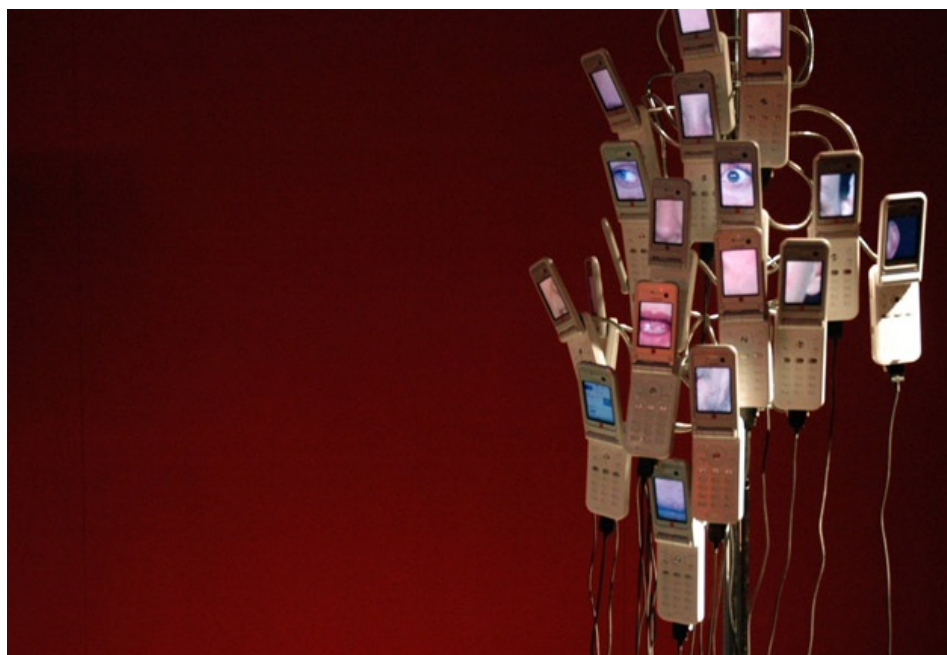


DES SMS FURTIFS SUR VOS PORTABLES

LE 26 JANVIER 2012 **FABIEN SOYEZ**

Les services de sécurité envoient des milliers de SMS furtifs pour localiser des personnes et réactiver leur téléphone à distance. Une technologie jusque-là méconnue, et pas vraiment encadrée par le droit. L'affaire fait grand bruit chez les experts allemands, avec lesquels nous nous sommes entretenus. En France, plusieurs acteurs nous ont concédé, du bout des lèvres, que ce procédé était également utilisé.



C'est une **question au gouvernement** qui nous a mis la puce à l'oreille. En juin 2011, Colette Giudicelli, sénatrice des Alpes Maritimes, écrit à Claude Guéant, ministre de l'intérieur :



Plusieurs services de police judiciaire et de renseignement étrangers utilisent des SMS furtifs pour localiser des suspects ou des personnes disparues : cette méthode consiste à envoyer vers le téléphone portable de ce suspect un SMS qui passe inaperçu et renvoie un signal à l'émetteur du message. Mme Colette Giudicelli aimerait savoir si cette procédure est déjà utilisée en France.



Sept mois plus tard, toujours pas de réponse du gouvernement. Le sujet aurait pu tomber aux oubliettes s'il n'y avait eu, fin décembre, la 28ème édition du **Chaos Communication Congress**, à Berlin. Lors de cette conférence de hackers, le chercheur Karsten Nohl expert en sécurité de mobiles **lance** : "En Allemagne, la police a envoyé en 2010 des milliers de SMS furtifs pour localiser des suspects."

Le SMS furtif obéit au principe du signal aller-retour que l'on ne voit pas, ou du "ping" dans le jargon des informaticiens. Les développeurs de la société **Silent Services**, à l'origine d'un des premiers logiciels permettant d'envoyer ce genre de SMS, expliquent :



Les SMS furtifs vous permettent d'envoyer un message à un autre

portable à l'insu de son propriétaire. Le message est rejeté sur le téléphone de ce dernier et il n'existe aucune trace. Vous obtenez, en retour, un message de l'opérateur vous attestant que votre message a été reçu.



