Ecole des hautes études en sciences de l'information et de la communication
Université de Paris-Sorbonne (Paris IV)

MASTER 2 Journalisme
Spécialité et option : **Journalisme et innovation en apprentissage**

"La sécurité numérique chez les journalistes : une indispensable pratique"

Préparé sous la direction de Madame la Professeure Karine Berthelot-Guiet
et accompagné par Madame Valérie Jeanne Perrier

Nom : LAURENT
Prénom : Pierre
Promotion : 2016-2017
Soutenu le : 24/11/2017

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

“From now, know that every border you cross, every purchase you make, every call you dial, every cell phone tower you pass, friend you keep, article you write, site you visit, subject line you type, and packet you route, is in the hands of a system whose reach is unlimited but whose safeguards are not. Your victimization by the NSA system means that you are well aware of the threat that unrestricted, secret abilities pose for democracies. This is a story that few but you can tell.”

Un des premiers mails envoyé par Edward Snowden à Laura Poitras

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Remerciements

En premier lieu, je remercie Madame Valérie Jeanne Perrier, en tant que directrice de ce mémoire et je tiens aussi à remercier Monsieur Tristan Mendès France pour ses conseils et son suivi pédagogique.

Je souhaite également remercier Jean-Marc Manach et à Grégoire Pouget qui m'ont accordé du temps pour répondre à mes questions, ainsi que celles qui m'ont aidé dans la relecture de ce mémoire.

Compte Twitter de veille

https://twitter.com/InfoSec_Media

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Avant-propos à la version en ligne

La sécurité numérique est un (très) long processus. J'ai commencé à m'y intéresser seulement depuis début 2017, d'où les probables erreurs, approximations et autres raccourcis. J'ai rédigé ce mémoire alors que j'étais en Master 2 de journalisme, cursus que j'effectuais en alternance dans une entreprise. Aussi, le temps m'a sans doute manqué et ce travail n'est pas quelque chose d'extrêmement fouillé ; les réflexions et solutions présentées ci-dessous restent assez basiques pour quelqu'un versé dans ces problématiques depuis un moment.

L'objectif, sans doute présomptueux, était de rendre accessible cette base au plus grand nombre. De nombreuses ressources pour prolonger la réflexion sont présentes à la fin de ce texte et dans le texte, sous la forme de liens.

Merci !

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Plan du mémoire

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Introduction

Plus que jamais dans l'histoire du monde, nous sommes tous soumis, à chaque instant, à une probable surveillance de la part des états, des grandes entreprises et même de nos amis. Volontairement ou non, nous mettons à la disposition de ces différents acteurs nos données les plus sensibles, nos secrets les mieux gardés. Ce terrifiant état de fait n'a qu'une origine et tient en un seul mot : internet. Ce réseau mondial, qui par le passé était le prolongement de l'utopie hippie des années 70, est devenu un potentiel réseau de surveillance et de contrôle. Comme l'a révélé Edward Snowden, les moyens des états sont encore plus incroyables que ce que les plus paranoïaques d'entre nous pouvaient croire. Et malgré cela, les grandes entreprises américaines, comme Facebook et Google, connaissent sans doute encore plus de choses sur nous-mêmes que nos propres gouvernements. Nous partageons tous les détails de nos vies sur les réseaux sociaux, et même les amis perdus de vue depuis des années pensent encore nous connaître.

Sur internet, l'anonymat et la discrétion ne sont plus les règles. Et internet est aujourd'hui partout : dans nos ordinateurs et nos téléphones, bien sûr, mais aussi dans les objets de la vie quotidienne qui commencent à envahir les certains domiciles : assistants personnels, montres connectées, frigo connectés…

Aujourd'hui, le travail de tout journaliste passe par internet : nous travaillons sur des ordinateurs connectés, nous faisons des recherches en ligne, nous appelons nos sources via nos smartphones, nos contacts sont synchronisés dans le "cloud", tout comme nos interfaces de travail avec nos collègues… Malgré les menaces avérées de piratage, de fuite et de surveillance, les journalistes ne semblent pas plus inquiets que leurs concitoyens concernant leurs données. Autrefois respectés, voire sacralisés à travers les lois édictant la "liberté de la presse" (ou du moins c'est l'image rétrospective que nous avons), les journalistes sont devenus des cibles comme les autres. Voire même peut-être des cibles de choix dans certaines situations.

Pourtant, contrairement à bon nombre d'autres professions, les journalistes ont un devoir primordial : celui de protéger les personnes qui les renseignent. Sans source, le journalisme n'existe plus. En France, comme dans d'autres pays, le secret des sources fait désormais partie de la loi. Puisqu'il est difficile de savoir si cela sera véritablement appliqué, il est absolument nécessaire, pour les journalistes, de savoir comment se protéger numériquement afin de pouvoir les protéger. Cette sécurité n'est pas quelque chose que l'on peut acheter ou trouver facilement : c'est un processus long qui peut être complexe, et qui

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

ne sera jamais sûr à 100%. Mais pour les journalistes, il est extrêmement important de s'y lancer.

Face à quelles menaces les journalistes font-ils aujourd'hui face ? Pourquoi la sécurité numérique est-elle indispensable dans cette profession ? Comment se lancer dans ce processus et par quels outils commencer ? C'est pour répondre à ces questions que nous articulerons cette réflexion en deux parties, en nous intéressant d'abord au contexte de la sécurité numérique, puis dans une seconde partie en s'intéressant plus précisément aux journalistes, à leurs stratégies et aux outils qu'ils peuvent commencer à mettre en place.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

I - Une société surveillée où les journalistes sont aussi des cibles

1 - CONTEXTE

A - Une société numérique sous surveillance ?

Aujourd'hui, pour beaucoup, internet occupe une grande partie de nos vies. Cela nous permet de nous divertir, de travailler, de sociabiliser, d'exprimer le fond de notre conscience, d'organiser des manifestations… Tous les pans de la vie, ou presque, se retrouvent sur le grand réseau mondial. En 2016, 156 millions de mails et 29 millions de messages WhatsApp étaient envoyés, 3,6 millions de recherches étaient effectuées sur Google et 4 millions de vidéos étaient regardés sur YouTube… chaque minute. Aujourd'hui, il y aurait 3,7 milliards d'utilisateurs d'internet. Soit plus de la moitié de la population du globe.

Malheureusement internet, cette utopie des années 70, comporte désormais un énorme revers : nos moindres mouvements sur nos ordinateurs et nos smartphones, nos moindres activités sur internet peuvent être surveillés, analysés, enregistrés.

Les révélations d'Edward Snowden

Nous sommes tous potentiellement sur écoute : en juin 2013, ce que l'on surnommera plus tard "l'affaire Snowden" éclate au grand jour. Sous la plume d'un journaliste nommé Glenn Greenwald, le journal britannique The Guardian révèle des documents provenant de la National Security Agency (NSA)[1] étatsunienne. Ces documents ont été transmis par un ancien analyste de la NSA, Edward Snowden. Selon ces documents, qui n'ont toujours pas fini de parler aujourd'hui, la NSA serait en mesure de collecter la quasi-totalité des communications mondiales, que ce soit sur internet ou bien sur les réseaux téléphoniques.

En juin 2013, les premiers documents révèlent que l'opérateur téléphonique Verizon livrerait chaque jour à la NSA la totalité des données téléphoniques en sa possession concernant les communications nationales et internationales transitant par les États-Unis.

[1] La *National Security Agency* (NSA) est un organisme gouvernemental en charge du renseignement électronique, liée au Département de la Défense (DoD). C'est la plus secrète des agences connues.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Les communications de tous les citoyens étatsuniens abonnés à cet opérateur, ainsi que tous les citoyens appelant des correspondants abonnés à Verizon, sont enregistrées.

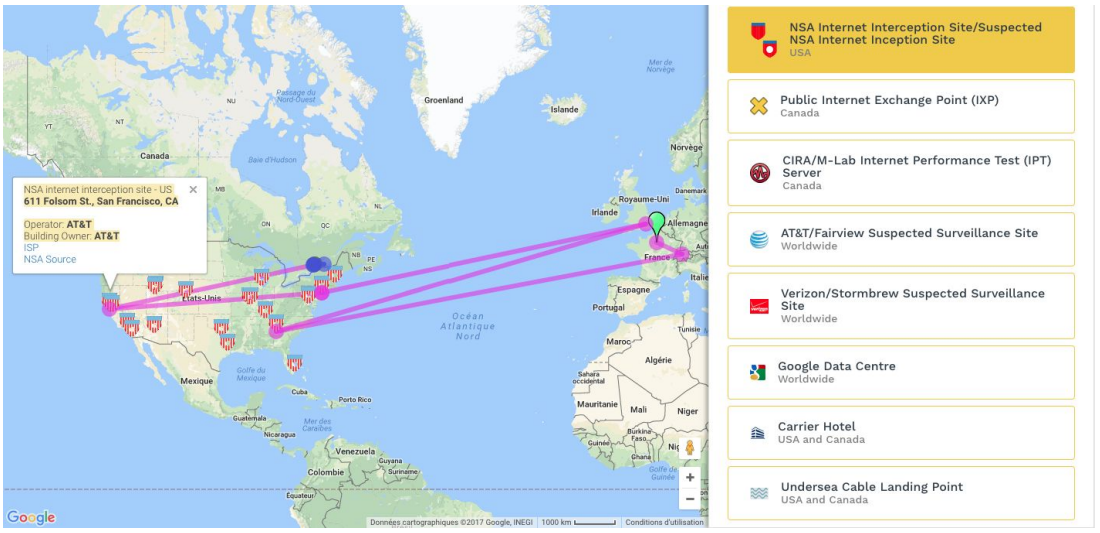
Le même jour, *The Guardian* et *The Washington Post* diffusent un autre article à propos d'un programme secret du FBI et de la NSA qui permettrait de collecter une grande majorité des données en provenance des internautes du monde : le programme PRISM. Très schématiquement, la NSA, à travers PRISM, est capable de récupérer des mails, messages, photos et vidéos que les utilisateurs croient protégés sur leurs comptes personnels hébergés par des grandes entreprises étatsuniennes telles Facebook, Google et Yahoo!.

Mais Edward Snowden révèle que les entreprises américaines ne sont pas les seules à être sous surveillance. Via un autre programme, appelé X-Keyscore et noué en partenariat avec la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande, la NSA aurait pu effectuer une "*collecte quasi systématique des activités de tout utilisateur d'internet*" grâce à plus de 700 serveurs localisés dans plusieurs dizaines de pays, notamment dans la quasi-totalité des pays européens, dont deux en France. Ce programme fonctionnerait, de manière très schématique, à la manière d'un moteur de recherches. Il permettrait d'archiver pendant quelques jours tout ce qui se passe sur internet. Il permet autant de récupérer les messages privés échangés sur Facebook que des courriels, mais aussi de retrouver l'historique de navigation, cibler les internautes en fonctions des technologies utilisées comme le chiffrement…

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Ces deux programmes cités, PRISM et X-Keyscore, ne sont que deux exemples parmi de nombreux autres révélés par Snowden. En effet, en plus du trafic internet, les données relatives aux conversations téléphoniques sont également surveillées, et ce partout dans le monde : en France, la NSA aurait aspiré les données correspondant à 70 millions de communications téléphoniques entre le 10 décembre 2012 et le 8 janvier 2013, aurait espionné des diplomates et intercepté les communications des passagers voyageant sur Air France, notamment. Pour résumer, la majorité des communications sont potentiellement surveillées par les États-Unis, comme le montre IXmaps, un outil cartographique publié en mars 2017 par Andrew Clement, un chercheur en sciences de l'information de l'Université de Toronto spécialisé dans la surveillance étatique :

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media



Le chemin emprunté par mon ordinateur pour accéder au site internet XImaps, le 13/10/2017, passerait par un site d'interception de données de la NSA situé à San Francisco.

Et la France ?

À travers les révélations d'Edward Snowden, nous connaissons bien l'implication des États-Unis dans cette chasse aux données. Pourtant, le gouvernement français est loin d'être en reste en terme de potentielle surveillance de ses concitoyens : la DGSI aurait même noué des partenariats avec la NSA pour mieux exploiter ses données. Mais, même sans l'aide étatsunienne, les organes français de défense et de contre-espionnage se débrouilleraient très bien.

En effet, dans un article publié en juillet 2013 dans le journal Le Monde, Jacques Follorou affirme que la DGSE (Direction Générale des Services Extérieurs) "*collecte systématiquement les signaux électromagnétiques émis par les ordinateurs ou les téléphones en France, tout comme les flux entre les Français et l'étranger : la totalité de nos communications sont espionnées. L'ensemble des mails, des SMS, des relevés d'appels téléphoniques, des accès à Facebook, Twitter, sont ensuite stockés pendant des années.*" Contrairement aux programmes américains, celui de la DGSE ne viserait que les *métadonnées* : qui parle à qui, pendant combien de temps, de quel endroit, le poids du message envoyé… Cela permet "*de dessiner une sorte de journal intime de l'activité de chacun, tant sur son téléphone que sur son ordinateur*". La DGSE aurait donc des capacités presque équivalentes à la NSA sur le territoire français…

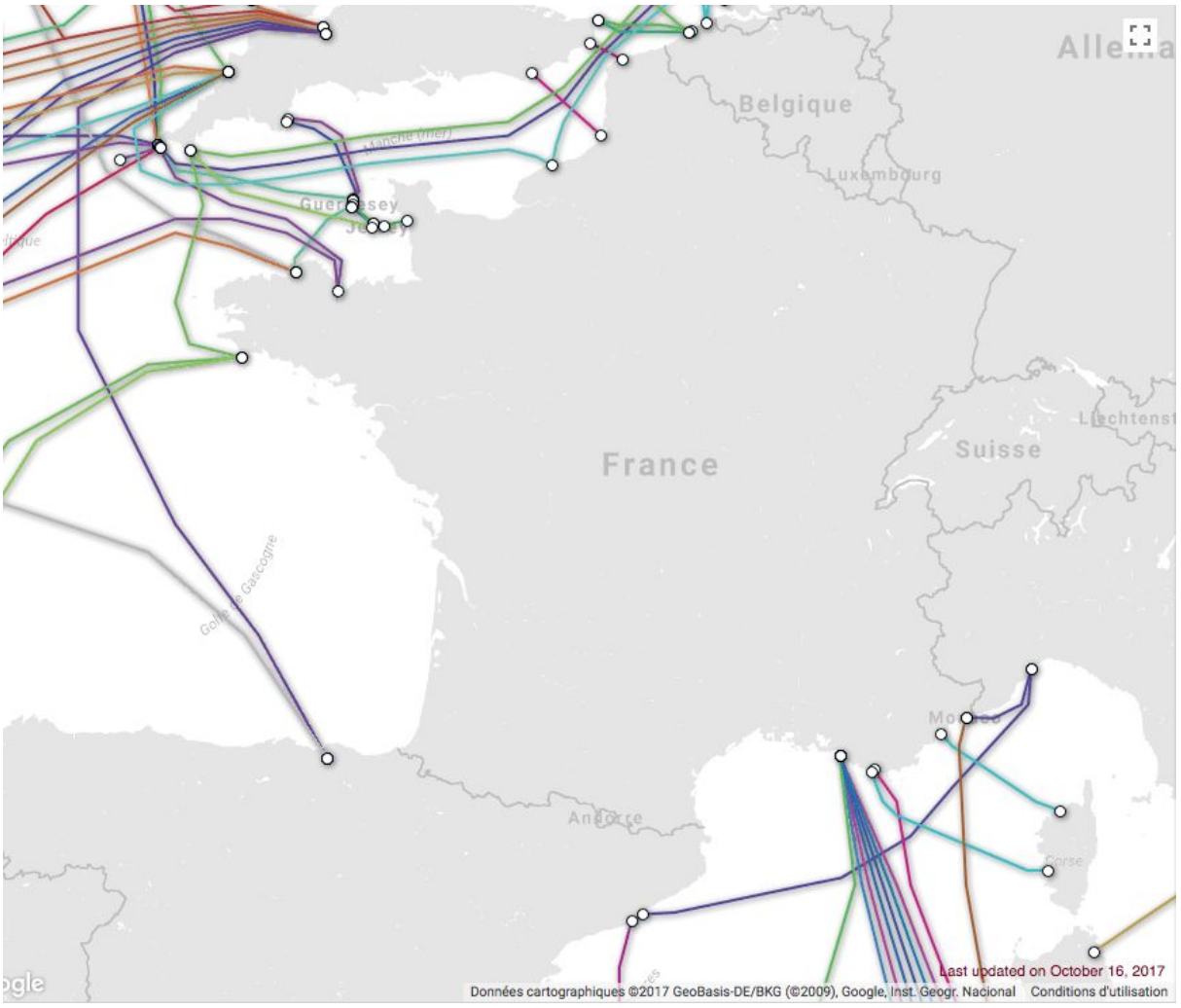
Pourtant, comme le soulève Jean-Marc Manach, journaliste d'investigation spécialisé dans la surveillance et de vie privée, cette "*surveillance de masse*" à la française et pour les Français serait assez improbable. D'une part parce que la DGSE est en charge de l'espionnage à l'étranger, mais aussi parce qu'elle serait *"techniquement improbable et*

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

financièrement impossible". Ce que semble confirmer "*un ancien espion"* dans un article paru en 2013 dans le Parisien : il confiait que la France "*n'avait pas les capacités financières ni les moyens humains pour traiter*" les données issues de toutes les communications françaises. Cette analyse, partagée par Jean-Marc Manach, est largement développée dans un article de son blog Bug Brother intitulé *"Pour en finir avec la surveillance de masse"* daté de septembre 2016 et dans un épisode de l'émission *What the fact?*.

