Des ransomwares sur Linux : autres moyens, autres objectifs ?

Les transports publics de Montréal, le système judiciaire brésilien… RansomEXX a fait des victimes de marque ces dernières semaines.

Découvert en juin, il entre dans la catégorie des « gros » *ransomwares*. En tout cas au vu des attaques qui l'impliquent. Il n'en est que l'ultime stade, consécutif à des infiltrations méthodiques sur les réseaux informatiques des entités ciblées.

Ces dernières ont d'ailleurs leur nom codé en dur dans l'exécutable malveillant qui leur est adressé. RansomEXX utilise cette information pour personnaliser la note et l'adresse mail de rançon, ainsi que l'extension qu'il accole aux fichiers chiffrés.

On connaissait jusqu'alors l'exécutable en question sous une forme visant les systèmes Windows. Mais il semble qu'une version Linux a commencé à émerger. Kaspersky lui trouve en tout cas une grande ressemblance avec la variante de RansomEXX exploitée en juin dernier contre l'autorité régulatrice des transports au Texas.

La méthode de compilation est différente, mais l'organisation du code laisse peu de doute. Surtout si on additionne le contenu du message de rançon et l'exploitation de la bibliothèque mbedtls pour implémenter les fonctions cryptographiques.

RansomEXX n'est pas le premier

La probable « version Linux » de RansomEXX consiste en un exécutable .elf 64 bits nommé svc-new. Pour chiffrer les fichiers, il emploie une clé AES-ECB 256 bits générée à la volée et elle-même chiffrée avec une clé publique RSA-4096 codée en dur. Par rapport à la version Windows, il n'y a pas de fonctionnalités supplémentaires qui permettraient par exemple de tuer des processus ou de se connecter à un serveur distant.

D'autres *ransomwares* ont déjà ciblé les systèmes Linux. PureLocker, repéré il y a environ un an, en est un exemple. Il était longtemps resté sous les radars grâce à diverses techniques d'évasion (il se faisait notamment passer pour la bibliothèque Crypto++). Snatch (illustré ci-dessous) en est un autre. Il avait la particularité de redémarrer les machines infectées en mode sans échec pour contourner les logiciels de sécurité.

On monte toutefois d'un cran avec RansomEXX, au regard des victimes qu'il a faites et du niveau de sophistication des attaques. Sa cible n'est évidemment pas tant les postes de travail (dévolus à la version Windows) que les serveurs, d'autant plus critiques.

Illustration principale © isaak55 – shutterstock.com