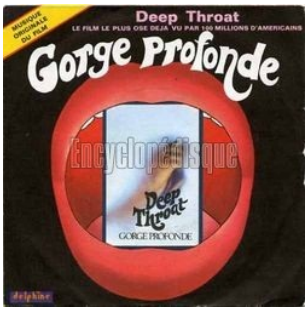
GORGE PROFONDE: LE MODE D'EMPLOI

LE 1 JUIN 2010 ***JEAN MARC MANACH***

Balancer un document confidentiel à Wikileaks, c'est bien. Permettre aux rédactions, journalistes, blogueurs, ONG, de créer leur propre Wikileaks, c'est mieux.



Le Net a beau être surveillé à l'envi, il est tout à fait possible de **contourner la cybersurveillance** (voir aussi mon **petit manuel de contre-espionnage informatique**). Restait à expliquer comment contacter quelqu'un, facilement, de façon sécurisée, et en toute confidentialité.

MaJ : article traduit en italien : ***Gola profonda: come assicurare la copertura delle fonti nell' era della sorveglianza totale***

Le Watergate n'aurait jamais eu lieu et entraîné la démission du président des États-Unis ni contribué à sacraliser de la sorte le journalisme d'investigation **si une "*gorge profonde*"** -du nom du **film X** qui, au même moment révolutionna les mentalités- **n'avait révélé, *en toute confidentialité* ,** à deux journalistes du **Washington Post les dessous de cette affaire** d'espionnage politique mêlant obstructions à la justice, faux témoignages, écoutes clandestines, détournements de fonds, etc.

Les **méthodes de communication** utilisées par **Bob Woodward** et **Carl Bernstein**, les deux journalistes, avec leur "*gorge profonde*" et les façons de garantir son anonymat font encore débat.

Il a fallu attendre 2005 pour que **William Mark Felt**, qui était à l'époque du Watergate le n°2 du FBI, **révèle** qu'il fut la "*gorge profonde*" du Watergate. Quel qu'il soit, leur mode opératoire a donc marché : nul n'a su qui, à l'époque, les avait contacté, ni comment ils avaient procédé… sinon qu'ils avaient probablement pour cela utilisé des méthodes dignes de polars, ou d'histoires d'espionnage.

Dans les années 70, tout comme aujourd'hui, les téléphones étaient écoutables. Le problème, aujourd'hui, c'est que l'Internet en particulier, et l'ensemble de nos télécommunications en général, sont **systématiquement** conservées, voire surveillées. L'informatique laisse des traces (qui communique avec qui, quand, pendant combien de temps), conservées par principe par les opérateurs de télécommunications (afin de se prémunir de tout litige).