En revanche, la DGSE possède bel et bien des systèmes de collecte de masse déployés sur les câbles sous-marins qui relient les réseaux de télécommunication français à l'étranger, afin de pouvoir surveiller les communications internationales. Et la France disposerait depuis 2009 d'un dispositif d'écoute de grande ampleur, visant les citoyens français, et baptisé IOL pour Interceptions Obligatoires Légales. Ce programme permettrait techniquement de mettre n'importe qui sur écoute tout en respectant la loi française qui était, pendant quelque temps, assez large pour intercepter les communications d'à peu près n'importe qui. En effet, l'article L-851-2 du code de la sécurité intérieure prévoyait de pouvoir non seulement surveiller les personnes en lien avec une menace terroriste, mais aussi "*l'entourage de la personne concernée".* Cette dernière phrase a récemment été déclarée anticonstitutionnelle.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media



Les nœuds des câbles sous-marins où transitent les données d'internet arrivant en France. La DGSE intercepterait les communications à ces endroits. Capture d'écran de https://www.submarinecablemap.com/#/

Les outils de surveillance à l'international

Pour surveiller ses concitoyens, les gouvernements ne sont pas non plus obligés d'avoir des capacités d'écoute faramineuses. Un gouvernement qui souhaite mettre en place une surveillance des communications doit simplement avoir de l'argent. En effet, des sociétés proposent désormais des systèmes de surveillance aux gouvernements : en 2007, la société Amesys vendait à la Libye de Kadhafi un système nommé *Eagle*. Très simplement, ce système permettait de surveiller tout le trafic internet et de stocker des données de connexion. Les boîtes mails, messageries instantanées, demandes de moteur de recherche, navigations web, tout pouvait être surveillé. Les téléphones portables, même éteints, pouvaient être géolocalisés. Ces données permettaient de cibler des personnes en particulier et, dans la Libye de Kadhafi, le système Eagle aurait permis d'arrêter et de

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

torturer des journalistes. Le *Wall Street Journal* a notamment enquêté sur Khaled Mehiri, journaliste libyen d'Al-Jazeera qui aurait été surveillé grâce à ce programme. Aujourd'hui, la société Amesys est poursuivie devant la justice française par la Fédération Internationale des Droits de l'Homme (FIDH) pour complicité de torture. Mais malgré cette poursuite judiciaire, toujours en cours, le système de surveillance a été vendu en 2014 à l'Égypte d'Al-Sissi avec "*la bénédiction des autorités françaises*". D'autres pays auraient acquis ce système ces dernières années, depuis l'Afrique de l'Ouest et Subsaharienne, en passant par l'Asie et l'Europe. Selon le même article, la France aurait seulement refusé de vendre ce système à deux pays, la Turquie et le Pakistan.

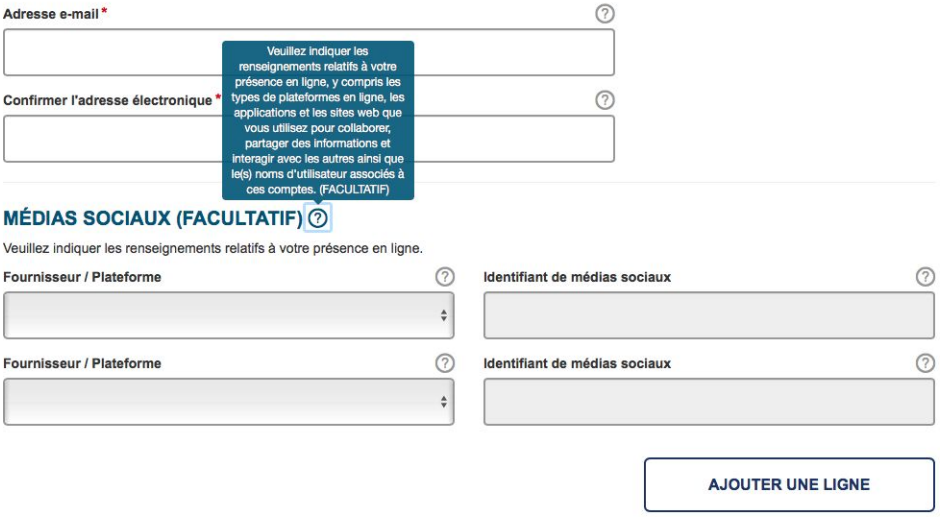
Ces programmes, bien souvent secrets, sont parfois doublés dans certains pays par l'adoption de lois bien précises. Ainsi, en novembre 2016, la Chine a mis en place une loi interdisant aux internautes de publier ou de diffuser quoi ce soit susceptible de "*salir l'honneur national*", "*déstabiliser l'ordre économique et social*" ou bien encore de "*renverser le système socialiste*". En outre, surfer anonymement sur internet est désormais illégal. Si critiquer ouvertement le pays sur les réseaux sociaux est puni d'au moins trois ans de prison, la question reste entière en ce qui concerne les échanges privés.

Des réseaux sociaux ouvertement surveillés

Outre les programmes secrets et les lois accentuant la censure mise en place dans des régimes dictatoriaux ou en passe de l'être, les pays dits démocratiques ne semblent pas en reste pour lutter "*contre le terrorisme*", avec les dérives que cela peut comporter.

Ainsi, depuis décembre 2016, les douaniers étatsuniens peuvent désormais requérir auprès de toute personne se rendant sur leur sol de nombreuses informations sur leurs activités passées sur les réseaux sociaux. Ce formulaire, pas obligatoire, mais "*conseillé*" pour ne pas "*retarder le processus de délivrance*" du visa, s'intéresse aux identifiants de réseaux sociaux des 5 dernières années. De nombreuses voix s'étaient fait entendre pour critiquer cette mesure pouvant aboutir très rapidement à "*la création de la plus grande base de données gouvernementale du monde*".

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media



Capture d'écran du formulaire "optionnel" à remplir
afin d'obtenir un visa de tourisme aux États-Unis

En France aussi, les législateurs s'étaient aussi intéressés aux identifiants des réseaux sociaux. Une proposition de loi avait été émise en septembre pour requérir auprès des personnes faisant l'objet d'une surveillance individuelle de contrôle, de déclarer les identifiants de communication électronique. Cette mesure a finalement été supprimée.

Ces mesures étatiques, secrètes ou non, permettent une surveillance potentielle des activités en ligne de n'importe qui, que ce soit justifié par la lutte contre le terrorisme ou non. Et ces mesures de surveillance peuvent être d'autant plus facilitées par des failles de sécurité ou des *backdoor** dans les logiciels et les outils que nous utilisons tous chaque jour.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

B - Pile ET face : nos outils du quotidien sont peu sûrs

L'architecture et les possibilités des outils informatiques que nous utilisons chaque jour nous sont strictement inconnues, ou presque. Pourtant, ils peuvent présenter de nombreux risques plus ou moins dangereux que peuvent exploiter des personnes, des sociétés ou des états.

Pile : recueil légal d'informations à travers les métadonnées

Tout ce que nous faisons, ou presque, sur internet produit des métadonnées. Nous pouvons les comparer à une enveloppe : seul le message situé à l'intérieur de l'enveloppe n'est pas lisible. Il est possible, en revanche, de lire le nom et l'adresse du destinataire, le nom et l'adresse de la personne qui l'a envoyé, vos positions géographiques respectives, la date de l'échange… Dans le monde numérique, ce sont les objets de nos mails, la taille de nos conversations, les positions géographiques, les durées d'appel, les sites consultés, les recherches effectuées, les achats… Sur nos smartphones, c'est nous-mêmes qui choisissons les métadonnées que nous partageons avec les entreprises qui éditent les applications : elles sont définies par les "*autorisations"* que nous délivrons machinalement avant leur installation.

Voici une définition des métadonnées donnée par Edward Snowden, dans une interview à Vice : *"Plutôt que d'envoyer des gens pour vous surveiller, on utilise les appareils que vous avez payés, les services et les systèmes qui vous entourent chaque jour de façon invisible, pour vous observer en notre nom. Les métadonnées, c'est le fait qu'une communication a eu lieu. Savoir que vous m'avez appelé, quand vous m'avez appelé, d'où vous m'avez appelé… Ces informations sont les mêmes que celles produites par un enquêteur privé qui vous suit toute la journée. Ils ne peuvent pas s'asseoir assez près de vous dans tous les cafés, pour écouter tous les mots que vous prononcez. Mais ils peuvent être assez proches pour savoir à quelle heure vous avez quitté votre maison, quel est le numéro de la plaque d'immatriculation que vous conduisez, où vous êtes allé, avec qui vous vous êtes assis, combien de temps vous êtes resté, quand vous êtes parti, où vous êtes allé ensuite… Tout ça, ce sont des métadonnées. "*

Aujourd'hui, de très nombreuses applications sur nos smartphones recueillent de telles données sans même que nous le sachions. Dans le documentaire *Nothing to Hide*, sorti en 2016 et disponible gratuitement depuis peu sur internet, Max Thommes accepte que les réalisateurs espionnent son ordinateur, son smartphone et ses applications pendant un

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

mois. Seules ses métadonnées seront analysées. Au bout d'un mois, ils parviennent à dresser un portrait très fidèle de cet artiste sans pour autant avoir ne serait-ce qu'une fois écouté ses conversations, qu'elles soient écrites ou orales. Cette analyse est largement corrélée par un article écrit par une équipe de chercheurs de Stanford, intitulé *Evaluating the privacy properties of telephone metadata*.

Dans une société capitaliste telle que la nôtre, l'utilité de ces données a été trouvée : elles permettent aux sociétés telles que Facebook de proposer de la "publicité ciblée" en fonction de ce qu'elle a pu recueillir sur vous. Outre l'aspect mercantile, ces métadonnées peuvent aussi (et surtout ?) permettre de nous surveiller : de nombreux gouvernements, et y compris la France, minimisent l'impact des programmes de surveillance et de collection des métadonnées. C'est d'ailleurs la conclusion de l'article écrit par l'équipe de Stanford : "*Les programmes de surveillance des métadonnées à grande échelle, comme ceux de la NSA, mettront forcément en lumière des informations très confidentielles à propos d'ordinaires citoyens".*

Face : recueil illégal d'informations

Dans une société où les données personnelles sont aussi massivement disponibles, notamment sur les serveurs des entreprises, les piratages de données sont très fréquents, comme le rappelle un article du Figaro écrit par Benjamin Ferran en octobre 2017 : "*Pas une semaine ne passe sans la découverte de vols de données majeurs, qui révèlent la légèreté avec laquelle ces sociétés gèrent nos informations personnelles. Le dernier en date [...] concerne le vol de 540.642 comptes d'une entreprise de géolocalisation de voitures, SVR Tracking. Il y a deux semaines, ce fut le vol de données personnelles de 143 millions d'Américains présents dans les fichiers de l'agence de crédit américaine Equifax."* Sans parler de vol de données, les actes de malveillance sont aussi très nombreux et sont utilisés depuis de nombreuses années par des groupes de hackers, souvent financés par des gouvernements souhaitant nuire à des entreprises. Les exemples sont très nombreux, puisque 80% des entreprises auraient déjà été la cible d'une cyberattaque, mais nous pouvons retenir le piratage de TV5Monde qui a eu lieu en 2015 et qui a coûté la bagatelle de 10 millions d'euros.

Pour quiconque un tant soit peu doué en informatique et ciblant des personnes moins douées, il n'est pas très compliqué d'installer des logiciels espions ou de subtiliser des données sur des ordinateurs à travers du *phishing*. Dans le meilleur des cas, ce seront de "simples pervers" souhaitant espionner de jeunes demoiselles dans leur bain via leur

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

webcam, mais ce peut être également utilisé sur des personnalités politiques, comme cela a été le cas avec les emails de John Podesta, le directeur de campagne d'Hillary Clinton.

Dans un logiciel ou une application, un *backdoor* ou *porte dérobée* est, d'après la définition de Wikipedia, "*une fonctionnalité inconnue de l'utilisateur légitime qui donne un accès secret au logiciel*". Par exemple, la société de sécurité Kryptowire a découvert en décembre 2016 que plusieurs modèles de smartphones tournants sous Android et fabriqués en Chine contenaient des logiciels secrets de collecte de données préinstallées. Les SMS, données de géolocalisation, listes de contact et autres seraient transmis à un serveur de Shanghaï afin de permettre aux autorités d'accéder à ces données, si besoin. Plus récemment, une porte dérobée a été découverte dans un logiciel très connu de nettoyage, CCleaner, et aurait permis de dérober des informations sur plus de 700 000 personnes. Cette attaque qui aurait été financée par "*un groupe de hacker payé par un état"*.

Les interfaces de connexion WIFI publiques, présentes un peu partout dans les aéroports et les cafés, peuvent aussi être compromises et permettre la surveillance totale des personnes s'y connectant comme le montrait les révélations de Wikileaks, publiées par Médiapart en mars 2017, ou encore la récente faille massive dans les protocoles de sécurité du WiFi, surnommée KRACK.

De la surveillance au piratage : nous avons tous des choses à cacher et les journalistes aussi (et surtout)

Les risques de vol de données, conscients ou non, sont légion et il serait vain de vouloir toutes les lister. Chaque jour, de nouvelles failles sont découvertes, de nouveaux piratages ont lieu, de nouvelles applications nous demandent plus de données quand ce n'est pas nous-mêmes qui les donnons volontairement. Pour autant qu'il y a utilisation d'un outil informatique associée à une interface de communication, les risques sont nombreux et peuvent être très dommageables.

Comme devant la vidéosurveillance, nombreux sont ceux qui disent "*ne rien avoir à cacher*" et ne pas se soucier de la potentielle collecte des gouvernements ou des piratages de leurs données, tant qu'ils n'en subissent pas directement les conséquences. Lors d'une conférence à laquelle j'ai assisté il y a quelques années, un activiste "défenseur de la vie privée sur internet" demandait au public de lui remettre sur un bout de papier tous leurs

identifiants et mots de passe de tous leurs comptes mails et de réseaux sociaux. Ainsi que leurs codes de comptes bancaires. Il leur promettait qu'il n'y toucherait jamais, qu'il ne les regarderait jamais. Combien l'ont fait ? Aucun. Tout le monde souhaite cacher des choses et devrait cacher des choses.

Photo extraite de l'article "Rien à cacher", publié par Laurent Chemla sur le site Reflets.info

De plus, Laurent Chemla a exposé quelque chose d'essentiel dans un article de Reflets, publié il y a déjà deux ans : "*L'information principale du programme PRISM et de ses suites, c'est que l'information recherchée n'est pas ce que nous disons, mais* à qui *nous le disons. Le contenu de nos conversations reste intéressant bien sûr (surtout pour les entreprises qui ont intérêt à tout savoir de nos vies), mais pas tellement pour les états. Ce que veulent les états, c'est tout savoir de nos réseaux. [...] La question n'est plus « pourquoi doit-on se protéger », mais bien « pourquoi doit-on protéger ceux avec qui on échange ». [...]*

Une image, peut-être plus parlante que mes histoires de selfies piégés et d'attentats futurs, est celle qui demande aux visiteurs de cette réserve – où vivent des rhinocéros – de ne pas diffuser les photos qu'ils prennent sur les réseaux sociaux, ou sinon de désactiver la géolocalisation de leurs appareils. Parce que celles-ci pourront, sinon, servir à indiquer aux braconniers où et quand vont les animaux qu'ils vont abattre pour leurs cornes. [...] Oui, se protéger soi-même est utile. Mais quand l'énorme majorité de nos correspondants ne le sont pas, alors nous sommes autant à l'abri de la surveillance que nos amis rhinocéros."

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Inconsciemment ou non, Laurent Chemla a exposé ce que devrait être essentiel dans le travail des journalistes, aujourd'hui : il est certes important de se protéger et de protéger son intégrité en tant que journaliste, mais il est tout aussi important, sinon plus, de de protéger ses sources. Ce devoir de protection est d'ailleurs l'objet de l'article 7 de la Charte de Munich : *Garder le secret professionnel et ne pas divulguer la source des informations obtenues confidentiellement.* Jean-Marc Manach, journaliste d'investigation, confirme aussi cela : "*Ce devrait être une obligation professionnelle. Énormément de citoyens sont soumis à un devoir de confidentialité, et les journalistes tout particulièrement.*" Comme nous l'avons vu tout au long de cette partie, il n'y a rien de plus facile que de pénétrer nos outils numériques, pour qui veut réellement.

Par leur rôle particulier dans la société, par leur volonté de révéler des secrets d'état, de corruption, d'arrangements entre grandes entreprises, certains journalistes peuvent représenter des cibles, comme l'a encore montré très récemment l'assassinat de la journaliste maltaise Daphne Caruana Galizia.

Mais se protéger numériquement ne devrait pas être uniquement l'apanage des journalistes d'investigation. Comme le souligne Jean-Marc Manach, la protection des sources est le premier devoir de tout journaliste et ce d'autant plus dans un monde où, on l'a vu, il est si facile de découvrir qui communique avec qui, sans même que les deux personnes qui échangent ne s'en aperçoivent.

2 - LES JOURNALISTES ET LEURS SOURCES

A - Des journalistes (et leurs sources) ciblés par leurs propres gouvernements

Le 26 octobre 2016, Edward Snowden était invité par le journal allemand *Süddeutsche Zeitung* à participer à une table ronde sur le journalisme. Il y soulignait notamment que la liberté de la presse ne pouvait exister sans ce lien de confidentialité entre les journalistes et leurs sources, mais qu'aujourd'hui, les journalistes étaient des cibles, notamment de la part de leurs propres gouvernements. Il prenait notamment comme exemple James Risen, un journaliste du New York Times qui avait subi des pressions pour révéler ses sources.

