Snowden : ce qui est maintenant avéré !

…et qui est concerné ?

Gilles Defer

gilles.defer@abiosconsulting.com

Sources des informations

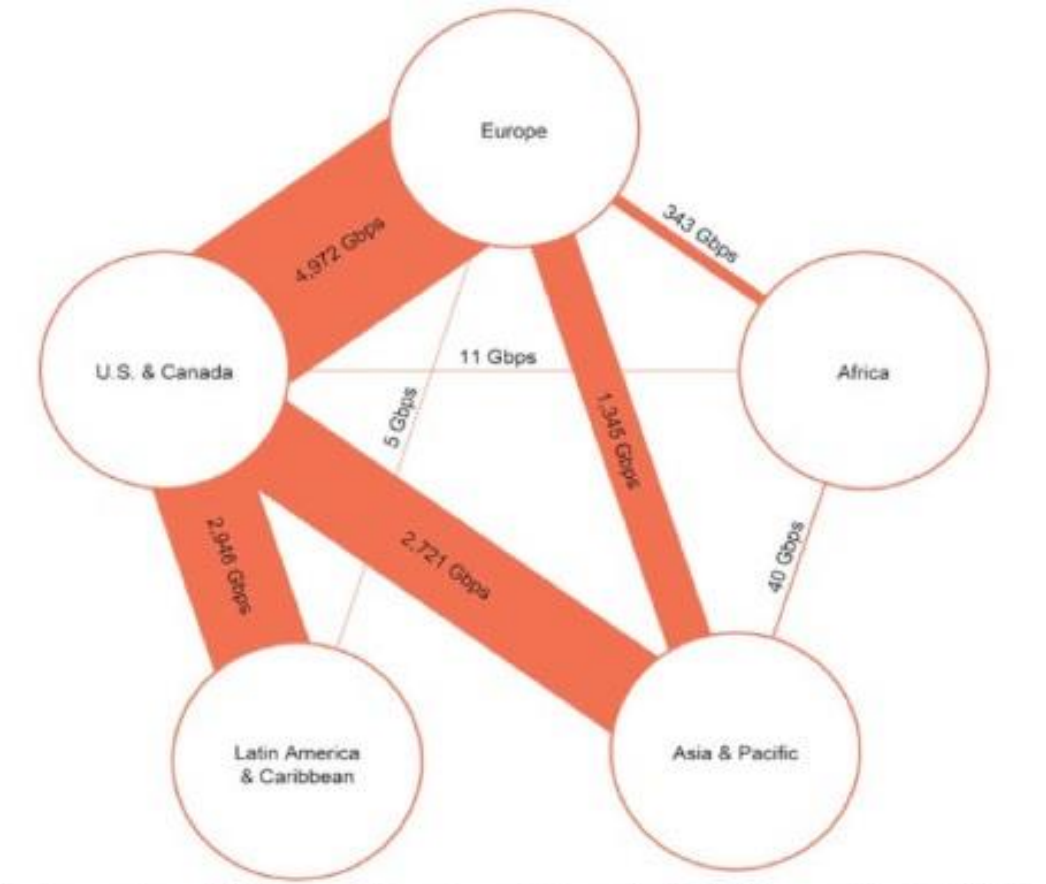
Toutes les informations de cette présentation sont publiquement disponibles sur internet

- **E. Snowden**, Glenn Greenwald, David Miranda, Laura Poitras, Bruce Schneier sont les principales sources;
- Journaux à grands tirage : The Guardian, The New York Times, Le Monde, Der Spiegel, The Independant;
- Mais également quelques ressources en ligne : cryptome, reflets, Owni…
- Les détails techniques sont retirés des informations divulguées au grand public sans en entacher la compréhension.

=> Plus importante fuite de données de haut niveau de l'histoire des États-Unis

Introduction

La plupart des communications mondiales passent par les US



International Internet Regional Bandwidth Capacity in 2011
Source: Telegeography Research

Espionnage sur le territoire US : de quel droit ?

- Transit Authority : Surveillance des communications transitant par les US;
- Foreign Intelligence Surveillance Act (FISA sections 702 et 715) : acquisition d'informations concernant des citoyens non-US. Bascule de cibles spécifiques sur demandes à la création d'une gigantesque base de données pouvant être interrogée de manière spécifique…
- FISA Amendment Act 2008 (FAA) : surveillance sur sol US de cibles raisonnablement présumées étrangères. Cet amendement n'oblige plus le gouvernement à identifier formellement les cibles;

=> Pas de surveillance de citoyens US "intentionnelle"

Espionnage sur le territoire US : de quel droit ?

- FISAA : toute société Américaine ou capitaux américains sont tenus de fournir les données. "En d'autres termes, quand bien même une donnée serait traitée formellement à l'intérieur de l'UE, dès lors qu'elle migrerait par l'intermédiaire des prestataires américains, elle serait soumise à la captation et à la surveillance des Etats-Unis. Ainsi une société Américaine qui aurait remporté un marché de services informatiques en France devrait, si elle était destinataire d'injonction sur le fondement de FISAA, communiquer à l'administration Américaine les données qu'elle détient";

- Non respect de l'accord d'entraide judiciaire depuis 2010 : véritable pillage des données européennes;

=> Les non-US sont dépouillés de tout droit au respect de leur vie privée et de la protection de leurs données;

Collecte sur le territoire des US

2 moyens de collecte :

