Les chercheurs d'ESET ont récemment découvert des sites web diffusant des applications de négociation de cryptomonnaie pour Mac contenant un cheval de Troie. Il s'agit d'applications légitimes détournées par le malware GMERA, utilisées par des cybercriminels pour voler des informations telles que des cookies de navigateur et des portefeuilles de cryptomonnaie, et effectuer des captures d'écran. Dans le cadre de cette campagne, l'application commerciale légitime Kattana a été rebaptisée, des sites web similaires ont été créés, et le malware a été intégré à son programme d'installation. Les chercheurs d'ESET ont noté quatre noms différents utilisés dans cette campagne pour l'application comportant le cheval de Troie : Cointrazer, Cupatrade, Licatrade et Trezarus.

« Comme lors de campagnes précédentes, le malware accède à un serveur de commande et de contrôle via http (C2, C&C), et se connecte à un autre serveur de commande et de contrôle via des sessions terminal distantes à l'aide d'une adresse IP codée en dur, » explique Marc-Etienne Léveillé, le chercheur d'ESET qui a mené l'enquête sur GMERA.

Les chercheurs d'ESET n'ont pas encore été en mesure de trouver la source exacte de ces chevaux de Troie. Cependant, en mars 2020, le site légitime de Kattana comportait une note avertissant que des victimes étaient approchées individuellement pour les inciter à télécharger une fausse application, ce qui semble indiquer des tentatives d'ingénierie sociale. Des sites web similaires sont mis en place pour donner l'impression que le téléchargement est légitime. Le bouton de téléchargement sur les faux sites est un lien vers une archive ZIP contenant le programme d'installation du cheval de Troie.

En plus de l'analyse du code du malware, les chercheurs d'ESET ont également mis en place des leurres sous la forme de honeypots pour attirer les exploitant de GMERA et leur donner le

contrôle à distance les honeypots. L'objectif des chercheurs était de révéler les motivations de ce groupe de cybercriminels. « D'après les activités dont nous avons été témoins, nous pouvons confirmer que les pirates ont collecté des informations sur les navigateurs, telles que des cookies et l'historique de navigation, des portefeuilles de cryptomonnaie et des captures d'écran, » conclut M. Léveillé.
Pour plus de détails techniques sur la dernière campagne malveillante de GMERA, consultez l'article complet « Mac cryptocurrency trading application rebranded, bundled with malware » sur WeLiveSecurity. Suivez l'actualité d'ESET Research sur Twitter.