Outre les pressions, il y a aussi les tentatives de piratage : en octobre 2016, lors d'une table ronde des "Assises de la sécurité" intitulée *Journalistes : la sécurité des données*

au service de l'information, le responsable de la sécurité informatique du journal Le Monde, José Bolufer annonçait que 21 attaques informatiques avaient visé des journalistes du Monde en moins de 18 mois, dont 8 attaques envers des journalistes bien identifiés. Pour des raisons de confidentialité, il ne dira pas si les attaquants étaient connus ni sur quels sujets travaillaient ces journalistes. Les attaques informatiques ne connaissent pas les frontières : les journalistes sont particulièrement visés, peut-être par des puissances extérieures, mais aussi par leurs propres gouvernements.

Au Mexique, de faux messages pour un véritable espionnage

Le Mexique est loin d'être le pays le mieux coté au classement de Reporters Sans Frontières : il se positionne à la 147e place. Cette année, dix journalistes y ont été tués. Sur les 92 journalistes tués depuis 1994, 13 travaillaient sur des sujets relatifs à la corruption tandis que 12 travaillaient sur la politique. Bien entendu, il ne s'agit pas de dire qu'ils ont été tués sous les ordres des différents gouvernements en place. En revanche, selon un rapport publié en avril 2017 par l'ONG Article19, au moins 53% des 426 actes de violence et d'intimidation concernant les journalistes en 2016 étaient liés d'une manière ou d'une autre aux autorités. Et quoi qu'il en soit, le gouvernement mexicain semble particulièrement surveiller ses journalistes.

En juin 2017, l'ONG de défense de la liberté de la presse Citizen Lab a révélé que le gouvernement mexicain avait tenté de déployer un spyware (logiciel espion) auprès de 7 journalistes, au moins. Ces journalistes enquêtaient sur des affaires de corruption concernant le président du Mexique, mais aussi sur la participation des autorités à des violations des droits de l'homme.

Ce logiciel espion, créé par la société israélienne NSO, permet d'envoyer un SMS ou un mail à une cible en lui proposant de cliquer sur un lien installant de manière frauduleuse un logiciel espion. Il est assez facile de tomber dans le panneau : le SMS peut sembler provenir d'une source officielle. Par exemple, un des SMS envoyés à Carlos Loret, journaliste de télévision, se faisait passer pour l'ambassade américaine et expliquait qu'il y avait un souci avec sa demande de visa ; s'il voulait en savoir plus, il devait cliquer sur le lien inclus dans le message. Des SMS envoyés à d'autres journalistes les prévenaient de menaces pesant sur leurs vies, de l'infidélité de leurs partenaires ou encore de messages en lien avec leur travail. Au moins 76 messages de ce type auraient été envoyés aux sept journalistes.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Exemple de SMS reçu par des journalistes, les prévenant que des individus semblent vouloir les menacer

Lorsque la personne ciblée clique sur le lien contenu dans le message, un logiciel espion s'installe sur son terminal (smartphone ou ordinateur) et permet la surveillance totale du terminal, y compris les messages et applications chiffrés. Il n'est pas explicitement prouvé que c'est le gouvernement mexicain qui soit à l'origine de ces messages, mais un faisceau de preuves oriente les enquêteurs dans cette direction. Dans ce cas précis, une protection spécifique est inutile : il faut simplement éviter de cliquer sur le lien. La liste des clients de NSO, l'entreprise israélienne à l'origine de ce programme, est inconnue. En revanche, il aurait été également utilisé aux Emirats Arabes Unis contre Ahmed Mansoor, un défenseur des droits de l'homme.

"Affaire Lagacé" : au Canada, les métadonnées comme outil de surveillance

Le Canada fait figure, aux yeux du monde, d'un pays plus que respectable. Dans le classement RSF, il a pourtant chuté de 14 places depuis 2015 : il est désormais placé à la 22e place. À titre de comparaison, la France est 39e. Pourtant, là aussi des journalistes ont

été ou sont espionnés par les autorités. L'exemple le plus récent et le plus frappant est celui du journaliste Patrick Lagacé.

En octobre 2016, "l'affaire Lagacé" est dévoilée : ce journaliste spécialisé en faits-divers pour le journal québécois La Presse (premier site d'information francophone au Canada) avait été surveillé par le Service de Police de la Ville de Montréal (SVPM) entre janvier et juillet 2016.

À l'origine de cette surveillance était la volonté du SVPM de savoir comment des informations confidentielles sur des enquêtes en cours étaient publiées par le journal. Ces enquêtes concernaient "*de banales affaires de droits communs"*, selon Patrick Lagacé. Ils ont donc espionné son téléphone tout à fait légalement, grâce à plusieurs mandats validés par un juge : numéros des appels entrants et sortants, numéros des SMS envoyés/reçus ainsi que ses positions GPS. Bref, ses métadonnées étaient enregistrées par les autorités. Le SVPM a affirmé que les données obtenues étaient protégées et n'étaient pas utilisées. Mais selon plusieurs autres personnes, dont un chercheur en droit public, cette surveillance avait été mise en place "*uniquement pour essayer d'obtenir des informations sur ses sources d'information, sur l'identité des personnes qui l'ont informé ou l'auraient informé dans le cadre de son travail*". Dans ce cas-là, cela relèverait d'une violation du secret des sources et de la "*violation caractérisée de la liberté de la presse"*.

Cette affaire a fait beaucoup de bruit au Canada, et beaucoup pensaient que ce n'était qu'un "dérapage". Pourtant, quelques jours plus tard, RSF révélait que 5 autres journalistes avaient été ainsi surveillés depuis 2013, tandis que d'autres s'étaient vus obligés par la Justice de livrer leurs sources. En avril 2017, un septième journaliste a appris qu'il avait été lui aussi placé sous surveillance. Très récemment, en octobre 2017, le Canada a adopté une loi protégeant les journalistes et leurs sources : l'amendement S-231. Reste à savoir s'il sera respecté.

En France, des lois peu claires

En France, c'est l'affaire Woerth-Bettencourt qui a défrayé la chronique en 2009-2010. Alors que l'affaire bat son plein et que les révélations sont toujours plus nombreuses, les ordinateurs de plusieurs journalistes de différents médias sont volés à quelques jours ou semaines d'intervalle. Parfois à leurs domiciles, parfois lors de cambriolages de leurs journaux. Leur point commun ? Tous les journalistes volés travaillaient sur ce même dossier.

Bien que rien ne peut prouver que ces vols ont été commandités par le gouvernement, tous s'interrogent. L'exécutif, lui, se cache derrière la garantie de la loi de

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

protection des sources adoptée en catastrophe en janvier 2010 à la suite des révélations du Canard Enchainé. Selon le palmipède, la DCRI (Direction centrale du renseignement intérieur) avait requis en 2009 les “fadettes” d’un journaliste du Monde dans le cadre de la même affaire Woerth, ceci pour découvrir qui était à l’origine des informations révélées par le journaliste Gérard Davet. Ces fadettes, ce sont les factures téléphoniques détaillées où tous les numéros de téléphone appelés et appelants sont recueillis, ainsi que les durées d’appel. Depuis, Bernard Squarcini, l’ancien directeur de la DCRI, a été reconnu coupable et a été condamné à 8000 euros d’amende. À ce jour, on ne connaît toujours pas l’identité des voleurs d’ordinateurs, mais ce qui est certain c’est que l’utilisation des fadettes aurait permis de déterminer l’identité de la source de Gérard Davet : il s’agirait du conseiller au ministère de la Justice, David Sénat, qui a été démis de ses fonctions très peu de temps après et muté à Cayenne, en Guyane. Il a toujours démenti son implication.

Quelques années après l’affaire Bettencourt et les fadettes, en 2015, la “Loi renseignement” est votée en France. Ceci pour permettre de “*lutter plus efficacement contre le terrorisme*”, de prévenir la criminalité organisée, de protéger les “*intérêts essentiels de la politique étrangère*” ou *“les intérêts économiques essentiels”* de la France. En outre, selon Le Figaro, elle permet de légaliser *“des pratiques jusqu’ici illégales des agents de renseignement*”. Parmi les moyens autorisés, l’accès direct aux réseaux des opérateurs télécom, services en ligne (comme Facebook) ou encore les hébergeurs de site. Elle autorise aussi le recours aux IMSI-catcher, de fausses antennes téléphoniques capables d’aspirer toutes les données d’un smartphone. Cette loi considérée par certains comme liberticide dit pourtant protéger quelques catégories de la population, dont les journalistes français : “*Les personnes qui exercent en France un mandat ou une profession mentionnée à l’article L. 821-7 ne peuvent faire l'objet d'une surveillance individuelle de leurs communications à raison de l'exercice du mandat ou de la profession concerné. “* Les journalistes étrangers sont donc exclus de cette protection.

En outre, Sergio Coronado, député européen, dénonçait les seules communications liées à *“l’exercice du mandat ou de la profession concernée”*. En clair, selon la loi, les journalistes ne seraient protégés de cette surveillance que lors de leurs heures de travail. Sergio Coronado précisait : *“Le tri entre les communications privées et professionnelles est impossible à opérer a priori : n’importe quel technicien vous le dira. En effet, cela implique d’abord une collecte des données, puis un traitement des renseignements collectés, pour ensuite faire le tri. “* Une Question Prioritaire de Constitutionnalité avait été lancée par la Quadrature du Net notamment à ce sujet. La réponse du “conseil des Sages” avait été

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

limpide : "*aucune disposition constitutionnelle ne consacre spécifiquement [...] un droit au secret des sources des journalistes*".

C'est donc pour préciser cette loi qu'en janvier 2016 le Syndicat National des Journalistes et la Fédération Internationale des Journalistes ont déposé une requête devant la Cour européenne des droits de l'homme (CEDH). Il y a quelques mois, la CEDH a jugé la plainte "recevable", mais aucune décision ou arrêt ne sera pris avant deux ou trois ans. Techniquement, les journalistes français peuvent donc être surveillés par le gouvernement français lorsqu'ils ne travaillent pas, et les journalistes étrangers peuvent l'être tout le temps. Une loi du même type a d'ailleurs été votée en Allemagne.

B - Des risques personnels

Les journalistes doivent absolument veiller à protéger leurs sources d'information afin que les informateurs n'aient pas peur de témoigner ou de transmettre des informations. Cela est rendu de plus en plus difficile avec les différents moyens technologiques et législatifs entrevus précédemment. Les conséquences réelles de ces atteintes à la protection des sources sont difficiles à établir : sauf cas précis, comme lors de l'affaire Woerth, impossible ou presque d'en connaître les conséquences. Mais parallèlement à ce devoir de protection essentiel, les journalistes peuvent aussi courir des risques à titre personnel lorsque leur sécurité numérique n'est pas bien établie.

Marie Colvin : l'interception d'un appel satellite ?

Par leur métier et leur terrain très particulier, les reporters de guerre courent souvent de gros risques. Depuis 2011 et le début du conflit syrien, 128 journalistes ont été tués en Syrie, d'après le *Comitee to Protect Journalists*. Mines, attentats, tirs croisés : ils sont au plus près des combats et s'exposent volontairement à ces risques. Mais, parfois, dans des conflits où l'on souhaite avoir le moins de "publicité" possible et malgré les accords internationaux, ils peuvent être visés. C'est ce qui semble s'être produit en 2012 pour Marie Colvin et Rémi Ochlik, respectivement journaliste pour le *Sunday Times* et photographe pour Paris Match. Ils auraient été tués à la suite d'un appel passé via un téléphone satellitaire qui aurait permis à l'armée syrienne de les géolocaliser.

Début 2012, les deux journalistes, ainsi que plusieurs autres confrères, couvrent le conflit qui fait rage dans la ville de Homs alors en état de siège. Ils travaillent depuis un appartement situé dans le quartier rebelle de Bab Amr, transformé en centre de presse. Le

22 février, Marie Colvin appelle via un téléphone satellitaire la BBC, Channel Four et CNN afin de leur livrer un reportage. Elle raconte notamment comment l'armée de Bachar Al-Assad pilonne la ville "avec impunité, sans merci à l'égard des civils". Quelques heures plus tard, une pluie d'obus s'abat sur le centre de presse : les deux journalistes trouvent la mort, deux autres journalistes sont blessés ainsi qu'un traducteur. Très rapidement, un lien semble s'établir : ils ont été délibérément visés par les forces d'Assad qui ont profité de cet appel téléphonique pour géolocaliser le centre. Le président français de l'époque, Nicolas Sarkozy, dénonce dès le lendemain des "*assassinats*", assurant "*tenir les autorités syriennes pour responsables*". Ce que nie en bloc le gouvernement syrien.

En juillet 2016, la famille de Marie Colvin porte plainte devant un tribunal de Washington contre le régime, l'accusant de l'avoir tuée "*délibérément et avec préméditation"*. Cette accusation repose sur des documents officiels interceptés et le récit de transfuges et une enquête menée pendant 4 ans par le *Center for Justice and Accountabilty* (CJA). Selon cette enquête, les services secrets syriens auraient tracé l'appel téléphonique afin de localiser le centre de presse, puis auraient fait confirmer l'information par un de leurs informateurs sur place. D'après les documents en possession du CJA, la frappe aurait été décidée ou approuvée par le frère de Bachar Al-Assad, Maher, alors commandant des gardes républicains, tandis que la décision de cibler les journalistes aurait été prise par le cabinet de Bachar Al-Assad lui-même.

De son côté, le président syrien affirme que Marie Colvin est "*responsable de tout ce qui lui est arrivé",* que *"personne n'a aucune preuve"* et que "*les forces armées ne savaient pas que Marie Colvin se trouvait quelque part"*. Le seul article qui confirme cette théorie a été écrit *par un "observateur informé à Damas"*, publié sur le site personnel de Joshua Landis, directeur du Centre d'études du Moyen-Orient de l'université d'Oklahoma. Dans l'article intitulé "*La mort de Marie Colvin était tragique, mais c'était un hasard"*, cet "*observateur"* affirme que les services secrets syriens présents à Homs *"n'avaient pas la capacité d'analyser et d'intercepter les signaux pour déterminer une position. [...] Il faudra un an avant que le gouvernement syrien n'obtienne du matériel capable d'identifier la position des communications"*.

Encore aujourd'hui, il est impossible d'établir avec certitude quelle version est la plus proche de la vérité. En revanche, une enquête effectuée par l'ONG Privacy International a montré fin 2016 que le gouvernement syrien s'est équipé de systèmes de surveillance globaux dès 2008, particulièrement pour surveiller internet, que ce soit via le réseau câblé ou satellitaire. En outre, un article du site *Safer Mobile*, publié par un "*contributeur anonyme*

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

travaillant dans l'industrie de la télécommunication", précise que localiser un téléphone satellite est "*relativement simple*" et peut se faire de plusieurs façons. Le moyen le plus simple et le plus accessible est d'utiliser un analyseur de spectre, disponible dans le commerce pour une vingtaine de milliers de dollars.

Ahmed Abba, des données non protégées sur son ordinateur ?

En juillet 2015, Ahmed Abba, correspondant de RFI au Cameroun, est arrêté. Il travaillait sur Boko Haram et se voit reprocher d'avoir été en contact avec certains des membres de ce groupe islamiste, de ne pas avoir partagé avec les autorités des informations qu'il aurait pu recueillir dans le cadre de son travail de journaliste. Il disparaît peu après lors d'un transfert : il est torturé par les services de renseignement et devra attendre quatre mois pour pouvoir voir son avocat. En février 2016 son procès commence, "*sans témoin, sans preuve*" ; il est accusé de non-dénonciation d'actes de terrorisme, d'apologie et de blanchiment d'actes terroristes. Il est condamné à mort, mais ses avocats réussissent à convertir sa peine à dix ans de prison.

Lors de son procès éclair, un collège d'experts a présenté des photos et des vidéos qui auraient été prises par Ahmed Abba sur les lieux d'attentats. De plus, "*des SMS annoncés comme cryptés (sic) et qui étaient, selon les experts, des messages d'attentat ont aussi été présentés".* Selon le collège d'experts, ces médias auraient été retrouvés sur l'ordinateur personnel du journaliste, mais cette expertise a été dénoncée comme à charge par les avocats de la défense.

Dans ce procès dont le verdict est contesté en appel, il est aujourd'hui impossible de déterminer si les photos, les vidéos et messages chiffrés présentés lors de l'audience sont bel et bien authentiques. De plus, impossible de savoir la raison première de son incarcération, ni s'il était sous surveillance ou si c'est à la suite de ses reportages qu'il a été décidé de le neutraliser. De leur côté, les avocats et RSF dénoncent un procès politique visant à "*effrayer les journalistes qui souhaiteraient couvrir la question de la sécurité dans le nord du Cameroun".* En effet, d'après les avocats, toutes les accusations envers Ahmed Abba sont infondées puisque, notamment, il aurait communiqué "*à chaque fois aux autorités toutes les informations qui parvenaient à sa connaissance et de nature suspecte".* Aujourd'hui, huit journalistes sont emprisonnés au Cameroun.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Protéger et se protéger pour éviter un tarissement des sources

Il est très difficile d'établir une liste de journalistes qui auraient été directement menacés par un manque de sécurité numérique. Même les deux cas cités ne sont pas forcément valables, si l'on y regarde de près. Dans le cas de Marie Colvin, impossible à l'heure actuelle de savoir si c'est bien à cause d'une interception qu'elle a été tuée. Dans l'autre cas, celui d'Ahmed Abba, impossible de savoir si les documents retrouvés sur son ordinateur lui appartiennent vraiment.

