Le chiffrement, maintenant (3)

Voici le troisième volet de l'initiation au chiffrement, initialement destiné aux journalistes sous l'égide de la Press Freedom Foundation, que nous avons traduit pour vous (vous pouvez retrouver le premier épisode et le deuxième).

Des logiciels de confiance

D'après Encryption Works

(Contributeurs : Slystone, Asta, goofy, lamessen, Bookynette)

Quand Snowden emploie les termes « endpoint security », il sous-entend que la sécurité sur les ordinateurs à chaque extrémité de la conversation est assurée par le chiffrement et le déchiffrement, contrairement à la sécurité assurée seulement pendant le transit du message. Si vous envoyez un courriel chiffré à un ami mais que vous avez un enregistreur de frappe sur votre ordinateur qui enregistre aussi bien l'intégralité de votre message que la phrase de passe qui protège votre clé de chiffrement, votre chiffrement n'est plus efficace.

Depuis que Glenn Greenwald et Laura Poitras, deux membres du conseil de la Freedom of the Press Foundation, ont révélé la surveillance généralisée des réseaux par la NSA, de nombreuses informations concernant les agences de renseignement ont été rendues publiques. Particulièrement Bloomberg, qui a publié des révélations sur des programmes volontaires de partage des informations entre les compagnies et les agences d'espionnage étatsuniennes.

Jusqu'à présent, la révélation la plus choquante au sujet de ces programmes de partage des informations, c'est que

Microsoft a une politique de communication des informations sur les vulnérabilités dans son logiciel au gouvernement étatsunien *avant de publier les mises à jour de sécurité pour le public*. L'article dit :

> *Microsoft Corporation, la plus grosse entreprise de logiciels du monde, fournit aux agences d'espionnage des informations sur les bogues dans ses logiciels grand public avant d'envoyer un correctif. Ces informations peuvent être utilisées pour protéger les ordinateurs du gouvernement et pour accéder aux ordinateurs de terroristes ou forces militaires ennemies.*

Cela signifie que la NSA a en main les clés pour accéder à n'importe quel ordinateur utilisant Windows, Office, Skype ou tout autre logiciel Microsoft. Si vous utilisez ces logiciels sur votre ordinateur, il est très probable que la NSA, avec suffisamment d'efforts, peut compromettre votre ordinateur ainsi que vos communications chiffrées, si vous devenez une de leurs cibles.

Nous avons aussi appris du New York Times que Skype, logiciel qui en dehors de la communauté de la sécurité a longtemps eu la réputation d'être un moyen sécurisé de communiquer, a envoyé des conversations privées au gouvernement étatsunien durant les cinq dernières années.

> *Skype, le service d'appel sur Internet, a commencé son propre programme secret, intitulé Project Chess, pour explorer les problèmes légaux et techniques afin de mettre les appels via Skype à disposition des agences de renseignements et des forces de l'ordre. Cette information vient de gens informés sur le programme qui ont demandé à ne pas être nommés pour éviter les ennuis avec les agences de renseignement.*
>
> *Le projet Chess, qui n'avait jamais été mentionné auparavant, était discret et limité à moins d'une douzaines de personnes chez Skype. L'une des personnes informées sur le projet a*

> *expliqué qu'il a été développé suite à des entretiens parfois houleux avec le gouvernement sur des questions juridiques. Il a commencé il y a 5 ans, avant que la majorité de la société ne soit vendue par son propriétaire, eBay, à des investisseurs externes en 2009. Microsoft a acquis Skype dans un accord de 8.5 milliards de dollars (environ 6.5 milliards d'euros) qui s'est conclu en octobre 2011.*
>
> *Un responsable de Skype a nié l'année dernière dans un article de blog que les récents changements dans le fonctionnement de Skype aient été faits à la demande de Microsoft pour faciliter l'application de la loi sur l'espionnage. Cependant, il semble que Skype ait compris comment collaborer avec les agences de renseignements avant même que Microsoft n'en prenne le contrôle, comme le dévoilent les documents divulgués par Edward J. Snowden, un ancien sous-traitant de la C.I.A. L'un des documents sur le programme PRISM qu'il a rendu public indique que Skype a rejoint le programme le 6 février 2011.*

Les logiciels propriétaires, comme la majorité de ceux proposés par Microsoft, Apple et Google, ont une autre faille. Il est beaucoup plus difficile pour les utilisateurs de vérifier de façon indépendante qu'il n'existe pas de portes dérobées secrètes à la demande clandestine de la surveillance d'état. Bien que des rapports récents aient montré que de nombreuses sociétés ont remis une quantité inconnue d'informations en réponse aux requêtes FISA, aucune de ces entreprises ne s'est avérée avoir *directement* de portes dérobées dans leurs systèmes.

