ntre hackers et journalistes à La Cantine. Avec la participation de RSF.org ; TELECOMIX, Reflets.info, Silicon Maniacs. - (cc) Ophelia Noor pour Owni Au rvie en milieu numérique" : - Comment protéger ses communication en ligne ? Okhin (Telecomix) - Comment surfer anonymement ? Kitetoa (Reflets.info) onnées ? Stephane Koch (RSF) - Quels sont les protections élémentaires des sources ? (RSF)

LES HACKERS FORMENT LES JOURNALISTES

LE 4 MARS 2012 ***OPHELIA NOOR ET PIERRE ALONSO***

La semaine dernière, hackers et journalistes avaient rendez-vous. L'objectif : apprendre à sécuriser ses connexions à l'heure où la surveillance des communications change d'échelle et se généralise. Retour sur les quatre ateliers avec les formateurs.

Comprendre le fonctionnement du réseau. Sécuriser son ordinateur. Chiffrer ses communications et ses données sensibles. Adapter sa solution de sécurité au contexte. Hackers, défenseurs de la liberté de la presse et journalistes avaient rendez-vous samedi

dernier à **la Cantine** autour de quatre ateliers.

Telecomix, un collectif d'hacktivistes très actif en Syrie notamment, **Reflets.info**, site d'information qui associe journalistes et hackers, et Reporters sans Frontières ont présenté quelques clés pour mieux protéger ses sources à l'heure où la surveillance **change de moyens et d'échelle**.

Dernière triste illustration en date : la mort de la journaliste américaine Marie Colvin et du jeune photojournaliste français Rémi Ochlik, tués en Syrie le 22 février dans des bombardement à Homs. **Selon l'*Electronic Frontier Foundation*** , ils auraient été trahis par leur téléphone satellitaire, qui a permis de connaître leur position.

Un réseau ouvert

Kitetoa, **journaliste à Reflets.info**, a présenté le fonctionnement du réseau, avant d'expliquer comment interviennent les technologies de surveillance, technologies que Reflets.info s'est fait **une spécialité de surveiller**. Protéger efficacement ses données personnelles, **un enjeu de taille**, passe par la compréhension de la nature d'Internet. Un réseau ouvert, issu d'une réflexion demandée par des militaires américains à des *"universitaires aux cheveux longs et aux idées larges"* . En somme, les machines communiquent entre elles et s'échangent des informations. Usant d'une métaphore, Kitetoa explique :

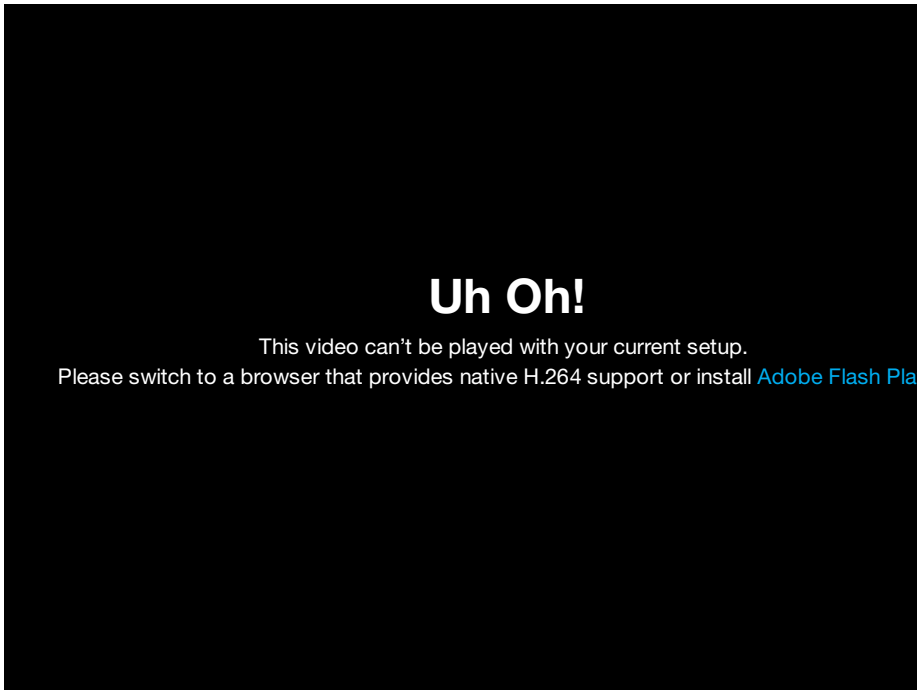
> ***Imaginez que vous êtes au comptoir dans un bar. Vous demandez à quelqu'un à l'autre extrémité une bière. Pour ce faire, l'information doit transiter par toutes les personnes entre lui et vous. Idem au retour pour obtenir votre bière. Si les gens sont polis, la bière vous parviendra intacte. Sinon, ils peuvent aussi cracher dedans.***

