10 questions pour comprendre l'affaire Shadow Brokers

1) Pourquoi un tel intérêt pour les Shadow Brokers ?

Lundi 15 août, un groupe de hackers appelé Shadow Brokers a annoncé avoir piraté des systèmes informatiques utilisés par Equation, une organisation réputée proche de la NSA. A l'appui de ses affirmations, ce groupe jusqu'alors inconnu a posté deux archives sur des sites de partage. La première, en libre accès, renferme 300 Mo de données, où se mêlent des outils et des techniques pour infiltrer des systèmes.

« Nous vous donnons quelques fichiers d'Equation Group gratuitement… Mais pas tous, nous mettons aux enchères les meilleurs », ont indiqué les Shadow Brokers dans un anglais approximatif. Dans une seconde archive, placée cette fois aux enchères, ils se targuent de proposer du code inédit, *« meilleur que Stuxnet »*, du nom du ver conçu par les services américains pour infiltrer le nucléaire iranien. Seulement, pour ce joyau de la couronne, les Shadow Brokers réclament un million de Bitcoins (plus de 500 millions d'euros au cours actuel). Ce qui ne manque pas d'interroger les experts, une telle somme étant par nature peu crédible.

« *L'annonce d'une deuxième archive promise par les Shadow Brokers est assez troublante. Car elle est associée à une rançon totalement fantaisiste, qui plus est en Bitcoin, une monnaie facilement traçable contrairement à ce qu'on pense*, explique Gérôme Billois, senior manager chez Wavestone (fruit de la fusion des cabinets de conseil Solucom et Kurt Salmon)**.** *Cette annonce me paraît avoir un rôle médiatique, et vise à amplifier le bruit que fait l'affaire. Si les Shadow Brokers voulaient faire peur, ils n'auraient pas utilisé l'arme de la rançon.* » Nicolas Weaver, un chercheur en sécurité de l'université de Berkeley en Californie, compare d'ailleurs l'enchère « *à un criminel demandant à être payé avec des billets neufs, marqués et dont les numéros de série se suivent. Parce que les acteurs en présence ici ne sont sûrement pas des amateurs, l'enchère s'apparente probablement à une scène du Docteur Evil (le méchant d'Austin Powers, qui parodie le rôle du vilain dans James Bond, NDLR) ».*

2) Le hacking de la NSA est-il établi ?

Bien entendu, ni la célèbre agence américaine ni le groupe de hackers Equation, réputé proche de celle-ci, n'a confirmé que les outils mis en ligne par les Shadow Brokers provenaient bien de leurs serveurs. Mais plusieurs éléments concordants établissent un lien direct entre les fichiers mis en ligne par les Shadow Brokers et le couple NSA/Equation. D'abord, c'est l'éditeur russe Kaspersky qui remarque que plus de 300 fichiers présents dans la première archive utilisent une implémentation des algorithmes de chiffrement RC5 et RC6 identique à celle utilisée par le groupe Equation. « *La probabilité que tout ceci (l'archive mise en ligne, NDLR) soit un faux ou ait été conçu par rétro-ingénierie est extrêmement faible* », écrivent les chercheurs de Kaspersky dans un billet de blog.

Des sources anonymes ayant travaillé pour la division de la NSA appelée TAO (Tailored Access

Operations), l'unité en charge des cyber-opérations offensives de l'agence, ont également confirmé à nos confrères du *Washington Post* que les fichiers mis en ligne semblaient bien provenir de la NSA. Leurs noms ne sont d'ailleurs pas sans rappeler les appellations mises au jour lors des révélations successives sur l'agence de Fort Meade parues dans la presse. Notons ainsi qu'on a déjà vu apparaître le nom de certains outils – comme Bananaglee, Jetplow ou FeedTrough, tous présents dans l'archive des Shadow Brokers – dans le catalogue ANT de la NSA, publié en fin d'année 2013 par *Der Spiegel*.

D'ailleurs, le journal en ligne *The Intercept* établit un lien direct entre les fichiers dévoilés par les Shadow Brokers et les documents révélés par Edward Snowden. S'appuyant sur un fichier exfiltré par le lanceur d'alerte et jamais publié jusqu'alors, le journal en ligne confirme que l'arsenal contient bien « *des logiciels authentiques issus de la NSA* ». A l'appui de ces affirmations, *The Intercept* se base sur un manuel d'implantation de malwares où la NSA recommande à ses opérateurs d'employer un code précis ("ace02468bdf13579"). Code qu'on retrouve dans un des outils mis en ligne par le groupe de hackers inconnu. Précisément dans un outil appelé SecondDate.

