Votre employeur peut espionner vos communications chiffrées, et la CNIL est d’accord | Le Net Expert Informatique

	Votre employeur peut espionner vos communications chiffrées, et la CNIL est d’accord

La Commission nationale informatique et libertés donne sa bénédiction au déchiffrement des flux HTTPS des salariés, à condition que cette pratique soit encadrée. Il reste néanmoins une zone de flou juridique côté pénal…

Saviez-vous que certains employeurs déchiffrent systématiquement les flux HTTPS de leurs salariés lorsqu'ils surfent sur Internet ? Ils disposent pour cela d'un équipement appelé « SSL Proxy » qui se place entre l'utilisateur et le serveur Web. Cette boîte magique déchiffre tous les échanges en usurpant l'identité du service interrogé (google.com, par exemple), par l'utilisation d'un certificat bidon. La pratique n'est pas du tout récente, mais se fait de manière un peu cachée en raison d'incertitudes juridiques et de l'impopularité de cette mesure auprès des salariés. Les directeurs informatiques n'ont, par conséquent, pas une folle envie d'en faire la publicité.
Mais l'employeur peut se rassurer : la CNIL vient de publier une note qui clarifie les choses. Ainsi, la Commission estime que le déchiffrement des flux HTTPS est parfaitement « légitime », car elle permet à l'employeur d'assurer « la sécurité de son système d'information », en bloquant les éventuels malwares qui s'y trouveraient. Evidemment, ce n'est pas la seule raison : ces équipements sont également utilisés pour prévenir les fuites d'informations. Un salarié qui enverrait des documents confidentiels à un concurrent pourrait, ainsi, être facilement repéré.

Infraction pénale ou pas ?
Toutefois, la CNIL met un (petit) bémol. L'utilisation de cette technique de surveillance doit être « encadrée ». Ainsi, les salariés doivent être informés en amont et de manière « précise » sur cette mesure : raisons invoquées, personnes impactées, nature de l'analyse effectuée, données conservées, modalités d'investigation, etc. L'employeur doit également mettre en place une « gestion stricte des droits d'accès des administrateurs aux courriers électroniques ». Autrement dit : éviter que tous les membres du service informatique puissent fouiller dans les messageries. Par ailleurs, les « traces conservées » doivent être réduites au minimum.
Il reste néanmoins une petite zone de flou juridique, nous explique la CNIL. En effet, le Code pénal interdit théoriquement « d'entraver ou de fausser le fonctionnement d'un système de traitements automatisés de données (STAD) ». Or, quand l'entreprise déchiffre les flux Gmail de ses salariés, on peut estimer que cela fausse le fonctionnement du STAD d'un tiers, à savoir Google. Cela pourrait donc constituer une infraction. Conclusion de la CNIL : il faudrait peut-être modifier le Code pénal pour que l'employeur puisse réellement surveiller ces flux chiffrés en toute tranquillité. Décidément, la situation n'est pas encore totalement claire…

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

Source : http://www.01net.com/editorial/651057/votre-employeur-peut-espionner-vos-communications-chiffrees-et-la-cnil-est-d-accord/
Par Gilbert Kallenborn

Ce mardi, attaque numérique lancée contre Israël jusqu'à

sa disparition de l’espace informatique | Le Net Expert Informatique

Ce mardi, attaque numérique lancée contre Israël jusqu’à sa disparition de l’espace informatique

Ces pirates informatiques, prétendant appartenir à Anonymous, se lancent dans une guerre virtuelle contre Israël. Anonymous, toujours prêt à l’attaque informatique
La prochaine attaque informatique contre Israël est qualifiée de « shoah électronique » par le groupe de hackers. Ceux-ci se disent révoltés par la terreur infligée au peuple palestinien dont les crimes, les tortures et les enlèvements. Ils crient aujourd’hui vengeance à travers un outil qu’ils maitrisent: la Toile!

