**France Leaks : Un constat, toutes les technologies de télécommunication sont compromises**

Comment la NSA a t-elle pu espionner les trois présidents français, les ministres mais aussi de nombreux haut-fonctionnaires et diplomates ? C’est la question que de nombreuses personnes se posent après la publication de nombreux documents de la part de WikiLeaks, [hier soir](http://www.frandroid.com/0-android/291182_wikileaks-la-republique-francaise-etait-sous-ecoute-americaine). On y apprend que les Etats-Unis ont intercepté de nombreuses discussions, dans plusieurs gouvernements, des cabinets ministériels mais aussi au sein de différents organismes.

Depuis 2013, face aux révélations d’écoutes téléphoniques commanditées par la NSA, la sécurisation des téléphones a été au coeur de la problématique du gouvernement et de la sécurité nationale. Malgré les consignes au sein même du gouvernement, Nicolas Sarkozy utilisait régulièrement un Blackerry ; et François Hollande, un iPhone et un BlackBerry. Lorsque nous avions appris que la ministre Mme Merkel avait été écoutée, la SGDSN nous avait assurée que le président français n’était pas concerné par d’éventuelles écoutes. Le premier signe de l’ignorance, c’est de présumer que l’on sait…

Suite à la révélation des produits documents de WikiLeaks, mais aussi d’Edward Snowden, des décisions avaient été prises à Matignon et à l’Elysée : il était alors interdit d’utiliser le fameux Blackberry, appareil favori des membres du gouvernement. BlackBerry, avec son système [BlackBerry OS](http://www.frandroid.com/culture-tech/os/blackberry-os) mais aussi son logiciel de messagerie instantanée BBM, posait un soucis majeur : fabriqué par la société canadienne Research in Motion (RIM), l’ensemble des données transite par des serveurs situés aux Etats-Unis et au Royaume-Uni.

Thales Teorem, un smartphone basique mais supposé inviolable

C’est ce qui embête la direction centrale des systèmes de sécurité et d’information, attachée au SGDSN. A partir de 2007, il a été décidé de concevoir un [smartphone](http://www.frandroid.com/smartphone)inviolable. Le Teorem est né, dans les laboratoires de Thalès. Malheureusement, le premier modèle était austère, et loin d’être un smartphone. Un smartphone à clapet, avec des outils compliqués et de nombreuses consignes d’utilisation contraignantes.

En octobre 2013, la Direction Générale de l’armement française (DGA) a tout de même commandé 14 000 terminaux (comprenez Teorem) pour une facture de 30 millions d’euros. Ce qui, après calcul, reviendrait à 2142,85 euros l’unité. L’information a été transmise par Le Canard Enchainé, et confirmé par plusieurs organismes.

Bull Hoox M2, le premier smartphone français sécurisé sous Android

Heureusement, une autre société française s’est penchée sur cette question, il s’agit de Bull.[Un smartphone Android a été conçu, le Hoox m2.](http://www.frandroid.com/smartphone/171323_hoox-premier-smartphone-securise-bull) Conçu en 2013, les caractéristiques de ce smartphone ne faisaient vraiment pas rêver, mais il a l’avantage d’intégrer des fonctions intelligentes. Vendu pour 2000 euros hors taxes, Bull a choisi Android, qui permet de modifier et de remodeler toutes les couches du système, une ROM ultra-sécurisée basée sur AOSP (Android Open Source Project) a donc été conçue.

Cette ROM Android permet de chiffrer les SMS, les conversations, et l’ensemble des données (OS et données utilisateurs). On retrouve un écran qHD (560 × 940 pixels) de 4,68 pouces, une puce à quatre cœurs Cortex-A5 cadencée 1,2 GHz, accompagnée par 1 Go de mémoire RAM ainsi que 8 Go de stockage.

Le chiffrement utilisé est plutôt classique, le système utilise une clef de session par appel avec une certaine longueur de clef, jusqu’à 2048 bits pour les mots de passe par exemple, 256 bits pour la voix et les SMS. Ensuite, les données transitent par un VPN connecté en permanence à la passerelle. L’enjeu de Bull était important. Pour que le smartphone soit utilisé, il ne doit pas frustrer ses utilisateurs. Une recette compliquée… l’utilisation des [applications](http://www.frandroid.com/comment-faire/applications-apprendre) tierces est très surveillée, et soumise au contrôle des directions informatiques. Ce qui n’a pas enrayé une pratique généralisée… l’utilisation des [smartphones](http://www.frandroid.com/produits-android/smartphone)et tablettes personnels, la plupart du temps non-sécurisés. Des smartphones et des tablettes sont souvent utilisés pour des conversations personnelles, mais aussi privées.

Les cartes SIM sont également touchées

[L’affaire Gemalto avait fait grand bruit](http://www.frandroid.com/0-android/operateurs/269096_laffaire-gemalto-la-bombe-qui-compromet-le-reseau-gsm). Pour rappel, l’entreprise Gemalto avait été attaquée conjointement par la NSA et le GCHQ. L’affaire était plutôt grave grave, les services de renseignement ayant pu mettre la main sur les clés servant au chiffrement des communications mobiles à travers nos cartes SIM : c’est tout le réseau GSM qui est compromis.

Le réseau peut également être en cause

Une autre hypothèse est plutôt sérieuse, celle de l’interception des communications. D’ailleurs, le « Special Collection Service », une unité composée de membres de la NSA et de la CIA, aurait mis en place un système d’écoute directement sur le toit de l’ambassade des Etats-Unis à Berlin.

A Paris, l’ambassade américaine, située place de la Concorde, est à quelques mètres à vol d’oiseau des principaux bâtiments du pouvoir français : l’Elysée, l’Assemblée nationale mais aussi les différents Ministères. [Le journal Libération](http://www.liberation.fr/monde/2015/06/23/a-paris-l-oreille-interne-de-l-ambassade-americaine_1335690) rappelait ainsi hier que le dernier étage de l’ambassade américaine en France « *est en effet surmontée d’une station d’espionnage des télécommunications du Special Collection Service (SCS)* » et recouverte d’une bâche en trompe l’œil qui cache des antennes.

Un constat, de la technologie américaine partout

Voilà un constat unanime chez les spécialistes de la sécurité. Nous n’avons pas le choix. Aujourd’hui, en Occident, tous les produits électroniques que nous achetons sont issus de la technologie américaine. Tous les logiciels et appareils ont été développés sous le contrôle de la NSA. Ce n’est pas simplement les gouvernements qui sont concernés, mais tous les acteurs technologiques, économiques et financiers. Apple, Google, Qualcomm, Intel, Facebook, Twitter… le FBI et la NSA, demandent constamment à ces entreprises technologiques de leur donner accès à leurs systèmes de chiffrement, qui empêchent l’interception des communications de leurs utilisateurs.

Dernièrement, l’empreinte digitale a été un des outils privilégiés dans la sécurisation des données. Néanmoins, nous avons appris dernièrement que la NSA a participé aux standards de cryptages biométriques des grands constructeurs afin de s’assurer de l’accès à l’information. Par exemple, les derniers iPhone avec Touch ID. Rien de surprenant, Apple a pris part au programme de surveillance PRISM mis en place par la NSA.

A partir du moment où les standards de sécurité sont eux même vérolés volontairement au départ, il ne peut y avoir de protection totale, sauf en prenant éventuellement un système russe ou chinois… mais au final le problème reste le même.