Geektionnerd : Crowdfunding Etherpad

Vous pouvez retrouver :

- Toutes les informations sur la campagne

- La page Ulule du projet

Crédit : Simon Gee Giraudot (Creative Commons By-Sa)

La surveillance de la NSA révélée par Snowden : un an après, on récapitule ?

Faire le point sur un an de révélations que nous devons à Snowden permet de comprendre comment nous sommes passés peut-être définitivement dans l'ère de la défiance. Quand la machine ubiquiste de surveillance de masse nous considère tous comme des suspects potentiels, nous ne pouvons faire autrement que de soupçonner à priori le plus vertueux des opérateurs téléphoniques ou des fournisseurs d'accès à l'internet d'être bon gré mal gré un complice de la NSA et de lui remettre les clés de nos vies privées, de nos engagements politiques etc. sans même parler de l'espionnage des grands de ce monde .

Cette liste tire sa force accusatrice de sa sècheresse factuelle. Chaque élément y est toutefois documenté par un lien (en anglais en général) vers un article de presse en ligne.

65 choses sur la surveillance par la NSA que nous savons maintenant mais que nous ignorions il y a un

an

Article original sur le site de l'Electronic Frontier Foundation

par Nadia Kayyali et Katitza Rodriguez

Traduction Framalang : hack, Diab, teromene, r0u, Thérèse, goofy, mrtino

Voilà un an que le journal The Guardian *a publié pour la première fois le* Foreign Intelligence Surveillance Court order*, révélé par Edward Snowden, ex-sous-traitant de la NSA. Le document démontrait que la NSA avait mené des opération de surveillance généralisée sur des millions de personnes innocentes. Depuis lors, toute une vague de révélations choquantes, de divulgations, d'aveux partiels des autorités gouvernementales, d'appels aux lois qui garantissent la liberté de l'information, et de poursuites judiciaires, a déferlé sans interruption. Pour l'anniversaire de cette première révélation, voici 65 choses sur la surveillance par la NSA que nous savons maintenant mais que nous ignorions il y a un an.*

1. Nous avons vu un exemple des décisions de justice qui autorisent la NSA à récolter potentiellement tout appel téléphonique aux USA – ce qui veut dire qui vous appelez, qui vous appelle, quand, pendant combien de temps et quelquefois même où.

2. Nous avons découvert les diaporamas en *Powerpoint* de la NSA qui détaillent comment est menée la récolte « en amont », par la collecte d'informations captées directement dans l'infrastructure des opérateurs de télécoms.

3. La NSA a conçu une vaste « drague du Web » en s'assurant qu'elle peut intercepter non seulement les communications d'une cible lorsqu'elle fait partie d'une communication mais

aussi celles qui « concernent une cible, même si la personne ciblée *ne participe pas à une communication* ».

4. La NSA a confirmé qu'elle recherche des données collectées selon les clauses de la section 702 des amendements à la FISA *(FISA Amendments Act)* pour avoir accès sans mandat aux communications des citoyens des USA, grâce à ce que le sénateur Ron Wyden a appelé « le vide juridique de la recherche via porte dérobée ».

5. Même si la NSA a déclaré de façon répétée qu'elle ne ciblait pas les citoyens des États-Unis, ses propres documents montrent que les fouilles de données menées sous l'égide de la section 702 sont conçues pour déterminer avec un degré de confiance de 51% seulement si la cible est étrangère.

6. Si la NSA n'établit pas l'origine étrangère d'une cible, elle ne va pas arrêter d'espionner cette cible pour autant. Au lieu de ça, la NSA va présumer que la cible est étrangère tant qu'elle ne peut être « identifiée positivement comme une personne des États-Unis ».

7. Un audit interne de la NSA révélé par une fuite a donné les détails de 2776 violations de règles ou de décisions judiciaires en une seule année.

8. Les hackers de la NSA ciblent les administrateurs systèmes, indépendamment du fait que ces administrateurs systèmes peuvent eux-mêmes être totalement innocents de tout acte répréhensible…

9. La NSA et la CIA ont infiltré des communautés de jeu en ligne comme *World of Warcraft* et *Second Life* pour récolter des données et mener leur surveillance.

10. Le gouvernement a détruit des preuves dans des procès pour espionnage intentés par l'EFF contre la NSA. Comble de l'ironie, le gouvernement a également prétendu que les clients de l'EFF avaient besoin de ces preuves pour établir la recevabilité de leur plainte.

11. Le directeur du renseignement national, James Clapper, a menti au Congrès lorsqu'il a été interrogé directement par le sénateur Ron Wyden pour savoir si la NSA était en train de rassembler des données de quelque nature que ce soit sur des millions d'habitants des USA.

12. Microsoft, comme d'autres sociétés, a collaboré étroitement avec le FBI afin de permettre à la NSA de « contourner le chiffrement pour avoir accès aux données des utilisateurs ».

13. Pendant la seule année 2013, le budget du renseignement était de 52,6 milliards de dollars – ce chiffre a été révélé par la fuite d'un document, et non par le gouvernement. Sur ce budget, 10,8 milliards de dollars ont été attribués à la NSA. Cela équivaut approximativement à 167 dollars par personne résidant aux Etats-Unis.

14. La Cour fédérale de la surveillance et du renseignement

(Foreign Intelligence Surveillance Court) a rendu des décisions qui autorisent la NSA à partager des données brutes – non expurgées des informations permettant d'identifier les personnes – avec le FBI, la CIA et le Centre national de lutte antiterroriste *(National Counterterrorism Center)*.

15. Conformément à un protocole d'accord *(memorandum of understanding)*, la NSA partage régulièrement des données brutes avec Israël sans en expurger les informations personnelles permettant d'identifier les citoyens des USA.

16. Les divulgations de Snowden ont montré clairement que l'administration Obama avait induit la Cour suprême en erreur à propos de questions clés dans le procès intenté par l'ACLU à la NSA pour espionnage, *Clapper v. Amnesty International*, ce qui a conduit à un renvoi de l'affaire pour manque de preuves.

17. La NSA « a pénétré le système de communication interne d'*Al Jazeera* ». Les documents de la NSA font état de ce que « les cibles sélectionnés avaient un "fort potentiel en tant que sources de renseignement" ».

18. La NSA a utilisé des cookies soi-disant anonymes de Google comme balises de surveillance, aidant ainsi à pister les utilisateurs individuels.

19. La NSA « intercepte "des millions d'images par jour" – dont environ 55 000 "images de qualité suffisante pour la reconnaissance faciale" » et les traite avec de puissants logiciels de reconnaissance faciale.

20. Le programme de reconnaissance faciale de la NSA « peut

maintenant comparer les photos des satellites d'espionnage avec les photos personnelles interceptées prises en extérieur, pour déterminer leur localisation ».

21. Bien que la réforme de la NSA se soit essentiellement focalisée sur la Section 215 du *PATRIOT Act*, et que la plupart des magistrats aient également poussé à réformer la Section 702 du *FISA Amendments Act*, certains des pires espionnages de la NSA ont été effectués conformément au décret 12333, que le président Obama pourrait abroger ou modifier dès aujourd'hui.

22. La NSA a collecté les informations de localisation des téléphones mobiles des citoyens des USA durant deux ans sous couvert d'un projet pilote ayant pour but de voir comment pourraient être analysées de telles informations dans ses énormes bases de données.

23. Au cours du seul mois de mars 2013, la NSA a rassemblé 97 milliards de renseignements en provenance de réseaux informatiques du monde entier, dont 3 milliards de renseignements des réseaux propres aux USA.

24. La NSA a ciblé Tor, un ensemble d'outils qui permet aux internautes de naviguer sur le net de manière anonyme.

25. Le programme MUSCULAR de la NSA infiltre des liens entre les *data centers* mondiaux des sociétés technologiques comme Google et Yahoo. De nombreuses sociétés ont répondu à MUSCULAR en chiffrant le trafic sur leur réseau interne.

27. Le programme XKEYSCORE analyse les courriers électroniques, les conversations en ligne et l'historique de navigation de millions de personnes n'importe où dans le monde.

28. À travers BULLRUN, la NSA sabote les outils de chiffrement auxquels se fient les utilisateurs ordinaires, les entreprises et les institutions financières, cibles ou non, dans un effort sans précédent visant à affaiblir la sécurité des utilisateurs

d'Internet, vous y compris.

28. L'opération Dishfire a collecté 200 millions de textos par jour à travers le globe, qui peuvent être utilisés pour extraire des informations intéressantes sur vous : localisation, contacts, données de carte de crédit, appels manqués, alertes d'itinérance (qui indiquent que vous franchissez une frontière), cartes de visite électroniques, informations sur vos paiements par carte, alertes aux voyageurs, et renseignements sur vos réunions.

