



Cyberguerre et cyberdéfense

23.03.2015

Gérard Peliks

LTC Réserve Citoyenne de Cyberdéfense DGGN

gerard.peliks@noos.fr

Expert Sécurité



Gérard Peliks

1 / 47

Cyberguerre et cyberdéfense

– **Les dangers du cyberspace**

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



Gérard Peliks

2 / 47

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

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 :



*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

Attaques sur les 3 couches du cyberspace

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 : l'Espresso.fr

Vélizy, mai 2011



Source : l'Espresso.fr



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

6/ 47

Attaques sur les 3 couches du cyberspace

Couche de la signification

Couche des logiciels

Couche des infrastructures

G rard Peliss

7/ 47

Faillles 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 s curit  informatique conseillent aux administrateurs de corriger une faille critique dans OpenSSL, une librairie Open Source de protocoles de chiffrement qui est utilis  par un grand nombre de sites web.

Plusieurs sp cialistes de la s curit  ont alert  les administrateurs des sites web afin qu'ils corrigent une faille importante dans OpenSSL. Cette vuln rabilit  est surnomm e « Heartbleed » et se trouve dans plusieurs versions d'OpenSSL, une biblioth que Open Source de chiffrement pour communiquer en

SSL (Secure Socket Layer) ou TLS (Transport Security Layer). La plupart des sites utilise ce syst me de chiffrement caract ris  par la pr sence dans les navigateurs du symbole du cadenas. La faille a  t  d couverte en d cembre 2011, mais elle vient d' tre corrig e par la version 1.0.1g d'OpenSSL publi e hier. Selon [un site sp cialement mis en place](#)

G rard Peliss

8/ 47

Attaques sur les 3 couches du cyberspace

Couche de la signification


Couche des logiciels

Couche des infrastructures

G rard Polks

9/ 47

Un r pertoire de Web d fac s : www.zone-h.org/archive

 zone-h unrestricted information						
Home News Events Archive Archive ★ Onhold Nobify Stats Register Login search...						
Time	Notifier	H	M	R	★ Domain	OS View
12:00	./Newbie4rt_ID				www.m-mehdzade.ir/Jamvan.php	Linux mirror
11:56	Kuroi/SH				jakprogramovat.cz/xmlrpc.php	Linux mirror
11:54	w4l3XzY3				teamche.com/vw.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	w4l3XzY3				simavis.nl/vw.htm	Linux mirror
11:51	Laakel En Person	H	M		cogipro.com	Linux mirror
11:50	w4l3XzY3				keepingfamiliestogether.net/vw.htm	Linux mirror
11:48	Laakel En Person	H			azulicreation.fr	Linux mirror
11:47	NeT.Defacer			R	projectcentral.astleygilbert.c...	Win 2000 mirror
11:47	ZeynnymouZ	H	M		perlengkapankostjogja.com	Linux mirror
11:46	NeT.Defacer			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		itsupportnelpfruit.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		produksisprejogja.com	Linux mirror
11:35	w4l3XzY3			R	interlaw.org/vw.htm	Linux mirror
11:32	w4l3XzY3				dvelopit.co.nz/vw.htm	Linux mirror
11:32	w4l3XzY3				ldag.net/vw.htm	Linux mirror
11:31	w4l3XzY3				gregmessel.com/vw.htm	Linux mirror
11:30	w4l3XzY3				eisenberg-allgaeu.de/vw.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 offensive 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

