https://www.zurbains.com/internet/facebook-un-terreau-fertile-pour-la-proliferation-de-logiciels-malveillants.html

Facebook, un terreau fertile pour la prolifération de logiciels malveillants

- Internet -

Date de mise en ligne : mardi 2 juillet 2019

Check Point Software Technologies Ltd. est l'un des principaux fournisseurs de solutions de cybersécurité pour les gouvernements et les entreprises dans le monde. Voici le compte-rendu de leur découverte.

Propagation de logiciels malveillants dans les environnements de bureautique et mobiles, via Facebook

Il semble que la situation politique tendue en Libye soit utile à certains, qui l'utilisent pour inciter leurs victimes à cliquer sur des liens et télécharger des fichiers censés fournir des informations sur les raids aériens ou la capture de terroristes dans le pays, mais qui contiennent en réalité des logiciels malveillants.

Page Facebook de Khalifa Haftar

Notre enquête a commencé lorsque nous sommes tombés sur une page Facebook se faisant passer pour Khalifa Haftar, le commandant de l'armée nationale libyenne. En plus d'être maréchal, Haftar est une figure importante de l'arène politique libyenne. Il a joué un rôle majeur en tant que chef militaire durant la guerre civile qui continue de déchirer le pays. Grâce à cette page Facebook, nous avons pu relier cette activité malveillante au pirate qui en est l'auteur, et découvrir comment il tirait parti de la plate-forme de réseau social depuis des années, en compromettant des sites web légitimes pour héberger des logiciels malveillants, puis en faisant des dizaines de milliers de victimes principalement en Libye, mais également en Europe, aux États-Unis et au Canada.

Grâce à ces informations que nous avons communiquées, Facebook a supprimé les pages et les comptes qui diffusaient des éléments malveillants dans le cadre de cette opération. Nous avons découvert par la même occasion plusieurs pages Facebook apparemment sans rapport, suivies par des milliers d'utilisateurs, et avons pu trouver le pirate les exploitant pour propager des logiciels malveillants. Nous avons pu observer l'évolution de ce pirate depuis l'époque de la dégradation de sites web jusqu'au lancement de campagnes plus sophistiquées.

Bien que l'ensemble des outils utilisés par le pirate ne soit ni avancé ni impressionnant en soi, l'utilisation de contenus personnalisés, de sites web légitimes et de pages très actives avec de nombreux abonnés facilitait considérablement l'infection de milliers de victimes. Les informations sensibles partagées dans le profil « Dexter Ly » impliquent que le pirate aurait réussi à infecter des responsables de haut rang.

Le pirate ne soutien apparemment aucun parti politique ni aucune des parties en conflit en Libye, mais ses actions semblent être motivées par des événements politiques, comme le sous-entend sa participation à des opérations telles que OpSyria il y a de cela plusieurs années, ainsi que sa volonté d'exposer des informations personnelles et des documents secrets dérobés au gouvernement libyen. Cela en parallèle du ciblage constant de victimes libyennes, qui pourrait cependant signifier que le pirate s'intéresse particulièrement à certains individus au sein de la foule.

Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (https://www.checkpoint.com) est l'un des principaux fournisseurs de

solutions de cybersécurité pour les gouvernements et les entreprises dans le monde. Les solutions de Check Point protègent les clients des cyberattaques de 5e génération grâce à un taux de blocage inégalé des logiciels malveillants, des logiciels rançonneurs et autres menaces ciblées avancées. Check Point propose « Infinity Total Protection avec prévention avancée des menaces de 5e génération », une architecture de sécurité à plusieurs niveaux, qui défend les Clouds, les réseaux et les appareils mobiles des entreprises. Check Point fournit le système d'administration unifiée de la sécurité le plus complet et le plus intuitif. Check Point protège plus de 100 000 entreprises de toute taille.