

INTERNET MASSIVEMENT SURVEILLÉ

LE 1 DÉCEMBRE 2011 JEAN MARC MANACH

En partenariat avec WikiLeaks, OWNI révèle l'existence d'un nouveau marché des interceptions massives, permettant d'écouter toutes les télécommunications à l'échelle d'une nation. Ses acteurs vendent leurs produits en Europe, aux États-Unis et à des dictatures.



WikiLeaks rend public aujourd'hui près de 1 100 documents internes, plaquettes commerciales et modes d'emploi des produits commercialisés par les industriels des systèmes de surveillance et d'interception des télécommunications.

Ces nouvelles fuites montrent un marché de la surveillance de masse représentant désormais cinq milliards de dollars, avec des technologies capables d'espionner la totalité des flux Internet et téléphoniques à l'échelle d'une nation. Les fleurons de ce marché s'appellent **Nokia-Siemens, Qosmos, Nice, Verint, Hacking Team, Bluecoat** ou **Amesys**. Les documents détaillant leurs capacités d'interception, contenant une multitude de détails technologiques, seront progressivement mis en ligne par WikiLeaks.

OWNI, partenaire de cette opération baptisée SpyFiles avec **Privacy International** et **The Bureau of Investigative Journalism**, deux ONG britanniques, ainsi que le **Washington Post**, **The Hindu**, **L'Espresso**, la chaîne allemande **ARD**, a tenté de visualiser cette industrie d'un genre nouveau, en créant une cartographie interactive sur un site dédié, **SpyFiles.org**. Et **Andy Mueller-Maguhn**, ancien porte-parole du Chaos Computer Club allemand (le plus influent des groupes de hackers au monde), également associé à cette enquête, y consacre un site, **BuggedPlanet.info** – traduisez "planète sur écoute".

Marchand d'armes de surveillance

À ce jour, nous avons répertorié 124 de ces marchands d'armes de surveillance, utilisant des technologies d'interception, dont 32 aux États-Unis, 17 au Royaume-Uni, 15 en Allemagne, dix en Israël, huit en France et sept en Italie... À l'instar des marchands d'armes "traditionnels", la majeure partie d'entre eux sont situés dans des pays riches, et démocratiques. 12 des 26 pays recensés font ainsi partie de l'Union européenne qui, au total, totalise 62 de ces entreprises.

87 vendent des outils, systèmes et logiciels de surveillance de l'Internet, 62 de surveillance du téléphone, 20 des SMS, 23 font de la reconnaissance vocale, et 14 de la géolocalisation GPS. Sept d'entre elles font également dans la "lutte informatique offensive", et commercialisent donc des **chevaux de Troie, rootkits** et autres **backdoors** (portes dérobées) permettant de prendre le contrôle d'ordinateurs, à distance, et à l'insu de leurs utilisateurs. Ces systèmes espions ont ceci de particulier par rapport à ceux utilisés par les

pirates informatiques qu'ils ne seraient pas repérés par la "majeure partie" des éditeurs d'antivirus et autres solutions de sécurité informatique.

Dans nos démocraties, la commercialisation, et l'utilisation, de ces systèmes de surveillance et d'interception des télécommunications est **strictement encadrée**. Mais rien n'interdit, en revanche, de les vendre à des pays moins regardants, même et y compris à des dictatures : bien que conçus à des fins d'espionnage, ils ne font pas partie de ces armes dont l'exportation est encadrée par les lois nationales, européennes ou internationales. Ce n'est donc peut-être pas moral, mais tout à fait légal, en l'état.

Et les marchands d'armes se font fort d'exploiter ce vide juridique, comme le **reconnaisait** récemment Jerry Lucas, l'organisateur d'**ISS**¹, le salon international qui rassemble tous les deux ou trois mois les professionnels de l'interception des communications :



Les systèmes de surveillance que nous exposons dans nos conférences sont disponibles dans le monde entier. Certains pays les utilisent-ils pour supprimer certaines déclarations politiques ? Oui, probablement. Mais ce n'est pas mon job de faire le tri entre les bons et les mauvais pays. Ce n'est pas notre métier, nous ne sommes pas des hommes politiques.

Notre business est de mettre en relation ceux qui veulent acheter ces technologies avec ceux qui les vendent. Vous pouvez bien vendre des voitures aux rebelles libyens, et ces voitures sont utilisées comme armes. General Motors et Nissan devraient-ils se demander comment leurs véhicules seront utilisés ? Pourquoi n'allez-vous pas également interroger les vendeurs de voiture ? C'est un marché ouvert. Vous ne pouvez pas enrayer la circulation de matériels de surveillance.



TeleStrategies®
ISS World Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering

Washington, DC
11-13 October, 2011

Brasilia, BR
24-26 July 2012

Prague, CZ
5-7 June 2012

Dubai, UAE
13-15 February 2012

Kuala Lumpur, MY
6-8 December 2011

More Info

Interrogé par le *Wall Street Journal*, Klaus Mochalski, co-fondateur d'Ipoque, une société leader dans ce secteur, répondait de son côté que "c'est un dilemme, moral et éthique, auquel nous sommes constamment confrontés : c'est comme un couteau. Vous pouvez vous en servir pour trancher des légumes, mais vous pouvez également tuer votre voisin"... à ceci près que ces outils ne sont pas en vente libre dans n'importe quel magasin, et que les sociétés qui les commercialisent n'en font pas la promotion dans des foires commerciales

ou marchés du coin, mais uniquement dans les salons réunissant marchands d'armes, et clients habilités à en acheter.