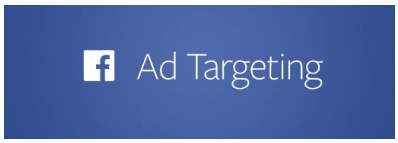
En effet, dans une vidéo postée sur Youtube, on peut y voir un membre du groupe Anonymous faire l’apologie du terrorisme informatique et menacer ouvertement Israël de cyberattaques…
La personne dit clairement: « **Le 7 avril prochain, les élites du cyberespace s’uniront solidairement pour soutenir les Palestiniens contre Israël… Nous allons faire disparaître l’état d’Israël de l’espace informatique** ».
Tout cela est dit en illustration d’une vidéo en arrière-plan montrant une scène de conflit entre Palestiniens et Israéliens. L’homme sur la vidéo tient une posture solennelle, comme s’il s’agissait d’un chef d’Etat qui faisait une déclaration officielle à ses citoyens. Il porte aussi un costume et le fameux masque de Vendetta. Sa voix a été changée pour la circonstance et son discours en anglais a été sous-titré en arabe. Il s’adresse aussi au Premier ministre israélien réélu dernièrement, le traitant d’imbécile et lui promettant d’attaquer le pays électroniquement jusqu’à ce que le peuple palestinien soit libre.
Il est évident que la date de la cyber-attaque n’ait pas été choisie au hasard puisque cela tombe juste quelques jours avant la journée de commémoration de la Shoah.
L’Etat d’Israël semble toutefois insensible à ces menaces et préfère en rire et ne pas les prendre au sérieux.
En effet, Mr Benjamin T. Decker, membre des services secrets et basé à Tel Aviv, s’est exprimé dans les colonnes de Newsweek, disant que c’est plus une blague de bas étage et que cela fait la quatrième année que ce groupe demande à ses supporters de mener une attaque pour effacer Israël du cyber espace. Il poursuit disant que leurs attaques ne portent pas toujours les fruits attendus puisque Israël se protège en menant des contre-attaques et se protégeant informatiquement en amont.
Lire la suite….

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://fr.blastingnews.com/international/2015/04/des-hackers-sortent-une-bombe-informatique-face-a-israel-00332177.html

Facebook accusé de traquer tous les internautes connectés ou non à son réseau | Le Net Expert Informatique



Facebook accusé de traquer tous les internautes connectés ou non à son réseau

Selon une étude menée pour la CPVP, l'équivalent belge de la CNIL, Facebook traquerait tous les internautes sans distinction, une accusation que réfute la firme de Mark Zuckerberg.

En Belgique, la Commission de la protection de la vie privée a commandé une étude sur les pratiques de Facebook. Celle-ci a été menée par l'université de Leuven et plus spécifiquement par le centre interdisciplinaire des lois et des technologies d'information et de communication (ICRI), le département de la sécurité informatique et du chiffrement industriel (Cosic) et le département des médias, de l'information et des télécommunications de l'université de Vrije à Bruxelles.
Selon les chercheurs, pour améliorer le ciblage publicitaire, Facebook traquerait les internautes sans leur consentement, qu'ils soient connectés ou non au réseau communautaire et même s'ils ne disposent pas de compte. Plus précisément, Facebook placerait un cookie sur ses pages accessibles sans connexion (comme les pages de fans).
Selon The Guardian, qui rapporte l'information, ce cookie renverrait des données lorsque l'internaute visite l'un des quelque 13 millions de sites faisant usage du dispositif Facebook Connect par exemple pour insérer le bouton J'aime. Le mécanisme fonctionnerait même lorsque l'utilisateur ne s'est pas connecté à son compte ou lorsqu'il n'a pas interagi avec le fameux bouton J'aime.
A en juger par ce rapport, Facebook ne respecterait pas la réglementation de l'Union Européenne selon lesquelles l'internaute doit exprimer son consentement pour accepter les cookies qui permettront de le suivre.
Interrogé par The Inquirer, Facebook dément avoir mis en place de telles pratiques. « Ce rapport contient des faits inexacts. Les auteurs ne nous ont jamais contacté, ni n'ont souhaité éclaircir leurs suppositions sur lesquelles ils ont basé leur rapport », affirme un porte-parole. Facebook explique avoir souhaité s'expliquer devant la CPVP ayant commandé cette étude mais ces derniers n'auraient pas souhaité les recevoir.

Retrouvez le rapport dans son intégralité (PDF)
http://www.law.kuleuven.be/icri/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf

---

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…

S o u r c e :
http://pro.clubic.com/blog-forum-reseaux-sociaux/facebook/actualite-761365-facebook-traquer-internautes-connectes-reseau.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_02/04/2015&partner=-&svc_position=922875434&svc_misc=-&crmID=639453874_922875434&estat_url=http%3A%2F%2Fpro.clubic.com%2Fblog-forum-reseaux-sociaux%2Ffacebook%2Factualite-761365-facebook-traquer-internautes-connectes-reseau.html

---

| Le Net Expert Informatique

5% des utilisateurs de Google seraient victimes d’un adware sur leur machine | Le Net Expert Informatique

5% des utilisateurs de Google seraient victimes d’un adware sur leur machine

Google a publié les résultats d’une étude sur la publicité intrusive et plus particulièrement les adware installés sur les machines des internautes à leur insu.

