Geektionnerd : TrueCrypt

Sources sur Numerama :

- [TrueCrypt ferme pour insécurité, et conseille de faire confiance à… Microsoft]

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

Geektionnerd : Heartbleed

Sources :

- Toute l'actualité sur Heartbleed sur Numerama
- OpenSSL est mort, vive (le futur) LibreSSL sur LinuxFr
- Explication du bug sur XKCD *(en)*

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

Geektionnerd : Fin du support de Windows XP

Lire aussi sur le Framablog :

- Windows XP est mort. Et après ?

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

Geektionnerd : Le goto fail de GnuTLS

Sources :

- GnuTLS sur Wikipédia

- Le fail de GnuTLS sur Numerama
- Le fail d'Apple sur Numerama

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

Mimi & Eunice les bestioles du Libre

Les deux personnages de la mini bande dessinée de Nina Paley se parlent maintenant en français.

— Vous voulez en lire davantage ? Allez voir quel petit cadeau nous vous avons préparé

sur cette page de Framabook

Quel niveau de surveillance

la démocratie peut-elle endurer ? par Richard Stallman

« Le niveau de surveillance actuel dans nos sociétés est incompatible avec les droits de l'homme… »

C'est ce qu'affirme et expose Richard Stallman dans ce long article argumenté en proposant un certain nombre de mesures pour desserrer l'étau.

Sur la photo ci-dessous, on voit Stallman lors d'une conférence en Tunisie muni d'un étrange badge. Il l'a recouvert lui-même de papier aluminium pour ne pas être pisté lors de l'évènement !

Quel niveau de surveillance la

démocratie peut-elle supporter ?

par Richard Stallman

URL d'origine du document (sur GNU.org)

Une première version de cet article a été publiée sur Wired en octobre 2013.

Traduction : aKa, zimadprof, Lamessen, Sylvain, Scailyna, Paul, Asta, Monsieur Tino, Marc, Thérèse, Amine Brikci-N, FF255, Achille, Slystone, Sky, Penguin et plusieurs anonymes
Révision : trad-gnu@april.org – Version de la traduction : 14 août 2014

Grâce aux révélations d'Edward Snowden, nous comprenons aujourd'hui que le niveau de surveillance dans nos sociétés est incompatible avec les droits de l'homme. Le harcèlement répété et les poursuites judiciaires que subissent les opposants, les sources et les journalistes (aux États-Unis et ailleurs) en sont la preuve. Nous devons réduire le niveau de surveillance, mais jusqu'où ? Où se situe exactement le *seuil tolérable de surveillance* que l'on doit faire en sorte de ne pas dépasser ? C'est le niveau au delà duquel la surveillance commence à interférer avec le fonctionnement de la démocratie : lorsque des lanceurs d'alerte comme Snowden sont susceptibles d'être attrapés.

Face à la culture du secret des gouvernements, nous, le peuple,[1] devons compter sur les lanceurs d'alerte pour apprendre ce que l'État est en train de faire. De nos jours, cependant, la surveillance intimide les lanceurs d'alerte potentiels, et cela signifie qu'elle est trop intense. Pour retrouver notre contrôle démocratique sur l'État, nous devons réduire la surveillance jusqu'à un point où les lanceurs d'alerte se sentent en sécurité.

L'utilisation de logiciels libres, comme je la préconise

depuis trente ans, est la première étape dans la prise de contrôle de nos vies numériques – qui inclut la prévention de la surveillance. Nous ne pouvons faire confiance aux logiciels non libres ; la NSA utilise et même crée des failles de sécurité dans des logiciels non libres afin d'envahir nos ordinateurs et nos routeurs. Le logiciel libre nous donne le contrôle de nos propres ordinateurs, mais cela ne protège pas notre vie privée dès l'instant où nous mettons les pieds sur Internet.

Une législation bipartisane ayant pour but de « limiter les pouvoirs de surveillance sur le territoire national » est en cours d'élaboration aux États-Unis mais elle le fait en limitant l'utilisation par le gouvernement de nos dossiers virtuels. Cela ne suffira pas à protéger les lanceurs d'alerte si « capturer le lanceur d'alerte » est un motif valable pour accéder à des données permettant de l'identifier. Nous devons aller plus loin encore.

Le niveau de surveillance à ne pas dépasser dans une démocratie

Si les lanceurs d'alerte n'osent pas révéler les crimes, délits et mensonges, nous perdons le dernier lambeau de contrôle réel qui nous reste sur nos gouvernements et institutions. C'est pourquoi une surveillance qui permet à l'État de savoir qui a parlé à un journaliste va trop loin – au delà de ce que peut supporter la démocratie.

En 2011, un représentant anonyme du gouvernement américain a fait une déclaration inquiétante à des journalistes, à savoir que les États-Unis n'assigneraient pas de reporter à comparaître parce que « nous savons avec qui vous parlez ». Parfois, pour avoir ces renseignements, ils obtiennent les relevés téléphoniques de journalistes par injonction judiciaire, mais Snowden nous a montré qu'en réalité ils adressent des injonctions en permanence à Verizon et aux

autres opérateurs, pour tous les relevés téléphoniques de chaque résident.

Il est nécessaire que les activités d'opposition ou dissidentes protègent leurs secrets des États qui cherchent à leur faire des coups tordus. L'ACLU[2] a démontré que le gouvernement des États-Unis infiltrait systématiquement les groupes dissidents pacifiques sous prétexte qu'il pouvait y avoir des terroristes parmi eux. La surveillance devient trop importante quand l'État peut trouver qui a parlé à une personne connue comme journaliste ou comme opposant.