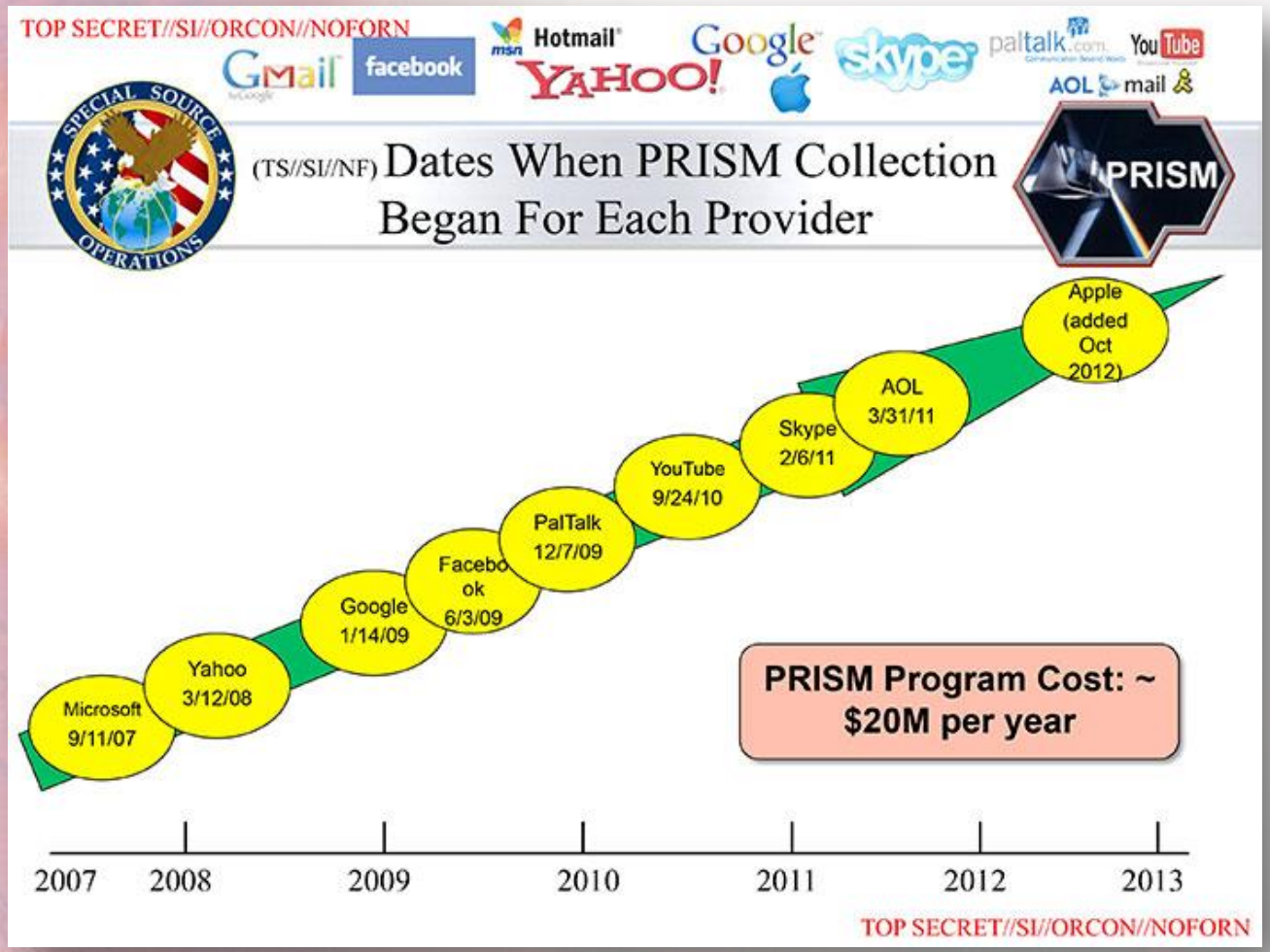
- PRISM directement sur les serveurs
- Upstream par interception des moyens de communications

Contenus interceptés :

- E-mails
- Chats voix et vidéo (retranscrits)
- Photos
- Données enregistrées et transférées
- VoIP
- Vidéo/audio conférences
- Notifications temps réel
- Demandes spécifiques

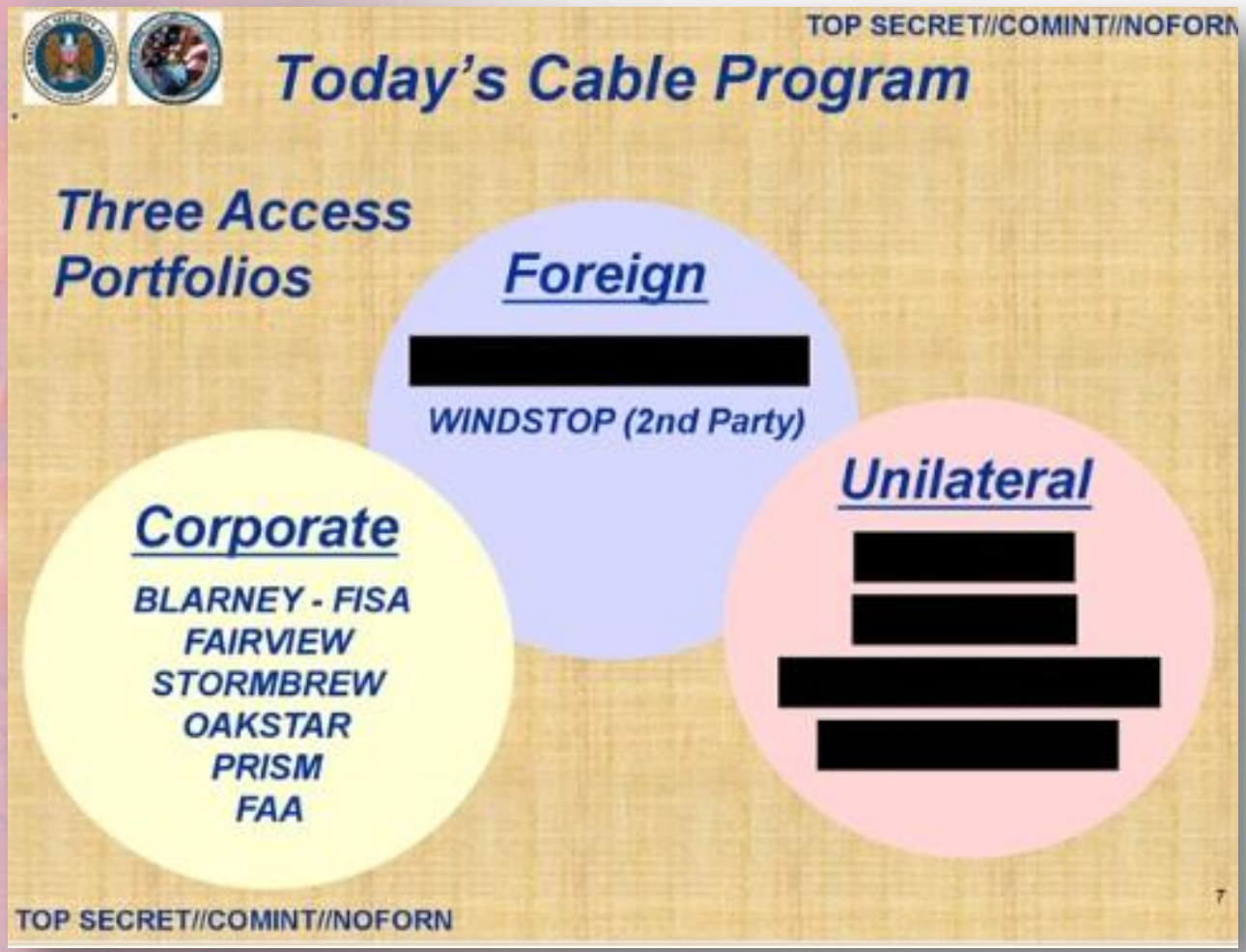
Programme PRISM :