« *Cette archive et les outils mis en ligne par les Shadow Brokers sont cohérents avec ce qu'on lisait dans les documents Snowden. Car, désormais, de nombreux indices pointent dans la même direction et semblent indiquer que les données exfiltrées proviennent bien de la NSA* », commente Gérôme Billois. Hervé Schauer, directeur de HSC by Deloitte, estime ces rapprochements « *assez convaincants, même s'il n'y a pas eu de confirmation officielle.* »

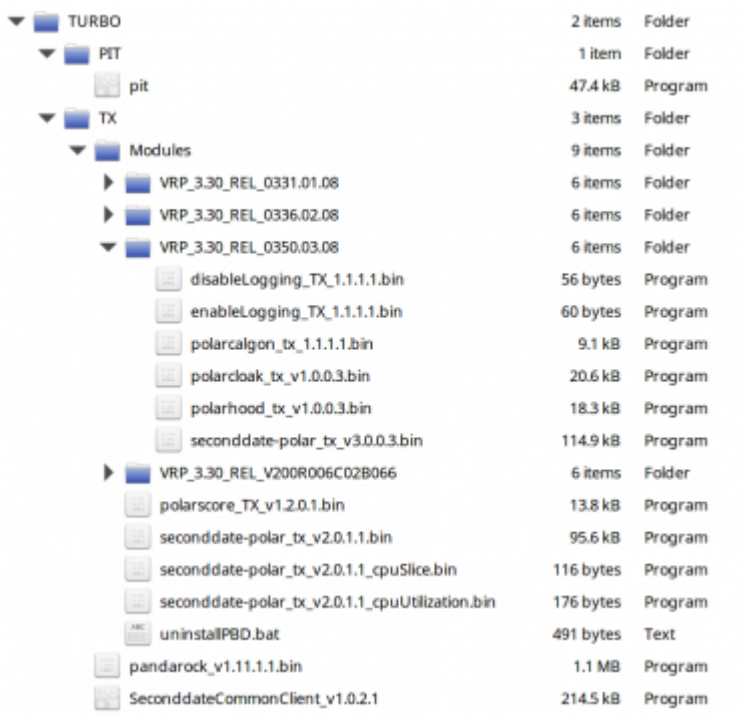
3) Que dit cette affaire du groupe Equation ?

Le nom de ce groupe, choisi en raison de sa prédilection pour les techniques de chiffrement de haut vol, a été donné début 2015 par Kaspersky à un groupe de hackers, que l'éditeur russe décrivait alors comme le plus techniquement doué qu'il ait jamais identifié. La société parlait alors « *d'une menace qui dépasse tout ce qui est connu en termes de complexité et de sophistication des techniques employées, une menace active depuis au moins deux décennies* ». Equation exploitait depuis 2008 des failles zero day qui ne seront mises à jour que plus tard, à l'occasion du piratage du nucléaire iranien par Stuxnet. Une opération attribuée, rappelons-le, aux Etats-Unis et à leurs alliés israéliens. Conjuguée à d'autres indices, cette proximité avait amené les analystes à faire d'Equation un groupe affilié à la NSA.

Les récentes révélations des Shadow Brokers, qui affirment avoir piraté Equation (et non la NSA), ne font que confirmer ces soupçons. « *A la lumière des indices qui s'accumulent, le groupe Equation apparaît de plus en plus comme une émanation directe de la NSA* », dit Gérôme Billois.

4) Que renferme l'archive des Shadow Brokers ?

Plusieurs chercheurs en sécurité se sont déjà penchés sur le cyber-arsenal mis à disposition par les Shadow Brokers (lire notamment l'analyse de Mustafa Al-Bassam ou la synthèse réalisée par *Softpedia*). On y trouve des *exploits*, autrement dit des codes d'exploitation permettant de prendre le contrôle ou d'espionner des pare-feu ou passerelles VPN fournis par de grands constructeurs comme Cisco, Juniper ou Fortinet. Des constructeurs qui ont déjà reconnu que les outils mis en ligne menaçaient bien certains de leurs matériels. Mais, dans tous les cas, il s'agit de générations anciennes de machines. Les appliances Cisco Pix, ciblées par plusieurs outils, ne sont par exemple plus supportées par le constructeur depuis 2009. Cela semble accréditer le fait que les fichiers mis à disposition soient assez anciens. Dans l'archive mise en ligne par les Shadow Brokers, les fichiers les plus récents remontent à fin 2013 si on se fie à leur date de création (une donnée qui est toutefois facilement manipulable).



