Le 10 juin 2011
Amesys
Olivier Tesquet

LA LIBYE SUR ÉCOUTE FRANÇAISE

En bon potentat qui se respecte, Mouammar Kadhafi a mis en place une architecture de surveillance des télécommunications particulièrement sophistiquée. Et pour l'y aider, il a fait appel à deux sociétés françaises.

Selon les confidences d'acteurs de la sécurité informatique, une entreprise française, Amesys, aurait vendu et déployé dès 2007 des technologies d'interception à la Libye du colonel Kadhafi. Dans le jargon, ces outils de surveillance très sophistiqués ont un nom: le DPI, pour "Deep Packet Inspection", soit une technologie permettant à un opérateur télécom d'analyser son réseau en profondeur. A tel point que ces solutions peuvent même aller fouiner dans votre courrier électronique ou dans vos messageries instantanées.

A travers son interface Eagle, présenté comme *"un système d'interception électronique permettant à un gouvernement de contrôler toutes les communications qu'elles entrent ou sortent du pays",* Amesys aurait équipé Mouammar Kadhafi. Voilà pour l'argument commercial. Fondée en 1979, cette structure a été rachetée en 2009 par Bull, pionnier tricolore de l'informatique. Signe d'une évolution assez nette en termes de stratégie, c'est le président d'Amesys (260 employés), Philippe Vannier, qui a pris la tête de Bull (8 600 salariés) en mai 2010. A la fin du mois d'avril, ce dernier commentait le bilan de sa société pour le premier trimestre 2011, et apportait cette précision intéressante:

> L'accueil de nos nouvelles offres en sécurité nous ouvre également des perspectives prometteuses même si le contexte politique dans certains pays ralentit les prises de décision. Les événements survenus au Proche et Moyen-Orient ont impacté l'activité commerciale de la division Security Solutions.

Joint au téléphone, Olivier Boujart, responsable de l'export, déclare *"ne pas avoir connaissances des activités du groupe [en Libye]"* mais ne les dément pas. Quand on lui demande de préciser les clients étatiques d'Amesys, il oppose un refus poli:

> Nous devons préserver nos prés carrés. Nous n'avons pas l'habitude de divulguer ce type d'informations.

Au moment de décrire le système Eagle, M. Boujart se veut rassurant: *"Nous parlons d'outils permettant d'analyser la qualité des réseaux"*. Un discours qui agaçe profondément Bluetouff, un blogueur et hacker qui s'est récemment lancé dans une vaste radiographie du DPI sur le site Reflets.info, qu'il coanime. Il répond par l'ironie, et remet en cause l'honnêteté des marchands de DPI:

> Il est de notoriété publique que les plugins de Gmail ou Hotmail sont fait pour manager les réseaux. Comment se fait-il que cette entreprise développe en pétaoctets (1 000 000 000 000 000 octets, ndlr) alors que le stockage ne sert à rien

pour manager des réseaux? C'est pour se prémunir contre une panne de Google? (rires)

Signature du Premier ministre

Plus surprenant encore, les commerciaux d'Amesys estiment que le GLINT par exemple, un *"outil stratégique d'interception au niveau national basé sur la technologie Eagle"*, n'a pas besoin de passer devant une commission CIEEMG, qui statue sur l'exportation de matériel militaire, pour être vendu à l'étranger. *"Ce ne sont pas des armes de guerre, tout de même"*, se défend Olivier Boujart. Pourtant, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) confirme que les armes informatiques sont régies par les mêmes règles que la logistique plus traditionnelle. Pour ajouter à la confusion, Amesys est bien enregistré sur le portail de l'armement du ministère de la Défense. Mais sur d'autres secteurs de son activité.

Le GLINT permet de surveiller les télécommunications à l'échelle d'un pays

De son côté, le code pénal est pourtant clair. Les technologies d'écoutes et d'interception légale doivent recevoir la signature du Premier ministre pour sortir de France:

> [Est puni d'un an d'emprisonnement et de 45 000 euros d'amende] la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par décret en Conseil d'Etat, d'appareils conçus pour réaliser les opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 [le fait de volontairement porter atteinte à l'intimité de la vie privée d'autrui en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel]

Spécialité française

Mais Amesys n'a pas le monopole de la surveillance. Thales serait également concerné. Un article du Figaro a récemment levé le voile sur les implications hexagonales dans ce genre de pratiques. Le 25 avril, au détour d'un article sur les écoutes légales, le quotidien lâche cette information étonnamment peu relayée:

> [Développée par Thales en France], cette technologie a été commercialisée par la France en 2008 en Libye, "sans les garde-fous de protection des citoyens qu'il y aura dans l'Hexagone", précise un proche du dossier.

Approchée trois fois pour réagir à cette allégation, la direction de Thales n'a pas donné suite à notre demande. Ce qu'on sait, en revanche, c'est qu'un an plus tôt, Alcatel-Lucent a signé un accord de transfert de ses activités de sécurité vers… Thales. La même année, Kadhafi attribue un vaste projet de déploiement de la fibre optique à Alcatel. *"Il consiste en la mise en place d'un backbone (une dorsale) reliant toutes les villes libyennes sur près de 8 000 kilomètres, pour un coût global estimé à 160 millions d'euros"*, détaille Faycel Saad, un consultant tunisien spécialisé dans les télécommunications. Le projet est placé sous l'égide de la Libyan Telecom & Technology, le principal fournisseur d'accès libyen, présidé par Mohammed Kadhafi, le fils ainé du Guide de la Révolution.

LA LIBYE SUR ÉCOUTE FRANÇAISE

Dès lors, on comprend mieux la structure du réseau libyen, si centralisé que le président de la Jamahiriya n'a eu aucun mal à le couper d'Internet à la mi-février. Dans un article publié en avril, le Wall Street Journal détaille le dispositif de contrôle mis en place par les autorités:

> « Kadhafi avait bâti son infrastructure de télécommunications pour qu'elle se déploie depuis Tripoli – routant tous les appels à travers la capitale et lui donnant ainsi qu'à ses agents de renseignement un contrôle total sur les téléphones et Internet.

Fin janvier, Narus, une filiale du géant de l'aéronautique Boeing, avait été vivement critiquée pour avoir fourni de tels logiciels au gouvernement égyptien d'Hosni Moubarak, qui s'en était abondamment servi pour surveiller sa population et ses dissidents. Après le scandale de Nokia et Siemens en Iran, un lobbying efficace a été entrepris aux Etats-Unis en 2009. L'objectif: faire interdire l'exportation de technologies fondées sur le Deep Packet Inspection. Et en France? Chez les hackers, on a coutume de dire que la France exporte trois spécialités: les droits de l'homme, le bon vin… et le DPI.

Crédits photo: Flickr CC François @ Edito.qc.ca, Abode of Chaos