Cyber Threat Intelligence en boucle courte avec un Honey Net

Laurent Aufrechter

Thales
laurent.aufrechter@thalesgroup.com

Résumé

Classiquement, les Honey Pots ont été utilisés pour mesurer les activités malveillantes sur Internet. Des Honey Pots ont ainsi été exposés avec comme objectif de découvrir de nouveaux modes d'attaques, ou des listes de mots de passe utilisées en « brut force ». La Cyber Threat Intelligence s'appuie en grande partie sur ce type de dispositifs. Cela permet de fournir des informations pertinentes pour la majorité des entreprises et des utilisateurs. Cependant, pour une société ayant des activités dans un domaine particulier ou étant suffisamment intéressante pour justifier du développement de moyens d'attaque spécifiques, il est parfois difficile de savoir si ces informations sont suffisamment précises.
Cette communication explique comment un Honey Net (sous-réseau hébergeant des Honey Pots) connecté au réseau d'entreprise peut permettre de créer une capacité de Cyber Threat Intelligence locale en complément des informations ciblées sur le domaine d'activité de cette entreprise.

Mots clés :
Honey Pot, Honey Net, Cyber Threat Intelligence