Techniquement, les **SMS furtifs**, ou “*silent SMS*”, serviraient donc à savoir si une personne a allumé son portable et permettraient aux opérateurs de “*tester*” les réseaux, sans gêner les usagers. Mais une toute autre utilisation en est faite par les services de renseignement et la police. Contacté par *OWNI*, Neil Croft, diplômé du département des sciences informatiques de l'Université de Pretoria, en Afrique du Sud, explique :



Envoyer un SMS furtif, c'est comme envoyer un SMS normal, sauf que le mobile ne voit pas le message qu'il a reçu. Les informations du SMS sont modifiées, dans le programme de codage des données, pour que l'utilisateur qui le reçoit ne s'aperçoive de rien. Un SMS furtif peut aider les services de police à détecter un mobile sans que la personne concernée soit au courant de la requête.



Pour trafiquer les informations du SMS et le rendre silencieux, les services de sécurité passent par une passerelle SMS, comme **Jataayu SMS gateway**, qui permet d'interconnecter les systèmes GSM et informatique. Neil Croft, désormais président d'une **société de marketing par SMS**, nous explique :



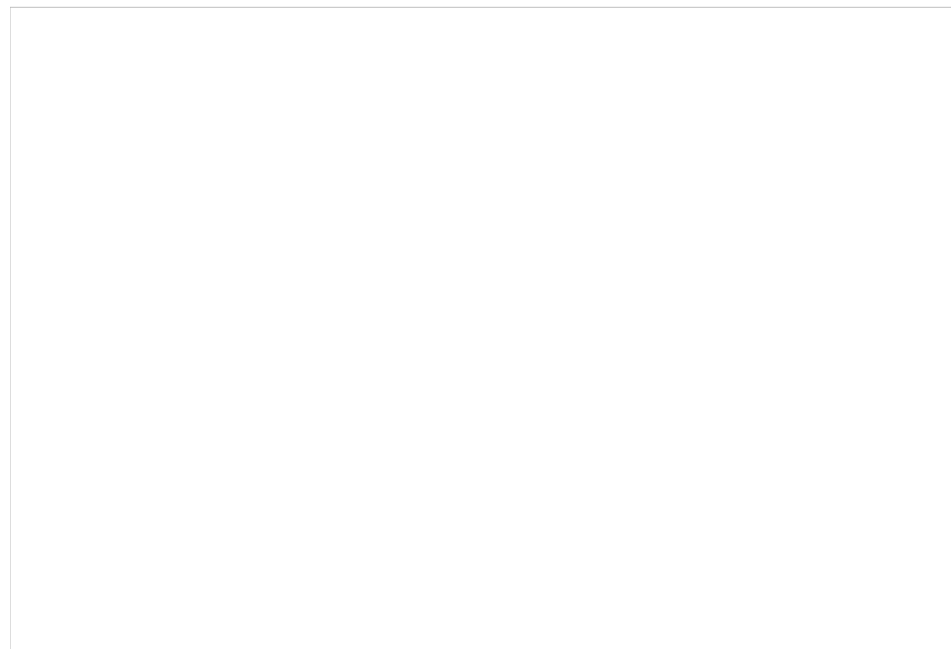
Ces SMS furtifs sont aussi utilisés par certains hackers pour mener des attaques dites “de déni de service” (DDOS). Le résultat, c'est une batterie qui se décharge anormalement vite, et l'impossibilité de recevoir des appels. Un tel procédé ne coûte pas cher : on peut envoyer un SMS furtif par seconde pendant une heure pour environ 36 euros.