Notons au passage que plusieurs constructeurs ont tendance à minimiser l'impact des outils mis en ligne. Dans son alerte, Juniper indique avoir affaire à un implant logiciel et non à une vulnérabilité de son OS ScreenOS (animant sa gamme Netscreen). Mais oublie de préciser que l'implant en question (FeedThrough) permet à un assaillant de se ménager un accès discret aux machines concernées et survit aux redémarrages. De son côté, Cisco a pour l'heure écarté la réalité d'une attaque appelée PixPocket, permettant de dérober les clefs de chiffrement des VPN de la gamme Pix. La technique a pourtant été validée par plusieurs chercheurs…

« *La première archive renferme de vraies bonnes données, avec des exploits fonctionnels. Ceux qui dévoilent ces outils perdent là un avantage important, car ce type d'outils leur permet à la fois de détecter les actions d'Equation et de mener leurs propres attaques. Peut-être l'utilité de ces informations avait-elle décru avec le temps ?* », suggère Gérôme Billois.

Comme le remarquent Hervé Schauer et Christophe Renard, consultant sénior en sécurité du cabinet HSC by Deloitte, l'archive des Shadow Brokers ne se limite pas à quelques exploits de haut niveau, mais comprend aussi des outils de reconnaissance, des implants (du code venant modifier l'environnement cible, NDLR), des outils de 'tunneling' et d'extraction de données ou encore des manuels d'utilisation. Plus surprenant : selon une analyse d'un chercheur de l'université de Chicago, la qualité du code est médiocre, « *en particulier sur les choix en matière de chiffrement* », notent Hervé Schauer et Christophe Renard. Qui ajoutent : « *Ceci peut s'expliquer par un faible niveau d'exigence (le recours à des sous-traitants ?) ou par le fait que les toolkits sont considérés comme jetables, ce qui expliquerait qu'investir dans la qualité soit alors considéré comme inutile.* »

5) L'archive a-t-elle livrée tous ses secrets ?

Sans risque de se tromper, la réponse est non. « *Comme il y a 300 Mo de code, de documentations, de binaires, personne n'a publié d'analyse complète* », remarquent Hervé Schauer et Christophe Renard. « *Ce sont des outils complexes qui prennent du temps à être interprétés et testés. Nous devons nous attendre à la sortie d'autres révélations* », abonde Gérôme Billois. Preuve en est que de grands constructeurs dotés de moyens colossaux, comme Cisco et Juniper, sont encore en train d'étudier les conséquences de la publication de ces outils sur leurs gammes.

Et il y a aussi les outils dont la vocation ne se limite pas à cibler une gamme de machines en particulier. *The Intercept* explique ainsi que des éléments d'une architecture exploitée par la NSA pour mettre en place des attaques de type Man-in-the-Middle, autorisant l'interception de requêtes Web, figurent dans l'archive des Shadow Brokers.

6) Quels sont les risques pour les entreprises ?

Voir de tels outils mis à la disposition de cybercriminels est évidemment inquiétant. « *On est ici face à des outils d'attaque de haut niveau, mis librement à disposition sur le Web*, explique Gérôme Billois. *Les entreprises doivent donc être très attentives, effectuer l'inventaire des matériels exposés sur leur parc et apporter les modifications nécessaires pour protéger leurs infrastructures. Heureusement, les exploits mis au jour sont assez anciens et ciblent donc du matériel âgé. Mais certaines machines peuvent toujours être en exploitation.* » Au fur et à mesure que les codes de l'archive des Shadow Brokers seront décortiqués, des correctifs et des indicateurs de compromission vont être publiés. Ce qui permettra aux RSSI de contrer la menace. C'est donc plutôt une course de fond qui s'engage. « *On assiste à une course entre l'exploitation des zero day contenus dans la fuite et leur correction qui a déjà commencée. Le rôle des RSSI est de faire en sorte que les entreprises appliquent les correctifs, surtout sur des équipements réseaux qui sont en bordure comme les routeurs, firewall ou têtes de tunnels* », analysent Hervé Schauer et Christophe Renard. A plus long terme, on peut aussi pronostiquer que l'archive des Shadow Brokers devrait être la source de nouvelles idées pour les hackers et cybercriminels.