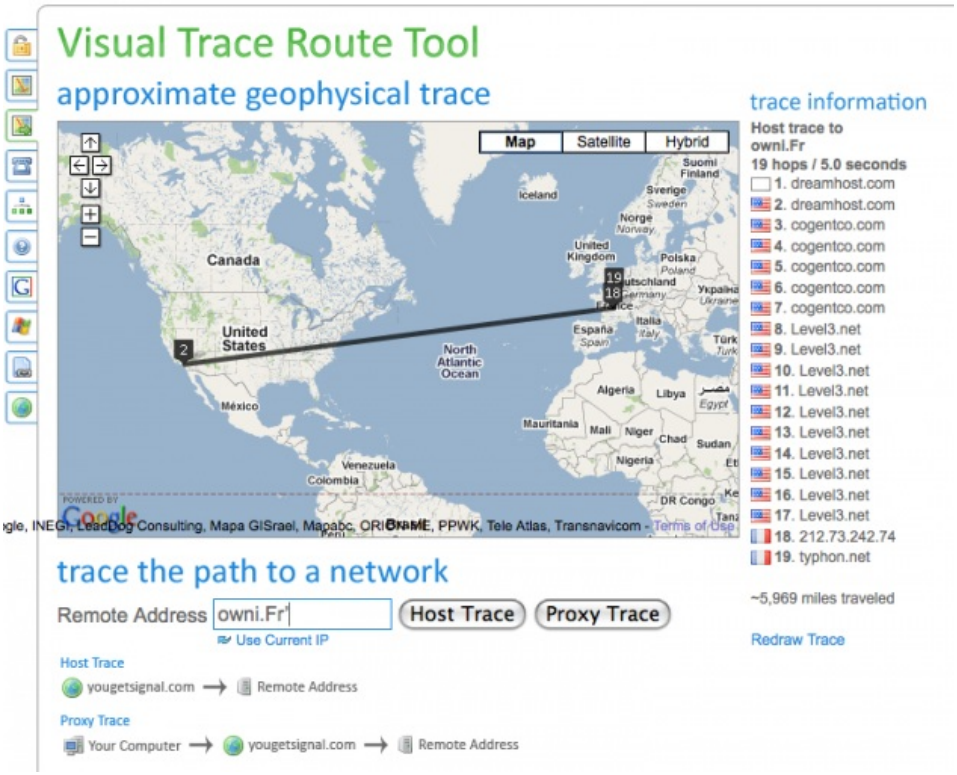
Les autorités obligent parfois ces mêmes opérateurs à conserver lesdites traces "*au cas où*" (**y compris en France** par exemple, et sans parler des systèmes de surveillance mis en place, souvent par des entreprises occidentales, dans les pays autoritaires).

Rajoutons-y un brin d'**Echelon** (le système global d'espionnage des télécommunications mis en place par les pays anglo-saxons), de **Frenchelon** (son "petit" équivalent français) et de leurs avatars exotiques, sans oublier, bien sûr, les systèmes et logiciels espions utilisés tant par les services de renseignement que par les officines d'intelligence économique (montés, ou truffés, d'anciens espions), les mouchards utilisés par les détectives privés, les employeurs qui veulent ainsi surveiller leurs employés, et de plus en plus de particuliers afin d'espionner leurs femmes, maris, nounous et enfants…

Le tableau n'est donc guère réjouissant, et l'on pourrait croire qu'il serait donc de plus en plus difficile, pour un journaliste ou n'importe quel autre professionnel censé garantir la confidentialité de ses sources, de pouvoir travailler correctement, dans la mesure où la surveillance, non contente de se banaliser de la sorte, deviendrait la règle, et non plus l'exception, comme c'était encore le cas du temps du Watergate.

De fait, le meilleur moyen de garantir la confidentialité de ses sources est encore… de ne pas passer par le Net, mais par le courrier papier : contrairement aux télécommunications (mail, tel, fax, SMS, etc.), les enveloppes papier sont fermées, rarement

surveillées et encore plus rarement ouvertes, alors que nos courriels sont, eux, d'autant moins confidentiels qu'ils ne sont jamais que des cartes postales, dont le contenu est lisible en clair par l'ensemble des serveurs (souvent plus d'une dizaine) par lesquels ils transitent.



De fait, aucune rédaction, aucun journaliste, n'explique aux gens comment les contacter *de façon simple, sécurisée, et en toute confidentialité* . Les seuls à le proposer sont un architecte fervent défenseur de la liberté d'expression, John Young, qui diffuse sur son site, **cryptome**, depuis des années, des documents confidentiels qui lui sont envoyés par email (**chiffrés ou non**) et **Wikileaks**, créé tout spécialement pour faciliter ce genre de "*fuites*" de documents confidentiels.

Il existe pourtant plusieurs possibilités, habilement mises en place par des hackers, ces "**bidouilleurs de la société de l'information**" sans qui l'informatique en général, et l'Internet en particulier, n'auraient pas été possibles.

Les développeurs et utilisateurs de logiciels libres utilisent ainsi, et depuis des années, un logiciel de **cryptographie** permettant de garantir, non seulement la confidentialité de leurs télécommunications, mais également leur authenticité, et leur intégrité, afin de s'assurer que les informations échangées proviennent bien, ou ne pourront être lues, que par tel ou tel individu dûment identifié, et non par quelqu'un qui chercherait à usurper son identité, ou bien à l'espionner : **GPG** (Gnu Privacy Guard, **mode d'emploi**).