Silence radio

ISS interdit ainsi aux journalistes d'assister à ses conférences, et même d'entrer dans son salon. Et il était étonnant de constater, à visiter les nombreux stands spécialisés dans les technologies de surveillance présents au récent salon Milipol, qui s'est tenu à Paris en octobre dernier, que les représentants de ces derniers étaient bien plus frileux que les marchands d'armes traditionnels pour ce qui est de répondre aux questions des journalistes ...

Contactée par *OWNI*, Amesys, la société française qui a vendu un système d'interception massive de l'Internet à la Libye de Kadhafi, se défousse ainsi auprès de son "client" :



Amesys est un industriel, fabricant de matériel. L'utilisation du matériel vendu (sic) est assurée exclusivement par ses clients.



A contrario, Thibaut Bechetoille, le PDG de Qosmos, une autre société française qui, à l'instar d'Ipoque, équipait ce même **Big Brother libyen**, et qui équipe également celui utilisé, actuellement, par les Syriens, a piteusement **expliqué** à l'agence Bloomberg que son conseil d'administration avait bien décidé de cesser ses activités en Syrie, mais que c'était "techniquement et contractuellement" compliqué...

A ce jour, quatre autres entreprises occidentales ont **été identifiées** comme prestataires de services des "grandes oreilles" syriennes : Area, une entreprise italienne qui a dépêché, en urgence, des équipes afin d'aider les services de renseignements syriens à identifier les (cyber) dissidents, Utimaco, filiale allemande de l'éditeur d'antivirus britannique Sophos – qui n'était pas au courant qu'Area utilisait ces systèmes en Syrie -, l'allemand Nokia Siemens, dont les équipements de surveillance de l'Internet **auraient été transmis** à la Syrie par son voisin iranien, et Bluecoat, une société américaine auquel le site *reflets.info* a consacré **de nombreux articles**.

On savait, depuis quelques années, que ces armes de surveillance étaient utilisées en Chine ou en Iran notamment, mais il a fallu attendre le printemps arabe, et les traces ou preuves laissées par ces marchands de surveillance (essentiellement occidentaux) en Tunisie, en Egypte, en Libye, à Bahrein ou en Syrie, pour en prendre toute la mesure.

La quasi-totalité de ces marchands d'armes de surveillance se targuent certes d'œuvrer en matière de "lawful interception" (interceptions légales en français) et se vantent de travailler avec des ministères de la défense, de l'intérieur ou des services de renseignement.

L'allemand Elaman, lui, va jusqu'à écrire, noir sur blanc, que cela permet aussi d'identifier les "opposants politiques" :



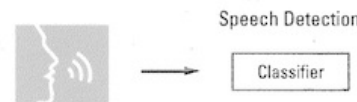
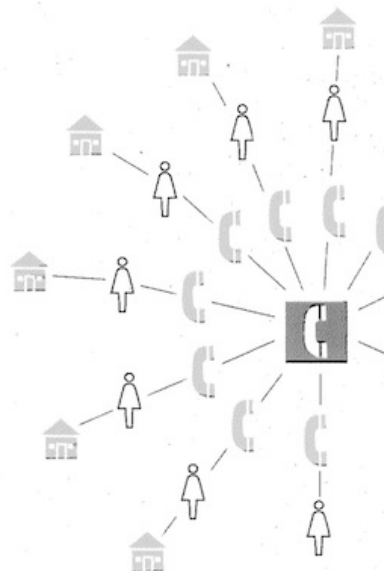
En matière de télécommunications, la notion de "rétention des données" porte généralement sur le stockage de toute information (numéros, date, heure, position, etc.) en matière de trafic téléphonique ou Internet. Les données stockées sont généralement les appels téléphoniques émis ou reçus, les e-mails envoyés ou reçus, les sites web visités et les données de géolocalisation.

Le premier objectif de la rétention des données est l'analyse de trafic et la surveillance de masse. En analysant les données, les gouvernements peuvent identifier la position d'un individu, de ses relations et des membres d'un groupe, tels que des opposants politiques.



Data Retention

In the field of telecommunications, data retention generally refers to the storage of call related information (numbers, date, time, position, etc.) of telephony and internet traffic. The stored data is usually telephone calls made and received, emails sent and received, web-sites visited and location data. The primary objective in data retention is traffic analysis and mass surveillance. By analyzing the retained data governments can identify an individual's location, their associates and members of a group, such as political opponents.



Initialement développés afin de permettre aux services de renseignements d'espionner en toute illégalité, ces systèmes, outils, logiciels et autres "gadgets" conçus pour écouter, surveiller, espionner, traçabiliser ou géolocaliser quelqu'un "à l'insu de son plein gré", sont aujourd'hui devenus un véritable marché. Interrogé par le *WSJ*, Jerry Lucas, l'organisateur d'ISS, expliquait ainsi que, parti de quasiment zéro en 2001, il avoisinerait aujourd'hui les 5 milliards de dollars de chiffre d'affaires, par an.

Les *Spy Files* sont publiés par WikiLeaks à [cette adresse](#).



Retrouvez **notre dossier** sur les *Spy Files* :

- **Mouchard sans frontière**
- **La carte d'un monde espionné**

Retrouvez nos articles sur **Amesys**.

Retrouvez tous **nos articles** sur **WikiLeaks** et **La véritable histoire de WikiLeaks**, un ebook d'Olivier Tesquet paru chez OWNI Editions.

@manhack (sur *Twitter*), **jean.marc.manach** (sur *Facebook* & **Google+** aussi) .

