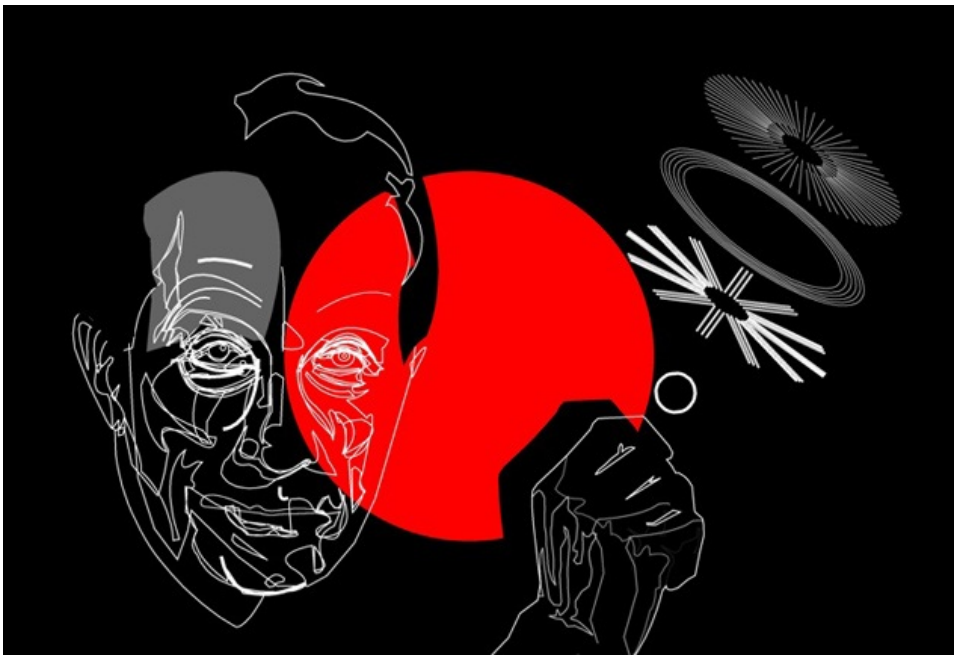
SILENT CIRCLE BROUILLE L'ÉCOUTE

LE 6 NOVEMBRE 2012 ***JEAN MARC MANACH***

Chiffrer tout ce qui passe à travers votre smartphone. C'est le pari de Silent Circle, dont l'un des fondateurs, Philip Zimmermann, n'est autre que le célèbre pionnier en matière de protection de la vie privée - créateur du logiciel de chiffrement PGP. Nous l'avons interviewé.



Dans les années 90, **Philip Zimmermann** s'était attiré les foudres des autorités américaines parce qu'il avait rendu public un logiciel permettant de chiffrer ses données, "***Pretty Good Privacy***", et donc de communiquer en toute confidentialité. Désormais considéré avec Tim Berners-Lee, Vint Cerf et Linus Torvalds comme membre majeur de l'**Internet hall of fames**, Zimmermann s'est embarqué dans une nouvelle aventure : **Silent Circle**.

Son principe : permettre **à quiconque**, grâce au protocole **ZRTP**, le chiffrement de ses mails, de ses appels, de ses SMS et de tout ce qui transite globalement en VOIP[1] sur son smartphone[2] pour 20 dollars par mois. Et qui autorise y compris le "paiement anonyme", grâce à ce qu'ils appellent la "Dark Card" : une carte métallique noire de 6 ou 12 mois, dont chacun peut acquérir le nombre qu'il souhaite, entièrement anonyme – sans nom ni adresse – avec un identifiant unique à 16 caractères. Le tout accompagné de **mentions légales** d'une grande transparence.

> ***I wish more companies posted law enforcement policies like this. Bravo @silent_circle: silentcircle.com/web/law-compli…***
>
> ***— Christopher Soghoian (@csoghoian) Novembre 1, 2012***

"This is designed for the citizens of the world"

"Conçu pour les citoyens du monde" , **clame** le PDG de Silent Circle, Mike Janke – ancien Navy **SEAL** – qui se défend de ne pouvoir être à la fois juge et juré, conscient que ce nouveau produit pourrait très bien être utilisé par des individus malveillants. Mais Janke **assène** également l'adage selon lequel *"tout ce que vous faites ou dites – mail, SMS, téléphone – est surveillé à un niveau ou à un autre"*. Et il refuse donc l'idée d'en priver les

99% de citoyens qui en feront un usage correct pour protéger leur vie privée.

Pour l'heure, la firme prétend avoir déjà reçu une commande en provenance d'une multinationale pour 18 000 de ses employés, et suscité de l'intérêt d'unités d'opérations spéciales et d'agences gouvernementales de plusieurs pays. Et le célèbre *pure player* spécialisé en journalisme d'enquête d'intérêt public *ProPublica* a confirmé avoir entamé des "discussions préliminaires" avec *Silent Circle*, sans doute avec pour objectif de protéger à la fois ses journalistes ainsi que leurs sources. A priori destinée à un public restreint – celui cité, plus quelques activistes, des diplomates, voire **des stars** qui se font voler leur mobile contenant des données sensibles – *Silent Circle* pourrait finalement toucher un public plus large. C'est ce que souhaiterait sans doute Philip Zimmermann.

> **Philip Zimmermann, décrivez *Silent Circle* en quelques mots.**

Silent Circle sécurise les télécommunications de ses utilisateurs. Nous ne vendons pas nos produits aux institutions, mais aux utilisateurs finaux, qui peuvent cela dit travailler pour des institutions, et se faire rembourser l'abonnement.