participation active des grands groupes américains



- Accès direct aux serveurs par backdoors
- Des 100ènes de millions de dollars sont versés en compensation pour couvrir les coûts des procédures de surveillance
- Accès à l'ensemble des informations : emails, fichiers, vidéo, notifications en temps réel, etc…

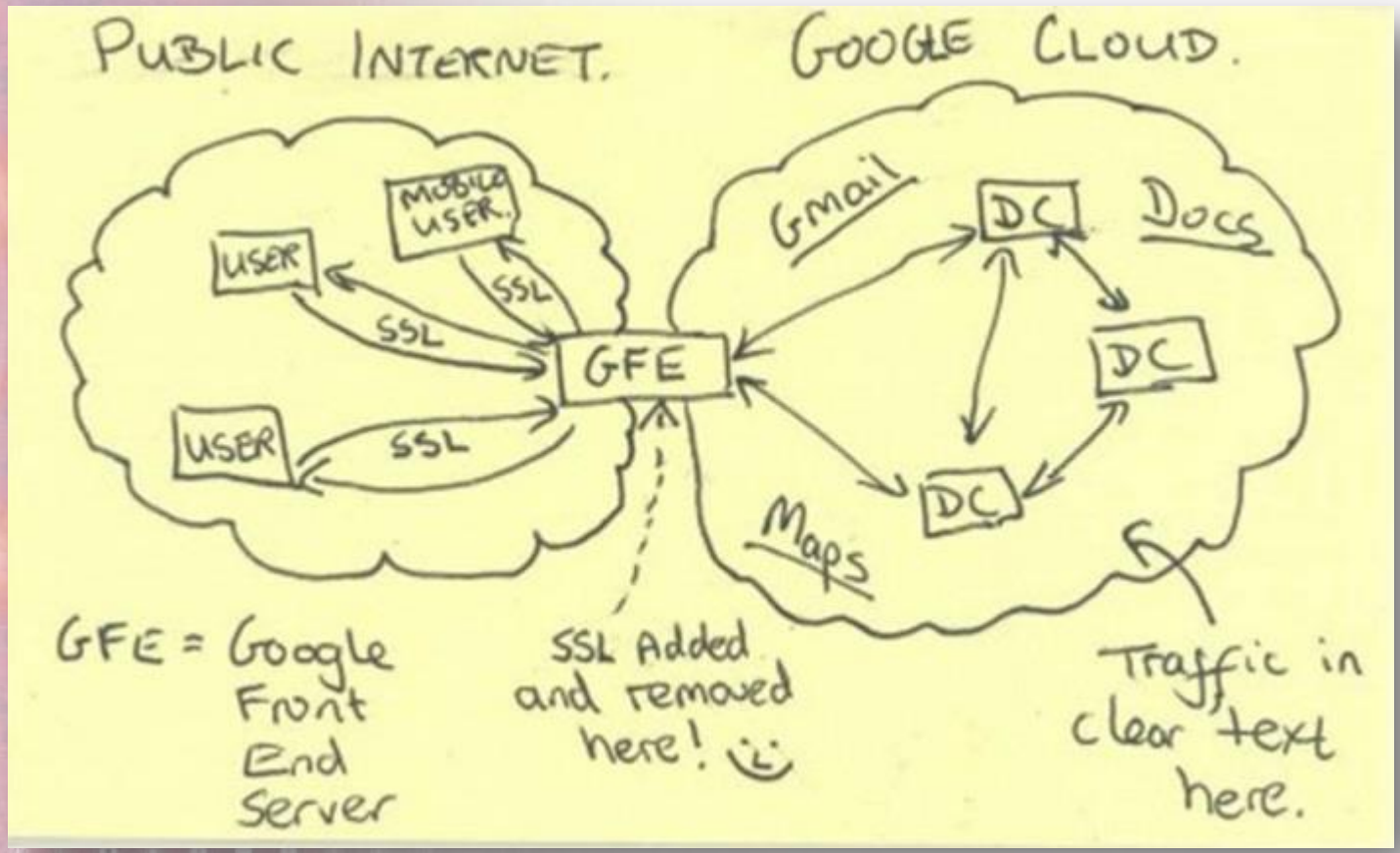
Collecte UPSTREAM



Special Source Operation

"Partenariats" avec le secteur privé pour se brancher sur les câbles

Programme Muscular



Partenariat
NSA + GCHQ

A l'étranger ?