Ce procédé d'envoi en masse apparaît largement utilisé par les services. En novembre 2011, **Anna Conrad**, du parti Die Linke (La Gauche), pose une **question écrite** au Landtag de Rhénanie du Nord-Westphalie, à propos de l'usage par la police allemande de SMS furtifs, ou "Stille SMS". **Réponse du Parlement local** : en 2010, le Land a mené 778 enquêtes et envoyé 256 000 SMS furtifs. Mais pour Mathias Monroy, journaliste à **Heise online** ces technologies de surveillance profitent surtout d'un vide juridique :



C'est très problématique pour la vie privée, parce que juridiquement, on ne sait pas si les SMS furtifs sont ou non une communication (...) Le Land a considéré que ce n'en était pas une, puisqu'il n'y a aucun contenu. C'est pratique, car s'il ne s'agit pas d'une communication, cela ne rentre pas dans le cadre de l'inviolabilité des télécommunications de l'article 10 de la Constitution allemande.



Mais le 6 décembre, suite à une question d'un député de gauche, Andrej Hunko, sur l'utilisation des SMS furtifs par la police allemande, le ministre de l'intérieur a joué le jeu de la **transparence**. Au total, ces dernières années, les services de police et de renseignement allemands auront **envoyé** une moyenne de 440 000 SMS furtifs en un an.

Après chaque SMS envoyé, le lien était fait avec **Vodafone, E-Plus, O2 et T-Mobile**, les quatre opérateurs de téléphonie mobile, afin d'accéder aux informations de communication des personnes surveillées. Pour agréger les données brutes fournies par les opérateurs, la police allemande utilise les logiciels **Koyote** et **rsCase**, fournis par **Rola Security Solutions**, une société qui élabore des "solutions logicielles pour la police" depuis 1983.



ET VOTRE MOBILE SE CHANGE EN BALISE

Des milliers de localisations cellulaires sont effectuées chaque année en France, notamment dans le cadre de procédures ...

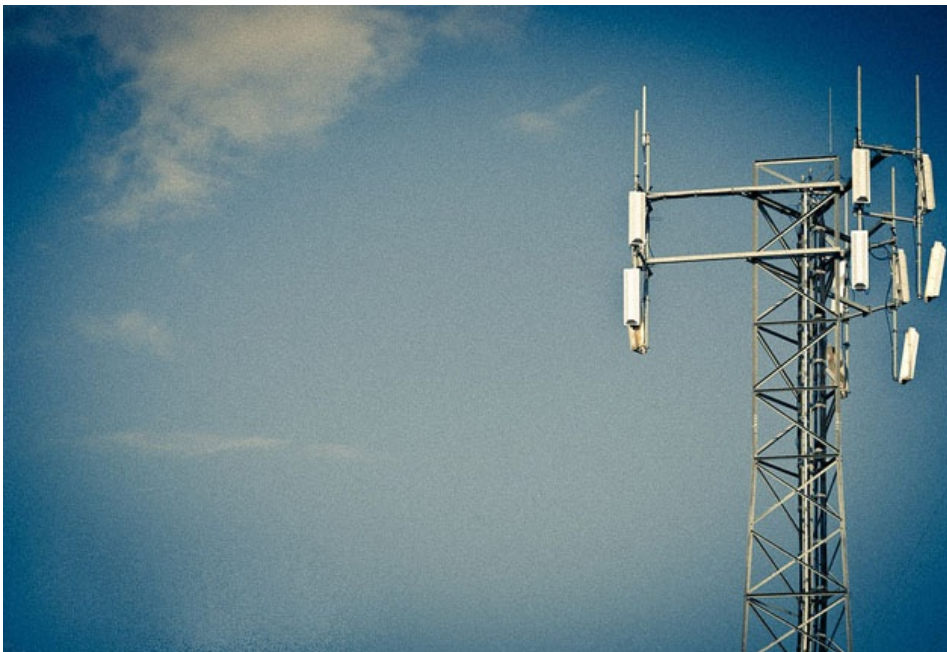
Souriez, vous êtes pistés

Le journaliste spécialisé Mathias Monroy s'inquiète d'une utilisation croissante de **ces technologies de surveillance**. Car les SMS furtifs permettent de connaître très finement la position des personnes espionnées. Cette localisation utilise le réseau GSM, comme nous l'explique Karsten Nohl :