L'information, une fois collectée, sera utilisée à de mauvaises fins

Quand les gens reconnaissent que la surveillance généralisée atteint un niveau trop élevé, la première réponse est de proposer d'encadrer l'accès aux données accumulées. Cela semble sage, mais cela ne va pas corriger le problème, ne serait-ce que modestement, même en supposant que le gouvernement respecte la loi (la NSA a trompé la cour fédérale de la FISA,[3] et cette dernière a affirmé être incapable, dans les faits, de lui demander des comptes). Soupçonner un délit est un motif suffisant pour avoir accès aux données, donc une fois qu'un lanceur d'alerte est accusé d'« espionnage », trouver un « espion » fournira une excuse pour avoir accès à l'ensemble des informations.

Le personnel chargé de la surveillance d'État a l'habitude de détourner les données à des fins personnelles. Des agents de la NSA ont utilisé les systèmes de surveillance américains pour suivre à la trace leurs petit(e)s ami(e)s – passés, présents, ou espérés, selon une pratique nommée « LOVEINT ». La NSA affirme avoir détecté et puni cette pratique à plusieurs reprises ; nous ne savons pas combien d'autres cas n'ont pas été détectés. Mais ces événements ne devraient pas nous surprendre, parce que les policiers utilisent depuis

longtemps leurs accès aux fichiers des permis de conduire pour pister des personnes séduisantes, une pratique connue sous les termes de « choper une plaque pour un rencard ».

Les données provenant de la surveillance seront toujours détournées de leur but, même si c'est interdit. Une fois que les données sont accumulées et que l'État a la possibilité d'y accéder, il peut en abuser de manière effroyable, comme le montrent des exemples pris en Europe et aux États-Unis.

La surveillance totale, plus des lois assez floues, ouvrent la porte à une campagne de pêche à grande échelle, quelle que soit la cible choisie. Pour mettre le journalisme et la démocratie en sécurité, nous devons limiter l'accumulation des données qui sont facilement accessibles à l'État.

Une protection solide de la vie privée doit être technique

L'Electronic Frontier Foundation et d'autres structures proposent un ensemble de principes juridiques destinés à prévenir les abus de la surveillance de masse. Ces principes prévoient, et c'est un point crucial, une protection juridique explicite pour les lanceurs d'alerte. Par conséquent, ils seraient adéquats pour protéger les libertés démocratiques s'ils étaient adoptés dans leur intégralité et qu'on les faisait respecter sans la moindre exception, à tout jamais.

Toutefois, ces protections juridiques sont précaires : comme nous l'ont montré les récents événements, ils peuvent être abrogés (comme dans la loi dite *FISA Amendments Act*), suspendus ou ignorés.

Pendant ce temps, les démagogues fourniront les excuses habituelles pour justifier une surveillance totale ; toute attaque terroriste, y compris une attaque faisant un nombre réduit de victimes, leur donnera cette opportunité.

Si la limitation de l'accès aux données est écartée, ce sera comme si elle n'avait jamais existé. Des dossiers remontant à des années seront du jour au lendemain exposés aux abus de l'État et de ses agents et, s'ils ont été rassemblés par des entreprises, seront également exposés aux magouilles privées de ces dernières. Si par contre nous arrêtions de ficher tout le monde, ces dossiers n'existeraient pas et il n'y aurait pas moyen de les analyser de manière rétroactive. Tout nouveau régime non libéral aurait à mettre en place de nouvelles méthodes de surveillance, et recueillerait des données à partir de ce moment-là seulement. Quant à suspendre cette loi ou ne pas l'appliquer momentanément, cela n'aurait presque aucun sens.

En premier lieu, ne soyez pas imprudent

Pour conserver une vie privée, il ne faut pas la jeter aux orties : le premier concerné par la protection de votre vie privée, c'est vous. Évitez de vous identifier sur les sites web, contactez-les avec Tor, et utilisez des navigateurs qui bloquent les stratagèmes dont ils se servent pour suivre les visiteurs à la trace. Utilisez GPG (le gardien de la vie privée) pour chiffrer le contenu de vos courriels. Payez en liquide.

Gardez vos données personnelles ; ne les stockez pas sur le serveur « si pratique » d'une entreprise. Il n'y a pas de risque, cependant, à confier la sauvegarde de vos données à un service commercial, pourvu qu'avant de les envoyer au serveur vous les chiffriez avec un logiciel libre sur votre propre ordinateur (y compris les noms de fichiers).

Par souci de votre vie privée, vous devez éviter les logiciels non libres car ils donnent à d'autres la maîtrise de votre informatique, et que par conséquent ils vous espionnent probablement. N'utilisez pas de service se substituant au logiciel : outre que cela donne à d'autres la maîtrise de votre informatique, cela vous oblige à fournir toutes les

données pertinentes au serveur.

Protégez aussi la vie privée de vos amis et connaissances. Ne divulguez pas leurs informations personnelles, sauf la manière de les contacter, et ne donnez jamais à aucun site l'ensemble de votre répertoire téléphonique ou des adresses de courriel de vos correspondants. Ne dites rien sur vos amis à une société comme Facebook qu'ils ne souhaiteraient pas voir publier dans le journal. Mieux, n'utilisez pas du tout Facebook. Rejetez les systèmes de communication qui obligent les utilisateurs à donner leur vrai nom, même si vous êtes disposé à donner le vôtre, car cela pousserait d'autres personnes à abandonner leurs droits à une vie privée.

