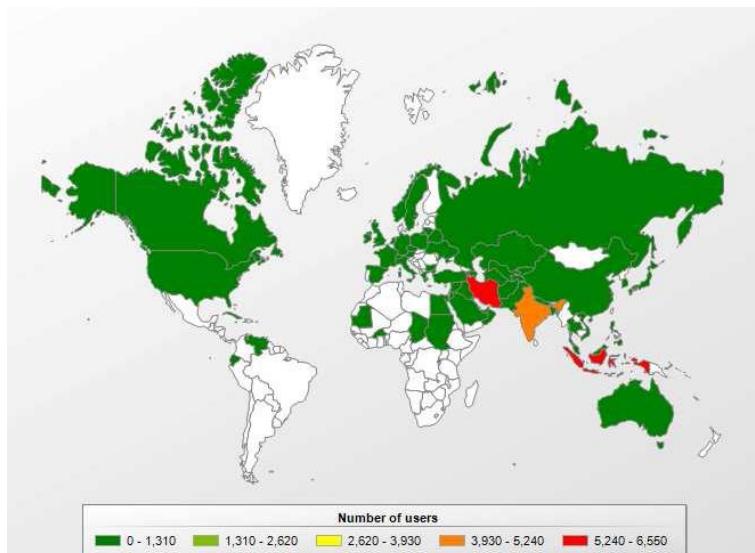
Une coopération USA / Israël (programme Olympic Games)

- 10 000 heures-hommes de développement
- 4000 fonctions différentes
- Exploitation de 4 "zero-day attacks" (= attaques sur des vulnérabilités inconnues)
- Logiciels signés par usurpation (les USA peuvent le faire...)
- Une erreur dans le sabotage : 100 000 ordinateurs infectés dans le monde

Gérard Peliks

19/ 47

Stuxnet, se répand hors de l'Iran



Gérard Peliks

20/ 47

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.

Gérard Peliks

21/ 47

Shodan, le moteur de recherche pour objets et systèmes connectés



<https://www.shodan.io/>

Gérard Peliks

22/ 47

Les attaques notables sur les organisations entre 2007 et 2011



Estonie 2007 : Les botnets



Iran 2010 : Le ver Stuxnet : Les SCADA



Bercy, Areva, Sony 2011 : **Les APT**

Gérard Peliks

23/ 47

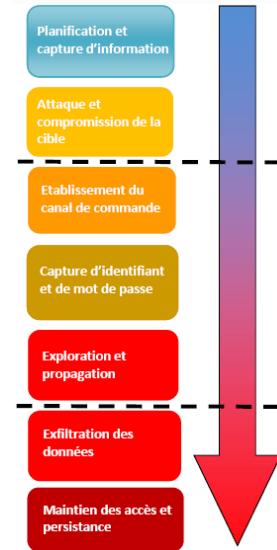
Les attaques par APT (advanced persistent threats)

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 !



Gérard Peliks

24/ 47

Quelques chiffres de perte suite à des attaques APT

- Areva :
 - plusieurs millions d'euros pour reconstruire le réseau ?
 - préjudice économique résultant du vol des informations ?
- Sony :
 - plusieurs centaines de millions de dollars ?
-

A



Gérard Peliks

29/ 47

Cyberguérilla, cybercombat de rue ou cyberguerre ? 2012...



Flame : Le **cyber espionnage** massif



Elysée : L'exfiltration et la destruction de données



Shamoon : La destruction du système de gestion

Gérard Peliks

28/ 47



Flame écoute vos conversations

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 logger et screen saver
- Il écoute les conversations des smartphones à proximité, par Bluetooth
- Il porte une boîte à outils de 20 Mo
- Il est écrit en un langage peu connu : Lua
- Il s'autodétruit sur commande à distance



Gérard Peliks

27/ 47

Cyberguérilla, cybercombat de rue ou cyberguerre ? 2012...



Flame : Le cyber espionnage massif



Elysée : **Exfiltration et destruction** de données

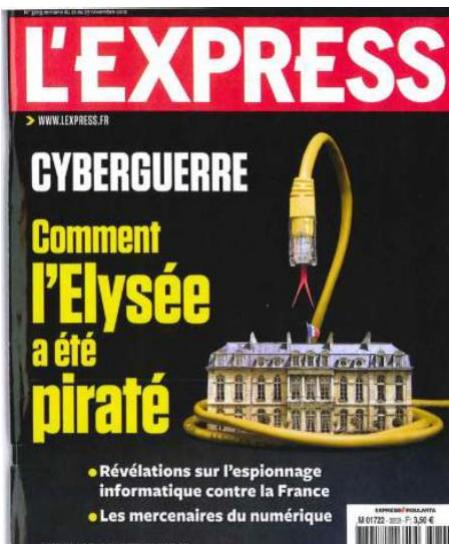


Shamoon : La destruction du système de gestion

Gérard Peliks

28/ 47

Gardez moi de mes amis, je m'occupe de mes ennemis...



Gérard Peliks

Source : L'express 20/11/2012

29/ 47

Cyberguérilla, cybercombat de rue ou cyberguerre ? 2012...