“

On peut localiser un utilisateur en repérant les trois antennes relais les plus proches de son mobile, puis en déduisant, par triangulation, la distance d'après la vitesse que met un signal [comme un SMS furtif, NDLR] à faire un aller-retour. Un téléphone mobile met à jour sa présence sur le réseau régulièrement, mais quand la personne se déplace, l'information n'est pas mise à jour tout de suite. En envoyant un SMS furtif, la localisation du mobile est instantanément mise à jour. C'est très pratique, parce que cela permet de localiser quelqu'un à un instant T, en fonction des ondes.

”



Un SMS furtif sert notamment (mais pas seulement) à affiner la position dans le temps, en forçant la mise à jour d'un mobile. Une technique bien plus efficace qu'une simple **localisation cellulaire** (Cell-ID). Contacté par *OWNI*, François-Bernard Huyghes, chercheur à l'**IRIS**, commente l'utilisation de ces SMS furtifs :

“

C'est la seule méthode immédiate et pratique pour suivre constamment un mobile hors des périodes d'utilisation. On parle alors de géopositionnement et non plus de géolocalisation. Après cela, soit les policiers suivent l'information via les opérateurs, soit des sociétés privées traitent les données et, par exemple renvoient à l'enquêteur une carte où apparaissent les déplacements du téléphone surveillé en temps réel.

”

Les bénéfices des SMS furtifs ne s'arrêtent pas là : en envoyant un grand nombre de ces SMS les services de sécurité peuvent aussi perturber le mobile, ou réactiver ses signaux à distance ou encore décharger sa batterie. Un porte-parole du **ministère de l'Intérieur Allemand** explique à *OWNI* :



La police et les services de renseignement allemands utilisent les SMS furtifs pour réactiver des mobiles inactifs et améliorer la géolocalisation d'un suspect, par exemple quand celui-ci se déplace lors d'une entrevue. Les SMS furtifs sont un outil précieux d'investigation, qui est utilisé uniquement dans le cadre d'une surveillance des télécommunications ordonnée par le juge, dans un cas précis, sans jamais violer le droit fondamental à la protection de la vie privée.



Réactiver à distance

En France, la police et les services de renseignement travaillent notamment avec **Deveryware**, un "opérateur de géolocalisation", qui vend également aux entreprises un service de "géopointage" de leurs salariés, le Geohub, accessible via une base de donnée baptisée **DeveryLoc**.

Pour alimenter son Geohub, Deveryware combine la **localisation cellulaire**, le GPS, ainsi que d'autres techniques de "localisation en temps réel". Quand on demande à la société si les SMS furtifs font partie de ces techniques, réponse évasive :



Nous sommes au regret de ne pouvoir répondre, vu le caractère confidentiel imposé par les réquisitions judiciaires.



Les applications de Deveryware permettent aux enquêteurs de cartographier les déplacements d'un suspect et d'en avoir un historique. Interrogé par **OWNI**, Laurent Yern, responsable investigation pour **SGP Police**, constate :



Tous les services d'investigation ont accès à la plateforme de Deveryware. Grâce à ce système, on peut suivre une personne sans être obligé d'être derrière elle. Pas besoin de filatures, donc moins de fonctionnaires et de matériel à mobiliser.



Alors qu'en Allemagne, le ministère de l'Intérieur répond dans les 48 heures, en France, étrange silence. Unique réponse, provenant du Service d'information et de communication de la police nationale :



Malheureusement, personne à la PJ ou à la sécurité publique ne veut communiquer sur le sujet, ce sont des techniques d'enquête...



Même silence chez les opérateurs, SFR et Bouygues Telecom. Sébastien Crozier, délégué syndical CFE-CGC-Unsa chez France Télécom-Orange, lance :



Les opérateurs collaborent toujours avec la police, c'est une obligation de service public : ils agissent sur réquisition judiciaire, tout comme pour les requêtes de fadettes. Il n'y a pas de méthode absolue, l'envoi de SMS est une partie des méthodes utilisées pour géolocaliser un utilisateur. On utilise surtout cette technique pour "réactiver" le téléphone : le réseau va se mettre en situation active.



