Aspect Juridique
(Licence 2)
(MI)

Pr. Ghalem BELALEM
Université d'Oran1 Ahmed Ben Bella
Ghalem1dz@yahoo.fr

Chapitre 2 :

Menaces courantes à connaître!

Plan :

1. **Introduction**
2. **Attaque informatique par déni de service distribué (DDoS)**
3. **Chevaux de Troie**
4. **Détournement de domaine**
5. **Écoute électronique par réseau Wi-Fi**
6. **Hameçonnage**
7. **Logiciels espions**
8. **…**

Introduction

Rappel Chapitrel

Menaces sont très variées!!

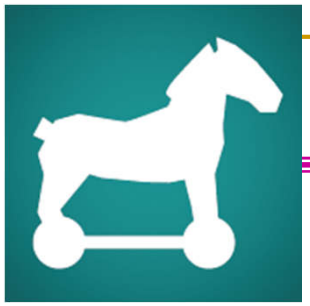
Sensibilisation!!

Attaque informatique par déni de service distribué (DDoS)

→→ ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser;
→→ visant à faire planter ou à rendre muette une machine en la **submergeant** de trafic inutile;

La grande majorité de ces attaques se font à partir de **plusieurs sources**, on parle alors d'attaque par déni de service distribuée (DDoS attack pour Distributed Denial of Service attack). Il peut s'agir de :

- l'inondation d'un réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- l'obstruction d'accès à un service pour une personne en particulier ;
- également le fait d'envoyer des milliards d'octets sur boîte internet.