29. À travers l'opération CO-TRAVELER, les États-Unis collectent des informations de localisation provenant de relais de téléphonie mobile GSM, d'émetteurs Wi-Fi et de concentrateurs GPS, qui sont ensuite analysées en fonction du temps pour déterminer entre autres avec qui une cible voyage.

30. Un mémo de 2004 intitulé *DEA – The "Other" Warfighter* (DEA – « l'autre » combattant) montre que la NSA et la DEA « profitent d'échanges réciproques d'information ».

31. Quand la DEA agit sur les renseignements que sa division « Opérations spéciales » reçoit de la NSA, ils cachent la source de l'information à travers une « construction parallèle », une mascarade recréant une enquête imaginaire destinée à cacher la source de l'indice, non seulement au défenseur, mais à la Cour. Il s'agit de faire en sorte qu'aucun tribunal ne rende de décision sur la légalité ou la finalité de l'usage qui sont faits des données de la NSA dans les enquêtes ordinaires.

32. Le produit de la surveillance de la NSA finit régulièrement entre les mains de l'IRS (NdT : le fisc des États-Unis). Tout comme la DEA, l'IRS utilise la « construction parallèle » pour dissimuler l'origine de l'indice.

33. Même le Conseil de surveillance de la vie privée et des libertés civiles *(Privacy and Civil Liberties Oversight Board)*, dont les membres sont triés sur le volet par le président des États-Unis, a recommandé que le gouvernement fasse cesser la collecte massive des enregistrements téléphoniques autorisée par la section 215 [NdT : du *PATRIOT Act*], cette collecte étant inefficace, illégale, et probablement anticonstitutionnelle.

34. La NSA a des projets pour infecter potentiellement des millions d'ordinateurs en y implantant des *malwares* dans le cadre du programme *Tailored Access Operations* (opérations d'accès personnalisé).

35. La NSA a eu un contrat secret de 10 millions de dollars avec la société de sécurité RSA pour créer une « porte dérobée » dans ses produits de chiffrement, largement utilisés par les entreprises.

36. « Dans le cadre d'une proposition visant à salir la réputation de ceux dont l'agence pense que les discours incendiaires radicalisent les autres », la NSA a surveillé leurs accès aux contenus pornographiques et rassemblé d'autres informations d'ordre explicitement sexuel.

37. La NSA et ses partenaires exploitent les applications mobiles, comme le jeu populaire *Angry Birds*, pour accéder à des informations privées sur les utilisateurs comme la localisation, l'adresse personnelle, le genre, et plus encore.

38. Le *Washington Post* a révélé que la NSA récolte « des centaines de millions de carnets d'adresses provenant de comptes personnels de courriel ou de messagerie instantanée du monde entier, dont beaucoup sont des citoyens des USA ».

Beaucoup de révélations de Snowden ont concerné les activités de la NSA à l'étranger, ainsi que les activités de certains des plus proches alliés de la NSA, comme son homologue britannique le GCHQ. Certaines de ces activités ont été des entreprises coopératives. En particulier, les « Cinq Yeux » – les États-Unis, la Nouvelle Zélande, l'Australie, le Royaume-Uni et le Canada – se communiquent mutuellement les données concernant leurs citoyens, constituant ainsi des failles susceptibles de saper la législation nationale.

39. La NSA a versé à son homologue britannique, le GCHQ, 155 millions de dollars ces trois dernières années « pour sécuriser l'accès aux programmes de collecte du renseignement britannique et les influencer ».

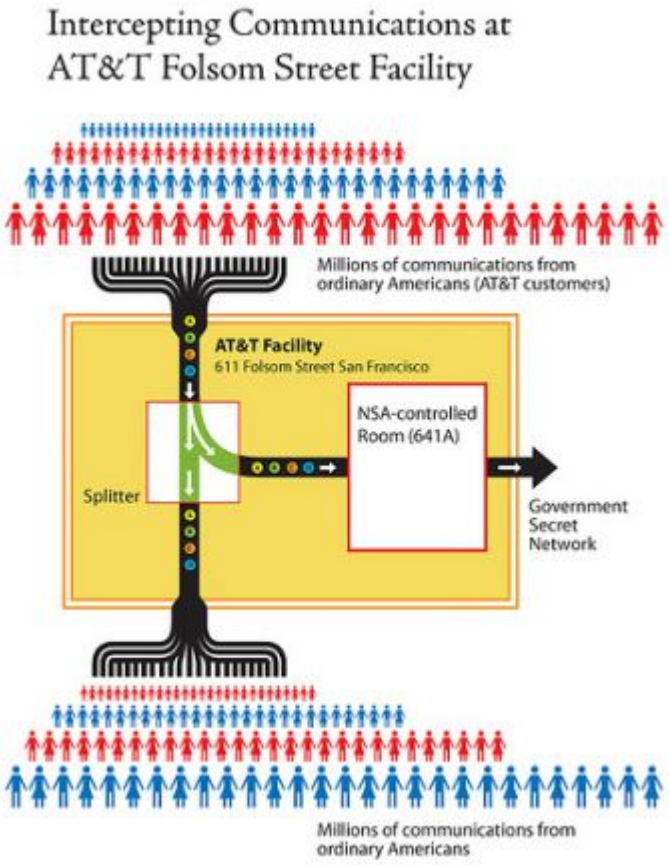
40. *The Guardian* a rapporté ceci : « Sur une période de six mois en 2008, [le GCHQ] a collecté les l'images de webcam – y compris une quantité importante de communications explicitement sexuelles – de plus d'1,8 millions de comptes utilisateurs Yahoo à l'échelle mondiale. »

41. Le GCHQ a utilisé des logiciels malveillants pour compromettre des réseaux appartenant à l'entreprise belge de télécommunications Belgacom.

42. Les principales entreprises de télécommunications, y compris BT, Vodafone, et Verizon business ont fourni au GCHQ un accès illimité à leurs câbles de fibre optique.

43. Le GCHQ a utilisé des attaques DDoS et autres méthodes pour interrompre les communications des Anonymous et de LulzSec, y compris les communications de personnes qui n'étaient accusées d'aucun délit.

44. La station Bude du GCHQ a surveillé des dirigeants de l'Union européenne, de l'Allemagne et d'Israël. Elle a également ciblé des organisations non gouvernementales comme Médecins du monde.



45. Partenaires de la NSA aux antipodes, les services de l'*Australian Signals Directorate*, ont été impliqués dans des violations de communications entre avocat et client couvertes par le secret professionnel, remettant en question un principe fondamental de notre système de justice pénal commun.

46. Les agents du renseignement australien ont espionné les téléphones mobiles du cabinet ministériel indonésien et du président Susilo Bambang.

47. En 2008, l'Australie a offert de partager les données

brutes concernant ses citoyens avec ses partenaires du renseignement.

48. Le CSEC a aidé la NSA à espionner les dirigeants politiques durant le sommet du G20 au Canada.

49. Le CSEC et le CSIS ont été récemment réprimandés par le juge d'une cour fédérale pour l'avoir induit en erreur dans une demande de réquisition faite il y a 5 ans, à propos de l'utilisation des ressources des Cinq Yeux pour pister les Canadiens à l'étranger.

Ironie du sort, certaines opérations de la NSA ont ciblé des pays qui avaient collaboré directement avec l'agence en d'autres circonstances. Et certaines semblaient simplement non indispensables et disproportionnées.

50. Les documents de la NSA montrent que tous les gouvernements ne sont pas transparents sur leur propre niveau de coopération avec la NSA. Comme le rapporte *The Intercept* : « Peu de dirigeants élus ont connaissance de cet espionnage, voire aucun ».

51. La NSA intercepte, enregistre et archive chaque communication de téléphone mobile des Bahamas.

52. La NSA a surveillé les communications téléphoniques d'au moins 35 chefs d'États.

53. La NSA a espionné des diplomates français à Washington et aux Nations Unies.

54. La NSA a piraté les réseaux de l'entreprise chinoise Huawei et volé les sources de son code.

55. La NSA a posé des mouchards dans les ambassades de l'Union européenne à New York et à Washington. Elle a copié des disques durs dans les bureaux de l'UE à New York, et a mis sur écoute le réseau informatique interne des ambassades de Washington.

56. La NSA a collecté les métadonnées de plus de 45 millions d'appels téléphoniques italiens sur une période de 30 jours. Elle a également entretenu des stations de surveillance à Rome et à Milan.

57. La NSA a stocké les données d'approximativement 500 millions de connexions des systèmes de communication allemands chaque mois.

58. La NSA a collecté les données de plus de 60 millions d'appels téléphoniques espagnols sur une période de 30 jours, fin 2012 et début 2013, et a espionné des membres du gouvernement espagnol.

59. La NSA a collecté les données de plus de 70 millions d'appels téléphoniques français sur une période de 30 jours, fin 2012 et début 2013.