La protection individuelle est essentielle, mais les mesures de protection individuelle les plus rigoureuses sont encore insuffisantes pour protéger votre vie privée sur des systèmes, ou contre des systèmes, qui ne vous appartiennent pas. Lors de nos communications avec d'autres ou de nos déplacements à travers la ville, notre vie privée dépend des pratiques de la société. Nous pouvons éviter certains des systèmes qui surveillent nos communications et nos mouvements, mais pas tous. Il est évident que la meilleure solution est d'obliger ces systèmes à cesser de surveiller les gens qui sont pas légitimement suspects.

Nous devons intégrer à chaque système le respect de la vie privée

Si nous ne voulons pas d'une société de surveillance totale, nous devons envisager la surveillance comme une sorte de pollution de la société et limiter l'impact de chaque nouveau système numérique sur la surveillance, de la même manière que nous limitons l'impact des objets manufacturés sur l'environnement.

Par exemple, les compteurs électriques « intelligents » sont paramétrés pour envoyer régulièrement aux distributeurs

d’énergie des données concernant la consommation de chaque client, ainsi qu’une comparaison avec la consommation de l’ensemble des usagers. Cette implémentation repose sur une surveillance généralisée mais ce n’est nullement nécessaire. Un fournisseur d’énergie pourrait aisément calculer la consommation moyenne d’un quartier résidentiel en divisant la consommation totale par le nombre d’abonnés, et l’envoyer sur les compteurs. Chaque client pourrait ainsi comparer sa consommation avec la consommation moyenne de ses voisins au cours de la période de son choix. Mêmes avantages, sans la surveillance !

Il nous faut intégrer le respect de la vie privée à tous nos systèmes numériques, dès leur conception.

Remède à la collecte de données : les garder dispersées

Pour rendre la surveillance possible sans porter atteinte à la vie privée, l’un des moyens est de conserver les données de manière dispersée et d’en rendre la consultation malaisée. Les caméras de sécurité d’antan n’étaient pas une menace pour la vie privée. Les enregistrements étaient conservés sur place, et cela pendant quelques semaines tout au plus. Leur consultation ne se faisait pas à grande échelle du fait de la difficulté d’y avoir accès. On les consultait uniquement sur les lieux où un délit avait été signalé. Il aurait été impossible de rassembler physiquement des millions de bandes par jour, puis de les visionner ou de les copier.

Aujourd’hui, les caméras de sécurité se sont transformées en caméras de surveillance ; elles sont reliées à Internet et leurs enregistrements peuvent être regroupés dans un centre de données *[data center]* et conservés ad vitam aeternam. C’est déjà dangereux, mais le pire est à venir. Avec les progrès de la reconnaissance faciale, le jour n’est peut-être pas loin où les journalistes « suspects » pourront être pistés sans

interruption dans la rue afin de surveiller qui sont leurs interlocuteurs.

Les caméras et appareils photo connectés à Internet sont souvent eux-mêmes mal protégés, de sorte que n'importe qui pourrait regarder ce qu'ils voient par leur objectif. Pour rétablir le respect de la vie privée, nous devons interdire l'emploi d'appareils photo connectés dans les lieux ouverts au public, sauf lorsque ce sont les gens qui les transportent. Tout le monde doit avoir le droit de mettre en ligne des photos et des enregistrements vidéo une fois de temps en temps, mais on doit limiter l'accumulation systématique de ces données.

Remède à la surveillance du commerce sur Internet

La collecte de données provient essentiellement des activités numériques personnelles des gens. D'ordinaire, ces sont d'abord les entreprises qui recueillent ces données. Mais lorsqu'il est question de menaces pour la vie privée et la démocratie, que la surveillance soit exercée directement par l'État ou déléguée à une entreprise est indifférent, car les données rassemblées par les entreprises sont systématiquement mises à la disposition de l'État.

Depuis PRISM, la NSA a un accès direct aux bases de données de nombreuses grandes sociétés d'Internet. AT&T conserve tous les relevés téléphoniques depuis 1987 et les met à la disposition de la DEA sur demande, pour ses recherches. Aux États-Unis, l'État fédéral ne possède pas ces données au sens strict, mais en pratique c'est tout comme.

Mettre le journalisme et la démocratie en sécurité exige, par conséquent, une réduction de la collecte des données privées, par toute organisation quelle qu'elle soit et pas uniquement par l'État. Nous devons repenser entièrement les systèmes numériques, de telle manière qu'ils n'accumulent pas de

données sur leurs utilisateurs. S'ils ont besoin de détenir des données numériques sur nos transactions, ils ne doivent être autorisés à les garder que pour une période dépassant de peu le strict minimum nécessaire au traitement de ces transactions.

Une des raisons du niveau actuel de surveillance sur Internet est que le financement des sites repose sur la publicité ciblée, par le biais du pistage des actions et des choix de l'utilisateur. C'est ainsi que d'une pratique simplement gênante, la publicité que nous pouvons apprendre à éviter, nous basculons, en connaissance de cause ou non, dans un système de surveillance qui nous fait du tort. Les achats sur Internet se doublent toujours d'un pistage des utilisateurs. Et nous savons tous que les « politiques relatives à la vie privée » sont davantage un prétexte pour violer celle-ci qu'un engagement à la respecter.