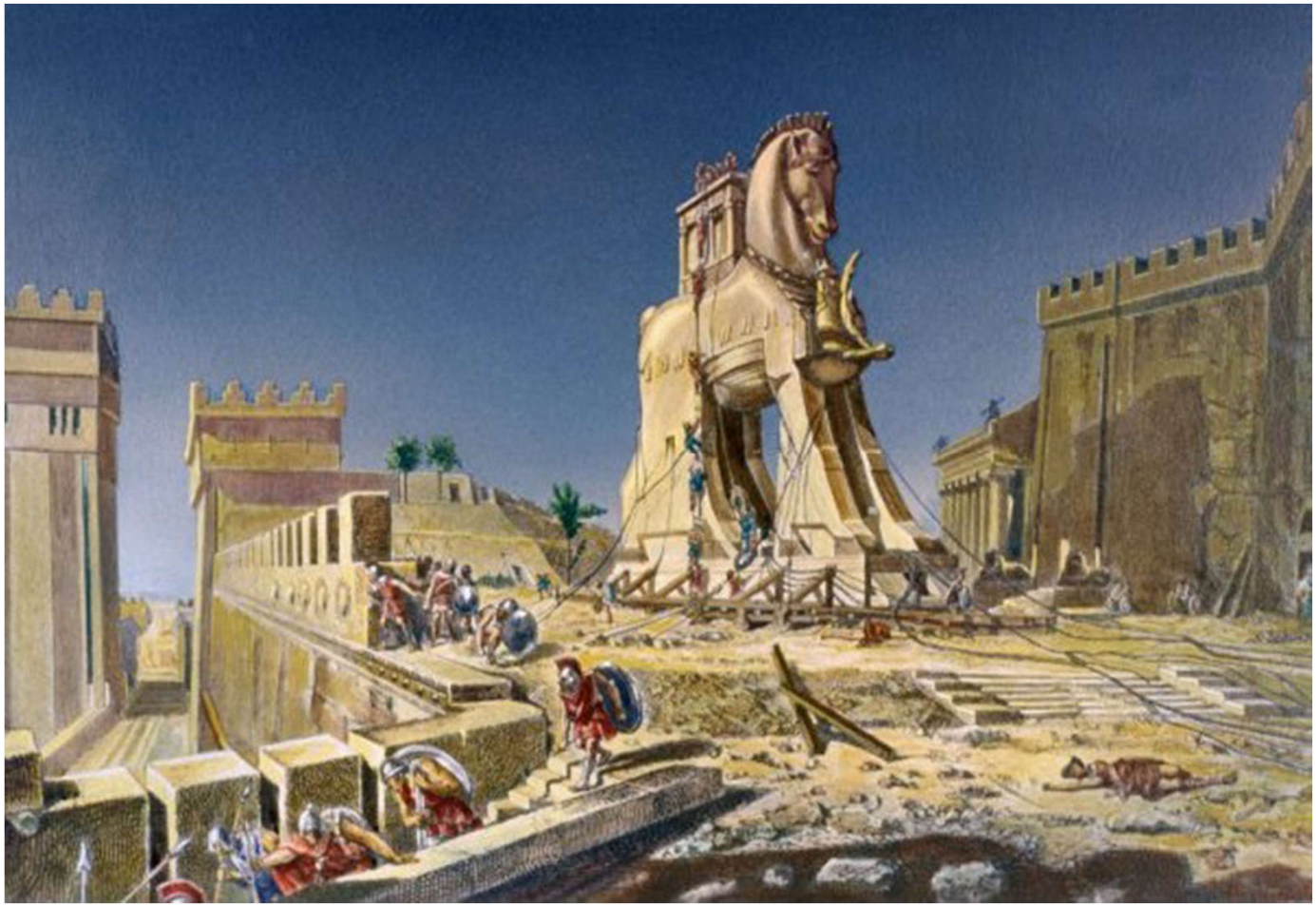
Chevaux de Troie

Un programme malveillant qui a l'apparence d'un logiciel légitime ou qui y est intégré.
Il s'agit d'un fichier exécutable qui s'installera et sera lancé automatiquement une fois téléchargé.

Quelles sont les conséquences?

- Les chevaux de Troie suppriment les fichiers.
- Ils utilisent votre ordinateur pour en pirater d'autres.
- Ils vous observent par l'intermédiaire de votre **caméra Web** *(Edward Snowden).*
- Ils enregistrent vos frappes de claviers (comme les numéros de carte de crédit entrés pour faire des achats en ligne);
- Ils enregistrent les noms d'utilisateurs, les mots de passe et d'autres informations personnelles.

Chevaux de Troie



Détournement de domaine

Le détournement de domaine est un type de fraude en ligne.

De quoi s'agit-il?

Un moyen de vous diriger vers un site malveillant et illégitime en redirigeant l'adresse URL légitime. Même si l'adresse URL est entrée correctement, il peut encore être redirigé vers un faux site.

Quelles sont les conséquences?

Le détournement de domaine a comme objectif de vous convaincre que le site est réel et légitime par **mystification** ou en ayant exactement la même apparence que le site actuel, et ce, dans les moindres détails. Par conséquent, vous pourriez entrer vos informations personnelles et, sans le savoir, les donner à quelqu'un de malintentionné.

Écoute électronique par réseau Wi-Fi

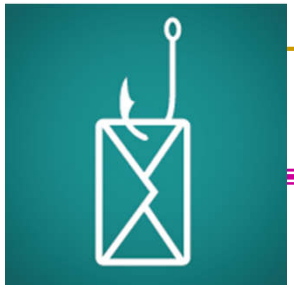
L'écoute électronique par réseau Wi-Fi est une autre méthode employée par les cybercriminels pour obtenir de l'information personnelle.

De quoi s'agit-il?

Écoute virtuelle de l'information qui est partagée sur un réseau Wi-Fi non sécurisé (non chiffré).

Quelles sont les conséquences?

- Grâce à l'écoute électronique par réseau Wi-Fi, il est possible accéder à votre ordinateur grâce à l'équipement adéquat.
- Les cybercriminels volent vos informations personnelles, y compris vos renseignements pour procéder à une ouverture de session et les mots de passe.



Hameçonnage

Hameçonnage : Utilisée par les cybercriminels,

De quoi s'agit-il?

De faux courriels, messages texte et sites Web conçus pour avoir exactement la même apparence que ceux des **entreprises réelles** ou qui semblent être envoyé par de vraies entreprises.

Les criminels les envoient pour vous voler votre information personnelle et financière (« mystification »).

Logiciels espions

Les logiciels espions et publicitaires sont souvent utilisés par des tiers pour s'infiltrer dans un ordinateur.

De quoi s'agit-il?

Ces logiciels se présentent souvent sous la forme d'un téléchargement «gratuit» et sont automatiquement installés avec ou sans votre autorisation. Il est difficile de les supprimer complètement et ils infecteront possiblement votre ordinateur avec de nouveaux virus.

Mystification

Cette technique est souvent utilisée conjointement avec l'hameçonnage dans le but de vous voler vos informations.

De quoi s'agit-il?

La création d'un faux site web ou d'une fausse adresse courriel pour qu'il ou qu'elle semble provenir d'une source légitime. Une adresse courriel peut même comprendre votre propre nom ou celui d'une de vos connaissances. Il est ainsi difficile de savoir si l'expéditeur est bien réel.