Problème (bis) : bien moins nombreux sont nos lecteurs, internautes, informateurs, à savoir que GPG existe, et donc à s'en servir pour nous contacter. Or, et a priori, seuls les utilisateurs de GPG (ou de **PGP**, son précurseur) peuvent "*chiffrer*" leurs messages de sorte qu'ils ne puissent être consultables, "*en clair*" que par leurs seuls destinataires : la sécurité de la **cryptographie à clef publique** repose en effet sur le fait que les personnes qui veulent ainsi s'échanger des données, en toute confidentialité, utilisent GPG (ou PGP).

A défaut, on peut utiliser une adresse e-mail jetable, ce que propose par exemple **anonbox**, créé par les hackers du Chaos Computer Club allemand afin d'envoyer ou recevoir des documents anonymement. Problème : elle n'est valable qu'un jour durant.

Lancé par la **Privacy Foundation** allemande, une ONG de défense de la vie privée et de la liberté d'expression, **privacybox.de** fait encore mieux, dans la mesure où elle permet à tous ceux qui ne peuvent ou ne veulent pas utiliser GPG ou PGP d'écrire de façon confidentielle, anonyme et sécurisée, à tout journaliste, blogueur ou internaute qui, utilisateur de GPG ou de PGP, s'y est inscrit (et c'est gratuit, forcément, et puis facile, aussi).

Mieux : plusieurs lecteurs ont bien voulu mettre la main à la pâte et traduire son interface **en français** (qu'ils en soient remerciés)~~, mais il reste encore quelques pages à traduire :~~
~~**https://privacybox.de/howto.en.html**~~
~~**https://privacybox.de/howto-apple-mail.en.html**~~
~~**https://privacybox.de/nutzen.en.html**~~

~~**https://privacybox.de/eval.en.html**~~

Les bonnes âmes peuvent me contacter par mail à privacybox[AT]rewriting.net, ou bien encore via le formulaire de **privacybox**.

Je ne sais combien de blogueurs, journalistes, rédactions ou ONG utiliseront ce service. Mais si ça peut aider, et notamment les journalistes d'investigation, et les **lanceurs d'alerte**…

Les hackers ne sont pas une partie du problème : ils nous donnent des solutions. Faites tourner !

—

> Illustration CC Flickr **Anonymous9000**

Retrouvez les deux articles de ce troisième volet du manuel de contre-espionnage informatique : **Votre historique mis à nu** et **Retour sur 10 ans de Big Brother Awards**.

Retrouvez également le **premier** et le **second** volet de notre série sur le contre-espionnage informatique.

METTOUT
le 1 juin 2010 - 18:08 • SIGNALER UN ABUS - PERMALINK

Bonjour Manach, reprends-moi si je me trompe, mais il me semblait que le cryptage des communications, à un niveau qui permette de tromper les services de sécurité, était interdit en France? Si c'est le cas, est-ce que ça remet en cause tout ou partie des méthodes ci-dessus? Merci de ta réponse.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

JEAN MARC MANACH
le 1 juin 2010 - 18:37 • SIGNALER UN ABUS - PERMALINK

Bonjour Mettout, le chiffrement a effectivement été considéré comme une arme de guerre jusqu'en 1996; il a ensuite été libéralisé en 2001 afin de contribuer à l'essor du commerce électronique, et a depuis été complètement libéralisé par la Loi pour la confiance dans l'économie numérique de 2004.

