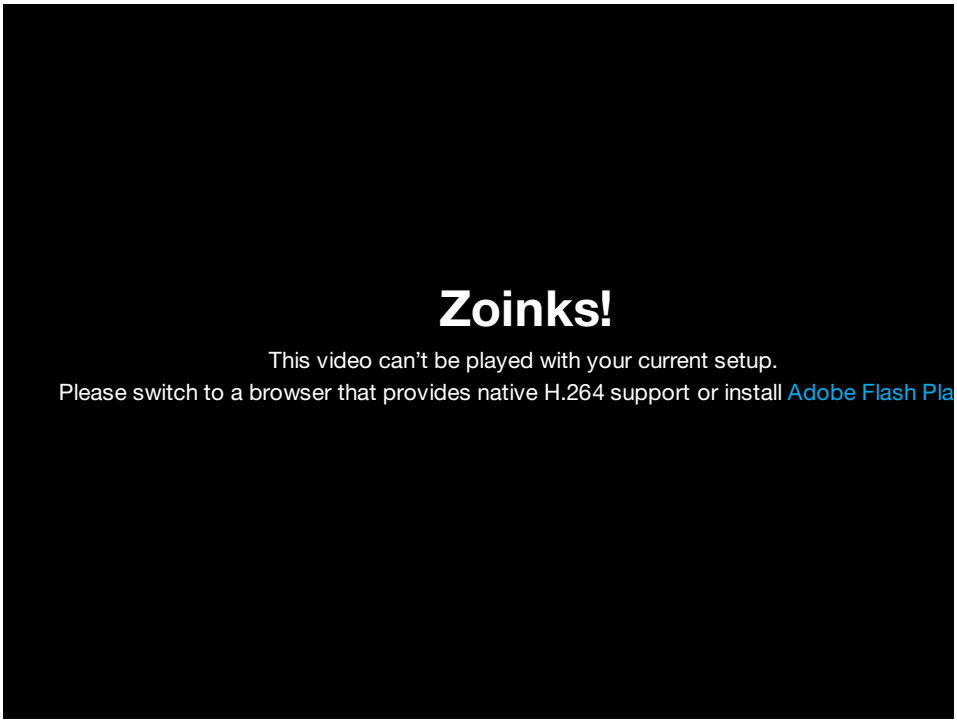
UN JOUR SOUS SURVEILLANCE

LE 3 DÉCEMBRE 2011 ***PIERRE ALONSO***

Les documents révélés par WikiLeaks laissent entrevoir le paysage de la surveillance. Un téléphone portable devient un parfait mouchard, des connexions (sécurisées ou non) des mines d'informations, et les réseaux peuvent être espionnés à l'échelle d'un pays.

Vivre une journée au milieu des nouvelles technologies de surveillance, un marché mondial de cinq milliards de dollars. Les fabricants redoublent d'inventivité. A partir des plaquettes et documents internes ***rendus publics jeudi par WikiLeaks*** *,* OWNI *plonge dans une journée sous surveillance. Une fiction réaliste dressant un panorama (non-exhaustif) des technologies vendues par les marchands d'armes de surveillance.*

7h15, sonnerie de réveil d'un smartphone. Entrer un code PIN. L'allumer et le reposer. Il est désormais un parfait mouchard. Hacking Team, une société italienne, propose d'installer à distance un logiciel compatible avec la plupart des systèmes d'exploitation (iPhone, BlackBerry, Windows Phone). Activé à distance, il permet de prendre le contrôle du téléphone sans que l'utilisateur ne se rende compte de rien (voir la vidéo ci-dessous du *Bureau of Investigative Journalism* en anglais.)



Katrin Verclas, co-fondatrice de MobileActive.org qui réfléchit à des utilisations militantes des smartphones, **explique** :

> ***Une fois installé directement ou à distance sur le mobile d'une personne, ces "spywares" (logiciels malveillants) peuvent (…) activer à distance le micro pour se transformer en mouchard.***

8h30, départ pour le bureau, téléphone portable en poche. Un bon moyen pour suivre à la trace. Sans utiliser d'appareil physique, un smartphone peut là aussi enregistrer un itinéraire ou indiquer une position géographique précise, comme le propose Hacking Team.