Vous pouvez également me contacter de façon sécurisée via **ma clef GPG/PGP** (ce qui, pour les non-initiés, n'est **pas très compliqué**). A défaut, et pour me contacter, de façon anonyme, et en toute confidentialité, vous pouvez aussi passer par **privacybox.de** (n'oubliez pas de me laisser une adresse email valide -**mais anonyme**- pour que je puisse vous répondre).

SOUMETTRE DES FICHIERS À OWNI SUBMIT FILES TO OWNI

OWNI vous offre la possibilité de lui envoyer **sous anonymat** des messages et fichiers.
*OWNI enables you to submit **anonymously** files and messages.*

Si votre message nécessite une réponse, veuillez à nous laisser une adresse email valide (mais anonyme). Voir aussi • Gorge profonde: le mode d'emploi • et • Petit manuel de contre-espionnage informatique •.

SOUMETTRE DES FICHIERS 
SUBMIT FILES

Pour plus d'explications sur ces questions de confidentialité et donc de sécurité informatique, voir notamment « **Gorge profonde: le mode d'emploi** » et « **Petit manuel de contre-espionnage informatique** ».

1. pour Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering, à savoir, et en français, systèmes de soutien au renseignement en matière d'interceptions légales, d'enquêtes criminelles et de collecte de renseignement. [↗]

BOXSONS

le 1 décembre 2011 - 14:04 • SIGNALER UN ABUS - PERMALINK



Beau travail et belles trouvailles en forme de polémiques.

J'ai toutefois une légère préférence pour la conclusion de votre article : "Vous pouvez également me contacter de façon sécurisée via ma clef GPG/PGP". Sinon, je serais dimanche au Nord Sud, Mairie du XVIII avec un Stetson et un journal de droite...mais lequel ???

B.

VOUS AIMEZ



1

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

LES INDIGNÉS MARSEILLE

le 1 décembre 2011 - 14:54 • SIGNALER UN ABUS - PERMALINK



Bravo, bravo et encore bravo !

Ça c'est du journalisme, du vrai. De l'enquête, de l'investigation.

—

PROVENCE DÉMOCRATIE

MARSEILLE Mouvement des indignés

Site : <http://www.provencedemocratie.com>

Facebook : [Marseille – Democratie Reelle](#)

Twitter : <https://twitter.com/#1Provencracie>

email : provencedemocratie@gmail.com

VOUS AIMEZ



1

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

LITTLESISTER

le 1 décembre 2011 - 15:16 • SIGNALER UN ABUS - PERMALINK



Et vous pensez vraiment que ces technologies développées en occident ne sont pas utilisées à la maison?

Avant de les vendre à prix d'or, ils les testent comment leurs "logiciels d'interception à l'échelle d'un pays" à votre avis?

VOUS AIMEZ



1

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

YT75

le 1 décembre 2011 - 15:30 • SIGNALER UN ABUS - PERMALINK



Et quand les gentils geeks hurlent à la censure au simple fait que le blocage des sites de piratage est évoqué, ne laissant de fait que la surveillance flux utilisateurs comme voie légale, il ne faut pas non plus trop s'étonner que tout cela se développe ... <http://iiscn.wordpress.com/2011/05/15/piratage-hadopi-etc/>

Et j'espère que tout le monde est conscient du fait que les "darknets" et compagnie, ne sont que des overlays n'ayant pas a priori vocation à poser des cables transatlantiques non ?

(On sait jamais aujourd'hui, quasi plus personne ne sachant lire ...)

Voir par exemple :

http://www.pcinpact.com/news/67215-sabam-cour-justice-filtrage-blocage.htm?vc=1&_page=2

"la terreur n'est pas française" écrivait Rimbaud dans la saison, mais à l'époque de la terreur imposée par la bêtise il est franchement possible d'en douter.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

NEMO

le 1 décembre 2011 - 17:24 • SIGNALER UN ABUS - PERMALINK



Bon, maintenant vous savez que nous savons, et nous savons que vous le savez.

Tout va bien, vous pouvez reprendre votre travail.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

ALAIN

le 1 décembre 2011 - 18:33 • SIGNALER UN ABUS - PERMALINK



Et qui croyez vous ont participé au développement de tous ces outils de surveillance? D'anciens hackers bien de chez nous aujourd'hui devenus de bons pères de famille et qui ne font que gagner leur vie honnêtement... en aidant les dictatures à éliminer les opposants. C'est évident que ces systèmes sont utilisés chez nous. La liberté de communication n'existe plus sur internet, ça fait au moins dix ans que je le sais. Je n'avais pas besoin de votre dossier pour le savoir mais au moins je peux maintenant vous citer dans mes conversations avec mes proches et ne plus me faire traiter de conspirationniste paranoïaque. Beau travail tout de même.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

JEROME

le 1 décembre 2011 - 23:54 • SIGNALER UN ABUS - PERMALINK



Belle enquête sur les Grandes Oreilles et les Gros Espions. Je suis informaticien et je sais bien que la tentation de l'espionnage des masses est grande chez tous les pouvoirs, y compris les plus démocratiques. Ne parlons même pas des dictatures (enfin surtout celles qui ont les moyens de se payer la technologie et les compétences nécessaires à sa mise en œuvre...).

Un petit bémol cependant : la Lybie s'était payée ce genre de joujou numérique et on peut supposer la même chose en Egypte (avec des dollars US of course !), en Tunisie ou en Syrie. Pourtant, à coup de SMS ou de Tweets, les populations se sont soulevées et 3 de ces dictatures ont été renversées. Même si les nouvelles technologies ne sont pas responsables, loin de là, à 100 pour 100 de ces chutes, elles ont quand même leur part de responsabilité.