Nous pourrions remédier à ces deux problèmes en adoptant un système de paiement anonyme – anonyme pour l'émetteur du paiement, s'entend (permettre au bénéficiaire d'échapper à l'impôt n'est pas notre objectif). Bitcoin n'est pas anonyme, bien que des efforts soient faits pour développer des moyens de payer anonymement avec des bitcoins. Cependant, la technologie de la monnaie électronique remonte aux années 80 ; tout ce dont nous avons besoin, ce sont d'accords adaptés pour la marche des affaires et que l'État n'y fasse pas obstruction.

Le recueil de données personnelles par les sites comporte un autre danger, celui que des « casseurs de sécurité » s'introduisent, prennent les données et les utilisent à de mauvaises fins, y compris celles qui concernent les cartes de crédit. Un système de paiement anonyme éliminerait ce danger : une faille de sécurité du site ne peut pas vous nuire si le site ne sait rien de vous.

Remède à la surveillance des déplacements

Nous devons convertir la collecte numérique de péage en paiement anonyme (par l'utilisation de monnaie électronique, par exemple). Les système de reconnaissance de plaques minéralogiques reconnaissent toutes les plaques, et les données peuvent être gardées indéfiniment ; la loi doit exiger que seules les plaques qui sont sur une liste de véhicules recherchés par la justice soient identifiées et enregistrées. Une solution alternative moins sûre serait d'enregistrer tous les véhicules localement mais seulement pendant quelques jours, et de ne pas rendre les données disponibles sur Internet ; l'accès aux données doit être limité à la recherche d'une série de plaques minéralogiques faisant l'objet d'une décision de justice.

The U.S. "no-fly" list must be abolished because it is punishment without trial.

Il est acceptable d'établir une liste de personnes pour qui la fouille corporelle et celle des bagages seront particulièrement minutieuses, et l'on peut traiter les passagers anonymes des vols intérieurs comme s'ils étaient sur cette liste. Il est acceptable également d'interdire aux personnes n'ayant pas la citoyenneté américaine d'embarquer sur des vols à destination des États-Unis si elles n'ont pas la permission d'y rentrer. Cela devrait suffire à toutes les fins légitimes.

Beaucoup de systèmes de transport en commun utilisent un genre de carte intelligente ou de puce RFID pour les paiements. Ces systèmes amassent des données personnelles : si une seule fois vous faites l'erreur de payer autrement qu'en liquide, ils associent définitivement la carte avec votre nom. De plus, ils enregistrent tous les voyages associés avec chaque carte. L'un dans l'autre, cela équivaut à un système de surveillance à grande échelle. Il faut diminuer cette collecte de données.

Les services de navigation font de la surveillance : l'ordinateur de l'utilisateur renseigne le service cartographique sur la localisation de l'utilisateur et l'endroit où il veut aller ; ensuite le serveur détermine l'itinéraire et le renvoie à l'ordinateur, qui l'affiche. Il est probable qu'actuellement le serveur enregistre les données de localisation puisque rien n'est prévu pour l'en empêcher. Cette surveillance n'est pas nécessaire en soi, et une refonte complète du système pourrait l'éviter : des logiciels libres installés côté utilisateur pourraient télécharger les données cartographiques des régions concernées (si elles ne l'ont pas déjà été), calculer l'itinéraire et l'afficher, sans jamais dire à qui que ce soit l'endroit où l'utilisateur veut aller.

Les systèmes de location de vélos et autres peuvent être conçus pour que l'identité du client ne soit connue que de la station de location. Au moment de la location, celle-ci informera toutes les stations du réseau qu'un vélo donné est « sorti » ; de cette façon, quand l'utilisateur le rendra, généralement à une station différente, cette station-là saura où et quand il a été loué. Elle informera à son tour toutes les stations du fait que ce vélo a été rendu, et va calculer en même temps la facture de l'utilisateur et l'envoyer au siège social après une attente arbitraire de plusieurs minutes, en faisant un détour par plusieurs stations. Ainsi le siège social ne pourra pas savoir précisément de quelle station la facture provient. Ceci fait, la station de retour effacera toutes les données de la transaction. Si le vélo restait « sorti » trop longtemps, la station d'origine pourrait en informer le siège social et, dans ce cas, lui envoyer immédiatement l'identité du client.

Remède aux dossiers sur les communications

Les fournisseurs de services Internet et les compagnies de téléphone enregistrent une masse de données sur les contacts

de leurs utilisateurs (navigation, appels téléphoniques, etc.) Dans le cas du téléphone mobile, ils enregistrent en outre la position géographique de l'utilisateur. Ces données sont conservées sur de longues périodes : plus de trente ans dans le cas d'AT&T. Bientôt, ils enregistreront même les mouvements corporels de l'utilisateur. Et il s'avère que la NSA collecte les coordonnées géographiques des téléphones mobiles, en masse.

Les communications non surveillées sont impossibles là où le système crée de tels dossiers. Leur création doit donc être illégale, ainsi que leur archivage. Il ne faut pas que les fournisseurs de services Internet et les compagnies de téléphone soient autorisés à garder cette information très longtemps, sauf décision judiciaire leur enjoignant de surveiller une personne ou un groupe en particulier.

Cette solution n'est pas entièrement satisfaisante, car cela n'empêchera pas concrètement le gouvernement de collecter toute l'information à la source – ce que fait le gouvernement américain avec certaines compagnies de téléphone, voire avec toutes. Il nous faudrait faire confiance à l'interdiction par la loi. Cependant, ce serait déjà mieux que la situation actuelle où la loi applicable (le PATRIOT Act) n'interdit pas clairement cette pratique. De plus, si un jour le gouvernement recommençait effectivement à faire cette sorte de surveillance, il n'obtiendrait pas les données sur les appels téléphoniques passés avant cette date.

