Sécurité : le ransomware Cryptowall 2.0 contourne les antivirus

Des chercheurs de **Cisco** se sont penchés sur la dernière version de **Cryptowall**. Ce dernier est un *ransomware*, qui bloque l'accès aux données stockées sur un ordinateur (lesquelles sont chiffrées), forçant l'utilisateur à payer pour en retrouver l'usage.

Cryptowall 2.0 utilise le réseau Tor pour masquer ses communications avec le cybercriminel ayant pris le contrôle de la machine. Depuis un même binaire, il sera également capable de produire **du code x86 32 bits ou 64 bits**. Le virus utilisé est ainsi adapté aux deux versions principales de Windows.

Un détecteur de détecteurs

Cryptowall 2.0 est particulièrement malin. Les offres de sécurité les plus récentes s'appuient sur de la virtualisation applicative pour tester le code d'un logiciel nouvellement téléchargé et en mesurer ainsi la dangerosité.

Le malware est ici capable de détecter de telles techniques de virtualisation. Si le binaire infecté fonctionne dans une machine virtuelle ou au sein d'un bac à sable, l'extraction de Cryptowall est avortée. **Il n'y a donc rien à détecter et l'antivirus signalera le fichier comme non contaminé.** Sauf que son utilisation mènera cette fois-ci bel et bien à l'extraction et l'installation de Cryptowall sur votre machine.

La connexion au centre de commande du pirate s'effectue pour sa part **en SSL sur un serveur placé sur le réseau Tor**. Il est donc quasi impossible de remonter à la source de l'attaque.

Cette menace est à ce jour particulièrement difficile à détecter et à stopper. Seule réelle parade : **sauvegarder régulièrement ses données sur des disques amovibles**, ou – pour les entreprises – protéger avec soin le serveur de fichiers des attaques menées depuis des machines infectées présentes sur le réseau local, et bloquer l'accès au réseau Tor.

À lire aussi :
Données personnelles et objets connectés au centre des attaques en 2015
Des chercheurs élaborent un malware via l'interface utilisateur des apps mobiles
La NSA, fournisseur numéro un de malwares dans le monde ?