Programmes malveillants

Les programmes malveillants sont l'une des façons les plus courantes d'infiltrer un ordinateur ou de l'endommager.

De quoi s'agit-il?

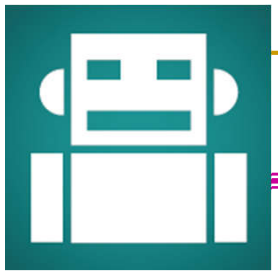
Un programme malveillant qui infecte votre ordinateur comme les virus informatiques, les chevaux de Troie, les logiciels espions et publicitaires.

Rançongiciel

Il existe deux types communs de rançongiciel :

• le rançongiciel avec verrouillage de l'écran : il affiche une image qui vous empêche d'accéder à votre ordinateur;
• le rançongiciel avec chiffrement : il chiffre les fichiers sur le lecteur de disque dur de votre système, et parfois ceux qui sont stockés dans les lecteurs réseau partagés, les dispositifs de stockage USB, les disques durs externes et même certains systèmes de stockage en nuage, vous empêchant de les ouvrir.

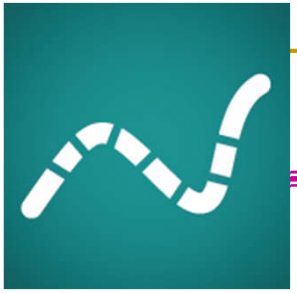
Le rançongiciel affichera un avis indiquant que vos données ou votre ordinateur ont été verrouillés et exigeant que vous effectuiez un paiement afin de récupérer l'accès.



Réseaux de zombies

Si vous n'avez jamais entendu parler de **réseaux de zombies**, c'est probablement, car ils passent souvent inaperçus.

De quoi s'agit-il?
Un ensemble de **robots Web**, ou de robots, qui créent une armée d'ordinateurs infectés (appelés « zombies ») et qui sont contrôlés à distance par l'initiateur. Votre ordinateur en fait peut-être partie sans que vous ne le sachiez.



Vers informatiques

Les vers informatiques sont une menace courante pour les ordinateurs et pour l'utilisation d'Internet dans son ensemble.

De quoi s'agit-il?

Un ver informatique, contrairement à un virus, travaille seul sans avoir à se joindre à des fichiers ou des programmes. Il vit dans la mémoire de votre ordinateur, n'endommage pas ou ne modifie pas le disque dur et se propage en s'envoyant lui-même à d'autres ordinateurs en réseau, que ce soit au sein d'une entreprise ou d'Internet.

Virus

Quelles sont les conséquences?

• Les virus envoient des pourriels.

• Ils fournissent aux criminels l'accès à votre ordinateur et à votre liste de contact.

• Accès à vos informations personnelles sur votre ordinateur, par exemple mots de passe.

• Ils piratent votre navigateur Internet.

• Ils désactivent vos paramètres de sécurité.

• Ils affichent des publicités indésirables.

Lorsqu'un programme est exécuté, le virus qui y est attaché peut s'infiltrer dans le disque dur, mais aussi dans les clés USB et les disques durs externes.

Virus

Comment saurez-vous si votre ordinateur a été infecté?

Quels sont les points à vérifier?

• L'ordinateur prend plus de temps à démarrer, il redémarre par lui-même ou ne démarre simplement pas.
• L'ordinateur prend beaucoup de temps à lancer un programme.
• Les fichiers et les données ont disparu.
• Le système et les programmes tombent constamment en panne.
• La page d'accueil installée n'est plus la même (à noter que cela pourrait être causé par un logiciel publicitaire qui a été installé sur l'ordinateur).
• Les pages Web prennent du temps à se charger.
• L'écran de l'ordinateur semble déformé.

Si vous soupçonnez un problème, assurez-vous que votre logiciel de sécurité soit à jour et lancez-le pour vérifier si un virus a infecté votre système. Si rien n'a été trouvé, ou si vous n'êtes pas certain de ce qu'il faut faire, demandez de l'aide technique.