Pour garder confidentielle l'identité des personnes avec qui vous échangez par courriel, une solution simple mais partielle est d'utiliser un service situé dans un pays qui ne risquera jamais de coopérer avec votre gouvernement, et qui chiffre ses communications avec les autres services de courriels. Toutefois, Ladar Levison (propriétaire du service de courriel Lavabit que la surveillance américaine a cherché à corrompre complètement) a une idée plus sophistiquée : établir un système de chiffrement par lequel votre service de courriel

saurait seulement que vous avez envoyé un message à un utilisateur de mon service de courriel, et mon service de courriel saurait seulement que j'ai reçu un message d'un utilisateur de votre service de courriel, mais il serait difficile de déterminer que c'était moi le destinataire.

Mais un minimum de surveillance est nécessaire.

Pour que l'État puisse identifier les auteurs de crimes ou délits, il doit avoir la capacité d'enquêter sur un délit déterminé, commis ou en préparation, sur ordonnance du tribunal. À l'ère d'Internet, il est naturel d'étendre la possibilité d'écoute des conversations téléphoniques aux connexions Internet. On peut, certes, facilement abuser de cette possibilité pour des raisons politiques, mais elle n'en est pas moins nécessaire. Fort heureusement, elle ne permettrait pas d'identifier les lanceurs d'alerte après les faits, si (comme je le recommande) nous empêchons les systèmes numériques d'accumuler d'énormes dossiers avant les faits.

Les personnes ayant des pouvoirs particuliers accordés par l'État, comme les policiers, abandonnent leur droit à la vie privée et doivent être surveillés (en fait, les policiers américains utilisent dans leur propre jargon le terme *testilying*[4] au lieu de *perjury*[5] puisqu'ils le font si souvent, en particulier dans le cadre de la comparution de manifestants et de photographes). Une ville de Californie qui a imposé à la police le port permanent d'une caméra a vu l'usage de la force diminuer de près de 60 %. L'ACLU y est favorable.

Les entreprises ne sont pas des personnes et ne peuvent se prévaloir des droits de l'homme. Il est légitime d'exiger d'elles qu'elles rendent public le détail des opérations susceptibles de présenter un risque chimique, biologique, nucléaire, financier, informatique (par exemple les DRM) ou politique (par exemple le lobbyisme) pour la société, à un

niveau suffisant pour assurer le bien-être public. Le danger de ces opérations (pensez à BP et à la marée noire dans le Golfe du Mexique, à la fusion du cœur des réacteurs nucléaires de Fukushima ou à la crise financière de 2008) dépasse de loin celui du terrorisme.

Cependant, le journalisme doit être protégé contre la surveillance, même s'il est réalisé dans un cadre commercial.

La technologie numérique a entraîné un accroissement énorme du niveau de surveillance de nos déplacements, de nos actions et de nos communications. Ce niveau est bien supérieur à ce que nous avons connu dans les années 90, bien supérieur à ce qu'ont connu les gens habitant derrière le rideau de fer dans les années 80, et il resterait encore bien supérieur si l'utilisation de ces masses de données par l'État était mieux encadrée par la loi.

A moins de croire que nos pays libres ont jusqu'à présent souffert d'un grave déficit de surveillance, et qu'il leur faut être sous surveillance plus que ne le furent jadis l'Union soviétique et l'Allemagne de l'Est, ils nous faut inverser cette progression. Cela requiert de mettre fin à l'accumulation en masse de données sur la population.

Notes :

Notes de traduction

1. Allusion probable à la Constitution de 1787, symbole de la démocratie américaine, qui débute par ces mots : *We, the people of the United States* (Nous, le peuple des États-Unis). ?
2. Union américaine pour les libertés civiles. ?
3. Loi sur la surveillance du renseignement étranger ; elle

a mis en place une juridiction spéciale, la FISC, chargée de juger les présumés agents de renseignement étrangers sur le sol américain. ?
4. *Testilying* : contraction de *testify*, faire une déposition devant un tribunal, et *lying*, acte de mentir. ?
5. *Perjury* : faux témoignage. ?

Le chiffrement, maintenant (7)

Tails : un système live anonyme et amnésique

L'utilisation de « systèmes crypto implémentés proprement » a une courbe d'apprentissage énorme et nécessite des utilisateurs dévoués qui soient prêts à travailler un peu plus pour reprendre le contrôle de leur vie privée. C'est principalement pour cette raison que OTR et PGP ne sont pas largement répandus. Mais même en utilisant ces outils, comment être sûr d'avoir une sécurité « de bout en bout » quand vous ne pouvez pas forcément faire confiance à votre système d'exploitation ou aux autres logiciels que vous utilisez tous les jours ?

La solution consiste à utiliser un système d'exploitation totalement différent composé uniquement de « logiciels de confiance » quand vous avez besoin d'une confidentialité absolue. Tails vous aide à résoudre ce problème.