Tu as donc, au choix, 14, 9 ou juste 6 ans de retard sur la législation… signe que la diabolisation de la cryptographie, et des outils utilisés par les hackers (qui ne sont donc pas des crypto-pédo-terroristes, mais rien moins que la cheville ouvrière du développement du Net) a bien fonctionné, hélas ;-(

En espérant avoir répondu à tes questions
Et en espérant aussi que nombreux seront les journalistes, et/ou les rédactions, à se mettre ainsi à GPG, et à la protection de leurs sources.

cordialement,
jmm

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MEXI
le 1 juin 2010 - 19:36 • SIGNALER UN ABUS - PERMALINK

il existe aussi

enigmail :

http://enigmail.mozdev.org/home/index.php

ou 7-zip

http://www.7-zip.org/

merci encore pour tout tes articles ;)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

JOUR DE FÊTE
le 2 juin 2010 - 18:54 • SIGNALER UN ABUS - PERMALINK

Au-delà du cas des «lanceurs d'alerte», je considère qu'il y a aujourd'hui un gros problème au niveau de la correspondance électronique (les «e-mails») : que ce soit GPG / PGP ou autres, on est encore au même stade qu'au début !

Même les organismes «sérieux» (voire même très sérieux) n'utilisent aucun des moyens qui existent. Et comme il faut que la clé publique soit disponible, ça n'avance pas… le paradoxe de l'œuf et de la poule, quoi.

Je crois que c'est un gros problème… qui dépasse le cas des «lanceurs d'alerte». Ne pas pouvoir avoir un système de correspondance (électronique) sur lequel on peut compter, ce n'est pas bon… pour tout le monde !

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OLIVIER
le 3 juin 2010 - 8:55 • SIGNALER UN ABUS - PERMALINK

Bonjour Manach,

Pour les emails "jettables" et "anonymes" je recommande le service yopmail.com , qui permet d'utiliser des adresses emails à la demande et sans mot de passe. Peut-être que la meilleure façon de se cacher est de rester public ?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MALCOLM
le 3 juin 2010 - 9:44 • SIGNALER UN ABUS - PERMALINK

Via le formulaire je vous ai envoyé en version word la traduction des 4 pages, je tiens à faire remarquer que quelques autres, aussi bien en français qu'en anglais contiennent des fautes.

Cordialement,

Malcolm

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CITIZENCLO
le 16 décembre 2010 - 11:05 • SIGNALER UN ABUS - PERMALINK

Passionnant! Merci Jean-Luc!
J'espère que tu vas bien depuis les entretiens du Webjournalisme de Metz.
Toujours partant pour lancer une campagne européenne en vue d'un Freedom of Information Act? Oui, tu as raison, c'est politique… Mais tout est politique, pas vrai et à l'heure où des bloggers – mais lesquels – sont invités à déjeûner à l'Elysée…il faudrait bien que nous pensions à avoir quelque chose à nous mettre sous la dent! Non?
On en cause demain à la soucoupe?
Claudine
http://www.citizenclo.wordpress.com
http://www.bloggerswithoutborders.wordpress.com
http://www.republiquevirtuelle.wordpress.com

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MAXY35
le 20 décembre 2010 - 23:03 • SIGNALER UN ABUS - PERMALINK

Bonjour,
Article intéressant, comme toujours. Mais, si j'ai déjà eu la tentation d'installer GPG, par simple principe de citoyen qui n'a pas envie d'être surveillé par big brother, j'y ai finalement renoncé en me disant qu'il était plus facile de passer inaperçu que de faire

des efforts trop visibles pour se cacher. Tu écris :
la sécurité de la cryptographie à clef publique repose en effet sur le fait que les personnes qui veulent ainsi s'échanger des données, en toute confidentialité, utilisent GPG (ou PGP).
Si j'étais chargé de surveiller les communications, je surveillerais particulièrement celles-là, non ? Bien sûr, le surveillant que je serais ne pourrait pas déchiffrer les messages, mais il pourrait assez vite trouver qui les envoie à qui, d'où à où, etc. C'est d'ailleurs ce que disait le patron du contre-espionnage français, si je me souviens bien.
Bonne continuation en tous cas.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GLB
le 8 mars 2011 - 12:14 • SIGNALER UN ABUS - PERMALINK

Bonjour,

Il existe des solutions facilement utilisables pour echanger des donnees de maniere securisee. Exemple RetroShare, egalement base sur PGP (http://retroshare.sourceforge.net).

