Sécurité : des chercheurs de Cisco ralentissent le kit Angler

Talos Research Group est une entité de Cisco dédiée à la sécurité. Elle regroupe des chercheurs qui viennent de porter un coup au kit d'exploits nommé Angler et notamment à une campagne de ransomware (combinant CryptoWall and TeslaCrypt).

Cette trousse à outils est devenue, en l'espace de quelques années, une référence pour les cybercriminels. SophosLab a récemment établi un palmarès où Angler détient 82,2% de part de marché sur ce secteur des outils de piratage. Angler intègre des failles zero day, des malwares, des techniques d'attaques, etc. Il a surtout réussi à prendre la place laissée vacante par BlackHole dont le fondateur a été arrêté en 2013.

Débrancher des serveurs proxy

Dans son enquête l'équipe de Cisco a découvert que les serveurs proxy utilisés par Angler provenaient de serveurs de Limestone Networks, un fournisseur de Dallas. Ces serveurs représentaient jusqu'à 50% de l'activité du kit Angler, ciblant 90 000 victimes par jour pour un revenu annuel estimé à 30 millions de dollars. En extrapolant, cela signifie qu'Angler génére chaque année 60 millions de dollars de revenus.

Après la découverte des serveurs proxy, Limestone Networks les a débranché et remis les données aux chercheurs de Cisco. Ils ont travaillé en collaboration avec l'opérateur Level3 pour récupérer les protocoles d'authentification et détecter les terminaux infectés au sein des entreprises. Les données issues des serveurs proxy donnent une cartographie et le modus operandi d'Angler. Des informations qui permettent de ralentir la propagation des menaces issues de ce kit, mais pas de le supprimer définitivement.

A lire aussi :

Télégrammes : Angler kit dominant, Oracle Android again, Google Nearline 100 Po, Microsoft Send
Hackers, Etats et Dark Web : le marché des failles Zero Day incontrôlable ?

crédit photo © Oleksandr Lysenko – shutterstock