60. *The Hindu*, sur la base de documents de la NSA, a rapporté que « Sur une liste exhaustive des pays espionnés par les programmes de la NSA, l'Inde est en cinquième place. »

61. La NSA a pénétré le compte officiel de courriel de l'ancien président mexicain Felipe Calderon.

62. D'après *The Guardian* : « La NSA a, pendant des années, systématiquement écouté le réseau des télécommunications brésiliennes et et a intercepté, collecté et stocké sans discrimination les courriels et enregistrements téléphoniques de millions de Brésiliens ».

63. La NSA a surveillé les courriels, les appels téléphoniques et les textos de la présidente brésilienne Dilma Rousseff et de ses plus proches collaborateurs.

64. Les agences du renseignement allemand ont coopéré avec la NSA et ont implémenté le programme de la NSA XKeyscore, tandis que la NSA était en train d'espionner les dirigeants allemands.

65. Le quotidien norvégien *Dagbladet* a rapporté que la NSA a acquis des données sur 33 millions d'appels de téléphones mobiles norvégiens sur une période de 30 jours.

Il ne fait aucun doute que les relations internationales qu'Obama s'était engagé à restaurer, de même que la confiance du peuple des États-Unis dans le respect de sa vie privée et de ses droits constitutionnels, ont été sapées par la surveillance tous azimuts de la NSA. Mais un an après, le gouvernement des USA aussi bien que les gouvernements d'autres pays n'ont pas pris les mesures nécessaires pour faire en sorte que cette surveillance cesse. C'est pourquoi chacun doit se mobiliser – contactez votre député, rejoignez Reset the Net, et apprenez comment la loi internationale s'applique à la surveillance états-unienne aujourd'hui.

Toutes les images sous licence CC BY 2.0, par EFF, JeepersMedia et Richard Loyal French,

---

Framasoft lance un crowdfunding pour améliorer Framapad/Etherpad

Framapad est l'un des services plus dynamiques du réseau Framasoft (plus de vingt mille pads voient le jour actuellement tous les mois). Il repose sur l'application libre Etherpad. Nous avons décidé de mener **une campagne de financement participatif** pour créer un plugin Etherpad fortement demandé par la communauté.

Ce plugin, baptisé « **MyPads** », permettra d'avoir un compte personnel pour gérer de manière fine ses pads, les grouper et les partager avec d'autres.

Nous proposons déjà, et ce depuis le début, la possibilité d'avoir des groupes privés. Mais cette fonctionnalité repose sur une ancienne version d'Etherpad qui n'est plus développée et qui pose de très nombreux problèmes techniques. C'est parce que nous sommes contraints de devoir fermer bientôt ce service, pourtant plébiscité par nos utilisateurs, que nous avons décidé de lancer cette campagne. Il s'agit donc de continuer à offrir ce service, en y ajoutant au passage de

nombreuses améliorations. Mais il s'agit également d'apporter collectivement notre propre pierre au développement d'Etherpad.

Pour de plus amples informations nous vous invitons à vous rendre **sur Ulule** où est hébergée la campagne (vidéo et gif animé inside).

L'objectif est fixé à dix mille euros, somme qui servira à créer et maintenir le plugin « MyPads » en finançant son développement. En cas de succès nous aurons un Etherpad à forte valeur ajoutée. Nous témoignerons également que nos utilisateurs sont soucieux de son caractère libre et participent à son développement au bénéfice de tous.

Nous espérons l'implication de nombreuses organisations (sociétés, associations, collectivités…), utilisatrices de Framapad/Etherpad et attachées à l'écosystème du Libre et à ses modèles économiques originaux. Nous comptons aussi – voire surtout – sur votre participation, qu'elle soit directe par une contribution financière et/ou indirecte en relayant massivement cette campagne.

Framapad/Etherpad est un service gratuit mais surtout **libre**. Il permet de faire l'expérience du travail collaboratif. Il permet à chacun de l'installer sur son propre serveur. Il permet de décentraliser le Web en offrant une alternative à Google & consorts et en ayant le souci de la vie privée et du respect de nos données personnelles. Il est important de prendre soin de telles applications.

-> **Améliorons ensemble Etherpad/Framapad**

NB : Il y a des paliers pour la participation mais vous pouvez également soutenir avec un montant libre (avec ou sans contreparties) en cliquant sur le gros bouton bleu Contribuez en haut à droite.

NB2 : Cette campagne se décline également en anglais (si vous

avez des relais dans la sphère anglophone…).

Merci.

Geektionnerd : Asile pour Snowden

Sources sur Numerama :

- Edward Snowden : 120 000 signataires pour son exil en France

Crédit : Simon Gee Giraudot (Creative Commons By-Sa)

Vous êtes « natif du numérique » ? – Ce n'est pas si grave, mais…

La vie privée est-elle un problème de vieux cons ? demandait Jean-Marc Manach dans un excellent ouvrage. Bien sûr que non, mais on aimerait tant nous le faire croire…

« Natifs numériques », « natifs du numérique », « génération numérique »… Ce genre d'expressions, rencontrées dans les

grands médias désireux d'agiter le grelot du jeunisme, peut susciter quelque agacement. D'autant que cette catégorie soi-disant sociologique se transforme bien vite en cible marketing pour les appétits des mastodontes du Web qui ont tout intérêt à présenter la jeunesse connectée comme le parangon des usages du net.

En s'attaquant à cette dénomination, Cory Doctorow [1] entend aussi remettre en cause ce préjugé. Selon lui, les adolescents sont tout à fait soucieux de la confidentialité et de leur vie privée. Mais ils sont loin de maîtriser tous les risques qu'ils sont susceptibles de prendre et comme nous tous, ils ont besoin d'outils et dispositifs qui les aident…

Vous n'êtes pas un « natif numérique » : la vie privée à l'ère d'Internet

par Cory Doctorow sur ce blog

Traduction Framalang : Amargein, lamessen, r0u, teromene, goofy, Clunär

On raconte que Frédéric II, à la tête du Saint-Empire Romain germanique, avait ordonné qu'un groupe d'enfants soit élevé sans aucune interaction humaine, afin que l'on puisse étudier leur comportement « naturel », sans que celui-ci ne soit corrompu par la culture humaine, et découvrir ainsi la véritable nature profonde de l'animal humain.

Si vous êtes né au tournant du XXIe siècle, vous avez certainement dû supporter au moins une fois que quelqu'un vous appelle « natif numérique ». Dans un premier temps, ça sonne de façon plutôt sympathique : une éducation préservée du monde hors ligne et très imprégnée d'une sorte de sixième sens mystique, donnant l'impression de savoir ce que devrait être Internet.

Mais les enfants ne sont pas d'innocents mystiques. Ce sont de jeunes personnes, qui apprennent à devenir adultes de la même manière que les autres : en commettant des erreurs. Tous les humains se plantent, mais les enfants ont une excuse : ils n'ont pas encore appris les leçons que ceux qui se sont déjà plantés peuvent leur éviter. Si vous voulez doubler vos chances de réussite, vous devez tripler vos risques d'échec.

Le problème quand vous êtes catalogué « natif numérique », c'est que cela transforme toutes vos erreurs en une vérité absolue sur la manière dont les humains sont censés utiliser Internet. Ainsi, si vous faites des erreurs concernant votre vie privée, non seulement les entreprises qui vous incitent à les commettre (pour en tirer profit) s'en sortent impunies, mais tous ceux qui soulèvent des problèmes de vie privée sont exclus d'emblée. Après tout, si les « natifs numériques » sont censés ne pas être soucieux de leur vie privée, alors quiconque s'en préoccupe sérieusement passe pour un dinosaure complètement à la ramasse, plus du tout en phase avec ''les Jeunes''.

« Vie privée » ne signifie pas que personne au monde ne doit être au courant de vos affaires. Cela veut dire que c'est à vous de choisir qui peut s'en mêler.

Quiconque y prête attention s'apercevra qu'en réalité, les enfants se soucient énormément de leur vie privée. Ils ne veulent surtout pas que leurs parents sachent ce qu'ils disent à leurs amis. Ils ne veulent pas que leurs amis les voient dans leurs relations avec leurs parents. Ils ne veulent pas que leurs professeurs apprennent ce qu'ils pensent d'eux. Ils ne veulent pas que leurs ennemis connaissent leurs peurs et leurs angoisses.