- Ambassades et gouvernements étrangers surveillés par le **Special Collection Service** : 80 sites dans le monde dont 19 en Europe (Paris…);
- Satellites étrangers;
- 35 leaders mondiaux sous surveillance;
- "*Infecter les ordinateurs ou téléphones d'un individu reste encore la meilleure façon d'en apprendre sur celui qui est installé derrière le clavier*"

Compromission des moyens de communication :

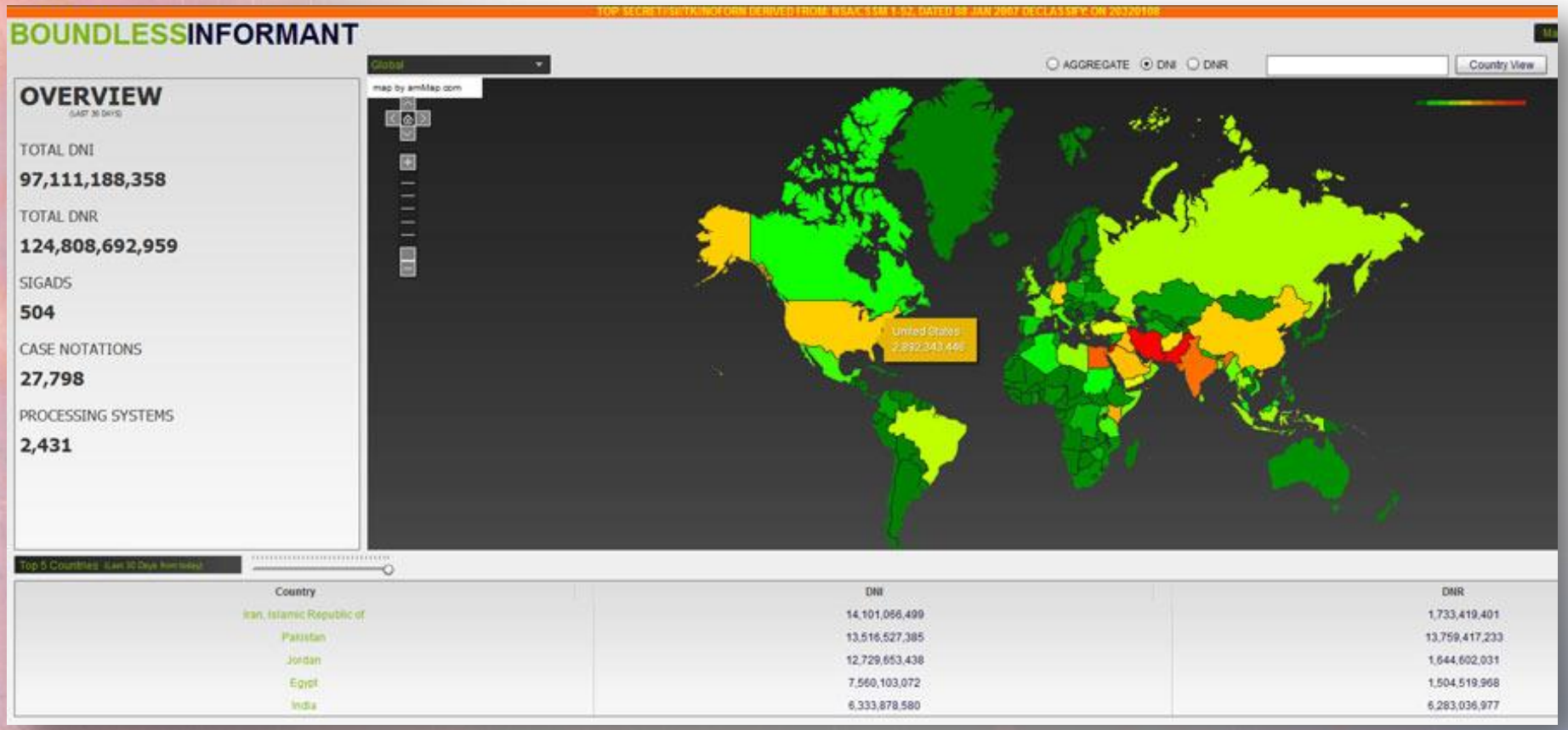
- Via les accords avec Apple, Google et Microsoft, les services secrets Américains ont accès à la quasi-totalité des téléphones mobiles en circulation dans le monde (accès aux contacts, SMS, Notes, position GPS et au moins 38 autres données)…y compris BlackBerry;

- **Evilolive :** sur la base du "volontariat" des opérateurs AT&T (Blarney depuis 1970, 65.96 millions de dollars) et Verizon. Quasi-totalité des métadonnées des communications internet et téléphoniques US et 75 % du trafic internet mondial. Sondes installées aux endroits stratégiques. ShellTrumpet en complément, 1 000 milliards de données collectées en 5 ans;

- **Team telecom :** s'assurer que le maximum de câbles télécom restent sous propriété ou influence Américaine. A fait capoter le rachat de Global Crossing par Hong Kong, importantes concessions faites par la compagnie acheteuse Singapourienne;

Tableau de bord Boundless Informant Mars 2013

Le programme Boundless Informant permet de visualiser la quantité d'informations recueillies :



Statistiques Boundless Informant

1. L'Iran (14 milliards de données collectées) 
2. Le Pakistan (13,5) 
3. La Jordanie (12,7) 
4. L'Égypte (7,6) 
5. L'Inde (6,3) 

- Origine de collecte : Câbles = 61 %, RF = 27 %, Protected = 6 %, Endpoint = 6 %

Compromission des outils cryptographiques
Le cas des technologies propriétaires/centralisées

- Échec du Clipper chip dans les années 1990;
- Plus de 250 millions de dollars par an pour rendre les produits commerciaux exploitables y compris les puces cryptographiques : CMEA (téléphones mobiles), 4G…
- Les éditeurs fournissent leurs clés … ou elles sont volées…
- Key provision service : base de données des clés des produits commerciaux;
- Influence les stratégies, standards et spécifications des technologies commerciales.

