31 mai 2020
Espionnage

La NSA lance une alerte sur le piratage par les hackers russes de nos serveurs d'emails

La NSA a publié un avis selon lequel le groupe de pirates informatiques russes Sandworm, une unité de l'agence de renseignement militaire GRU, a exploité une vulnérabilité dans un agent de transfert de courrier couramment utilisé aux État-Unis, fonctionnant sur des serveurs d'emails dans le monde entier.

Avec Baptiste Robert

Atlantico : Jeudi, la NSA a publié un avis selon lequel le groupe de pirates informatiques russes connu sous le nom de Sandworm, une unité de l'agence de renseignement militaire GRU, a activement exploité une vulnérabilité connue dans Exim, un agent de transfert de courrier couramment utilisé aux État-Unis comme une alternative à des acteurs plus importants comme Exchange et Sendmail, fonctionnant sur des serveurs de courrier électronique dans le monde entier. Cette cyber attaque est-elle d'une autre nature que celle que les serveurs informatiques ont connus jusqu'à présent ?

Baptiste Robert : Un avertissement selon lequel des pirates informatiques exploitent des serveurs de courrier électronique vulnérables ne peut être considéré comme un événement inhabituel en général. Ils utilisent cette vulnérabilité pour mettre un « pied dans la porte » des différents serveurs ciblés et obtenir les données qu'ils veulent obtenir. C'est malheureusement un phénomène assez courant à l'heure actuelle. Tous les jours, des acteurs étatiques utilisent ce type d'opération afin de répondre à leurs besoins, que ce soit de l'espionnage industriel ou autre.

Dans ce cas précis, l'alerte a été donnée par l'Agence de sécurité nationale américaine et les pirates sont parmi les agents étatiques les plus dangereux au monde. Sandworm, dont l'identité en tant qu'unité du GRU a été confirmée pour la première fois par les gouvernements américain et britannique en février, est responsable des cyberattaques qui ont provoqué le black-out en Ukraine en 2015 et 2016, du ver NotPetya qui a infligé des dommages sans précédent de 10 milliards de dollars dans le monde en 2017, ainsi que des attaques contre plusieurs commissions électorales d'États américains en 2016 qui ont représenté un élément de l'ingérence de la Russie dans l'élection présidentielle cette année-là. Ce piratage devient de fait beaucoup plus alarmant. Pour autant cette affaire doit être prise avec des pincettes. Les enjeux sont ici d'avantage politiques que techniques.

Pourquoi la NSA a-t-elle choisie de communiquer sur cette question ?

C'est une façon pour les États-Unis de montrer à la Russie que la NSA voit ce que les hackers russes font, qu'ils sont capables de détecter leurs mouvements et de la prévenir d'une probable contre-attaque s'ils devaient recommencer.

Les citoyens peuvent-ils protéger leurs données e-mail malgré les failles des serveurs ?

La seule règle que peuvent appliquer les citoyens c'est d'utiliser la dernière version de tous les logiciels exploités par leurs

ordinateurs. Il faut savoir qu’il y aura toujours de nouvelles failles. Une personne suffisamment financée, suffisamment motivée sera toujours capable de trouver et d’exploiter cette nouvelle vulnérabilité dans le logiciel.