Cyberattaque de TV5 Monde : des pirates russes à la manœuvre ? | Le Net Expert Informatique

Cyberattaque de TV5 Monde : des pirates russes à la manœuvre ?

Cette cyberattaque avait été menée par des inconnus se réclamant de l'organisation Etat islamique. L'enquête se tourne désormais vers la Russie.

La piste jihadiste semble s'éloigner. L'enquête sur le piratage d'envergure subi le 8 avril par la chaîne de télévision francophone TV5 Monde s'oriente vers « un groupe de hackers russes », selon une source judiciaire, mardi 9 juin. Cette cyberattaque avait été menée par des inconnus se réclamant de l'organisation Etat islamique. Des messages de propagande jihadiste avaient été diffusés sur le site de la chaîne, ainsi que sur ses comptes Facebook et Twitter.
Le parquet antiterroriste avait alors ouvert une enquête préliminaire. Dans ce cadre, « les investigations conduisent à ce stade vers un groupe de hackers russes désignés sous le nom APT28 », d'après la même source. Ce groupe serait aussi parfois désigné sous les noms de « Pawn Storm » et « Sofacy group ».
Selon un rapport de la société américaine FireEye, APT28 est « un groupe aguerri de développeurs et d'opérateurs qui collectent des données relatives aux problématiques de défense et de géopolitique, des données qui ne pourraient être mises à profit que par un gouvernement ». L'ampleur des moyens déployés et le fait que cette cellule mène des attaques avec régularité depuis « au moins 2007 » témoignent, selon FireEye, du fait qu'elle est « soutenue par un gouvernement, plus précisément un gouvernement basé à Moscou ».

Un travail d'investigation sur les adresses IP
D'après ce même rapport, APT28 a notamment mené des attaques contre des ministères géorgiens. Selon un autre rapport de la société japonaise Trend Micro, Pawn Storm a aussi visé des dissidents russes ainsi que des intérêts américains, notamment des infrastructures militaires et des ambassades.
Les enquêteurs ont pu remonter la trace des hackers par « le travail d'investigation sur les adresses IP des ordinateurs d'où sont parties les attaques », selon une source proche du dossier. D'après les rapports des deux sociétés de cybersécurité, la cellule utilise des méthodes très sophistiquées, notamment pour recueillir mots de passe et codes d'accès. Ils enregistrent, par exemple, des noms de sites internet avec des adresses très proches de sites institutionnels reconnus afin de tromper leurs cibles.

Source : http://www.francetvinfo.fr/culture/tv/cyberattaque-de-tv5-monde-des-pirates-russes-a-la-manoeuvre_944085.html
Par Francetv info avec AFP