Il existe un autre type de logiciel qui est plus fiable à cet égard. Les logiciels libres et open source ne sont pas forcément ergonomiques ? et ne sont pas nécessairement sans risques ? Cependant quand ils sont développés de façon ouverte, avec un logiciel de suivi de bogue ouvert, des listes de diffusion ouvertes, une architecture ouverte et un code

open source, il est plus difficile pour ces projets d'avoir une politique de trahison de leurs utilisateurs comme celle de Microsoft.

GNU/Linux est un système d'exploitation qui est entièrement composé de logiciels libres et *open source*. On peut prendre l'exemple de distributions GNU/Linux comme Ubuntu, Debian ou Fedora, qui sont les alternatives à Windows et Mac OS X les plus courantes. Bien que les projets de logiciels libres puissent toujours intégrer du code malveillant (voir le concours C Underhanded), la personne qui écrit ce code doit le cacher proprement et espérer qu'aucun des autres développeurs ou en aval des packagers GNU/Linux qui préparent et compilent le code source du projet pour l'intégrer à leur distribution ne le détectent.

Dans les années 1990, quand le chiffrement public est devenu populaire et que le gouvernement étatsunien faisait tout ce qu'il pouvait pour l'empêcher, le mouvement « cypherpunk » est né. De nombreux logiciels permettant aux gens de chiffrer sont nés de ce mouvement.

> *Les cypherpunks écrivent du code. Nous savons que quelqu'un doit développer des logiciels pour défendre notre vie privée. Et comme nous ne pouvons pas avoir de vie privée tant que nous ne le feront pas tous, nous allons les développer. Nous publions notre code pour que nos compatriotes cypherpunks puissent s'entrainer et jouer avec. Notre code est utilisable librement par n'importe qui dans le monde. Nous n'en avons rien à faire que vous n'approuviez pas le logiciel que nous développons. Nous savons que le logiciel ne peut être détruit et qu'un système largement dispersé ne peut être stoppé.*
>
> — Eric Hughes, dans son *Manifeste du Cypherpunk* de 1993

Ce code, qui est ouvert et public de façon à ce que d'autres cypherpunks puissent s'entraîner et jouer avec, que n'importe qui dans le monde peut utiliser librement, est à l'origine des

logiciels et protocoles dans lesquels nous pouvons avoir confiance : LUKS (le chiffrement de disque intégré à GNU/Linux), OpenPGP, Off-the-Record et Tor.

[mise à jour] Écartons TLS, le chiffrement à l'origine du HTTPS qui selon les dernières révélations semblerait perméable à l'espionnage par la NSA.

Le collectif de technologie tactique a conçu un très bon guide sur les logiciels de sécurité open source dans lesquels on peut avoir confiance pour préserver notre vie privée de toute surveillance. Il est important de rappeler que la simple utilisation de ces logiciels, même à la perfection, ne peut pas garantir la sécurité de votre chiffrement. Nous ne savons pas, par exemple, si Apple a transmis des failles 0-day de iOS à la NSA comme a pu le faire Microsoft. ChatSecure, qui permet d'avoir des discussions chiffrées sur les terminaux iOS, n'est pas plus sécurisé que le système d'exploitation sur lequel il fonctionne.

Il est important de rappeler que le simple fait d'utiliser du logiciel libre ne veut pas dire que l'on ne peut pas s'introduire dans vos systèmes. Des gens trouvent tout le temps des failles 0-day pour du logiciel libre, et parfois les vendent à des gouvernements ou d'autres attaquants malveillants. Des utilisateurs de logiciels libres téléchargent toujours des pièces jointes malveillantes avec leurs courriels, et ils ont souvent mal configuré des services simples sur leurs ordinateurs. Pire encore, les malwares sont souvent très bons pour se dissimuler. Si un utilisateur de logiciel libre attrape sur son ordinateur un malware, ce dernier peut y demeurer jusqu'à ce que l'utilisateur formate ses disques durs.

Tails, qui est une distribution GNU/Linux bootable sur live USB et live CD et dont je vais parler plus loin, résout beaucoup de ces problèmes.

(à suivre…)