Ceux qui veulent s'insinuer dans la vie privée des jeunes ne communiquent pas du tout sur ce point. Facebook est une entreprise dont le modèle économique repose sur l'idée que si elle vous espionne suffisamment et vous amène à révéler malgré vous suffisamment sur votre vie, elle pourra vous vendre des tas de trucs à travers la publicité ciblée. Quand on l'interpelle sur ce point, elle se justifie en disant que puisque les jeunes finissent par dévoiler tant de choses de leur vie personnelle sur Facebook, ça ne doit pas être un problème, vu que les natifs numériques sont censés savoir comment se servir d'Internet. Mais quand les gamins grandissent et commencent à regretter ce qu'ils ont dévoilé

sur Facebook, on leur dit qu'eux non plus ne comprennent plus ce que ça signifie d'être un natif numérique, puisqu'ils sont devenus adultes et ont perdu le contact avec ce qui fait l'essence même d'Internet.

Dans « It's Complicated: The Social Lives of Networked Teens[2] » [NdT « La vie sociale des jeunes connectés, un problème complexe »], une chercheuse nommée danah boyd[3] résume plus de dix ans d'étude sur la manière dont les jeunes utilisent les réseaux, et dévoile une lutte continue, voire désespérée, pour préserver leur vie privée en ligne. Par exemple, certains des jeunes interviewés par Boyd suppriment leur compte Facebook à chaque fois qu'ils s'éloignent de leur ordinateur. Si vous supprimez votre compte Facebook, vous avez six semaines pour changer d'avis et réactiver votre compte, mais durant le temps où vous êtes désinscrit, personne ne peut voir votre profil ou quelque partie que ce soit de votre journal (''timeline''). Ces jeunes se réinscrivent sur Facebook à chaque fois qu'ils reviennent devant leur ordinateur, mais s'assurent de cette manière que personne ne peut interagir avec leur double numérique à moins qu'ils ne soient là pour répondre, supprimant les informations si elles commencent à leur causer des problèmes.

C'est assez extraordinaire. Cela nous enseigne deux choses : premièrement, que les jeunes vont jusqu'à prendre des mesures extrêmes pour protéger leur vie privée ; deuxièmement, que Facebook rend extrêmement difficile toute tentative de protection de notre vie privée.

Vous avez certainement entendu un tas d'informations concernant Edward Snowden et la NSA. En juin dernier, Edward Snowden, un espion étatsunien, s'envola pour Hong Kong et remit à un groupe de journalistes étatsuniens des documents internes à la NSA. Ces documents décrivent un système d'une ampleur presque inimaginable – et absolument illégal – de

surveillance d'Internet de la part des agences de surveillance étatsuniennes. Celles-ci choisissent littéralement au hasard un pays et enregistrent le moindre appel téléphonique passé depuis ce pays, juste pour voir si cela fonctionne et peut être transposé dans d'autres pays. Ils puisent littéralement dans le flux complet d'informations circulant entre les centres de données de Google ou de Yahoo, enregistrant les parcours de navigation/, les e-mails, les discussions instantanées et d'autres choses dont personne ne devrait avoir connaissance chez des milliards de personnes innocentes, y compris des centaines de millions d'Étatsuniens.

Tout cela a modifié les termes du débat sur la vie privée. Tout à coup, les gens ordinaires qui ne se préoccupaient pas de la vie privée s'y sont intéressés. Et ils ont commencé à penser à Facebook et au fait que la NSA avait récolté beaucoup de données par leur biais. Facebook a collecté ces données et les a mises à un endroit où n'importe quel espion pouvait les trouver. D'autres personnes dans le monde y avaient déjà pensé. En Syrie, en Égypte et dans beaucoup d'autre pays, rebelles ou agents du gouvernement ont mis en place des barrages que vous ne pouvez franchir qu'en vous connectant à votre compte Facebook de sorte qu'ils ont accès à votre liste d'amis. Si vous êtes ami-e avec les mauvaises personnes, vous êtes abattu ou emprisonné ou bien vous disparaissez.

Les choses ont été si loin que Marck Zuckerberg – qui avait dit à tout le monde que la vie privée était morte tout en dépensant 30 millions de dollars pour acheter les quatre maisons à côté de la sienne afin que personne ne voie ce qu'il faisait chez lui – a écrit une lettre ouverte au gouvernement des États-Unis pour lui reprocher d'avoir « tout gâché ». Comment avait-il tout gâché ? Ils ont montré au gens d'un seul coup que toutes leurs données privées étaient en train de migrer de leur ordinateur vers ceux de Facebook.

Les enfants savent intuitivement ce que vaut la vie privée.

Mais comme ce sont des enfants, ils ont du mal à comprendre tous les détails. C'est un long processus que d'apprendre à bien la gérer, car il se passe beaucoup de temps entre le moment où on commence à négliger la protection de sa vie privée et celui où les conséquences de cette négligence se font sentir. C'est un peu comme l'obésité ou le tabagisme. Dans les cas où une action et ses conséquences sont clairement distinctes, c'est une relation que les gens ont beaucoup de peine à comprendre. Si chaque bouchée de gâteau se transformait immédiatement en bourrelet de graisse, il serait bien plus facile de comprendre quelle quantité de gâteau était excessive.

Les enfants passent donc beaucoup de temps à réfléchir sur leur vie privée préservée de leur parents, des enseignants et de ceux qui les tyrannisent, mais ils ne se demandent pas à quel point leur vie privée sera protégée vis-à-vis de leurs futurs employeurs, de l'administration et de la police. Hélas, au moment où ils s'en rendent compte, il est déjà trop tard.

Il y a toutefois de bonne nouvelles. Vous n'avez pas à choisir entre une vie privée et une vie sociale. De bons outils sont disponibles pour protéger votre vie privée, qui vous permettent d'aller sur Internet sans avoir à livrer les détails intimes de votre vie aux futures générations d'exploitants de données. Et parce qu' il y a des millions de personnes qui commencent à avoir peur de la surveillance – grâce à Snowden et aux journalistes qui ont soigneusement fait connaître ses révélations – de plus en plus d'énergie et d'argent sont utilisés pour rendre ces outils plus faciles à utiliser.

La mauvaise nouvelle, c'est que les outils propices à la vie privée tendent à être peu pratiques. C'est parce que, avant Snowden, quasiment tout ceux qui se sentaient concernés par l'adéquation entre leur vie privée et la technologie étaient déjà experts d'un point de vue technologique. Non pas parce

que les nerds ont besoin de plus de vie privée que les autres, mais parce qu'ils étaient les plus à même de comprendre quel genre d'espionnage était possible et ce qui était en jeu. Mais, comme je le dis, cela change vite (et les choses ne font que s'améliorer).

L'autre bonne nouvelle c'est que vous êtes des « natifs numériques », au moins un peu. Si vous commencez à utiliser des ordinateurs étant enfant, vous aurez une certains aisance avec eux, là où d'autres auront à travailler dur pour y parvenir. Comme Douglas Adams l'a écrit :

1. Tout ce qui existe dans le monde où vous êtes né est normal et ordinaire, et ce n'est qu'un rouage dans le mécanisme naturel du système.

2. Tout ce qui est inventé entre le moment de vos quinze ans et celui de vos trente-cinq est nouveau, excitant et révolutionnaire et vous pourrez probablement y faire carrière.

3. Tout ce qui sera inventé après vos trente-cinq ans est contraire à l'ordre naturel des choses.

Si j'étais un enfant aujourd'hui, je saurais tout au sujet des sécurités opérationnelles. J'apprendrais à me servir d'outils pour garder mes affaires entre moi et les personnes avec qui j'aurais décidé de les partager. J'en ferais une habitude, et j'inciterais mes amis à adopter cette habitude aussi (après tout, ça ne change rien si tous vos e-mails sont chiffrés mais que vous les envoyez à des idiots qui les gardent tous sur les serveurs de Google sous une forme déchiffrée, là où la NSA peut venir y fourrer son nez).

Voici quelques liens vers des outils de sécurité pour vous y initier :

- Tout d'abord, téléchargez une version de Tails (pour « The Amnesic Incognito Live System »). Il s'agit d'un

système d'exploitation que vous pouvez utiliser pour démarrer votre ordinateur sans avoir à vous soucier si le système d'exploitation installé est exempt de tout virus, enregistreur de frappe ou autre logiciel-espion. Il est fourni avec une tonne d'outils de communication sécurisés, ainsi que tout ce dont vous avez besoin pour produire les contenus que vous souhaitez diffuser de par le monde.

- Ensuite, téléchargez une version du Tor Browser Bundle, une version spéciale de Firefox qui envoie automatiquement votre trafic à travers quelque chose appelé TOR (The Onion Router, le routeur en oignon, à ne pas confondre avec Tor Books, qui publie mes nouvelles). Cela vous permet de naviguer sur Internet avec beaucoup plus d'intimité et d'anonymat que vous n'en auriez normalement.
- Apprenez à utiliser GPG, qui est une excellente manière de chiffrer vos courriers électroniques. Il existe une extension pour Chrome qui vous permet d'utiliser GPG avec GMail et une autre pour Firefox.
- Si vous appréciez les messageries instantanées, procurez-vous OTR (« ''Off The Record messaging'' »), un outil pour sécuriser ses conversations en ligne, incluant des fonctionnalités telles que « l'inviolabilité des messages passés » (une façon de dire que même si quelqu'un arrive à le casser demain, il ne pourra pas lire les conversations interceptées aujourd'hui).