Conclusion

Il est irréaliste d'attendre une sécurité à 100%!!. Surtout s'ils sont ouverts sur l'extérieur. →→ **Protection et Prudence**

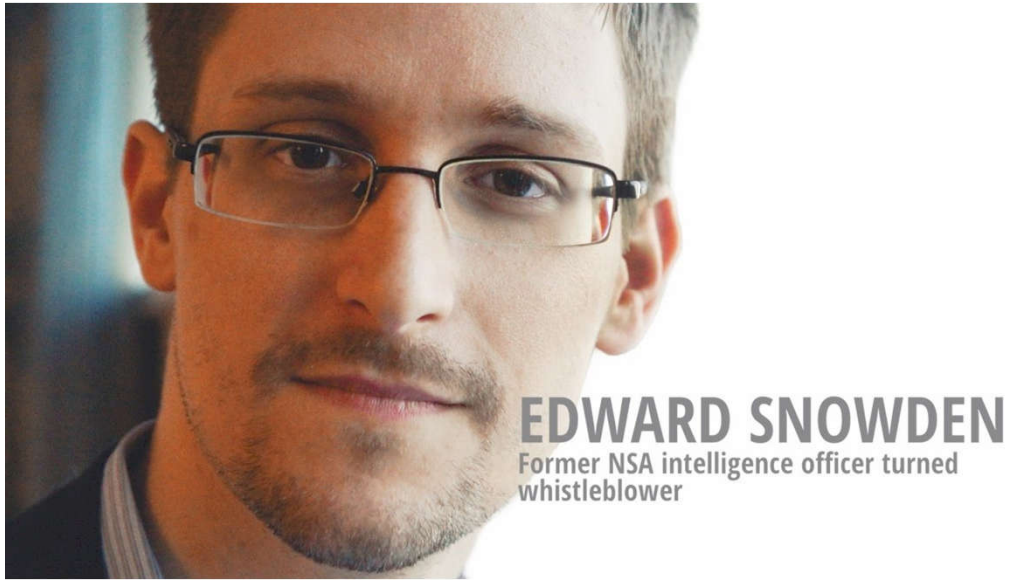
Recommandations:

1- Ne pas répondre aux e-mails indésirables ou spontanés.
2- Ne rien acheter qui a été recommandé par un e-mail indésirable.
3- Ne jamais cliquer sur les liens d'e-mails pressants.
4- Ne jamais répondre à un e-mail demandant des informations personnelles ou confidentielles.
5- Savoir que sa banque ne demandera jamais d'informations personnelles par e-mail.
6- Utiliser des mots de passe compliqués (mélanges de chiffres et de lettres, de minuscules et de majuscules).
7- Utiliser des mots de passe différents pour chacun de ses comptes.
8- Ne jamais enregistrer ses mots de passe sur des ordinateurs étrangers.
9- Ne pas installer de programmes suggérés.
10- Ne pas utiliser n'importe quel USB tombant sous la main.
11- Verrouiller l'accès à son ordinateur.
12- Protéger l'accès à son smartphone et le configurer pour qu'il s'autoverrouille.
13- Considérer comme "spam" toutes les demandes d'inconnus sur les réseaux sociaux.
14- Se méfier des bannières sur les sites web clamant que l'on est "le millionième visiteur" ou le vainqueur d'un "prix incroyable".
15- Utiliser un antivirus.

Merci pour votre attention

Vos Questions !!!

Discussions …



Edward Joseph Snowden, né le 21 juin 1983 à Elizabeth City, Caroline du Nord, est un lanceur d'alerte américain. Informaticien, ancien employé de la **Central Intelligence Agency** et de la **National Security Agency**, il a révélé les détails de plusieurs **programmes de surveillance** de masse américains et britanniques.

Date et lieu de naissance : 21 juin 1983 (Âge: 35 ans), Elizabeth City, Caroline du Nord, États-Unis
Compagne : Lindsay Mills
Pays de résidence : **Russie** (asile temporaire depuis 2013)
Livres : Everything You Know about the Constitution is Wrong, Supernerds: Conversations with Heroes

Télés, **iPhone**, **voitures**: Wikileaks révèle un programme de piratage de la CIA

Le site fondé par Julian Assange a publié près de 9000 documents qui visent à prouver que l'agence de renseignement a élaboré plus d'un **millier de programmes malveillants** pouvant infiltrer et prendre le contrôle d'appareils électroniques.