7) Qui a fait le coup ?

La liste des suspects s'est très vite limitée à quelques noms. Très rapidement, Nicolas Weaver, de l'université de Berkeley, pointe la Chine, soupçonnée de nombreux actes de cyber-espionnage contre les intérêts américains, et la Russie. Une seconde hypothèse que défend lui aussi Edward Snowden, précisément réfugié en Russie après avoir été à l'origine de la plus importante fuite de données de l'histoire de la NSA. Le lanceur d'alerte y voit un avertissement de Moscou après « *l'escalade autour du hack du DNC (Democratic National Committee) ».* En juin dernier, WikiLeaks a publié des milliers de courriels internes du DNC dont les serveurs ont été piratés. Malgré les revendications d'un hacker présumé roumain (Guccifer 2.0), le parti démocrate US voit la main de la Russie derrière cette opération…

Pour Snowden, la fuite des Shadow Brokers pourrait provenir d'un serveur mal 'nettoyé' par les hackers de la NSA. Et apparait « *comme un avertissement montrant aux Etats-Unis que quelqu'un peut prouver leur responsabilité pour toute attaque venant de ce serveur de malware. Ce qui pourrait avoir des*

conséquences politiques internationales importantes. Particulièrement, si une opération offensive menée dans ce cadre cible un allié des États-Unis. Particulièrement, si une de ces opérations a ciblé des élections. »

Bref, les Shadow Brokers voudraient avant tout faire passer un message. A noter que ceux-ci ont tenté de brouiller les pistes, en s'exprimant par écrit dans un très mauvais anglais, à la limite de la caricature. Selon un chercheur en linguistique de Taia Global, les erreurs grammaticales et structurelles commises seraient intentionnelles. Pour la société, l'auteur des messages postés par les Shadow Brokers serait même probablement anglophone…

8) Un second lanceur d'alertes à la NSA ?

Car une autre hypothèse a également de nombreux partisans : celle de l'implication d'un 'insider', un nouveau lanceur d'alerte à la NSA. Plusieurs éléments viennent étayer cette hypothèse. Primo, l'archive en question renferme différentes versions d'un même outil, des manuels d'utilisation ou des fichiers à vocation interne. Ce qui cadre mal avec l'hypothèse d'un serveur d'attaque, ou d'un serveur de pré-production, qui aurait été compromis par un assaillant externe. Par ailleurs, dans Information Management, Lance James, responsable des recherches en cybersécurité de Flashpoint, explique qu'une des adresses IP trouvées dans un des fichiers pointe vers un *« espace d'adresse IP non routable* » appartenant au Département de la Défense américain. Selon lui, les fichiers mis en ligne par les Shadow Brokers auraient donc été récupérés depuis l'intérieur, probablement depuis un catalogue d'outils dans lequel piochent les équipes chargées des opérations offensives de la NSA.

Après discussion avec un employé de la division TAO, le Français Matt Suiche, hacker et entrepreneur, parvient à la même conclusion : « *Le catalogue renfermant le kit d'outils de la TAO est stocké sur un réseau physiquement séparé qui n'a aucun lien avec Internet et n'a aucune raison d'en avoir. Il n'y a aucune raison que ces fichiers se soient un jour retrouvés sur un serveur de tests ou de pré-production à moins que quelqu'un ne l'ait fait à dessein. La hiérarchie des fichiers et le fait que les conventions de nommage soient restées inchangées tendent aussi à prouver que ces fichiers ont été copiés directement depuis la source (donc le catalogue, NDLR).* »

Electrospaces inscrit d'ailleurs cette nouvelle révélation dans la série de fuites émanant d'une seconde source au sein de la NSA. Comme le rappelle le blog, un certain nombre de révélations sur les pratiques de la NSA ne sont pas attribuées à Edward Snowden. Citons la publication du

catalogue de techniques de hacking (ANT en décembre 2013), les détails sur XKeyScore ou les révélations sur l'espionnage d'Angela Merkel. Pour *Electrospaces*, l'irruption des Shadow Brokers pourrait ainsi être une nouvelle manifestation de cette « *seconde source* ».

