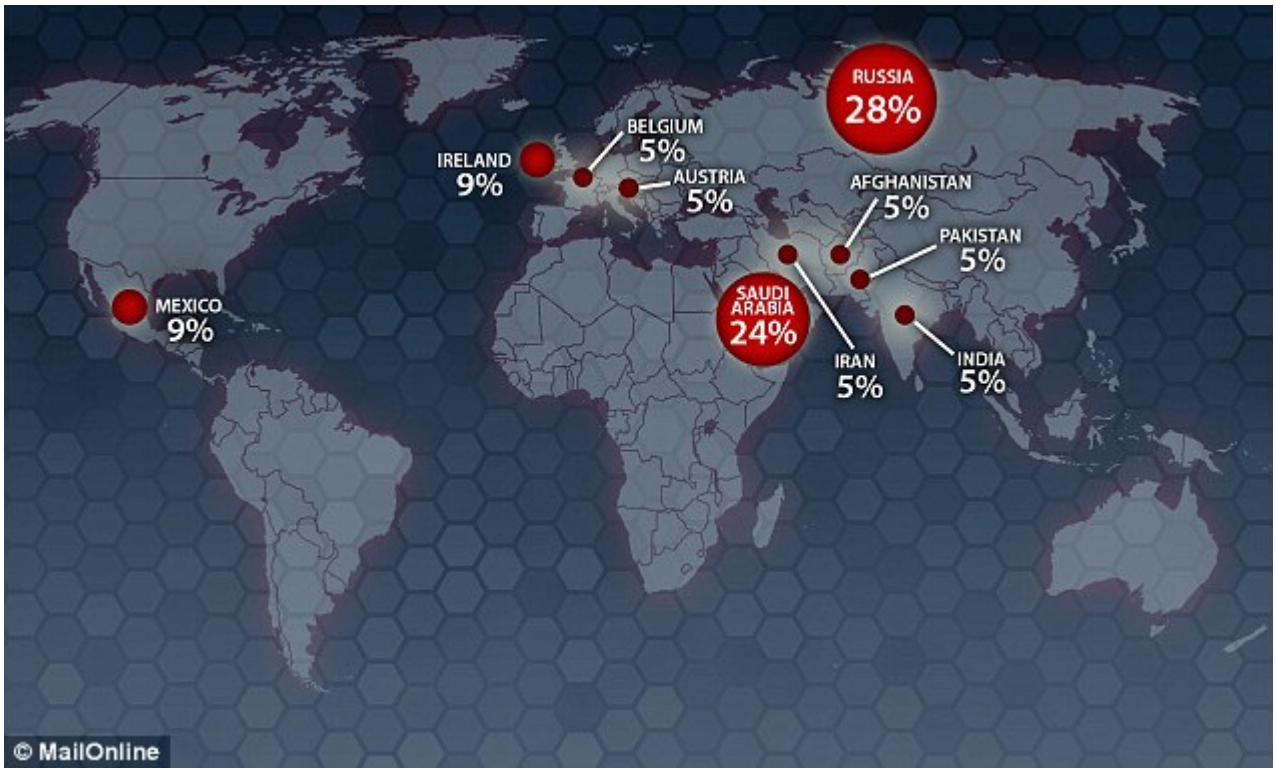
Quand je vous dis que la **cybercécurité est à prendre au sérieux…** Symantec, un grand groupe informatique spécialisé dans la sécurité informatique, **a découvert* ce week end un cheval de Troie extrêmement sophistiqué**, de type «backdoor», une porte dérobée informatique qui permet de s'introduire en toute transparence dans l'ordinateur infecté. «Regin», son petit nom, est extrêmement sophistiqué. Actif depuis plus de 6 ans, ce logiciel d'espionnage furtif n'est pas le fait d'un petit hacher ou d'un groupuscule. Sa complexité technique montre que son développement a, au minimum, été supervisée par les services de renseignement d'un Etat. En effet il a été développé sur plusieurs années, avec un investissement financier important.



%tage d'attaque de Regin par zone géographique

Regin n'est pas sans rappeler Stuxnet qui visait les centrifugeuses d'enrichissement de l'uranium en Iran. A contrario, sans réel but de destruction de données, ce logiciel espion cible des entreprises, des organisations gouvernementales et des instituts de recherche afin de collecter différents types de données (sensibles ou non) et non pas de saboter un système ou un process informatique. Il est capable de réaliser des captures d'écran, prendre le contrôle d'une souris et de son curseur, voler des mots de passe, surveiller le trafic d'un réseau, et récupérer des fichiers effacés.

Encore actif aujourd'hui, il est une réelle menace pour l'économie, l'industrie et

plus encore…

*Ce n’est pas vraiment une découverte mais un constat de la ré activation du virus qui avait disparu entre 2007 et 2013