Une fois que vous aurez maîtrisé ce genre de choses, mettez-vous à réfléchir à votre téléphone. Les appareils sous Android sont de loin plus faciles à sécuriser que les iPhones d'Apple (Apple essaie de verrouiller ses téléphones pour que vous ne puissiez pas y installer d'autres logiciels que ceux de leur logithèque, et en raison de la loi DMCA de 1998, il est

illégal de créer un outil pour les déverrouiller (''jailbreaker''). Il existe de nombreux systèmes d'exploitation concurrents d'Android, avec des niveaux variables de sécurité. Le meilleur point de départ est Cyanogenmod, qui vous facilitera l'utilisation d'outils de confidentialité sur votre mobile.

Il existe également des quantités de projets commerciaux qui traitent la vie privée bien mieux que le tout-venant. Je suis par exemple consultant de l'entreprise Wickr, qui reproduit les fonctionnalités de Snapchat mais sans moucharder à tout moment. Wickr a cependant beaucoup de concurrents, il vous suffit de regarder dans votre logithèque préférée pour vous en convaincre, mais assurez-vous d'avoir bien lu comment l'entreprise qui a conçu l'application vérifie que rien de louche ne vient interférer avec vos données supposées secrètes.

Tout ceci est en constante évolution, et ce n'est pas toujours facile. Mais c'est un excellent exercice mental que de chercher comment votre usage d'Internet peut vous compromettre. C'est aussi une bonne pratique dans un monde où des milliardaires voyeurs et des agences d'espionnage hors de contrôle essayent de transformer Internet en l'outil de surveillance le plus abouti. Si vous trouvez particulièrement pénible que vos parents espionnent votre historique de navigation, attendez que tous les gouvernements et toutes les polices du monde en fassent autant.

Notes

[1] Lisez ses très bons romans, notamment Little Brother

[2] Lien direct vers le téléchargement de cet essai au format PDF, en anglais : http://www.danah.org/books/ItsComplicated.pdf

[3] …et non Danah Boyd, c'est elle qui insiste pour ne pas

mettre de capitales à ses nom et prénom, dit sa page Wikipédia

---

Une déclaration de Snowden : le 5 juin on redémarre le Net !

Texte original paru le 4 juin 2014 sur le portail de l'opération Reset The Net. Au bas de la page d'accueil figurent les liens vers les objectifs et initiatives, ainsi que les logos des entreprises et organisations qui soutiennent ce mouvement. On y trouve pêle-mêle le parti Pirate et Google, Mozilla et l'Electronic Frontier Foundation, Piwik et Amnesty international…

Au fait, avez-vous signé la pétition pour réclamer le droit d'asile en France pour Edward Snowden ?

Edward Snowden a publié cette déclaration par l'intermédiaire de son avocat pour soutenir l'initiative *Reset The Net*, que l'on peut traduire par Réinitialiser le Net.

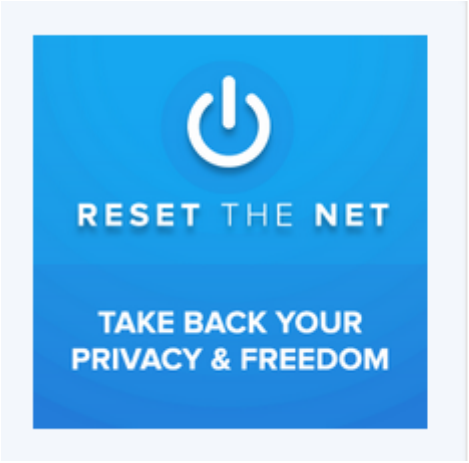
Il y a un an, nous avons appris que l'Internet est sous surveillance, que nos activités sont surveillées pour créer des dossiers permanents sur nos vies privées – peu importe si nos vies sont celles de gens ordinaires qui n'ont rien à se reprocher…

Aujourd'hui, nous pouvons commencer à agir efficacement pour arrêter la collecte de nos communications en ligne, même si le Congrès des États-Unis ne parvient pas à l'obtenir. C'est pourquoi je vous demande de vous joindre à moi le 5 Juin pour la Réinitialisation du Net, quand les gens et les entreprises du monde entier vont se concerter pour concevoir des solutions technologiques qui pourront mettre un terme aux programmes de surveillance de la masse de n'importe quel gouvernement. C'est le début d'une période où nous les peuples commençons à protéger nos droits universels humains avec des lois naturelles[1] plutôt qu'avec les lois des nations.

Nous avons la technologie : adopter le chiffrement est la première mesure efficace que tout le monde peut prendre pour mettre fin à la surveillance de masse. C'est pourquoi je suis très heureux pour l'opération Réinitialiser le net – il marquera le moment où nous nous transformerons une expression politique en action concrète et où nous nous protégerons en agissant à grande échelle.

Rejoignez notre action le 5 Juin, et ne demandez pas le droit à votre vie privée. Reprenez-le.

– Edward Snowden



Notes

[1] En V.O : *…where we the people begin to protect our universal human rights with the laws of nature rather than the laws of nations.* Perplexité de ma part pour la traduction de ces *“laws of nature”*. S’agit-il de « nature… humaine » ? si quelqu’un a une idée…

Plus rien ne marche, qu’est-ce qu’on fait ?

Désormais conscients et informés que nos actions et nos données en ligne sont faciles à espionner et l’enjeu de monétisation en coulisses, il nous restait l’espoir que quelques pans des technologies de sécurité pouvaient encore faire échec à la surveillance de masse et au profilage commercial. Pas facile pour les utilisateurs moyens d’adopter des outils et des pratiques de chiffrement, par exemple, cependant de toutes parts émergent des projets qui proposent de nous aider à y accéder sans peine.

Mais quand les experts en sécurité, quittant un moment leur regard hautain sur le commun des mortels à peine capables de

choisir un mot de passe autre que 123AZERTY, avouent qu'ils savent depuis longtemps que tout est corrompu directement ou indirectement, jusqu'aux services soi-disant sécurisés et chiffrés, le constat est un peu accablant parce qu'il nous reste tout à reconstruire…

Plus rien ne fonctionne

*article original : Everything is broken par **Quinn Norton***

Traduction Framalang : Diab, rafiot, Omegax, Scailyna, Amine Brikci-N, EDGE, r0u, fwix, dwarfpower, sinma, Wan, Manu, Asta, goofy, Solarus, Lumi, mrtino, skhaen

Un beau jour un de mes amis a pris par hasard le contrôle de plusieurs milliers d'ordinateurs. Il avait trouvé une faille dans un bout de code et s'était mis à jouer avec. Ce faisant, il a trouvé comment obtenir les droits d'administration sur un réseau. Il a écrit un script, et l'a fait tourner pour voir ce que ça donnerait. Il est allé se coucher et il a dormi environ quatre heures. Le matin suivant, en allant au boulot, il a jeté un coup d'œil et s'est aperçu qu'il contrôlait désormais près de 50 000 ordinateurs. Après en avoir pratiquement vomi de trouille, il a tout arrêté et supprimé tous les fichiers associés. Il m'a dit que finalement il avait jeté le disque dur au feu. Je ne peux pas vous révéler de qui il s'agit, parce qu'il ne veut pas finir dans une prison fédérale ; et c'est ce qui pourrait lui arriver s'il décrivait à qui que ce soit la faille qu'il a découverte. Cette faille a-t-elle été corrigée ? Sans doute… mais pas par lui. Cette histoire n'est en rien exceptionnelle. Passez quelque temps dans le monde des hackers et de la sécurité informatique, et vous entendrez pas mal d'histoires dans ce genre et même pires que celle-là.

Il est difficile d'expliquer au grand public à quel point la technologie est chancelante, à quel point l'infrastructure de nos vies ne tient qu'avec l'équivalent informatique de bouts de ficelle. Les ordinateurs et l'informatique en général sont

détraqués.

Quand c'est codé avec les pieds, bonjour les vautours

Pour un bon nombre d'entre nous, en particulier ceux qui ont suivi l'actualité en matière de sécurité et les questions d'écoutes sauvages, rien de surprenant dans toutes les dernières révélations. Si nous ne connaissions pas les détails, nous savions tous, dans le monde de la sécurité, que la technologie est vacillante et malade. Depuis des années nous voyons tourner les vautours qui veulent profiter de cet état de fait. La NSA n'est pas et n'a jamais été le grand prédateur unique fondant sur Internet. C'est simplement le plus gros de ces charognards. S'ils arrivent à aller aussi loin, ce n'est pas parce que leurs employés sont des dieux des maths.

