Popcorn Time : le ransomware qui se refile aux amis pour éviter de payer

Il fallait oser et les cybercriminels ont sauté le pas. Les chercheurs de Malware Hunter Team ont découvert sur le Dark Web, un ransomware d'un genre un peu particulier dans son mode opératoire. Nommé Popcorn Time (sans avoir de lien de parenté avec le service de vidéo décrié), il infecte d'abord un utilisateur en chiffrant ses données. Il est capable de bloquer jusqu'à 500 types de fichiers et il est configuré pour verrouiller les fichiers en AE-256 avec l'extension .filock.

Pour récupérer ses données, la victime a 2 options. La première est de payer la rançon à savoir 1 bitcoin, soit un peu plus de 770 dollars. Pour y échapper et récupérer ses informations gratuitement, les cybercriminels proposent d'envoyer un lien de parrainage à des contacts pour les infecter et leur demander également une rançon. *« Nous sommes désolés de vous dire que votre ordinateur et vos fichiers ont été chiffrés, mais attendez, ne vous inquiétez pas. Il y a une manière de restaurer votre ordinateur et tous vos fichiers … Envoyez le lien ci-dessous à d'autres personnes, si deux ou plusieurs personnes installent le fichier et payent, nous décrypterons vos fichiers gratuitement. »* Un moyen diabolique de faire payer les autres pour se débarrasser du rançongiciel.

Les cybercriminels rajoutent des fonctions perverses

Popcorn Time est encore en développement souligne Bleepingcomputer qui a eu accès au code du ransomware. En effet, pour éviter d'être contourné, le ransomware prévoit une fonction qui efface les données si la victime tape 4 mauvaises clés pour déchiffrer ses fichiers. De même, le verrouillage est actif pendant 1 semaine avec un compte à rebours pour la paiement de la rançon ou l'envoi du lien à des amis.

La revendication de ce ransomware sur le mode collaboratif et crowdfunding est un peu nébuleuse. Il s'agirait « d'un groupe d'étudiants syriens en informatique » et d'expliquer les effets de la guerre en Syrie. Les fonds récoltés de cette extorsion de fonds vont servir, selon eux, « *à apporter de la nourriture, des soins, des abris à notre peuple* ». Si les motivations et les revendications sont à prendre avec des pincettes, il n'en demeure pas moins que *le modus operandi* existe et qu'il peut faire des ravages au sein d'une entreprise par exemple.

A lire aussi :

Le ransomware Locky s'invite sur Facebook

Ransomwares : les entreprises françaises touchées, se distinguent