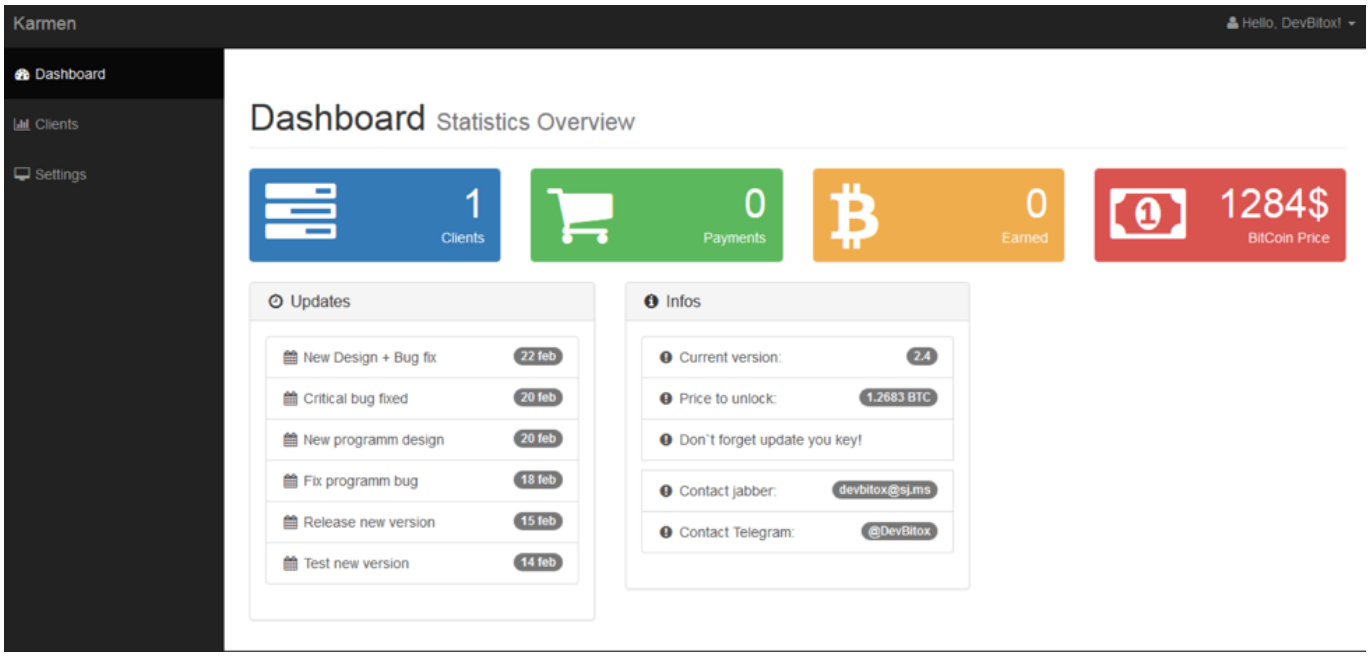
Prenez garde à Karmen, le ransomware low-cost

Un service de ransomware à des prix défiant toute concurrence ? C'est en tout cas ce à quoi ressemble Karmen, déniché par les chercheurs de Recorded Future, spécialisée dans l'intelligence sur la menace. Car, dans le monde des cybercriminels aussi, les tâches sont taylorisées, avec des développeurs de menaces qui mettent leurs créations à disposition d'autres cybercriminels sous forme de service. C'est dans cette famille que se range Karmen, qui offre à des malfaiteurs souhaitant lancer une campagne infectieuse un service de ransomware (RaaS, pour ransomware as-a-service). Le RaaS peut être exploité par à peu près quiconque – le niveau d'expertise requis étant très limité -, et à bas coût (175 dollars seulement, soit un peu plus de 160 euros).



Pour le reste, Karmen se configure comme un logiciel SaaS standard : on détermine le prix de la rançon, la durée dont disposent les victimes pour s'en acquitter et les moyens de communiquer avec elles. La console d'administration se présente comme un tableau de bord permettant aux cybercriminels de faire, à tout instant, le bilan de leur campagne infectieuse. « *Le ransomware Karmen est vendu comme une variante de ransomware, à laquelle on accède via un paiement unique au démarrage. Ce qui permet à un acheteur de conserver 100 % des montants versés par les victimes* », résume Recorded Future, dans un billet de blog.

20 licences de Karmen seulement ?

En pratique, Karmen s'apparente à un ransomware Open Source appelé Hidden Tear, une souche publiée en août 2015 par un chercheur en sécurité turc. Deux versions de Karmen sont proposées, la mouture light ne proposant la fonctionnalité de détection des outils de protection (bacs à sable, et outils d'analyse). Recorded Future explique avoir découvert cette souche début mars sur les forums underground ; elle était proposée par un cybercriminel russophone connu sous les pseudos DevBitox et Dereck1. Selon les chercheurs, il s'agirait du premier projet 'commercial' de ce

hacker. DevBitox aurait prévu de vendre 20 'licences' de son outil de RaaS. Dans leur billet de blog, les chercheurs indiquent que seulement 5 copies restent disponibles.

Les premiers cas d'infection par Karmen remontent à décembre 2016, avec des victimes identifiées en Allemagne et aux Etats-Unis. Le ransomware chiffre les données sur les PC infectés avec l'algorithme AES-256. Signalons que le projet NoMoreRansom, une initiative conjointe des forces de police et de l'industrie, dispose désormais d'un outil gratuit permettant de déchiffrer les données prises en otage par Hidden Tear (et Karmen).

A lire aussi :

Ransomwares : 38 % des victimes paient leur rançon

Ransomware : les cybercriminels font maintenant la tournée des hôtels

Comment le ransomware est devenu le gagne-pain des cybercriminels

Photo : portalgda via Visual Hunt / CC BY-NC-SA