Comment un chercheur français a infecté des arnaqueurs avec Locky

Un chercheur en sécurité, Ivan Kwiatkowski, explique dans un billet de blog comment il a convaincu des escrocs en ligne (*scammers*) d'installer le ransomware Locky.

Tout commence lorsque les parents de ce chercheur français ont atterri sur une page web douteuse. Celle-ci indiquait que leur système, Windows, avait détecté une infection par le virus Zeus, et les invitait à composer le numéro d'un prétendu *« support technique »* pour s'en débarrasser… Après s'être assuré du bon fonctionnement du PC familial, le spécialiste veut en savoir davantage sur les arnaqueurs ayant tenté d'abuser ses parents.

Pour ce faire, le chercheur lance une machine virtuelle (VM) sous Windows XP, puis compose le numéro indiqué. Ivan Kwiatkowski dit avoir eu trois communications téléphoniques avec deux interlocuteurs d'un centre d'appels vraisemblablement basé en Inde. Leur français est hésitant.

L'arnaqueur arnaqué

Lors du dernier appel, le chercheur prétend accepter l'achat d'un pack de support et donne un premier numéro de carte bancaire valide (de test), puis un autre. L'escroc tente, à plusieurs reprises et sans succès, d'effectuer une transaction bancaire avec ces numéros.

C'est alors qu'Ivan Kwiatkowski a l'idée d'ouvrir le dossier spam de sa messagerie et d'y récupérer un programme d'installation de Locky, programme qu'il dépose dans sa machine virtuelle de test. Il s'agit d'une archive ZIP contenant un fichier JavaScript qui, une fois exécuté, télécharge et installe le célèbre ransomware…

Ensuite, le chercheur fait passer ce fichier pour la photo de sa carte bancaire, prétextant une mauvaise vue. Et utilise pour ce faire la fonction de partage de fichiers du client d'assistance de l'arnaqueur. Puis invite l'escroc à l'ouvrir, prétendument pour qu'il lise et tape les numéros lui-même… Après un moment, l'opérateur aurait indiqué : *« j'ai essayé d'ouvrir votre photo, mais il ne se passe rien »*. Or, pendant ce temps, un processus chiffrait, à son insu, son système de fichiers avec le ransomware Locky.

La conclusion que dresse Ivan Kwiatkowski est des plus limpides : *« quand on tombe sur une arnaque de ce type, il me semble que l'acte civique est de prétendre qu'on est dupe. Ma logique est la suivante : les arnaqueurs n'ont pas la possibilité de faire la différence entre les véritables victimes et ceux qui font semblant : leur business plan part du principe que seuls les gens les plus crédules vont mordre à l'hameçon. Si en revanche une pluie de faux pigeons s'abattait sur eux, leur charge de travail augmenterait tellement que leurs arnaques ne seraient plus profitables. Si vous parlez français, je vous invite donc à prendre 15 minutes de votre temps, les appeler au +339 75 18 77 63 et les pousser à faire quelque chose de drôle »*.

Lire aussi :

Ransomwares : ingéniosité, perversité et persévérance

Le ransomware Locky mute pour multiplier ses victimes en France

crédit photo © adlike / Shutterstock.com