Dans l'extrême majorité des cas et sauf environnements très précis, la sécurité numérique des journalistes n'est donc utile qu'à une seule chose : protéger leurs sources et assurer aux futures sources que leurs identités seront fermement protégées.

Dans deux des cas présentés, Patrick Lagacé et Gérard Davet, les sources ont été découvertes et celles-ci ont souffert de conséquences directes. Nous ne savons pas si les sources des journalistes visés au Mexique ont été découvertes, mais les conséquences probables peuvent être bien pires que la prison. Concernant Edward Snowden et les autres lanceurs d'alerte, l'assurance d'être bien protégé est essentielle : si les potentielles sources et lanceurs d'alerte pensent qu'ils peuvent être repérés, ils ne diront rien. Et si les sources se tarissent, le journalisme est en état de mort clinique.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Conclusion de la première partie

Les sociétés, qu'elles soient démocratiques ou dictatoriales, ont toujours raffolé des dispositifs de surveillance. C'est en partie grâce à ceux-ci que le contrôle est possible. Et dans nos sociétés aujourd'hui largement numériques, ce contrôle et cette surveillance passent par les outils que nous utilisons chaque jour pour communiquer, travailler et nous divertir. Nous l'avons vu, les états aujourd'hui possèdent des moyens d'énormes moyens de surveillance et n'hésitent pas à les utiliser, même dans les états démocratiques. Ce qui nous rend d'autant plus vulnérables, c'est que les services auxquels nous faisons confiance pour nos communications n'hésitent que très rarement à travailler avec les autorités. Et la situation est encore pire dans les états où la liberté de la presse est absente ou largement discutable. Il est donc essentiel de savoir se protéger.

Peut-être plus que pour les autres catégories de la population, la protection numérique devrait être un devoir essentiel pour les journalistes puisqu'ils doivent assurer aux personnes qui leur parlent qu'elles sont protégées. D'après deux chercheurs en sécurité de Google, les journalistes du monde entier étaient d'ailleurs *"massivement surreprésentés"* parmi les cibles d'attaques électroniques.

La grande difficulté, quand on en vient à la sécurité numérique, est que la menace est strictement invisible : à moins d'être particulièrement versé dans la technique, impossible de savoir si l'on est surveillé à travers nos outils électroniques. Il est donc nécessaire de prendre des dispositions en amont pour éviter au maximum cette possibilité.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

II - Se protéger pour protéger ses sources : l'indispensable travail des journalistes

1 - LES JOURNALISTES ET LA SÉCURITÉ NUMÉRIQUE

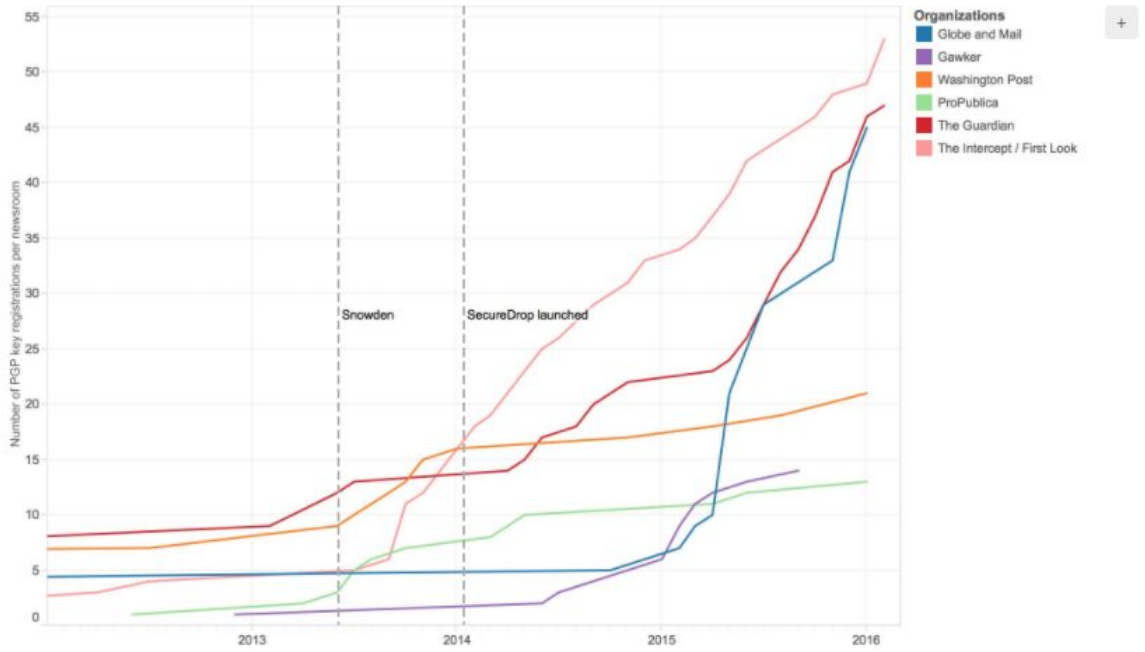
A - Une certaine prise de conscience

Les révélations Snowden et le développement de PGP

Depuis 2012 et les révélations d'Edward Snowden concernant les capacités d'écoute du gouvernement américain, une prise de conscience a semblé émerger concernant la nécessité de protéger nos communications. D'après James Clapper, le directeur du renseignement américain jusqu'en 2017, les révélations de Snowden auraient largement fait accélérer le développement des outils de chiffrement, jusqu'à prendre plus de sept ans d'avance par rapport à ce que la NSA avait prévu.

Peu d'études montrent le développement des outils de chiffrement dans les rédactions (encore moins en France), mais voici un graphique illustrant l'évolution du nombre de clé PGP (permettant d'envoyer et recevoir des mails chiffrés) générée dans cinq médias anglo-saxons depuis 2012. La courbe s'accélère nettement après les révélations de Snowden :

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media



https://towcenter.gitbooks.io/guide-to-securedrop/content/case_studies_news_organizations/index.html

Entre autres indices plus visibles, de nombreux journalistes ont commencé à afficher sur leurs comptes Twitter leur “clé PGP”. Pourtant, un certain nombre d’entre eux semblent ne pas le faire correctement. Et reste à savoir s’ils savent vraiment l’utiliser, parce que les erreurs peuvent être nombreuses, et si leurs sources connaissent aussi bien qu’eux ce protocole.

Très peu de formations systématiques

Les formations pour les journalistes partant sur des terrains de conflit existent depuis un certain temps. En France, ces stages peuvent être notamment réalisés via l’armée. Mais cela ne fait que peu de temps que des formations concernant la sécurisation des communications existent et concordent également avec les révélations d’Edward Snowden. Par exemple, en France, le premier guide de RSF à ce sujet date de 2013 et il semblerait que les premières formations physiques datent de la même année. À part ces formations de RSF et une formation proposée au CFPJ, il est difficile de trouver des formations en présentiel pour les journalistes professionnels.

Du côté des écoles de journalisme reconnues, elles sont encore rares à intégrer de véritables sessions concernant la protection des sources au sein de leur cursus initial. Voici un tableau regroupant les 14 écoles, avec en regard s’ils évoquent ou non dans leurs

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

plaquettes, sur leurs sites ou bien dans leur communication des cours relatifs à la protection des sources et/ou à la sécurité numérique :

ESJ	CFJ	IFP	IPJ	CELSA	CUEJ	EJT
Non	Non	Non	Non	Non*	Non	Non

EDC	EJDG	EJCAM	EPJT	IJBA	Lannion	Sciences Po Paris
Non	Non	Non	Non*	Non	Non	Non*

CELSA : "CryptoParty", atelier d'initiation de 3 heures avec Amaëlle Guiton en 2016

EPJT : Conférence avec Fabrice Arfi sur "la protection des sources", détails inconnus

Sciences Po Paris : Master Class avec Amaëlle Guiton en 2013

Aucune école n'évoque directement des cours à propos de la sécurité numérique. Il n'est pas question de dire qu'aucune école de forme ses étudiants sur ce point précis, les plaquettes et sites internet sont trop liminaires pour déterminer cela. Mais en tout état de cause cet aspect n'est probablement pas assez vendeur pour de futurs apprentis journalistes.

Les étudiants en première année du CFJ, quant à eux, ont bénéficié pour la première fois en septembre dernier d'une formation de 4 jours organisée par l'association Nothing2Hide. L'EJDG devrait également recevoir une formation de deux jours. Cette association, créée au début de l'année 2017 a pour principale vocation de "*donner les moyens à ceux qui en ont les besoins de protéger leurs informations*". À l'origine de ce projet, Jean-Marc Bourguignon et Grégoire Pouget, "*technophiles et journalistes*", mais surtout deux anciens formateurs en sécurité numérique pour RSF. En plus des formations en France, ils ont animé de nombreuses formations à l'étranger à travers RSF et le CFI. À côté des deux fondateurs sont présents des journalistes, des avocats, des hacktivistes et des spécialistes de la sécurité numérique. Leur cycle de formation complet s'articule en 9 points, peut être suivi en quatre jours complets et part des principes de base de la sécurité pour aller jusqu'au chiffrement des mails et l'utilisation d'outils tels que Tails.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Les écoles ne communiquent pas forcément sur ces aspects dans leurs plaquettes de présentations mais proposent pourtant, pour la plupart, au moins une sensibilisation à ces enjeux concernant la sécurité numérique.

Voici un tableau récapitulatif :

ESJ	CFJ	IFP	IPJ	CELSA	CUEJ	EJT
Oui	Oui	Oui	Sensibilisation	Oui	N/C	N/C

EDC	EJDG	EJCAM	EJT	IJBA	Lannion	Sciences Po Paris
Sensibilisation	Oui	Sensibilisation	Sensibilisation	N/C	Oui	Oui

ESJ : Réponse de Mme Menegaux, responsable de la formation numérique à l'ESJ Lille : "*Les étudiants de 2e année de Master passent 2 jours avec Jean-Marc Manach sur le volet sécurité des communications. Ils apprennent essentiellement à gérer les boîtes mails de manière sécurisée et à utiliser Signal et Tor. Nous envisageons de renforcer cet enseignement car il paraît de plus en plus essentiel.*"

CFJ : Formation de 4 jours avec l'association NothingToHide

IFP : Réponse de M. Lagavre, directeur de l'IFP : "*Depuis deux ans, il y a une ou deux interventions, environ 4h de cours spécifiques dans le cadre des enseignements numériques. De plus, dans le cadre d'un séminaire sur les journalistes et leurs sources où des journalistes d'investigation sont invités, ils abordent à chaque fois la question de la protection numérique de leurs sources. L'année dernière, 3 intervenants pendant cette semaine ont par exemple donné leurs "trucs" concernant la sécurité numérique. Mais là, ce n'était pas un cours à proprement parler.*"

IPJ : Réponse de M. Guénée, directeur de l'IFP : "*La sécurité numérique (mais également la sécurité physique sur le terrain) sont en effet des sujets que nous traitons dans nos enseignements. Notre approche est plus globale que de seuls enseignements théoriques. Nous prévoyons donc de modifier prochainement l'ensemble des échanges digitaux avec nos étudiants. Pour ce faire, il faut une collaboration active de la DSI de l'université. Par ailleurs, nous formons actuellement certains de nos enseignants à la*

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

cyber-sécurité et à la prévention de la cybercriminalité envers les journalistes. Ceci devrait être pleinement opérationnel lors de notre prochain contrat quadriennal avec l'Etat."

CELSA : Réponse de Mme Jeanne-Perrier, directrice pédagogique du CELSA : "*Atelier prévu autour du livre "la face cachée de l'internet" avec une double approche théorique et pratique en présence de l'auteure"*

EDC : Réponse de M. Araszkiewiez, directeur de l'école : "*à l'occasion des cours généraux sur Internet ou le Web on a discuté des protocoles d'échanges sécurisés, de la confidentialité des données stockées sur le Web, mais pas de cours spécialisé. Reste à avoir quelque chose de sérieux à dire au delà des évidences.*

- Je demande aux étudiants de me faire un exposé sur ces questions de cybersécurité dans le cours de culture numérique. En gros, après une présentation générale des problématiques et enjeux de la cybersécurité pour tout un chacun, ils doivent se demander pour quelles raisons et dans quelles situations en particulier un journaliste doit sécuriser ses données et ses communications ? Avec quels outils (description de leur fonctionnement) ? Quelles habitudes de travail ?

Ca ne s'est fait qu'une fois l'an passé, et ça n'a concerné qu'un groupe de 4 élèves, hormis lors de la présentation de l'exposé à la promo (20 min) où tous les actuels J2 étaient présents.

Ça fait peu… On peut donc évoquer une première sensibilisation sans enseignement structuré."

EJDG : Formation de 2 jours avec l'association NothingToHide

EJCAM : Réponse de M. Joux, directeur de l'EJCAM : "*Pas de cours spécifiques sur ce sujet avec des pro, même si sensibilisation dans les cours magistraux à ces enjeux"*

EJT : Réponse de M. Ginabat, coordinateur pédagogique de l'EJT : "*Il n'y a pas de cours spécifique sur la sécurité numérique. En effet, le sujet est tellement vaste et l'évolution dans ce domaine est telle qu'il faudrait une année complète pour être efficace et recommencer dès l'année suivante pour être à jour… Notre mission n'est pas de former des spécialistes en cyber criminalité, mais des journalistes. La totalité de nos cours est consacrée à ce but.*

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

En revanche, ce sujet n'est bien évidemment pas négligé et une sensibilisation à ce phénomène est effectuée par l'équipe d'encadrement avec des rappels réguliers dans le cadre de différents séminaires que nous organisons. De même, lorsqu'ils intègrent une entreprise lors d'un stage ou d'une embauche, nos étudiants s'informent des procédures existantes en termes de sécurité, chaque média ayant ses spécificités quant à la manière d'aborder ce problème."

IJBA : Non spécifié

Lannion : Réponse de Mme Montanola, responsable du DUT : "*nous avons depuis 3 ans des modules sur la sécurité numérique, le cryptage de données. L'un plutôt technique avec un binôme journaliste / informaticien, l'autre lié à un module sur le reportage, réalisé par un journaliste reporter de guerre, sur la protection des sources, les échanges etc."*

Sciences Po Paris : *"Cet enseignement est en effet prévu et intégré à nos ateliers, notamment sur les cours de Veiller, chercher, vérifier dès le M1, et ensuite, en M2, lors de l'atelier contenus et code, ainsi que lors de master class spécifiques."*

Multiplication des "kits de protection"

Autre corollaire aux révélations de Snowden et à la prise de conscience de la surveillance est la multiplication des "kits de protection numérique". Ces guides, destinés à l'autoformation des personnes qui le souhaitent sont aujourd'hui très nombreux. Au cours de mes recherches, j'en ai dénombré plus d'une vingtaine.

Leur qualité peut être variable et surtout d'anciens kits existent toujours (comme le premier de RSF, qui date de 2012). Le danger principal de ces kits réside dans leur ancienneté : lorsqu'ils sont trop vieux, ils peuvent faire appel à des technologies qui ne sont plus efficaces aujourd'hui.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

B - Des journalistes protégés

Il n'existe à ce jour aucune étude évaluant le nombre de journalistes français utilisant des outils de protection numérique. Afin d'alimenter ce mémoire et d'essayer d'avoir un aperçu de leur nombre, j'ai donc publié un questionnaire sur la plateforme libre Framasoft et je l'ai partagé, notamment via mon compte Twitter de veille et les groupes Facebook de journalistes. En plus de ne pas utiliser l'outil de questionnaire Google dans une perspective de "protection de mes sources", j'ai décidé de rendre ce questionnaire anonyme pour que les journalistes ne craignent pas de répondre honnêtement.

Ce questionnaire comporte plusieurs biais, que je vais détailler avant de passer aux résultats. Étant un questionnaire anonyme, je n'ai aucun moyen de vérifier que toutes les personnes ayant répondu sont véritablement des journalistes. Puisqu'il a été partagé en premier lieu sur mon compte de veille Twitter, et qu'il a été retweeté une vingtaine de fois, particulièrement par des comptes sensibilisés aux questions de sécurité numérique, les résultats ne reflètent pas forcément la réalité.

Enfin, 113 journalistes ont répondu : sur les 36 000 journalistes détenteurs de la carte de presse, ce n'est qu'un échantillon très minime. Il est donc nécessaire d'aborder les résultats que je vais présenter de manière très prudente.

Profil type

À partir des 113 réponses, il est possible d'établir un profil type de la personne qui a répondu à mon questionnaire : un.e journaliste entre 20 et 30 ans travaillant en presse écrite ou dans une rédaction web, plutôt rédacteur.trice, travaillant en tant que pigiste et uniquement en France. Il/elle pense que la sécurité numérique est un enjeu utile ou vital pour se protéger, mais surtout pour protéger ses sources.

Le/la journaliste a été sensibilisé.e à ces sujets à travers des lectures persos et formée tout.e seul.e, tandis que le média pour lequel il/elle travaille ne lui a jamais donné de consignes relatives à cette problématique.

La stratégie la plus utilisée est la messagerie instantanée sécurisée, suivie par les VPN et l'authentification double facteur. L'application de messagerie la plus utilisée est WhatsApp, largement devant Signal.