> **Comment est né le projet ?**

J'ai été contacté à la fin de 2011, par Mike Janke, qui voulait lancer *Silent Circle*, au sujet duquel il pensait depuis des mois, peut-être des années, afin de développer des outils de chiffrement des télécommunications. L'un des premiers marchés qu'il voulait approcher, ce sont les militaires américains déployés à l'étranger, afin de leur permettre de pouvoir parler à leurs familles, parce qu'ils n'ont pas le droit d'utiliser Skype, de dire où ils sont, parce qu'ils doivent utiliser un langage codé pour communiquer… ils ont tellement de restrictions, et comme ils ne peuvent pas non plus utiliser les réseaux de communication sécurisés du Pentagone…

On peut aussi penser aux employés des sociétés militaires privées qui sont, eux aussi, déployés à l'étranger, aux professionnels envoyés dans des pays où ils pourraient être espionnés, comme la Chine par exemple… Et j'ai trouvé que c'était une formidable marché tout trouvé[3] qui pourrait s'élargir au fur et à mesure. En créant des outils censés servir dans des environnements très hostiles, afin d'aider des agences gouvernementales à s'en servir, il deviendrait d'autant plus difficile de nous stopper, en particulier en matière de téléphonie par IP, où nous allons probablement devoir mener des combats juridiques assez controversés dans les prochaines années. Et cette start-up nous facilitera ces combats législatifs ou judiciaires, du simple fait que nous aurons beaucoup de clients au sein des agences gouvernementales…

> **Qu'est-ce que cela fait, pour un pacifiste, de travailler avec d'anciens commandos de marine des forces spéciales ?**

Je passe de très bons moments à travailler avec les *Navy SEAL* dans cette start-up. J'ai toujours été ravi de voir comment PGP a été adopté, dans le monde entier, par les forces de l'ordre et de sécurité, et les services de renseignement, ceux-là même qui, initialement, voulaient pourtant me mettre en prison : on a gagné, la preuve ! *Silent Circle* suscite beaucoup d'intérêt de la part d'organisations militaires, services secrets, l'OTAN, le département d'État américain, qui veulent utiliser notre technologie, et protéger leurs appels téléphoniques avec nos technologies. Et c'est très satisfaisant de voir qu'ils s'en serviront probablement encore plus que PGP parce que mes partenaires sont d'anciens militaires, et qu'ils m'aident à pénétrer ces marchés.

Au début, les agences gouvernementales exprimaient des réticences à utiliser PGP, à cause de l'investigation criminelle dont j'avais fait l'objet, et du côté anti-establishment qui lui avait donc été associé. Quand le FBI est venu toquer à notre bureau, je me suis dit : "Oh non, c'est reparti !", mais non, ils venaient nous voir parce qu'ils voulaient s'en servir ! Et ça, c'est très satisfaisant, je n'y serais jamais parvenu tout seul. En travaillant avec ces anciens commandos de marine, je parviens à toucher des clients que je n'aurais jamais pu toucher tout seul. Et cela va également rendre beaucoup plus difficile aux gouvernements de tenter de nous empêcher de protéger les communications de nos clients, puisqu'ils s'en servent ! Il y aurait trop de dommages collatéraux.

> ***Le prochain champ de bataille de la cryptographie est la téléphonie.***

Historiquement, les interceptions légales des télécommunications ont été utilisées par les forces de l'ordre pour résoudre des crimes, et elles en sont devenues dépendantes. Mais si vous regardez le nombre de crimes résolus au regard du nombre d'écoutes téléphoniques, ça ne représente qu'un pourcentage infime. La majeure partie des crimes sont résolus par d'autres modes d'enquête. Les crimes laissent des traces dans le monde physique.

Rendre les écoutes téléphoniques plus difficiles n'aura pas beaucoup d'impact dans la lutte contre la criminalité. Les choses changent, avec la migration de la téléphonie du réseau analogique vers l'Internet, parce qu'il devient possible, pour le crime organisé, d'espionner tout un chacun. Mais les dommages collatéraux qu'entraîneront l'impossibilité de mettre des individus sur écoute seront bien moins dommageables que la possibilité offerte au crime organisé de mettre tout le monde sur écoute.

Google avait installé une porte dérobée[4], et les Chinois s'en sont servis pour espionner des activistes ! Si vous installez une porte dérobée dans un logiciel, elle sera utilisée par les "*bad guys*". Et puis je suis aussi contre les portes dérobées parce qu'elles vont à l'encontre de nos libertés ! Et tous ceux qui travaillent dans cette entreprise le font parce qu'ils partagent eux aussi ce à quoi je crois. Mike Janke, mon partenaire, a les mêmes opinions que moi en matière de vie privée et de libertés. Il a vu le pouvoir des services de renseignement, et il en a peur : il n'a pas envie de voir nos libertés mises à mal parce qu'elles seraient capables d'espionner leurs concitoyens. Et il est d'accord avec moi.

---

1. Voix sur IP [↩]
2. Pour l'instant, seules les applications iPhone et iPad existent, celles pour Android et Windows étant prévues pour arriver assez rapidement. [↩]
3. "*ready made*", en VO, ndlr [↩]
4. pour permettre aux autorités de placer des utilisateurs de Gmail sur écoute, ndlr [↩]

SWÂMI PETARAMESH
le 7 novembre 2012 - 10:47 • SIGNALER UN ABUS - PERMALINK

Le contrepet s'imposait ;-)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GILLES
le 8 novembre 2012 - 13:55 • SIGNALER UN ABUS - PERMALINK

20 dollars / mois c'est complètement prohibitif pour le grand public dommage.

Ça évoluera peut-être vers le grand public avec le temps…

VOUS AIMEZ 2 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE