Espionnage de la NSA : les 8 leçons d'Edward Snowden

Mise à jour le 19/08 à 15h35 *: suite à cet article, la société Barracuda Networks, cité au point 2, a souhaité apporter quelques précisions. A lire ici.*

Un an après les premières révélations d'Edward Snowden sur l'ampleur des opérations d'écoute mises en place par la NSA, le cabinet de conseil en cybersécurité Lexsi publie une analyse de l'affaire. Une analyse qui pointe **l'ampleur des mécanismes de collecte** dont dispose l'agence de renseignement américaine, qui emploie environ **40 000 employés**, sans compter des dizaines de milliers de prestataires. Une analyse qui doit surtout permettre aux responsables de la sécurité en entreprise de tirer quelques enseignements de ce qui est, à ce jour, la plus importante fuite de données d'un service de renseignement américain.

1) Une fuite à l'ampleur inédite

Depuis la bombe lancée le 6 juin 2013 mettant au jour un système d'espionnage massif des appels téléphoniques sur le réseau de l'opérateur Verizon, les révélations sur les pratiques de la NSA se sont enchaînées. « *En moyenne, un scoop tous les 3 jours* », soulignent les consultants de Lexsi, **Thibaut Gadiolet** et **Vincent Hinderer**. Et ce n'est pas fini. « *Quand les autorités britanniques ont intercepté l'ami de Glenn Greenwald (l'un des deux journalistes à qui Snowden a confié ses documents, NDLR), il avait en sa possession 58 000 documents couvrant une période allant de 2006 à 2013. Les révélations aujourd'hui connues concernent moins de 1 % de cette base documentaire* ». Selon un officier de la NSA, interrogé fin 2013, dans le cadre du magazine 60 minutes de CBS, la fuite de données concernerait **pas moins de 1,7 million de documents**. De très loin la plus importante affaire de ce type de l'histoire du renseignement américain. Sans compter que la NSA pourrait être confrontée non pas à un mais à deux lanceurs d'alerte. L'analyse récente, parue dans la presse allemande, d'une partie du code source de Xkeystore, l'outil de requête utilisé par la NSA pour explorer les masses de données collectées, a poussé les analystes, comme le spécialiste de la cryptographie Bruce Schneier, à soupçonner la présence d'une seconde taupe. Soupçon confirmé par les autorités américaines qui ont confirmé traquer un deuxième lanceur d'alertes suite à un article paru début août dans la presse américaine et s'appuyant sur un document produit après le départ en exil d'Edward Snowden.

Malgré l'importance de cette réserve de documents, notons que, ces derniers mois, les révélations marquantes portant sur les mécanismes de collecte et d'exploitation des données se sont raréfiées. Et leur portée s'est réduite. On peut donc raisonnablement émettre l'hypothèse qu'**on connaît aujourd'hui l'essentiel de la toile mise en place par l'agence de Fort Meade** pour collecter des données partout dans le monde. Un dispositif dont l'ampleur et la portée n'avaient jusqu'alors jamais été dévoilées, même si les spécialistes du renseignement en soupçonnaient l'existence. Notons que les précédentes révélations sur les écoutes américaines – notamment autour du réseau Echelon au milieu des années 90 – laissaient entrevoir un système déjà très perfectionné mais largement moins complet que celui que dessine les documents de Snowden.

2) Des mécanismes de collecte multiples

Une année de révélations basées sur les documents qu'a pu exfiltrer Edward Snowden montre en effet toute la richesse et la diversité des mécanismes de collecte d'informations mis en place par l'agence de Fort Meade. Et cela commence… dès l'usine. « *De nombreux produits renferment des backdoor* », souligne Thibault Gadiolet. Des portes dérobées notamment signalées dans les **VPN et firewall de Barracuda, les téléphones et routeurs de Huawei, les Bios de certains PC** et même dans certaines puces programmables d'Actel. Liste non exhaustive. « *On peut penser que la NSA travaille à mettre en place des backdoor dans d'autres systèmes, comme des antivirus ou des librairies de chiffrement* », assure Lexsi. Qui fait aussi part de ses soupçons concernant les boîtiers HSM (appliances de chiffrement).

