L'OPÉRATION EN SYRIE VUE DE L'INTÉRIEUR

LE 14 SEPTEMBRE 2011 ***PIERRE ALONSO***

KheOps est l'un des hackers de l'opération menée en Syrie pour contourner la censure. Il revient sur la genèse du projet, son déroulement, les découvertes surprenantes, en insistant toujours sur la formation et les conseils apportés aux internautes syriens.

Dans la nuit du 4 au 5 septembre, le même message s'affiche pendant quelques minutes sur les navigateurs en Syrie : *"Vos activités sur Internet sont surveillées. Des outils existent pour échapper à cette surveillance."* Plusieurs activistes travaillent depuis quelques mois sur cette opération.

Le but : permettre aux Syriens de pouvoir communiquer vers l'extérieur et à l'intérieur sans se mettre en danger. Telecomix est derrière l'opération. L'un de ces hacktivistes, connu sous le pseudonyme KheOps, a accepté de raconter #OpSyria à OWNI.

En quoi l'opération consiste-t-elle ?

L'opération a débuté il y a deux mois avec une équipe de moins de 10 personnes. J'étais le seul Français, il y avait des Allemands, des Suédois… Le point de départ est la frustration face à l'absence d'informations sur ce qu'il se passe en Syrie. Elle est menée par Telecomix, mais je parle en mon nom propre, pas au nom de Telecomix.

L'opération est découpée en plusieurs parties. La première a été la plus critique. On voulait atteindre les Syriens et rentrer en contact avec eux, mais on n'avait aucun contact là-bas. On était un peu désemparé. Le message qu'on voulait leur faire passer était simple : leurs communications sont surveillées et écoutées. Certains s'en doutent mais nous savons précisément quelles méthodes sont utilisées.

La partie technique n'était pas très poussée. Il s'agissait d'installer des ponts sur TOR[1] et des VPN[2]. On a commencé à scanner le réseau TCP/IP pour déterminer quelles machines étaient responsables des blocages. Le port 80 est contrôlé par la censure de l'Etat syrien. D'autres sont carrément bloqués. Il a fallu scanner l'ensemble des ports pour déterminer ceux qui ne le sont pas et faire passer le traffic IP dans un VPN. Pour ce faire, il y a eu une opération de piratage pur. Nous avons dû utiliser des machines à l'intérieur du pays pour faire des tests de connexion et observer comment le système réagissait là-bas. Mais il faut garder ce système opérationnel de façon continue parce qu'il peut y avoir des changements. Après ce diagnostic, nous avons mis en place des VPN et des ponts TOR.

> **Qu'avez-vous expliqué aux internautes syriens une fois en contact avec eux ?**

Au-delà des questions techniques, l'opération comprenait toute une partie de conseil et d'accompagnement. L'aspect humain était central dans cette opération. Les débutants n'arrivaient pas à installer les outils qu'on mettait à leur disposition. Des conseils simples permettent de faire beaucoup pour éviter la surveillance du régime : naviguer en https, vérifier l'identité des certificats, apprendre ce qu'est un finger print SSL et lesquels sont les bons.

Des attaques récentes ont été menées via de faux SSL, y compris sur Facebook. On a aussi eu peur que se produise un scénario comme en Iran il y a quelques jours. Un faux certificat a permis à de piéger **300 000 utilisateurs de gmail**. Mais l'essentiel de la tâche consiste à rassurer et à conseiller les utilisateurs syriens.

> ***On a conseillé des choses très simples mais très importantes pour se prémunir contre la censure.***

Les internautes, en Syrie mais aussi en France, ne connaissent pas toujours ces pratiques comme utiliser TOR ou naviguer en https. Après, il y a aussi beaucoup de bon sens ! Ne pas révéler son identité, ne pas avoir de conversations en clair sur ses activités militantes.

Sur la page apparue sur l'ensemble des navigateurs dans la nuit du 4 au 5 septembre figuraient plusieurs outils : un lien vers un serveur IRC, un **plugin pour Firefox** permettant de naviguer en https, des serveurs **Mumble** (un service de VOIP), **Pidgin** avec le plugin OTR((Off-the-Record messaging permet de chiffrer les communications. **En savoir plus.**)).

Comment ont réagi les internautes syriens ?

Autant on avait peu de réactions après l'envoi des mails le 11 août, autant il y a eu un afflux massif le 4 septembre. Il faut dire qu'on leur avait moins laissé le choix… Beaucoup étaient étonnés et se demandaient où ils étaient. Dans l'ensemble, on a eu peu de réactions agressives. La première question était souvent :

> ***"Est-ce qu'il y a des gens du gouvernement ici ?"***

Une personne soutenant explicitement le gouvernement a essayé de nous prendre par défaut. Il prétendait que ce système n'était pas sécurité, qu'on n'avait aucune légitimé pour mener cette action. Mais globalement, c'est la surprise qui a dominé. Et puis, beaucoup voulaient savoir comment installer TOR.

Cette nouvelle phase est donc un succès ?

C'est difficile de parler de succès. Techniquement, ça fonctionne. Ce que nous avons développé est réutilisable pour échanger à l'intérieur du pays ou vers l'étranger. L'utilisation de TOR a l'air de se développer, le bouche-à-oreille prend le relais : ceux qui l'ont installé diffusent à leurs connaissances. Quelque chose a changé. Mais la fréquentation irrégulière reste une source de frustration. On peut faire mieux, faire plus.

Avez-vous rencontré des difficultés pour rentrer dans le réseau syrien ?

Non, pas du tout ! C'était un gruyère. Nous n'avons pas forcé dans cette direction parce que notre action n'était pas purement informatique mais visait l'humain. On a donc pas creusé très loin la possibilité de pirater, mais on a quand même vu des trous béants.

On a aussi une idée assez précise de la façon dont ils surveillent les internautes. On a l'impression qu'ils ont branché simplement les proxies filtrants et appuyé sur le bouton. Beaucoup de matériel est utilisé, ils sont équipés massivement mais ils ont vraiment l'air d'être des amateurs.

> **Dans le réseau syrien, avez-vous fait des découvertes ?**

On a trouvé la trace d'un boîte californienne, Bluecoat. 20 à 30 machines sont utilisées pour le filtrage, mais on ne sait pas comment elles sont arrivées là. Elles y sont, c'est tout ce qu'on peut dire.

Retrouvez sur Reflets.info le récit détaillé de #OpSyria par KheOps.
Crédits Photo FlickR CC : by-nc-sa **CharlesFred**

1. TOR est un réseau mondial décentralisé de **routeurs** qui permet d'anonymiser tout échange sur Internet. **En savoir plus.** [↩]
2. *Virtual Private Network* est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. **En savoir plus**. [↩]

3 pings

La revue du web | MagZcanada 07062011-01 le 16 septembre 2011 - 16:41

[...] Piratage : l'opération en Syrie vue de l'intérieur [...]

La revue du web | iCoaching 26062011-01 le 16 septembre 2011 - 17:05

[...] La revue du web septembre 16, 2011By magzadminPiratage : l'opération en Syrie vue de l'intérieur [...]

[Solidarité avec la ZAD! Attaquons-les de tous les côtés!] Des hackers atterrissent à Notre-Dame-des-Landes | blog du collectif de lutte contre l'aéroport de Notre Dame des Landes le 7 novembre 2012 - 11:54

[...] tout avec une connexion pourrie, en attendant que Kheops, le grand blondinet sorti de son anonymat lors des opérations du Printemps arabe, mette en place d'un réseau WiFi meshé. Pour l'instant, les attaques DDoS et le défaçage, [...]