Si la NSA s'en sort si bien, c'est parce que les logiciels en général sont merdiques.

Huit mois avant que Snowden ne fasse ses révélations, j'ai twitté ça :

« alerte de sécu : tout a une faille 0 day, tout le monde est suivi à la trace, toutes les données fuitent, tout est vulnérable, tout est compromis jusqu'à l'os. »

J'en étais arrivée à cette conclusion un peu désespérée : chercher des logiciels de qualité est un combat perdu

d’avance. Comme ils sont écrits par des gens n’ayant ni le temps ni l’argent nécessaires, la plupart des logiciels sont publiés dès qu’ils fonctionnent assez bien pour laisser leurs auteurs rentrer chez eux et retrouver leur famille. Pour nous le résultat est épouvantable.

Si les logiciels sont aussi mauvais, c’est parce qu’ils sont très complexes, et qu’il cherchent à parler à d’autres logiciels, soit sur le même ordinateur, soit au travers du réseau. Même votre ordinateur ne peut plus être considéré comme unique : c’est une poupée russe, et chaque niveau est fait de quantité d’éléments qui essaient de se synchroniser et de parler les uns avec les autres. L’informatique est devenue incroyablement complexe, alors que dans le même temps les gens sont restés les mêmes, pétris de la même boue grise originelle pleine d’une prétention à l’étincelle divine.

Le merdier qu’est votre ordinateur sous Windows est tellement complexe que personne sur Terre ne sait tout ce qu’il fait vraiment, ni comment.

Maintenant imaginez des milliards de petites boites opaques qui essaient en permanence de discuter les unes avec les autres, de se synchroniser, de travailler ensemble, partageant des bouts de données, se passant des commandes… des tous petits bouts de programmes aux plus gros logiciels, comme les navigateurs – c’est ça, Internet. Et tout ça doit se passer quasi-simultanément et sans accrocs. Sinon vous montez sur vos grand chevaux parce que le panier de la boutique en ligne a oublié vos tickets de cinéma.

On n’arrête pas de vous rappeler que le téléphone avec lequel vous jouez à des jeux stupides et que vous laissez tomber dans les toilettes au troquet du coin est plus puissant que les ordinateurs utilisés pour la conquête de l’espace il y a de cela quelques décennies à peine. La NASA dispose d’une armée de génies pour comprendre et maintenir ses logiciels. Votre téléphone n’a que vous. Ajoutez à cela un mécanisme de mises à

jour automatiques que vous désactivez pour qu'il ne vous interrompe pas au beau milieu d'une séance de Candy Crush…

À cause de tout ça, la sécurité est dans un état effrayant. En plus d'être truffés de bugs ennuyeux et de boîtes de dialogue improbables, les programmes ont souvent un type de faille piratable appelée *0 day* (« zéro jour ») dans le monde de la sécurité informatique. Personne ne peut se protéger des *0 days*. C'est justement ce qui les caractérise : 0 représente le nombre de jours dont vous disposez pour réagir à ce type d'attaque. Il y a des *0 days* qui sont anodins et vraiment pas gênants, il y a des *0 days* très dangereux, et il y a des *0 days* catastrophiques, qui tendent les clés de la maison à toute personne qui se promène dans le coin. Je vous assure qu'en ce moment même, vous lisez ceci sur une machine qui a les trois types de *0days*. Je vous entends d'ici me dire : « Mais, Quinn, si personne ne les connaît comment peux-tu savoir que je les ai ? » C'est parce que même un logiciel potable doit avoir affaire avec du code affreux. Le nombre de gens dont le travail est de rendre le logiciel sûr peut pratiquement tenir dans un grand bar, et je les ai regardé boire. Ce n'est pas rassurant. La question n'est pas : « est-ce que vous allez être attaqué ? » mais : « quand serez-vous attaqué ? »

Considérez les choses ainsi : à chaque fois que vous recevez une mise à jour de sécurité (apparemment tous les jours avec mon ordi sous Linux), tout ce qui est mis à jour a été cassé, rendu vulnérable depuis on ne sait combien de temps. Parfois des jours, parfois des années. Personne n'annonce vraiment cet aspect des mises à jour. On vous dit « Vous devriez installer cela, c'est un patch critique ! » et on passe sous silence le côté « …parce que les développeurs ont tellement merdé que l'identité de vos enfants est probablement vendue en ce moment même à la mafia estonienne par des script kiddies accrocs à l'héro ».

Les bogues vraiment dangereux (et qui peut savoir si on a

affaire à eux lorsqu'on clique sur le bouton « Redémarrer ultérieurement » ?) peuvent être utilisés par des hackers, gouvernements, et d'autres horreurs du net qui fouillent à la recherche de versions de logiciels qu'ils savent exploiter. N'importe quel ordinateur qui apparaît lors de la recherche en disant « Hé ! Moi ! Je suis vulnérable ! » peut faire partie d'un botnet, en même temps que des milliers, ou des centaines de milliers d'autres ordinateurs. Souvent les ordinateurs zombies sont possédés à nouveau pour faire partie d'un autre botnet encore. Certains botnets patchent les ordinateurs afin qu'ils se débarrassent des autres botnets, pour qu'ils n'aient pas à vous partager avec d'autres hackers. Comment s'en rendre compte si ça arrive ? Vous ne pouvez pas ! Amusez-vous à vous demander si votre vie en ligne va être vendue dans l'heure qui suit ! La prochaine fois que vous penserez que votre grand-mère n'est pas cool, pensez au temps qu'elle a passé à aider de dangereux criminels russes à extorquer de l'argent à des casinos offshore avec des attaques DDoS.

Récemment un hacker anonyme a écrit un script qui prenait le contrôle d'appareils embarqués Linux. Ces ordinateurs possédés scannaient tout le reste d'Internet et ont créé un rapport qui nous en a appris beaucoup plus que ce que nous savions sur l'architecture d'Internet. Ces petites boîtes hackées ont rapporté toutes leurs données (un disque entier de 10 To) et ont silencieusement désactivé le hack. C'était un exemple délicieux et utile d'un individu qui a hacké la planète entière. Si ce malware avait été véritablement malveillant, nous aurions été dans la merde.

Et ceci parce que les ordinateurs sont tous aussi inévitablement défectueux : ceux des hôpitaux et des gouvernements et des banques, ceux de votre téléphone, ceux qui contrôlent les feux de signalisation et les capteurs et les systèmes de contrôle du trafic aérien. Chez les industriels, les ordinateurs destinés à maintenir l'infrastructure et la chaîne de fabrication sont encore

pires. Je ne connais pas tous les détails, mais ceux qui sont les plus au courant sont les personnes les plus alcooliques et nihilistes de toute la sécurité informatique. Un autre de mes amis a accidentellement éteint une usine avec un ‘“ping”’ malformé au début d’un test d’intrusion. Pour ceux qui ne savent pas, un ‘“ping”’ est seulement la plus petite requête que vous pouvez envoyer à un autre ordinateur sur le réseau. Il leur a fallu une journée entière tout faire revenir à la normale.

Les experts en informatique aiment prétendre qu’ils utilisent des logiciels d’un genre complètement différent, encore plus géniaux, qu’eux seuls comprennent, des logiciels faits de perfection mathématique et dont les interfaces semblent sortir du cul d’un âne colérique. C’est un mensonge. La forme principale de sécurité qu’ils offrent est celle que donne l’obscurité – il y a si peu de gens qui peuvent utiliser ces logiciels que personne n’a le moindre intérêt à concevoir des outils pour les attaquer. Sauf si, comme la NSA, vous voulez prendre le contrôle sur les administrateurs systèmes.

Une messagerie chiffrée et bien codée, il ne peut rien nous arriver, hein ?

Prenons un exemple que les experts aiment mettre sous le nez des gens normaux qui ne l’utilisent pas : OTR. OTR, ou *Off The Record messaging*, ajoute une couche de chiffrement aux échanges via messagerie instantanée. C’est comme si vous utilisiez AIM ou Jabber et que vous parliez en code sauf que c’est votre ordinateur qui fait le code pour vous. OTR est bien conçu et robuste, il a été audité avec attention et nous sommes bien sûrs qu’il ne contient aucune de ces saloperies de vulnérabilités zéro jour.

Sauf que OTR n’est pas vraiment un programme que vous utilisez tel quel.

Il existe un standard pour le logiciel OTR, et une

bibliothèque, mais elle ne fait rien par elle-même. OTR est implémentée dans des logiciels pour des neuneus par d'autres neuneus. À ce stade, vous savez que ça va se terminer dans les pleurs et les grincements de dents.