Un autre élément plaide pour une fuite interne : les dates des fichiers mis en ligne. « *La date des dernières modifications (octobre 2013), soit peu après la publication des fuites par Snowden, donc en pleine folie de vérification et de durcissement des systèmes à la NSA, pourrait correspondre à une fermeture d'accès superflus et la fin de la capacité pour la taupe à accéder à ces éléments* », échafaudent Hervé Schauer et Christophe Renard. Mais, considérant que la fuite actuelle n'est passée ni par un journaliste, ni par Wikileaks, les deux experts estiment qu'il s'agit plutôt d'une manipulation politique ou d'une action criminelle, pouvant éventuellement s'appuyer sur une taupe. Et relèvent que d'autres hypothèses sont également recevables. Y compris la récupération des fichiers chez des tiers qui les auraient eux-mêmes subtilisés à la NSA. Une tactique que l'agence américaine a d'ailleurs conceptualisée sous l'appellation « *4th party source* » et qu'elle a aussi mise en pratique pour récupérer des documents de l'ONU que des pirates chinois avaient subtilisés à l'institution. « *Les Russes ? Un 'insider' au sein de la NSA ? La situation est trop floue aujourd'hui et il est trop facile de bondir sur la première hypothèse recevable* », résume Gérôme Billois.

9) Quelles sont les conséquences possibles ?

D'ores et déjà, la fuite a dû déclencher un branle-bas de combat au sein de la NSA, qui doit chercher l'origine de cette encombrante archive et, surtout, comment mettre fin aux révélations successives sur ses activités offensives. L'agence devra également s'assurer qu'elle n'exploite plus les codes révélés au public pour ses opérations actuelles. Car, très rapidement, les outils de sécurité seront en mesure de détecter les signatures des outils révélés par les Shadow Brokers. L'examen des traces stockées par l'industrie, notamment par les éditeurs d'antivirus, devrait aussi permettre de détecter des attaques passées ayant eu recours à certains de ces outils.

Aux Etats-Unis, la révélation des Shadow Brokers ne manquera pas de relancer le débat sur la communication autour des failles zero day. Notamment quand celles-ci touchent des constructeurs locaux – comme c'est le cas ici pour Cisco, Juniper ou Fortinet. De facto, les techniques de l'agence américaine, basées sur l'exploitation de failles qu'elle se garde bien de publier (malgré l'existence d'un très opaque processus de divulgation appelé VEP, pour Vulnerabilities Equities Process), constituent un handicap commercial pour certains industriels américains. Un point que n'avait pas manqué de souligner John Chambers, l'ancien patron de Cisco.

Reste enfin à savoir si les Shadow Brokers dévoileront réellement d'autres fichiers issus de la NSA. Rappelons qu'ils affirment détenir une seconde archive renfermant les codes les plus intéressants à leur disposition. Une menace qui permet également de maintenir la NSA sous tension…

10) Qu'en pense Bernard Cazeneuve ?

Passée la boutade, le ministre de l'Intérieur français, qui entend prendre la tête d'une initiative internationale permettant d'encadrer le chiffrement, a devant les yeux une autre illustration des limites que pointent de nombreux spécialistes, y compris le Conseil national du numérique (CNNum).

Après l'affaire Juniper (le constructeur avait employé un algorithme de chiffrement affaibli par la NSA, qui avait été détourné par un acteur inconnu), les révélations des Shadow Brokers illustrent une fois encore le caractère spécifique des armes cyber. Des armes qui ne se détruisent pas après usage, et qui, parfois, finissent par se retourner contre vous. C'est ce sujet qui est au cœur des débats sur l'affaiblissement du chiffrement. Si l'installation de backdoors dans les outils de chiffrement peut apparaître comme une bonne idée pour faciliter les enquêtes sur le terrorisme, rien ne permet de garantir que ces failles ne soient pas exploitées un jour par d'autres acteurs menaçant nos intérêts…

A lire aussi :

Juniper reconnaît (enfin) une faille mise au jour par les Shadow Brokers

Cisco et Fortinet valident le sérieux des Shadow Brokers, hackers de la NSA

crédit photo © igor.stevanovic / shutterstock