INTERNET MASSIVEMENT SURVEILLÉ

En partenariat avec WikiLeaks, OWNI révèle l'existence d'un nouveau marché des interceptions massives, permettant d'écouter toutes les télécommunications à l'échelle d'une nation. Ses acteurs vendent leurs produits en Europe, aux États-Unis et à des dictatures.

WikiLeaks rend public aujourd'hui près de 1 100 documents internes, plaquettes commerciales et modes d'emploi des produits commercialisés par les industriels des systèmes de surveillance et d'interception des télécommunications.

Ces nouvelles fuites montrent un marché de la surveillance de masse représentant désormais cinq milliards de dollars, avec des technologies capables d'espionner la totalité des flux Internet et téléphoniques à l'échelle d'une nation. Les fleurons de ce marché s'appellent Nokia-Siemens, Qosmos, Nice, Verint, Hacking Team, Bluecoat ou Amesys. Les documents détaillant leurs capacités d'interception, contenant une multitude de détails technologiques, seront progressivement mis en ligne par WikiLeaks.

OWNI, partenaire de cette opération baptisée SpyFiles avec Privacy International et The Bureau of Investigative Journalism, deux ONG britanniques, ainsi que le Washington Post, The Hindu, L'Espresso, la chaîne allemande ARD, a tenté de visualiser cette industrie d'un genre nouveau, en créant une cartographie interactive sur un site dédié, SpyFiles.org. Et Andy Mueller-Maguhn, ancien porte-parole du Chaos Computer Club allemand (le plus influent des groupes de hackers au monde), également associé à cette enquête, y consacre un site, BuggedPlanet.info – traduisez "planète sur écoute".

Marchand d'armes de surveillance

À ce jour, nous avons répertorié 124 de ces marchands d'armes de surveillance, utilisant des technologies d'interception, dont 32 aux États-Unis, 17 au Royaume-Uni, 15 en Allemagne, dix en Israël, huit en France et sept en Italie… À l'instar des marchands d'armes "*traditionnels*", la majeure partie d'entre eux sont situés dans des pays riches, et démocratiques. 12 des 26 pays recensés font ainsi partie de l'Union européenne qui, au total, totalise 62 de ces entreprises.

87 vendent des outils, systèmes et logiciels de surveillance de l'Internet, 62 de surveillance du téléphone, 20 des SMS, 23 font de la reconnaissance vocale, et 14 de la géolocalisation GPS. Sept d'entre elles font également dans la "*lutte informatique offensive*", et commercialisent donc des chevaux de Troie,rootkits et autres backdoors (portes dérobées) permettant de prendre le contrôle d'ordinateurs, à distance, et à l'insu de leurs utilisateurs. Ces systèmes espions ont ceci de particulier par rapport à ceux utilisés par les pirates informatiques qu'ils ne seraient pas repérés par la "*majeure partie*" des éditeurs d'antivirus et autres solutions de sécurité informatique.

INTERNET MASSIVEMENT SURVEILLÉ

Dans nos démocraties, la commercialisation, et l'utilisation, de ces systèmes de surveillance et d'interception des télécommunications est strictement encadrée. Mais rien n'interdit, en revanche, de les vendre à des pays moins regardants, même et y compris à des dictatures : bien que conçus à des fins d'espionnage, ils ne font pas partie de ces armes dont l'exportation est encadrée par les lois nationales, européennes ou internationales. Ce n'est donc peut-être pas moral, mais tout à fait légal, en l'état.

Et les marchands d'armes se font fort d'exploiter ce vide juridique, comme le reconnaissait récemment Jerry Lucas, l'organisateur d'ISS, le salon international qui rassemble tous les deux ou trois mois les professionnels de l'interception des communications :

> “ Les systèmes de surveillance que nous exposons dans nos conférences sont disponibles dans le monde entier. Certains pays les utilisent-ils pour supprimer certaines déclarations politiques ? Oui, probablement. Mais ce n'est pas mon job de faire le tri entre les bons et les mauvais pays. Ce n'est pas notre métier, nous ne sommes pas des hommes politiques.

> “ Notre business est de mettre en relation ceux qui veulent acheter ces technologies avec ceux qui les vendent. Vous pouvez bien vendre des voitures aux rebelles libyens, et ces voitures sont utilisées comme armes. General Motors et Nissan devraient-ils se demander comment leurs véhicules seront utilisés ? Pourquoi n'allez-vous pas également interroger les vendeurs de voiture ? C'est un marché ouvert. Vous ne pouvez pas enrayer la circulation de matériels de surveillance.