Le réseau peut être observé à plusieurs endroits à l'aide du *Deep Packet Inspection* , une technique qui permet d'explorer les paquets de données en profondeur, donc les données qui transitent. Une technologie duale utilisée tant pour mesurer la qualité du trafic qu'à des fins de filtrage et de censure. Lorsque Orange propose à ses clients un outil pour recevoir de la publicité ultra-ciblée, il fait du DPI sur la box du client. Pour Kitetoa, un tel outil revient *"à se mettre volontairement sous surveillance"*. Le filtrage peut aussi être à l'échelle d'une nation, comme en Libye avec l'aide de l'entreprise française **Amesys**, ou en Syrie grâce à **QOSMOS** et **BlueCoat** notamment.

La constat est grave mais des solutions existent. L'utilisation d'un réseau privé virtuel (un VPN) permet de court-circuiter quelques dispositifs de surveillance. Le VPN est un tunnel fermé qu'il est plus difficile de pénétrer, surtout lorsque les **VPN sont de confiance**.

Continuum de sécurité

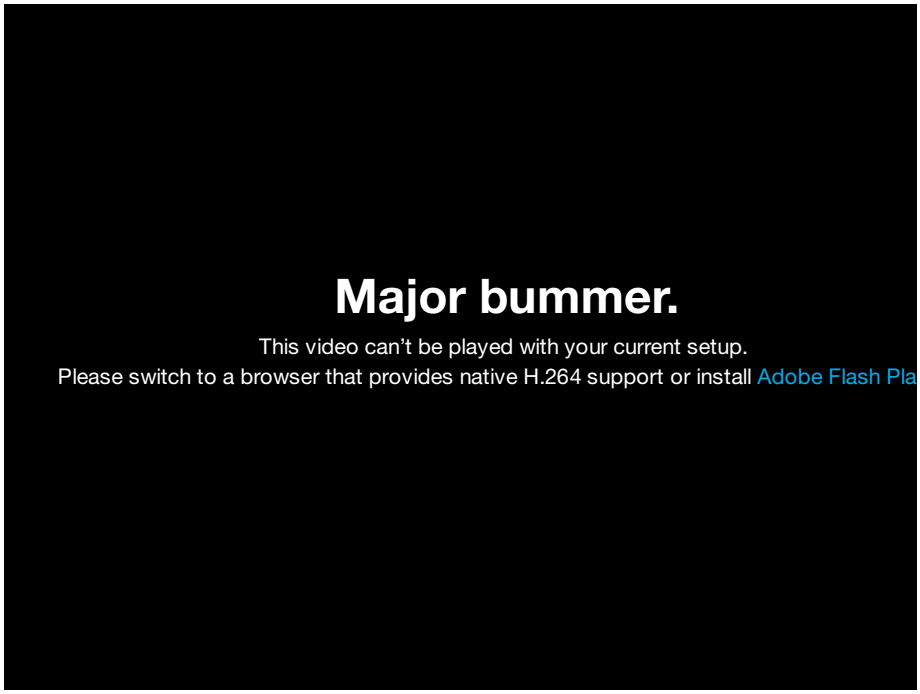
Comprendre le fonctionnement du réseau et de ses failles est un premier pas vers une meilleure protection de ses données personnelles. Une autre partie se joue hors ligne, sur son ordinateur. **Stéphane Koch**, expert en sécurité informatique et intervenant auprès de RSF, décrit une chaine de sécurisation. Le chiffrement des données stockées sur son disque dur, en utilisant le logiciel **TrueCrypt**, est une étape, mais pas une fin en soi. Le continuum passe par le choix d'un mot de passe solide, le verrouillage systématique de sa session lorsqu'on s'éloigne de son poste de travail, l'effacement définitif des données supprimées…



