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

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

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

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

Article original sur le site de l'Electronic Frontier Foundation

par Nadia Kayyali et Katitza Rodriguez

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

Voilà un an que le journal The Guardian *a publié pour la*

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

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

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

3. La NSA a conçu une vaste « drague du Web » en s'assurant qu'elle peut intercepter non seulement les communications d'une cible lorsqu'elle fait partie d'une communication mais aussi celles qui « concernent une cible, même si la personne ciblée *ne participe pas à une communication* ».

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

5. Même si la NSA a déclaré de façon répétée qu'elle ne

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

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

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

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

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

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

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

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

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

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

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

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

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

que sources de renseignement” ».

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

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

20. Le programme de reconnaissance faciale de la NSA « peut maintenant comparer les photos des satellites d’espionnage avec les photos personnelles interceptées prises en extérieur, pour déterminer leur localisation ».

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

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

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

renseignements des réseaux propres aux USA.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

britannique et les influencer ».

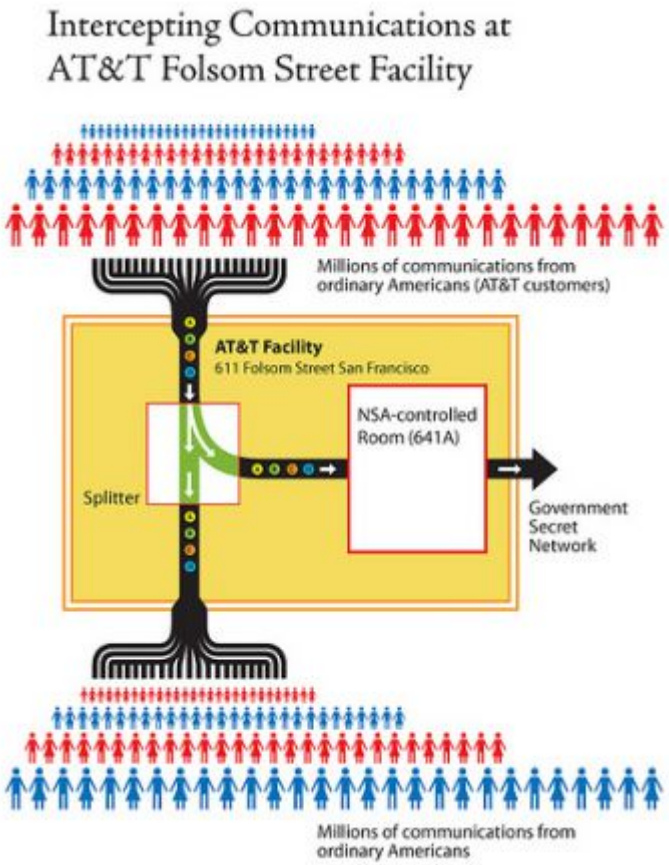
40. *The Guardian* a rapporté ceci : « Sur une période de six mois en 2008, [le GCHQ] a collecté les l'images de webcam – y compris une quantité importante de communications explicitement sexuelles – de plus d'1,8 millions de comptes utilisateurs Yahoo à l'échelle mondiale. »

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

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

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

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



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

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

47. En 2008, l'Australie a offert de partager les données brutes concernant ses citoyens avec ses partenaires du renseignement.

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

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

Canadiens à l'étranger.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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