Malware : Hammertoss se cache derrière Twitter pour voler des données

Les équipes de FireEye ont découvert un malware espion, baptisé **Hammertoss**, qui a la faculté de s'appuyer sur Twitter pour masquer ses actions malveillantes. L'objectif est de recevoir des commandes et de voler des données sans être détecter par les solutions de sécurité. La firme américaine soupçonne un groupe de pirates russes, connu sous le nom d'APT 29 probablement parrainé par le gouvernement d'être à l'origine de cette menace.

Dans un rapport, ils expliquent la complexité du malware qui fonctionne en 5 étapes. La première vise à analyser les différentes URL associés à l'identifiant de l'utilisateur comme @FireEye renvoie sur https://www.twitter.com/fireeye . L'objectif est de s'en créer une pour pouvoir dialoguer avec elle en même temps que l'utilisateur se connecte. Hammertoss dispose d'un algorithme pour créer chaque jour ce type d'association et analyser les fréquences d'utilisation (heures de bureau,vacances, quotidien, hebdomadaire).

Seconde étape, le malware va recevoir ses commandes sous la forme d'un tweet qui contient une URL plus un hastag qui lui servira pour extraire des instructions chiffrées dans une image. Troisième étape, dans la démonstration de FireEye, l'URL renvoie à un lien sur GitHub pour télécharger une image via Internet Explorer. En cas de détection, le groupe APT 29 peut changer d'URL pour pointer sur un autre site très rapidement.

De la stéganographie à l'extraction de données sensibles

4ème étape, Hammertoss récupère l'image depuis le cache du navigateur. Dans cette photo, les pirates ont placé des données chiffrées en utilisant le procédé de sténagographie. Hammertoss est donc capable de le déchiffrer avec le hashtag de la seconde étape et de l'exécuter. C'est la 5ème et dernière étape, une fois exécuté via PowerShell ou via une commande directe, le malware peut se créer un compte sur un service de stockage Cloud et extraire les données sensibles de l'utilisateur.

Hammertoss a été observé au début de l'année 2015 par les équipes de FireEye sur le réseau d'un de ses clients. Mais, ils concèdent qu'il est très difficile de détecter le malware, car il s'appuie sur le bruit du trafic réseau généré par Twitter pour cacher ses différentes actions. Les entreprises peuvent donc avoir du mal à savoir si elles sont piratées ou non. FireEye indique le groupe APT 29 cible particulièrement les organisations gouvernementales

A lire aussi :

Twitter patine sur le recrutement d'utilisateurs

Damien Viel va diriger Twitter en France

Crédit Photo : Ventura-Shutterstock