En France, d'ici à 2013, l'utilisation de ces procédés de surveillance entreront dans une phase industrielle. Le ministère de la Justice mettra sur place, avec le concours de la société d'armement Thales, une nouvelle **plateforme nationale des interceptions judiciaires** (PNIJ), qui devrait permettre de centraliser l'ensemble des interceptions judiciaires, autrement dit les écoutes, mais aussi les réquisitions telles que les demandes de



Cette interface entre officiers de police judiciaire et opérateurs permettra de rationaliser les frais de justice, de réduire les coûts de traitement de moitié, parce que jusqu'ici, les réquisitions sont gérées commissariat par commissariat... Il y aura encore plus de demandes, mais ça sera moins coûteux pour les opérateurs comme pour la police.



Couverture, Illustrations et photos sous licences **Creatives Commons** via Flickr par Nicolas Nova ; Arlo Bates ; Keoshi ; Luciano Belviso ; Meanest Indian ; Photo de couverture remixée par Ophelia Noor avec l'aimable autorisation de Spo0nman [CC-by-nc-nd]

JEFFBEBACK

le 26 janvier 2012 - 13:09 • SIGNALER UN ABUS - PERMALINK



Il est vraiment temps que les populations ce mette au courant et s'oppose à ces techniques (avec les systèmes de surveillance d'internet) utilisées sans aucun cadre réglementaire.

VOUS AIMEZ



10

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

GUILLAUME

le 26 janvier 2012 - 13:14 • SIGNALER UN ABUS - PERMALINK



*"Un téléphone mobile met à jour sa présence sur le réseau régulièrement, mais quand la personne se déplace, l'information n'est pas mise à jour tout de suite"
Ce n'est pas tout à fait vrai (et laisse penser le contraire de la réalité) : c'est quand un portable se déplace peu (par exemple, quand il reste dans la même ville) qu'il est difficile à localiser. Qd il se déplace sur de grandes distances, il subit automatiquement un changement de zone "LAC" et donc une réinscription auprès des serveurs du réseau.*

VOUS AIMEZ



6

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

BOB DENARD

le 26 janvier 2012 - 19:10 • SIGNALER UN ABUS - PERMALINK



Il existe un système "similaire" pour le suivi des sms avec accusé de réception qui vous permet de savoir si le destinataire la reçu.

Idem avec internet où l'on copie votre adresse IP ou utilise un cookie, idel avec le GPS.

De toute les façons avec facebook pas besoin d'espionner les gens, ils disent tout librement chez une gentille marque qui ne se permettrait pas de garder des infos pour les vendre à des tiers.

VOUS AIMEZ



1

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

N'IMPORTE

le 29 janvier 2012 - 0:40 • SIGNALER UN ABUS - PERMALINK



Vous dites n'importe quoi.

Le principe des SMS furtifs est qu'ils ne sont pas visibles par l'utilisateur, au contraire des messages avec accusé de réception.

Renseignez-vous sur le système GPS également, purement passif côté terminal.

VOUS AIMEZ



VOUS N'AIMEZ PAS



LUI RÉPONDRE

NANAR

le 26 janvier 2012 - 20:09 • SIGNALER UN ABUS - PERMALINK



et en ce qui concerne l'ecoute il y a des possibilitees d'enregistrement audio en dehors des temps d'appel ????

Ce qui est sure c'est qu'on est suivie a la trace !!!

VOUS AIMEZ



VOUS N'AIMEZ PAS



LUI RÉPONDRE

GUILLAUME

le 26 janvier 2012 - 21:21 • SIGNALER UN ABUS - PERMALINK



Seulement si on a injecté une saloperie dans le portable au préalable. Plusieurs vecteurs possibles (bluetooth, mail infecté par exemple), mais en général c'est le fuit d'un travail "ciblé" donc ça ne risque pas d'arriver au quidam.