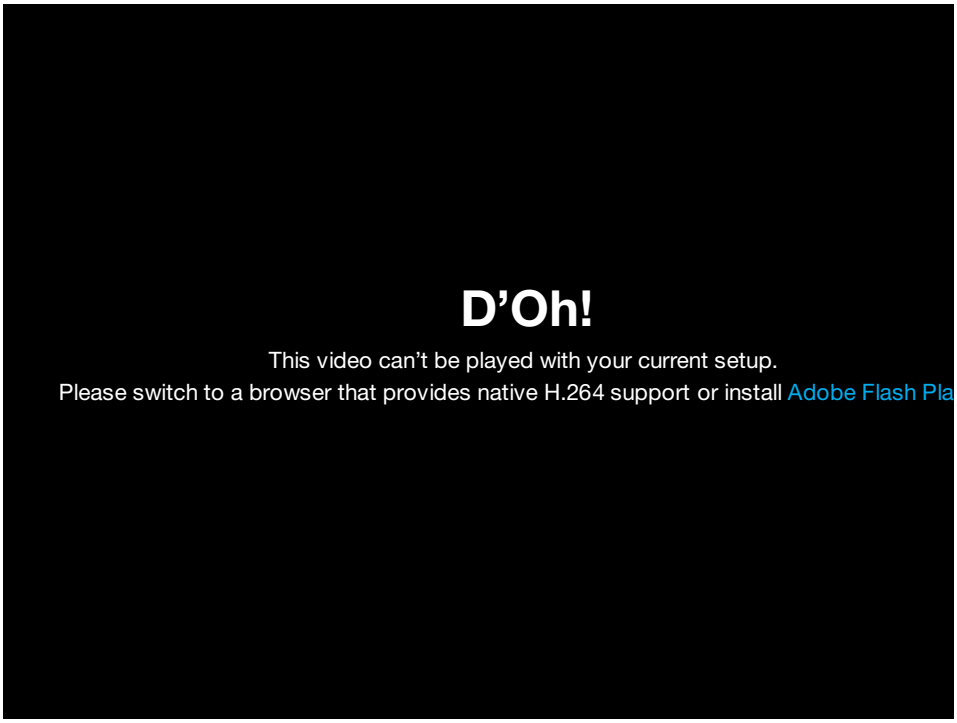
L'ancienne méthode, celle des mouchards, fonctionne toujours. SPEI, une entreprise allemande, a créé **Sleuth-Hound Software**, qui permet de *"contrôler à distance et visualiser la position GPS d'un ou plusieurs appareil de traçage GPS"*. Les trajets peuvent être visualisés sur *"Google Earth, Microsoft MapPoint, Navigator 7…"* , le tout sur *"une interface simple d'utilisation"*.

Les communications entrantes et sortantes, qu'elles durent quelques secondes ou plusieurs minutes, fournissent des mines d'information. D'abord en les interceptant. **L'indien Shoghi Communications** offre des systèmes de *"surveillance totale du trafic incluant SMS et appels du mobile ciblé"*. Ensuite en analysant le spectre vocal. L'analyse de la voix permet d'identifier précisément les interlocuteurs. L'entreprise tchèque **Phonexia parvient** à déterminer le genre, mais aussi l'âge de l'interlocuteur. Le tout, en détectant des mots-clés dans le dialogue. Une performance minimale comparée aux possibilités actuelles, **décrites par Simon Davies**, directeur général de l'ONG *Privacy International* :

> ***Les nouveaux systèmes commercialisés par les entreprises de sécurité ont recours au rythme, à la vitesse, la modulation et l'intonation, en se fondant sur le type de personnalité et l'influence parentale, ainsi que la sémantique, les idiolectes[1], les prononciations et les particularités liés au lieu de naissance, au statut socio-économique et au niveau d'éducation.***

Voir ce que les utilisateurs voient

Au bureau, un ordinateur fixe ou portable, connecté à Internet. Une cible privilégiée par les marchands d'armes de surveillance. La société américaine SS8 **se vante** de développer des solutions pour *"voir ce que [les utilisateurs] voient en temps réel"* .