لا إله إلا الله



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

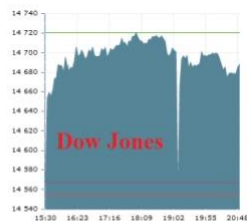
Reply Retweet Favorite More

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

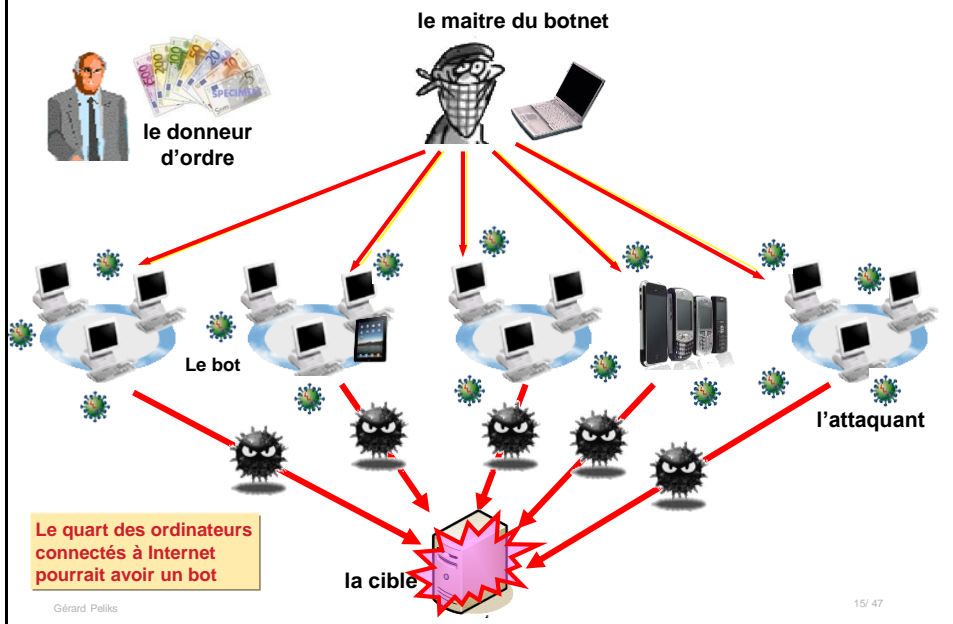


Bercy, Areva, Sony 2011 : Les APT

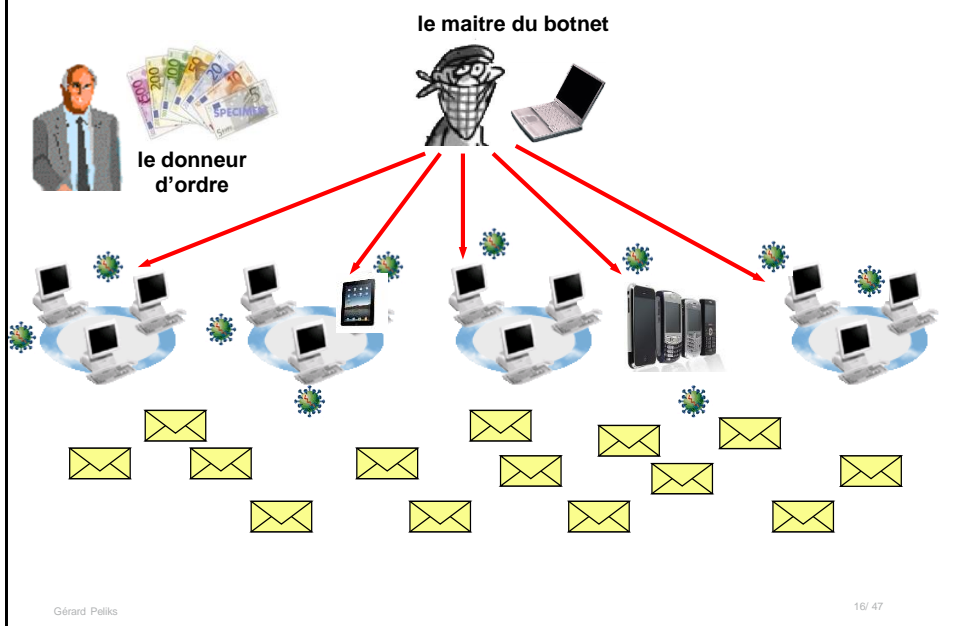
Gérard Peliks

14/ 47

Le botnet : attaques en dénis de services distribués



Le botnet pour spammer



Les attaques notables sur les organisations entre 2007 et 2011



Estonie 2007 : Les botnets

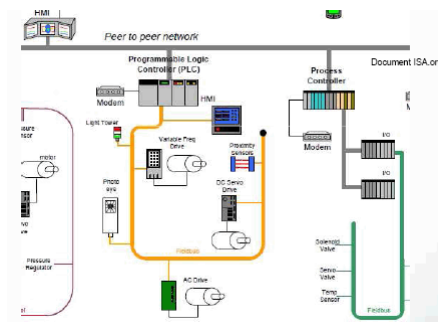


Iran 2010 : Le ver Stuxnet : Les SCADA



Bercy, Areva, Sony 2011 : Les APT

Stuxnet : Attaques sur les SCADA (*)