VOUS AIMEZ



VOUS N'AIMEZ PAS



LUI RÉPONDRE

PIERRE

le 27 janvier 2012 - 13:22 • SIGNALER UN ABUS - PERMALINK



Salut. Il manque la principale information, Quels sont les téléphones concernés ?

Il existe sous windows mobile un logiciel qui permet d'envoyer ces sms silencieux. Il me semble que pour Symbian il existe également. Mais ca ne marche pas à tous les coups . Sous l'OS Android j'en ai pas trouvé encore.

VOUS AIMEZ



VOUS N'AIMEZ PAS



LUI RÉPONDRE

JEROME D

le 27 janvier 2012 - 13:35 • SIGNALER UN ABUS - PERMALINK



Sans oublier que chaque téléphone contient une SIM qui est sous l'entier contrôle des opérateurs. Il est possible depuis toujours de communiquer avec elle par SMS "furtif". Depuis quelques années et l'arrivée du protocole BIP (Bearer Independent Protocol) il est possible d'établir une communique via IP, toujours de façon invisible pour l'utilisateur. La stratégie des fabricants de SIM a toujours été de vendre des SIMs de plus en plus puissantes aux opérateurs et d'inventer de nouveaux standards pour chaque nouvelle fonction.

Ils ont ainsi mis sur le marché des SIM capables de faire tourner des applications de plus en plus puissante, de servir de serveur web (SCWS), de sauvegarder l'ensemble du contenu du téléphone, d'implémenter des fonctions NFC voire GPS indépendantes de celle du téléphone... Toutes ses informations étant stockées directement sur la puce, hors du contrôle de l'abonné mais pas de celui de l'opérateur...

Fort heureusement la plupart des OS récents (iOS, Android et windows phone) n'implémentent pas ou peu des fonctions nécessaires à ces "superSIM" pour fonctionner.

VOUS AIMEZ



VOUS N'AIMEZ PAS



LUI RÉPONDRE

PIERRE

le 27 janvier 2012 - 14:23 • SIGNALER UN ABUS - PERMALINK



Exact ces cartes SIM évoluent de plus en plus. C'est un terrain jeu passionnant.

Patrick gueulle publie régulièrement ces découvertes sur le site acbm.com. Pour ceux qui en ont envie ou le temps y a de quoi s'amuser.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

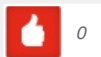
QUENT

le 27 janvier 2012 - 18:40 • SIGNALER UN ABUS - PERMALINK



*Pour info, les sms furtifs son dispo sur l'appli Free-iSMS (symbian OS).
Et ils sont également dispo sur le logiciel libre wammu (qui permet de se connecter a son portable et d'envoyer des sms écrit sur le pc).*

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

LEO

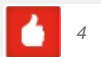
le 27 janvier 2012 - 19:25 • SIGNALER UN ABUS - PERMALINK



C'est très dommage, votre article ne donne aucune précision ou référence "technique" (par exemple, ce qui fait que ces SMS sont différents, ou le nom de la norme qui les définit, etc..) pour rester dans la "magie" (des SMS 'furtifs', comme si cela voulait dire quelque chose en informatique / télécoms...).

A la lecture de votre article, on a l'impression que tout cela est ésotérique, insaisissable, incontrôlable. Dommage, du coup votre publication perd beaucoup de son sérieux.

VOUS AIMEZ



4

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

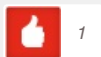
SCOUT123

le 27 janvier 2012 - 22:59 • SIGNALER UN ABUS - PERMALINK



On notera que cette technologie sera indépendante de l'architecture du téléphone, du moment qu'il supporte l'usage des SMS. Très fâcheux, car cela permettrait une surveillance accrue est impossible à contourner...

VOUS AIMEZ



1

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

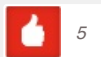
AKIRA

le 28 janvier 2012 - 14:12 • SIGNALER UN ABUS - PERMALINK



reste une solution: se déplacer sans son portable. il fut un temps ou les êtres humains reussissaient à vivre sans leur "tétines" numérique. C'était il y a bien longtemps... 15 ans en arrière, je crois. A nous de voir...