Il faut quand même croire que les gens chargés de l'espionnage et de l'analyse des flux sont plus efficaces pour analyser nos habitudes de consommation et nous gaver de pub sur Internet que pour anticiper une révolution menaçant de renverser ceux-là même qui les payent. Etrange. A rapprocher avec le cas Américain du 11 Septembre 2001 où la NSA, la CIA, Echelon et toutes les agences suréquipées n'avaient pas vraiment su analyser les indices et les prémices des attentats à venir. Je suis certain qu'en grattant un peu on trouverait d'autres exemples de la toute relative efficacité de ces agences. Derrière tout ça, et vous le dites dans l'article, il y a surtout un gros marché très juteux qui se chiffre en milliards de dollars.

Et puis, pour éviter de se faire espionner par Big Brother, on devra peut-être à l'avenir retourner aux bonnes vieilles méthodes. Vous savez les trucs de vieux du XXème siècle : les réunions secrètes sans téléphone ni ordinateur, le courrier, l'écriture, la rencontre réelle avec des vrais gens qui parlent vraiment. Je sais, cela n'est pas très moderne mais c'est totalement "analogique", non numérique et sans intérêt pour les grandes oreilles de l'informatique et de la communication.

En fait, il est possible que toutes ces agences soient omniprésentes, qu'elles cherchent à nous dominer. Il est même possible qu'il soit trop tard et qu'elles y parviennent. Mais elles ne sont certainement pas omniscientes. Elles peuvent bien contrôler tous les flux numériques du monde, mais comprendre un homme, ou un groupe d'hommes et leurs véritables motivations à travers ces seuls éléments, c'est comme regarder à travers un prisme : on n'y voit au fond qu'une représentation déformée de la réalité...

J.

VOUS AIMEZ



2

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

CLOY

le 2 décembre 2011 - 4:14 &bullet; SIGNALER UN ABUS - PERMALINK



Si autant de sociétés font du business avec ce genre d'arme c'est qu'il n'y a pas que les quelques pays cités qui les utilisent! De la même façon qu'est utilisé Echelon depuis des décennies par les usa. Tout le monde utilise le même matériel, il n'y a que les mots qui changent. Dans nos pays "démocratiques" quand on espionne c'est pour notre sécurité tandis que dans les autres pays c'est pour surveiller. Mais l'action et le résultat sont les mêmes sauf dans les médias qui nous citent toujours les pays qui surveillent car chez nous cela semble normal et admis, c'est pour notre sécurité.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

CANYON

le 2 décembre 2011 - 9:55 &bullet; SIGNALER UN ABUS - PERMALINK



Un peu de détails techniques serait bienvenu. Bon, pour le reste, on s'en doutait un peu ... Quand à ceux qui vendent des solutions matérielles ou logicielles à des dictateurs, j'espère qu'ils comprennent que ce qu'ils voient dans leurs miroirs, le matin, est moche ... très moche ...

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

GGRRREEE

le 2 décembre 2011 - 10:01 &bullet; SIGNALER UN ABUS - PERMALINK



Bien , ce que je retiens surtout c'est : "Ces systèmes espions ont ceci de particulier par rapport à ceux utilisés par les pirates informatiques qu'ils ne seraient pas repérés par la "majeure partie" des éditeurs d'antivirus et autres solutions de sécurité informatique."

Ce serait une bonne idée si nos hackers anti Big brothers pouvaient nous concocter un vrai antivirus en open qui trackerait tous ces trucs indésirables.

Possible d'après vous ?

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

BARDAMOR

le 2 décembre 2011 - 10:04 &bullet; SIGNALER UN ABUS - PERMALINK



- Pourquoi continuer de dire "démocratiques" des Etats dont vous démontrez qu'ils ne le sont pas, dont les institutions contrôlent lesdits citoyens bien plus qu'elles ne sont contrôlées par eux ?

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

AN391

le 2 décembre 2011 - 10:33 &bullet; SIGNALER UN ABUS - PERMALINK



@Bardamor

Oui enfin, il y a aussi la mouvance "le système c'est l'ennemi" il faut tout hacker ! vive le chaos et tout et tout; internet c'est virtuel ! immatériel même !! Tout doit être gratuit même l'énergie !! Aucune loi on en a pas besoin !!

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

ARZW

le 2 décembre 2011 - 10:59 • SIGNALER UN ABUS - PERMALINK



Très bon article.

J'ai parcouru le site SpyFiles.org, et chose étrange parmi tous les pays industrialisés, le Japon n'est jamais mentionné dans aucunes catégories.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

LATEO

le 2 décembre 2011 - 11:25 • SIGNALER UN ABUS - PERMALINK



@gggrrreee:

la faiblesse de l'écrasante majorité des antivirus, c'est qu'ils sont basés sur des signatures de virus.

et donc ils ne connaissent que ce qu'on leur a appris.

il existait à une époque 2 ou 3 antivirus utilisant une logique différente ; pas du tout infallible, mais capable de détecter des trucs inconnus.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

FAB ZIO

le 2 décembre 2011 - 14:10 • SIGNALER UN ABUS - PERMALINK



Je crois que plus que jamais ce t-shirt est d'actualité !

<http://www.kdbzclothing.com/bigbrotheriswatchingyou.html>

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

GRAOU

le 2 décembre 2011 - 15:20 • SIGNALER UN ABUS - PERMALINK



@ fab :

Est-il réellement nécessaire de payer 20€ le t-shirt fabriqué en chine pour autant ?

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

LUC

le 3 décembre 2011 - 13:44 • SIGNALER UN ABUS - PERMALINK



@JEROME (1 décembre à 11:54)

"... Et puis, pour éviter de se faire espionner par Big Brother, on devra peut-être à l'avenir retourner aux bonnes vieilles méthodes. Vous savez les trucs de vieux du XXème siècle : les réunions secrètes sans téléphone ni ordinateur, le courrier, /..."

