17 octobre 2017
Android

KRACK la nouvelle faille sur les smartphones : voilà comment savoir si vous êtes concernés

Des attaquants peuvent désormais lire le trafic Wi-Fi entre des périphériques et des points d'accès sans fil, et même le modifier pour injecter des logiciels malveillants sur des sites Web. Il semble que les appareils Android et Linux soient les plus touchés par ces multiples vulnérabilités.

Avec Fabrice Epelboin

Atlantico : Qu'est-ce que le Krack du protocole de chiffrement WPA2 qui est survenu hier ? Comment peut-on savoir quand on est concerné par ces découvertes de failles ?

Fabrice Epelboin : Il y a plusieurs protocoles pour sécuriser une connexion entre la borne wifi et la machine. Le plus sophistiqué étant le protocole de chiffrement WPA2, et le moins sophistiqué a été craqué depuis bien longtemps. Maintenant donc, tous les protocoles qui permettent d'établir une connexion wifi peuvent être craqués. Ce qui donne des conséquences dramatiques. La loi Hadopi impose une obligation de sécurisation qui n'est finalement plus pas applicable : on ne peut plus sécuriser sa connexion wifi, c'est techniquement impossible aujourd'hui. On ne peut donc pas appliquer la Loi.

Le simple utilisateur n'est pas du tout au courant de ces problématique de cybersécurité. Il n'est pas du tout au courant du fait qu'aujourd'hui, utiliser Windows, veut dire donner accès à sa machine à la NSA ainsi qu'a plein d'autres personnes. Le problème du crack du protocole wifi n'est finalement pas si important. Ce n'est qu'une petite partie des problèmes liés à la cyber sécurité auquel l'utilisateur devrait être au courant.

Doit-on s'attendre à une attaque informatique et un piratage de données de grande ampleur étant donné l'étendue du système d'authentification sécurisé (le protocole de chiffrement WPA2 (Wi-Fi Protected Access II)) utilisé aujourd'hui par la quasi-totalité des réseaux wifi personnels ou pro ?

Encore une fois, aucun protocole n'est aujourd'hui donc sécurisé. Est-ce que l'on peut s'attendre à des attaques de grande ampleur ? A priori non parce qu'il faut être à proximité du réseau wifi pour pouvoir le craquer. Donc, même par exemple, dans une grande entreprise, on compterait seulement quelques centaines de machine attaquées. Ce n'est cependant pas impossible d'imaginer des logiciels qui se répandent sur des myriades d'ordinateurs. Cela arrivera peut-être. Cet évènement a une résonnance particulière dans les média parce que ceux-ci ne sont pas en mesure de distinguer ce qui est grave ou pas, et découvrent complètement le domaine de la cybersécurité. En fait il n'y a pas de quoi s'alerter outre mesure dans le sens ou les gens devraient déjà être au courant. C'est un épiphénomène par rapport à des phénomènes qui sont aujourd'hui infiniment plus grand (comme par exemple l'armement

électronique de la NSA qui a été dérobé et distribué aux quatre coins du monde depuis déjà plusieurs mois. Ou encore cette cyber mafia que l'on soupçonne d'être russe, qui a distribué un utilitaire qui permet de prendre le contrôle à distance d'une machine Windows). Dans ces cas-là, l'espionnage d'un homme politique, d'un concurrent dans une entreprise est possible. La connexion wifi est dans un environnement ultra locale, le wifi porte à quelques dizaines de mètres. Donc finalement, l'événement est moindre.

Le pas franchi est médiatique essentiellement. Mais il a quand même des conséquences lourdes : la première, la plus drôle, est la plus évidente : c'est qu'il rend la Loi Hadopi caduque. La loi Hadopi a été traduite par une chose : vous êtes en tant que citoyen responsable de la sécurisation de votre connexion internet. Mais aujourd'hui ce n'est pas possible d'appliquer la loi. La totalité des utilisateurs de wifi en France sont dans l'illégalité au regard de la loi Hadopi. Si demain j'ai une lettre qui me reproche d'avoir enfreint la loi, je peux attaquer l'état devant un tribunal administratif en montrant que cette loi n'est pas applicable. Cela souligne la stupidité de la plupart des débats qui ont lieu en matière de cybersécurité à l'Assemblée nationale. En ce sens, cette faille est intéressante d'un point de vue juridique.

Traduire dans la loi "vous n'avez pas le droit de pirater" est très compliqué. La façon dont la loi l'a traduit était de rendre le citoyen responsable de sa connectivité wifi. Ce n'était déjà pas judicieux parce que cela sous-entendait que les citoyens avaient le savoir-faire technique pour sécuriser leur wifi. Ce qui n'est pas le cas. Et aujourd'hui, avoir un réseau wifi sécurisé est devenu techniquement impossible : même le plus grand expert ne pourrait pas sécuriser un wifi, il choisira le réseau filaire. Mais c'est n'est pas une solution très pragmatique. C'est donc le citoyen qui est responsable.

Les opérateurs sont-ils en mesures de donner réponses rapides, efficaces, et faire en sorte que les failles soient à l'avenir corrigé avant d'être détecté par un utilisateur ?

Les opérateurs, eux, ont des lobbies qui leurs permettent d'éviter les lois stupides.

On peut imaginer développer une nouvelle norme wifi mais peu de machine dans tous les cas ne pourront intégrer ces nouvelles normes. Et puis la plupart des gens ne pourront pas mettre à jour leur borne wifi car ils en seraient incapables. Beaucoup d'installation ne pourront pas être mise à jour et beaucoup d'installations qui pourront être mise à jour ne le seront pas par manque de compétences de la part des utilisateurs. Il n'y a pas vraiment de solutions pour l'instant.