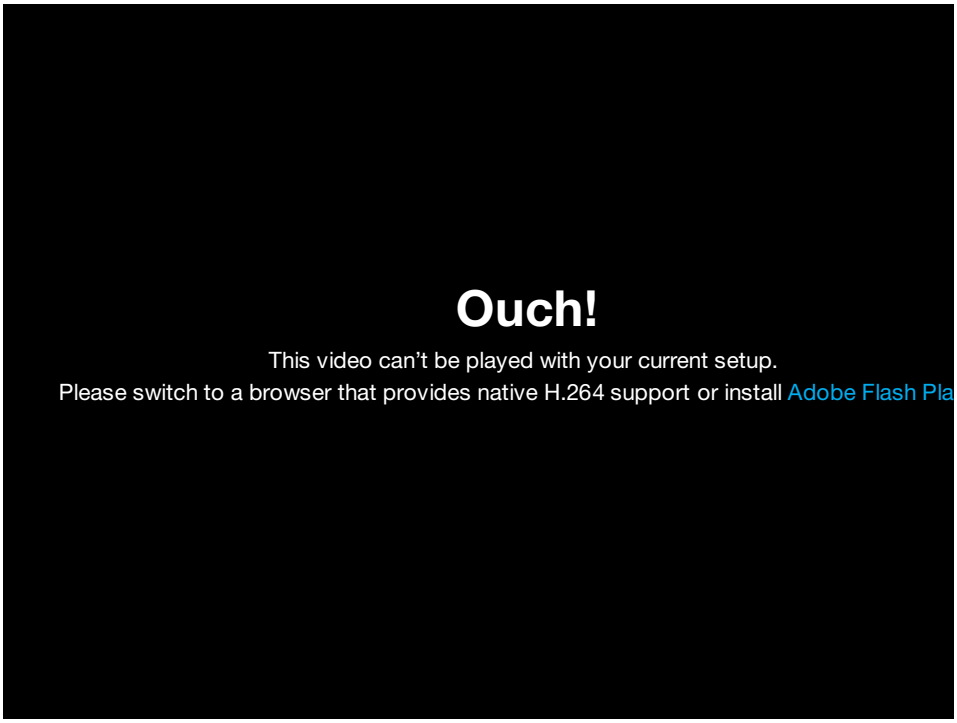
Aller sur les réseaux sociaux. La **technologie *Intellego*** de SS8 est un modèle de *Social network Analysis* (SNA), soit la capacité à connaître *"le nombre de connexions entre les individus ou groupes, leur proximité, l'intensité de leur relation, le degré d'influence d'une personne sur les autres ou un groupe, le mode de propagation d'une idée dans un réseau"* d'après **Solon Barocas**, doctorant à la NYU. *Intellego* met en forme et réorganise les données des réseaux sociaux interceptées :

> ***Intellego automatise le processus qui génère l'analyse d'un réseau social. Chaque individu, site web, adresse mail ou cible est représenté comme un noeud. Chaque communication qui connecte deux nœuds est représentée par un pont.***

DigiTask, une entreprise allemande, a créé ***Wifi catcher*** qui permettent d'intercepter l'ensemble du trafic passant sur un réseau. Adapté à la mobilité, *Wifi Catcher* peut être *"utilisé discrètement sur des hotspots publics en déposant simplement la petite unité de réception près de la cible (…) ou à distance avec de grandes antennes directionnelles"*. Et nombreux sont les fabricants à le proposer pour les réseaux ADSL. Comme l'entreprise israélienne Trace Span et son *DSL Phantom "entièrement non-intrusif permettant aux agences de chargées de la sécurité (*law enforcement agencies*) de surveiller des informations sans être détecté*".