VOUS AIMEZ



5

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

HARDKOR

le 28 janvier 2012 - 15:51 • SIGNALER UN ABUS - PERMALINK



Ou leur mettre un grosse pression pour qu'ils soient enfin respectueux de nos vies privés. Mais ça c'est plus compliqué à faire...

VOUS AIMEZ



1

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE



GILOU

le 28 janvier 2012 - 15:12 • SIGNALER UN ABUS - PERMALINK



*Bonjour.
J'aimerais savoir si comme en informatique, il etait possible de se proteger de cela?
Car apres le scandale (étouffé?) du programme de log aux USA sous Android, peut on
esperer une sorte de bidouille sur les GSM de sorte a ce que le genre d'opération
décrite ici plus haut soit impossible? Linux, firewall, "proxy" etc ?*

Ou, dès lors que l'appareil est connecté au réseau, est il ouvert a tout ce que le réseau permet?
MErci

VOUS AIMEZ  0 VOUS N'AIMEZ PAS  0

LUI RÉPONDRE

HARDKOR

le 28 janvier 2012 - 15:49 • SIGNALER UN ABUS - PERMALINK





Solution simple : retirer la batterie.

Je pense que c'est la seule methode sure. Pour le reste étant donné qu'il n'y a aucun moyen controler totalement ce que fait un portable étant donné que c'est programmé et packagé par de grosses boites c'est très compliqué.

Il n'y a pas de debian sur portable. De plus je ne sais pas si les drivers (qui sont souvent des backdoor redoutables) sont libres.

Si le sujet t'intéresse sur ordinateur je t'invite à regarder ça : <http://hardkor.info/anonymat-censure-digital-forensic-evasion/>

VOUS AIMEZ  4 VOUS N'AIMEZ PAS  0



LUI RÉPONDRE

ETIENNE

le 28 janvier 2012 - 18:44 • SIGNALER UN ABUS - PERMALINK



Si, si, mon tel tourne sur debian, c'est un n900.

VOUS AIMEZ  0 VOUS N'AIMEZ PAS  0

LUI RÉPONDRE

BENOIT



le 30 janvier 2012 - 9:13 • SIGNALER UN ABUS - PERMALINK



Ho, un possesseur de N900 :) !

Je confirme pour mes dires de cet OS, plus précisément le N900 tourne sous Freemantle aka Maemo 5 (voire CSSU si l'on utilise les mises à jour communautaires).

Autre solution pour éviter le tracking : le mode avion.

VOUS AIMEZ  0 VOUS N'AIMEZ PAS  0



LUI RÉPONDRE

LUDOVIC

le 28 janvier 2012 - 15:39 • SIGNALER UN ABUS - PERMALINK



Je ne savais pas que les constructeurs de téléphones mettaient en place ce genre de service.

VOUS AIMEZ  1 VOUS N'AIMEZ PAS  0

LUI RÉPONDRE

GILLES

le 29 janvier 2012 - 5:59 • SIGNALER UN ABUS - PERMALINK



Justement, je me demandais si ce genre de truc pouvait exister ! Lorsque je reçoit un sms ou un appel, mon téléphone crée des interférences avec mes haut-parleurs. Or, depuis peu, j'ai remarqué j'ai ces interférences malgré le fait, que je ne reçoit rien (de visible). Vous pensez que ça peut-être des sms turtifs ? (euh... je ne vois

pas qui pourrais me surveiller ^^)

