Créer des ransomwares, une petite entreprise qui rapporte

Fournisseur d'analyses des Deep et Dark web, Flashpoint a étudié les dessous d'une campagne de *« ransomware-as-a-service »* (RaaS) pilotée, selon lui, par des escrocs russes. Le RaaS consiste pour l'auteur du rançongiciel à proposer à d'autres de diffuser des versions personnalisées de son programme pour chiffrer les données et verrouiller les terminaux d'utilisateurs. Les cibles sont appelées à payer en cryptomonnaie pour reprendre le contrôle de leurs données. La rançon est perçue par l'auteur du ransomware qui la partagera ensuite avec les diffuseurs.

C'est ainsi qu'une pointure des ransomwares en Russie aurait mené la campagne RaaS étudiée ces cinq derniers mois par Flashpoint. L'auteur de la campagne, qui ciblait des entreprises occidentales et des particuliers depuis au moins 2012, selon Flashpoint, aurait recruté des diffuseurs du programme ayant pour mission de trouver et infecter des cibles en échange d'un pourcentage sur les profits générés. Les novices étaient également invités à se lancer, sans frais d'entrée, le programme malveillant à diffuser étant accompagné d'instructions détaillées qu'un *« écolier »* pourrait suivre.

L'appât du gain

Le *« patron »* russe aurait ainsi recruté 10 à 15 *« affiliés »* chargés de diffuser le code de son ransomware. Soit en achetant un accès à des ordinateurs infectés, soit en passant par des serveurs insécurisés, ou du spam, ou encore en leurrant des utilisateurs de sites de rencontre et réseaux sociaux. Une fois que le code est installé et s'exécute, son auteur se charge des communications avec les victimes pour obtenir une rançon d'un montant moyen de 300 dollars par clé de déchiffrement et par victime, mais une somme additionnelle peut être exigée avant l'envoi de la clé.

Pour le paiement, la cryptomonnaie Bitcoin a été utilisée. 40 % des fonds ainsi détournés auraient été partagés entre les affiliés et 60 % seraient revenus au pilote de la campagne. Le *« boss du ransomware »* aurait ainsi empoché 7 500 dollars par mois en moyenne (90 000 dollars par an) et ses affiliés près de 600 dollars par mois chacun. Cela représente près de 30 paiements de rançon par mois.

« Nos résultats contestent la perception commune de cybercriminels hors du commun, éclairés, aisés, inaccessibles, inexposables et inarrêtables », soulignent les auteurs de l'étude. Et *« Les montants des revenus du ransomware ne sont pas aussi séduisants et juteux »* que l'on pourrait le croire. Il n'empêche, ces montants sont bien supérieurs au salaire moyen russe passé, selon une analyse de la Sberbank citée par RFI, de 1058 dollars par mois en 2012 à 433 dollars par mois en 2016.

Lire aussi :

Ransomwares : ingéniosité, perversité et persévérance

Les ransomwares tirent et réclament à tout va

crédit photo © frank_peters / Shutterstock.com