Slingshot : Kaspersky présente le malware comme ultra-sophistiqué

Le malware Slingshot a été présenté au Security Analyst Summit de la firme Kaspersky Lab qui s'est tenu à Cancun au Mexique du 7 au 11 mars dernier.

L'occasion pour l'éditeur russe de donner plus de détails sur ce logiciel malveillant découvert accidentellement, après avoir repéré un dll suspect répondant au nom de fichier scesrv.dll.

Selon la firme de sécurité informatique, il procède de manière très singulière en compromettant des **routeurs de marque MikroTik**. Si ce dernier aurait réglé le problème sur ses serveurs, d'autres types de serveurs pourraient également servir de vecteur d'infection à Slingshot.

Les routeurs infectés téléchargent des fichiers DLL (Dynamic Link Library) avant de les exécuter. Une première extension DLL téléchargée agit comme un cheval de Troie afin de télécharger ensuite divers autres fichiers malveillants.

Deux modules ultra-sophistiqués

Par ailleurs, Slingshot s'appuie sur deux modules que Kaspersky qualifie de chefs-d'oeuvre dans son billet de blog : **GollumApp** et **Cahnadr**.

Exécuté par le kernel de l'OS, ce dernier offre aux attaquants un contrôle total, sans aucune limitation, de l'ordinateur infecté. Malgré ce mode de fonctionnement via le kernel, il parvient à ne pas causer de crash. Ce qui le rend difficile à détecter.

GollumApp, est encore plus sophistiqué, avec près de 1500 fonctions de code utilisateur.

Ces deux piliers de Slingshot permettent de réaliser du cyberespionnage avec une kyrielle de possibilités telles que des captures d'écran, le sniffing des saisies au clavier, la collecte de données de réseau, de mots de passe, du presse-papier…

Le tout sans exploiter de faille dite zero-day.

Un malware très furtif

Mais, Slingshot se distingue également par sa capacité à passer sous le radar grâce à une multitude d'astuces mises en oeuvre.

Il dispose ainsi de son propre espace de fichiers chiffrés stockés sur le disque dur de l'ordinateur infecté. Slingshot se fend même d'une stratégie dite « anti-débogage » spécifique qui adopte les contre-mesures suivant les différentes solutions de sécurité.

Ce malware semble également avoir une longue durée de vie. A tel point qu'il est qualifié de menace persistante avancée (APT). De plus, le code malveillant étudié par les chercheurs étant

estampillé « version 6.x », cela tend à confirmer qu'il soit en activité depuis une lognue période.

Slingshot semble si sophistiqué qu'il est très probable qu'un Etat soit derrière la menace.

Enfin, Kaspersky Lab préconise de s'assurer que le routeur a été mis à jour avec la dernière version de son système d'exploitation. Il est aussi conseillé d'avoir recours à un logiciel de sécurité éprouvé.

(Crédit image : bloomua – Shutterstock.com)