(*) Supervisory Control And Data Acquisition

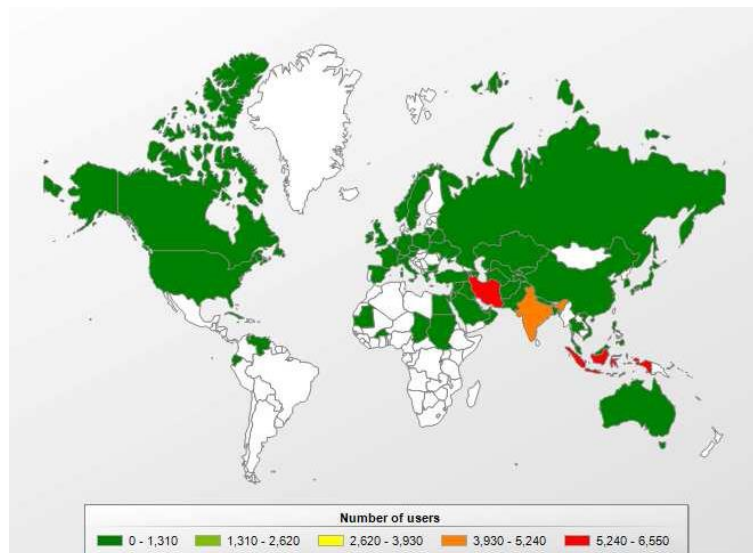


Le ver Stuxnet : Les attaques sur les SCADA

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

Stuxnet, se répand hors de l'Iran



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

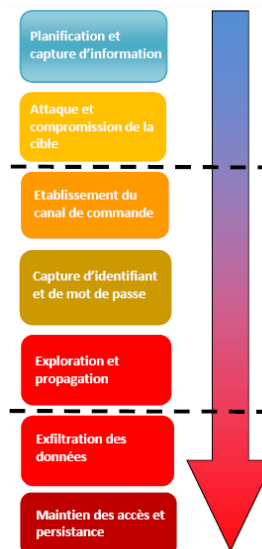
Les attaques par APT (advanced persistent threats)

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 ?
-



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



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



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

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

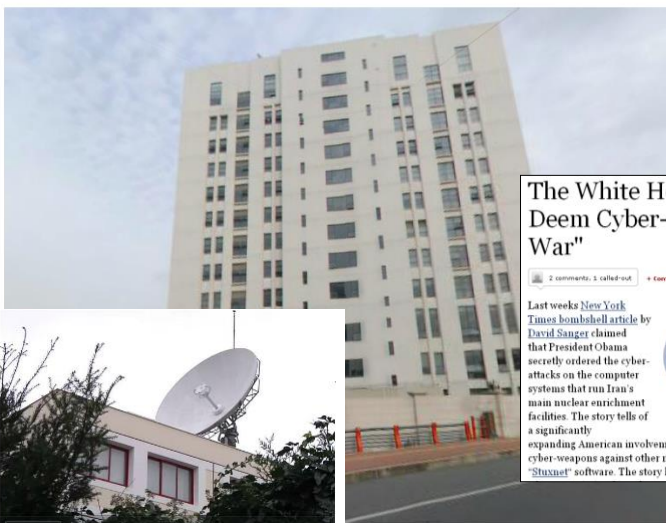


APT1 : Le rapport Mandiant accuse la Chine



PRISM : L'espionnage par les Américains

APT1 : L'espionnage par les Chinois



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

2 comments, 1 called-out • Comment Here • Follow Conversation

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. Eut

THE WHITE HOUSE
WASHINGTON

0
0
0
10
0
0

Source : Forbes

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

Vos fichiers chiffrés par bitlocker



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt the files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
12/1/2013
10:18 AM

Time left
42 : 48 : 44

Next >>

Cyberguerre et cybergdéfense

- 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

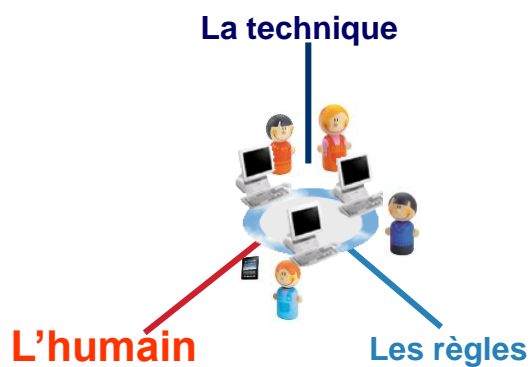
Qu'est ce que la sécurité de l'information ?

Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements 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

L'humain au centre de la sécurité



L'humain au centre de la sécurité



Gérard Peliks

44/ 47

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



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

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

Le nombre de signalements a augmenté en ... - 03/01/2013 Vous nous avez adressé 123 987 signalements en 201...

Le Point de Contact fête ses 15 ans de l... - 21/11/2013 Le Point de Contact (Association des Fournisseurs ...

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

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

用瓦盖 Proverbe chinois

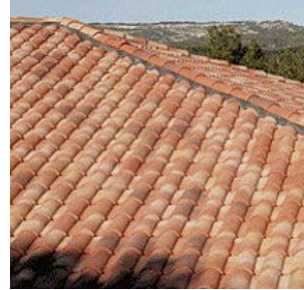
Merci pour votre attention!

Des questions?



Gérard Peliks

Gérard Peliks
gerard.peliks@noos.fr



46/ 47