Tails est un système live dont le but est de préserver votre

> *vie privée et votre anonymat. Il vous permet d'utiliser Internet de manière anonyme et de contourner la censure quasiment partout où vous allez et sur n'importe quel ordinateur. Tails ne laisse aucune trace de ce que vous avez fait, sauf si vous le demandez explicitement.*
>
> *Tails est un système d'exploitation complet destiné à être utilisé depuis un DVD ou une clef USB indépendamment du système installé sur l'ordinateur. C'est un logiciel libre basé sur Debian GNU/Linux.*
>
> *Tails est livré avec de nombreuses applications, configurées avec une attention particulière accordée à la sécurité : navigateur web, client de messagerie instantanée, client email, suite bureautique, éditeur d'image et de son, etc.*

Tails n'est pas destiné à tout le monde. Il est toujours difficile de le comparer à un système d'exploitation classique. Il est lent, il ne comporte pas tous les logiciels que vous pourriez vouloir. Mais Tails a ces particularités parce qu'il a été conçu spécifiquement pour être plus difficile de compromettre la protection des points d'accès. Si vous êtes dans une situation qui vous fait penser que la NSA ou n'importe quel attaquant potentiel peut vous cibler vous et vos collègues (les journalistes ou les relations des lanceurs d'alarme me viennent à l'esprit), c'est l'un des meilleurs outils disponibles.

Comme Tails n'est pas pratique pour une utilisation quotidienne de l'ordinateur, c'est une bonne idée de s'habituer à utiliser OTR et PGP sur votre système d'exploitation principal autant que possible. Tails n'aide pas à adoucir les effets de la surveillance en elle-même, mais chiffrer autant que possible les actions quotidiennes le permettra.

À chaque fois que vous lancez Tails, vous démarrez sur un système propre. Tout ce que vous avez fait lors de vos

précédentes sessions sur Tails est effacé et vous repartez de l'état initial. Ce qui signifie que si vous avez été infecté par un malware en utilisant Tails, celui-ci aura disparu à votre prochaine connexion.

Vous pouvez commencer à utiliser Tails en téléchargeant l'image ISO et en la gravant sur un DVD. Vous devez alors démarrer sur le DVD. Cette étape dépend de votre modèle d'ordinateur, mais nécessite généralement d'entrer dans le BIOS et de changer l'ordre de démarrage de votre ordinateur de façon à ce qu'il tente de démarrer sur le DVD avant d'essayer sur votre disque dur. Sur les nouveaux PC, vous devrez peut-être désactiver le « secure boot » de l'UEFI : il s'agit du crypto utilisé pour être sûr que votre ordinateur ne va démarrer que sur une version de Windows signée numériquement (ce qui, en fait, rend le démarrage sur un système d'exploitation non-Windowsien plus difficile). Le site web de Tails propose davantage d'informations sur les outils de démarrage sur un DVD ou une clé USB.

Après avoir démarré sur le DVD, vous avez la possibilité d'installer Tails sur une clé USB. C'est particulièrement utile car cela permet de configurer un volume persistant, c'est à dire une partie de votre clé USB chiffrée pour stocker vos données. Malgré le retour à un espace propre à chaque démarrage, il est important de pouvoir accéder à vos clés OTR et PGP, vos configurations Claws mail (voir plus bas) et Pidgin ainsi que les documents sur lesquels vous travaillez. Votre volume persistant vous permet tout ceci.

PGP et courriels sur Tails

Je parlais de l'utilisation de Thunderbird avec l'add-on Enigmail pour accéder à vos courriels et utiliser PGP. Cependant, ce logiciel n'est pas fourni avec Tails. Tails est livré avec Claws Mail qui comprend un plug-in PGP.

Au lieu d'utiliser l'interface graphique utilisateur du

gestionnaire de clé d'Enigmail pour importer, exporter, générer et voir le détail des clés signées, vous pouvez cliquer sur l'icône du presse-papiers en haut à droite de l'écran et choisir le gestionnaire de clés pour ouvrir SeaHorse, qui propose ces mêmes fonctions.

Procédure

Pour commencer à avoir un espace de communication privé avec vos amis et collègues, et disposant d'un haut niveau de sécurité des points d'accès, voici les étapes à suivre.

- Rencontrez vos amis en face à face. Chacun devra apporter son propre PC portable ou clé USB.
- Téléchargez et gravez un DVD de Tails, puis démarrez dessus et créez une clé USB pour chaque personne.
- Quand tout le monde a sa clé USB Tails, chacun doit démarrer dessus sur son propre PC et configurer un volume persistant. Une fois que ce volume est chiffré, chacun peut générer sa propre phrase de passe sécurisée qu'il devra entrer à chaque démarrage sur Tails, avant de redémarrer sur son PC avec Tails et cette fois monter le volume persistant.
- Chacun crée alors un nouveau pseudo pour compte Jabber. L'une des solutions est d'aller sur https://register.jabber.org depuis iceweasel. Comme Tails fait transiter les échanges internet via Tor, cela permet bien de créer un compte jabber anonyme.
- Chacun ouvre alors Pidgin et le configure en utilisant ce nouveau compte Jabber et crée une nouvelle clé OTR. Chacun ajoute les autres dans sa liste d'amis et démarre une session OTR avec les autres. Une fois que tout le monde est dans la même discussion, c'est le moment idéal pour comparer les empreintes et vérifier l'identité de chaque personne afin de pouvoir communiquer de façon sécurisée via internet à l'avenir.
- Chacun devrait se créer une nouvelle adresse de courriel

de la même façon. Certains fournisseurs de courriels, comme Gmail, rendent difficile la création de nouveaux comptes en utilisant Tor et en restant anonyme. Dans ce cas, utilisez un autre fournisseur de courriels. Assurez-vous que celui-ci supporte IMAP (de façon à pouvoir utiliser un client de messagerie courriel) à travers un SSL (pour que votre client de messagerie utilise une communication chiffré avec le serveur courriel). Si vous choisissez tous le même fournisseur de courriels, envoyer des courriels entre les comptes ne devrait jamais quitter le serveur, ce qui réduit les métadonnées disponibles relatives à votre utilisation du courrier électronique pour ceux qui surveillent internet.