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

BONKSA
le 15 septembre 2011 - 17:02 • SIGNALER UN ABUS - PERMALINK

Gorge profonde : mode d'emploi

ca fait vomir ce titre, hyper sexiste, ca sonne hyper révolutionnaire en tout cas !! ?

je vois d'autres noms bien glauque plus appropriés et vulgaires, genre petite bites, révoltez vous ou que sais je !!

Il vous aura peut-être échappé que Gorge Profonde (Deep Throat) fut le surnom donné à William Mark Felt , cet agent du FBI américain, devenu numéro deux de cette agence à la fin des années 1960 qui fut la source des deux journalistes du Washington Post qui seront à l'origine de l'affaire du Watergate, conduisant à la démission du Président Nixon en 1974… Personne ne sut jamais qui il était (le côté protection des sources) jusqu'à ce qu'il le révèle lui-même en 2005.

jmm

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PC REPAIR MIAMI
le 11 novembre 2011 - 1:15 • SIGNALER UN ABUS - PERMALINK

I definitely enjoy every little bit of it and I have bookmarked your blog.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

JULIE
le 18 mars 2012 - 13:11 • SIGNALER UN ABUS - PERMALINK

Oh que oui, cela peut aider et que l'on devrait tous l'utiliser… Seulement, ce n'est pas si facile. Quand tu es su le terrain et qu'un red chef veut recevoir sons ou papiers par mail et ne connait rien du tout à tout ça. Ca m'est arrivé en Syrie au tout début de l'insurrection… Et pas question de laisser les pièces jointes en brouillon, ils ne comprenaient pas non plus comment aler les récupérer…
Ce sont les red chefs et chefs de rubrique qu'il faudrait former (et de toute urgence. Certains appartiennent à l'ancienne génération. ils peuvent être très bon dans ce qu'ils font, là n'est pas le problème, mais il faudrait qu'ils comprennent que parfois, en obligeant les gens sur le terrain à envoyer des mails en clair ou en faisant des directs par téléphone, ils mettent vraiment leur équipe ou les "freelances" avec qui ils travaillent, en danger.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

19 pings

Les tweets qui mentionnent Gorge profonde: le mode d'emploi » Article » owni.fr, digital journalism -- Topsy.com le 1 juin 2010 - 17:01

[...] Ce billet était mentionné sur Twitter par Owni, Arnaud Bousquet. Arnaud Bousquet a dit: Gorge profonde: contre espionnage et watergate où en sommes nous ? http://tinyurl.com/3477m58 #owni [...]

Votre historique mis à nu » Article » owni.fr, digital journalism le 1 juin 2010 - 21:23

[...] powered by BackType Sur owni à la une les derniers articles votre sélection Gorge profonde: le mode d'emploi Le Mardi 1 juin 2010 I Partager Écrit par Jean Marc [...]

Renseignement Economique I Archives de Sécurité Tube le 2 juin 2010 - 8:47

[...] Gorge profonde: le mode d'emploi » Article » owni.fr, digital … [...]

Retour sur 10 ans de Big Brother Awards » Article » owni.fr, digital journalism le 2 juin 2010 - 15:37

[...] powered by BackType Sur owni à la une les derniers articles votre sélection Gorge profonde: le mode d'emploi Le Mardi 1 juin 2010 I Partager Écrit par Jean Marc [...]

WikiLeaks « Antoine Singer le 2 juin 2010 - 18:59

[...] Une révélation étonnante, tant pour ce qui est des méthodes de Wikileaks que pour ce qui est de la compétences des espions informatiques chinois, et alors que je viens précisément de publier un mode d'emploi expliquant comment protéger ses sources en leur permettant de vous contacter facilement, de façon sécurisée, et en toute confidentialité : Gorge profonde, mode d'emploi. [...]