La NSA adore les technologies propriétaires/centralisées

Compromission des outils cryptographiques : Le cas des technologies libres

- Bruce Schneier à propos d'IPSEC = "*We do not believe that it will ever result in a secure operational system. It is far too complex, and the complexity has lead to a large number of ambiguities, contradictions, inefficiencies, and weaknesses. We have found serious security weaknesses in all major components of Ipsec. We strongly discourage the use of IPsec in its current form for protection of any kind of valuable information*";

- SSL + VPN (bullrun) = "enormous breakthrough". Décryptage complet et à la volée du SSL et VPN et non plus de manière unitaire (Bye bye HTTPS…);

- La NSA a "très largement participée" au développement de SELinux : qu'en est-il des distributions et du noyau ? Réponse de Linus : "Noooooooon" en hochant oui de la tête :-) Il est citoyens Américain depuis 3 ans et maintenant soumis aux même lois que les grands groupes…

Compromission des outils cryptographiques : Le cas des technologies libres

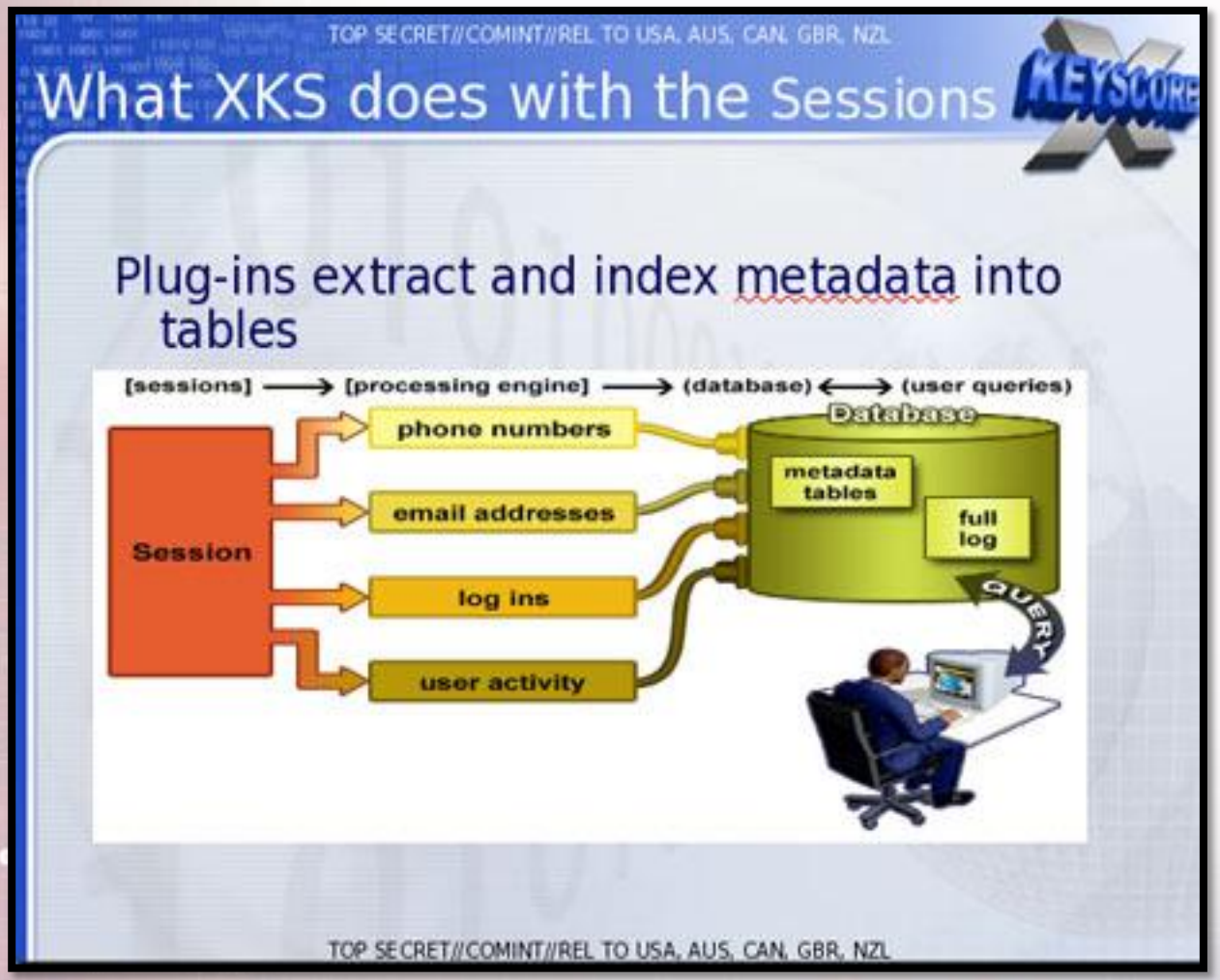
Le fonctionnement décentralisé et public de l'Opensource rend les tentatives directes difficiles

Utilisation de moyens plus "sournois"…

Pour quoi faire ? XKeyScore !