La partie principale qu'utilise OTR est un autre programme qui utilise une bibliothèque appelée ‘“libpurple”’. Si vous voulez voir des snobs de la sécurité aussi consternés que les ânes qui ont pondu leur interface, apportez-leur ‘“libpurple”’. ‘“Libpurple”’ a été écrit dans un langage de programmation appelé C.

Le C est efficace dans deux domaines : l'élégance, et la création de vulnérabilités jour zéro critiques en rapport avec la gestion de la mémoire.

Heartbleed, le bogue qui a affecté le monde entier, permettant la fuite de mots de passe et de clés de chiffrement et qui sait quoi encore ? — Du classique et superbe C.

La ‘“libpurple”’ a été écrite par des gens qui voulaient que leur client de discussion *open source* parle à tous les systèmes de messagerie instantanée du monde, et se foutaient complètement de la sécurité ou du chiffrement. Des gens du milieu de la sécurité qui en ont examiné le code ont conclu qu'il y avait tellement de façons d'exploiter la ‘“libpurple”’ que ça n'était probablement pas la peine de la patcher. Elle doit être jetée et réécrite de zéro. Ce ne sont pas des bugs qui permettent à quelqu'un de lire vos messages chiffrés, ce sont des bugs qui permettent à n'importe qui de prendre le contrôle total de votre ordinateur, regarder tout ce que vous tapez ou lisez et même probablement vous regarder vous mettre les doigts dans le nez devant la webcam.

Ce magnifique outil qu'est OTR repose sur la ‘“libpurple”’ dans la plupart des systèmes où il est utilisé. Je dois éclaircir un point, car même certains geeks n'en ont pas conscience : peu importe la force de votre chiffrement si

celui qui vous attaque peut lire vos données par-dessus votre épaule, et je vous promets que c'est possible. Qu'il sache le faire ou pas encore, cela reste néanmoins possible. Il y a des centaines de bibliothèques comme '"libpurple"' sur votre ordinateur : des petits bouts de logiciels conçus avec des budgets serrés aux délais irréalistes, par des personnes ne sachant pas ou ne se souciant pas de préserver la sécurité de votre système.

Chacun de ces petits bugs fera l'affaire quand il s'agit de prendre le contrôle de tout le reste de votre ordinateur. Alors on met à jour, on remet à jour, et peut-être que ça mettra les intrus dehors, ou peut-être pas. On n'en sait rien ! Quand on vous dit d'appliquer les mises à jour, on ne vous dit pas de réparer votre navire. On vous dit de continuer à écoper avant que l'eau n'atteigne votre cou.

(Crédit image : sridgway, licence CC BY 2.0)

Pour prendre un peu de recul par rapport à cette scène d'horreur et de désolation, je dois vous dire que la situation est tout de même meilleure que par le passé. Nous disposons aujourd'hui d'outils qui n'existaient pas dans les années 90, comme le '"sandboxing"', qui permet de confiner des programmes écrits stupidement là où ils ne peuvent pas faire beaucoup de

dégâts. (Le « sandboxing » consiste à isoler un programme dans une petite partie virtuelle de l'ordinateur, le coupant ainsi de tous les autres petits programmes, ou nettoyant tout ce que ce programme essaie de faire avant que d'autres puissent y accéder).

Des catégories entières de bugs horribles ont été éradiqués comme la variole. La sécurité est prise plus au sérieux que jamais, et il y a tout un réseau de personnes pour contrer les logiciels malveillants 24h sur 24. Mais ils ne peuvent pas vraiment garder la main. L'écosystème de ces problèmes est tellement plus vaste qu'il ne l'était ne serait-ce qu'il y a dix ans, qu'on ne peut pas vraiment dire que l'on fait des progrès.

Les gens, eux aussi, sont cassés

« Je vous fais confiance… » est ce que j'aime le moins entendre de la part des mes sources Anonymous. C'est invariablement suivi de bribes d'informations qu'ils n'auraient jamais dû me confier. Il est naturel de partager quelque chose de personnel avec quelqu'un en qui on a confiance. Mais c'est avec exaspération que je dois rappeler aux Anons qu'avant d'être connectés à un autre être humain ils sont d'abord connectés à un ordinateur, relayé à travers un nombre indéterminé de serveurs, switches, routeurs, câbles, liaisons sans fil, et en bout de chaîne, mon ordinateur parfaitement ciblé par les attaques. Tout ceci se déroule le temps d'une longue inspiration. Cela semble une évidence, mais il est bon de le rappeler : les humains ne sont pas conçus pour penser de cette manière.

Personne n'arrive à utiliser les logiciels correctement. Absolument tout le monde se plante. OTR ne chiffre pas avant le premier message, un fait que des éminents professionnels de la sécurité et des hackers qui subissent une chasse à l'homme dans une vingtaine de pays oublient en permanence. Gérer toutes les clés de chiffrement et de déchiffrement dont vous

avez besoin pour garder vos données en sûreté sur plusieurs appareils, sites, et comptes est théoriquement possible, de la même façon que réaliser une appendicectomie sur soi-même est théoriquement possible. *Il y a un gars qui a réussi à le faire en Antarctique, pourquoi pas moi, hein ?*

Tous les experts en programmes malveillants que je connais ont un jour oublié ce que faisait là un certain fichier, ont cliqué dessus pour le voir et ensuite compris qu'ils avaient exécuté un quelconque logiciel malveillant qu'ils étaient censés examiner. Je sais cela parce que ça m'est arrivé une fois avec un PDF dans lequel je savais qu'il y avait quelque chose de mauvais. Mes amis se sont moqués de moi, puis m'ont tous confessé discrètement qu'ils avaient déjà fait la même chose. Si quelques-uns des meilleurs spécialiste de rétro-ingénierie de logiciels malveillants ne peuvent surveiller leurs fichiers malveillants, qu'espérer de vos parents avec cette carte postale électronique qui est prétendument de vous ?

Les pièces jointes exécutables (ce qui inclut les documents Word, Excel, et les PDF) des emails que vous recevez chaque jour peuvent provenir de n'importe qui (on peut écrire à peu près ce que l'on veut dans le champ « De : » d'un email) et n'importe laquelle de ces pièces jointes pourrait prendre le contrôle de votre ordinateur aussi facilement qu'une vulnérabilité jour zéro. C'est certainement de cette façon que votre grand-mère s'est retrouvée à travailler pour des criminels russes, ou que vos concurrents anticipent tous vos plans produits. Mais dans le monde d'aujourd'hui, vous ne pourrez sûrement pas conserver un emploi de bureau si vous refusez d'ouvrir des pièces jointes. Voilà le choix qui s'offre à vous : prendre en permanence le risque de cliquer sur un dangereux programme malveillant, ou vivre sous un pont, laissant sur la pelouse de votre ancienne maison des messages pour dire à vos enfants combien vous les aimez et combien ils vous manquent.

Les experts de la sécurité et de la vie privée sermonnent le public à propos des métadonnées et des réseaux d'échange de données, mais prendre en compte ces choses est aussi naturel que de se faire une batterie de tests sanguins tous les matins, et à peu près aussi facile. Les risques sur le plan sociétal de renoncer à notre vie privée sont énormes. Et pourtant, les conséquences pour chacun de ne pas y renoncer sont immédiatement handicapantes. Il s'agit au final d'un combat d'usure entre ce que l'on veut pour nous-mêmes et nos familles, et ce que l'on doit faire pour vivre dans notre communauté en tant qu'humains – un champ de mines monétisé par les entreprises et monitoré par les gouvernements.

Je travaille en plein là-dedans, et je ne m'en sors pas mieux. J'ai dû une fois suivre un processus pour vérifier mon identité auprès d'un informateur méfiant. J'ai dû prendre une série de photos montrant où je me trouvais ainsi que la date. Je les ai mises en ligne, et on m'a permis de procéder à l'interview. Au final, il se trouve qu'aucune de ces vérifications n'avait été envoyées, parce que j'avais oublié d'attendre la fin du chargement avant d'éteindre nerveusement mon ordinateur. « Pourquoi m'avez-vous quand même permis de vous voir ? » demandais-je à ma source. « Parce qu'il n'y a que vous qui pourrait faire une chose aussi stupide », m'a-t-il répondu.

Touché.

Mais si cela m'arrive à moi, une adulte relativement bien entraînée qui fait attention à ce genre de sujets systématiquement, quelle chance ont les gens avec de vrais boulots et de vraies vies ?

Finalement, c'est la culture qui est cassée.

