

# RSF HACKE LA CENSURE

LE 23 JUILLET 2012 SABINE BLANC ET OPHELIA NOOR

Samedi, un hackaton était organisé à la Cantine à Paris pour tester la sécurité de la future plate-forme de diffusion de contenus censurés de Reporters sans frontières, WeFightCensorship. Une expérience qui illustre une fois de plus les liens fructueux que les ONG ont commencé à tisser avec les hackers.



Ils lui ont fait mal, ils lui ont fait mal, les hackers à la future plate-forme WeFightCensorship de Reporters sans frontières (RSF). Ce samedi, ils étaient conviés par l'ONG à un **hackaton organisé à la Cantine** à Paris pour tester la sécurité de l'outil. Vu l'enjeu, WeFightCensorship a intérêt à viser un système sûr au maximum. Lucie Morillon, en charge du bureau des nouveaux médias à RSF, présente le but du projet :



*Jean-François Julliard, notre ancien secrétaire général, souhaitait mettre en avant le travail des gens qui ont été arrêtés ou ont été poursuivis pour s'être exprimé, en leur donnant une tribune, avec la traduction des textes censurés. Nous ferons remonter des documents en s'appuyant sur notre réseau.*



LA CARTE D'UN MONDE D'ESPIONS

OWNI en partenariat avec Wikileaks vous propose cette carte interactive permettant d'identifier toutes les sociétés à ...

Bien sûr, il peut aussi s'agir de photos ou de vidéos. Il sera aussi possible de soumettre de façon anonyme et sécurisée des contenus, dont la fiabilité sera vérifiée. Que les contenus proviennent de journalistes professionnels ou amateurs n'a pas d'importance : Internet a brouillé les frontières entre les deux, RSF l'a bien intégré et défend les deux du moment qu'ils diffusent de l'information.

Et quelle que soit leur origine, les documents mis en ligne bénéficieront d'une mise en contexte pour que le grand public comprenne les risques que prennent des blogueurs, par exemple, pour simplement exercer leur esprit critique contre leur gouvernement.

Par un jeu de sites miroirs, les contenus trouveront autant d'échos supplémentaires. Si un miroir tombe ou est bloqué, il y en aura toujours un autre en ligne et

accessible.

## Jouer sur l'effet Streisand

WeFightCensorship veut "rendre caduque la censure en jouant sur l'effet Streisand" , détaille Grégoire Pouget, webmaster de RSF. **L'effet Streisand** est un des grands principes qui régissent l'Internet : plus on essaye de censurer un contenu en tentant de le supprimer, plus il est dupliqué. L'actrice Barbara Streisand en avait fait l'expérience en essayant de faire retirer des photos de sa maison, donnant son nom à ce phénomène.

Le système doit donc assurer une sécurité maximale aux utilisateurs. RSF a fait appel à **Linagora**, son partenaire habituel, spécialisé dans l'open source, pour la développer. William Bonnet, le directeur technique de Linagora, a détaillé la longue liste des risques. Aperçu non exhaustif :