Interrogé par le *Wall Street Journal*, Klaus Mochalski, co-fondateur d'Ipoque, une société leader dans ce secteur, répondait de son côté que “*c'est un dilemme, moral et éthique, auquel nous sommes constamment confrontés : c'est comme un couteau. Vous pouvez vous en servir pour trancher des légumes, mais vous pouvez également tuer votre voisin*“… à ceci près que ces outils ne sont pas en vente libre dans n'importe quel magasin, et que les sociétés qui les commercialisent n'en font pas la promotion dans des foires commerciales ou marchés du coin, mais uniquement dans les salons réunissant marchands d'armes, et clients habilités à en acheter.

Silence radio

ISS interdit ainsi aux journalistes d'assister à ses conférences, et même d'entrer dans son salon. Et il était étonnant de constater, à visiter les nombreux stands spécialisés dans les technologies de surveillance présents au récent salon Milipol, qui s'est tenu à Paris en octobre dernier, que les représentants de ces derniers étaient bien plus frileux que les marchands d'armes traditionnels pour ce qui est de répondre aux questions des journalistes…

INTERNET MASSIVEMENT SURVEILLÉ

Contactée par *OWNI*, Amesys, la société française qui a vendu un système d'interception massive de l'Internet à la Libye de Kadhafi, se défausse ainsi auprès de son "*client*" :

> Amesys est un industriel, fabricant de matériel. L'utilisation du matériel vendu (sic) est assurée exclusivement par ses clients.

A contrario, Thibaut Bechetoille, le PDG de Qosmos, une autre société française qui, à l'instar d'Ipoque, équipait ce même Big Brother libyen, et qui équipe également celui utilisé, actuellement, par les Syriens, a piteusement expliqué à l'agence Bloomberg que son conseil d'administration avait bien décidé de cesser ses activités en Syrie, mais que c'était "*techniquement et contractuellement*" compliqué…

A ce jour, quatre autres entreprises occidentales ont été identifiées comme prestataires de services des "*grandes oreilles*" syriennes : Area, une entreprise italienne qui a dépêché, en urgence, des équipes afin d'aider les services de renseignements syriens à identifier les (cyber) dissidents, Utimaco, filiale allemande de l'éditeur d'antivirus britannique Sophos – qui n'était pas au courant qu'Area utilisait ces systèmes en Syrie -, l'allemand Nokia Siemens, dont les équipements de surveillance de l'Internet auraient été transmis à la Syrie par son voisin iranien, et Bluecoat, une société américaine auquel le site reflets.info a consacré de nombreux articles.

On savait, depuis quelques années, que ces armes de surveillance étaient utilisées en Chine ou en Iran notamment, mais il a fallu attendre le printemps arabe, et les traces ou preuves laissées par ces marchands de surveillance (essentiellement occidentaux) en Tunisie, en Egypte, en Libye, à Bahrein ou en Syrie, pour en prendre toute la mesure.

La quasi-totalité de ces marchands d'armes de surveillance se targuent certes d'oeuvrer en matière de "*lawful interception*" (interceptions légales en français) et se vantent de travailler avec des ministères de la défense, de l'intérieur ou des services de renseignement. L'allemand Elaman, lui, va jusqu'à écrire, noir sur blanc, que cela permet aussi d'identifier les "*opposants politiques*" :

> En matière de télécommunications, la notion de "rétention des données" porte généralement sur le stockage de toute information (numéros, date, heure, position, etc.) en matière de trafic téléphonique ou Internet. Les données stockées sont généralement les appels téléphoniques émis ou reçus, les e-mails envoyés ou reçus, les sites web visités et les données de géolocalisation.
>
> Le premier objectif de la rétention des données est l'analyse de trafic et la surveillance de masse. En analysant les données, les gouvernements peuvent identifier la position d'un individu, de ses relations et des membres d'un groupe, tels que des opposants politiques.