D'accord sur l'essentiel, mais avec tout de même une réserve : en fait la pratique de l'interception et de l'ouverture du courrier à une large échelle était déjà parfaitement rôdée et instituée, dans le cas des Etats-Unis, à la date de 1925. Les historiens de type universitaire se moquent du monde, lorsque confrontés à cette réalité, ils tentent de la minimiser et de botter en touche du côté de quelques chantages datant des années... 1960 (ce qui en plus leur permet de refile le bébé au parti démocrate, avec la mise en avant des Kennedy brothers, et d'ajouter une image subliminaire croustillante avec Marilyn Monroe).

@BARDAMOR (2 décembre 2011 à 10:04)

" Pourquoi continuer de dire "démocratiques" des Etats dont vous démontrez qu'ils ne le sont pas, dont les institutions contrôlent lesdits citoyens bien plus qu'elles ne sont contrôlées par eux ?"

La question présente aussi un intérêt tactique. En effet, dans un pays comme la France, beaucoup acceptent sans trop broncher, de la part de soi-disant démocraties, ce qu'à juste titre ils combattraient, venant de dictatures. La tentation dès lors est grande, de

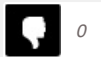
simplement changer les étiquettes. Mais à ce petit jeu : "ça passe, ou ça casse". Et le risque n'est pas négligeable, si on n'est pas cru, d'alimenter le dispositif qui permet alors à ceux-qui-nous gouvernent de se poser en... victimes d'accusations ridicules, et à leurs spameurs-de-service sur Internet de crier à la "diabolisation" etc. etc.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

YALON

le 4 décembre 2011 - 21:36 • SIGNALER UN ABUS - PERMALINK



Japan, Yes. Le Japon C kan même pas 1 Tsunami réel (this is may be n

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

YALON

le 4 décembre 2011 - 22:13 • SIGNALER UN ABUS - PERMALINK



Japan, Yes. Le Japon C quand même pas 1 Tsunami réel (this is may be not the place nor the time but I wanted to share with all JAPANESE AND ABOVE ALL WITH THE FAMILLIES WHO SUFFERED AND WILL CONTINUE TO SUFFER UNLESS WE HELP YOU WITH MONEY, MEDICAL EXPERTS . JAPAN HAD MORE THAN ENOUGH I PTRSUME TO BE ALONE IN RADIOACTIVITIES DISASTERS) I AM ISRAELI AND SWISS AND I HAVE A LOT OF PAIN 4 ALL JAPANESE PEOPLE . LA QUESTION SUBSISTE ... pourquoi le Japon n 'est pas dan la course l'armement numérique?! ou bien ils ont de bonnes raisons de cacher leurs web non éthique – morale oui il fevraii

VICTIMS OF THIS HORRIBLE

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

YALON

le 4 décembre 2011 - 22:14 • SIGNALER UN ABUS - PERMALINK



saloppes

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

YALON

le 4 décembre 2011 - 22:22 • SIGNALER UN ABUS - PERMALINK



japan u suffered from radioactivities disasters alone u should react !!!? b the leaders of watching those who watch 4 Bad Reasons and sell arms : real or wide & wild use of the net...

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

REGARDS

le 5 décembre 2011 - 9:47 • SIGNALER UN ABUS - PERMALINK



Tout ceci accrédite que DSK était bel et bien surveillé et que l'espionnage tous azimuts est devenu la norme;)

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

CARADO

le 5 décembre 2011 - 12:13 • SIGNALER UN ABUS - PERMALINK



Et bien il ne nous reste qu'une chose à faire (tous et toutes) Porter plainte devant les tribunaux lorsque nous nous apercevrons que nous sommes (effectivement) surveillé.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

LUCHONT EMILIE

le 5 décembre 2011 - 18:47 • SIGNALER UN ABUS - PERMALINK



je félicite toute l'équipe de et je voudrais savoirs concernant cet article qu'elle sont les logiciels précis utiliser pour l'espionnage concernant internet quelle logiciel utilise t'ils pour infiltrer des ordi sans ce faire prendre et donc pouvoirs obtenir les mots de passe de certain adresse électronique. je précise que je suis moi aussi étudiante un communication option journalisme j'aimerais bien faire un article concernant ce sujet . merci d'avance

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

LUCA

le 5 décembre 2011 - 21:26 • SIGNALER UN ABUS - PERMALINK



Petition de Access contre la vente des armes informatiques:

<https://www.accessnow.org/page/s/stop-the-sale>

Et Merci pour l'enquête.

VOUS AIMEZ



1

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

NIGSEN

le 6 décembre 2011 - 0:50 • SIGNALER UN ABUS - PERMALINK



En clair,cet espionnage qui se légalise,enfin officieusement,pour un début,ne vise ni plus ni moins qu'à museler certaines organisations comme AVAAZ,Amnesty International et bien d'autres encore!Et alors,tout contenu susceptible de contrecarrer des mesures impopulaires seront purement et simplement...censurés avant d'être portés à la connaissance du public.Et on continuera de vanter les mérites de la démocratie!Vive la démocratie!!!

Je félicite les auteurs de cet article qui doit rendre bien mal à l'aise beaucoup de gouvernements...

