COLÈRES D'ARABIE : LE LOGICIEL ESPION

LE 6 SEPTEMBRE 2012 ***JEAN MARC MANACH***

Cruel paradoxe de ce printemps arabe : les défenseurs des droits de l'homme bahreïnis utilisent les réseaux sociaux occidentaux pour manifester ; leurs tortionnaires, des systèmes de surveillance occidentaux pour les espionner.

Au printemps dernier, un Bahreïni exilé à Londres, une économiste britannique résidant à Bahreïn et le propriétaire d'une station service en Alabama, naturalisé Américain, recevaient un e-mail émanant apparemment d'une journaliste d'Al-Jazeera.

Il y était question d'un rapport rédigé par Zainab Al-Khawaja, sur les tortures infligées à Nabeel Rajab, deux des défenseurs des droits de l'homme incarcérés (**et probablement torturés**) à Bahreïn, suivi de cette précision :

"***Merci de vérifier le rapport détaillé en pièces jointe, avec des images de torture.***"

ARABES EN COLÈRE

Le Bahreïn vient de condamner le principal défenseur des droits de l'homme bahreïni à la prison à perpétuité, après ...

----- Forwarded Message -----
From: Melissa Chan <melissa.aljazeera@gmail.com>
To:
Sent: Tuesday, 8 May 2012, 8:52
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.

Quelques jours plus tard, ils recevaient d'autres emails évoquant l'arrestation d'opposants bahreïnis, ou encore l'agenda du roi de Bahreïn, et systématiquement accompagnés de fichiers compressés en pièce jointe, laissant penser qu'il pourrait s'agir de virus informatiques.

Ces e-mails, **transmis** au journaliste de *Bloomberg* **Vernon Silver** (qui a **particulièrement suivi** l'utilisation de technologies de surveillance occidentales par les dictatures arabes), ont ensuite été analysés par deux chercheurs associés au Citizen Lab, un laboratoire de recherche canadien qui étudie notamment les technologies de surveillance politique.

Morgan Marquis-Boire, un ingénieur en sécurité informatique travaillant chez Google, est un **spécialiste (.pdf)** des logiciels espions utilisés par les barbouzes libyens et syriens pour pirater les ordinateurs des cyber-dissidents. **Bill Marczak**, un doctorat en informatique de Berkeley, fait quant à lui partie de **Bahrain Watch**, qui veut promouvoir la transparence au Bahreïn, et dont le site tient la comptabilité des manifestants et civils **tués par les autorités, des armes** (chevrotine, grenades et gaz lacrymogènes) achetées à des entreprises occidentales, et des entreprises de relations publiques anglo-saxonnes **financées** par le régime.

En analysant les e-mails envoyés aux défenseurs des droits de l'homme bahreïnis, les deux chercheurs **ont découvert** un logiciel espion particulièrement perfectionné, utilisant une "*myriade de techniques destinées à échapper à toute forme de détection*", notamment par les antivirus, dont le code n'en mentionnait pas moins, et plusieurs fois, le mot *FinSpy*, la société Gamma International, et le nom de plusieurs de ses responsables.


UN GROS REQUIN DE L'INTRUSION

En partenariat avec WikiLeaks, OWNI révèle le fonctionnement de FinFisher, l'une de ces redoutables armes d'espionnage ...

FinSpy, à en croire cette **proposition de contrat** trouvée en mars 2011 dans l'un des bâtiments de la sécurité égyptienne après la chute du régime Moubharak, est vendu près de 300 000 euros. C'est l'un des produits phares de la gamme d'outils de "*lutte informatique offensive*" commercialisés par FinFisher, filiale de la société britannique Gamma, spécialisée dans les systèmes de surveillance et d'interception des télécommunications. *Owni* avait déjà eu l'occasion de présenter sa **gamme de produits**, et même de réaliser un montage vidéo à partir des clips promotionnels expliquant le fonctionnement de ses logiciels.

A l'occasion de l'opération **SpyFiles**, WikiLeaks et Privacy International avaient révélé que FinFisher faisait partie des **cinq marchands d'armes de surveillance numérique** spécialisés dans les chevaux de Troie. Derrière ce nom, des logiciels espions créés pour prendre le contrôle des ordinateurs qu'ils infectent afin d'activer micro et caméra, d'enregistrer toutes les touches tapées sur le clavier (et donc les mots de passe) ou encore les conversations sur Skype, par messagerie instantanée, par e-mail etc. avant de renvoyer, de façon furtive et chiffrée, les données interceptées via des serveurs situés dans plusieurs pays étranger.

DES CHEVAUX DE TROIE DANS NOS DÉMOCRATIES

OWNI lève le voile sur les chevaux de Troie. Ces logiciels d'intrusion vendus aux États, en particulier en France et en ...