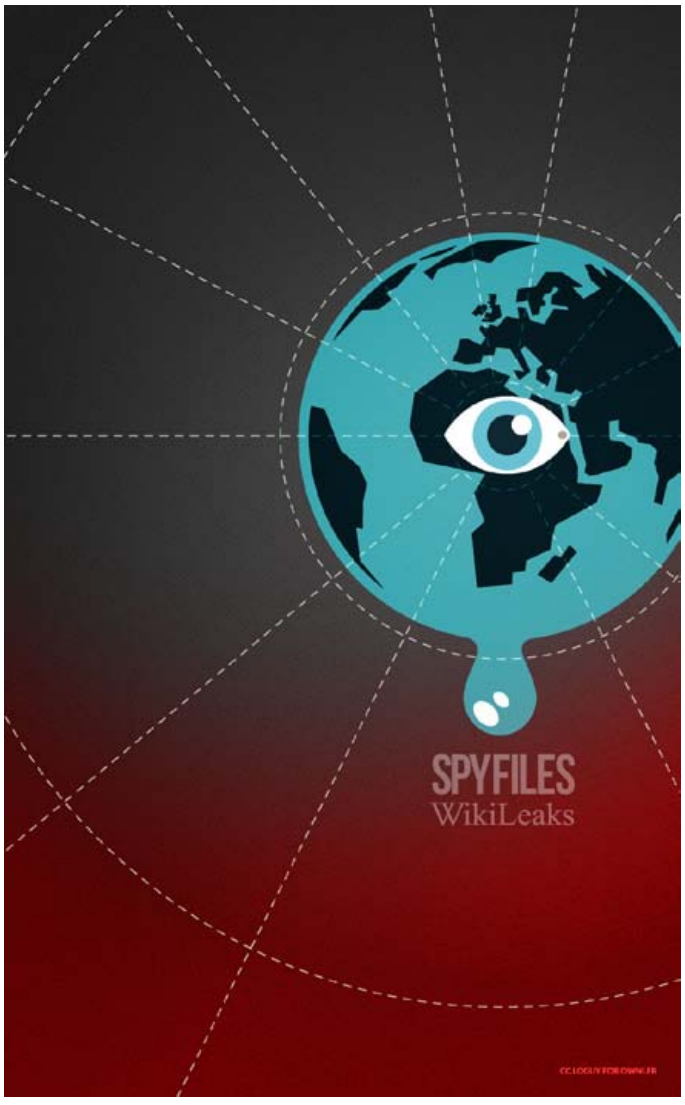
Data Retention
In the field of telecommunications, data retention generally refers to the storage of call related information (numbers, date, time, position, etc.) of telephony and internet traffic. The stored data is usually telephone calls made and received, emails sent and received, web-sites visited and location data. The primary objective in data retention is traffic analysis and mass surveillance. By analyzing the retained data governments can identify an individual's location, their associates and members of a group, such as political opponents.

Initialement développés afin de permettre aux services de renseignements d'espionner en toute illégalité, ces systèmes, outils, logiciels et autres "*gadgets*" conçus pour écouter, surveiller, espionner, traçabiliser ou géolocaliser quelqu'un "*à l'insu de son plein gré*", sont aujourd'hui devenus un véritable marché. Interrogé par

INTERNET MASSIVEMENT SURVEILLÉ

le *WSJ*, Jerry Lucas, l'organisateur d'ISS, expliquait ainsi que, parti de quasiment zéro en 2001, il avoisinerait aujourd'hui les 5 milliards de dollars de chiffre d'affaires, par an.

Les *Spy Files* sont publiés par WikiLeaks à cette adresse.



Retrouvez notre dossier sur les *Spy Files* :

- Mouchard sans frontière

- La carte d'un monde espionné

Retrouvez nos articles sur Amesys.

Retrouvez tous nos articles sur WikiLeaks et *La véritable histoire de WikiLeaks*, un ebook d'Olivier Tesquet paru chez OWNI Editions.

@manhack *(sur Twitter),* jean.marc.manach *(sur Facebook &* Google+ *aussi) .*

Vous pouvez également me contacter de façon sécurisée via ma clef GPG/PGP (ce qui, pour les non-initiés, n'est pas très compliqué). A défaut, et pour me contacter, de façon anonyme, et en toute confidentialité, vous pouvez aussi passer par privacybox.de (n'oubliez pas de me laisser une adresse email valide -mais anonyme- pour que je puisse vous répondre).

Pour plus d'explications sur ces questions de confidentialité et donc de sécurité informatique, voir notamment « Gorge profonde: le mode d'emploi » et « Petit manuel de contre-espionnage informatique ».