Chiffrement

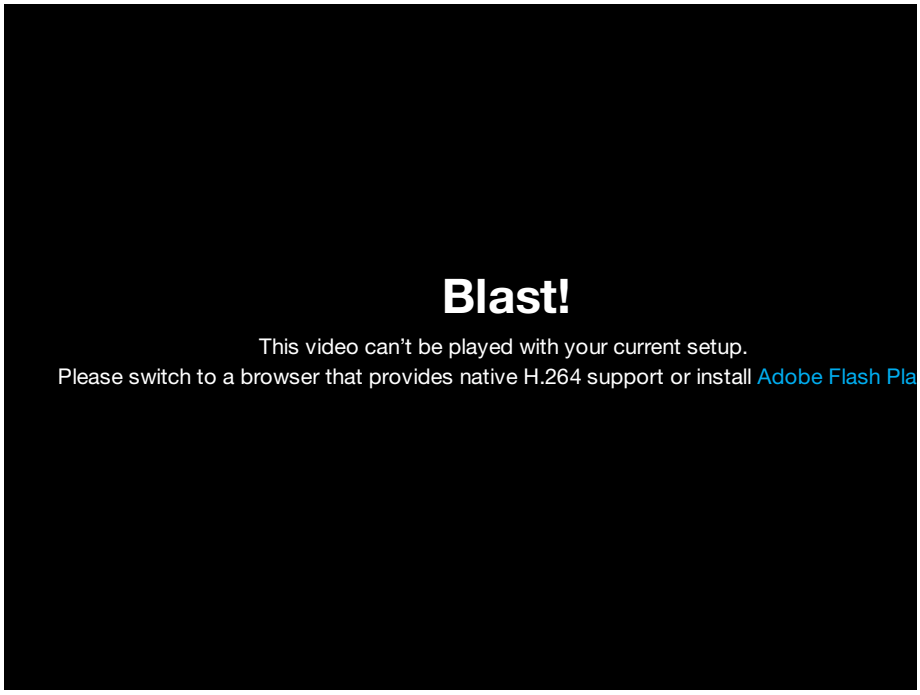
Okhin, hacker du collectif Telecomix, **a présenté les solutions** de chiffrement, quelles que soient les activités en ligne : navigation, discussions instantanées, envois d'emails. Pour chaque catégorie existent des solutions gratuites et sûres. Le **pack TOR** comprend tous les outils pour protéger sa navigation en ligne et contourner la censure éventuelle. Les conversations en temps réel peuvent aussi être chiffrées en utilisant l'extension *Off The Reccord* (OTR) sur certains programmes, dont **Pidgin** ou **Adium**.

Le **logiciel de chiffrement GPG** permet à la fois d'authentifier la provenance des emails et de chiffrer leur contenu. Chaque interlocuteur possède une clé publique et une clé privée correspondante. La première permet de chiffrer le message, la seconde de déchiffrer les messages reçus. Le client de messagerie Thunderbird, utilisé avec **EnigMail**, offre la possibilité d'utiliser le GPG.



Anonymat ou chiffrement

Les responsables Internet à Reporters sans Frontières, Grégoire Pouget et Lucie Morillon, travaillent quotidiennement avec des sources potentiellement en danger, en Iran, en Biélorussie ou ailleurs. L'arbitrage entre chiffrement et anonymat est une question récurrente. Quand chiffrer devient suspect, il vaut mieux utiliser des stratégies d'anonymisation, comme des boites au lettre virtuelles mortes estiment-ils. La solution de sécurité doit être adaptée au contexte.



Erratum : Dans son interview, Okhin évoque l'arrestation de personnes en contact régulier via Skype avec RSF. Il ne s'agit pas de RSF mais de la Fédération international des droits humains (FIDH).
A (re) lire : **Petit manuel de contre-espionnage informatique**.
A consulter également, **les podcasts de l'évènement** pour chaque atelier et la table ronde, sur le site de Silicon Maniacs, co-organisateur de cette journée de formation.
Photos par Ophelia Noor pour Owni /-)
Vidéos à l'iPhone par Ophelia Noor et Pierre Alonso

OOPS!
le 4 mars 2012 - 20:45 • SIGNALER UN ABUS - PERMALINK

Je suis impatient de pouvoir lire un jour le même genre d'article, mais, pour et à partir d'un smartphone.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MAD
le 5 mars 2012 - 16:40 • SIGNALER UN ABUS - PERMALINK