Système de surveillance massive

Bien au-delà d'un réseau d'entreprise ou de particulier, **l'entreprise française Amesys** commercialise *Eagle*, un *"système massif conçu pour répondre aux besoins d'interception et de surveillance à l'échelle d'une nation [et] capable d'agréger tout type d'informations [et] d'analyser, en temps réel, un flux de données à l'échelle nationale, de quelques terabytes à plusieurs dizaines de petabytes".* Les réseaux entiers peuvent être visés par le DPI, *Deep Packet Inspection*, une technologie à usage dual, utilisée tant pour mesurer la qualité d'un réseau que pour le filtrer et le censurer. Des technologies que proposent **le français Qosmos** ou **l'allemand Ipoque**.



Même les connexions sécurisées, les fameux protocoles SSL qui rassurent lors d'un paiement en ligne, peuvent être brisés. Packet Forensics (littéralement "autopsie du paquet") dont le siège est en Arizona, a développé **"man-in-the-middle"**. Sa force est d'intercepter toute communication *"transitant dans une session SSL ou TLS"* .

Avant de quitter le bureau, faire une mise à jour d'un logiciel. C'est l'une des voies que **DigiTask a trouvé** pour *"surmonter le chiffrement, manipuler une cible nomade, surveiller [son] activité"* : les logiciels furtifs développés par *"le leader du marché allemand"* peuvent être installés via des *"logiciels modifiés."*

Débrancher sa connexion. Eteindre son ordinateur. Le *digital forensic* ("autopsie numérique") **les ressuscitent** : fichiers supprimés, historique de navigation web, etc. Cellebrite, une entreprise israélienne propose ***Ufed Logical*** , le même service adapté aux smartphones.

23h30. Laisser son smartphone en veille. Même ainsi, il peut enregistrer **les conversations alentours**.

Dormir, sous bonne surveillance.

Illustration via FlickR [cc-byncnd] **Martin Gommel**
Retrouvez notre dossier sur le sujet :
Un gros requin de l'instruction et **Des chevaux de Troie dans nos démocraties**

Tous les articles OWNI/Wikileaks **sont là**

1. ensemble des usages du langage propres à un individu donné, s'exprimant oralement. [↩]

YO
le 3 décembre 2011 - 21:04 • SIGNALER UN ABUS - PERMALINK

faudra aussi s'intéresser aux superbes possibilités des IDS / firewall qui font en fin de compte du DPI sur des puces SOCs …

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

DJALLILE
le 4 décembre 2011 - 14:12 • SIGNALER UN ABUS - PERMALINK

la technologie au service du despotisme……chute vous est surveillez

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

KOON
le 6 décembre 2011 - 0:08 • SIGNALER UN ABUS - PERMALINK

C'est quoi ce truc "Man-in-the-middle" de Packet Forensics qui date de 2009 ?

Ça voudrait dire qu'une société a annoncé clairement avoir craqué le ssl et le tls et que personne ne s'en serait rendu compte depuis 2009 ?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ERIC
le 6 décembre 2011 - 18:43 • SIGNALER UN ABUS - PERMALINK

je viens de recevoir une information de mon Pole Emploi.
qui propose une appli pour Smartphone.
https://market.android.com/details?id=com.amesys.poleemploi.si2
appli devellopé par AMESYS.
Existe il un lien ?
Pouvons nous faire confiance a cette application proposé par un service publique?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

3 pings

VIE PRIVÉ ! by sergedemontreal - Pearltrees le 3 décembre 2011 - 15:46

[...] DigiTask, une entreprise allemande, a créé Wifi catcher qui permettent d'intercepter l'ensemble du trafic passant sur un réseau. Une journée sous surveillance » OWNI, News, Augmented [...]

CQFT #6 : parce que 6 euros pour le téléthon c'est pas grand chose… « Résolument 2.0 le 3 décembre 2011 - 18:54

[...] Où est votre vieux NOKIA sans internet ? Si vous pensez être surveillé via votre mobile, NE LISEZ PAS LA SUITE. À découvrir ici. [...]

Sota vigilància permament | Elliot.cat le 15 décembre 2011 - 12:16

[...] les informacions publicades pel diari digital Owni.fr, “els documents revelats per WikiLeaks dibuixen el paisatge de la vigilància. Un telèfon [...]