Avec Threat Extraction, Check Point nettoie les documents avant livraison

La sécurité informatique est souvent une question de gestion de risques, mais elle nécessite parfois un changement de façon de penser. Avec Threat Extraction qui sera disponible à partir du 1er avril prochain, Check Point propose de nettoyer les pièces jointes des mails avant leur ouverture. L'approche traditionnelle de protection d'une entreprise contre les documents infectés consiste à rechercher les malwares alors même qu'ils ont déjà produits leurs effets.

Pour Philippe Rondel, directeur technique de Check Point en France, « *le service se focalise sur la messagerie avec comme objectif de traiter a priori tous les fichiers pour retourner in fine des fichiers sains. Il faut être plus proactif sur une application comme la messagerie qui est encore largement utilisée* ». Concrètement, Threat Extraction procède à « *la désactivation d'éléments actifs comme les macros dans les documents ou les liens externes* », précise le responsable. Ce service est paramétrable pour définir des politiques de sécurité en matière de pièce jointe.

Cette fonctionnalité vient en complément du service Threat Emulation, une sandbox pour éviter les attaques classiques à travers les documents PDF corrompus ou l'ingénierie sociale. Si on ajoute un IPS (système de prévention d'intrusion), la firme israélienne fournit un package pour un tarif débutant à 3500 dollars. On notera que l'éditeur travaille aussi à l'intégration de Hyperwise, société achetée en février dernier, focalisée sur la détection des menaces dès la phase de pré-infection.

A lire aussi :

Amnon Bar-Lev, CheckPoint : « les botnets envahissent les entreprises

Crédit Photo : Wavebreakmedia-shutterstock