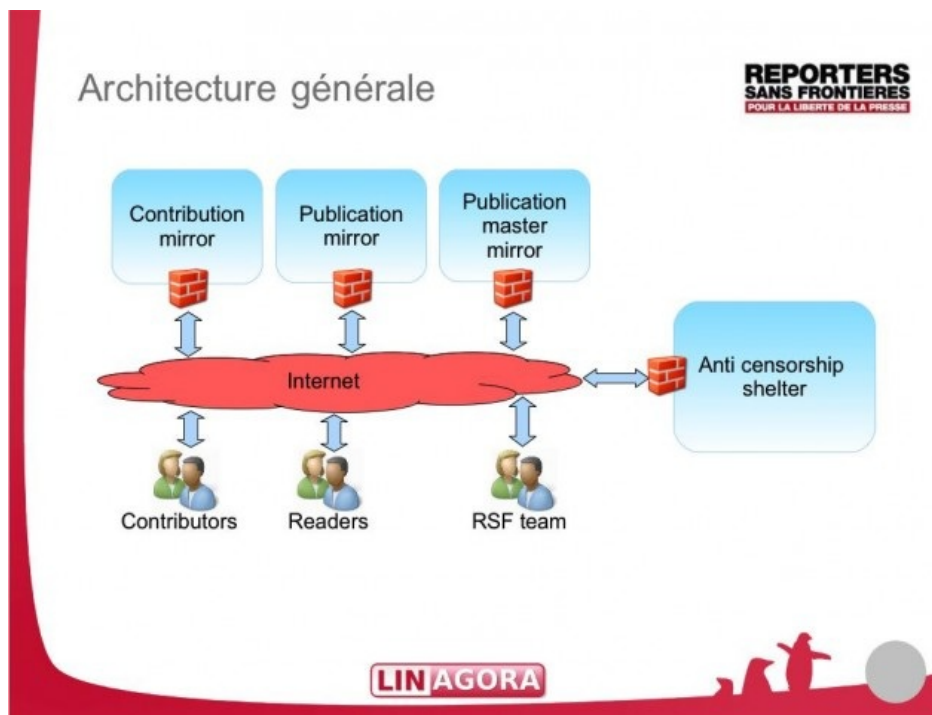


**Il faut se prémunir contre l'identification des miroirs et la captation des données ou le blocage ; il faut diffuser du contenu en limitant le risque d'altération comme les fausses informations ou le défaçage ; protéger l'anonymat en ne gardant pas d'informations qui permettent de remonter aux contributeurs...**



## Architecture résiliente

C'est donc toute la palette des techniques de signature et de chiffrement qui a été utilisée, comme par exemple "le chiffrement des données de bout en bout" a-t-il détaillé. L'architecture globale a été conçue pour être au maximum résiliente :

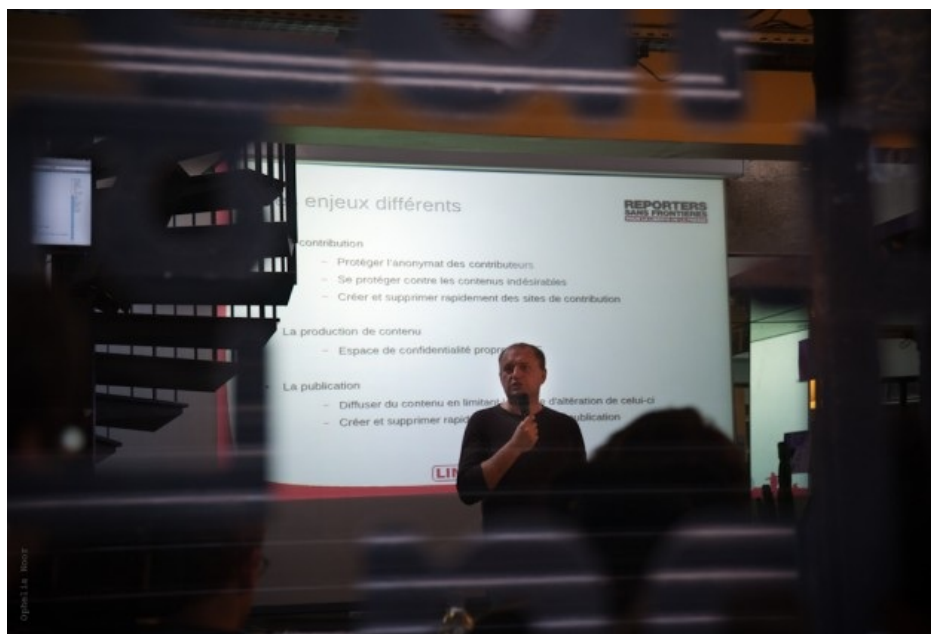


C'est ce système complexe que les hackers ont été conviés ce samedi à passer à l'épreuve du feu. Et la bête semble bien robuste. Dès juin, la communauté avait été invitée à lui faire passer un premier crash-test, qui avait permis de colmater quelques belles brèches. L'ensemble tient maintenant bien la route, se réjouit fo0, membre du cluster **Telecomix** qui s'est illustré pendant les révolutions arabes en aidant les internautes à communiquer, et de façon sécurisée :



