Ransomware Locky : la France parmi les deux principaux pays ciblés

Selon une analyse de l'éditeur Kaspersky, les attaques du ransomware Locky se sont avant tout concentrées sur l'Allemagne (où l'éditeur russe en a identifié 3 989) et sur la France (2 372). Ces chiffres, qui ne prennent pas en compte les attaques qui ont pu être déjouées avant le téléchargement du ransomware, montrent que les deux côtés du Rhin ont été – et de loin – les premières cibles des pirates. Troisième, le Koweit n'a enregistré 'que' 976 attaques. Les États-Unis en totalisent seulement 188, même si, outre Atlantique, l'une des victimes, un hôpital à Hollywood, a bénéficié d'une exposition médiatique considérable.

Country	Number of attacks
Germany	3989
France	2372
Kuwait	976
India	512
China	427
South Africa	220
United States	188
Italy	128
Spain	105
Mexico	92

Au total, **114 pays ont été ciblés**. « *Il apparaît que la fonction la plus dangereuse et la plus remarquable de Locky n'est pas logé dans son code, mais plutôt dans sa propagation très agressive* », explique l'auteur de l'analyse de Kaspersky Lab, Fedor Sinitsyn. Celui-ci revient aussi sur les mutations qu'a connues le ransomware pour mieux atteindre ses cibles. Après avoir d'abord misé sur **une infection via des macros** de Microsoft Office placées en pièces jointes d'e-mails, le kit de téléchargement Locky a **ensuite été logé dans une archive Zip** renfermant un code Javascript malicieux.

Comment Locky endort l'utilisateur

« *Cela est peut-être dû au fait que les dernières versions de Microsoft Office n'acceptent plus par défaut les macros* », explique Fedor Sinitsyn. Pour améliorer le taux d'infection, donc la rentabilité de leurs actions, les pirates se seraient donc tournés vers une nouvelle technique contournant les sécurités mises en place par Microsoft. Avec les kits de téléchargement Javascript, l'utilisateur n'aura pas à passer outre un message d'avertissement le prévenant qu'il est sur le point d'ouvrir un fichier potentiellement dangereux.

Une fois en place, Locky, un malware de **100 Ko développé en C++** et compilé avec Microsoft Visual

Studio, se déploie sur le système et efface des fichiers qui permettent habituellement à Windows de prévenir l'utilisateur que des éléments suspects ont été téléchargés depuis Internet. Le ransomware commence alors à dialoguer avec un centre de commande et de contrôle, afin de signaler la réussite de l'infection et de recevoir une clef de chiffrement RSA-2048 ainsi qu'un identifiant se rapportant au système corrompu. A partir de là, le mécanisme de blocage par chiffrement des données de l'ordinateur infecté, via la recherche de fichiers comportant certaines extensions, puis de demande de rançon peut s'enclencher.

Fedor Sinitsyn note que le russe et d'autres langues de l'ex-Union soviétique sont supportés par le processus de demande de rançon… alors que ces pays n'ont pas été l'objet de campagnes d'attaques via Locky. « *Pour une raison quelconque, les cybercriminels n'ont pas été très enthousiastes à l'idée de cibler des utilisateurs dans des pays où ces langues sont parlées* », écrit le chercheur. Les experts en cybersécurité y voient souvent un indice du fait que les cybercriminels sont basés dans ces pays.

A lire aussi :

Ransomware Locky : l'AFP touchée, son RSSI témoigne

Le ransomware Locky mute pour multiplier ses victimes en France

Le ransomware Locky inonde la France, via de fausses factures Free Mobile

Crédit photo : Carlos Amarillo / Shutterstock