Publié le 6 février 2015 | par **Lurinas**

La masse de documents exfiltrés par Snowden est telle que les révélations se succèdent ad nauseam. Le Conseil de l'Europe lui-même vient de livrer un rapport très critique sur les pratiques de la NSA. Si même lui le dit, c'est dire l'ampleur du scandale !

Les révélations de Snowden ont sérieusement relancé un intérêt certain pour la sécurité informatique, et notamment sur les risques d'espionnage. Pourtant, les révélations sont tellement innombrables et de tous ordres que nous avons tendance à régurgiter ces informations boulimiques. Heureusement, le Conseil de l'Europe est là pour nous rappeler le caractère attentatoire à nos libertés que représente cette société de surveillance.

Le rapport accablant

Encore un me direz-vous ?! Mais celui-ci a été mené pendant plus d'un an et cette fois par une commission du **Conseil de l'Europe**. Et ce **rapport est pour le moins très critique sur les programmes américains de surveillance électronique de masse** de la National Security Agency (NSA), et leurs conséquences pour l'Europe. Le 26 janvier, les membres de la commission des affaires juridiques et des libertés de l'assemblée parlementaire du Conseil, représentant 47 pays, ont carrément adopté le rapport à l'unanimité, sans amendement ! Étonnant, non ?

Le cœur du rapport est une énumération de l'ensemble des révélations d'Edward Snowden. Une compilation impressionnante : on redécouvre que grâce aux réseaux électroniques, les États-Unis se sont réellement donnés les moyens d'espionner la Terre entière en permanence. Tous les canaux imaginables ont été exploités, depuis la captation de trafic sur les câbles transatlantiques jusqu'au détournement de jeux vidéo en ligne.

Mais ces programmes n'ont plus de secret pour vous. Ils sont décortiqués au fur et à mesure de la lecture des documents de Snowden sur un site wiki dédié où nous pouvons retrouver le populaire Prism, mais aussi FoxAcid, BullRun, Quantum et tellement d'autres si imaginatifs encore : **https://www.nsa-observer.net/category/program**

Sur cette base, le rapport condamne les Etats-Unis sans réserve :

> ***« Ces opérations mettent en danger les droits de l'homme fondamentaux, notamment le droit au respect de la vie privée […], le droit à la liberté d'information et d'expression […], le droit à un procès équitable et à la liberté de religion »***

Ce qui n'est pas un rappel inopportun à l'heure de l'empilement et de l'accumulation des lois anti-terroristes et d'exception, quoi qu'on en dise (et les récents événements dramatiques laissent **présager le pire**). Une piqûre de rappel officielle donc.

Car des lois d'orientation et de programmation pour la performance de la sécurité intérieure (**Loppsi**) à celle de la programmation militaire (**LPM**), en passant par la **loi relative à la lutte contre le terrorisme**, les libertés publiques sont gangrénées par une marche forcée vers la surveillance de masse, entre autres.

Juridiquement pourtant, cet espionnage constitue une violation de la Convention européenne des droits de l'homme et de la Convention du Conseil de l'Europe sur la protection des données personnelles.

La commission à l'origine de ce rapport de lister alors des **recommandations**, objectifs démocratiques primordiaux.

C'est un fait indéniable que cette course à l'échalote : toutes ces opérations massives de surveillance et de renseignements numériques n'ont pas vraiment contribué à prévenir les attentats terroristes. D'où l'idée de plus en plus partagée que le Parlement européen mette limites par la loi pour prévenir les abus des services de renseignement. Une redondance avec les cadres juridique et conventionnel existants. Mais nécessaire et de salubrité publique.

Brèfle, en attendant, certains défenseurs des droits l'ont déjà dit et l'itèrent encore : il faut faire prosélytisme de l'utilisation du chiffrement. La tâche sacerdotale qui incomberait alors aux services de renseignement de déchiffrer une masse sans cesse plus importante de données permettra d'assurer une certaine protection de la vie privée des citoyens.

Pourtant, le problème central n'est pas encore complètement celui-ci. Il semble avéré que NSA and co. ne soient pas encore en mesure de traiter toutes ces masses numériques (mails, communications téléphoniques, etc.). Sans doute dans des temps de plus en plus proches, quand l'informatique quantique sera à disposition ?… En attendant, NSA, GCHQ, DGSE… se sont spécialisés ces dernières années à la reconstitution des réseaux. Ce qui n'est pas sans incidence potentielle pour nous tous (**http://latelelibre.fr/2013/07/21/demain-tous-suspects/**).

