Applis de traçage : scénarios pour les non-spécialistes

Un document de plus sur les dangers de l'application de traçage ? Nous n'allons pas reproduire ici les 13 pages documentées et augmentées de notes de référence d'une équipe de 14 spécialistes en cryptographie :

Xavier Bonnetain, University of Waterloo, Canada ; Anne Canteaut, Inria ; Véronique Cortier, CNRS, Loria ; Pierrick Gaudry, CNRS, Loria ; Lucca Hirschi, Inria ; Steve Kremer, Inria ; Stéphanie Lacour, CNRS ; Matthieu Lequesne, Sorbonne Université et Inria ; Gaëtan Leurent, Inria ; Léo Perrin, Inria ; André Schrottenloher, Inria ; Emmanuel Thomé, Inria ; Serge Vaudenay, EPFL, Suisse ; Christophe Vuillot, Inria.

… mais ils ont fait un effort tout à fait louable de pédagogie pour qu'au-delà des problèmes techniques réels, nous comprenions tous. Le document s'intitule : **Le traçage anonyme, dangereux oxymore, Analyse de risques à destination des non-spécialistes**

Nous vous invitons évidemment à en découvrir l'intégralité, mais voici simplement les cas fictifs (hélas réalistes), les scénarios que les spécialistes nous proposent.

Au moment où va peut-être se déclencher une offensive médiatique *en faveur* d'une application de surveillance de la part du gouvernement ou de Google+Apple, il n'est probablement pas inutile d'avoir *des exemples simples et faciles à comprendre* pour expliquer notre opposition.

Nous avons ajouté en complément la conclusion de l'ensemble du document qui précise clairement les limites de toute solution technique et les valeurs que doit respecter l'informatique. Que les auteurs soient vivement remerciés de cet exercice d'éducation de tous qu'ils ont eu l'excellente idée de placer

⇒ **Accéder aux articles déjà publiés dans notre dossier StopCovid**

---

1. Fausse déclaration

Le joueur de foot Gronaldo doit disputer le prochain match de Ligue des champions. Pour l'empêcher de jouer, il suffit pour un adversaire de laisser son téléphone à côté de celui de Gronaldo à son insu, puis de se déclarer malade. Gronaldo recevra une alerte, car il aurait été en contact avec une personne infectée, et devra rester 14 jours éloigné des terrains

2. Le suspect unique

M. Lambda qui, pour éviter la contamination, ne sort de chez lui que pour faire ses courses à l'épicerie du quartier, reçoit une notification de son téléphone. Il en déduit que le responsable n'est autre que l'épicier.

3. Croisement d'informations

Mme Toutlemonde qui, elle, croise beaucoup de gens dans la journée, reçoit une notification. Il lui suffit de discuter quelques instants avec son voisin de palier et un collègue de bureau, pour savoir que le malade ne fait pas partie de son entourage professionnel, mais qu'il habite l'immeuble. Grâce à ces indices, elle suspecte fortement (peut-être à tort) M. Harisk du 3^{e} étage, qui est ambulancier, d'avoir contaminé tous ses voisins. Elle s'empresse de prévenir le reste des habitants de l'immeuble via les réseaux sociaux.

4. Mes voisins sont-ils malades ?

M. Ipokondriac voudrait savoir si ses voisins sont malades. Il récupère son vieux téléphone dans un placard, y installe l'application TraceVIRUS, et le laisse dans sa boîte aux lettres en bas de l'immeuble. Tous les voisins passent à côté à chaque fois qu'ils rentrent chez eux, et le téléphone recevra une notification si l'un d'entre eux est malade.

5. Candidat à l'embauche

L'entreprise RIPOUE souhaite recruter une personne pour un CDD. Elle veut s'assurer que le candidat ne tombe pas malade entre l'entretien d'embauche et la signature du contrat. Elle utilise donc un téléphone dédié qui est allumé uniquement pendant l'entretien, et qui recevra une alerte si le candidat est testé positif plus tard.

6. Les paparazzi

M. Paparazzo cherche des informations sur la vie privée de Mme Star. Il soudoie Mme Rimelle, la maquilleuse qui intervient sur le tournage de son dernier film pour qu'elle allume un téléphone dédié et qu'elle le place à proximité de celui de Mme Star. M. Paparazzo récupère ensuite le téléphone. Il recevra une notification si Mme Star est infectée par le virus.