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

ZOÉ

le 19 décembre 2011 - 1:45 • SIGNALER UN ABUS - PERMALINK



Tous de mèche, tous pourris et nous tous victimes? Monde de merde...? A ceux qui pensent que tout ceci n'est qu'émergence d'un phénomène nouveau, erreur! Quel que soient les moyens rien de nouveau sous le soleil. Je sais qu'ils existent, je sais ce qu'ils font, ils savent que je sais, on continue à vivre ou on se terre comme des bêtes apeurées qu'ils veulent que nous soyons.. flippant.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

LUC

le 19 décembre 2011 - 11:23 • SIGNALER UN ABUS - PERMALINK



bien d'accord avec toi, Zoé... Et je suis même surpris de la légèreté avec laquelle certains commentaires semblent tenir pour évident que la surveillance serait moindre dans "nos" (sic) "démocraties" (resic).

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

AN391

le 19 décembre 2011 - 11:54 • SIGNALER UN ABUS - PERMALINK



*La démocratie c'est aussi l'état de droit, normalement.
Et quand on voit les mêmes hurler à la surveillance et hurler au fait que les centres de piratages seraient bloquer, il y a de quoi sourire.
Surtout que "s'en prendre aux centres" permettrait justement de se foutre des flux et IPs utilisateurs, et pourquoi pas interdire tout monitoring flux utilisateurs ? (sauf demande express etc)
<http://iiscn.wordpress.com/2011/05/15/piratage-hadopi-etc/>*

Mais à une époque tellement naïve qu'elle passe son temps à violer des adjectifs comme virtuel ou immatériel à propos de trucs électroniques permettant de transmettre des signes, lettres, symboles et autres, sans doute ne faut-t-il pas trop demander non plus ...

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

LUC

le 19 décembre 2011 - 13:35 • SIGNALER UN ABUS - PERMALINK



de toute façon AN391 quand on parle de communication (et de communicants etc.) à propos de ce qui n'est que monologue et sodomisation collective, c'est bien, que les mots n'ont plus aucun sens.

PS. pour ce qui est de "l'Etat de droit" il me semble en avoir causé, dans un courriel adressé à l'avorton du Faubourg. L'Etat de droit ce n'est pas : celui où il y un juge, deux assesseurs -et trois raisons d'être content ? Car à ce compte-là l'Italie fasciste, l'Allemagne nazie et l'URSS stalinienne auraient vite fait de devenir des Etats de droit : il y avait un Droit fasciste (etc., etc.), et les tribunaux des dictatures rendaient des arrêts qui, dans leur forme (même si les charlatans de "la démocratie" n'aiment pas qu'on le leur rappelle), étaient peu différents de ceux rendus par les nôtres ; et ce pour la bonne raison que ces juges avaient pour la plupart été formés à l'école traditionnelle. L'Etat de droit, c'est celui devant lequel ceux-qui-nous-gouvernent (et ceux qui se verraient bien prendre la suite) n'en finissent pas de péter de trouille, si tant est que leur rêve indépassé est de régner sur un troupeau d'esclaves : l'Etat de droit c'est celui QUI RESPECTE LE DROIT DES GENS. Et bastaközy.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

AN391

le 19 décembre 2011 - 14:31 • SIGNALER UN ABUS - PERMALINK



@Luc

Certes, les lois c'est aussi fait pour être discuter et évoluer, mais bon ici c'est plutôt l'ambiance hackifiante de cet espèce d'anarchisme geekeste technoïde et gentillet, dogme tout gratuit tout pub, et bien sous tout rapport (très petit bourgeois en fait)

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

LUC

le 19 décembre 2011 - 14:35 • SIGNALER UN ABUS - PERMALINK



@AN391

ben oui, et personne les empêche de faire joujou avec leur souris, mais enfin ils pourraient tout de même comprendre que s'il y avait moyen de faire l'économie d'une révolution, ça se saurait...

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

REQUIS

le 7 juillet 2012 - 2:00 • SIGNALER UN ABUS - PERMALINK



Ha ha comme vous êtes surprenant. Vous dénoncez la surveillance du net, l'espionnage et à la fois vous invitez à utiliser facebook, twitter, RSS etc. La CIA ne finance donc plus facebook ? Et les RSS ne donnent plus les adresses courriels permettant de retrouver le propriétaire et toutes ses correspondances ? Serriez-vous de ceux qui enfument afin de mieux surveiller ceux qui tombent dans la toile tendue ? Ou alors, vous enfumez-vous vous même ?

Mais bon, ces mots ne sont qu'une vision intellectuelle. Merci quand même pour vos infos. Elles seront toujours utiles car savoir c'est prévenir.

VOUS AIMEZ



1

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

29 pings

Wikileaks : les Spy Files sont en ligne | ☹️ Bluetouff's blog le 1 décembre 2011 - 15:16

[...] fait exceptionnel car il offre un instantané de l'état de l'art de la ... Wikileaks, épaulé par OWNI, vient de publier aujourd'hui même les Spy Files, une liste de 1100 documents relatifs aux [...]

La planète sur écoute | Chrétienté Info | Eglise Catholique le 1 décembre 2011 - 16:29

[...] planète sur écoute Le Salon Beige , le 1 décembre 2011 Dossier intéressant sur le marché ouvert de la surveillance de masse. Pour quelle raison y échapperions-nous ? On [...]

Révolte Numérique » Wikileaks publie une carte du monde de la surveillance numérique le 1 décembre 2011 - 20:36

[...] du dossier du site OWNI fortement conseillée! – Internet massivement surveillé – Des réfugiés sur écoute – La carte d'un monde [...]

Révélations de Wikileaks sur la surveillance des communications – LCMmedia Ile Maurice le 1 décembre 2011 - 20:42

[...] de système de surveillance ont été dévoilés jeudi, en collaboration avec le site français Owni, le Washington Post, The Hindu, L'Espresso, la chaîne allemande ARD et l'ONG [...]