Google explique que depuis le début de l’année, la société a reçu 100 000 plaintes émanant des utilisateurs du navigateur Chrome, victimes d’adware. Ces logiciels malveillants injectent littéralement de la publicité au sein des pages Web affectant leur lisibilité, mais générant également des erreurs réseau ou malmenant les performances du navigateur.
En partenariat avec l’université de Berkeley en Californie, Google annonce avoir lancé une étude dont les résultats finaux seront dévoilés au 1er mai prochain. Celle-ci a été menée sur 100 millions de pages vues sur les sites de Google au travers des navigateurs Chrome, Firefox et Internet Explorer.
Google explique que les adware ciblent aussi bien les systèmes Windows et OS X ainsi que les trois navigateurs. En outre, plus de 5% des internautes visitant les sites de Google auraient au moins un injecteur publicitaire installé sur leur machine. La moitié d’entre eux en disposeraient d’au moins deux et un tiers en auraient au moins quatre.
En outre, 34% des extensions pour Chrome injectant des publicités seraient directement classées en tant que malwares. Les chercheurs ont trouvé 192 extensions malveillantes. Avant d’être bloquées celles-ci affectaient 14 millions d’utilisateurs. Google indique avoir implémenté les technologies de ces chercheurs pour scanner automatiquement le Chrome Web Store à la recherche de nouvelles menaces potentielles.

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://www.clubic.com/antivirus-securite-informatique/actualite-761347-google-5-internautes-disposeraient-adware-machine.html?estat_svc=s%3D223023201608%26crmID%3D639453874_922037053

Les 12 outils de communication des commerçants, pme, tpe et professions libérales | Le Net Expert Informatique

Les 12 outils de communication des commerçants, pme, tpe et professions libérales

Le développement de la communication numérique est une formidable opportunité pour accroître votre visibilité et augmenter votre clientèle. Ce serait dommage de ne pas la saisir ! Vos clients sont au bout de leur smartphone, derrière leurs ordinateurs et leurs tablettes.
Pour vous accompagner dans la mise en place d'actions de communication locale nous avons listé pour vous 12 outils.

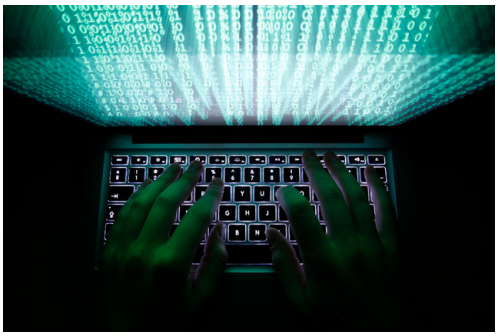
1. L'identité de marque
2. Documents print
3. Le site internet
4. Le référencement
5. Les réseaux sociaux
6. Le micro-blogging
7. Le marketing direct
8. Le marketing relationnel
9. Le street marketing
10. Les relations presse
11. L'achat média
12. Le Sponsoring

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 : https://www.1min30.com/ressource/outils-pme-tpe

Les sites Internet trompeurs visent de plus en plus les PME| Le Net Expert Informatique

 Image: Photo d’illustration/Reuters	**Les sites Internet trompeurs visent de plus en plus les PME**

Les petites et moyennes entreprises sont aussi concernées par les attaques sur le web. Les pirates se servent des données des sites pour tromper les clients. La manœuvre la plus courante est d'envoyer des mails aux clients en se faisant passer pour l'entreprise.

Les escrocs opérant via Internet ne s'en prennent plus uniquement à des grandes marques connues: de plus en plus, ils imitent les sites web de petites et moyennes entreprises pour tromper leurs clients. Ils accèdent ainsi à leurs mots de passe ou données de cartes de crédit.
La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) intervient quotidiennement pour retirer ce type de contenus frauduleux du web, a-t-elle annoncé le mardi 31 mars. Les derniers cas rapportés témoignent même d'une sophistication accrue.
Les attaques de phishing, par lesquelles des escrocs cherchent à accéder à des données sensibles, concernent différents types de PME ayant un site WEB et qui enregistrent des adresses mail de clients, par exemple pour l'envoi d'une newsletter.
Dans un premier temps, les criminels attaquent le site web de l'entreprise. La plupart du temps, ils exploitent une faille sur le site. Cela leur permet d'accéder à une base de données contenant des mails de clients.
Ensuite, ils envoient des mails à ces clients en se faisant passer pour l'entreprise. Les messages font par exemple état d'un remboursement pouvant être demandé par le biais d'un lien indiqué. Derrière ce lien se cache un site web imitant à l'identique celui de l'entreprise et utilisant un nom de domaine très similaire.

