Quels sont les gadgets de la NSA utilisés par la police ?

Quels sont les gadgets de la NSA utilisés par la police ?

The Intercept a pu mettre la main sur un catalogue de périphériques utilisés par les agences américaines de renseignement pour espionner et collecter des données. Un inventaire digne de James Bond. Des questions se posent quant à la légalité de ces appareils et la nécessité d'encadrer leur utilisation par la justice.

A vos portefeuilles ! En effet, les équipements présentés par *The Intercept* et que l'on peut découvrir à cette adresse ne sont accessibles ni à toutes les bourses ni à tous les quidams. Il s'agit en effet d'appareils particulièrement sophistiqués qui permettent aux agences américaines, et tout particulièrement la NSA, de se livrer à leurs activités d'écoute et de surveillance. Certains de ces appareils sont fixes alors que d'autres peuvent être installés dans des automobiles, avions ou drones. Ces différents appareils portent des noms évocateurs comme Cyberhawk, Yellowstone, Blackfin, Maximus, Cyclone ou encore Spartacus. Selon notre confrère, un tiers de ces équipements n'auraient jamais été décrits publiquement jusqu'à présent.

Les possibilités sont différentes selon les appareils. Certains sont destinés à cibler 10000 identifiants téléphoniques différents. La plupart sont capables de géolocaliser les personnes ciblées et, selon les modèles, des fonctions plus avancées comme l'écoute des appels ou la capture des SMS sont proposées. Deux modèles permettent de récupérer les fichiers contenus sur les smartphones ainsi que les carnets d'adresses, notes ou encore récupérer les messages préalablement supprimés.

Spoofing d'adresses

L'un des appareils les plus répandus est le StingRay qui est utilisé pour récupérer les conversations en se faisant passer pour les relais officiels des opérateurs mobiles comme Verizon, AT&T et autres. Cette technique d'interception, baptisée Spoofing, est aujourd'hui largement répandue non seulement par les agences de renseignement mais également par la police fédérale ou municipale. Et c'est là que les défenseurs des libertés individuelles commencent à se faire entendre, arguant que l'utilisation de ces appareils n'est pas suffisamment encadrée et que des dizaines de milliers de personnes voient leurs conversations espionnées au seul motif qu'elles se trouvent dans une même zone géographique qu'une personne suspectée et écoutée.

Stingray I/II

Ground Based Geo-Location (Vehicular)

"Ensnares bystanders, drains batteries, blocks calls"

Review by Nathan Wessler

$134,952.00

Le 4ème amendement mis à mal

Les défenseurs de la vie privée expliquent que l'utilisation de ces appareils, dans des conditions pas ou trop peu encadrées, viole le 4ème amendement de la constitution américaine. En effet, dans un premier temps, ces différents appareils, et tout particulièrement le StingRay commercialisé par la société Harris, était essentiellement utilisé à des fins militaires ou par des agences fédérales. Cependant à partir de 2007, l'usage croissant fait par les polices municipales a commencé à poser problème car cette utilisation semble s'effectuer hors de tout cadre juridique. *The Intercept* prend l'exemple de la police de Baltimore qui a utilisé le StingRay plus de 4300 fois depuis 2007. Comme à l'habitude, la lutte contre le terrorisme sert de viatique à l'emploi de ces appareils et techniques de surveillance. Toutefois, cet argument laisse trop souvent à désirer. En effet, nos confrères citent le cas de la police de l'Etat du Michigan qui a employé 128 fois le StingRay l'année dernière dans le but d'identifier la localisation physique d'une personne suspectée de terrorisme mais l'Association de défense des libertés civiles a précisé que sur les 128 utilisations aucune n'avait un quelconque rapport avec un acte terroriste.

Des fonds douteux utilisés pour les acquérir

Plus ennuyeuses encore sont les modalités d'acquisition de ces appareils. En effet, puisqu'ils sont achetés « hors la loi », les fonds utilisés sont également hors la loi et proviendraient de saisies financières lors des découvertes de trafics en tous genres, de drogue notamment. *The Intercept* écrit que les forces de police de l'Illinois, du Michigan et du Maryland ont utilisé des fonds d'origine crapuleuse pour procéder à leurs achats. L'accusation est particulièrement grave puisque cela revient à accuser les services de police de blanchiment d'argent sale pour mener des opérations notoirement illégales.

Dans ces conditions, un certain nombre de juges américains s'alarment des dérives et souhaitent une évolution de la loi encadrant l'utilisation de ces appareils. Au mois de novembre dernier, le juge fédéral de l'Illinois, Iain Johnston a publié un mémorandum sur la manière dont avaient été utilisées ces techniques de spoofing dans une enquête autour d'un trafic de drogue. « *Un simulateur de ce type est simplement trop puissant et les informations capturées sont trop vastes pour que l'autorisation d'emploi ne soit pas délivrée par une cour dûment habilitée* ».

Réagissez à cet article

Source : *Les gadgets de la NSA utilisés par toute la police*