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

GUILLAUME

le 29 janvier 2012 - 12:15 • SIGNALER UN ABUS - PERMALINK



Comme expliqué dans l'article, la surveillance n'est pas gratuite pour l'Etat, il faut donc que vous ayez une sacrée bonne raison pour être surveillé ! Il faut savoir que la rareté des ressources radio oblige équipementiers et opérateurs à développer des algorithmes complexes d'interaction entre réseau et terminaux pour optimiser le fonctionnement du service. L'ensemble est donc un système asservi où le réseau s'enquiert, de manière non-déterministe, d'états détaillés des terminaux pour optimiser le point de rattachement de chaque terminal, la puissance sur les différents canaux... Des phénomènes spécifiques peuvent amplifier ces effets, par exemple si vous êtes à la limite de réception de 2 cellules, il y a une probabilité que vous 'oscilliez' entre les 2 malgré les mécanismes d'hystérésis mis en place pour contenir ce genre de phénomène. Mais votre commentaire n'est pas dénué d'intérêt, je dirais que "vous chauffez" ;-) commentaire

VOUS AIMEZ



1

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

XAVIER

le 29 janvier 2012 - 20:24 • SIGNALER UN ABUS - PERMALINK



Les terminaux se signalent à chaque fois que l'on change de Local Area Country (LAC: ensemble de cellules). Vous êtes probablement situé entre deux LAC...ce qui fait que votre terminal émet très souvent.

VOUS AIMEZ



1

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

DESUISSE

le 29 janvier 2012 - 9:49 • SIGNALER UN ABUS - PERMALINK



Cette pratique devrait être encadrée par la justice pour vraiment protéger les libertés individuelles et collectives des honnêtes gens contre le crime. Dans ce cadre, cette pratique serait tout à fait normale.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

DIAN

le 24 juin 2012 - 23:59 • SIGNALER UN ABUS - PERMALINK



J'offre 500 € a celui qui me trouve la géolocalisation de la personne que je cherche en effet j'ai était amaqner de 2500 € mais la personne a toujours son telephone allumé

*Micheldian@live.fr
Contactez moi*

VOUS AIMEZ



1

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

8 pings

Vie privée & surveillance | Peartrees le 26 janvier 2012 - 11:25

[...] Vos SMS furtifs Les SMS furtifs sont un outil précieux d'investigation, qui est utilisé uniquement dans le cadre d'une surveillance des télécommunications ordonnée par le juge, dans un cas précis, sans jamais violer le droit fondamental à la protection de la vie privée. [...]

Géolocalisation, Biométrie, contrôles au faciès : 3 coups portés contre les libertés individuelles | Europe-Ecologie-Les Verts (EELV) Joinville-Autrement le 26 janvier 2012 - 17:29

[...] d'abord, Owni a relayé cette information selon laquelle les forces de police françaises et notamment la police [...]

Flash SMS | Korben le 27 janvier 2012 - 13:30

[...] SMSPar Korben0Tiens, tiens, Owni a publié tout un article qui parle des SMS furtifs ou Flash SMS. Je ne connaissais pas le principe mais en gros, c'est une [...]

insolite : L'etat traquerait les téléphones portable à votre insu grace à des sms furtifs | Musulmans de France le 27 janvier 2012 - 16:16

[...] source : <http://owni.fr/> [...]

DES SMS FURTIFS SUR VOS PORTABLES | Think Differently le 27 janvier 2012 - 21:33

[...] source [...]

Les SMS furtifs, l'arme des services de renseignement contre les mobiles | Scout123 le 27 janvier 2012 - 22:57

[...] Encore une sombre histoire, concernant une technologie détournée à des fins de surveillance ou de géolocalisation : les SMS furtifs, présentés par Owni. [...]

SMS Furtifs, dangers. | G33kZ0ne Mosaïque de l'actualité numérique et jeux vidéos le 28 janvier 2012 - 0:26

[...] une info retrouvée sur le site d'owni, des SMS furtifs seraient envoyés par des services de sécurité pour nous localiser par [...]

Revue du web du 10/02/2012 « www.aurelienpiat.com le 10 février 2012 - 14:50

[...] Des SMS furtifs sur vos portables OWNi, News, Augmented, Via owni.fr Tweet Bonjour ! Si vous êtes nouveau ici, vous pouvez souscrire à mon flux RSS si vous le souhaitez et ainsi être tenu au courant des derniers posts publiés. Articles lies: [...]