La protection numérique : inutile pour certains

Parmi les 113 journalistes ayant répondu à la question "Selon vous, quel est l'intérêt de se protéger numériquement dans le cadre de votre travail ?", seuls 20 ont déclaré que se

protéger numériquement était "*inutile*" : cela ne représente que 17,5% du total, ce qui est assez peu. Ce chiffre est largement à relativiser compte tenu des biais évoqués au début de cette partie et il est donc nécessaire de s'intéresser à leurs réponses. Les précisions apportées sont, les mêmes à quelques variantes : "*je ne travaille pas sur des sujets sensibles donc je n'ai pas besoin de me protéger ou de protéger mes sources".* Cette affirmation est en totale contradiction avec l'article 7 de la Charte de Munich, comme nous l'avons vu en fin de première partie, mais totalement compréhensible. Parmi les 21 des journalistes qui ont jugé que c'était "plutôt utile", plusieurs ont mentionnés eux aussi n'utiliser que ces services lorsqu'ils travaillaient sur des sujets sensibles. Pour les personnes répondant qu'il n'y avait aucun intérêt à se protéger, l'enquête s'arrêtait là.

Parmi les journalistes qui jugent la sécurité numérique "plutôt utile", "utile" ou "vitale" (respectivement 21, 36 et 38 personnes, soit environ 83% des répondants), ils sont 90% à penser que protéger ses sources est le principal intérêt. Ces réponses sont bien entendu à mettre en relation avec les biais évoqués : en réalité, le score serait sans doute très différent.

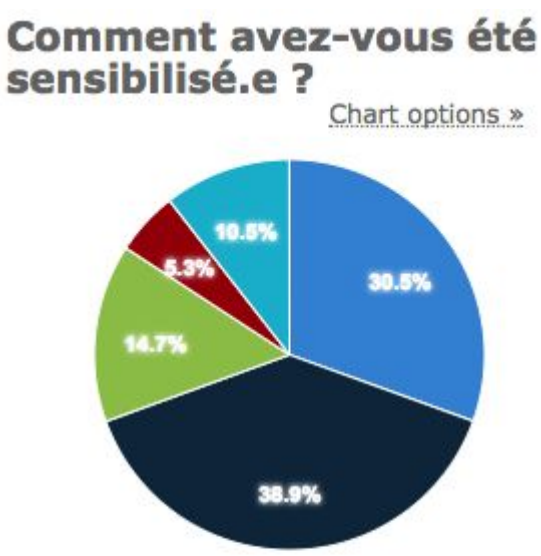
Une catégorie de personnes est intéressante à analyser : les encadrants. Il semblerait qu'ils soient assez peu sensibilisés à cette problématique. Sur les 15 répondants dont le poste est soit rédacteur en chef, soit chef de rubrique ou chef d'édition, 5 jugent que protéger ses sources est inutile dans le cadre de leur travail tandis que les 10 autres pensent au contraire que c'est vital ou au moins utile. Le biais de cette question provient peut-être du fait qu'ils considèrent uniquement leur travail, plutôt que leur travail ainsi que celui des journalistes sous leurs ordres.

Sensibilisation et formation

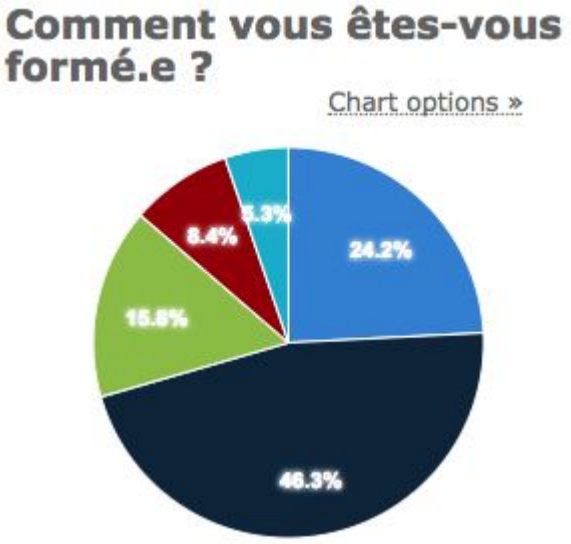
Les répondants au questionnaire sont assez jeunes (70% des répondants ont entre 21 et 30 ans), mais seulement 30% des journalistes jugeant que la sécurité était "plutôt utile", "utile" ou "vitale" ont été sensibilisés à cette question lors de leur formation en journalisme. En outre, à peine 24% ont reçu des enseignements lors de cette formation. Malgré la proportion assez faible, cela semble infirmer les résultats du tableau comparatif des écoles sus-cité et probablement valider la thèse que les écoles ne communiquent pas du tout sur cet aspect.

Alors si à peine un quart des journalistes ont été sensibilisés/formés dans leur école de journalisme, comment ont-ils fait ? 38% ont été sensibilisés à travers leurs lectures

personnelles et 15% lors de conférences ou des ateliers. Question formation, ils sont 46% à répondre qu'ils se sont formés seuls.



Lors de ma formation en journalisme	29
Lectures perso	37
Conférences/Ateliers	14
Amis	5
Autre	10



Lors de ma formation en journalisme	23
Autoformation	44
Conférences/Ateliers (CryptoParty ou autres)	15
Amis	8
Autre	5

Statistiques portant sur les journalistes jugeant "plutôt utile", "utile" ou "vitale" la sécurité numérique

Autre donnée très intéressante, 90% des journalistes sensibilisés n'ont jamais reçu de consigne par rapport à la sécurité et/ou à la protection numérique des sources.

Stratégies utilisées

L'outil de protection le plus répandu, parmi les répondants, est la messagerie instantanée chiffrée, avec 55 personnes, suivi de près par les VPN (40 personnes) et l'authentification double facteur (35 personnes). Ici, la facilité d'utilisation semble prévaloir : plus de la moitié utilisent des messageries comme Telegram, Signal ou WhatsApp qui ne nécessitent a priori aucune

connaissance particulière (ce qui est faux, nous le verrons dans la partie suivante). Lorsque le processus devient plus complexe, comme l'envoi de mails chiffrés via les protocoles PGP/GPG, leur nombre tombe à 22.

En analysant ces résultats, nous pourrions conclure que les journalistes ne sont pas forcément techniciens : lorsque des solutions faciles se présentent à eux, elles semblent facilement adoptées. Ce qui n'est pas le cas des processus plus lourds et complexes, comme PGP/GPG.

En outre, il est intéressant de constater que moins de la moitié utilisent l'authentification double facteur, essentiel pour protéger ses comptes de messageries et réseaux sociaux d'un hack, comme nous le verrons cela dans la partie suivante.

Journalistes travaillant dans des pays étrangers jugés sensibles

Parmi les répondants,12 journalistes disaient travailler régulièrement à l'étranger, et plus particulièrement dans "*des environnements jugés sensibles et/ou dangereux"*. Pour 5 d'entre eux, les protections numériques étaient jugées "*vitales"*, 4 les jugeaient "*utiles*", 2 "*plutôt utiles*" et enfin, assez étonnamment au premier abord, l'un d'entre eux disait n'en pas voir l'intérêt. Ce ou cette dernière journaliste a précisé sa réponse : "*Cela attire l'attention (leurs utilisateurs sont les premiers surveillés)*". En effet, dans certains pays sensibles comme l'Iran, l'envoi de mails chiffrés est surveillé. Puisque chiffré, le gouvernement ne connaît pas le contenu des messages… mais il peut vous surveiller de plus près puisque vous semblez vouloir cacher des choses.

Parmi ces journalistes, seul un a reçu des consignes de la part du média pour lequel il travaillait concernant sa sécurité numérique. Et, d'après sa réponse, les consignes n'étaient pas très développées puisqu'il s'agissait uniquement "*d'utiliser des pseudo pour certains collègues".*

Un questionnaire un peu trop parfait

Comme précisé en introduction, les résultats sont très probablement biaisés, mais en tout cas laissent percevoir des tendances très intéressantes parmi les 95 personnes voyant un intérêt à sécuriser ses données. La majorité d'entre eux se sont formés eux-mêmes et l'outil le plus utilisé sont les applications de messagerie chiffrées : la simplicité d'utilisation est un atout de taille pour une profession comme la nôtre qui n'est pas forcément très portée sur la technique pure. La chose étonnante reste que la majorité des personnes disant utiliser

ce type d’outil se sert de WhatsApp qui est loin d’être l’application la plus sécurisée qui soit, comme nous le verrons dans la sous-partie suivante.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

2 - UN “MINIMUM STANDARD” ?

La sécurité informatique n’est pas une science exacte : il est clairement impossible d’être protégé à 100% dans un monde où chaque mois égrène son lot de nouvelles failles, de nouvelles technologies, de nouvelles révélations programmes de surveillance et de projets de loi sécuritaires. Comme nous l’avons vu, il est pourtant essentiel de protéger nos communications et nos données, ne serait-ce que pour protéger les personnes qui nous font confiance.

Cependant, comme le note Martin Sheldon, un chercheur en journalisme et en sécurité, “*Les technologies ne meurent pas, mais elles vieillissent très très vite. Même le plus riche des sites internet consacré à la sécurité devient rapidement obsolète, et bien qu’il y ait de nombreux “kits de sécurité” pour apprendre à se protéger numériquement, très peu d’entre eux comportent des informations que vous pouvez utiliser aujourd’hui.”* Outre le sentiment qu’il n’est pas forcément vital de se protéger, cette rapide obsolescence peut achever de miner les journalistes motivés à se protéger.

Aussi, ce que je propose dans cette partie n’est qu’une tentative basique et incomplète de fournir quelques clés essentielles de sécurité.

A - Le “modèle de menace”, base de la sécurité en terrain hostile

Pourquoi, avant toute chose, il est important de l’établir

Chacun est différent : ce truisme est aussi vrai pour nos stratégies de protection numérique. Un journaliste d’investigation français travaillant sur des affaires de corruption ne sera pas confronté aux mêmes problématiques qu’un journaliste d’investigation américain conversant avec un lanceur d’alerte, qu’un correspondant camerounais enquêtant dans sa région sur Boko Haram, ou bien qu’un fait-diversier québécois ou encore un reporter de guerre. Ces exemples, issus de la partie précédente, peuvent se démultiplier à l’infini et même dans des cas “plus banals”.

Ainsi, le journaliste de PQR doit aussi être capable de protéger ses contacts : qui sait si les noms, adresses ou numéros de téléphone des opposants à l’installation des compteurs Linky peuvent intéresser ses rédacteurs en chef, en lien avec les politiciens locaux ? Ce rédacteur en chef n’a pas les mêmes moyens que la NSA, bien sûr, mais rien ne l’empêche d’aller jeter un œil sur l’ordinateur de bureau de son collègue. Et qui sait s’il n’est pas surveillé, le fixeur birman de cette enquêtrice travaillant dans une société de

production parisienne pour une émission d'évasion ? Dans des états dictatoriaux, il n'est pas rare que les fixeurs fassent des recherches et donnent des informations aux dépens de leur sécurité. Alors, autant connaître les bonnes pratiques et les lui imposer pour sa propre sécurité.

Tous les journalistes ne font pas face aux mêmes menaces. Il est absurde de vouloir se protéger comme Laura Poitras lorsqu'elle travaillait avec Edward Snowden si l'on travaille sur des affaires de corruption à une échelle régionale : plus les procédures sont lourdes, plus elles sont difficiles à respecter, et moins vous les respecterez au fur et à mesure du temps si vous n'en avez pas réellement l'utilité. C'est pour cela que se protéger correctement sans trop en faire est la base de la sécurité : Il est essentiel de bien comprendre ce qui nous menace, comment et comment se protéger : c'est le "modèle de menace" à établir. Une fois le modèle établi, reste à s'y tenir et à l'adapter au fil du temps.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Quoi qu'il en soit, la première et parfois la seule raison de se protéger, partagée par tous les journalistes sans exception, est la suivante : l'assurance que les personnes avec qui nous parlons — nos "sources" — ainsi que toutes nos interactions avec elles sont protégées, comme le requiert l'article 7 de la Charte de Munich.

Établir son propre modèle de menace

Plusieurs sites proposent peuvent aider à établir son propre modèle de menace. Le site le plus simple d'utilisation, le plus complet et ergonomique est sans doute celui conçu par l'*Electronic Frontier Fondation* (EFF), une ONG de "*défense de la liberté d'expression dans le monde numérique*" créée en 1990. Cette page est disponible en français, mais la traduction parfois bancale peut faire préférer la version anglaise.

Sur son site, l'EFF conseille de répondre à cinq questions afin d'établir son propre modèle de menace. Pour les besoins de ce mémoire, je vais donc établir mon propre modèle en prenant comme exemple mon travail de journaliste dans une agence de presse audiovisuelle où je suis régulièrement en contact avec des députés français de tous bords politiques. Tout ce qui est de ma vie personnelle ou de ma vie privée n'est pas l'objet de ce modèle de menace.

- ***Qu'est-ce que je veux protéger ?***

  Les numéros de téléphone personnels des députés et de leurs collaborateurs, le contenu de nos conversations (SMS/email/appels) parfois en rapport avec leurs intérêts, leurs habitudes ou bien encore sur des commissions en cours ainsi que nos heures et lieux de rendez-vous.

Mes historiques de navigation, pour ne pas révéler mes enquêtes en cours

En terme matériel, cela signifie protéger : mon ordinateur de bureau, mon ordinateur portable et mon smartphone.

D'un point de vue logiciel : mes outils en ligne tels que Drive, ma boîte mail professionnelle et personnelle, mes SMS.

- ***Contre qui je veux protéger tout ça ?***

Conseil de l'EFF : Il est important d'identifier qui pourrait vous cibler ou cibler vos informations.

Mes supérieurs et collègues

Le gouvernement

D'autres gouvernements

Des groupes terroristes

- ***Quelles seraient les conséquences si j'échouais à le protéger ?***

Conseil de l'EFF : Vos adversaires ont de nombreux moyens de menacer vos données. Les motivations de vos adversaires sont très différentes, comme leurs attaques. Il est nécessaire de comprendre à quel point les conséquences pourraient être mauvaises si un adversaire parvient à attaquer l'une des choses que vous protégez. Afin de déterminer cela, vous devez considérer les capacités de votre adversaire. Par exemple, votre opérateur téléphonique peut accéder à vos factures détaillées. Un hacker peut accéder à vos données non chiffrées si vous vous connectez sur un réseau WIFI ouvert. Votre gouvernement peut-être plus puissant

Ni mes supérieurs ni mes collègues n'ont à connaître le contenu des conversations que j'ai avec les députés ou leurs numéros de téléphone sans leur consentement. De plus, ils pourraient envoyer des mails depuis mon ordinateur de bureau en se faisant passer pour moi ;

Le gouvernement peut être curieux de connaître certains de nos échanges afin de vérifier qu'aucune information compromettante ne filtre de la part des députés ;

Concernant la menace terroriste (état d'urgence permanent oblige) : certaines de ces informations, notamment nos rendez-vous, pourraient intéresser de potentiels groupes terroristes afin de planifier des attentats contre des députés. Tout ce qu'ils auraient à faire, c'est de compromettre un réseau WIFI public pour infiltrer mon téléphone ou bien tout simplement le voler ;

- ***Quelle est la probabilité que j'aie besoin de le protéger ?***

Conseil de l'EFF : Il est important de distinguer la menace du risque. Une menace est une catastrophe qui peut arriver tandis qu'un risque est la probabilité que cela arrive. Faire une analyse de risque est à la fois personnel et subjectif ; tout le monde n'a pas les mêmes priorités ni ne voit les menaces de la même façon. De nombreuses personnes trouvent certaines menaces inacceptables, peu importe le risque, parce que la simple présence de cette menace peut changer trop de choses.

J'ai toutes les raisons de croire que je devrais protéger les coordonnées des députés de mes supérieurs et collègues, ainsi que le contenu de nos conversations : je n'ai pas du tout envie d'être espionné ;

Étant en contact direct avec l'opposition, il y a des chances que le gouvernement souhaite connaître l'objet de nos conversations, mais elles sont faibles si on l'en croit la loi française ;

Concernant le risque terroriste, c'est là aussi faible, mais je sais que leurs compétences informatiques sont très élevées et ça vaut quand même le coup de tout faire pour protéger des élus.

- ***Quels désagréments suis-je disposé à affronter afin de m'en prémunir ?***

Conseil de l'EFF : Pour répondre à cette question, vous devez conduire une analyse de risques. Tout le monde n'a pas les mêmes priorités ou n'envisage les menaces de la même manière. Écrivez les possibilités que vous avez pour atténuer une à une ces menaces.

Mettre des mots de passe forts sur tous mes appareils et services en ligne

Chiffrer mes appareils (ordinateur, smartphone) et transporter des données sur une clé chiffrée

Naviguer de manière sécurisée

Communiquer de manière chiffrée avec les députés

Conclusion

Établir le "modèle de menace" est aussi ce qui rend aussi difficile l'appréhension et la diffusion d'une culture de la sécurité numérique parmi les journalistes. C'est un processus long et fastidieux qui peut conduire à une certaine forme de paranoïa vue d'un regard extérieur : ici, j'imagine que des terroristes pourraient en vouloir à mes données. En réalité,

c'est vraiment très peu probable et j'en suis parfaitement conscient. Mais d'après ses réactions, Patrick Lagacé était persuadé de ne pas être surveillé.

Là où cela devient vraiment compliqué, c'est qu'un même journaliste peut avoir plusieurs modèles de menace. Jean-Marc Manach l'expliquait lors de notre entretien : "*quand je travaille avec Wikileaks sur des documents très sensibles, je n'utilise pas les mêmes outils que lorsque je travaille sur l'évolution de la "loi renseignement" en France, par exemple."* En effet, certaines procédures peuvent être très lourdes et peu utiles dans certains cas. Comme dit dans l'introduction de cette partie, plus les procédures sont lourdes et moins on sera motivés à les respecter si ce n'est pas justifié, d'où l'importance d'avoir plusieurs modèles de menace.

B - Se protéger et protéger ses sources — Tentative de définition d'un minimum

Protéger ses sources est le travail essentiel d'un journaliste, nous l'avons vu. Aussi, lorsque nous cherchons à protéger nos sources, il est indispensable de se protéger soi-même : les deux vont forcément de pair.

