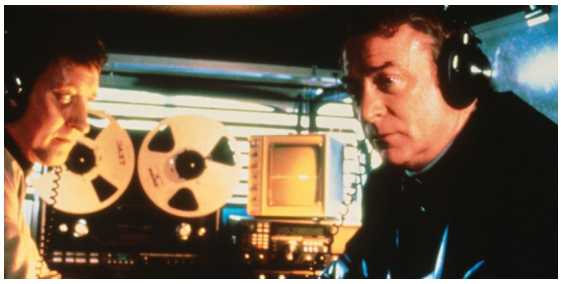
Les 8 techniques les plus ahurissantes des espions d’aujourd’hui | Le Net Expert Informatique

	Les 8 techniques les plus ahurissantes des espions d’aujourd’hui

Un projet de loi entend multiplier les possibilités de surveillance des agents du renseignement français. Tour des outils à disposition des services secrets dans le monde. Les services de renseignement français vont bientôt voir leurs possibilités d'espionnage multipliées, avec le projet de loi concocté par le gouvernement. L'occasion de faire le point sur l'éventail des outils à disposition des services secrets à travers le monde.

1. Ecouter les téléphones
Il s'agit de la pratique la plus évidente : l'écoute des conversations. En France, n'importe quel particulier peut être mis sur écoute dans le cadre d'une affaire portant « sur la sécurité nationale, la prévention du terrorisme, de la criminalité et de la délinquance organisée ».
Cette capacité s'est généralisée (pour atteindre un budget de 43 millions d'euros en 2013) et va parfois très loin. L'agence de renseignement américaine NSA s'est dotée d'une gigantesque capacité d'interception, avec son programme Mystic. En 2011, celui-ci aurait même servi à enregistrer 100% des appels passés dans un pays.
Pour simplifier les interceptions, la NSA a également des millions de données, notamment de Français, en se branchant directement sur le câble sous-marins ou les infrastructures internet par lesquels transitent 99% des télécommunications. L'agence était ainsi capable de récupérer en moyenne chaque jour 3 millions de données concernant des Français (conversations téléphoniques, SMS, historiques de connexions internet, e-mails échangés…).

Une écoute téléphonique dans le film « Le quatrième protocole » de John Mackenzie (1987) (AFP)

2. Ecouter Skype, Whatsapp et BBM
Les autorités françaises peuvent mettre en place des écoutes, sur simple décision administrative. Mais cette capacité d'écouter aux portes devrait s'étendre. Le projet de loi souhaite étendre les interceptions également aux SMS et aux e-mails. De plus, un discret amendement au projet de loi Macron va permettre d'étendre les écoutes aux services internet. A terme, les services pourront écouter/lire les conversations sur Skype, Hangout de Google, Whatsapp, WeChat, Line, Facebook Messenger, Viber, BBM, etc.
Microsoft aime à rappeler que, sur son service Skype, deux clefs de chiffrement aléatoires et inconnues de l'entreprise sont créées à chaque conversation, rendant techniquement impossible de brancher des écoutes. Seulement, l'argumentaire a été mis à mal à la suite d'une polémique en 2012 où le site Slate expliquait que des dispositifs techniques avaient été mis en place pour faciliter les interceptions de communication. L'année suivante, le « New York Times » révélait que Skype aidait les forces de l'ordre américaines à accéder aux données de ses clients.

3. La mallette qui écoute tout
Si l'écoute classique ne suffit pas, les services peuvent faire appel à une précieuse mallette : l'IMSI-catcher (parfois aussi désignée par sa marque, StingRay). Cet appareil permet de capter et d'enregistrer toutes les communications (appels, SMS) des téléphones à proximité. Techniquement, il se fait passer pour l'antenne de l'opérateur pour faire transiter par son disque dur toutes les conversations. Il suffit alors de se trouver à portée d'un suspect pour l'écouter.
Une solution largement utilisée par les agences de renseignement dans le monde entier. Aux Etats-Unis, pas moins de 46 agences locales dans 18 Etats y ont recours. Il faut dire que l'IMSI-catcher est plus accessible que jamais : il faut compter 1.800 dollars pour acquérir une mallette prête à l'emploi sur internet, selon « Wired ».

Le projet de loi du gouvernement prévoit d'autoriser leur utilisation par les services français, après avoir reçu l'aval d'un juge.
La NSA aurait même poussé le concept d'IMSI-catcher plus loin puisque, selon des documents d'Edward Snowden, la police fédérale américaine (US Marshall) utilise de petits avions de tourisme dotés de la même technologie afin de capter les communications de suspects.

4. L'aide des hackers
A l'image de James Bond, les services secrets peuvent utiliser micros et caméras pour surveiller des suspects. Ils peuvent aussi utiliser des balises GPS afin de les géolocaliser « en temps réel ». Des dispositifs que le projet de loi français entend légaliser. Mais il souhaite aller plus loin et permettre l'usage de logiciels espions.