- Chacun devra générer une nouvelle clé PGP pour son adresse de courriel. comme pour le chiffrage du disque, il est important de choisir une phrase de passe complexe au moment de cette génération de clé PGP.
- Le client de messagerie compatible PGP livré avec Tails s'apelle Claws Mail. Chacun doit configurer Claws Mail pour utiliser sa nouvelle adresse courriel, et envoyer une copie de sa clé publique aux autres personnes présentes dans votre réunion. Puis chacun devra importer la clé publique des autres dans son propre trousseau de clé, puis vérifier manuellement l'empreinte PGP. Ne sautez pas cette étape. Finalement, chacun devra avoir un trousseau de clé contenant les clés signées de tous les autres.

Si quelqu'un de malveillant vole physiquement votre clé USB Tails, la modifie et vous la rend, il peut compromettre toute la sécurité de Tails. C'est pour cela qu'il est très important de toujours garder votre clé USB avec vous.

Si le directeur de la CIA David Petraeus (général 4 étoiles à la retraite) et sa biographe Paula Broadwell avaient décidé d'utiliser Tails, OTR et PGP, leur liaison extra-conjugale

serait sans doute restée secrète.

Comment la NSA déploie des logiciels malveillants

Nouvelles révélations, nouvelles précautions

Nous reprenons ici l'article récemment publié par KoS, il s'agit de la traduction française de l'article de l'Electronic Frontier Foundation : How The NSA Deploys Malware: An In-Depth Look at the New Revelations par : Sphinx, KoS, Scailyna, Paul, Framatophe et 2 auteurs anonymes

– – – – – –

Nous avons longtemps suspecté que la NSA, la plus grande agence d'espionnage du monde, était plutôt douée pour pénétrer les ordinateurs. Désormais, grâce à un article de Bruce Schneier, expert en sécurité qui travaille avec The Guardian sur les documents de Snowden, nous avons une vision bien plus détaillée de la manière dont la NSA utilise des failles pour infecter les ordinateurs d'utilisateurs ciblés.

La méthode utilisée par la NSA pour attaquer les gens avec des logiciels malveillants est largement utilisée par les criminels et les fraudeurs ainsi que par les agences de

renseignement, il est donc important de comprendre et de se défendre contre cette menace pour éviter d'être victime de cette pléthore d'attaquants.

Comment fonctionnent les logiciels malveillants exactement ?

Déployer un logiciel malveillant via le Web nécessite généralement deux étapes. Premièrement, en tant qu'attaquant, vous devez attirer votre victime sur un site web que vous contrôlez. Deuxièmement, vous devez installer un logiciel sur l'ordinateur de la victime pour prendre le contrôle de sa machine. Cette formule n'est pas universelle, mais c'est souvent ainsi que les attaques sont exécutées.

Pour mener à bien la première étape, qui consiste à amener un utilisateur à visiter un site sous le contrôle de l'attaquant, ce dernier peut envoyer à la victime un courriel avec un lien vers le site web concerné : c'est ce que l'on appelle une attaque par hameçonnage (*phishing*). La NSA aurait parfois eu recours à ce type d'attaque, mais nous savons à présent que cette étape était généralement accomplie via une méthode dite de « l'homme du milieu » (*man-in-the-middle*)[1]. La NSA contrôle un ensemble de serveurs dont le nom de code est « Quantum », situés sur les dorsales Internet et ces serveurs sont utilisés pour rediriger les cibles vers d'autres serveurs contrôlés par la NSA et chargés d'injecter le code malveillant.

Dans ce cas, si un utilisateur ciblé visite, par exemple, le site yahoo.com, son navigateur affichera la page d'accueil ordinaire de Yahoo! mais sera en réalité en communication avec un serveur contrôlé par la NSA. La version malveillante du site web de Yahoo! demandera au navigateur de l'utilisateur d'adresser une requête à un autre serveur contrôlé par la NSA et chargé de diffuser le code néfaste.

Quand un utilisateur ciblé visite un site web mal intentionné, quels moyens l'attaquant utilise-t-il pour infecter

l'ordinateur de la victime ? Le moyen le plus direct est probablement d'amener l'utilisateur à télécharger et à exécuter un logiciel. Une publicité intelligemment conçue s'affichant dans une fenêtre pop-up peut convaincre un utilisateur de télécharger et d'installer le logiciel malveillant de l'attaquant.

Toutefois, cette méthode ne fonctionne pas toujours et repose sur une initiative de l'utilisateur visé, qui doit télécharger et installer le logiciel. Les attaquants peuvent choisir plutôt d'exploiter des vulnérabilités du navigateur de la victime pour accéder à son ordinateur. Lorsqu'un navigateur charge une page d'un site, il exécute des tâches telles que l'analyse du texte envoyé par le serveur et il arrive souvent qu'il charge des greffons (plugins) tels que Flash pour l'exécution de code envoyé par le serveur, sans parler du code JavaScript que peut aussi lui envoyer le serveur. Or, les navigateurs, toujours plus complexes à mesure que le web s'enrichit en fonctionnalités, ne sont pas parfaits. Comme tous les logiciels, ils ont des bogues, et parfois ces bogues sont à la source de vulnérabilités exploitables par un attaquant pour prendre le contrôle d'un ordinateur sans que la victime ait autre chose à faire que visiter un site web particulier. En général, lorsque les éditeurs de navigateurs découvrent des vulnérabilités, ils les corrigent, mais un utilisateur utilise parfois une version périmée du navigateur, toujours exposée à une attaque connue publiquement. Il arrive aussi que des vulnérabilités soient uniquement connues de l'attaquant et non de l'éditeur du navigateur ; ce type de vulnérabilité est appelée *vulnérabilité zero-day*.