Techniques de contre-espionnage : se protéger des Etats et des professionnels « Guillaume Payre's new blog le 3 juin 2010 - 0:17

[...] – Article sur comment échanger des informations sur Internet anonymement avec messagerie anonyme et c…. [...]

Il giornalismo investigativo, il non profit e il trattamento delle fonti: due articoli su Lsdi le 5 juin 2010 - 0:37

[...] In lingua originale: Gorge profonde: le mode d'emploi [...]

JEAN-MARC MANACH: « LE PROBLÈME C'EST LA SURVEILLANCE, PAS LA TRANSPARENCE « Libertes & Internets le 2 juillet 2010 - 9:10

[...] contourner la cybersurveillance ?, mon Petit manuel de contre-espionnage informatique, ainsi que Gorge profonde, le mode d'emploi, qui explique comment garantir la confidentialité de ses sources, un devoir professionnel pour [...]

Les effets de bord de la mise en place la HADOPI gênent les Etats Unis « My Life le 4 octobre 2010 - 13:12

[...] Les internautes sont ainsi de plus en plus nombreux à faire de la crypto comme Mr Jourdain faisait de la prose, sans parler de ceux, de plus en plus nombreux, qui chiffrent sciemment leurs communications, par obligation professionnelle ou par convenance personnelle, pour se protéger de l'espionnage industriel ou encore de la cybersurveillance que des entreprises comme TMG effectue au profit de l'Hadopi (voir Gorge profonde : mode d'emploi). [...]

Frenchelon, les grandes oreilles à la française de la DGSE / IG le 11 octobre 2010 - 11:46

[...] Et pas seulement : les internautes sont ainsi de plus en plus nombreux à faire de la crypto comme Mr Jourdain faisait de la prose, sans parler de ceux, de plus en plus nombreux, qui chiffrent sciemment leurs communications, par obligation professionnelle ou par convenance personnelle, pour se protéger de l'espionnage industriel ou encore de la cybersurveillance que des entreprises comme TMG effectue au profit de l'Hadopi (voir Gorge profonde : mode d'emploi). [...]

"Allô, c'est Julian Assange" » Article » OWNI, Digital Journalism le 22 octobre 2010 - 22:53

[...] informations que vous voulez transmettre de manière sécurisée, utilisez le service Privacy Box, détaillé sur OWNI, à l'adresse [...]

L'enfer, c'est les « internautres » | BUG BROTHER le 1 juin 2011 - 19:16

[...] précisément rédigé afin de défendre les libertés, et la vie privée, des "internAutres" : Gorge profonde : le mode d'emploi Journalistes : protégez vos sources ! Petit manuel de contre-espionnage informatique Comment [...]

Peut-on obliger les policiers à violer la loi ? | BUG BROTHER le 15 septembre 2011 - 16:31

[...] Ceux qui, à l'instar de Thierry V., de Philippe Pichon ou de cet ancien policier "sans casque ni bouclier", voudraient eux aussi témoigner de la réalité de leur métier, et des dysfonctionnements de l'institution, peuvent me contacter en toute confidentialité, via le formulaire sécurisé de privacybox.de (n'oubliez pas d'y préciser une adresse e-mail, même anonyme, que je puisse vous recontacter et, pour plus d'explications, cf Gorge profonde, le mode d'emploi). [...]

Hadopi : la France s'est fait "engueuler" par les Etats-Unis | VOI38.com le 7 février 2012 - 17:00

