La 2ème taupe de la NSA serait liée aux Shadow Brokers

Arrêté fin août par le FBI, Harold Thomas Martin III, un salarié de Booz Allen Hamilton ayant travaillé comme sous-traitant pour la NSA, est soupçonné par les autorités américaines d'être la source des Shadow Brokers. Ce groupe de pirates jusqu'alors inconnu a publié mi-août des outils de hacking issus de l'agence de renseignement américaine. Mercredi, le *New York Times* affirmait, sur la base du témoignage d'enquêteurs, que l'informaticien était, au moment de la perquisition à son domicile, en possession d'outils de hacking top secrets de la NSA récemment mis en vente par les Shadow Brokers. Rappelons en effet une première publication en libre accès, le 15 août dernier, les pirates promettent de nouvelles révélations, avec la publication d'une seconde archive renfermant des documents ou codes sources secrets. Mais celle-ci n'est accessible que contre rémunération.

L'article du *New York Times* ne précise pas comment les services d'enquête américains auraient eu connaissance du contenu de cette seconde archive. Pas plus qu'il n'établit un lien définitif entre 'Hal' Martin et les Shadow Brokers. Les enquêteurs interrogés par nos confrères expliquent en effet avoir trouvé des traces informatiques montrant que le suspect pourrait être la source de la fuite, mais reconnaissent que ces éléments de preuve ne suffisent pas à tirer une conclusion définitive.

Une fuite pire que Snowden

Dans un document officiel déposé devant la justice du Maryland, les procureurs en charge de l'affaire expliquent que ce sont pas moins de l'équivalent de 50 To de données et des milliers de pages de documents, dont certains marqués « secret » ou « top secret », qui ont été saisies au domicile de cet homme de 51 ans, parmi lesquels des informations sur des *« plans d'une opération spécifique contre un ennemi connu des Etats-Unis et de ses alliés* ». Certaines de ces informations top secrètes étaient stockées dans la voiture du suspect.

Selon le gouvernement américain, les documents dérobés couvrent une vaste période – de 1996 à 2016. Il s'agirait là de la plus importante fuite de l'histoire des renseignements américains, même si, à ce stade, il est impossible d'affirmer que Hal Martin a bien transmis tout ou partie de ce trésor à des tiers. Les enquêteurs soulignent toutefois qu'il a communiqué sur Internet dans d'autres langues que l'anglais. Il aurait ainsi employé le Russe et téléchargé des informations relative à cette langue.

Le volume d'informations stocké par l'informaticien de 51 ans dépasse en tout cas les centaines de milliers de documents dérobés par Edward Snowden en 2013. Il est aussi 20 fois plus volumineux que les Panama Papers, cet ensemble d'informations sur les sociétés offshore gérées par le cabinet d'avocats panaméen Mossack Fonseca.

Dans l'unité de hacking de la NSA

Pour la NSA et plus largement pour la communauté américaine du renseignement, cette nouvelle affaire fait figure d'électrochoc. Les spécialistes se demandent, en effet, comment Hal Martin a pu réunir un tel volume d'informations sur une si longue période sans être détecté par les mesures de sécurité mises en place par ses donneurs d'ordre successifs, la NSA, mais aussi le bureau du directeur du renseignement américain et le Pentagone. Hal Martin a eu accès à des informations top secrètes dès 1996, lors de son service dans la réserve de la marine américaine. Un privilège qui n'a jamais été remis en cause par la suite chez les sept sous-traitants du gouvernement pour lesquels il a travaillé.

L'enquête ciblant Hal Martin n'a réellement démarré qu'après la publication des premiers outils de hacking *made in* NSA par les Shadow Brokers, le 15 août dernier. Selon le *New York Times*, l'informaticien aurait attiré l'attention en postant sur Internet un élément non précisé qui a éveillé les soupçons des enquêteurs. Au sein de l'agence de Fort Meade, Hal Martin a travaillé pour le département Tailored Access Operations, l'unité chargée des cyber-opérations offensives de la NSA et du développement d'outils de hacking. Ce sont certains de ces outils qu'ont publiés les Shadow Brokers, qui assurent disposer encore d'autres informations confidentielles.

Dès 2014, un an environ après la publication des premiers documents Snowden, l'analyse, 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 au sein de la NSA. Soupçons confirmés par les autorités américaines qui ont reconnu traquer un deuxième lanceur d'alertes suite à un article paru en août 2014 dans la presse américaine et s'appuyant sur un document produit après le départ en exil d'Edward Snowden. L'hypothèse d'un nouveau lanceur d'alerte au sein de la célèbre agence avait refleuri après la mise en ligne de kits de hacking made in NSA par les Shadow Brokers, en août dernier.

A lire aussi :

Espionnage des e-mails : Yahoo pouvait-il refuser d'aider la NSA ?

Menwith Hill : le porte-avion de la NSA au cœur de l'Europe

10 questions pour comprendre l'affaire Shadow Brokers

Crédit Photo : produktionsbuero TINUS-Shutterstock