#OpSyria S04E01 : The Iron Strike

Aujourd'hui est un jour très spécial, c'est le jour où Qosmos présente à San Francisco sa formidable technologie de surveillance, avec une grande nouveauté, les sondes DeepFlow®. Encore une technologie duale, présentée pour vous assurer « *de la sécurité* » et que Qosmos n'aura, une fois de plus, probablement aucun scrupule à vendre à des fins de surveillance, parfois à des régimes autoritaires, ou des régimes notoirement violents, comme celui de Bachar El Assad.

Pour les syriens en revanche, c'est un jour comme les autres. Ils seront des dizaines à tomber sous les balles et les bombes, identifiés et localisés grâce à des technologies américaines ou européennes. Internet, comme les émissions de téléphones satellites, sont de bons moyens de « *loger* » les opposants au régime de Bachar El Assad. Les technologies qui permettent de surveiller ces moyens de communication et dont nous dénonçons vigoureusement depuis des mois la vente au régime syrien sont en place, bien en place… et nous les soupçonnons même, aujourd'hui, d'avoir été renforcées.

AreaSPA, entreprise d'origine italienne a été prise la main dans le pot de confiture il a quelques semaines par Bloomberg. Area SPA est un intégrateur chargé du déploiement d'une solution globale de surveillance. Le matériel et les logiciels intégrés par Area SPA sont américains (NetAPP), Français (Qosmos), Allemands (Utimaco).

Aux USA, l'embargo sur la Syrie a conduit le département d'Etat américain à enquêter. Après avoir nié, BlueCoat a finalement été condamné une lourde (mais indolore) amende, pour avoir contourné l'embargo sur la Syrie. C'est Reflets qui avait révélé ce business, en allant jusqu'à publier, en cloture de la saison 3 de l'#OpSyria, plus de 54Go de journaux de connexion attestant de la censure syrienne opérée grâce à ce matériel américain. En France, on continue à se cacher derrière son petit doigt, à l'image de Qosmos qui émettait des réserves quand à la « *faisabilité* » de son retrait du marché syrien.

> *When Bloomberg News contacted Qosmos, CEO Thibaut Bechetoille said he would pull out of the project. "It was not right to keep supporting this regime," he says. The company's board decided about four weeks ago to exit and is still figuring out how to unwind its involvement, he says. The company's deep- packet inspection probes can peer into e-mail and reconstruct everything that happens on an Internet user's screen, says Qosmos's head of marketing, Erik Larsson.*

Qosmos dont le dirigeant que nous avions interviewvé quelques mois auparavant jurait devant tous les grands dieux ne pas vendre à des régimes autoritaires… Il s'est bien foutu de nous le Thibaut Bechetoile. Et pas qu'une fois.

Si vous ne l'avez pas encore visionné, regardez et écoutez attentivement ceci.

#OpSyria S04E01 : The Iron Strike

Ce cynisme appelait donc une réponse. *Reflets* n'a rien lâché et ne lâchera rien.

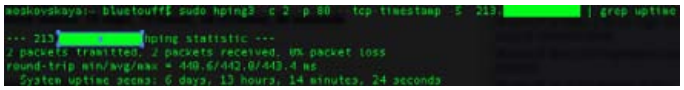
Aujourd'hui est un jour spécial donc. Il marque le lancement de la Saison 4 de l'#OpSyria menée conjointement par Telecomix, FHIMT et *Reflets*. La saison 4, baptisée IRON STRIKE se déroulera en 3 épisodes (peut-être 4) :

- Exploration et collecte
- Identification des matériels et acteurs
- Communication publique
- OPTION : Frappe stratégique du système de surveillance

