La CIA collectionne les outils de hacking d'autres Etats… pour masquer ses traces

Les révélations de *Wikileaks* sur les pratiques de hacking de la CIA tombent à point nommé pour jeter le trouble sur le rôle potentiel de l'administration Obama dans les récentes affaires qui ont secoué les Etats-Unis. Parmi les documents publiés par le site de Julian Assange, une section intitulée **Umbrage** montre comment l'agence de Langley peut détourner à son profit des techniques imaginées par d'autres nations. Ce qui lui permettrait, sur le papier, de mener des actions offensives tout en laissant des traces numériques pointant, par exemple, vers Cozy Bear et Fancy Bear, les noms de codes des services secrets russes. Rappelons que ce sont ces derniers qui ont été accusés officiellement dans le hacking des démocrates, qui a plombé la campagne d'Hillary Clinton.

Même si les documents dévoilés par *Wikileaks* ne contiennent aucun élément concret permettant d'imaginer que la CIA a orchestré l'opération ciblant le camp démocrate, il n'en fallait pas plus pour que des scénarios de ce type soient échafaudés, notamment par des sites américains étiquetés à droite.

Diriger l'attribution sur d'autres

Au-delà de ces polémiques, les documents publiés par *Wikileaks*, s'ils sont bien authentiques, dévoilent l'existence d'une entité de la CIA – le groupe Umbrage – qui catalogue les méthodes de hacking des autres nations. Et pas uniquement à des fins de documentation. L'objectif est bien de réemployer ces méthodes dans le cadre d'opérations offensives afin de tromper l'enquête et de détourner l'accusation sur d'autres. « *Avec Umbrage et des projets connexes, la CIA peut non seulement augmenter son nombre total de types d'attaque, mais aussi diriger l'attribution vers d'autres en laissant des empreintes numériques des groupes auxquels elle a dérobé ces techniques d'attaque* », explique *Wikileaks*. Au passage, l'existence de cette organisation à Langley amène une preuve supplémentaire de la difficulté à pointer les responsabilités dans le cyberespace. Et font figure de nouvelle démonstration pratique du caractère réutilisable des cyber-armes.

Selon *Wikileaks*, les quelque 8 700 documents publiés hier proviennent d'un réseau sécurisé et isolé, le Center for Cyber Intelligence (CCI) situé à Langley, en Virginie, au siège de la CIA. « *Cette archive semble avoir été diffusée de façon non autorisée chez certains anciens pirates et sous-traitants du gouvernement américain, l'un d'entre eux ayant fourni à Wikileaks des parties de cette archive* », écrit le site de Julian Assange, qui parle d'une première publication représentant des centaines de millions de lignes de code. Même si, pour l'instant, *Wikileaks* ne dévoile que la documentation associée à ces logiciels. Cette publication et les suivantes qu'annoncent déjà *Wikileaks* est un accroc de plus dans la sécurité interne des services secrets américains, la NSA ayant déjà été écornée par les fuites Snowden et Shadow Brokers.

La seconde NSA

Selon le site, à la fin de 2016, la division de la CIA spécialisée dans le hacking comptait 5000 utilisateurs enregistrés sur le réseau du CCI et avait produit plus d'un millier de techniques de pénétration, virus, chevaux de Troie et autres malwares. Pour *Wikileaks*, on parle là d'une sorte de seconde NSA, offrant encore moins de transparence et devant encore moins rendre de comptes sur son activité que son homologue de Fort Meade.

A lire aussi :

La CIA n'a pas cassé le chiffrement de WhatsApp, Signal ou Telegram

Fuite Shadow Brokers : la preuve d'une nouvelle taupe à la NSA ?