

# DANGEREUX HACKERS D'INTÉRÊT PUBLIC

LE 13 AVRIL 2012 SABINE BLANC

Depuis jeudi et jusqu'à samedi soir, en plein Paris, le festival Hackito Ergo Sum réunit la crème des hackers sur les questions de sécurité. Un enjeu fondamental. Mais que ne semble pas saisir le législateur. Un projet de loi européen étend les sanctions contre les hackers, sans véritable débat sur le contre-pouvoir qu'ils représentent à l'heure où les États étendent leurs contrôles sur les réseaux.



***Le hack est quelque chose d'intérêt public qu'il faut protéger dans notre société de plus en plus technique.***



Tout au long de la présentation inaugurale d'**Hackito Ergo Sum** (HES), un événement réunissant jusqu'à demain au siège du Parti Communiste à Paris des hackers passionnés de sécurité informatique, **Cédric "Sid" Blancher** n'a eu de cesse de démontrer ce que la majorité des gens ne comprennent pas : le hacking, cet usage créatif des technologies, est par essence politique, au sens profond du terme. Philippe Langlois, figure "historique" de la scène hacker française, fondateur du hackerspace **le TMP/LAB**, et organisateur, explique :



***Nous faisons de la politique réelle, concrète, par les actes, sans rentrer dans un schéma de parti. Nous participons à l'élaboration de la loi ("policy making"), il faut comprendre les enjeux, les dynamiques sociétales, pour élaborer un cadre afin que les gens se pluggent de façon intelligente, c'est ça la politique. À HES, nous le faisons avec une approche technique.***



La faute revient en partie, aux médias qui parlent de plus en plus de hacking, mais mal, en assimilant hack et pratiques illégales. Notre conférencier, ingénieur-chercheur en sécurité des systèmes et réseaux informatiques, a rappelé en quoi le hack est nécessaire pour le bon fonctionnement de la démocratie à travers une série de mots-clés comme :



***Apprendre. Nous avons besoin d'apprendre pour nous et nos enfants car les systèmes sont de plus en plus complexes. On perd ce pouvoir d'apprendre.***



Protection des données, systèmes fermés, les exemples sont infinis de systèmes que tout un chacun devrait pouvoir ouvrir, manipuler, se réapproprier, pour comprendre les enjeux et mieux le maîtriser. Sauf qu'actuellement, cela peut vous coûter cher, par exemple si vous cassez des systèmes propriétaires, comme l'iPad en regorge par exemple.



***Innovation. Le hack est une grande source d'innovation.***



Cédric Blancher a souligné le rôle que les individus jouent dans les processus d'innovation, face à des entreprises sclérosées qui ne favorisent pas la créativité.



***Empowerment. C'est une question de citoyenneté.***



Souvenez-vous les machines à vote électroniques, censées mettre fin aux fraudes qui entachent les élections. Trouées comme pulls mités, **ont révélé** des chercheurs ! Dans ce contexte, le "prenez le pouvoir" marxiste affiché sur les murs résonnait de plus belle, à la lumière technologique.

## **Législation "débile et contre-productive"**

Précieux, les hackers ne sont pourtant pas aidés, et pas uniquement par le JT de TF1 et ses reportages racoleurs sur les pirates biélorusses. **Un projet de loi européenne** inquiète la communauté, préparé en toute discrétion. Il étendrait à toute l'Europe ce que la loi pour la confiance dans l'économie numérique (LCEN) française de 2004 prévoit, du moins en théorie : rendre illégal la possession d'outil de piratage. Décryptage en colère de Philippe Langlois :



***C'est complètement débile et contre-productif. Je comprends la nécessité pour le législateur d'avoir un texte pour taper sur les méchants, mais pourquoi n'ont-ils pas appris de leurs erreurs ? L'Allemagne a voté une loi similaire en 2007 et sa jurisprudence a dit qu'il était impossible de faire passer un tel texte. Les techniques duales, par exemple les scanners de vulnérabilité sont autorisées, par contre tout ce qui est déni de service, qui ne peut être utilisé qu'en mode attaque illégale est interdit. Ils auraient pu se limiter à ça mais***

*même pas.*

*On risque de construire un nouveau système où les poids lourds du secteur ont un droit non écrit d'avoir des outils de sécurité hostiles. Sauf que celui qui innove dans la sécurité, ce n'est pas la grosse boîte, c'est le petit gosse de 14 berges qui déchire tout, qui n'est pas identifié.*