Flame : Le cyber espionnage massif



Elysée : **Exfiltration et destruction** de données 



Rapport Bockel ANSSI



LPM



Réserve Citoyenne de Cyberdéfense



Shamoon : La destruction du système de gestion

Gérard Peliks

30/ 47

Cyberguérilla, cybercombat de rue ou cyberguerre ? 2012...



Flame : Le cyber espionnage massif



Elysée : Exfiltration et destruction de données



Shamoon : La **destruction du système** de gestion



Gérard Peliks

31/ 47

Shamoon, la réponse de l'Iran

- Une attaque destructrice
- 30 000 ordinateurs détruits en octobre 2012
- 2 semaines pour rétablir les services informatiques
- Les installations gazières du Qatar aussi touchées



Source : TradeArabia

Gérard Peliks

32/ 47

2013, l'année du cyber espionnage

 **APT1** : Le rapport Mandiant accuse la Chine

 PRISM : L'espionnage par les Américains

Gérard Peliks

33/ 47

APT1 : L'espionnage par les Chinois



Chevilly-la-Rue

Shanghai, Unité 61398



The White House and Pentagon Deem Cyber-Attacks "An Act of War"



Source : Datanews



Last weeks New York Times bombshell article by David Sanger claimed that President Obama secretly ordered the cyber-attacks on the computer systems that run Iran's main nuclear enrichment facilities. The story tells of a significantly expanding American involvement in the sustained use of so called cyber-weapons against other nations using the "Stuxnet" software. The story has caused quite the uproar. But

Source : Forbes

Gérard Peliks

34/ 47

2013, l'année du cyber espionnage



- APT1 : L'espionnage par les Chinois
- Prism : L'espionnage **par les Américains**



Gérard Peliks

35/ 47

PRISM : L'espionnage par les Américains



Source : 01net



Source : Gizmodo

36/ 47

2014, vols d'identités numériques et grosses failles décelées

- Vols de données à caractère personnel
 - Target  Vol de données de 110 millions de clients
 - Orange  avril : 1.3 millions de e-mails clients et prospects volées
 - Cybervor  1,2 milliards de login / mots de passe hackés par des russes
 - JP Morgan  octobre : 80 millions de comptes utilisateurs
- Grosses failles décelées
 - Heart Bleed
 - Shell Shock

Gérard Peliks

37/ 47

Vos fichiers chiffrés par bitlocker



Cyberguerre et cyberdéfense

- Les dangers du cyberspace
- Des attaques sur les organisations
- Vivre avec les menaces, mais réagir**

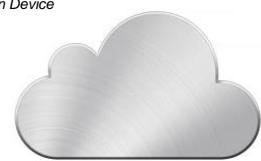


Gérard Peliks

39/ 47

Demain, entre la paranoïa et la naïveté, l'heure est aux sueurs froides...

- Smartphones, tablettes, BYOD ? *Bring Your Own Device*
- Cloud Computing ?
- HaaS ?
- APT ? *Advanced Persistent Threats*
- SCADA ? *Supervisory Control and Data Acquisition*
- Big Data ?
- Objets communicants ?
- Monnaies virtuelles
- HFT
-



... et l'heure est à la cybersécurité

Gérard Peliks

40/ 47

La sécurité des systèmes d'information

Qu'est ce que la sécurité de l'information ?

Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.



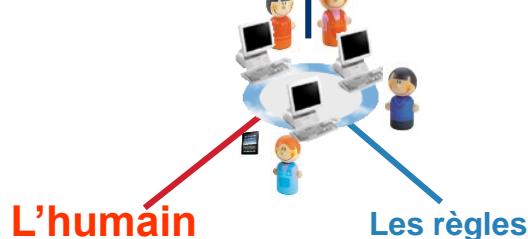
www.ssi.gouv.fr

Gérard Peliks

42/ 47

L'humain au centre de la sécurité

La technique



Gérard Peliks

43/ 47

L'humain au centre de la sécurité



Source : Hapsis

Gérard Peliks

44/ 47

Plate-forme PHAROS de l'OCLCTIC : www.internet-signalement.gouv.fr/

The screenshot shows the homepage of the internet-signalement.gouv.fr website. At the top, there is a logo for the Ministry of the Interior of France. Below the logo, the website's name "internet-signalement.gouv.fr" is displayed, followed by the subtitle "Portail officiel de signalement des contenus illicites de l'Internet". On the left side, there is a sidebar with links for "Signaler", "SE RENSEIGNER", "Questions et Réponses", "Conseils", "Conseils aux Jeunes", "Conseils aux Parents", "Internet Prudent", "Protéger son ordinateur", and "Liens Utiles". In the center, there is a large button labeled "Signaler >>". To the right, there is a section titled "ACTUALITÉS" with several news items. At the bottom, there is a summary of the platform's activity: "130 000 signalements par an, 400 par jour" and "38 000 signalements entre le 7 et le 30 janvier 2015".

130 000 signalements par an, 400 par jour

38 000 signalements entre le 7 et le 30 janvier 2015

Gérard Peliks

45/ 47

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

用瓦蓋 *Proverbe chinois*

Merci pour votre attention!

Des questions?



Gérard Peliks

Gérard Peliks
gerard.peliks@noos.fr



46/ 47