Maze : vers un « cartel » du ransomware ?

Vers un « cartel du *ransomware* » ?

Les pirates à l'origine de Maze semblent prendre cette direction.

Une publication récente sur leur « site vitrine » en témoigne. Elle comprend des données issues d'une opération menée avec un autre groupe cybercriminel.

Ce groupe est connu sous le nom de LockBit.
L'équipe Maze confirme la collaboration, axé sur le « partage de son expérience et de sa plate-forme ». Elle ajoute mener des discussions avec d'autres collectifs, dont l'un devrait rejoindre la boucle « dans quelques jours ».

LockBit fait partie des *ransomwares* vendus « en tant que service ». On en loue des composantes par l'intermédiaire d'un programme d'affiliation lancé début 2020.

Sophos en avait publié, il y a quelques semaines, une analyse détaillée.

Discret, mais pas trop

L'entreprise britannique observe notamment que LockBit est conçu pour ne pas attaquer les systèmes liés à la Russie et à d'anciennes républiques soviétiques (réunies au sein de la Communauté des États indépendants).
Le filtrage s'effectue sur la base de la langue principale du système. Avec des exceptions pour l'azéri, l'arménien, le biélorusse, le géorgien, le kazakh, le russe, le tadjik, l'ouzbek et l'ukrainien.

Le *ransomware* présente plusieurs optimisations destinées à améliorer ses performances. Entre, la technologie d'extension de jeu d'instructions Intel (SSE) et l'API IOCP, qui permet d'effectuer plusieurs opérations d'entrée-sortie asynchrones.

Il présente aussi des éléments curieux. Par exemple, le blocage de l'exécution dès lors que celle-ci se fait avec des paramètres ajoutés en ligne de commande. D'après Sophos, c'est plutôt l'inverse qui devrait se produire, en reflet d'une technique classique permettant de détecter l'exécution en *sandbox*.

S'il ne dispose pas des privilèges d'administrateur, LockBit les obtient en contournant l'UAC (contrôle de compte d'utilisateur Windows). À ces fins, il se fait passer pour un processus de confiance (explorer.exe).
Il liste ensuite les lecteurs réseau chiffrables. Y compris ceux qui nécessitent une identification. Pour cela, il tente une connexion avec le login et le mot de passe de la session en cours.

Au-delà des processus et des services qu'il tente de fermer avant de s'exécuter, le *ransomware* dispose d'une liste d'éléments à ne pas chiffrer. Parmi eux, les fichiers qui pourraient empêcher le système de démarrer… et d'afficher la demande de rançon.

Le message apparaît en papier peint. Mais Sophos a repéré un cas dans lequel LockBit a sévi plus

en amont. Il a chiffré une partie du secteur d'amorçage du disque, empêchant le démarrage aussi longtemps qu'un mot de passe n'est pas saisi.

De nombreuses mesures ont été mises en place pour ne pas laisser de traces. Mais LockBit ne se cache pas lorsqu'il tente d'empêcher l'extinction du système cible : les messages d'avertissement sont…à son nom.

Photo d'illustration © Yu. Samoilov via *Visualhunt / CC BY*