Un bon début :
http://korben.info/orbot-tor-android.html

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ANTOINECHAMPAGNE
le 5 mars 2012 - 11:53 • SIGNALER UN ABUS - PERMALINK

Précision : L'image du verre de bière m'a été rapportée par Okhin qui la tenait de quelqu'un d'autre.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LAURENT
le 5 mars 2012 - 13:46 • SIGNALER UN ABUS - PERMALINK

Sébastien Pouget ou Grégoire Pouget, il faut choisir :)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OPHELIANOOR
le 6 mars 2012 - 16:21 • SIGNALER UN ABUS - PERMALINK

Grégoire of course. Merci pour votre vigilance. c'est corrigé sur Viméo.

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OSABRIE@GMAIL.COM
le 5 mars 2012 - 13:50 • SIGNALER UN ABUS - PERMALINK

Naturellement en tant que chantres de l'open data / open source. Vous avez filmé/podcasté cette réunion pour en diffuser le contenu au plus grand nombre … Ou vous vous êtes contenté de vous réunir à 8 dans un garage ;)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CLÉMENT BEAUFILS
le 6 mars 2012 - 14:00 • SIGNALER UN ABUS - PERMALINK

Étudiant en informatique à Londres, spécialisé en sécurité informatique, ce n'est pas la première fois que je vois ce genre d'initiative.
À Londres, il y a le groupe Hacks/Hackers: London qui met en relation des journalistes et des hackers (dans tous les sens du terme hackers), à travers des rendez-vous mensuels, conférences, évènements, etc.

On remarque souvent que ces deux professions s'accordent plutôt bien. Il est toujours enrichissant d'apprendre des autres, je ne peux que saluer une pareille initiative en France.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OPHELIANOOR
le 6 mars 2012 - 16:25 • SIGNALER UN ABUS - PERMALINK

Nous mettons en place depuis un peu plus d'un an un évènement qui se rapproche beaucoup des rencontres Hack/Hackers, il s'agit de HACK THE PRESS.

Le deuxième édition :
http://owni.fr/2012/01/16/ils-ont-hacke-la-presse/

La première :
http://hackthepress.net/2010/09/20/hackthepress-a-la-cantine-le-28-septembre/

Quant à cette journée de formation, elle était organisée par nos collègues du webzine Silicon Maniacs, ainsi que RSF, Reflets.info et Telecomix. Nous étions simples participants à Owni /-)

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CLÉMENT BEAUFILS
le 6 mars 2012 - 16:28 • SIGNALER UN ABUS - PERMALINK

Génial ! Merci pour le lien.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PHILIPPE
le 7 mars 2012 - 9:43 • SIGNALER UN ABUS - PERMALINK

Bonjour

article intéressant mais je suis toujours étonné qu'on mette en avant l'aspect "anonyme" de Tor alors que des travaux menés par l'expert en sécurité Eric Filiol ont démontré qu'il était possible "d'intercepter" des connexions.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CULTUR GEEK
le 7 mars 2012 - 17:42 • SIGNALER UN ABUS - PERMALINK

Comme quoi, peu à peu, l'activité (en même temps que le terme) de hackers se démocratise à l'usage des professionnels, et parvient à renvoyer une vitrine responsable en tant qu'aide à la sécurité, et non forcément l'inverse. Une évolution des mœurs qui, j'ai l'impression, aura mis du temps à arriver en France, mais finalement, est bien là !

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

3 pings

Anonymous+wikileaks dénoncent notre surveillance | Section Mios le 4 mars 2012 - 23:50

[...] de paranoïa que nous avons créé avec ce qui précède :0, nous vous donnons rendez-vous sur la page d'Owni relatant la formation à la sécurité des journalistes par les hackers [...]

sécurité | Pearltrees le 5 mars 2012 - 12:58

[...] Adapter sa solution de sécurité au contexte. Les hackers forment les journalistes » OWNI, News, Augmented [...]

De l'Internet | Pearltrees le 7 mars 2012 - 12:25

[...] Les hackers forment les journalistes » OWNI, News, Augmented Kitetoa, journaliste à Reflets.info, a présenté le fonctionnement du réseau, avant d'expliquer comment interviennent les technologies de surveillance, technologies que Reflets.info s'est fait une spécialité de surveiller. [...]