Il y a quelques années, j'ai rencontré plusieurs personnes respectées qui travaillent dans la confidentialité et la

sécurité logicielle et je leur ai posé une question. Mais d'abord j'ai dû expliquer quelque chose : « La plupart des gens n'ont pas de droits d'administration sur les ordinateurs qu'ils utilisent. »

(Crédit image : amelungc, licence CC BY 2.0)

C'est-à-dire que la plupart des gens qui utilisent un ordinateur dans le monde n'en sont pas propriétaires… Que ce soit dans un café, à l'école, au travail, installer une application bureautique n'est pas directement à la portée d'une grande partie du monde. Toute les semaines ou toutes les deux semaines, j'étais contacté par des gens prêts à tout pour améliorer la sécurité et les options de confidentialité, et j'ai essayé de leur apporter mon aide. Je commençais par « Téléchargez le… » et on s'arrêtait là. Les gens me signalaient ensuite qu'ils ne pouvaient pas installer le logiciel sur leur ordinateur. En général parce que le département informatique limitait leurs droits dans le cadre de la gestion du réseau. Ces gens avaient besoin d'outils qui marchaient sur ce à quoi ils avaient accès, principalement un navigateur.

Donc la question que j'ai posée aux hackers, cryptographes, experts en sécurité, programmeurs, etc. fut la suivante :

quelle est la meilleure solution pour les gens qui ne peuvent pas télécharger de nouveau logiciel sur leurs machines ? La réponse a été unanime : aucune. Il n'y a pas d'alternative. On me disait qu'ils feraient mieux de discuter en texte brut, « comme ça ils n'ont pas un faux sentiment de sécurité ». À partir du moment où ils n'ont pas accès à de meilleurs logiciels, ils ne devraient pas faire quoi que ce soit qui puisse déranger les gens qui les surveillent. Mais, expliquais-je, il s'agit d'activistes, d'organisateurs, de journalistes du monde entier qui ont affaire à des gouvernements et des sociétés et des criminels qui peuvent vraiment leur faire du mal, ces gens sont vraiment en danger. On me répondait alors que dans ce cas, ils devraient s'acheter leurs propres ordinateurs.

Et voilà, c'était ça la réponse : être assez riche pour acheter son propre ordinateur, ou bien littéralement tout laisser tomber. J'ai expliqué à tout le monde que ce n'était pas suffisant, j'ai été dénigrée lors de quelques joutes verbales sans conséquences sur Twitter, et je suis passée à autre chose. Peu de temps après, j'ai compris d'où venait l'incompréhension. Je suis retourné voir les mêmes experts et j'ai expliqué : dans la nature, dans des situations vraiment dangereuses — même quand les gens sont traqués par des hommes avec des armes — quand le chiffrement et la sécurité échouent, personne n'arrête de parler. Ils espèrent seulement ne pas se faire prendre.

La même impulsion humaine qui nous pousse vers le hasard et les loteries depuis des milliers d'années soutient ceux qui luttent même quand les chances sont contre eux. « Peut-être bien que je m'en sortirai, autant essayer ! » Pour ce qui est de l'auto-censure des conversations dans une infrastructure hostile, les activistes non techniques s'en sortent de la même manière que les Anons, ou que les gens à qui l'on dit de se méfier des métadonnées, ou des réseaux d'échanges de données, ou de ce premier message avant que l'encodage OTR ne s'active.

Ils foirent.

Cette conversation a été un signal d'alerte pour quelques personnes de la sécurité qui n'avaient pas compris que les personnes qui devenaient activistes et journalistes faisaient systématiquement des choses risquées. Certains ont rallié mon camp, celui où on perd son temps à des combats futiles sur Twitter et ils ont pris conscience que quelque chose, même quelque chose d'imparfait, pouvait être mieux que rien. Mais beaucoup dans le domaine de la sécurité sont toujours dans l'attente d'un monde parfait dans lequel déployer leur code parfait.

Alors apparaît l'*Intelligence Community* (Communauté du renseignement), ils s'appellent entre eux le IC. Nous pourrions trouver ça sympathique s'ils arrêtaient d'espionner tout le monde en permanence, et eux aimeraient bien que l'on cesse de s'en plaindre. Après avoir passé un peu de temps avec eux, je pense savoir pourquoi ils ne se préoccupent pas de ceux qui se plaignent. Les IC font partie des humains les plus surveillés de l'histoire. Ils savent que tout ce qu'ils font est passé au peigne fin par leurs pairs, leurs patrons, leurs avocats, d'autres agences, le président, et parfois le Congrès. Ils vivent surveillés, et ne s'en plaignent pas.

Dans tous les appels pour augmenter la surveillance, les fondamentaux de la nature humaine sont négligés. Vous n'allez pas apprendre aux espions que ce n'est pas bien en faisant encore plus qu'eux. Il y aura toujours des failles, et tant qu'elles existeront ou pourront être utilisées ou interprétées, la surveillance sera aussi répandue que possible. Les humains sont des créatures généralement égocentriques. Les espions, qui sont humains, ne comprendront jamais pourquoi vivre sans vie privée est mal aussi longtemps qu'ils le feront.

Et pourtant ce n'est pas cela le pire. La catastrophe culturelle qu'ils provoquent rend plus facile leur boulot

d'épier le monde. Les aspects les plus dérangeants des révélations, ce sont le marché des failles *0 day*, l'accumulation des moyens de les exploiter, l'affaiblissement des standards. La question est de savoir qui a le droit de faire partie de ce « nous » qui est censé être préservé de ces attaques, écoutes et décryptages et profilages. Quand ils ont attaqué Natanz avec Stuxnet et laissé tous les autres centres nucléaires vulnérables, nous avons été tranquillement avertis que le « nous » en question commençait et finissait avec l'IC lui-même. Voilà le plus grand danger.

Quand le IC ou le DOD ou le pouvoir exécutif sont les seuls vrais Américains, et que le reste d'entre nous ne sommes que des Américains de deuxième classe, ou pire les non-personnes qui ne sont pas associées aux États-Unis, alors nous ne pouvons que perdre toujours plus d'importance avec le temps. À mesure que nos désirs entrent en conflit avec le IC, nous devenons de moins en moins dignes de droits et de considération aux yeux du IC. Quand la NSA accumule des moyens d'exploiter les failles, et que cela interfère avec la protection cryptographique de notre infrastructure, cela veut dire qu'exploiter des failles contre des gens qui ne sont pas de la NSA ne compte pas tellement. Nous sécuriser passe après se sécuriser eux-mêmes.

En théorie, la raison pour laquelle nous sommes si gentils avec les soldats, que nous avons pour habitude d'honorer et de remercier, c'est qu'ils sont supposés se sacrifier pour le bien des gens. Dans le cas de la NSA, l'inverse s'est produit. Notre bien-être est sacrifié afin de rendre plus aisé leur boulot de surveillance du monde. Lorsque cela fait partie de la culture du pouvoir, on est en bonne voie pour que cela débouche sur n'importe quel abus.

Mais le plus gros de tous les problèmes culturels repose toujours sur les épaules du seul groupe que je n'aie pas encore pris à partie – les gens normaux, qui vivent leurs vies dans cette situation démentielle. Le problème des gens normaux

avec la technologie est le même qu'avec la politique, ou la société en général. Les gens pensent être isolés et sans pouvoir, mais la seule chose qui maintient les gens seuls et sans pouvoir est cette même croyance. Ceux qui travaillent ensemble ont un énorme et terrible pouvoir. Il existe certainement une limite à ce que peut faire un mouvement organisé de personnes qui partagent un rêve commun, mais nous ne l'avons pas encore trouvée.

Facebook et Google semblent très puissants, mais ils vivent à peu près à une semaine de la ruine en permanence. Ils savent que le coût de départ des réseaux sociaux pris individuellement est élevé, mais sur la masse, c'est une quantité négligeable. Windows pourrait être remplacé par quelque chose de mieux écrit. Le gouvernement des États-Unis tomberait en quelques jours devant une révolte générale. Il n'y aurait pas besoin d'une désertion totale ou d'une révolte générale pour tout changer, car les sociétés et le gouvernement préfèreraient se plier aux exigences plutôt que de mourir. Ces entités font tout ce qu'elles peuvent pour s'en sortir en toute impunité – mais nous avons oublié que nous sommes ceux qui les laissons s'en sortir avec ces choses.

Si les ordinateurs ne satisfont pas nos besoins de confidentialité et de communication, ce n'est pas en raison d'une quelconque impossibilité mathématique. Il existe un grand nombre de systèmes qui pourraient chiffrer nos données de façon sécurisée et fédérée, nous disposons de nombreuses façons de retrouver la confidentialité et d'améliorer le fonctionnement par défaut des ordinateurs. Si ce n'est pas ainsi que les choses se passent en ce moment c'est parce que nous n'avons pas exigé qu'il en soit ainsi, et non pas parce que personne n'est assez malin pour que ça arrive.

C'est vrai, les geeks et les PDG et les agents et les militaires ont bousillé le monde. Mais en fin de compte, c'est l'affaire de tous, en travaillant ensemble, de réparer le monde.