Les puristes diront sans doute qu'il n'existe pas de minimum standard en terme de protection. Jean-Marc Manach précisait également, lors de notre entretien, qu'il "*est inutile d'acheter une porte blindée si on laisse la fenêtre ouverte"* : en terme de protection, l'illusion de la sécurité est sans doute le pire qui puisse arriver, tout en sachant qu'il est impossible d'être sécurisé à 100%. La sécurité, et particulièrement la sécurité numérique, est un processus long et fastidieux, où il faut régulièrement se tenir à jour.

De nombreux "kits de sécurité" existent déjà. Mais pour les besoins de ce mémoire, je vais tout de même tenter de proposer une ébauche de minimum standard en fonction du modèle de menace que j'ai établi dans la partie précédente et classé par ordre d'importance.

Mise à jour, antivirus et pare-feu : pour une "hygiène numérique"

Nos appareils électroniques sont très sensibles et très complexes. Il est nécessaire, selon les mots de Jean-Marc Manach, d'entretenir une bonne "*hygiène numérique*". Comprenez : mettre ses appareils à jour et les protéger contre les infections potentielles à l'aide d'un antivirus et d'un pare-feu.

En effet, contrairement à ce que l'on pourrait croire, il est essentiel de mettre à jour les différents appareils que nous possédons : très régulièrement, ces mises à jour corrigent des failles de sécurité qui peuvent rendre les appareils très vulnérables à des attaques. Très

récemment, lors de la découverte de la faille du réseau WIFI nommée KRACK, des mises à jour ont ainsi été proposées afin de combler ce défaut de sécurité.

L'antivirus, de son côté, permettra de détecter les fichiers infectés par des malwares ou autres présents sur vos appareils et les supprimera. De très nombreux antivirus existent et de nombreux comparatifs aussi. Et, contrairement à une légende largement répandue, les ordinateurs Mac aussi ont besoin d'antivirus : entre janvier et juillet 2017 seulement, il y aurait eu une augmentation de 230% des malwares sur Mac, d'après une étude de Malwarebytes. De son côté, le pare-feu sera comme un écran de protection entre votre ordinateur et internet, vous permettant de vous protéger d'éventuelles attaques ; il est à noter qu'il existe un pare-feu intégré aux systèmes d'exploitation iOS, mieux vaut l'activer.

Lors de ma rencontre avec Grégoire Pouget, cofondateur de Nothing2Hide, il insistait sur la nécessité de n'utiliser que des logiciels non crackés. En effet, les logiciels crackés peuvent abriter des malwares, mais ne peuvent en outre généralement pas être mis à jour : des failles de sécurité peuvent apparaître et compromettre vos données.

Une phrase de passe, et non un mot de passe

Pourquoi est-il nécessaire d'avoir de bons mots de passe ? Vos mails, comptes de réseaux sociaux, codes de banques… Toute notre vie numérique en dépend. Si vous ne le faites pas pour votre vie privée, faites-le pour respecter vos sources qui communiquent avec vous (cf. les rhinocéros de Laurent Chemla).

La base de la sécurité informatique repose dans les mots de passe. Régulièrement, les bases de données de grandes entreprises se font attaquer et les mots de passe sont volés et/ou diffusés sur internet. En 2016, au moins 10 millions de mots de passe ont été révélés, selon Keeper Security, une société de sécurité informatique. Ces fuites leur ont permis d'étudier quels étaient les mots de passe les plus fréquemment utilisés : avec 17% des occurrences, le mot de passe "123456" est le plus utilisé depuis plusieurs années, suivi de près par "123456789"... Il est intéressant de rajouter que les 25 mots de passe les plus fréquents constituent plus de 50% des occurrences totales. De nombreux outils permettent aujourd'hui de "cracker" les mots de passe en quelques secondes, en utilisant notamment ces mêmes bases de données ainsi que les nombreuses ressources (dictionnaires, lives, paroles de chanson disponible sur internet, etc.). Aucun mot de passe n'est inviolable, mais plus complexe il sera, plus il sera difficile à trouver, quel que soit le type d'attaque.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

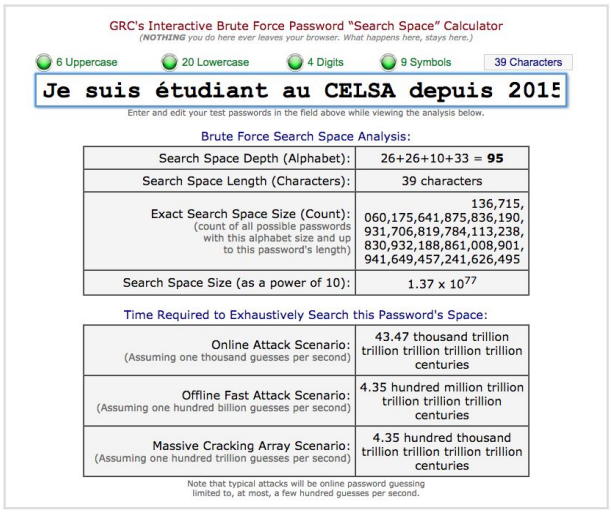
Sans le savoir, nous faisons tous des erreurs en créant nos mots de passe. D'après [un tutoriel de la Rory Peck Trust], voici les principales : utiliser le même mot de passe pour plusieurs comptes, utiliser des mots de passe courts, utiliser des mots communs que nous trouvons dans le dictionnaire ou des références à la pop culture, utiliser un nom ou quelque chose de significatif pour nous et enfin utiliser des substitutions classiques comme remplacer la lettre "o" par un zéro.

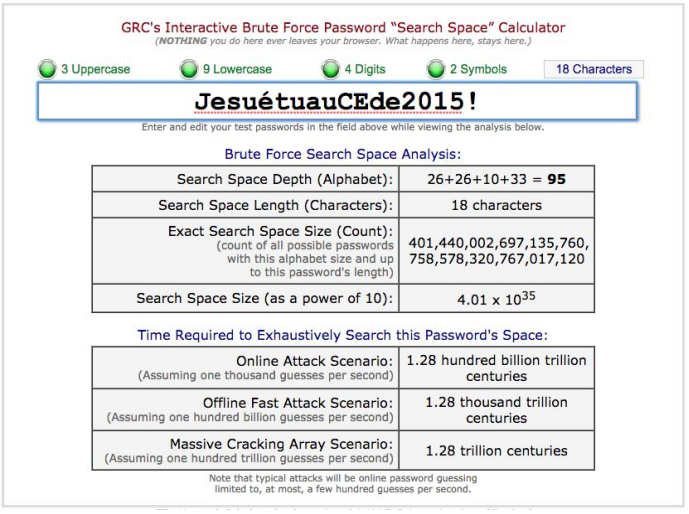
Alors, comment faire ?

Plusieurs méthodes existent (voir le site de la Rory Peck Trust sus-citée), mais une méthode simple évitera sera suffisante pour la majeure partie des cas : plutôt qu'un mot de passe, utiliser une *phrase de passe*. En effet, plus les mots de passe sont longs et comprennent de caractères spéciaux, plus mettront du temps à les trouver. Mais utiliser des mots de passe complexes avec des caractères spéciaux et/ou des suites de lettres sans sens n'est pas évident : le risque de les oublier est grand.

Aussi la solution la plus simple et la plus efficace aujourd'hui serait d'utiliser des phrases de passe avec des espaces, des majuscules, par exemple : "Je suis étudiant au CELSA depuis 2015 !". La solution consistant à ne prendre que les premières lettres de cette phrase pour faire un mot de passe n'est pas forcément la meilleure : il est plus difficile de s'en rappeler et l'un des critères essentiels dans la sécurité des mots de passe est la longueur.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media





Temps que mettrait un attaquant à casser un mot de passe par la méthode dite "brute force", en faisant plusieurs milliers ou centaines de milliards d'essais consécutifs à la seconde https://www.grc.com/haystack.htm

La question des mots ou phrases de passe divise les chercheurs. Pour Micah Lee, journaliste à *The Intercept*, ainsi que de nombreux autres, la meilleure des méthodes reste celle du *Diceware* qui existe aussi en français : à partir d'une liste de mots préétablis et d'un ou plusieurs dés, on peut créer une phrase de passe complètement par hasard. L'entropie générée par le lancement des dés rend mathématiquement le mot de passe encore plus compliqué.

Quoi qu'il en soit, il faut préciser une nouvelle fois qu'il faut utiliser un mot de passe par service. Dans le cas contraire, si quelqu'un trouve votre mot de passe, toutes les portes de votre vie privée lui seront ouvertes.

Voir différentes méthodes sur le site de la Rory Peck Trust :
https://rorypecktrust.org/resources/digital-security/the-basics/passwords

La meilleure solution reste d'utiliser un gestionnaire de mots de passe comme KeePass ou pwSafe (tous les deux gratuits et open source). Ceux-ci permettent à l'utilisateur de générer et d'enregistrer pour chaque service un mot de passe très complexe. Cet ensemble de mots de passe est chiffré et protégé par une phrase ou un mot de passe "maître", le seul que vous devez connaître.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Authentification double facteur (2FA)

L'authentification double facteur, désormais possible sur de nombreux services en ligne, peut être considérée comme une deuxième ligne de défense derrière ~~le mot~~ la phrase de passe. Par exemple, si l'authentification double facteur (2FA) est activée sur votre compte Gmail : vous rentrez votre ~~mot~~ phrase de passe, puis peuvent se présenter trois solutions, par ordre croissant de sécurité :

- Un SMS est envoyé sur votre smartphone : il contient un code que vous devez rentrer sur l'ordinateur pour valider votre connexion (pourquoi ce n'est pas vraiment sûr, d'après un article de Wired);

OU

- Ouvrir une application tierce comme Google Authentificator qui permet de générer un code aléatoire qui change toutes les minutes. Ce code doit être rentré dans l'application, comme les SMS ;

OU

- Utiliser une clé physique de sécurité qui se présente comme une clé USB, que vous connectez à votre ordinateur pour vous authentifier.

Chiffrer son ordinateur, son téléphone et ses supports externes sans le savoir

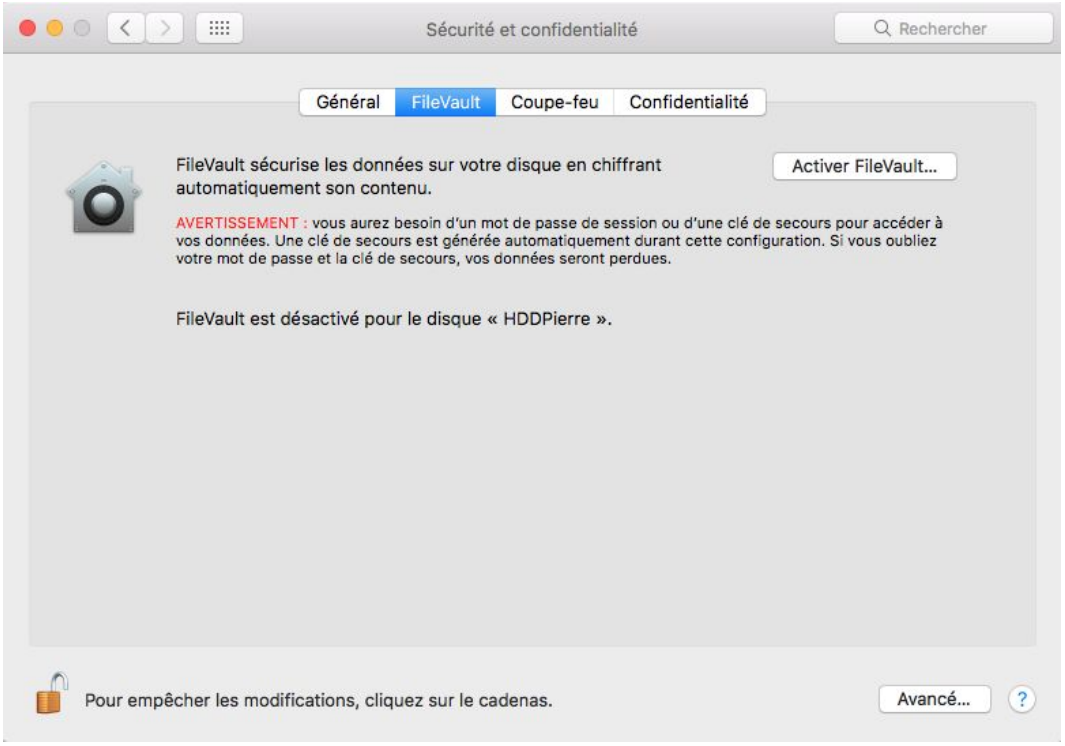
Qu'apporte le chiffrement des différents outils de travail ? Si quelqu'un accède à l'un des nombreux outils que les journalistes utilisent aujourd'hui (Smartphone, ordinateur, clé USB, disque dur externe…), il ne pourra pas lire les données tant qu'il n'aura pas "cracké" la phrase de passe. Cela aurait par exemple évité à la personne qui a retrouvé la clé USB contenant des documents relatifs à la sécurité de l'aéroport d'Heathrow de pouvoir la lire. Pourquoi le faire ? C'est extrêmement simple à réaliser et cela protège nos vies numériques ainsi que la vie des sources, si jamais quelqu'un rentrait en possession des appareils. Mais cela ne change rien si quelqu'un attaque l'ordinateur et y installe un malware ou si l'on est victime de phising : ce n'est utile que lors d'une saisie "physique" du matériel.

Sans que l'on ne le sache forcément, la plupart des appareils récents sont déjà chiffrés. En effet depuis la version 5.1 d'Android (Lollipop), tous les smartphones sont chiffrés par défaut. Et si la version d'Android du téléphone est plus ancienne, il est très facile de le faire, et très rapidement. Concernant les iPhone, c'est le même principe : tous les iPhone tournant sur iOS 8 et plus sont chiffrés par défaut. De plus, Apple affirme désormais qu'ils ne feront "*aucune extraction de données en réponse aux mandats gouvernementaux parce que les données à extraire sont protégées par une clé de chiffrement qui est lié à la phrase de passe de l'utilisateur qu'Apple ne possède pas"*.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Preuve de son efficacité (si cela est vrai), Christopher Way, le directeur du FBI a récemment avoué que le chiffrement était "*un gros gros problème*" pour eux. En effet, le FBI serait aujourd'hui incapable de récupérer les données de plus de 7000 smartphones saisis. Début 2016, l'agence étatsunienne avait par ailleurs demandé à Apple de casser la protection de l'iPhone de l'auteur de l'attentat de San Bernardino : l'entreprise avait refusé, mais le FBI avait finalement contourné les protections grâce à une entreprise tierce, à l'heure actuelle toujours inconnue. Le chiffrement n'est donc pas inviolable, mais demande beaucoup de moyens et de temps : si vous ne cachez pas de secrets d'état dans votre téléphone, peut de risque qu'on prenne le temps d'en casser le chiffrement.

Du côté des ordinateurs, la firme à la pomme s'est engagée sur le même chemin : lors de la première utilisation d'un ordinateur, Apple incite désormais ses utilisateurs à utiliser FileVault, leur solution de chiffrement. Si FileVault n'est pas encore actif, rien de plus simple, la manipulation ne prend que quelques minutes. Windows propose également sa propre solution de chiffrement maison, mais uniquement dans certaines versions de licence (Entreprise, Pro ou encore Ultimate. "Home" n'est pas supporté). Si ce n'est pas le cas, il est facile de chiffrer son disque à l'aide de plusieurs logiciels.



Mon disque dur n'est pas encore chiffré. C'est chose faite, simplement en cliquant sur "Activer FileVault" et en redémarrant l'ordinateur.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

VeraCrypt semble être une très bonne solution, tant pour les partitions Windows que pour les clés USB ou les disques durs externes. Ce logiciel est en effet open source, ce qui permet d'être certain qu'aucune backdoor ne s'y cache. Un tutoriel très clair de NextInpact explique la procédure en détail. Sur les ordinateurs suffisamment récents, il n'y a pas de perte de vitesse notable : il n'y a rien à perdre à faire cette manipulation, et vraisemblablement tout à gagner.

Messagerie instantanée chiffrée

Cette partie se voulant être un "minimum vital" pour les journalistes, je n'y évoquerai pas le chiffrement des emails via le protocole PGP : je ne maîtrise pas suffisamment le sujet pour pouvoir l'expliquer, mais de nombreux tutos existent sur le sujet.

Ce qui reste extrêmement simple, en revanche, c'est l'utilisation des messageries instantanées chiffrées. L'intérêt ? Les messages envoyés via la connexion internet du smartphone ne transitent pas en clair : seules les deux personnes de la conversation (ou le groupe) peuvent les voir.

Encore une fois sans le savoir, de nombreuses personnes utilisent chaque jour l'une de ces messageries : WhatsApp, la messagerie qui compte plus d'un milliard d'utilisateurs quotidiens, est chiffrée de bout de en bout. Facebook Messenger le permet également, si vous l'activez. De plus, depuis l'émergence de Daech, nous avons beaucoup entendu parler de Telegram, la "*messagerie préférée des djihadistes"* qu'aujourd'hui de nombreux politiques français utilisent (voir d'ailleurs à ce sujet le décryptage de la bulle médiatique autour de cette app sur le site de Reflets.info) malgré ses gros défauts.

