BackdoorDiplomacy s'attaque aux représentations diplomatiques

Les chercheurs de l'éditeur ESET révèlent l'existence de BackdoorDiplomacy, Ce nouveau groupe de pirates sévit principalement contre des ministères des Affaires étrangères au Moyen-Orient et en Afrique. Plus rarement , il cible des entreprises de télécommunication.

La technique utilisée est connue : installer une porte dérobée (backdoor) en exploitant des applications vulnérables exposées à Internet sur des serveurs,

« BackdoorDiplomacy utilise des tactiques, des techniques et des procédures communes à d'autres groupes basés en Asie. Turian { le nom donné à la back door, NDLR} représente probablement l'évolution suivante de Quarian, dont l'utilisation a été observée pour la dernière fois en 2013 contre des cibles diplomatiques en Syrie et aux États-Unis, » explique Jean-Ian Boutin, Head of Threat Research chez ESET.

Un chiffrement déjà utilisé en Asie

Selon les chercheurs, le groupe de pirates est « capable de détecter les supports amovibles, notamment des clés USB, et de copier leur contenu dans la corbeille du disque principal ». Il est aussi en mesure de faire des captures d'écran et de créer, déplacer ou supprimer des fichiers

Ils ont aussi constaté que Turian utilise un protocole de chiffrement déjà utilisé pour attaquer des représentations diplomatiques du Kazakhstan et du Kirghizistan par un autre groupe de pirates basé en Asie. Un webshell une (interface web malveillante) lui aussi déjà utilisé par différents groupes fait aussi partie de l'arsenal d'outils de BackdoorDiplomacy.