Cybersécurité : qui est Lazarus/Blueronoff, le groupe de pirates à l'origine de Wanacry ?

Kaspersky Lab a identifié « Lazarus/Blueronoff » depuis mars 2013 lorsque le groupe de pirates engage une campagne de piratage baptisée « DarkSeoul » en s'attaquant à des médias et des banques de Corée du sud.

» Ses liens avec la Corée du nord sont établis dès 2013 et reposent sur une analyse de sa victimologie, son infrastructure et les codes malveillants utilisés. Il est adepte des « false flags » et des avatars sur les réseaux sociaux. » explique Kasperky.

Selon l'éditeur, le groupe Lazarus/Blueronoff est responsable de plusieurs attaques majeures ces dernières années :

> L'attaque de sabotage contre Sony Pictures Entertainment en novembre 2014 suite à la diffusion de la comédie « L'interview qui tue ! »

> La réalisation du ver WannaCry à des fins de dissuasion en 2017

> Le cyber-braquage de la banque centrale du Bangladesh en février 2016, qui avait entrainé la perte de 81 millions de dollars.

Chercheur en cyber sécurité chez l'éditeur, Félix Aimé partage les informations sur cette organisation cybercriminelle.

« Il s'agit de la seule unité cybercriminelle sponsorisée par un état qui a fait du vol de fonds monétaires une priorité, un choix qui s'explique sans doute par les sanctions économiques qui pèsent aujourd'hui sur la Corée du Nord. »

« Le mode opératoire de Bluenoroff, et notamment son intérêt pour le réseau financier SWIFT, est particulièrement intéressant car révélateur de son influence, au-delà du monde cyber. En effet, non seulement les attaques contre SWIFT requièrent une expertise pointue des systèmes interbancaires mais surtout, l'argent dérobé doit ensuite être blanchi. Quand les sommes en question s'élèvent à plusieurs millions de dollars, comme c'est le cas pour Lazarus, cette dernière étape est extrêmement complexe et implique de disposer d'une structure criminelle solide. »

Crédit Photo-©-GlebStock-Shutterstock