L’attaque de TV5 Monde, un coup des Russes ?

C’est toujours un exercice délicat de retrouver l’origine d’une attaque informatique. Et celle qui a touché TV5 Monde le 8 avril dernier n’échappe pas à cette règle. Pour mémoire, cette offensive a permis la prise de contrôle du site Internet de TV5 Monde, de ses comptes de réseaux sociaux, et a provoqué la coupure des programmes télévisés pendant plusieurs heures. Une cyberattaque d’une portée inédite donc, puisque le SI interne de l’entreprise a été atteint, permettant ainsi aux pirates d’interrompre purement et simplement la diffusion des programmes de la chaîne, et ce dans le monde entier.

Ces actions ont été revendiquées par Cyber Caliphat, un groupe de hackers se réclamant de Daesh. A l’époque, TV5 Monde avait fait appel aux experts techniques de l’ANSSI (Agence Nationale de Sécurité des Systèmes d’Information) pour rétablir le service et mener l’enquête afin de découvrir les traces et les indices de l’attaque. Devant l’ampleur des dégâts, pas moins de 13 personnes avaient été sollicitées.

Or, selon nos confrères de *l’Express* et du *Monde*, les résultats de l’enquête de l’ANSSI ne penchent pas pour la mise en cause de l’Etat Islamique. Les soupçons se portent sur la Russie. En effet, les différents éléments récoltés par les experts correspondent à un *modus operandi* similaire et déjà utilisé par un groupe de pirates russes.

Un groupe de hackers russes déjà connu

Ce groupe est qualifié différemment selon les spécialistes de la sécurité informatique. « APT28 » chez FireEye, « Sednit » pour Eset, et « Pawn Storm » pour le japonais Trend Micro. Les analystes des 3 sociétés ont trouvé des faisceaux de présomptions qui mènent à la Russie. La signature des pirates aurait été retrouvée dans des attaques contre des cibles militaires américaines ou des opposants au régime de Vladimir Poutine.

Reste que malgré ces différents indices, les preuves d’un lien avec la Russie sont maigres. Tout au plus, on connaît des détails supplémentaires sur le mode opératoire de l’attaque lancée sur la chaîne française. Les pirates ont utilisé des VPN pour masquer leur présence. Ils se sont infiltrés dans TV5 Monde en janvier dernier, « *sur l’ordinateur d’un poste de production servant à contrôler les caméras sur le plateau, auquel ils ont réussi à accéder grâce à un mot de passe peu sécurisé d’un prestataire du groupe de télévision* », précise nos confrères du Monde. Par la suite, ils ont patiemment obtenu le contrôle de plusieurs éléments réseaux avec des élévations de privilèges. En avril, ils ont pris trois cibles : « *Les réseaux sociaux, le site Internet et, surtout, les outils de production, nécessaires à la diffusion des images sur l’immense réseau de TV5 Monde.* »

L’enquête continue donc pour approfondir et trouver des liens supplémentaires avec l’origine Russe de l’attaque. Dans le climat politique actuel, il est peu probable que Moscou soit très coopératif et propose son aide dans cette affaire.

A lire aussi :

TV5 Monde : le révélateur des failles de sécurité de nos télés

3 questions sur l'attaque cyberjihadiste de TV5 Monde (MAJ)

Crédit Photo : Duc Dao-Shutterstock