Plus surprenant, les experts de la NSA s'attaquent également à un maillon souvent négligé de la chaîne d'approvisionnement en technologie : **le transport**. « *Le service TAO (Tailored Access Operations, un groupe de la NSA spécialisé dans les opérations spéciales électroniques, NDLR) intercepte le matériel et y implante des backdoors*, rappellent Thibaut Gadiolet et Vincent Hinderer. *Il bénéficie, pour ce faire, d'accords avec des transporteurs comme UPS, Fedex ou TNT, via des liens directs sur les systèmes de commande de ces spécialistes de la logistique.* »

3) Des réseaux d'entreprise corrompus

En complément de ces techniques 'amont', la NSA dispose d'un catalogue de techniques de piratage visant à infiltrer les réseaux informatiques des cibles de l'agence. Selon un document d'Edward Snowden, pas moins de **50 000 réseaux étaient compromis en 2012**. Et ce, via une multitude de méthodes. Certaines assez classiques, comme l'installation d'implants exploitant les vulnérabilités de certains systèmes (par exemple dans les routeurs de Cisco, Juniper et Huawei ou sur les serveurs Dell PowerEdge). D'autres plus originales, comme Ragemaster, un câble VGA permettant d'intercepter et transmettre les flux vidéos par radiofréquence jusqu'à une distance de 20 km. Un équipement que l'équipe de piratage de la NSA facture en interne pour la modique somme de 30 $…

4) Des hackers aux techniques pointues

Même sans l'exploitation d'une backdoor, la NSA dispose, via sa division TAO, de techniques d'infection à distance, comme l'attaque de type *Man in the middle* nommée Quantum Insert. Celle-ci consiste à intercepter des requêtes Web vers des sites légitimes pour injecter des malwares calibrés pour compromettre les postes ciblés.

Le problème auquel s'est heurté la NSA ? La montée en puissance ; cette technique ayant un taux de 'réussite' supérieur à 50 %, il a fallu gérer de plus en plus de cibles infectées. Afin de limiter les interventions humaines, la NSA a créé un système, appelé Turbine, conçu pour « *permettre au réseau d'implants (des malwares, NDLR) d'atteindre une échelle plus large (des millions d'implants) en créant un système qui automatise le contrôle des implants par groupes plutôt qu'individuellement* », est-il écrit dans un document cité par *The Intercept* en mars dernier. L'infrastructure de Turbine repose sur un système expert, agissant « *comme un cerveau* » gérant les malwares déployés et décidant quels

outils employer pour rapatrier les données de telle ou telle cible. Ces décisions sont ensuite exécutées par des modules de contrôle & commandes, sur les groupes d'implants auxquels elles s'appliquent. Selon les documents de Snowden, en 2004, l'agence n'exploitait qu'un petit nombre d'implants – 100 à 150 –, un chiffre qui a explosé au cours des six à huit ans qui ont suivi, passant à des dizaines de milliers.

C'est ce type de techniques qui a été **exploitée contre l'opérateur belge Belgacom**, par le GCHQ anglais, un partenaire de la NSA. « *Pourquoi cet opérateur en particulier ? Il faut garder en tête que Belgacom se situe à la confluence des institutions européennes importantes et de grandes entreprises dont le siège est à Bruxelles* », insiste Lexsi.

5) Les fournisseurs de service pour alliés… ou pour cibles

L'exemple de Belgacom est d'ailleurs significatif de la tendance de la NSA à miser sur les prestataires pour récupérer un maximum d'informations. Ici par compromission. Mais la NSA peut aussi utiliser **l'arme juridique ou la complicité directe ou indirecte** des opérateurs. « *AT&T et Sprint font transiter à eux deux 80 % des communications internationales* », observe Lexsi. On sait ainsi que le premier de ces deux opérateurs opère pour l'agence au moins une installation dédiée (connue sous le nom de Room 641A et installée dans un immeuble à San Francisco). Par ailleurs, la NSA bénéficie de partenariats avec une trentaine de nations dans le monde, avec lesquelles elle effectue des échanges bilatéraux. On peut ainsi remarquer que, après la révélation des écoutes ciblant les communications françaises, la NSA a nié être à l'origine de ces interceptions expliquant que les journalistes avaient mal interprété les documents qu'ils analysaient. Faut-il y lire le signe d'une complicité des services français qui pourraient avoir fourni ces données à leurs partenaires nord-américains ?

A noter que l'arsenal mis en place par la NSA pour les communications téléphoniques – visant à la collecte de métadonnées – a été répliqué pour Internet, notamment via **le programme Prism** (impliquant les plus grands prestataires américains de services Internet) mais aussi via **l'écoute des backbone d'Internet**. « *Les points d'échange, les câbles, les satellites sont visés. Il en va de même pour les réseaux GSM pour des interceptions plus ciblées* », rappellent les consultants de Lexsi.

L'outil Boundless Informant, qui agrège les données remontées par certains des programmes mentionnés ci-dessus, permet de se faire une idée de la volumétrie des données – ici des métadonnées – stockées par l'agence de Fort Meade. Au cours d'une période de 30 jours, près de 125 milliards de métadonnées téléphoniques et 97 milliards de métadonnées numériques ont été interceptées et injectées dans Boundless Informant.