- Tous ces outils alimentent XKeyScore : agrégation du renseignement qualifié de "google pour espions". 700 serveurs sur 150 sites;
- Conservation de 3 jours à plusieurs années, croisement de bases de données;
- Réalisation d'un diagramme des connexions d'un individu y compris nullement suspect au moment de la collecte (toiles de connexion, graphes sociaux);
- 850 000 employés top secret ont accès mais sans justification particulière : un vague prétexte suffit;
- Recherche par nom, email, etc…
- Marina : utilisation de l'historique de navigation pour construire des résumés et profils des cibles.

Pour quoi faire ? XKeyScore !



Exemple d'une carte sociale

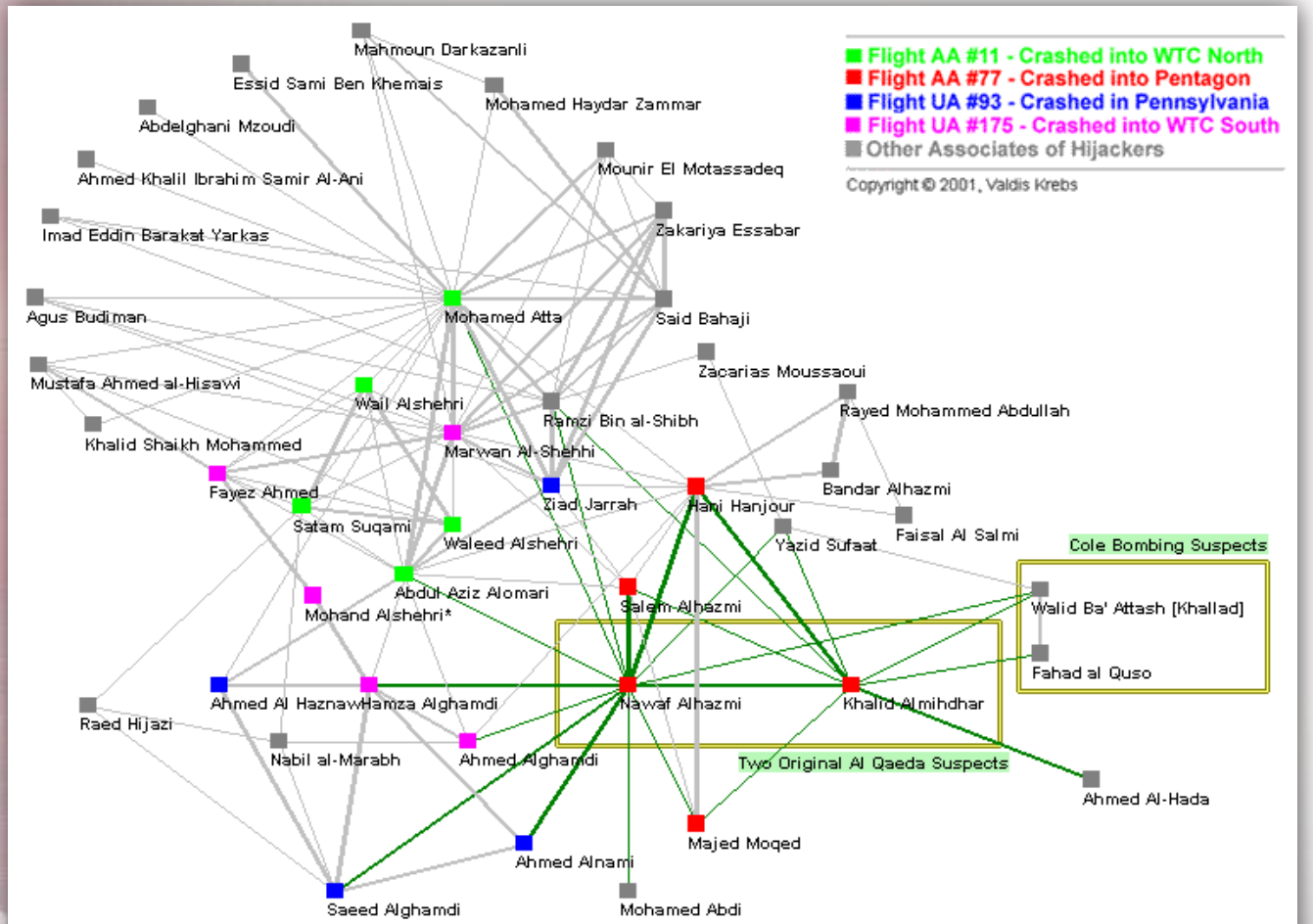


Figure 3 - All Nodes within 2 steps / degrees of original suspects

Attaques offensives : Tailored Access Operation

Joyaux de la couronne de la NSA : attaques personnalisées de cibles spécifiques

Quantum :

- Emplacements stratégiques sur Internet
- Man on the side attack et race condition
- Packet inspection et redirection vers FoxAcid

FoxAcid :

- Exploit orchestrator
- Des URLs uniques déclenchent l'exploitation de "charges" spécifiques selon les cibles
- Obfuscation et évitement des systèmes de protection hôtes (malicious software detection)
- Librairies d'exploits selon les systèmes, classification des exploits par valeur
- Remontée des données sur FrugalShot

Attaques offensives

Exemple d'attaques types :

1. Identification des employés : maintenance ou sécurité privilégiés
2. Sélection des cibles et renseignements
3. Création des charges dédiées
4. Interception des cibles avec Quantum et injection des charges avec FoxAcid (surf vers LinkedIn par exemple)
5. Prise de contrôle puis pillage

