Auto-protection – Anti-surveillance : extensions du domaine de la lutte

dimanche 21 juin 2015, par ALONSO Pierre, GUITON Amaelle (Date de rédaction antérieure : 8 juin 2015).

DÉCRYPTAGE. L'ère de la surveillance de masse a sonné et le Sénat devrait l'entériner ce mardi dans le cadre de la loi sur le renseignement. Les conseils de « Libération » pour préserver votre vie privée sur les réseaux.

Avec la loi sur le renseignement, la France s'apprête à graver dans le marbre la surveillance massive de nos communications. Voté aujourd'hui au Sénat, le texte prévoit des dispositifs de détection d'une potentielle « menace terroriste », des « boîtes noires » installées chez les opérateurs et les hébergeurs. Une surveillance algorithmique qui confie à des logiciels le soin de trouver des aiguilles dans des bottes de foin - et ce, alors que de nombreux chercheurs alertent sur le caractère intrusif d'une telle méthode et sur les risques d'erreurs, les « faux positifs ».

Les révélations d'Edward Snowden l'ont amplement démontré : avec la possibilité d'intercepter, de stocker et de traiter de très grandes quantités de données, la surveillance a changé de dimension, et même de nature. *« Ce n'est plus « suivez cette voiture », c'est « suivez chaque voiture » »*, dit ainsi l'expert en sécurité informatique américain Bruce Schneier. Pourtant, comme l'explique Snowden lui-même (lire *Libération* de vendredi), de nombreuses entreprises du numérique ont revu leur copie et renforcé la sécurité de leurs services. Et des équipes de développeurs travaillent sur des outils qui *« peuvent permettre un accès à une protection de base du droit à la vie privée »*. A l'inverse des « boîtes noires », ceux-ci sont transparents : leur code source, librement accessible, peut être examiné par des experts. Contrairement aux idées reçues, plus besoin d'être un geek averti pour s'en servir. Tour d'horizon de quelques moyens techniques pour retrouver un peu de confidentialité à l'ère de la surveillance de masse (plus d'infos dans le guide de l'ONG Tactical Tech).

SURFER HORS DES FILETS

C'est en quelque sorte le « péché originel » du Web : par défaut, on y navigue tout nu, tout ce qu'on y fait est visible - se connecter à un site, mais aussi lui transmettre un mot de passe… A partir de 1994, le protocole de connexion sécurisée HTTPS est venu remédier à cet état de fait. Il crypte (ou « chiffre », en bon français) le contenu de la communication avec un site web. Un petit cadenas apparaît alors dans la barre de navigation. Les banques et les sites de e-commerce ont été les premiers à l'utiliser. Plus récemment, la plupart des grands services internet (Google, Facebook, Twitter…) l'ont adopté. L'Electronic Frontier Foundation, l'association américaine de défense des libertés sur Internet, a lancé il y a quatre ans HTTPS Everywhere, une extension qui fonctionne avec la plupart des navigateurs, s'installe en un clic et « force » la connexion sécurisée partout où elle est possible.

En revanche, un curieux saura qui communique avec qui. C'est à cela que veut répondre l'équipe qui travaille sur le réseau d'anonymisation Tor, et sur le Tor Browser, un navigateur « dédié » très simple à installer (la connexion, qui passe par plusieurs relais, est cependant plus lente). *« Tor cache*

un utilisateur parmi les autres », explique Nick Mathewson, l'un de ses principaux architectes. Une image tenace voudrait que seuls des criminels s'en servent ; dans les faits, partout dans le monde, des activistes, des ONG, des journalistes l'utilisent - sans compter les forces de l'ordre. Le réseau compte aujourd'hui deux millions d'utilisateurs quotidiens. Signe qu'il se démocratise, Facebook a travaillé à faciliter l'accès à ses services via Tor.

SÉCURISER SES MAILS

Avec le développement du webmail (à savoir la gestion des e-mails dans un navigateur web), nos échanges ont longtemps plus tenu de la carte postale que de la lettre cachetée. Il a fallu attendre 2010 pour que Gmail, le premier, active par défaut la connexion sécurisée à ses boîtes de messagerie. D'autres ont attendu l'affaire Snowden…

S'assurer qu'on accède à son service de messagerie en HTTPS et non en HTTP est un minimum pour protéger un tant soit peu ses échanges épistolaires en ligne. Encore faut-il avoir confiance en son fournisseur de messagerie.

Le cryptage (ou chiffrement) du contenu des messages entre deux correspondants reste une autre paire de manches. Le logiciel PGP, pour « *Pretty Good Privacy* » (« assez bonne confidentialité »), a beau avoir près de 25 ans, son usage n'est toujours pas à la portée du premier venu. Mailvelope, une extension pour Chrome et Firefox, permet au moins de l'utiliser plus facilement dans un navigateur. Plusieurs équipes de développeurs travaillent à le rendre véritablement accessible à tous. Signe de ce retour de hype, Google comme Facebook s'y intéressent. Le premier a promis pour cette année la sortie officielle d'une extension pour Chrome. Le second propose désormais à ses utilisateurs familiers de PGP l'envoi de notifications cryptées.