Victime en confiance
Le client y est prié de fournir les détails de sa carte de crédit (numéro, validité, cryptogramme), à l'image d'une page de phishing «classique». En usurpant le mail et en imitant le site web d'une entreprise avec laquelle la victime potentielle est en relation, les escrocs augmentent leurs chances de succès, puisque la cible aura plus de chances de se sentir en confiance.
MELANI conseille aux entreprises d'informer rapidement leurs clients lorsqu'elles remarquent le vol d'e-mails. Quant aux utilisateurs, ils sont priés d'effacer les courriels leur enjoignant de fournir des données de cartes de crédit: aucune entreprise sérieuse ne demande de telles informations par mail, rappelle MELANI.
De plus, il faut se méfier des mails évoquant des conséquences (perte financière, plainte pénale, blocage d'un compte ou d'une carte etc) si le destinataire n'agit pas. Enfin, il faut toujours contrôler l'«adresse Internet» (URL) sur laquelle on est redirigé. Pour ce faire, il suffit de positionner la souris sur le lien sans cliquer. (ats/Newsnet)

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

Source : http://www.tdg.ch/high-tech/sites-internet-trompeurs-visent-plus-pme/story/15578282

La Commission européenne conseille de quitter Facebook | Le Net Expert Informatique

La Commission européenne conseille de quitter Facebook

Un avocat de la Commission européenne a conseillé au procureur général de la Cour de Justice de l'Union Européenne (CJUE) de fermer son compte Facebook pour éviter que ses données personnelles soient exploitées aux Etats-Unis.

« Vous devriez envisager de fermer votre compte Facebook si vous en avez un » a conseillé Bernhard Schima, l'avocat de la Commission européenne, au procureur général de la JUE Yves Bot la semaine dernière. Une recommandation lancée dans le cadre d'une audience concernant la confidentialité des données des Européens vis-à-vis de l'utilisation qu'en fait le géant américain. La question avait été soulevée il y a plusieurs années par Max Schrems, un étudiant en droit autrichien qui a déclenché en août 2014 une procédure d'action collective mondiale à l'encontre de Facebook.
Mais le procès actuellement en cours oppose Max Schrems à l'équivalent irlandais de la CNIL, contre laquelle l'Autrichien a porté plainte, refusant de voir ses données personnelles stockées par Facebook – dont le siège européen se trouve en Irlande – transférées aux Etats-Unis pour alimenter le ciblage publicitaire de l'entreprise. Le réseau social n'est pas le seul concerné : Microsoft, Apple ou encore Yahoo sont également pointés du doigt.

Ciblage et espionnage
Max Schrems considère que les révélations d'Edward Snowden concernant l'espionnage des données pratiqué par la NSA met les Européens en danger à partir du moment où leurs données personnelles transitent aux Etats-Unis. Une accusation qui remet en question l'application du Safe Harbor, un ensemble de principes de protection des données personnelles, négociés entre les autorités américaines et la Commission européenne en 2001. Les entreprises qui adhèrent à ces principes peuvent recevoir des données en provenance de l'UE, mais la surveillance généralisée de la NSA remettrait en question l'application de ces règles.
On comprend mieux en quoi la petite phrase de l'avocat de la Commission européenne est lourde de sens : elle semble donner raison à la théorie de Max Schrems, engagé depuis longtemps contre la collecte d'information, jugée abusive, par Facebook.
Le commissaire irlandais à la protection des données considère quant à lui qu'il n'existe aucune preuve que le transfert des données de Max Schrems aux Etats-Unis lui a porté préjudice. « Ce n'est pas étonnant dans la mesure où la NSA n'est pas intéressée par les essais écrits par les étudiants en droit autrichiens » a-t-il ironisé. L'avocat général devrait rendre son avis sur l'affaire le 24 juin prochain.

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://pro.clubic.com/blog-forum-reseaux-sociaux/facebook/actualite-760937-protection-donnees-personnelles-commission-europeenne-conseille-quitter-facebook.html

HoloLens, l’ordinateur du futur ? | Le Net Expert Informatique

HoloLens, l’ordinateur du futur ?

Le projet « Windows Holographic », avec son masque HoloLens, permettra de manipuler des objets virtuels dans un environnement réel.Microsoft assure que ce dispositif ambitieux préfigure « l’ordinateur du futur ».

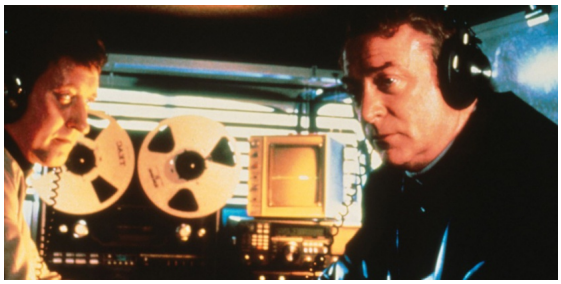
Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin 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://www.01net.com/editorial/642445/hololens-lordinateur-du-futur-video-du-jour/

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.

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