Un autre chercheur en sécurité informatique a ainsi réussi à **identifier** des serveurs utilisés pour contrôler FinSpy, et donc espionner des ordinateurs, en Estonie, Éthiopie, Indonésie, Lettonie, Mongolie, au Qatar, en république tchèque et aux USA, mais également en Australie, ainsi qu'à Dubai, deux des pays placés "*sous surveillance*" dans le classement des **Ennemis d'Internet** émis par Reporters sans frontières.

Dans une **seconde note**, publiée fin août, CitizenLab révèle avoir identifié d'autres serveurs dans 2 des 12 pays considérés comme des "*Ennemis d'Internet*" par RSF : l'un au **Bahreïn**, l'autre contrôlé par le ministère des télécommunications du **Turkménistan**, considéré comme l'un des régimes les plus répressifs au monde.

Les deux chercheurs détaillent par ailleurs le fonctionnement de *FinSpy Mobile*, qui permet d'infecter les iPhone et autres téléphones portables Android, Symbian, Windows et Blackberry, afin de pouvoir espionner les SMS, emails et télécommunications, exfiltrer les contacts et autres données, géolocaliser le mobile, et même d'activer, à distance, le téléphone à la manière d'un micro espion, sans que l'utilisateur ne s'aperçoive de la manipulation.

A Bloomberg, qui l'**interrogeait**, Martin J. Muench, 31 ans, le concepteur de FinFisher, a nié avoir vendu son cheval de Troie à Bahreïn, tout en reconnaissant qu'il pourrait s'agir d'une version de démonstration de son logiciel espion qui aurait été volée à Gamma.

Au *New York Times* , où il **démentait** toute espèce d'implication, expliquant, tout comme l'avait fait Amesys, que ses produits ne servaient qu'à combattre les criminels, **à commencer par les pédophiles** :

> ***Les utilisations les plus fréquentes visent les pédophiles, les terroristes, le crime organisé, le kidnapping et le trafic d'être humain.***

Dans une déclaration publiée moins d'une heure après la publication de la deuxième note de Citizen Lab, Martin J. Muench envoyait un communiqué **mentionné par le *New York Times*** pour expliquer que l'un des serveurs de Gamma aurait été piraté, et que des versions de démonstrations de FinSpy auraient bien été dérobées. Dans la foulée, plusieurs des serveurs utilisés par FinFisher pour permettre aux données siphonnées de remonter jusqu'à leurs donneurs d'ordre ont disparu des réseaux.

Comme notre enquête sur Amesys, le marchand d'armes français qui avait créé un système de surveillance généralisé d'Internet à la demande de Kadhafi (voir ***Au pays de Candy***) l'avait démontré, les logiciels espions et systèmes d'interception et de surveillance des télécommunications ne font pas partie des armes dont l'exportation est juridiquement encadrée (voir **Le droit français tordu pour Kadhafi**). Aucune loi n'interdit donc à un marchand d'armes occidental de faire commerce avec une dictature ou un pays dont on sait qu'il se servira de ces outils pour espionner opposants politiques et défenseurs des droits humains.

Interrogé lors d'un point presse ce 4 septembre, le porte-parole de l'ambassade de France à Bahreïn a **expliqué** avoir "*appris avec déception les décisions de la Cour d'appel du Bahreïn qui confirment les lourdes peines infligées à ces opposants*" :

> ***Le cas de Monsieur Khawaja nous préoccupe tout spécialement. Nous espérons vivement qu'un réexamen de ces condamnations aura lieu lors d'un éventuel pourvoi en cassation.***
>
> ***Nous restons préoccupés par la persistance des tensions dans le royaume de Bahreïn et rappelons notre profond attachement aux principes de liberté d'expression et de droit à manifester pacifiquement.***

Le 23 juillet dernier, François Hollande recevait **très discrètement** le roi du Bahreïn, Hamed ben Issa Al Khalifa, à Paris. Etrangement, cette visite officielle ne figurait pas sur l'agenda du président, et n'a été connue que parce qu'une journaliste de l'AFP a tweeté, interloquée, leur poignée de main sur le perron de l'Elysée. Officiellement, côté français, il a été question de la situation en Syrie, et de la menace nucléaire en Iran. Jean-Paul Burdy, maître de conférences à l'Institut d'Etudes Politiques de Grenoble, **relève** cela dit que l'agence de presse de Bahreïn avance que de nombreux autres sujets ont été abordés, y compris la coopération entre les deux pays en matière de lutte contre "*toutes les formes de terrorisme et d'extrémisme*", ainsi que de "*l'importance de la promotion de la démocratie et des droits humains*".