The Spyfiles de Wikileaks - GeekCenter le 1 décembre 2011 - 22:40

[...] une fois en partenariat avec plusieurs médias comme le Washington Post aux Etats-Unis, ou le site Owni.fr. Mais cette fois-ci, les médias ont eux aussi contribué à enrichir la base documentaire. Owni a [...]

Actualize-me » Espionnage et surveillance : WikiLeaks révèle un business mondial le 2 décembre 2011 - 1:01

[...] d'un marché mondial de la surveillance et de l'espionnage étatique. Owni note : « Ce marché de la surveillance de masse représentent désormais cinq milliards de [...]

Révélations de Wikileaks sur la surveillance des communications « My Mauritius le 2 décembre 2011 - 1:01

[...] de système de surveillance ont été dévoilés jeudi, en collaboration avec le site français Owni, le Washington Post, The Hindu, L'Espresso, la chaîne allemande ARD et l'ONG [...]

Baptisé "les documents d'espionnage", WikiLeaks évoque "l'interception massive" de populations. Des technologies vendues aux dictateurs, notamment en Libye | Résistance Inventerre le 2 décembre 2011 - 1:56

[...] éléments publiés sur Owni.fr montrent qu'Amesys ne s'est pas contentée de vendre du matériel de surveillance à la [...]

Wikileaks met un coup de pied dans le filtrage des réseaux | Allomonsite.com le 2 décembre 2011 - 2:10

[...] A ce jour, ces ventes n'entrent pas dans le spook des réglementations internationales note Owni. L'exemple de la Libye est, en Lire la suite sur l'article source: [...]

Wikileaks : les entreprises françaises qui aident les dictateurs | Gadgets Etonnants le 2 décembre 2011 - 11:41

[...] et étrangères, dont faisait partie Amesys, ont noué des liens commerciaux avec la Libye". Owni.fr précise qu'il existe 124 marchands de tels systèmes d'espionnage à travers le monde. [...]

WikiLeaks dénonce l'espionnage massif sur le Net | Gadgets Etonnants le 2 décembre 2011 - 19:36

[...] Des courriels internes publiés par WikiLeaks montreraient que la filiale sécurité de Bull a activement aidé le gouvernement libyen dirigé par le colonel Kadhafi à surveiller les communications électroniques des opposants du régime, situés en Lybie mais aussi en Europe, souligne OWNI. [...]

Internet massivement surveillé | CentPapiers le 4 décembre 2011 - 6:03

[...] ce vide juridique, comme le reconnaissait récemment Jerry Lucas, l'organisateur d'ISS1, le salon international qui rassemble tous les deux ou trois mois les professionnels de [...]

Going Digital by arslan - Peartrees le 4 décembre 2011 - 14:36

[...] La surveillance massive d'Internet révélée » OWNI, News, Augmented Dans nos démocraties, la commercialisation, et l'utilisation, de ces systèmes de surveillance et d'interception des télécommunications est strictement encadrée. Mais rien n'interdit, en revanche, de les vendre à des pays moins regardants, même et y compris à des dictatures : bien que conçus à des fins d'espionnage, ils ne font pas partie de ces armes dont l'exportation est encadrée par les lois nationales, européennes ou internationales. Ce n'est donc peut-être pas moral, mais tout à fait légal, en l'état. Et les marchands d'armes se font fort d'exploiter ce vide juridique, comme le reconnaissait récemment Jerry Lucas, l'organisateur d'ISS, le salon international qui rassemble tous les deux ou trois mois les professionnels de l'interception des communications : 87 vendent des outils, systèmes et logiciels de surveillance de l'Internet, 62 de surveillance du téléphone, 20 des SMS, 23 font de la reconnaissance vocale, et 14 de la géolocalisation GPS. [...]

Julian Assange : nous sommes tous sous surveillance | Fredzone le 5 décembre 2011 - 12:31

[...] En fait, tout est de la faute du capitalisme. En effet, c'est un réseau de firmes spécialisées dans la surveillance de masse qui vendraient à certains gouvernements des solutions pour mieux contrôler les foules. Parmi ces entreprises, on trouverait Qosmos, Nice, Amesys ou... Nokia-Siemens. Mieux, leurs technologies permettrait

d'espionner la totalité des flux du web mais aussi l'intégralité des échanges téléphoniques (SMS et MMS inclus, forcément). Alors bien sûr, dans les pays démocratiques, nos dirigeants ne peuvent pas faire n'importe quoi (enfin c'est ce qu'on dit, en tout cas), mais il n'en va évidemment pas de même pour les dictatures de ce monde et ces dernières seraient d'ailleurs de très bons clients de toutes les sociétés spécialisées dans ce secteur. Pour en savoir un peu plus sur le sujet, je vous invite d'ailleurs à lire l'article publié chez Owni.fr. [...]

Edito du 05/12: Streaming et Spy Files | Gizeek le 5 décembre 2011 - 13:48

[...] y a donc une demande forte. Je ne peux que vous conseiller la lecture de ces articles d'Owni: <http://owni.fr/2011/12/01/spy-files-interceptions-ecoutes-wikileaks-qosmos-amesys-libye-syrie/> Le dossier: <http://owni.fr/navigation-temporelle/?jour=2&mois=12&annee=2011> Et bien sûr [...]