7. Le militant antisystème

M. Hanty, qui présente des symptômes du COVID-19, est un militant antisystème. Pour dénoncer la mise en place de l'application TraceVIRUS, il attache son téléphone à son chien, et le laisse courir dans le parc toute la journée. Le lendemain il va voir le médecin et il est testé positif ; tous les promeneurs reçoivent une notification.

8. L'ingérence étrangère

Le sous-marin Le Terrifiant doit appareiller dans quelques jours, mais Jean Bond est un agent étranger qui veut empêcher son départ. Il recrute Mata-Hatchoum qui présente des

symptômes, et lui demande de faire le tour des bars de marins. Mata-Hatchoum va ensuite se faire tester, et 5 marins reçoivent une notification de l'application. Le Terrifiant est obligé de rester à quai.

9. L'élève Ducovid

L'élève Ducovid a un contrôle de français la semaine prochaine, mais il n'a pas lu l'œuvre au programme. Grâce à une petite annonce, il trouve M. Enrumais qui présente des symptômes et accepte de lui prêter son téléphone. Il fait passer le téléphone de M. Enrumais dans toute la classe, puis le laisse traîner en salle des profs. Il le rend ensuite à M. Enrumais, qui va voir un médecin. Le médecin constate que M. Enrumais est malade du COVID et le déclare dans l'application du téléphone. Ceci déclenche une alerte pour toute la classe et pour tous les professeurs, le lycée est fermé !

10. Le cambriolage

M. Rafletou veut cambrioler la maison de l'oncle canard. Avant d'entrer, il utilise une antenne pour détecter les signaux Bluetooth. Il sait que l'oncle canard utilise TraceVIRUS, et s'il n'y a pas de signal c'est que la maison est vide.

11. Le centre commercial

Le centre commercial La Fayote veut protéger ses clients, et refuser ceux qui n'utilisent pas l'application TraceVIRUS. Comme l'application diffuse régulièrement des messages, il suffit que le vigile à l'entrée utilise une antenne Bluetooth pour détecter les clients qui utilisent l'application, et ceux qui ne l'utilisent pas.

12. L'application GeoTraceVIRUS

Peu après avoir installé l'applicationTraceVIRUS, Mme Toutlemonde entend parler de l'application GeoTraceVIRUS qui réutilise les informations TraceVIRUS pour localiser les malades. Mme Toutlemonde apprend ainsi qu'un malade s'est

rendu samedi dernier au supermarché PetitPrix. Par crainte (peut-être infondée) d'attraper le virus, elle ne fera pas ses courses chez PetitPrix cette semaine.

13. L'assurance

La chaîne de supermarché SansScrupule utilise des traceurs Bluetooth pour suivre les clients dans ses magasins. Ils relient l'identifiant Bluetooth à l'identité réelle à partir de l'application MySansScrupule, ou avec les cartes bancaires lors du passage en caisse. Pendant que M. Lambda fait ses courses, ils peuvent simuler un contact avec son téléphone, et ils seront donc prévenus si M. Lambda est malade. Cette information sera transmise au service assurance du groupe.