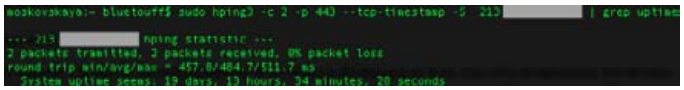
IRON STRIKE se veut une réponse mesurée, à la mise en place d'équipements de surveillance électronique en Syrie. Ces outils de répression font de vrais morts en Syrie. Il aura fallu des milliers de morts, des centaines d'activistes, de blogueurs, de journalistes tombés sous les balles, pour que nos démocraties daignent enfin mettre leur nez dans ce business nauséabond… Et pourtant, tout continue comme avant. De nouveaux équipements ont fait leur apparition à la Syrian Computer Society (SCS), un fournisseur d'accès Internet d'un genre un peu particulier créé par Bachar El Assad lui même en 2001. **Ils ont fait leur apparition alors que le monde entier savait que la Syrie massacrait l'opposition en utilisant ces outils**. Le système autonome de SCS concentre probablement la majeure partie des moyens de surveillance. Certains, actifs, sont visibles, mal sécurisés, mis en place par des admins d'une incompétence crasse et probablement aidés par des commerciaux d'Area SPA (vous auriez pu leur envoyer des techniciens quand même…).

Nous vous en montrons un exemple de ces équipements ici :

Ici un proxy BlueCoat SG400 qui semble avoir été activé (ou rebooté) il y a moins d'une semaine :

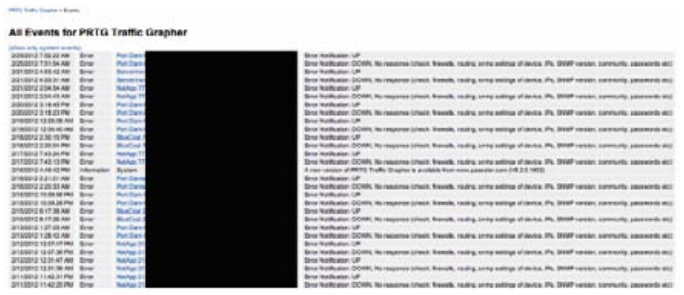


Et ici, un NetAPP semblant avoir été activé (ou rebooté) il y a 19 jours :



Not shown: 989 closed ports PORT STATE SERVICE VERSION 22/tcp filtered ssh 23/tcp filtered telnet **80/tcp open http-proxy NetApp NetCache http proxy 6.0.7** 135/tcp filtered msrpc 139/tcp filtered netbios-ssn 1720/tcp filtered H.323/Q.931 1723/tcp filtered pptp 2000/tcp filtered callbook 4444/tcp filtered krb524 5060/tcp filtered sip **8080/tcp open http-proxy NetApp NetCache http proxy 6.0.7**

Et deux photos souvenir…



Ça marche bien mais pas top…

Ci-dessous un BlueCoat activé fin Août, quelques jours après que nous ayons révélé l'exportation frauduleuse de ces équipements en Syrie

#OpSyria S04E01 : The Iron Strike

La grappe de machines que nous avons identifié est composée de 6 proxys BlueCoat et de 4 NetApp. Sur le réseau de la SCS, elle est baptisée Fast Iron Caches et elle a été activée à la fin du mois d'août. Elle connait quelques ratés et n'est pas du tout stabilisée et encore moins sécurisée, mais elle est bien en production. Les équipements, le nom donné à ce petit monde, nous font penser que nous avions parfaitement raison quand nous soupçonnions BlueCoat d'être au coeur d'une attaque par Man In The Middle de grande envergure. Area SPA a mené sa mission à bien et vous vous doutez bien que si nous nous apercevons que cette dernière assure toujours le support et la formation des personnels surveillants, comme c'est l'usage dans ces contrats, nous publierons… tout.

Cher Bachar,
nous lisons par dessus ton épaule,
nous surveillons les battements de ton coeur de réseau,
les frappes de clavier de tes tocards d'admins,
les coups de main des entreprises qui t'aident à mettre en place tes outils de cyber répression…

Nous te surveillons, nous murmurons à l'oreille des machines des opérateurs de ta cyber-milice, nous connaissons même les goûts de l'un d'entre eux pour les enfants prépubères.

From the Internetz, with love.