Ransomware : un retour sur investissement très lucratif

En début de semaine, G-Data donnait un aperçu des tarifs pratiqués sur le blackmarket pour acheter des attaques ou des exploits. Ce catalogue montrait que les méthodes les plus recherchées comme les failles zero day peuvent se monnayer plusieurs dizaines de milliers d'euros.

Une autre étude montre que le métier de cybercriminel est très lucratif. Dans son rapport Global Security 2015, Trustwave prend l'exemple d'une campagne de ransomware pour démontrer le niveau de retour sur investissement. Et le moins que l'on puisse dire, c'est que la rentabilité est au rendez-vous avec un taux de 1425%. Non, vous ne rêvez pas !

Entrons dans les détails de la campagne. Pour un mois d'offensive, le cybercriminel va investir 5900 dollars dans la création du ransomware. Ce poste se décompose en 3000 dollars pour l'acquisition d'une variante de CTB-Locker sur le marché souterrain, 1800 dollars pour de l'acquisition de trafic (à raison de 20 000 visites quotidiennes). Il faut compter en plus 500 dollars pour un kit d'attaque (en l'occurrence RIG Exploit pour piéger les utilisateurs) et 600 dollars pour masquer le ransomware face aux anti-virus.

ITEM	TOTAL INVESTMENT
Payload	– $3,000
Infection Vector	– $500
Traffic Acquisition	– $1,800
Daily Encryption	– $600
Total Expenses	– $5,900

Attaquer plus pour gagner plus

Trustwave estime à 10% le taux d'infection sur les 20 000 visites quotidiennes. Seul 0,5% des utilisateurs infectés paieront 300 dollars pour déverrouiller leur ordinateur. Le revenu total généré sur 1 mois est de **90 000 dollars**. Au final, le calcul du ROI aboutit au taux mirobolant de 1425%. Un taux exceptionnel pour une attaque qui n'a nécessité aucune écriture de lignes de code.

Le rapport souligne avoir eu une approche « conservatrice » sur les différents tarifs et sur les

objectifs de l'attaque. Trustwave souligne notamment qu'un même cybercriminel peut mener plusieurs frappes en simultané. On se souvient de Cryptolocker, un ransomware particulièrement virulent qui se servait du botnet GameOver Zeus pour prospérer. Lors d'une enquête pour stopper ce botnet, les autorités ont constaté qu'aux Etats-Unis le ransomware avait frappé 20 000 PC et récolté 27 millions de dollars en 2 mois.

A lire aussi :

Sécurité : DSI et direction juridique unies, mais dialogue à approfondir

Cybercrime : un coût de 2100 milliards de dollars pour les entreprises d'ici 2019

Crédit Photo : Andrey Armyagov-Shutterstock