Vous pouvez lire aussi …

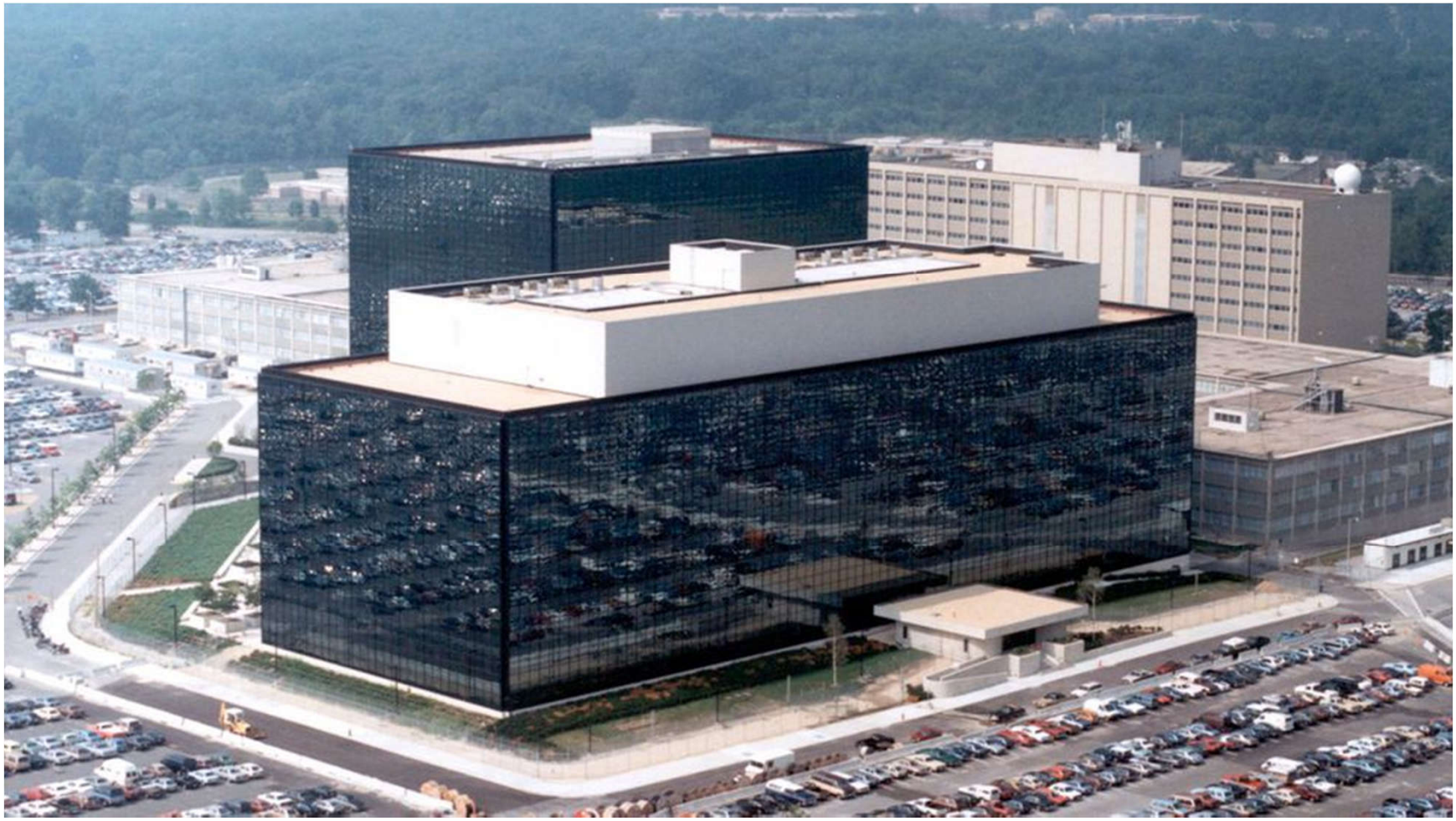
- Quatre jours à l'écoute de l'Europe pour George Bush

(Par Jean Quatremer et Véronique Soulé — 23 février 2005)

- La NSA, l'Agence de sécurité nationale américaine aurait produit 70,3 millions enregistrements à partir des données téléphoniques de Français entre le 10 décembre 2012 et le 8 janvier 2013.
Jean-Marc Ayrault s'est dit « profondément choqué », et a rajouté que « des initiatives s'imposent et elles seront prises ».

- Les services allemands du BND sont accusés d'avoir écouté la Turquie depuis plusieurs années. Des révélations gênantes alors que Berlin dénonçait il y encore quelques semaines l'espionnage «entre amis».