Au moins une dizaine d'autres applications de messagerie chiffrée pour téléphone existent, aujourd'hui. Mais mis à part le chiffrement, toutes ne répondent pas aux mêmes critères, loin de là. Il arrive que le chiffrement ne soit pas activé par défaut (comme sur Telegram ou Messenger) ou encore que malgré le chiffrement, les entreprises aient déjà donné des informations à différents gouvernements (comme WhatsApp ou iMessage). Pour essayer d'y voir plus clair, la personne derrière le site Securemessaginapps.com a fait un énorme tableau récapitulatif comprenant 32 critères, classés par couleur en fonction de ce qui est "*safe"* ou non. Voici un extrait :

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

App name	Allo	iMessage	Messenger	Signal	Skype	Telegram	Threema	Viber	Whatsapp	Wickr	Wire
TL;DR: Does the app secure my messages and attachments?	No	No	No	Yes	No	No	Yes	No	No	No	Yes
Company jurisdiction	USA	USA	USA	USA	USA	USA / UK / Belize	Switzerland	Luxembourg / Japan	USA	USA	Switzerland
Infrastructure jurisdiction	USA, Belgium, Finland, Ireland,the Netherlands, Chile, Taiwan,and Singapore	USA (Ireland and Denmark planned); iMessage runs on AWS and Google Cloud	USA, Sweden (Ireland planned)	USA	USA, the Netherlands, Australia, Brazil, China, Ireland, Hong Kong, and Japan	UK, Singapore, USA, and Finland	Switzerland	USA	USA (unsure of other locations)	USA (unsure of other locations)	Germany / Ireland
Implicated in giving customers' data to intelligence agencies?	Yes	Yes	Yes	No	Yes	No	No	No	Yes	No	No
Surveillance capability built into the app?	No	No	No	No	Yes	No	No	No	No	No	No
Does the company provide a transparency report?	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Company's general stance on customers' privacy	Poor	Poor	Poor	Good	Poor	Good	Good	Poor	Poor	Good	Good
Funding	Google	Apple	Facebook	Freedom of the Press Foundation, the Knight Foundation, the Shuttleworth Foundation, and the Open Technology Fund	Microsoft	Pavel Durov	User pays	Rakuten, friends and family of Talmon Marco (it's very unclear)	Facebook	Gilman Louie, Juniper Networks, the Knight Foundation, Breyer Capital, CME Group, and Wargaming	Janus Friis, Iconical, Zeta Holdings Luxembourg
Company collects customers' data?	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	No
App collects customers' data?	Yes	Yes	Yes	Minimal	Yes	Yes	No	Yes	Yes	No	Minimal

À retrouver complet ici : https://www.securemessagingapps.com/

Il n'y a pas de classement des applications : chacun est censé tirer les leçons de ce tableau et d'agir en fonction de son propre modèle de menace (ou ses envies). Pour ma part, de toutes ces applications, je préfère utiliser Signal. Pourquoi ?

1. De manière complètement panurgienne, parce qu'Edward Snowden ne jure que par elle, ainsi que Laura Poitras ou encore Bruce Schneier;
2. Elle permet d'appeler en toute sécurité ;
3. Elle est open source ;
4. Le chiffrement "bout à bout" est activé par défaut, ainsi que le chiffrement des documents joint ;
5. Les métadonnées générées sont chiffrées et sont réputées minimales ;

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

6. C'est la *Freedom of The Press Foundation* et la *Knight Foundation* (notamment) qui la financent. Ce sont deux ONG engagées pour la liberté de la presse;
7. Il existe désormais un logiciel Signal qui permet d'utiliser cette messagerie sur un ordinateur;

En revanche, cette application est mal connue, peu utilisée. Sur les 500 contacts et quelques de mon téléphone, seuls une dizaine l'ont installée. Et comme on pouvait s'y attendre, elle n'est pas parfaite. Comme le souligne sur Medium @thegrugq, un chercheur en sécurité, Signal reste comme toutes les autres applications de messagerie chiffrée : "*le chiffrement ne permet que la confidentialité, pas l'anonymat".* Aucune technologie installée sur un smartphone n'est complètement "*safe"* pour ce chercheur qui écrit "*qu'utiliser un téléphone est un risque pour sa sécurité"*.

Bien que Signal dit ne pas stocker beaucoup de métadonnées (dernière date de connexion, les interlocuteurs et la longueur de l'appel), mais la seule assurance que Signal offre vis-à-vis du stockage des métadonnées est une déclaration. @thegrucq précise que *"en théorie, Open Whisper System [la société qui édite l'app] est entièrement capable de stocker votre carnet d'adresses et l'utiliser pour concevoir un graphe détaillé de vos relations sociales. Leurs serveurs reçoivent des carnets d'adresses en entier et peuvent le stocker, même s'ils disent qu'ils ne le font pas."*

En voyage — WiFi public, VPN obligatoire

Les journalistes qui voyagent beaucoup où ceux qui vivent dans des pays moins respectueux de la liberté de la presse ont tout intérêt à se protéger particulièrement. Les pays démocratiques ne sont pas forcément plus sûrs : comme nous l'avons vu dans la première partie, il est aujourd'hui connu que le BND allemand espionn(ait)e les journalistes étrangers depuis des années et les services français peuvent faire la même chose avec les journalistes étrangers. Laura Poitras, la réalisatrice du documentaire sur Edward Snowden, *Citizen Four*, était chaque fois retenue des heures par la douane lors de son entrée sur le sol des États-Unis, notamment pour fouiller et l'interroger : en six ans, elle a subi plus de 50 contrôles sans jamais savoir pourquoi.

D'après Glenn Greenwald et de nombreux autres activistes, les zones internationales où interviennent les douanes sont des "zones grises" où le droit ne s'applique pas vraiment. En effet, aux États-Unis et comme dans de nombreux pays, il est interdit sauf rares exceptions de saisir et fouiller les effets personnels d'un citoyen sans mandat. Mais

"*désormais, [le gouvernement] n'a qu'à attendre que vous partiez du pays et une fois que vous reviendrez, les douanes pourront fouiller et copier tous vos fichiers. Cela comprend vos emails, les sites que vous avez visités, les conversations en ligne que vous avez eues, les identités de ceux avec qui vous avez communiqué, vos contacts de votre téléphone, vos reçus de carte de crédit, les vidéos que vous avez tournées, les brouillons des articles que vous écrivez et tout ce que vous stockez sur vos appareils électroniques."*

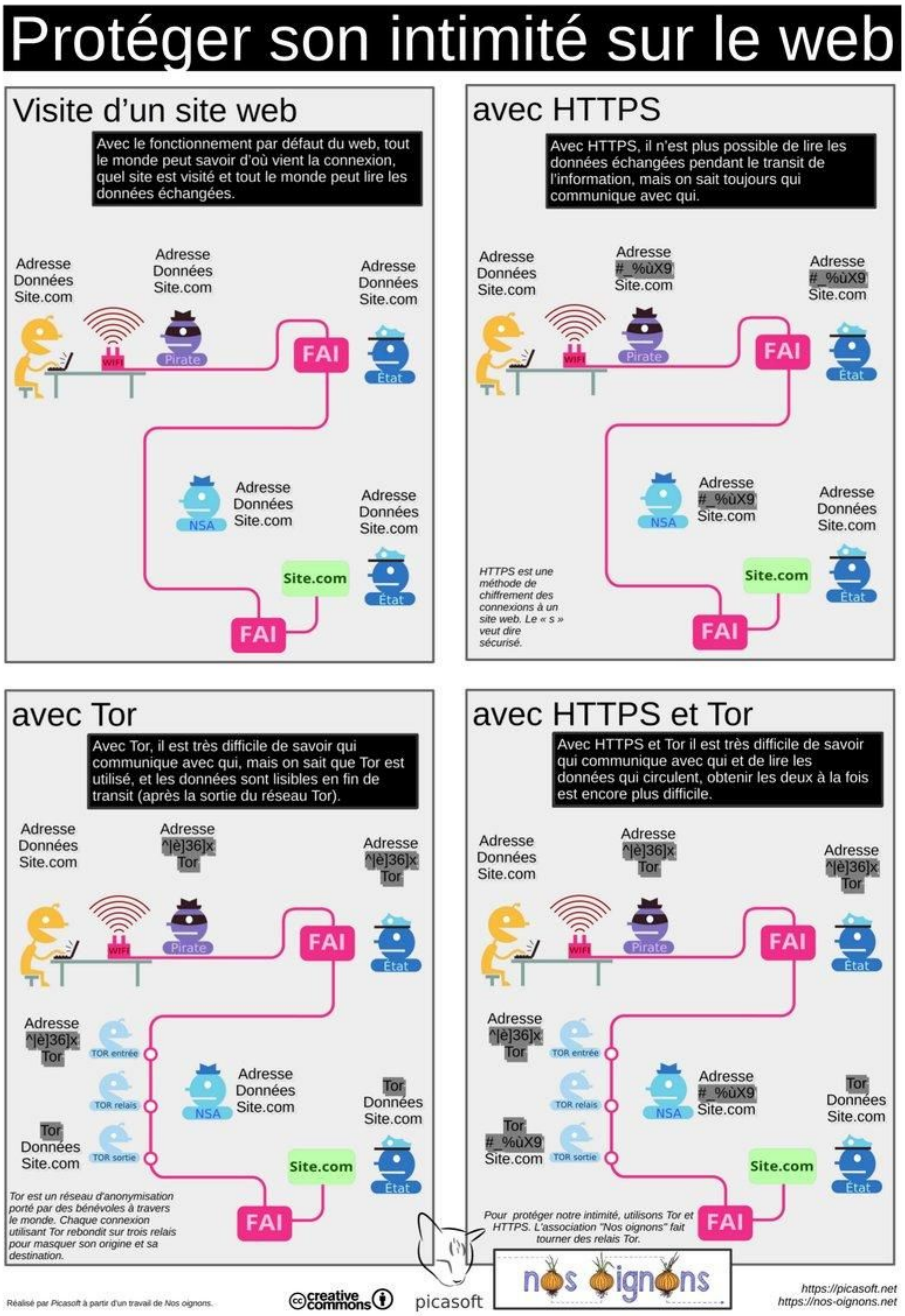
Cet exemple extrême est l'arbre qui cache la forêt : de nombreux pays ont ce genre de politiques vis-à-vis des journalistes, et mieux vaut y être préparé. Le magazine WIRED a écrit un long article à ce sujet. La majorité des conseils sont relativement extrêmes et surtout applicables pour les citoyens étatsuniens rentrant aux États-Unis, mais il y a de très bonnes idées pour les journalistes travaillant sur des sujets très sensibles.

Et une fois arrivé dans le pays en question, on n'a pas forcément de connexion internet sécurisée disponible et il n'est pas rare de se connecter sur des réseaux ouverts dans les bars, restaurants, hôtels, etc. Et cela peut être très dangereux : pour quelqu'un d'un peu aguerri, il est très facile de pénétrer votre ordinateur, d'y récupérer des données ou encore d'y installer des malwares lorsque vous êtes connecté à un réseau WIFI non protégé. En outre, dans certains pays, de nombreux sites sont bloqués par les autorités et cela peut être ennuyant pour les recherches liées au métier de journaliste. La solution s'écrit en trois lettres : VPN, pour *Virtual Private Network.*

Les VPN sont des logiciels qui, basiquement, font office d'écran de protection entre internet et votre ordinateur/smartphone. Ce service coûte quelques euros par mois, mais il reste essentiel dans de nombreux pays.

Il existe de très nombreux VPN aujourd'hui, et d'après le site arstechnica.com, *"il est impossible de créer une liste des meilleurs VPN".* Cet article répertorie en revanche quelques solutions, ainsi que cet article plus récent de *Motherboard*. Les VPN vont protéger toutes les activités en ligne (de la navigation au torrent), tandis que le navigateur Tor ne protégera "que" l'anonymat lors de la navigation. Voici un schéma explicatif du fonctionnement de Tor :

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media



Affiche réalisée par picasoft.net, partagée par @StphCrozat sur Twitter

Conclusion : pour ne pas se perdre, suivre les bonnes personnes, poser des questions et réfléchir

Pour éviter de se perdre dans les nombreux kits, sites et conseils, il est donc recommandé de suivre via les réseaux sociaux des personnes de confiance et reconnus par leurs pairs. Ceci pour se tenir au courant des évolutions des outils, de manière aussi

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

assidue que nos thèmes de travail. En effet, la sécurité reste un processus : les outils utilisés aujourd'hui seront peut-être compromis demain. Martin Sheldon, cité plusieurs fois, semble aujourd'hui être l'un des chercheurs en sécurité les plus actifs sur la plateforme Medium et il tient ses tutoriaux à jour.

Ces réflexes de sécurité sont une base : chaque journaliste, si ce n'est chaque citoyen, devrait les appliquer. En revanche, pour les affaires un tant soit peu sensibles, ce ne sera peut-être pas suffisant.

En outre, il faut rester conscient que l'utilisation de certains outils dans certains pays ne protège pas, bien au contraire. Certains outils comme PGP ou Tor laissent des traces sur le réseau : on ne sait pas ce que les utilisateurs de ces outils consultent ou envoient comme mail, mais les fournisseurs d'accès à internet savent que de tels services sont utilisés. Envoyer des mails via PGP dans un pays comme l'Iran, où personne ou presque ne l'utilise, peut être très dangereux : le gouvernement peut se dire qu'il est très étrange que vous utilisiez ce genre de technologie. Alors, pour communiquer, mieux vaut utiliser des mails "normaux" ou alors d'autres techniques comme, par exemple, le masquage de message dans vos photos, aussi appelé la stéganographie. Ce genre de pratiques, de choses à faire ou à ne pas faire est connu par les ONG comme Reporter Sans Frontière. Il ne faut donc pas hésiter à les consulter avant de partir afin d'éviter les impairs qui pourraient avoir de lourdes conséquences.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Conclusion de la deuxième partie

Cela fait quelques années que les journalistes commencent à prendre conscience des risques qui pèsent sur leur profession, notamment depuis les révélations de Snowden en 2013. Le nombre de personnes utilisant par exemple le protocole PGP ou GPG pour envoyer des emails est en augmentation, tandis que le nombre d'affichages de cette "compétence" sur Twitter est de plus en plus répandu (sans pour autant savoir si les journalistes qui l'affichent savent réellement s'en servir).

Quoi qu'il en soit, les formations en journalisme sont aujourd'hui encore assez mal dotées concernant les problématiques de sécurité numérique. Concernant le CELSA, seule école que je connaisse de l'intérieur, nous avons eu la chance d'avoir deux ou trois heures d'atelier (salutaire) sur cet aspect avec Amaelle Guiton. Évidemment, vu la complexité du processus de protection et des outils, c'est largement insuffisant pour se dire réellement protégés. Au moins, cela a pu éveiller les consciences.

L'étude réalisée pour ce mémoire a laissé voir des conclusions pour le moins surprenantes : la majorité des répondants étaient conscients de la nécessité de se protéger. Bien que le résultat total soit sans doute biaisé, il est tout de même intéressant de noter que les journalistes prennent volontiers en main les outils de protection lorsqu'il s'agit d'outils simples à manipuler (comme les messageries chiffrées). En revanche, leurs choix ne sont pas forcément très pertinents : l'application de messagerie instantanée WhatsApp est la plus utilisée de toutes, ce qui est sans doute dû au fait qu'elle soit la plus répandue au monde (plus d'un milliard d'utilisateurs).

Contrairement à l'intention de départ pour cette partie, qui était de réaliser une sorte de petit kit de sécurité en parlant d'outils spécifiques tels que Tor, j'ai préféré me pencher sur les bases de la base, ce qu'on oublie souvent et ce qui, pourtant, reste essentiel : les mots de passe, mise à jour, VPN etc. N'étant pas moi-même particulièrement technicien et sachant que j'allais sans doute partager ce travail sur internet, je ne souhaitais pas raconter de bêtise concernant des outils plus complexes, étant donné les enjeux que cela représente. Et ce d'autant plus qu'il existe de nombreux kits et formations gratuites en ligne pour ces outils.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

CONCLUSION GÉNÉRALE

Nos outils électroniques sont tous susceptibles d'être écoutés, hackés, volés. Le scandale des révélations de Snowden n'a fait que confirmer ce qu'un certain nombre de ceux qu'on appelait "paranoïaques" redoutaient. Même dans nos démocraties et malgré les lois en faveur de leur protection, les journalistes peuvent être sous surveillance, comme en témoigne une nouvelle fois le très récent témoignage de Camille Polloni, journaliste du média en ligne Les Jours : elle a exercé le droit de tout citoyen français, à savoir demander si elle était "fichée" et pour quelles raisons. Après six ans de procédures, de rendez-vous et de formulaires à envoyer, elle a obtenu une réponse : des fichiers la concernant figuraient bel et bien au renseignement militaire. Le Conseil d'État a reconnu que "*les données concernant Mme Polloni figuraient illégalement dans les traitements d'informations nominatives de la direction du renseignement militaire*". Mais couvert par le secret défense pendant les deux audiences, le Conseil d'État a "*ordonné l'effacement des données"*. Camille Polloni n'aura donc vraisemblablement jamais accès aux fichiers la concernant, elle ne connaîtra jamais la teneur de ses fiches ni leur origine et, par exemple, si ses sources étaient connues.