Réussites avec Firefox à 100 % avec contrôle total

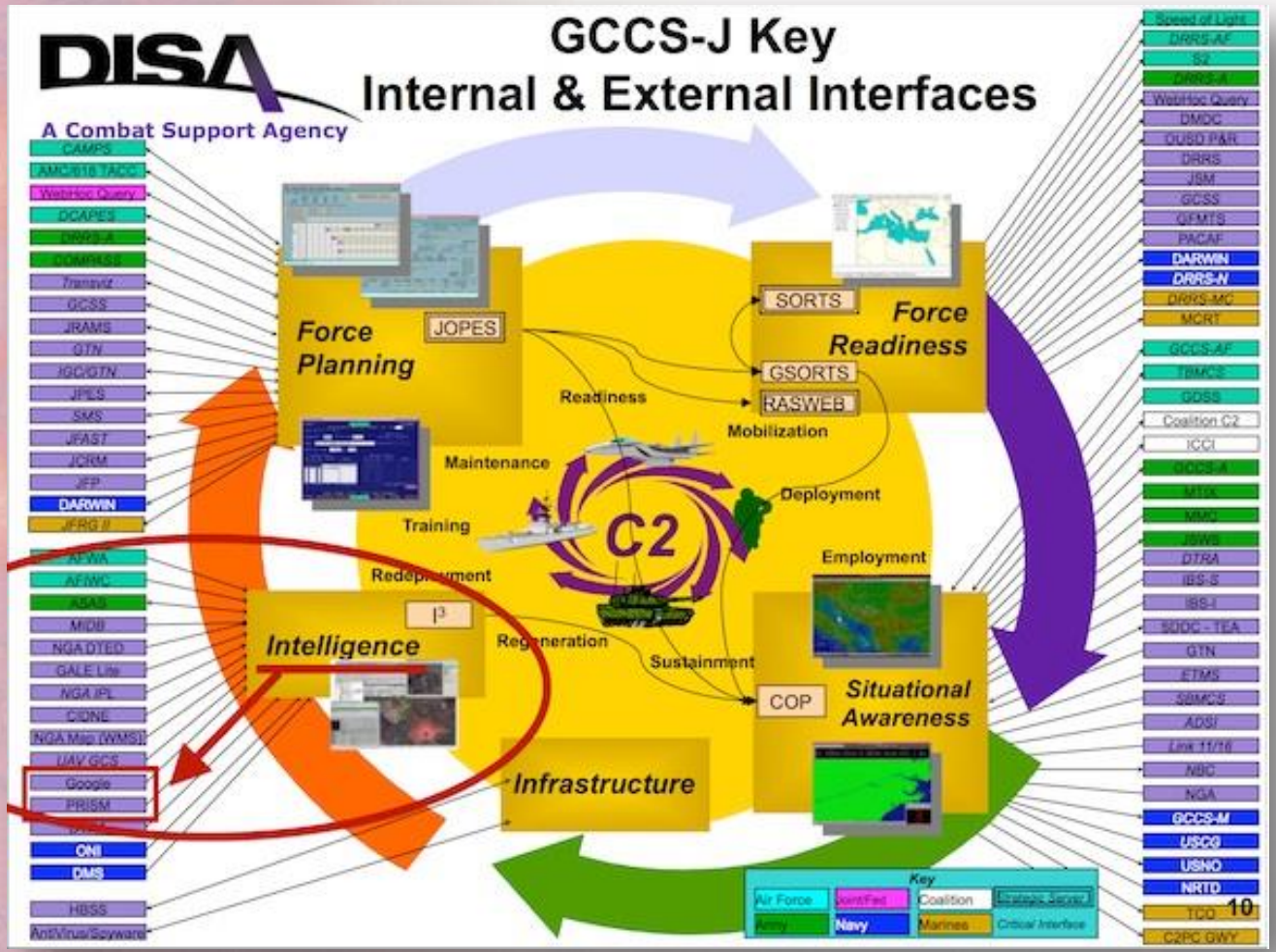
Quelques exemples : Belgacom (opération socialist), OPEC, TOR…

Attaques offensives

- Programme Génie (Highlands) : plus de **600 millions de dollars**, pose d'implants espions à distance dans les ordinateurs, routeurs, firewalls… > 1 000 000 d'implants déployés;
- "*Users bad at patching Windows… horrible at patching routers…*" : pas de mises à jour ni de tests d'intégrité ou d'anti-virus sur les routeurs, switchs, etc…;
- Un ver développé par Mike Lynn aurait permis de se répandre et crasher un réseau complet.

Defense Information Systems Agency

Information superiority



DISA provides information sharing capabilities

Information superiority is the capability to collect, process and disseminate an uninterruptible flow of information while exploiting and denying an adversary's ability to do the same.

Participation "active" des partenaires

- Israël / unité 200 : échanges de données et métadonnées de manière routinière et complète y compris d'Américains. Seules les communications gouvernementales sont exclues;

- Brésil / SilverZephyr : Espionnage des communications transitant par le Brésil. Partenariats contraints avec opérateurs télécom locaux suite à des pressions commerciales. Espionnage de la présidence à leur insu;

- Mexique / FlatLiquid : accord depuis 2007 pour la collecte de métadonnées et de données ciblées. Espionnage de la présidence à leur insu.

Participation active des partenaires Européens :

Angleterre / GCHQ (Government Communication Headquarters)

- Programme TEMPORA : partenariats contraints avec 7 compagnies privées (British Telecom, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel et Interoute);
- Accès direct aux câbles d'acheminement du trafic internet mondial (fibre optique et sous-marins) : + de 200 câbles et 57 pays concernés;
- Partenariat actif en échange de l'accès à une partie des informations de la NSA : 60 % du renseignement Anglais provient de la NSA;
- GCHQ "hub" de l'espionnage Européen : a formé les Allemands à XKeyScore;
- Espionnage du G20 à Londres (2009) : piratage boîtes emails des délégations;
- Royal concierge : piratage de 350 établissements hôteliers.