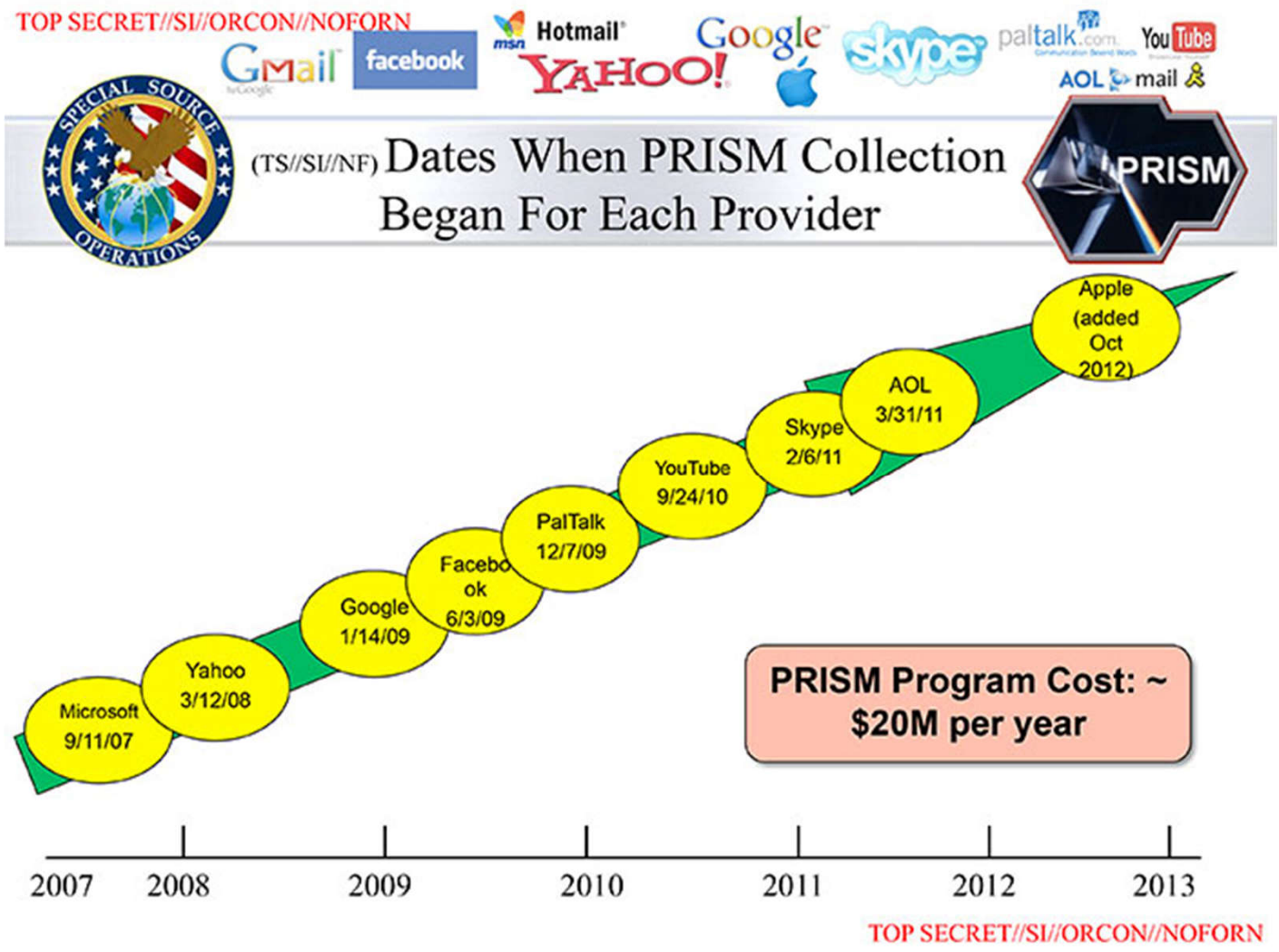
- DOSSIER: LA FRANCE ET L'ALLEMAGNE SUR ÉCOUTE
Trois chefs d'État français, des ministres, des hauts fonctionnaires, des parlementaires et des diplomates ont été espionnés pendant près d'une décennie par les services secrets américains.
- …



Harold Thomas Martin III travaillait comme sous-traitant à l'agence de renseignements NSA. Il est soupçonné d'avoir volé des codes informatiques **ultra-secrets** utilisés pour pirater des réseaux de gouvernements étrangers.
(Par Victor Garcia avec AFP., publié le 05/10/2016)

PRISM, également appelé **US-984XN**, est un programme américain de surveillance électronique par la collecte de renseignements à partir d'Internet et d'autres fournisseurs de services électroniques. Ce programme classé, relevant de la National Security Agency(NSA), prévoit le ciblage de personnes vivant hors des États-Unis.

PRISM est supervisé par la United States Foreign Intelligence Surveillance Court (FISC) conformément au *FISA Amendments Act of 2008* (FISA)


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
2013
TOP SECRET//SI//ORCON//NOFORN