La NSA dispose d'un ensemble de serveurs sur l'internet public désignés sous le nom de code « FoxAcid », dont le but est de déployer du code malveillant. Une fois que des serveurs Quantum ont redirigé une cible vers une URL spécialement forgée et hébergée sur un serveur FoxAcid, un logiciel installé sur ce serveur se sert d'une boîte à outils

d’exploitation de failles pour accéder à l’ordinateur de l’utilisateur. Cette boîte à outils couvre vraisemblablement des vulnérabilités connues, utilisables contre des logiciels périmés, et des vulnérabilités *zero-day*, en règle générale réservées à des cibles de haute valeur [2]. Nos sources indiquent que l’agence utilise ensuite ce code malveillant initial pour installer d’autres logiciels à le plus long terme.

Quand un attaquant réussit à infecter une victime avec du code malveillant, il dispose d’ordinaire d’un accès complet à l’ordinateur de cette dernière : il peut enregistrer les saisies du clavier (qui peuvent révéler mots de passe et autres informations sensibles), mettre en route la webcam ou lire n’importe quelle donnée conservée sur cet ordinateur.

Que peuvent faire les utilisateurs pour se protéger ?

Nous espérons que ces révélations pousseront les éditeurs de navigateurs à agir, que ce soit pour renforcer leurs logiciels contre les failles de sécurité ou pour tenter de détecter et de bloquer les URL utilisées par les serveurs FoxAcid.

Entre-temps, les utilisateurs soucieux de leur sécurité s’efforceront de suivre des pratiques de nature à assurer leur sécurité en ligne. Gardez toujours vos logiciels à jour, en particulier les greffons des navigateurs tels que Flash, qui nécessitent des mises à jour manuelles. Assurez-vous de bien faire la différence entre les mises à jour légitimes et les avertissements sous forme de pop-ups qui se font passer pour des mises à jour. Ne cliquez jamais sur un lien suspect dans un courriel.

Les utilisateurs qui souhaitent aller un pas plus loin – selon nous, tout le monde devrait se sentir concerné –, utiliseront l’activation en un clic de greffons Flash ou Java de manière à ce que ces derniers ne soient exécutés sur une page web qu’à

la condition que l'utilisateur l'approuve. Pour Chromium et Chrome, cette option est disponible dans Paramètres => Afficher les paramètres avancés => Confidentialité => Paramètres du contenu => Plug-ins.

La même chose peut être faite pour Firefox à l'aide d'une extension comme Click to Play per-element. Les greffons peuvent également être désactivés ou complètement désinstallés. Les utilisateurs devraient également utiliser un bloqueur de publicité afin d'empêcher les requêtes superflues du navigateur destinées aux publicitaires et aux pisteurs du web. Ils devraient en outre utiliser l'extension HTTPS Everywhere afin d'utiliser le chiffrement des connexions associées à HTTPS sur le plus de sites possibles.

Si vous êtes un utilisateur prêt à supporter quelques désagréments au bénéfice d'une navigation plus sûre, regardez du côté de NotScripts (Chrome) ou de NoScript (Firefox), qui permettent de limiter l'exécution des scripts. Cela signifie qu'il vous sera nécessaire d'autoriser par un clic l'exécution des scripts un à un. JavaScript étant très répandu, attendez-vous à devoir cliquer très souvent. Les utilisateurs de Firefox peuvent s'orienter vers une autre extension utile, RequestPolicy, qui bloque le chargement par défaut des ressources tierces sur une page. Ici aussi, votre navigation ordinaire pourrait être perturbée car les ressources tierces sont très utilisées.

Enfin, pour les plus paranoïaques, HTTP Nowhere permettra de désactiver l'ensemble du trafic HTTP, avec pour conséquence que votre navigation sera entièrement chiffrée et, par la même occasion, limitée aux seuls sites offrant une connexion HTTPS.

Conclusion

Le système de la NSA pour déployer les logiciels malveillants n'a rien de particulièrement novateur, mais avoir un aperçu de la façon dont il opère devrait aider les utilisateurs et les

éditeurs de logiciels et de navigateurs à mieux se défendre contre ces types d'attaques, et contribuer à une meilleure protection de tous contre les criminels, les agences de renseignement et une pléthore d'autres attaquants. C'est pourquoi nous jugeons vital que la NSA soit transparente quant à ses capacités et aux failles ordinaires de sécurité auxquelles nous sommes exposés – notre sécurité en ligne en dépend.

---

1. Le terme « homme du milieu » est parfois réservé aux attaques sur les connexions sécurisées par cryptographie, par exemple au moyen d'un certificat SSL frauduleux. Dans cet article, toutefois, on entend plus généralement toute attaque où l'attaquant s'interpose entre un site et la victime.
2. D'après l'article de The Guardian, « Les exploits les plus précieux sont réservés aux cibles les plus importantes ».