[...] > Société 2.0 – Les services de renseignement américains n'aiment pas du tout l'idée que la chasse aux pirates incite les internautes à user d'outils de cryptologie jusqu'à présent utilisés essentiellement par les réseaux criminels et terroristes. Ils auraient « engueulé » la France par crainte que la loi Hadopi ne rende difficile l'identification d'activités suspectes sur le réseau. L'information avait déjà filtré sous la plume d'un ingénieur d'Orange qui, en mai 2009, avait expliqué les dangers de l'Hadopi pour le gouvernement français. Elle est aujourd'hui confirmée par Jean-Marc Manach qui, au détour d'un billet passionnant sur un colloque dédié à la cryptographie, cite sur son blog Bug Brother les propos du directeur technique de la Direction Générale de la Sécurité Extérieure (DGSE). En s'obstinant dans la voie de la riposte graduée, la France incite les internautes lambdas à s'armer des mêmes outils de chiffrage de leurs communications que ceux employés par les réseaux criminels, ce qui rend ces derniers difficilement reconnaissables : Les internautes sont ainsi de plus en plus nombreux à faire de la crypto comme Mr Jourdain faisait de la prose, sans parler de ceux, de plus en plus nombreux, qui chiffrent sciemment leurs communications, par obligation professionnelle ou par convenance personnelle, pour se protéger de l'espionnage industriel ou encore de la cybersurveillance que des entreprises comme TMG effectue au profit de l'Hadopi (voir Gorge profonde : mode d'emploi). [...]

« Au Pays de Candy », mon livre, en ligne | BUG BROTHER le 16 mars 2012 -

15:02

[...] n'oubliez pas d'y laisser une adresse email valide (mais anonyme). PLus d'explications : « Gorge profonde: le mode d'emploi » et « Petit manuel de contre-espionnage informatique ». Voir aussi [...]

OUTILS | Pearltrees le 22 mars 2012 - 15:49

[...] Gorge profonde: le mode d'emploi » OWNI, News, Augmented Le Watergate n'aurait jamais eu lieu et entraîné la démission du président des États-Unis ni contribué à sacraliser de la sorte le journalisme d'investigation si une " gorge profonde " -du nom du film X qui, au même moment révolutionna les mentalités- n'avait révélé, en toute confidentialité , à deux journalistes du Washington Post les dessous de cette affaire d'espionnage politique mêlant obstructions à la justice, faux témoignages, écoutes clandestines, détournements de fonds, etc. MaJ : article traduit en italien : Gola profonda: come assicurare la copertura delle fonti nell' era della sorveglianza totale [...]

Securite | Pearltrees le 17 avril 2012 - 1:29

[...] Le Watergate n'aurait jamais eu lieu et entraîné la démission du président des États-Unis ni contribué à sacraliser de la sorte le journalisme d'investigation si une " gorge profonde " -du nom du film X qui, au même moment révolutionna les mentalités- n'avait révélé, en toute confidentialité , à deux journalistes du Washington Post les dessous de cette affaire d'espionnage politique mêlant obstructions à la justice, faux témoignages, écoutes clandestines, détournements de fonds, etc. MaJ : article traduit en italien : Gola profonda: come assicurare la copertura delle fonti nell' era della sorveglianza totale Les méthodes de communication utilisées par Bob Woodward et Carl Bernstein , les deux journalistes, avec leur " gorge profonde " et les façons de garantir son anonymat font encore débat. Le Net a beau être surveillé à l'envi, il est tout à fait possible de contourner la cybersurveillance (voir aussi mon petit manuel de contre-espionnage informatique). Gorge profonde: le mode d'emploi » OWNI, News, Augmented [...]

« Faites chier, vous avez encore ramené un mineur ! » | BUG BROTHER le 13 juillet 2012 - 9:01

[...] Pour me contacter de façon anonyme et sécurisée, en toute confidentialité, utilisez donc ma clef GPG. Si vous ne savez pas utiliser GPG, passez par ma privacybox (n'oubliez pas d'y préciser votre mail pour que je puisse vous recontacter -pour plus d'explications, cf Gorge profonde, le mode d'emploi). [...]

Tout le monde à droit à son 1/4h d'anonymat | BUG BROTHER le 2 novembre 2012 - 9:11

[...] travaille. Cf ces quelques articles et modes d'emploi que j'ai eu l'heur de consacrer à ce sujet : Gorge profonde : le mode d'emploi Journalistes : protégez vos sources ! Comment contourner la cybersurveillance ? Petit manuel de [...]