Voilà donc le nerf de la guerre de renseignements actuel : qui parle avec qui, combien de fois, depuis quel endroit ? Etc. Ce que l'on nomme les métadonnées.

Dans ce contexte, le programme MoreCowBell dernièrement dévoilé montre la volonté farouche de dessiner dans les plus fins détails les réseaux et les connexions à toutes échelles.

« Davantage de cloches à vaches »

L'opération secrète au nom de code MoreCowBell désigne l'attaque massive au système qui gère les noms de domaine, le Domain Name System (appelé DNS).

Le DNS gère les répertoires de noms à l'échelle mondiale. Les serveurs DNS sont des annuaires géants qui reçoivent les demandes de connexion sous forme d'adresses explicites (les url telles **latelelibre.fr**) puis trouvent la correspondance au numéro Internet (IP) sous forme de 4 paquets de chiffres (92.243.0.201).

Parmi tous les serveurs DNS existants, certains sont indispensables et sont appelés « **serveurs racine** », au nombre de 13, centralisant les répertoires pour le monde entier. Ces serveurs racines sont le '.' invisible et par défaut de toutes les adresses Internet (soit http://latelelibre.fr.).

L'opération MoreCowBell consiste donc en l'espionnage de tout le système des noms de domaine. Objectifs : une récolte passive de données pour cartographier les réseaux internes de grandes entreprises, d'administrations et d'organismes divers (ce qui parait aisé puisque le trafic DNS est en clair, facilité couplée par un stockage incommensurable dans une base de données) ; et préparer des offensives de la NSA (le pendant actif du programme) visant à pénétrer ou à perturber un serveur ou un réseau étranger.

En sus, la NSA intercepte directement le trafic Internet circulant sur certains câbles internationaux, et participe secrètement à la gestion de nœuds de communication appartenant au secteur privé. Et MoreCowBell semble servir en priorité à surveiller quasiment en temps réel « des sites Web de gouvernements étrangers, des forums terroristes et extrémistes, des sites de téléchargement de logiciels malveillants… », selon les documents que s'est procuré **Le Monde**.

Qui communique avec qui, quand, combien de fois, etc. ? A échelle des personnes. Mais aussi des entreprises, des administrations, des États !… On ne s'étonne plus de rien. Techniques maintenant classiques de la part de la NSA, mais déployées à grande échelle.

Des solutions existent

Petite revue des solutions offertes pour contrecarrer les velléités des services de renseignements.

Tor, logiciel libre anonymisant les connexions sur Internet par un routage dit « en oignon ».
OTR, pour un chiffrement des communications.
GPG, pour un chiffrement des mails, un fichier ou un dossier entier. Sa signature vaut authenticité du correspondant ou du document.
TAILS, système d'exploitation live (c'est-à-dire disponible sur un DVD, une clé USB ou une carte SD) pour un démarrage sur quasiment n'importe quel ordinateur. Son but est de préserver votre vie privée et votre anonymat, et de vous aider à utiliser Internet de manière anonyme voire contourner la censure (toutes les connexions sortantes vers Internet sont obligées de passer par le réseau Tor).
Redphone, application pour Android qui permet d'avoir des conversations chiffrées (tout comme **Textsecure**, application Android pour chiffrer les sms).

Le point commun de tous ces logiciels ? Ce sont des logiciels libres et opensource. La transparence du code pour l'anonymisation de nos libertés, rester dans l'ombre légitime. Vivons heureux, vivons cachés !

Lurinas

Lien

Pour en savoir plus sur MoreCowBell, le **site GNUnet**

À la une

Fous, et Alors ?
Israël – Palestine : Un Festival pour se Toucher
[Vox Pop] Le DG d'UBER en Garde à Vue
[DOC] Daivika, Un Corps à Croquer
Start Up Contest : 2 min pour Convaincre !

Le meilleur

SEMAINE DE LA PRESSE ET DES MÉDIAS À L'ÉCOLE : LE MONTEUR
PUTES PRIDE 2008
SAUVER KOKOPELLI ? MAMÈRE A UNE IDÉE...
SOUS LES PAVÉS... DENIS ROBERT – 1/3
SOUS LES PAVÉS... DENIS ROBERT – 2/3

Journal

[DOC] La Villeneuve : Objectif 8000€
J'ai le SIDA. Touche moi...
USA : Vortex Géant dans le Lac Texoma
Tiny Hamster is a Giant Monster !
[Rediff] Qui a Peur de l'Islam? Ce Soir sur France 4

À propos

Qui sommes-nous ?
L'association
Ils nous soutiennent
Charte éditoriale
Mentions légales
Nous contacter

Culture Économie Médias Monde Politique Société Sport