*Vous êtes en train de tuer la capacité de développement par une nation de personnes qui vont grandir, murir, passer d'un moment où ils ont fait des bêtises peut-être, à celui où ils font des trucs fondamentaux pour la communauté et le développement général du domaine. HES existe pour essayer de faire changer les choses.*



## Politique par la pratique

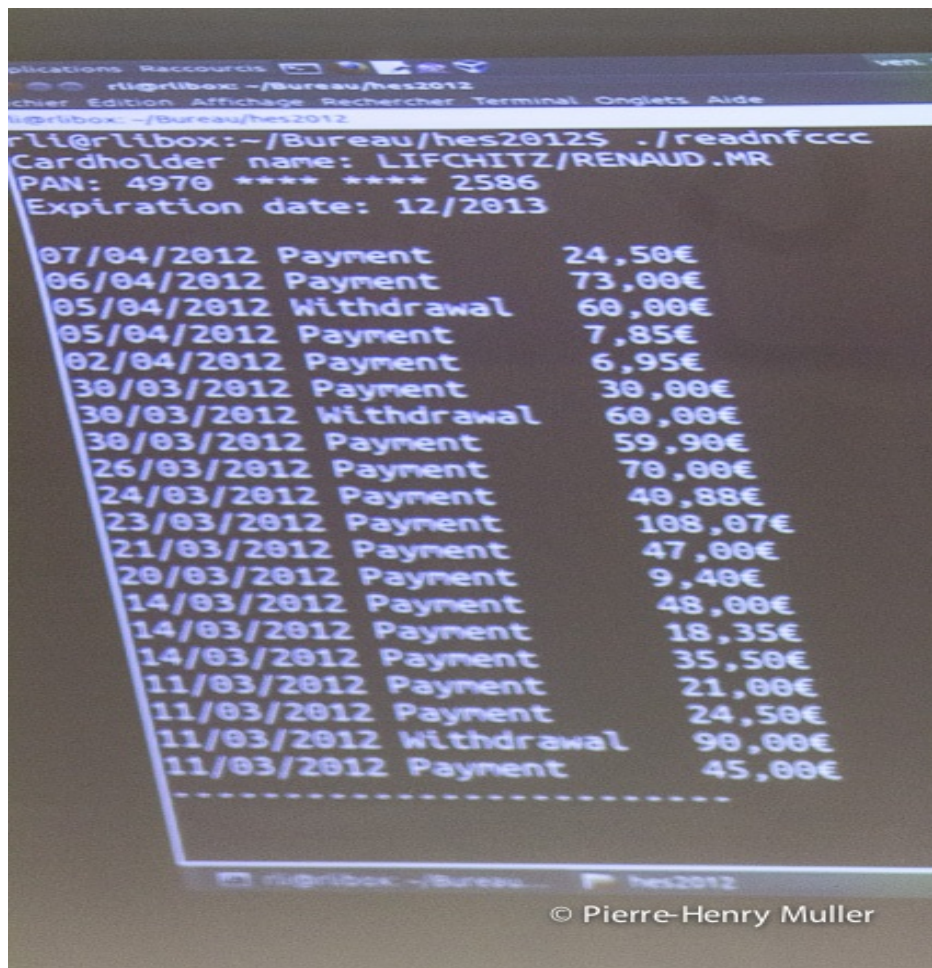
Et la meilleure façon de prouver que le législateur européen est "à la ramasse" passe donc "par des trucs concrets, des projets, des ateliers". Mais attention, si le fond est sérieux, il ne faut pas oublier un aspect important du hack, il faut s'amuser, même si l'intitulé des conférences et des ateliers peut sembler aussi drôle qu'une blague de Christine Boutin. Un exemple (smiley d'origine) : la conférence **Hacking the NFC credit cards for fun and debit** 😊. Une préoccupation absconse de nerds ? Non, cela concerne monsieur tout-le-monde.