***Le système est plus stable, même s'il n'est pas encore prêt à être mis en production demain, il ne présente pas vraiment de grosses failles, rien qui ne mette en danger la sécurité des gens. Cette séance permet à Linagora de se projeter à long terme. Nous avons juste eu un problème d'upload de fichier, il était trop lourd et le système a bugué.***

***Nous avons aussi pu réfléchir à quelques idées en cas de scénario d'attaque. Il faudrait par exemple essayer de faire passer un fichier infecté à travers toute la chaîne de process, un virus qui passe l'anti-virus.***



Car l'enjeu majeur est surtout de savoir réagir en cas de problèmes, qui ne manqueront pas de surgir. William Bonnet est aussi satisfait de cette journée qui a permis de renforcer les liens avec les hackers :



***La journée s'est très bien passée, nous avons pu échanger des informations avec les testeurs.***



L'expérience illustre une nouvelle fois la relation fructueuse que les ONG ont commencé à nouer avec cette communauté encore trop souvent mal vue, à tort. WeFightCensorship est d'ailleurs un bébé hacker, a rappelé Grégoire Pouget :



***Il y a un avant et un après WikiLeaks, on les a soutenus d'ailleurs au début, avant que l'organisation ne connaisse des problèmes en ne prenant pas assez de précautions, ils avaient divulgués des noms. Nous nous en sommes inspirés, avec le côté ONG : le contrôle est plus important, l'idée n'est pas de produire des contenus bruts. Nous ne publierons rien sans l'accord de l'auteur pour ne pas aggraver la situation.***



## Sensibiliser encore plus les journalistes

Le rapprochement entamé depuis 2010 avec cette communauté est logique, pour peu que l'on connaisse ses fondamentaux : non, ce n'est pas le piratage de carte bleue, mais la libre circulation de l'information. Et sa marotte pour la sécurité s'avère bien précieuse.

Parmi les collaborations notables, les **J\_Hack**, des échanges entre journalistes, activistes et hackers. Cet hiver, une journée d'ateliers avait été montée pour apprendre aux journalistes à sécuriser leur connexion.

Des journalistes qui ont bien le réflexe de prendre un gilet pare-balles mais pas forcément **une clé PGP** pour chiffrer leurs communications, a regretté Lucie Morillon, alors que le contexte se dégrade :



**LES HACKERS FORMENT LES JOURNALISTES**

**La semaine dernière, hackers et journalistes avaient rendez-vous. L'objectif : apprendre à sécuriser ses connexions à ...**



***WeFightCensorship servira aussi d'espace dédié à la sécurité, avec une boîte à outils. Notre grande inquiétude, c'est la banalisation de la surveillance. Les SpyFiles de WikiLeaks ont montré l'étendu de ce marché.***



D'ici son lancement début octobre, WeFightCensorship va encore peaufiner sa carapace, en profitant des retours d'expérience. *"Ce hackaton n'est qu'une étape dans la vie du système"*, poursuit William Bonnet. Les menaces évoluent, et les abris aussi : quand il s'agit de sécurité, c'est le hackaton continu. Le directeur technique conclut :



***C'est à la fois une grande responsabilité et une grande fierté.***



L'application à tester est accessible à ces deux adresses :

<http://miroir-prim-pub-01.wefightce...> pour la partie publication

<http://miroir-contrib-01.wefightcen...> pour la partie contribution

Texte Sabine Blanc

Photos Ophelia Noor pour *Ovni*

**MWI**

le 24 juillet 2012 - 8:54 &bullet; SIGNALER UN ABUS - PERMALINK



<http://www.voltairenet.org/spip.php?>

[page=recherche&lang=fr&recherche=reporters+sans+fronti%C3%A8res](http://www.voltairenet.org/spip.php?page=recherche&lang=fr&recherche=reporters+sans+fronti%C3%A8res)

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

**QDSFMLQDJFMLQKJ**

le 25 juillet 2012 - 16:55 &bullet; SIGNALER UN ABUS - PERMALINK



*On dirai du wikileaks tout mou. RSF caca !*

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

**1 ping**

Reporters Sans Frontières lance WeFightCensorship, un abri anti-censure |  
LesNews le 23 juillet 2012 - 19:25

[...] Sources RSF et Ovni [...]