Au lendemain de cette visite, la presse bahreïnie salue en "*une*" l'accord de coopération signé entre la France et le Bahreïn, et visant à mettre en place, **souligne** *Le Monde*, des réformes dans les secteurs de la presse et de la justice, ce qui fait bondir l'opposition :

> ***La France prend le risque de devenir la complice des tours de passe-passe de la monarchie, s'indigne Abdel Nabi Al-Ekry, un vieil opposant de gauche. Comment peut-elle prétendre réformer la justice bahreïnie alors que 21 des dirigeants de l'opposition croupissent en prison, au terme de procès bidons ? C'est décevant de la part d'un socialiste comme Hollande.***

L'agenda de l'Élysée, **dépiauté par Rue89**, révèle qu'"*au moins six autres représentants de pays autoritaires ou franchement dictatoriaux ont été reçus par François Hollande depuis son élection*", alors même que François Hollande avait pourtant **promis** de "*ne pas inviter de dictateurs à Paris*". Cinq d'entre eux sont soupçonnés d'avoir voulu acheter le système *Eagle* de surveillance généralisé de l'Internet conçu par la société française Amesys à la demande de Kadhafi, et dont le nom de code, en interne, était *Candy*, comme bonbon, en anglais.

AU PAYS DE CANDY

Candy : c'est le nom de code de l'opération organisée depuis la France et consistant à aider le régime de Kadhafi à ...

À la manière d'un mauvais polar, les autres contrats négociés par Amesys portent en effet tous un nom de code inspiré de célèbres marques de friandises, bonbons, chocolats, crèmes glacées ou sodas : "*Finger*" pour le Qatar (sa capitale s'appelle… Doha), "*Pop Corn*" pour le Maroc, "*Kinder*" en Arabie Saoudite, "*Oasis*" à Dubai, "*Crocodile*" au Gabon, et "*Miko*" au Kazakhstan, dont le dictateur-président est le seul à ne pas avoir encore été reçu par François Hollande, quand bien même il utiliserait par contre le système FinSpy de FinFisher.

Depuis le **classement sans suite** de la plainte déposée à l'encontre d'Amesys, à la veille de la présidentielle, le nouveau gouvernement ne s'est jamais prononcé sur cette affaire, par plus que sur l'implication de Claude Guéant, Brice Hortefeux et des services secrets français, non plus que sur une éventuelle interdiction, à l'exportation, de la commercialisation des armes de surveillance numérique.

Pour se prémunir de ce genre de chevaux de Troie, Citizen Lab rappelle tout d'abord que ces logiciels espions ne peuvent être installés que si le pirate a un accès physique à la machine (ordinateur ou téléphone portable), ou si la victime accepte d'ouvrir une pièce jointe ou une application que les espions prennent cela dit généralement soin de maquiller de sorte qu'elle émane d'une personne ou institution de confiance. Les

PETIT MANUEL DE CONTRE-

chercheurs recommandent également de régulièrement mettre à jour systèmes d'exploitation et logiciels -à commencer par l'anti-virus, les suites Office, Acrobat, Java, Flash, en vérifiant que les mises à jour proviennent de sources légitimes et de confiance-, mais également d'installer des fonds d'écran protégés par mot de passe (pour éviter à un intrus de profiter d'une pause pipi pour pirater votre système), et enfin d'utiliser si possible des mots de passe forts, et des logiciels de chiffrement. Voir aussi, à ce titre, notre **petit manuel de contre-espionnage informatique**.

ESPIONNAGE INFORMATIQUE

GPS, téléphones portables, logiciels espions: les outils de la surveillance se démocratisent. Conseils utiles pour s'en ...

4 pings

"Colères d'Arabie, le logiciel espion": FinFisher, FinSpy et Gamma International « Wikileaks Actu le 9 septembre 2012 - 2:14

[...] http://owni.fr/2012/09/06/coleres-darabie-le-logiciel-espion/ Share this:TwitterFacebookPlusEmailPrintJ'aime ceci:J'aimeSoyez le premier à aimer ceci. [...]

"Colères d'Arabie, le logiciel espion": FinFisher, FinSpy et Gamma International « Actualités Alternatives « Je veux de l'info le 9 septembre 2012 - 3:32

[...] Source: http://www.wikileaks-forum.com/index.php/topic,14457.0.htmlhttp://owni.fr/2012/09/06/coleres-darabie-le-logiciel-espion/ [...]

Sete'ici - Les deux pieds en balade, les yeux ouverts (des fois) » Blog Archive » Les liens de la semaine le 23 septembre 2012 - 11:47

[...] Bahrein, silence, on tire dans la foule. On espionne aussi. On [...]

Colères d'Arabie, le logiciel espion » : FinFisher, FinSpy et Gamma International l seponsors le 26 octobre 2012 - 14:18

[...] Source: http://www.wikileaks-forum.com/index.php/topic,14457.0.html http://owni.fr/2012/09/06/coleres-darabie-le-logiciel-espion/ [...]