Un peu de traduction : les NFC credit cards, ce sont tout simplement des cartes de crédit sans contact, sur le principe du Pass Navigo bien connu des Parisiens. On les utilise pour du micropaiement, 20 euros maximum. Visa a son payWave et Mastercard son PayPass. Très courant aux Etats-Unis, ce système monte en puissance en France, avec déjà 100 000 terminaux. Renaud Lifchitz, un jeune ingénieur en sécurité informatique s'est posé la question :



*Est-ce plus sécurisée que le pass Navigo ? Non car il n'y a pas d'authentification ni de chiffrement.*





© Pierre-Henry Muller

En bref, on peut lire à livre ouvert, moyennant un lecteur NFC USB qui coûte quelques dizaines d'euros et un programme. Le tout tournant dans un téléphone portable. Il faut juste être proche de la victime, dans la version low cost de son hack. Par exemple dans une queue à la boulangerie. Il est ainsi très aisé de récupérer le contenu de la bande magnétique et sa tripotée de données personnelles pour faire un double de la carte : nom, prénom, âge, numéro complet de la carte bancaire, historique des transactions, etc.

Il est donc possible de faire des achats sur des sites de e-commerce. Et comme le rappelait lors de sa keynote son confrère **Fyodor Yarochkin**, il est très lucratif de piquer un grand nombre de fois une petite somme.

Sa démonstration en direct de son programme a provoqué une salve d'applaudissements. En bon hacker, Renaud a aussi émis des recommandations pour améliorer la sécurité des cartes de crédit et comment se protéger. À part investir dans un porte-monnaie métallique qui coupe les ondes, la solution est simple :



***Jetez-la !***



Dans l'absolu notre brillant hacker prend des risques juridiques avec cet exposé d'utilité public. Une contradiction que les nombreuses personnes travaillant pour le gouvernement qui ont assisté à Hackito Ergo Sum remonteront avec force aux pontes législateurs, espérons.

—

Pour poursuivre :

**Le livestream de Hackito Ergo Sum**

**Eric Filliol : "L'État doit s'appuyer sur les hackers"**

## Les étonnantes fuites de la carte bancaire sans contact

Photographies © **Pierre-Henry Muller**, tous droits réservés

### REGNAROCK

le 14 avril 2012 - 4:50 &bullet; SIGNALER UN ABUS - PERMALINK



*Très bon article ! Il fait du bien de voir ce que le "hack" est vraiment, au lieu de l'assimiler à un vulgaire terrorisme technologique comme le font trop souvent nos médias.*

*Une coquille à noter : "Sauf qu'actuellement, cela peut vous coûter cher, par exemple si vous cassez des systèmes propriétaires, comme l'iPad en regorge par exemple."*

*C'est : "vous cassez"*

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

### SABINE BLANC

le 14 avril 2012 - 14:28 &bullet; SIGNALER UN ABUS - PERMALINK



*Merci, faute corrigée :)*

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

## 7 pings

Black Eco's Blog » Dangereux hackers d'intérêt public le 13 avril 2012 - 19:35

[...] Via owni.fr Catégorie: Veille Partager cet article: Tweeter +1 Partager [...]

stz | Pearltrees le 15 avril 2012 - 22:37

[...] Dangereux hackers d'intérêt public » OWNI, News, Augmented Est-ce plus sécurisée que le pass Navigo ? Non car il n'y a pas d'authentification ni de chiffrement. [...]

Dangereux hackers d'intérêt public le 17 avril 2012 - 15:13

[...] [ Source : Lire la suite ] [...]

Techno | Pearltrees le 23 avril 2012 - 10:32

[...] Dangereux hackers d'intérêt public » OWNI, News, Augmented Est-ce plus sécurisée que le pass Navigo ? [...]

La Cnil se penche sur les failles des cartes sans contact » revue du web, Just another weblog le 10 mai 2012 - 18:02

[...] et d'autres vous en avaient parlé : les cartes sans contact, en pleine expansion en France, présentent de grosses failles de [...]

Sete'ici » Archive » RFIDanger le 30 juillet 2012 - 7:52

[...] En bref, on peut lire à livre ouvert, moyennant un lecteur NFC USB qui coûte quelques dizaines d'euros et un programme. Le tout tournant dans un téléphone portable. Il faut juste être proche de la victime, dans la version low cost de son hack. Par exemple dans une queue à la boulangerie. Il est ainsi très aisé de récupérer le contenu

*de la bande magnétique et sa tripotée de données personnelles pour faire un double de la carte : nom, prénom, âge, numéro complet de la carte bancaire, historique des transactions, etc. dixit ce papier d'Owni [...]*

Les hackers d'intérêt public « Social Media Student le 7 août 2012 - 14:07

*[...] <http://owni.fr/2012/04/13/les-hackers-un-danger-dinteret-public/> J'aime ceci:J'aimeBe the first to like this. ►Aucune réponse /\* 0) { [...]*