

La cryptographie peut aussi se mettre au service des activistes et des journalistes

mercredi 20 février 2019, par [CASSAUWERS Tom](#) (Date de rédaction antérieure : 11 février 2019).

Un groupe de journalistes et d'activistes entrent lentement dans une salle et s'assoient. Certains discutent entre eux, d'autres s'occupent sur leurs téléphones. Ils pensent être là pour participer à un atelier, mais à leur insu, ils sont en train d'être piratés. Cinq minutes à peine après leur arrivée, un expert en sécurité a réussi à s'introduire dans la plupart de leurs téléphones et, ce faisant, pirater des informations sensibles sur des contacts, des co-activistes, des manifestations prévues et sur leurs reportages.

L'histoire est réelle, mais personne n'a subi de préjudice. Le cours était organisé par l'ONG néerlandaise Free Press Unlimited et ce piratage fait partie d'un atelier dont le but est de sensibiliser les journalistes et les activistes sur l'importance de la sécurité en ligne. Il s'agissait d'une espèce de thérapie de choc, en quelque sorte.

Mais dans la vie réelle, ce genre d'incidents n'est pas exceptionnel. À travers le monde, l'autoritarisme se répand et, par conséquent, la répression des activistes et des journalistes. Celle-ci ne se manifeste cependant pas uniquement en face à face, mais aussi en ligne. Les ordinateurs et téléphones des activistes sont des cibles privilégiées partout dans le monde, en particulier dans les pays du Sud. Malgré tout, une nouvelle génération d'activistes de la cryptographie met ses compétences spécialisées au service d'autres activistes.

« La cryptographie est d'une grande importance pour les activistes », déclare Jaap-Henk Hoepman, professeur adjoint à l'Université Radboud de Nimègue aux Pays-Bas, où il se consacre notamment à la cryptographie, à la protection des données et à la sécurité sur Internet.

« Lorsque des activistes agissent à contre-courant des normes sociétales, en particulier dans les pays moins démocratiques, ils doivent pouvoir échanger des informations et des contacts en toute sécurité afin d'éviter des représailles. La cryptographie peut y contribuer. »

Surtout du fait que le nombre d'activistes qui vivent dans des pays à risque est en hausse. Freedom House, une organisation basée à Washington DC qui a pour mission de protéger la liberté d'expression à travers le monde, a calculé que 71 pays ont subi un déclin des libertés civiles et politiques en 2017, alors que seulement 35 ont enregistré des gains dans ces domaines.

Sofía Celi est l'une des activistes qui a assisté de première main à cette montée de l'autoritarisme. Initialement installée au Brésil, cette activiste de la cryptographie est retournée à Quito, en Équateur, après l'élection du président d'extrême droite Jair Bolsonaro en 2018, ce dernier ayant à de multiples reprises exprimé son admiration pour la dictature militaire qui était auparavant au pouvoir dans son pays. « Nous sommes proches d'activistes au Brésil, mais après les troubles des derniers mois, nous avons décidé de retourner à Quito », déclare Sofía Celi.

Autonomie numérique

À Quito, Sofía Celi collabore avec le Centro de Autonomía Digital (CAD), un groupe d'activistes qui travaillent sur la cryptographie et la sécurité numérique. Leurs groupes cibles sont les autres ONG et activistes des pays du Sud.

Un des principaux défis qu'ils doivent relever est la facilité d'utilisation. « Certains projets se sont efforcés de rendre leur logiciel plus facile d'emploi, comme le projet Tor », explique Sofía Celi, en référence à un navigateur et à un réseau à code ouvert qui permettent aux utilisateurs de naviguer sur Internet dans l'anonymat et d'accéder à des sites Web qui ne sont pas listés sur le Web ordinaire. « Les experts en sécurité pensent souvent que ces outils sont faciles à configurer, mais la plupart du temps, ils sont inaccessibles aux profanes. Ces outils sont souvent basés sur des concepts et des démonstrations mathématiques de toute beauté, mais en général les gens ne les utilisent pas parce qu'ils sont très difficiles à maîtriser. »

Et ceci se révèle être particulièrement important dans les pays du Sud. « Les activistes du Sud sont souvent beaucoup plus vulnérables et leurs gouvernements beaucoup plus répressifs », déclare M^{me} Celi.