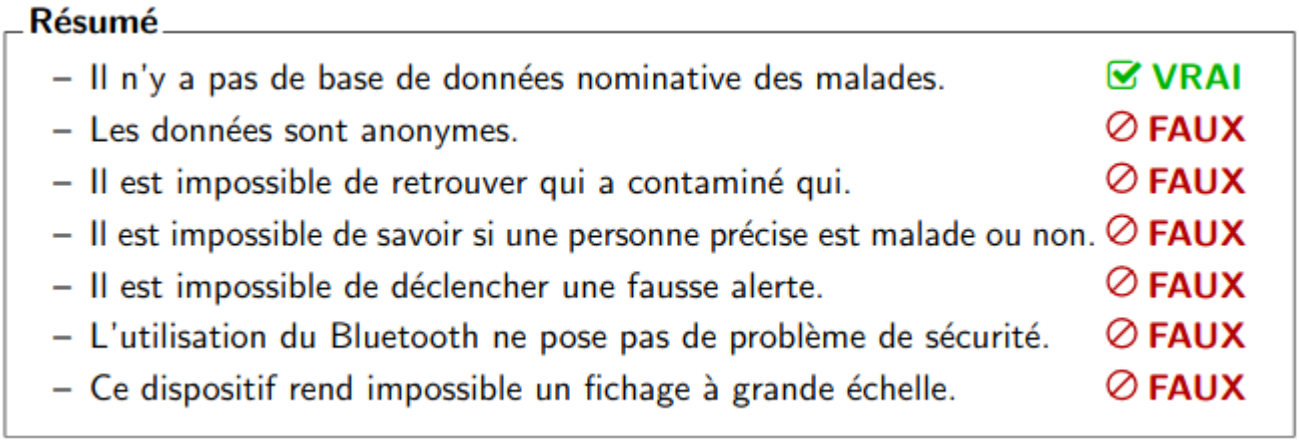
14. Le malware

Mme Toutlemonde a installé l'application chatsMignons sur son téléphone, sans savoir que c'est un logiciel espion (un « malware ») qui l'espionne. Après avoir déclaré dans TraceVIRUS qu'elle est malade, elle reçoit un message pour la faire chanter, menaçant de révéler sa maladie à son assurance et à son employeur qui risque de mettre fin à sa période d'essai. Une autre activité lucrative du crime organisé, très facile à mettre en œuvre dans certains des systèmes de traçage proposés, consisterait à garantir, moyennant finances, la mise en quatorzaine obligatoire de personnes ciblées.

15. Vente d'alertes positives

Don Covideone vend une application InfecteTonVoisin sur Internet. Après avoir téléchargé l'application, il suffit d'approcher son téléphone d'une personne pour qu'elle reçoive une notification lui signalant qu'elle est à risque. Les attaques sont désormais possibles sans compétence technique. Ainsi, Monsieur Bouque-Maeker compte parier lors du prochain match de Ligue des champions. Par chance, il assistera à la conférence de presse de Gronaldo. Il mise alors fortement sur l'équipe adverse, pourtant donnée perdante à 10 contre 1. Il télécharge l'application InfecteTonVoisin et approche son

téléphone de Gronaldo pendant l'interview. Gronaldo reçoit une alerte, il ne pourra pas disputer le match. Son équipe perd et Monsieur Bouque-Maeker remporte la mise !
[L'image ci-dessous résume l'ensemble de l'argumentaire de 13 pages, pas seulement les cas de figure plus haut mentionnés.]



Conclusion

Le traçage des contacts pose de nombreux problèmes de sécurité et de respect de la vie privée, et les quelques scénarios que nous avons présentés n'illustrent qu'un petit nombre des détournements possibles. À cet égard, la cryptographie n'apporte que des réponses très partielles.

Nombre des situations que nous avons présentées exploitent en effet les fonctionnalités de ce type de technique, plutôt que leur mise en œuvre. **Dès lors, l'arbitrage de ces risques ne pourra pas être résolu par la technique.** Il relève de choix politiques qui mettront en balance les atteintes prévisibles aux droits et libertés fondamentaux et les bénéfices potentiels qui peuvent être espérés dans la lutte contre l'épidémie. À notre connaissance, l'estimation des bénéfices d'un éventuel traçage numérique est aujourd'hui encore très incertaine, alors même que les scénarios que nous avons développés ici sont, eux, connus et plausibles.

Un principe essentiel en sécurité informatique est que

l'innocuité d'un système ne doit en aucun cas être présumée en comptant sur l'honnêteté de certains de ses acteurs. Ce même principe apparaît dans l'évolution de notre droit en matière de protection des données à caractère personnel. Si, avec la loi « Informatique et libertés » de 1978, c'était de la part des pouvoirs publics, et singulièrement de l'état, que des dérives étaient redoutées, les acteurs privés puis, à travers le RGPD, tous les acteurs de la société ont été associés à ces craintes. Les atteintes que les systèmes de traçage peuvent faire subir aux droits et libertés de chacun et chacune d'entre nous peuvent venir non seulement des pouvoirs publics qui en recommandent le développement et la mise en œuvre, mais aussi d'autres acteurs, collectifs ou individuels, qui sauront tirer profit des propriétés de ces systèmes comme autant de failles.

Le premier alinéa de l'article 1 de la loi de 1978 a survécu à toutes ses révisions et évolutions. L'urgence que nous ressentons collectivement face à notre situation actuelle ne doit pas nous le faire oublier : ***L'informatique doit être au service de chaque citoyen. […] elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.***

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.

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 ».