Surveillance d'Internet décembre 2011 by josselinhenno - Pearltrees le 5 décembre 2011 - 16:52

[...] Internet massivement surveillé » OWNI, News, Augmented WikiLeaks rend public aujourd'hui près de 1 100 documents internes, plaquettes commerciales et modes d'emploi des produits commercialisés par les industriels des systèmes de surveillance et d'interception des télécommunications. [...]

internet - liberté by stz - Pearltrees le 5 décembre 2011 - 17:09

[...] Ces nouvelles fuites montrent un marché de la surveillance de masse représentant désormais cinq milliards de dollars, avec des technologies capables d'espionner la totalité des flux Internet et téléphoniques à l'échelle d'une nation. Les fleurons de ce marché s'appellent Nokia-Siemens, Qosmos, Nice, Verint, Hacking Team, Bluecoat ou Amesys. Les documents détaillant leurs capacités d'interception, contenant une multitude de détails technologiques, seront progressivement mis en ligne par WikiLeaks. OWNI, partenaire de cette opération baptisée SpyFiles avec le Washington Post, The Hindu, L'Espresso, la chaîne allemande ARD et l'ONG britannique The Bureau of Investigative Journalism a tenté de visualiser cette industrie d'un genre nouveau, en créant une cartographie interactive sur un site dédié, SpyFiles.org. Internet massivement surveillé » OWNI, News, Augmented [...]

La vengeance dans le lien | MatooBlog le 5 décembre 2011 - 23:42

[...] Le marché de la surveillance globale du web est en explosion, et la France est un des bons fournisseurs mondiaux de systèmes logiciels de traque via internet. On comprend rapidement dans cet excellent article à quel point l'hypocrisie est grande et simple entre se targuer d'un réseau qui libère les opprimés, tout en commercialisant les outils pour réprimer encore plus. L'exact parallèle avec le commerce des armes est permis évidemment. #armes #trackingsystems #internet #liberté #hypocrisie [...]

Blue Coat Systems, des SpyFiles de WikiLeaks à la Syrie de Bachar el-Assad | NewZilla.NET le 6 décembre 2011 - 5:59

[...] 2.0. {lang: 'fr'}ShareLa récente publication par WikiLeaks, reprise en France par le site Owni.fr, de 287 documents baptisés SpyFiles, jette une lumière drue sur un monde parallèle, le plus [...]

Toute l'actualité de la High Tech - Semaine 49 le 10 décembre 2011 - 15:21

[...] vous recommande la lecture d'Owni qui consacre un excellent article à ce [...]

DOCS by tourist.information - Pearltrees le 12 décembre 2011 - 0:21

[...] Internet massivement surveillé » OWNI, News, Augmented Dans nos démocraties,

la commercialisation, et l'utilisation, de ces systèmes de surveillance et d'interception des télécommunications est strictement encadrée. Mais rien n'interdit, en revanche, de les vendre à des pays moins regardants, même et y compris à des dictatures : bien que conçus à des fins d'espionnage, ils ne font pas partie de ces armes dont l'exportation est encadrée par les lois nationales, européennes ou internationales. Ce n'est donc peut-être pas moral, mais tout à fait légal, en l'état. Et les marchands d'armes se font fort d'exploiter ce vide juridique, comme le reconnaissait récemment Jerry Lucas, l'organisateur d'ISS, le salon international qui rassemble tous les deux ou trois mois les professionnels de l'interception des communications : [...]

ویکی لیکس: افشای شرکت هایی که تجهیزات جاسوسی به دیکتاتورها می فروشند! « آقا اجازه؟ » le 13 décembre 2011 - 23:32

اسناد تمام شرکت OWNI و سازمان فرانسوی Bureau of Investigative Journalism بریتانیایی [...] [...] هایی که تجهیزات نرم افزاری و مخابراتی

Internet massivement surveillé « annie bannie's Weblog le 14 décembre 2011 - 15:16

[...] le 1 décembre 2011 – 2:04 Signaler un abus – [...]

(H)activisme by stonehenge - Pearltrees le 16 décembre 2011 - 1:30

[...] La surveillance massive d'Internet révélée » OWNI, News, Augmented Dans nos démocraties, la commercialisation, et l'utilisation, de ces systèmes de surveillance et d'interception des télécommunications est strictement encadrée. Mais rien n'interdit, en revanche, de les vendre à des pays moins regardants, même et y compris à des dictatures : bien que conçus à des fins d'espionnage, ils ne font pas partie de ces armes dont l'exportation est encadrée par les lois nationales, européennes ou internationales. Ce n'est donc peut-être pas moral, mais tout à fait légal, en l'état. [...]

Retranscription de la #Conf #DPI du 14.12.11 à l'Assemblée Nationale | Patchidem le 17 janvier 2012 - 22:18

[...] de la société Amesys que vous avez cité d'ailleurs dans un article publié sur le site Owni cet après-midi. Interrogé sur le fait que ce type de pratique commerciale pouvait porter un coup [...]

Anonymous fuck You ! is not good? - FAICMFSF_FAICMFSF le 20 janvier 2012 - 19:23

[...] Internet massivement surveillé [...]

Source | Nous avons tous quelque chose à cacher le 8 février 2012 - 7:42

[...] Benjamin Franklin. Les exemples sont nombreux, et font ponctuellement l'actualité : – OWNI et Wikileaks qui publient une compilation de documents publics concernant des sociétés spécialisées dans [...]

Anonymous fuck You ! is not good? - FAICMFSF le 20 février 2012 - 14:04

[...] Internet massivement surveillé [...]

189 » NEW R-sistons à la crise le 24 février 2012 - 16:28

[...] SpyFiles, cette nouvelle opération de Wikileaks menée en partenariat avec plusieurs médias, dont Owni en France, épingle des grands noms de l'industrie comme Nokia-Siemens, Qosmos, Thales, Bluecoat, [...]

