Publié le 17 janvier 2014
Vers l'infini et au-delà !

Toujours plus loin : au-delà des révélations déjà faites, de quoi est encore capable la NSA pour nous surveiller ?

Pirater un ordinateur non connecté à internet, c'est possible, nous dit le journal Der Spiegel, relayé par le New York Times. La NSA aurait implanté des logiciels pirates dans 100 000 appareils, qui réagissent à des ondes émises par une station relais de la taille d'une mallette, et qui n'a besoin de se trouver qu'à quelques kilomètres.

Avec Jérémie Zimmermann
Jérémie Zimmermann est le co-fondateur et porte-parole de l'organisation de défense des droits et libertés des citoyens sur Internet La Quadrature du Net.

Voir la bio en entier

Atlantico : Dernière révélation en date sur les techniques d'espionnage : la NSA serait capable de pirater des ordinateurs non connectés à internet grâce à l'implantation par agent, ou même par le fabricant, d'un logiciel de surveillance. Les informations sont ensuite relayées par une station relais qui peut se trouver à quelques kilomètres de l'appareil concerné. 100 000

ordinateurs seraient ainsi surveillés Outre cet exemple, quelles sont les autres techniques d'espionnage dont on n'entend pas forcément parler ?

Jérémie Zimmermann : Cette information du New York Times, publiée le 14 janvier, est tirée d'un catalogue qui été décortiqué par Der Spiegel dans un article publié le 30 décembre 2013. On y voit **un inventaire qui relègue "Q" (de James Bond, NDLR) au rang d'un enfant avec une pelle et un saut dans un bac à sable : ordinateurs totalement fonctionnels tenant dans l'équivalent d'une pièce de 25 cents US, implants physiques... Cela va au-delà de ce qu'on pouvait imaginer il n'y a pas si longtemps, mais s'intègre tout de même dans une continuité.**

Il en va ainsi de la technique "Tempest", inventée par les Russes pendant la guerre froide et qui consistait à capter les radiations d'écrans et autres composants électriques. Les fameuses camionnettes garées devant les ambassades… Ce que l'on découvre aujourd'hui s'inscrit dans la même logique : **des *devices* quasiment passifs réagissent à des signaux radars en faisant de la modulation de fréquences, modulation captée en retour par les radars. Celle-ci peut correspondre aussi bien au son ambiant dans une pièce ou à l'affichage de l'écran d'un ordinateur**. Ces techniques, qui sont aussi impressionnantes que communes, amènent à faire la distinction entre l'espionnage ciblé et l'espionnage de masse.

A mesure que les révélations de Snowden continueront de s'égrener, dont une source proche du dossier m'a indiqué que l'on en connaissant seulement 5 %, il sera intéressant d'étudier l'articulation entre surveillance ciblée et surveillance de masse. On peut se demande par exemple si le fait d'essayer d'échapper à la surveillance de masse en utilisant des technologies de chiffrement, sans utiliser ni Google, ni Facebook, ne vous fait pas automatiquement devenir l'objet désigné d'une surveillance ciblée.

Or si la surveillance de masse est totalement inacceptable, puisqu'il s'agit d'une violation massive des libertés fondamentales, le fait d'espionner un nombre déterminé de personnes en vue déjouer des attentats terroristes est justifié. On ne peut pas faire de lien entre les deux, car la surveillance de masse ne sert pas à déjouer des attentats terroristes. **Le principe de l'espionnage est aussi vieux que l'État-nation, est peut être légitime tant qu'il se fait dans un cadre transparent et soumis à un rétrocontrôle démocratique.** Il ne serait pas réaliste de s'opposer à toute forme de surveillance, en revanche il faut se protéger de l'espionnage de masse.

Les "gadgets" du programme Quantum, dont fait partie le logiciel mentionné par le New York Times, servent à intercepter les communications et à procéder à de l'injection de paquet en masse, c'est-à-dire d'utiliser les propriétés du réseau pour prétendre être le site que l'internaute souhaite consulter. **Le login et le mot de passe entrés par l'utilisateur, en même temps qu'ils sont transmis à Google, sont envoyés à la NSA, ou bien permettent à un virus de pénétrer l'ordinateur. Ces technologies-là se trouvent à mi-chemin entre la surveillance ciblée et la surveillance de masse.** On aura beau jeu de nous expliquer qu'il existe 100 000 suspects de terroristes dans le monde. Le chercheur américain Jacob Appelbaum a mis en évidence le fait que la NSA est sûre à 100 % de pénétrer les appareils Apple. La marque à la pomme s'est bien entendu récriminée, mais le programme Bullrun, qui a été révélé après le programme Prism, montre que la NSA a investi 250 millions de dollars par an pour saboter une par une toutes les technologies commerciales censées protéger nos communications et nos données personnelles.