Intitulés « keyloggers », ces logiciels-mouchards permettent de recopier en temps réel tout ce qui se passe sur un ordinateur, un smartphone ou une tablette. La navigation internet, les mots de passe saisis, les fichiers stockés… tout est accessible. Le texte du gouvernement précise que « des agents spécialement habilités » pourront « poser, mettre en œuvre ou retirer les dispositifs de captation ». Concrètement, des hackers des services de renseignement pirateront en toute légalité les machines des suspects pour mieux les espionner.

Issue du monde du piratage informatique, la pratique a fait des émules dans les services de renseignement. La NSA aurait ainsi développé un ver informatique, caché dans les disques durs vendus, capable d'espionner tous les faits et gestes, mais aussi de voler n'importe quel document de dizaine de milliers d'ordinateurs à travers le monde.

Mais la France n'est pas en reste puisque deux rapports indiquent que les services de renseignement hexagonaux ont développé leur propre logiciel malveillant, baptisé « Babar », qui renferme un keylogger. Objectif : écouter les conversations en ligne sur Skype, Yahoo Messenger et MSN, mais aussi de savoir quels sites ont été visités.

5. Ecouter autour du téléphone, même éteint
Le téléphone portable est décidément devenu le meilleur ami des agences de renseignement. Outre les écoutes et la géolocalisation, le mobile peut facilement se transformer en micro, même s'il est éteint.

Des documents d'Edward Snowden ont ainsi mis en lumière que la NSA (encore et toujours) est capable d'installer à distance un programme fantôme sur un portable afin de le transformer en espion. Le magazine « Wired » qui rapporte l'information n'entre pas dans les détails, mais ce ver permet de faire croire que l'appareil s'éteint alors qu'il continue de transmettre des informations (sur son contenu notamment). Pour s'en prémunir, la seule solution est de retirer la batterie.

Des hackers ont fait savoir depuis longtemps qu'il est possible de pirater un téléphone et d'en faire un véritable mouchard : écoute des appels, copie des SMS, géolocalisation, écouter les sons environnant (dans un rayon de 5 à 8 mètres), enregistrer la vidéo captée par l'objectif… Et la fonction micro fonctionne même si l'appareil est éteint (mais conserve sa batterie). Une fonction qui a sûrement déjà séduit des agences de renseignement à travers le monde.

6. La carte des interactions humaines
La NSA a aussi un appétit vorace pour les métadonnées. Tous les échanges électroniques (appels, SMS, e-mails, surf sur internet) colportent également des détails sur ceux-ci : qui communique avec qui, à quelle heure, pendant combien de temps, depuis où, etc. Des données qui se rapprochent des fadettes (les factures téléphoniques détaillées) et qui intéressent grandement la NSA.

L'agence a mis en place un programme visant à collecter et à stocker l'ensemble des métadonnées obtenues par les opérateurs télécoms américains. Objectif : constituer une gigantesque base de données permettant, à tout moment, de connaître les interactions entre personnes sur le sol américain. Une idée qui plaît aussi aux renseignements français, déjà experts des fadettes. Le projet de loi souhaite que les autorités puissent avoir accès aux métadonnées d'une personne ciblée sans demander l'avis d'un juge, il suffira d'une autorisation administrative.

Afin de mieux appréhender ce que les métadonnées peuvent dire de nous et de nos interactions, le Massachusetts Institute of Technology (MIT) propose l'outil Immersion qui permet de visualiser sa galaxie de relations basée sur son adresse Gmail de Google.

7. La constitution d'une banque de photos
Toujours selon des documents de Snowden, la NSA collecte chaque jour une quantité astronomique de photos (« des millions d'images ») afin de s'en servir dans le cadre de reconnaissance faciale. Le tout est récupéré dans des e-mails, SMS, sur les réseaux sociaux, via les outils de vidéo-conférences, etc.
Quotidiennement, l'agence obtiendrait 55.000 photos permettant d'identifier des individus, afin d'alimenter une immense banque d'images. L'objectif étant de pouvoir identifier rapidement un suspect, en particulier quand la banque d'images des photos de passeports ne suffit pas.

8. Fouiner dans les téléchargements illégaux
Les téléchargements illégaux peuvent aussi aider les autorités, ou du moins les aiguiller. Un document d'Edward Snowden a révélé que les services secrets canadiens ont chaque jour scruté l'ensemble des téléchargements réalisés sur des plateformes comme MegaUpload ou RapidShare, afin de repérer les manuels et documents édités par des groupes terroristes, afin d'identifier leurs auteurs et ceux qui les consultent. Ils produisaient alors une liste de suspects, transmise à leurs alliés, dont les Etats-Unis. En somme, une aiguille dans une botte de 10 à 15 millions de téléchargements quotidiens.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://tempsreel.nouvelobs.com/tech/20150317.OBS4818/les-8-techniques-les-plus-ahurissantes-des-espions-d-aujourd-hui.html
Par Boris Manenti