Alerte : un malware Android commandé par… Twitter

Alerte : un malware Android commandé par… Twitter

Les concepteurs du malware Android Twittor se servent du réseau social pour envoyer des instructions à la souche infectieuse. Une technique plus furtive que les classiques serveurs de commande et contrôle.

L'éditeur d'antivirus Eset affirme avoir découvert le premier malware commandé… par des tweets. Selon la société slovaque, Android/Twittor est une application Android malveillante, probablement diffusée par SMS ou via des URL piégées, qui masque sa présence et se connecte à un compte Twitter dans l'attente d'instructions. Ces dernières peuvent le conduire à télécharger une autre app malveillante ou à changer de compte Twitter de contrôle. Actuellement, selon Eset, Twittor sert à importer différentes versions d'un malware bancaire. Mais pourrait tout aussi bien passer au ransomware…

« *Utiliser Twitter plutôt que des serveurs de commande et contrôle (C&C) est plutôt innovant pour un botnet Android* », souligne Lukas Stefanko, le chercheur d'Eset qui a mis au jour cette nouvelle souche infectieuse. L'objectif des cybercriminels est, comme l'indique ce chercheur, de constituer un réseau de machines esclaves, soit un botnet. Le point faible des constructions de ce type réside souvent dans l'envoi régulier d'instructions aux éléments de ce réseau, des communications susceptibles de révéler l'existence du botnet. Par ailleurs, les serveurs C&C constituent le maillon faible des botnets : si les autorités les localisent et parviennent à les fermer, c'est tout le réseau criminel qui s'effondre.

Passer d'un compte Twitter à un autre

Autant de raisons qui pourraient avoir poussé les concepteurs de Twittor à complexifier les techniques de communication entre les machines esclaves et l'entité les contrôlant, selon Eset. En plus de l'emploi de Twitter, les cybercriminels chiffrent leurs messages et utilisent des topologies complexes pour leur architecture de C&C, avance l'éditeur. « *Ces canaux de communication sont difficiles à mettre au jour et encore plus difficiles à bloquer totalement*, reprend Lukas Stefanko. *De l'autre côté, il est très simple pour les escrocs de rediriger les communications vers un compte nouvellement créé.* » Et pas de risque de voir la police fermer purement et simplement Twitter pour ce motif…

Dans l'univers Windows, dès 2009, un botnet a eu recours à Twitter, fondé seulement 3 ans auparavant, pour envoyer des instructions. Mais Twittor est bien le premier malware créateur de bot commandé via le réseau social.

Article original de Reynald Fléchaux

Réagissez à cet article

Original de l'article mis en page : Inédit : un malware Android commandé par… Twitter