Est-ce un signe de plus de la connivence entre fabricants/concepteurs et services d'espionnage ? La NSA, pour ne citer qu'elle, s'adapte-t-elle a posteriori aux dernières innovations, ou bien suit-elle de près la R&D ?

Ces révélations montrent que le niveau technologique de la NSA est extrêmement avancée. Mais, dans le même temps, la NSA est très fière d'indiquer que la plupart des composants viennent du commerce grand public, *off the shelf*. La Maestro 2, qui est le circuit de la taille d'une pièce de 25 cents, vaut seulement 3 à 4 000 dollars. Par rapport au prix d'un avion de chasse ou d'un char, le prix est ridiculement faible. **Le programme Bullrun, qui est certainement l'un des plus importants dont on ait pris connaissance, nous montre que la NSA a encore besoin de saboter les implémentations des "crypto maps", ce qui prouve que ces dernières tiennent encore**. La NSA ne détenant pas la baguette magique permettant de casser lesdites "maps", la crypto est encore du côté des citoyens. Ces 250 millions de dollars sont un investissement considérable pour être au plus près des entreprises et ainsi suivre les avancées technologiques. C'est ainsi que dans chaque mise à jour d'IOS, d'iTunes,

etc. des portes dérobées laissées à dessein sont ménagées.

Pour en revenir à ce que je disais plus tôt, il serait intéressant de savoir à quel point la NSA se trouve *dans* Apple, *dans* Microsoft… **Ces produits utilisés par des milliards de personnes sont un *open bar* potentiel pour l'Agence**. Espérons qu'on en découvre un peu plus dans les mois à venir.

L'espionnage sans internet ne concerne que 100 000 ordinateurs actuellement. Pourrait-il porter sur tous les ordinateurs non connectés, et même sur d'autres appareils ?

C'est toute la question, il va falloir savoir à quel point la NSA est insérée au cœur des produits informatiques grand public. Au stade actuel, le droit de la NSA à faire faire ce qu'elle veut à une entreprise américaine, en toute discrétion, car autrement c'est la case prison, fait que techniquement, **on ne peut plus faire confiance à une entreprise US pour garantir le secret des communications privées.** Et on n'en est qu'au début de la prise en compte de la mesure de ces révélations, car **cela invite à repenser intégralement les structures en place et notre rapport à la technologie proposée par Google, Yahoo !, Facebook, Skype, auxquels on ne peut plus faire confiance**. Les mentalités, les comportements et les réflexes d'achat mettront un certain temps à s'adapter, par conséquent il faudra encore d'autres révélations sur les rapports entre les services de renseignement et partenaires publics et privés, ainsi que des politiques nationales incitant à libérer les individus des technologies *made in NSA* au travers des logiciels libres, des architectures décentralisées et du chiffrement. Ces technologies ont en commun de devoir être apprises, et **je pense que de plus en plus de gens, à commencer par les journalistes, dont la protection des sources est essentielle, se rendent compte de cette nécessité.** Car signer un contrat avec Facebook sans s'interroger sur l'architecture sous-jacente de cet outil de communication, cela revient à signer un contrat sans savoir lire.

Le grand public apprend régulièrement ce qu'il n'osait pas imaginer sur les méthodes d'espionnage. Que peut-on encore envisager ? Le champ des possibles est-il infini ?

Une telle chose est désagréable à dire et à entendre, mais "on vous l'avait bien dit". Par "on", j'entends la communauté des hackers. Le logiciel libre existe depuis 30 ans, et cela fait aussi longtemps que l'on sait que l'informatique peut être utilisée pour contrôler les individus ou les rendre plus libres.

Nous ne voyons pour le moment que la surface du phénomène. Les premières révélations avaient montré l'ampleur de la surveillance de masse, les plus récentes donnent une idée de la profondeur de la surveillance ciblée, **il nous reste à voir les interconnexions entre les différents services de renseignement. On commence par exemple à supposer que la DGSE et la NSA s'entendent sur le partage des flux passant par les câbles transatlantiques et des données Google**. Les services britanniques, qui n'ont pas le droit d'espionner leurs concitoyens, peuvent demander aux Américains de le faire à leur place, et vice versa. Résultat, tout le monde espionnerait tout le monde.

Nous allons encore en apprendre sur le réseau très dense des partenaires privés de la NSA. **Certains disparaissent, d'autres rouvrent, d'autre encore sont virés et réembauchés ailleurs, des anciens de l'armée se retrouvent chez des contractants…** On sait que 950 000 citoyens américains ont l'habilitation pour accéder à des informations classées top secret. Comment tolérer dans une société démocratique ce jeu de chaises musicales entre service public et privé, entre espionnage d'État et espionnage commercial ?

Propos recueillis par Gilles Boutin