6) Un intérêt très marqué pour le cryptage

La NSA s'intéresse de très très près à tout ce qui a trait au cryptage. Logique car ce dernier a le potentiel de rendre les grandes oreilles américaines inopérantes. Les révélations d'Edward Snowden ont de facto accru l'usage du protocole chiffré HTTPS, aujourd'hui en voie de

généralisation sur Internet.

La NSA dispose d'**un programme baptisé Bullrun** visant à contrer les effets du chiffrement. Et ce de plusieurs manières distinctes : en influençant directement la conception des protocoles afin de les affaiblir à la source, en persuadant l'industrie d'insérer des backdoor ou des protocoles affaiblis dans leurs produits (comme ce fut le cas avec RSA) ou en cassant les algorithmes par le recours à des supercalculateurs surpuissants (méthode de la force brute). Bullrun était doté, en 2013, d'un budget de 250 millions d'euros. Le partenaire britannique de la NSA, le GCHQ, dispose d'un programme similaire, Edgehill. En 2015, ce dernier doit permettre de déchiffrer les communications cryptées de 15 FAI et de 300 VPN.

Dans son analyse, Lexsi sous-entend que d'autres affaires, notamment l'arrêt de TrueCrypt, la faille HeartBleed ou celle affectant la librairie SSL sur iOS, pourraient être reliées à l'effort au long court de la NSA pour pervertir les technologies de chiffrement utilisées largement sur le marché.

7) Un cadre juridique inchangé

Malgré les déclarations de l'administration Obama, le cadre juridique permettant à la NSA de collecter et exploiter ce vaste océan de données n'a que peu changé suite aux révélations du lanceur d'alerte. « *La portée de la réforme Obama est mince. Les différences entre avant et maintenant sont minimes* », assurent les consultants de Lexsi. Le FISA Amendment Act reste l'outil juridique principalement utilisé par la NSA. En 2012, 1788 demandes avaient été formulées sur la base de ce texte, toutes acceptées et mise en place rapidement (en une journée) pour une durée d'un an renouvelable. « *La réforme Obama ne changera rien ; les Etats-Unis ont besoin de ce type de texte pour que la NSA puisse continuer à fonctionner* », assure Lexsi. Inutile donc de chercher de ce côté des éléments rassurants.

D'ailleurs, malgré les pressions qu'ils exercent sur leur gouvernement, **les industriels IT américains n'ont toujours pas obtenu de réelles garanties** quant à la confidentialité des données de leurs clients, particulièrement étrangers. En témoigne la bataille juridique pour l'instant infructueuse que mène Microsoft pour que les données stockées hors des États-Unis ne soit plus accessibles directement aux requêtes de la justice américaine.

8) Les entreprises ciblées et (presque) sans défense

Pour Lexsi, les choses sont on ne peut plus claires : il faudrait être le dernier des naïfs pour croire que les écoutes de la NSA se bornent à lutter contre le terrorisme. D'ailleurs, si c'était le cas, pourquoi l'agence de Fort Meade aurait-elle écouté le téléphone mobile d'Angela Merkel ? « *Derrière la lutte contre le terrorisme, les écoutes sont exploitées à des fins diplomatiques mais aussi économiques*, assurent Thibaut Gadiolet et Vincent Hinderer. *Des sociétés sont la cible directe de la NSA* ». Et, étant donné l'étendue des capacités de l'agence de renseignement, celles-ci ont **bien peu de garanties de se prémunir** totalement de la curiosité des services américains si ceux-ci les ont inscrites sur la liste de leurs cibles.

« *La première chose à faire est de comprendre pourquoi on pourrait être une cible potentielle, directement ou par ses clients ou partenaires, afin d'identifier les éléments les plus sensibles*, assure Lexsi. *Ensuite, il faut éviter d'être une cible trop facile en instaurant des mesures de sécurité physique autour des équipements, en généralisant le chiffrement sans oublier de vérifier les mesures déployées par les prestataires.* » Mais l'étanchéité totale n'existe pas d'autant que les SI sont aujourd'hui bâtis sur des technologies majoritairement américaines, or les documents mis au jour par les documents Snowden montrent l'implication de nombre d'industriels IT d'outre Atlantique dans les divers programmes de la NSA. « *A l'avenir, il faudra privilégier les équipements certifiés par l'ANSSI. Mais la liste est aujourd'hui très limitée ; c'est un travail en cours* », remarque Lexsi. Le cabinet recommande de **sensibiliser les directions générales** à ces questions, y compris sur les questions relatives au déplacement à l'étranger des cadres de l'entreprise.

A lire aussi :

Tout sur l'arsenal secret des espions de la NSA

Le scandale NSA coûterait jusqu'à 180 milliards de dollars à l'industrie américaine