Daech se forme au piratage : « Le risque, c’est un cyber-11-Septembre » | Le Net Expert Informatique

	Daech se forme au piratage : « Le risque, c’est un cyber-11-Septembre »

Le groupe islamiste aurait tenté de pirater les firmes énergétiques américaines, avec dans l'idée de produire des black-out. Il n'a pour l'instant pas réussi.

La chaîne de télévision raconte que Daech a tenté (en vain) de pirater des firmes énergétiques américaines lors d'une grande conférence organisée la semaine dernière. Toutefois, le groupe islamiste utilise des outils de piratage dépassés, incapables de pénétrer dans les systèmes pour les couper ou les faire exploser.

L'intention est forte, heureusement les capacités sont faibles », commente à CNN John Riggi, responsable de la division cyber au FBI. « Mais, nous restons préoccuper s'ils achètent plus de capacités. »

En effet, il existe un important marché noir pour les outils de piratage. Un logiciel malveillant se vend ainsi entre 12 et 3.500 dollars, selon la firme de sécurité Symantec. Avec le bon arsenal et en apprenant à exploiter les failles de sécurité, l'Etat islamique pourrait s'introduire dans les systèmes des fournisseurs d'énergie américains.

Vers un « cyber-armageddon » ?

Le réseau électrique américain présente la particularité d'être essentiellement mécanique, alimenté par 7.000 centrales, 700.00 kilomètres de lignes à haute tension et 3,5 millions de lignes de raccord… Le tout sert 150 millions de foyers, via 3.300 sociétés différentes. Cette infrastructure, vétuste et obsolète, a déjà montré des failles, à savoir la multiplication des black-out ces dernières années dans les grandes villes, y compris New York. Ainsi, en 2013, à Cookeville (Tennessee), le simple passage d'un raton-laveur dans une installation électrique a produit une boule de feu, privant 6.000 Américains d'électricité pendant 24 heures…

Les Etats-Unis disent depuis longtemps redouter des cyber-attaques sur son réseau électrique (et sur l'ensemble de ses infrastructures, toutes faibles), craignant un « cyber-armageddon » ou un « cyber Pearl Harbor » qui mettrait à bas l'ensemble du pays. L'intérêt de Daech pour le système donne déjà des sueurs froides aux autorités américaines. Une cyber-attaque qui réussirait à s'introduire dans le système pourrait ainsi couper le courant dans de larges régions du pays, voire pourrait faire exploser les machines pour un black-out durable.

Un somme un « cyber-sabotage » qui porterait la marque de l'organisation islamiste. Dès 2013, l'ancien directeur de l'Anssi, Patrick Pailloux (aujourd'hui à la DGSE), prévenait « l'Obs » :

Ma plus grande crainte concerne le cybersabotage, c'est-à-dire l'introduction dans un système pour le saboter, soit une utilisation quasi militaire de l'informatique. A la manière de ce qu'on a vu en Iran avec le virus Stuxnet. »

En 2010, Stuxnet, un programme malveillant, sans doute coproduit par les services américains et israéliens, a été introduit dans les systèmes informatiques contrôlant les centrifugeuses iraniennes qui enrichissent l'uranium nécessaire à la fabrication de l'arme atomique.

« Le risque d'un cyber-11-Septembre »

« Le risque de demain, c'est un cyber-11-Septembre », a lancé en début d'année le député socialiste Eduardo Rihan Cypel, co-auteur du dernier Livre blanc sur la défense et la sécurité nationale.

La possibilité que des terroristes s'emparent des outils informatiques pour lancer « une cyberattaque massive » ne relève plus du fantasme. « Il faut se préparer à tous les scénarios possibles, jusqu'à des attaques massives financées par des groupes terroristes », estime le lieutenant-colonel Eric Freyssinet, chef de la division de lutte contre la cybercriminalité. Avant d'ajouter :

Malheureusement, les groupes terroristes ont de l'argent. Il n'y a qu'un pas pour qu'ils se munissent de cyber-armes, surtout qu'il n'y a pas besoin de beaucoup de moyens humains pour les utiliser, quelques dizaines de personnes suffisent pour lancer une attaque massive. »

Inquiétant. Pour autant, les officiels américains se veulent rassurant sur une éventuelle cyber-attaque contre le réseau électrique. Selon les autorités, citées par CNN, il faudrait des capacités techniques importantes pour comprendre le fonctionnement de l'infrastructure acheminant l'énergie, et encore plus pour la saboter. Surtout que l'ensemble est désormais surveillé par le FBI, mais aussi la CIA et la NSA.

Source :
http://tempsreel.nouvelobs.com/tech/20151019.OBS7872/daech-se-forme-au-piratage-le-risque-c-est-un-cyber-11-septembre.html
Par Boris Manenti