« Mais le milieu de la sécurité ne conçoit pas nécessairement des solutions pour eux, car ils supposent souvent que ces activistes du Sud ont accès à des logiciels high-tech ou même à des smartphones. Ce n'est pas toujours le cas. Dans le Sud, par exemple, certains activistes doivent partager un seul ordinateur entre 10 personnes. »

C'est pour cette raison que le CAD conçoit une gamme de systèmes qui sont adaptés à toutes sortes d'activistes, et ce, où qu'ils se trouvent. Le CAD conçoit, par exemple, un système antihameçonnage qui détecte si un courriel reçu est réel ou non. L'hameçonnage (phishing en anglais) est une technique permettant à des acteurs malveillants de se faire passer pour quelqu'un d'autre et d'essayer de subtiliser des informations sensibles (comme des mots de passe).

Et bien que la recherche plus complexe en mathématiques de la cryptographie soit attrayante pour M^{me} Celi, elle estime que la lutte contre ces types d'attaques peu sophistiquées pourrait avoir un impact beaucoup plus important. « Évidemment, il est plus captivant d'étudier des problèmes académiques en profondeur », déclare-t-elle. « Mais l'hameçonnage est l'un des risques de sécurité les plus courants pour les activistes et il est essentiel de se doter d'une défense contre ce phénomène ».

Cryptographie illégale

Mais comment les cryptographes réagissent-ils aux utilisations non souhaitées de leurs outils ? Par exemple, les criminels se servent de logiciels comme Tor, tout comme les activistes. Une étude réalisée en 2016 par le King's College de Londres affirme que 57 % des sites du réseau Tor contiennent des contenus illicites.

« Nous devons être conscients des conséquences négatives de ces technologies », déclare M. Hoepman. « Toutefois, il n'appartient pas aux cryptographes de décider qui peut ou ne peut pas utiliser la cryptographie. Ce que nous pouvons faire cependant, c'est communiquer sur ses avantages et ses inconvénients. »

M^{me} Celi estime que la facilité d'utilisation occupe à nouveau une place centrale dans la résolution de ce problème éthique. « Nous avons une responsabilité morale », déclare-t-elle. « Les criminels trouveront toujours des outils pour canaliser leurs agissements. C'est pour cette raison que nous devons faire en sorte que ces types de technologies soient aussi accessibles que possible, afin que les personnes ordinaires et les activistes puissent les utiliser. »

De par le monde, les journalistes sont un autre groupe clé qui tire profit d'une cryptographie forte et Free Press Unlimited soutient les journalistes lorsqu'ils pénètrent dans ce domaine.

L'ONG se spécialise notamment dans les droits des lanceurs d'alerte. « Aujourd'hui, les lanceurs d'alerte sont souvent démasqués après avoir divulgué des informations », explique Leon Willems, directeur de Free Press Unlimited. « La plupart du temps, ils finissent par se retrouver dans une situation pire que celle dans laquelle ils se trouvaient avant de divulguer [les informations]. Parfois, ils doivent s'enfuir ou subissent des représailles ou encore perdent leur emploi. Ces personnes ont rendu un service à la collectivité, mais la plupart des cas, elles sont punies pour leur acte. »

C'est donc pour cette raison que l'ONG a développé un système, Publeaks, fondé sur un logiciel similaire appelé GlobaLeaks, visant à sécuriser et à protéger le lancement d'alerte par la cryptographie. « Nous avons d'abord testé le système aux Pays-Bas, » explique M. Willems. « Parce que si une erreur devait se produire dans ce pays, nos protections juridiques relativement solides ne feraient pas payer le prix ultime aux personnes. Et sur la base de cette expérience, nous soutenons désormais des opérations au Mexique, au Nigeria et en Indonésie. »

En Indonésie, un dérivé de GlobaLeaks, appelé IndonesiaLeaks, a déjà contribué à révéler un scandale majeur de corruption avec le soutien de Free Press Unlimited. Pourtant, Free Press Unlimited tient à souligner que ce sont les acteurs des pays du Sud qui ont adopté cette technologie. « Ce sont eux qui ont décidé d'utiliser le logiciel, qui s'appelle GlobaLeaks, et ils sont les maîtres du projet », explique M. Willems. « Mais nous avons fourni un soutien technique dans la mise en œuvre du système. »

Peu importe que les activistes et les journalistes soient basés en Indonésie, au Brésil ou aux Pays-Bas, la cryptographie devient un outil de plus en plus important. Et en dissimulant leurs propres actions, les défenseurs des droits seront peut-être en mesure d'exposer les personnes dont les agissements doivent être révélés au grand jour.

Tom Cassauwers

[Abonnez-vous](#) à la Lettre de nouveautés du site ESSF et recevez chaque lundi par courriel la liste des articles parus, en français ou en anglais, dans la semaine écoulée.

P.-S.

Equal Times

<https://www.equaltimes.org/la-cryptographie-peut-aussi-se#.XGziiVRKjIU>