Bien que de nombreux journalistes estiment ne rien avoir à cacher, comme nombre de nos concitoyens, il est important de mettre en exergue le devoir essentiel de la profession : protéger au mieux les personnes qui livrent des informations et qui nous font confiance. Toutes les personnes auxquelles nous parlons et échangeons, quelle que soit leur profession ou leur sensibilité par rapport aux appareils étatiques, locaux ou entrepreneuriaux, devraient avoir la certitude d'être protégées. Et même si les sujets sur lesquels nous travaillons ne sont pas "sensibles", la charte qui régit notre métier indique clairement que nous devons protéger toutes nos sources. Cette charte ne mentionne aucune exception. Si les journalistes ne font pas ce travail pour leurs sources, ils devraient donc au moins le faire pour eux-mêmes. Et qui sait si ces journalistes qui ne travaillent pas sur des sujets sensibles ne tomberont pas un jour sur une information qui mérite vraiment d'être précautionneux ? Si ces journalistes n'ont jamais fait appel à des outils et des processus de sécurité, ils seront incapables de protéger correctement leurs sources et le risque sera grand. Dans le cas des révélations Snowden, Glenn Greenwald était le premier journaliste choisi par Edward. Mais le journaliste n'était incapable de mettre en place des processus de protection et de sécurité, malgré les nombreuses tentatives du lanceur d'alerte. Edward Snowden a donc dû faire appel à Laura Poitras, en passant par Micah Lee.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Elle connaissait les procédures et a pu les enseigner à Greenwald. Les documents sont finalement sortis, mais ils auraient bien pu ne jamais trouver “preneur”.

Toutes les personnes qui veulent révéler des informations ne sont pas aussi au courant qu’Edward Snowden : le rôle du journaliste est donc d’être capable de prendre ces précautions pour ses sources.

Si nous faisons mal ce travail et que les personnes détenant des informations intéressantes craignent pour leur sécurité ou leur emploi, alors il n’y aura bientôt plus de sources du tout. Et un tarissement des sources peut signifier un tarissement de l’information. Cette menace qui pèse sur la profession peut, je pense, être comparée à une subtile forme de censure de la part des états ou des entreprises, comme en témoigne Scribble, le logiciel développé par la CIA pour piéger les lanceurs d’alerte.

Contrairement à ce que l’on pourrait penser, un début de sécurité peut être mis en place assez facilement, comme nous l’avons vu dans la seconde partie de ce mémoire. Ce sont des gestes simples, mais qui sont le point de départ essentiel du processus. La sécurité informatique est un long processus, jamais sûr à 100%. Et il faut être conscient que les outils plus complexes tels que les échanges de mail chiffrés, Tor ou encore Tails sont inefficaces si cette base n’est pas respectée.

Enfin, d’un point de vue très pragmatique, la maîtrise de ces différents outils peut permettre aux journalistes de recevoir des scoops qu’ils n’auraient pas pu avoir autrement : c’est ce qu’a confirmé Jean-Marc Manach, lors de notre entretien, et cela fait écho à l’origine de l’affaire Snowden.

La majorité des journalistes sensibilisés et formés à cette problématique l’ont été via leurs activités personnelles. Étant donné l’importance que revêtent aujourd’hui les communications électroniques dans le travail de tout journaliste, il devrait peut-être être obligatoire, en plus de mentionner les devoirs des journalistes issus de la Charte de Munich, que les formations de journalisme sensibilisent vraiment leurs étudiants à cette problématique et leur donnent les moyens de pouvoir les appliquer pleinement. Certaines écoles ont commencé : pourvu que cela se développe, pour l’avenir de la profession.

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Pour aller plus loin

Quelques ressources pour aller plus loin que les conclusions de ce mémoire.

Des informations supplémentaires :

À propos des gouvernements qui surveillent leurs citoyens (et les journalistes)

Aux États-Unis :

http://www.thenorthernecho.co.uk/news/14034294.Northern_Echo_journalists__phone_records__accessed__by_Cleveland_Police/?ref=twtrec

https://theintercept.com/2017/01/31/secret-rules-make-it-pretty-easy-for-the-fbi-to-spy-on-journalists-2/

En Grande Bretagne :

https://apnews.com/791aa30b21c5467499babf130754c593/Reporters'-spy-saga-gives-glimpse-of-UK-surveillance-culture

Au Canada :

http://www.cbc.ca/news/canada/montreal/trudeau-airport-spying-1.4055803

https://news.vice.com/story/were-canadian-spies-watching-me?

En Hongrie :

https://budapestbeacon.com/govt-proposes-new-guidelines-for-surveilling-journalists-church-leaders-and-mps/amp/

En Allemagne :

http://www.lemonde.fr/europe/article/2017/02/24/l-allemagne-a-espionne-des-medias-etrangers-affirme-le-spiegel_5085271_3214.html

En Irlande :

https://www.irishtimes.com/news/politics/irish-data-law-amounts-to-mass-surveillance-says-ex-chief-justice-1.3243354?mode=amp

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

En France, très récemment :

http://www.liberation.fr/societe/2017/10/27/ecoutes-judiciaires-la-nouvelle-plateforme-ne-dissipe-pas-les-inquietudes_1606253

A propos des possibilités offertes par les métadonnées :

“Nous tuons des gens à partir des métadonnées”, dit le directeur de la NSA :

https://www.youtube.com/watch?v=kV2HDM86XgI&t=17m53s

Comment réguler les métadonnées ?

https://medium.com/r%C3%A9flexions-sur-le-chiffrement-des-donn%C3%A9es/les-m%C3%A9tadonn%C3%A9es-surveiller-et-pr%C3%A9dire-7ddb669cb3c6

Ce que vos métadonnées disent de vous :

https://lexpansion.lexpress.fr/high-tech/loi-sur-le-renseignement-tout-ce-que-les-metadonnees-peuvent-dire-de-vous_1677322.html

Des ressources utiles pour apprendre à se protéger :

“Surveillance Self Defense”, par l’Electronic Frontier Foundation (en français) :

https://ssd.eff.org/fr

RoryPeckTrust “Digital Security” (très complet) :

https://rorypecktrust.org/resources/digital-security

La protection des sources en 2017 : À starter guide (en anglais)

https://medium.com/@quinnnorton/source-protection-in-2017-a-starter-guide-d44b20f2af2d

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Une check-list faite par The Intercept :

https://medium.com/the-intercept/surveillance-self-defense-for-journalists-ce627e332db6

Une page écrite par Martin Sheldon relevant les meilleurs guides présents sur la toile (en anglais) :

https://medium.com/@mshelton/current-digital-security-resources-5c88ba40ce5c

Plein de ressources intéressantes :

https://guardianproject.info/

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

ANNEXES

Questionnaire proposés aux journalistes concernant la sécurité numérique :

Vous et votre travail

Quel âge avez-vous ? *

- ◯ Moins de 20 ans
- ◯ Entre 20 et 30 ans
- ◯ Entre 31 et 40 ans
- ◯ Entre 41 et 50 ans
- ◯ 51 ans et plus

Pour quel type de média travaillez-vous PRINCIPALEMENT ? *

- ◯ Presse écrite
- ◯ Radio
- ◯ Web
- ◯ Télé
- ◯ Etudiant.e
- ◯ Autre

Si "Autre", précisez : *

Quel est votre fonction principale ? *

- ◯ Enquêteur/trice
- ◯ Rédacteur/trice
- ◯ Reporter
- ◯ JRI
- ◯ Photographe
- ◯ Red-chef/chef de rubrique/chef d'ed/...
- ◯ Autre

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Si "autre", quelle est votre fonction ? *

Êtes-vous pigiste ? *

- ◯ Oui
- ◯ Non

Travaillez-vous régulièrement à l'étranger (correspondant.e ou non) ? *

- ◯ Oui
- ◯ Non

Si oui, dans des environnements jugés sensibles et/ou dangereux ? *

- ◯ Oui
- ◯ Non

Vous et votre stratégie de protection numérique

Selon vous, quel est l'intérêt de se protéger numériquement (applications de messagerie chiffrée, GPG, Tails...) dans le cadre de votre travail ? *

- ◯ Aucun intérêt
- ◯ C'est plutôt utile
- ◯ C'est utile
- ◯ C'est vital

Pourquoi ?

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Selon vous, l'intérêt principal de se protéger numériquement, c'est : *

- ◯ Se protéger soi-même
- ◯ Protéger ses sources
- ◯ Les deux mais plutôt réponse 1
- ◯ Les deux mais plutôt réponse 2
- ◯ Les deux tout pareil

Comment avez-vous été sensibilisé.e ? *

- ◯ Lors de ma formation en journalisme
- ◯ Lectures perso
- ◯ Conférences/Ateliers
- ◯ Amis
- ◯ Autre

Si "Autre", comment ? *

Comment vous êtes-vous formé.e ? *

- ◯ Lors de ma formation en journalisme
- ◯ Autoformation
- ◯ Conférences/Ateliers (CryptoParty ou autres)
- ◯ Amis
- ◯ Autre

Si "Autre", comment ? *

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Le média pour lequel vous travaillez principalement vous a-t-il donné des consignes relatives à la protection de vos données et de vos sources ? *

- ◯ Oui
- ◯ Non

Si "oui", lesquelles ? *

Qu'utilisez-vous comme stratégies et outils de protection numérique ? (Plusieurs options peuvent être cochées) *

- ☐ Authentification double facteur
- ☐ Application de messagerie chiffrée (Telegram, Signal, ...)
- ☐ Envoi de mail avec protocole GPG
- ☐ Clé USB ou disque dur chiffré
- ☐ VPN
- ☐ TOR
- ☐ Tails
- ☐ Prise de note chiffrée (i.e. équivalent de Drive, par exemple)
- ☐ Autre(s)

Si "Autre(s)", précisez : *

Si "Application de messagerie chiffrée", lesquelles ou laquelle ? (notez) *

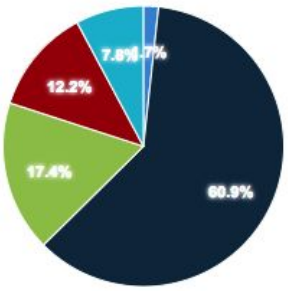
	Jamais	Un peu	Souvent	Très Souvent
Telegram *	◯	◯	◯	◯
WhatsApp *	◯	◯	◯	◯
Signal *	◯	◯	◯	◯
Dust *	◯	◯	◯	◯
Wire *	◯	◯	◯	◯

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Réponses au questionnaire

Quel âge avez-vous ?

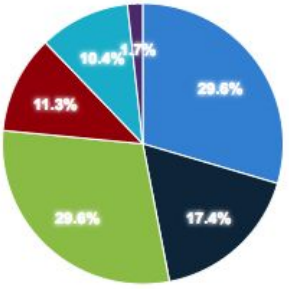
Chart options »



Moins de 20 ans	2
Entre 20 et 30 ans	70
Entre 31 et 40 ans	20
Entre 41 et 50 ans	14
51 ans et plus	9

Pour quel type de média travaillez-vous PRINCIPALEMENT ?

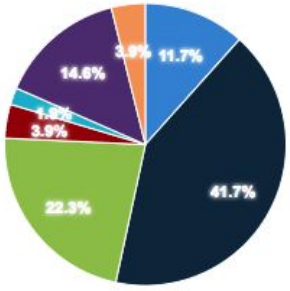
Chart options »



Presse écrite	34
Radio	20
Web	34
Télé	13
Etudiant.e	12
Autre	2

Quel est votre fonction principale ?

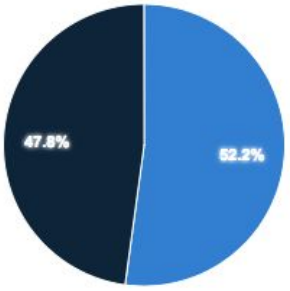
Chart options »



Enquêteur/trice	12
Rédacteur/trice	43
Reporter	23
JRI	4
Photographe	2
Red-chef/chef de rubrique/chef d'ed/...	15
Autre	4

Êtes-vous pigiste ?

Chart options »

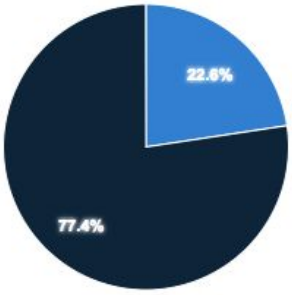


Oui	60
Non	55

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Travaillez-vous régulièrement à l'étranger (correspondant.e ou non) ?

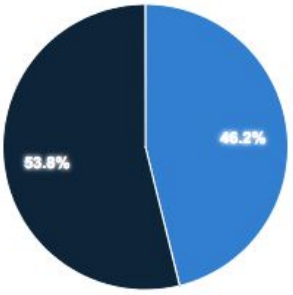
Chart options »



Oui	26
Non	89

Si oui, dans des environnements jugés sensibles et/ou dangereux ?

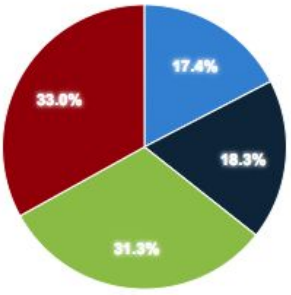
Chart options »



Oui	12
Non	14

Selon vous, quel est l'intérêt de se protéger numériquement (applications de messagerie chiffrée, GPG, Tails...) dans le cadre de votre travail ?

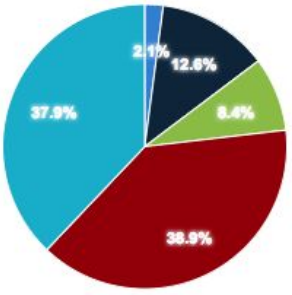
Chart options »



Aucun intérêt	20
C'est plutôt utile	21
C'est utile	36
C'est vital	38

Selon vous, l'intérêt principal de se protéger numériquement, c'est :

Chart options »

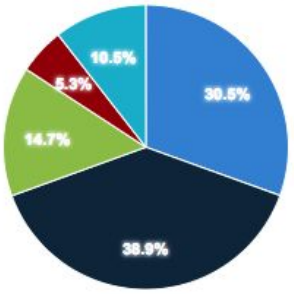


Se protéger soi-même	2
Protéger ses sources	12
Les deux mais plutôt réponse 1	8
Les deux mais plutôt réponse 2	37
Les deux tout pareil	36

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Comment avez-vous été sensibilisé.e ?

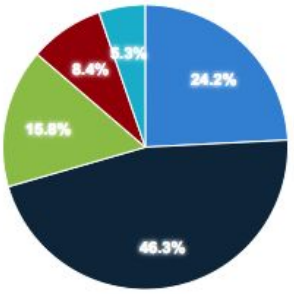
Chart options »



Lors de ma formation en journalisme	29
Lectures perso	37
Conférences/Ateliers	14
Amis	5
Autre	10

Comment vous êtes-vous formé.e ?

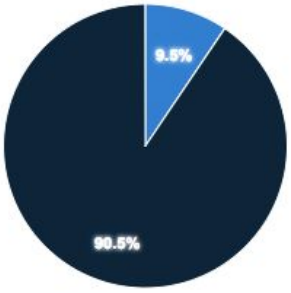
Chart options »



Lors de ma formation en journalisme	23
Autoformation	44
Conférences/Ateliers (CryptoParty ou autres)	15
Amis	8
Autre	5

Le média pour lequel vous travaillez principalement vous a-t-il donné des consignes relatives à la protection de vos données et de vos sources ?

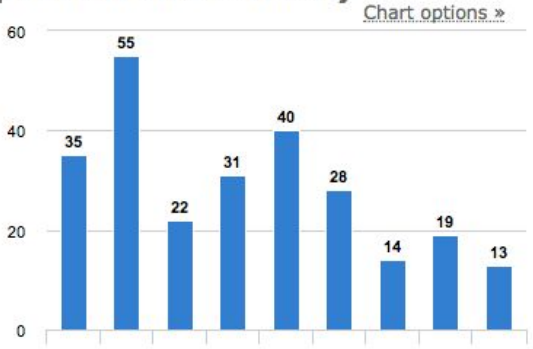
Chart options »



Oui	9
Non	86

Qu'utilisez-vous comme stratégies et outils de protection numérique ? (Plusieurs options peuvent être cochées)

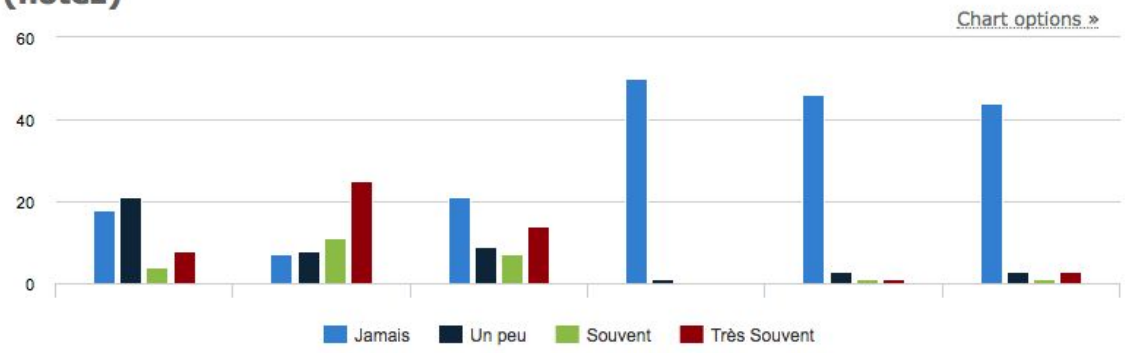
Chart options »



Authentification double facteur	35
Application de messagerie chiffrée (Telegram, Signal, ...)	55
Envoi de mail avec protocole GPG	22
Clé USB ou disque dur chiffré	31
VPN	40
TOR	28
Tails	14
Prise de note chiffrée (i.e. équivalent de Drive, par exemple)	19
Autre(s)	13

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media

Si "Application de messagerie chiffrée", lesquelles ou laquelle ? (notez)



	Jamais	Un peu	Souvent	Très Souvent
Telegram	18	21	4	8
WhatsApp	7	8	11	25
Signal	21	9	7	14
Dust	50	1	0	0
Wire	46	3	1	1
Autre	44	3	1	3

Auteur : Pierre Laurent
pierrelrnt@protonmail.com
Twitter : @Infosec_Media