TCHATER COUVERT

Le regard indiscret ne verra qu'une suite de caractères incohérents, du type « 0I1Egb3uPK4 ». Seuls les destinataires connaîtront leur traduction en langage courant. C'est l'avantage des messages cryptés, qui ne sont plus réservés aux militaires (l'usage de la cryptographie est libre depuis 2004 en France), ni aux experts en sécurité. Ainsi, Cryptocat, une extension pour navigateurs web (Firefox, Chrome…), permet au néophyte de renforcer la confidentialité de ses échanges instantanés. Son jeune fondateur, Nadim Kobeissi, l'a pensé pour le plus grand nombre : *« Il y avait un « class gap », mais au lieu des riches et des pauvres, un gouffre entre ceux qui peuvent utiliser la cryptographie et ceux qui ne peuvent pas. »*

Pour combler le fossé et permettre à chacun de protéger sa vie privée, Nadim a lancé Cryptocat en 2011. Plus designer qu'expert en cryptographie, il mise d'emblée sur une interface très simple et un logo sympathique, un petit chat pixellisé. Les failles initiales, qui lui avaient valu de vives critiques, ont depuis été corrigées. Pour toucher un public toujours plus large, Cryptocat peut être utilisé avec le tchat de Facebook, pour protéger ses conversations , y compris du géant du Net.

« SKYPER » SANS SKYPE

Depuis que Microsoft et Google ont été mis en cause dans les révélations sur le programme Prism de la NSA, Skype et Hangouts sont regardés de travers par les défenseurs de la vie privée, et écopent de scores peu glorieux dans le comparatif des outils de communication en ligne de l'Electronic Frontier Foundation. Des concurrents à ces solutions de conversation audio et vidéo ont commencé à voir le jour. L'un des plus prometteurs vient de la fondation Mozilla, l'organisation à but non lucratif qui développe le navigateur Firefox. Firefox Hello (c'est son nom) ne nécessite même pas de créer un compte : il suffit d'ouvrir une « conversation » et d'y inviter un ami (y compris s'il utilise de

son côté les navigateurs Chrome ou Opera). Pas encore disponible, la conversation à plusieurs fait partie de la feuille de route.

POUR NE PAS ÊTRE GÉOLOCALISÉ…

Idée reçue : pour éviter la géolocalisation, il suffirait de la couper sur son smartphone. Faux. Cela permet, au mieux, d'éviter le pistage commercial d'Apple, de Google et de toutes les applis qui ont accès à ces données. Mais pour suivre un téléphone, et son propriétaire, il existe un moyen beaucoup plus simple et difficile à contourner : le bornage. Les téléphones communiquent à intervalle régulier avec les antennes-relais à proximité. Ces données de localisation sont conservées pendant un an par les opérateurs de téléphonie français. Il est donc possible, *a posteriori*, de savoir où se trouvait un téléphone (« smart » ou non). De manière générale, les métadonnées (qui communique avec qui, quand, où) constituent l'angle mort de la protection de la vie privée : par exemple, si le contenu d'un mail crypté est illisible par un tiers, l'expéditeur, le destinataire et l'objet du mail demeurent accessibles. Les méthodes les plus rustiques restent parfois les meilleures. Pour éviter d'être géolocalisé à cause de son téléphone, rien de mieux que de le laisser dans un tiroir.

CRYPTER SES SMS

Pas facile d'échanger de façon sécurisée sur un téléphone portable. Un certain Nicolas Sarkozy l'a appris à ses dépens. S'il s'était renseigné, il aurait pu découvrir l'offre pléthorique d'applications permettant de sécuriser ses communications sur les smartphones. Toutes ne sont pas recommandables, notamment celles qui n'ouvrent pas leur code source aux regards extérieurs. Depuis 2011, Open Whisper System fait le pari inverse. L'entreprise propose les applications TextSecure et RedPhone, pour envoyer des SMS et des appels cryptés sous Android, ainsi que Signal, qui regroupe les deux fonctions sur iPhone. Elles sont évidemment compatibles entre elles.

Des applications pensées pour être faciles à utiliser. L'un des développeurs, Frederic Jacobs, pas encore 25 ans, prône *« la facilité d'usage de la cryptographie »* pour qu'elle se répande au-delà des cercles d'initiés. Le pari de la simplicité est réussi. Comme pour n'importe quel outil de tchat, il suffit de sélectionner le nom d'un correspondant qui l'utilise pour entamer une conversation cryptée, écrite ou orale. Consécration ultime, Edward Snowden lui-même en a recommandé l'usage lors de son intervention, l'an dernier, au festival South by Southwest.

Pierre ALONSO et Amaelle GUITON

P.-S.

*

http://www.liberation.fr/economie/2015/06/08/anti-surveillance-extensions-du-domaine-de-la-lutte_1325549