Allemagne

- Partenariat permettant de surveiller une grande partie du réseau internet et téléphonique;
- Avec le consentement des services secrets Allemands : mise à disposition des bases de Bad Aibling depuis 2002 et Griesheim depuis 2007;
- Récolte de 500 millions de métadonnées par mois (15 fois plus que la France);
- Utilisation de XKeyScore ;
- Espionnage du Reichstag depuis les ambassades Américaines et Britanniques.

Chine

- Espionnage des sociétés télécom pour accès aux SMS;
- Tsinghua university : backbone du réseau universitaire et de recherche chinois;
- Hong Kong university (Hong Kong internet exchange);
- Pacnet : 46 000 Kms de fibre optique, 23 datacenters…

Et la France ? Espionnée…

- ALCATEL, WANADOO : collecte des métadonnées et données. 4.5 millions de personnes utilisent encore des adresses wanadoo;
- 70 millions de communications entre le 10 décembre 2012 et le 8 janvier 2013. Concerne également le monde des affaires, politique et administrations Françaises;
- US-985D : Enregistrement des conversations, interceptions SMS et historique des connexions pour des cibles sélectionnées;
- Ambassade de France à Washington : PBX (mise sur écoute des conférences), Highlands (piratage à distance des PC) et Wabash (micros);
- Représentation Française à l'ONU : Vagrant (captage d'informations des écrans), Highlands (piratage à distance des PC) et Wabash (micros);
- VPN quai d'Orsay : opération qualifiée de cas d'école.

A quelle échelle ?

- Allemagne : environ 20 millions d'enregistrements par jour
- France : environ 3 millions d'enregistrements par jour
- Audition du GEN Keith Alexander (octobre 2013) : "*Pour être parfaitement clair, nous n'avons pas recueilli ces informations sur les citoyens Européens, il s'agissait de données fournies à la NSA*".

En Europe ?

Rapport de l'Union Européenne en 2013 sur les programmes de surveillance en Europe :

- *"Les objectifs et l'ampleur de la surveillance sont précisément au cœur de ce qui différencie les régimes démocratiques des États policiers".*

- *"D'un point de vue légal, les programmes de surveillance des populations Européennes sont incompatibles avec les règles démocratiques de base, et compromettent la préservation des Droits de l'Homme pour les citoyens Européens et ceux qui résident sur le continent".*

Compromission des moyens de communication : L'exemple Français d'un outil d'interception

- Trafic IP, Réseaux téléphoniques fixes et mobiles, WiFi, Satellites, Radio V/UHF, Micro-ondes…;

- Grâce à des sondes passives invisibles;

- Mail (SMTP, POP3, IMAP), Webmails (Yahoo! Mail Classic & Yahoo! Mail v2, Hotmail v1 & v2, Gmail), VoIP (SIP / RTP audio conversation, MGCP audio conversation, H.323 audio conversation), Chat (MSN Chat, Yahoo! Chat, AOL Chat, Paltalk qui permet aux utilisateurs de Windows de chatter en mode texte, voix ou vidéo), Http, Moteurs de recherche (Google, MSN Search, Yahoo!), Transferts (FTP, Telnet).

Juste des soupçons ?

- Room 641A (mai 2006) : salles secrètes (AT&T) voient passer tout le trafic internet;
- Debian OpenSSL, générateur de nombres aléatoires prévisibles (mai 2008) : concerne clés SSH, OpenVPN, DNSSEC, certificats X509…;
- Archives BlackBerry vulnérables (octobre 2010) : l'algorithme générant le chiffré ne fait qu'une seule itération (10 000 sur IOS 4). Haute prédictivité du mot de passe et l'archive contient même les clés privées des certificats;
- IPSEC OpenBSD (décembre 2010) : Gregory Perry annonce qu'IPSEC OpenBSD a été backdooré depuis 2000;
- Coordonnées GPS (avril 2011) : Google et Apple enregistrent jusqu'à 1 an de coordonnées GPS avec horodatage. Fichiers sauvegardés sur ordinateur et même restaurés sur un nouveau terminal.

Mesures de protection : l'exemple Yahoo!

Les déclarations :

- Chiffrement des données entre les différents serveurs de l'entreprise;
- Les utilisateurs pourront chiffrer l'intégralité des données entrantes et sortantes;
- Élargissement de ces changements aux partenaires.

Et les questions :

- Chiffrement des données "au repos" ?
- Qui a les clés de chiffrement ?
- Le trafic chiffré est-il décodé en temps réel par la NSA ?

Ensuite ?

- Snowden : de 50 000 à 200 000 documents soit 42 à 150 ans au rythme de publication actuel;

- Nouveau datacenter NSA : 1 million de m², 2 milliards de dollars, 5 zetaoctet (1 milliards de giga…) soit 1000 années du trafic internet prévu en 2015. Prévu pour des données financières, transactions boursières, accords commerciaux, secrets militaires et diplomatiques étrangers… Centre critique pour cassage de code : "*NSA made an enormous breakthrough several years ago in its ability to cryptanalyze, or break, unfathomably complex encryption systems employed by not only governments around the world but also every users in the world*".

Ensuite ?

Les dernières technologies sont des chevaux de Troie pour introduire des méthodes de surveillance :

- Reconnaissance vocale;
- Identification digitale;
- Caméras dans le salon avec écoute;
- Portiques autoroutes;
- Bientôt authentification forte pour naviguer sur Internet ?

Conclusion

Changement de paradigme :
de la surveillance ciblée à la surveillance globale

Qui contrôle le contrôleur ?

Ne pas se tromper d'ennemi : les US ou la Chine ?

Conclusion

Merci Mr Snowden : maintenant le monde entier est sensibilisé à la SSI ☺

Les utilisateurs commencent à changer de comportement

Les entreprises intègrent plus sérieusement la SSI dans leur business

Questions ?

Gilles Defer

gilles.defer@abiosconsulting.com