ACTUALITES

LockBit : à quoi s'attendre avec la version 4.0 de son ransomware ?

En décembre 2024, l'opérateur de la franchise de rançongiciel LockBit a lancé la quatrième version de son maliciel de chiffrement. Depuis, les premiers échantillons ont été collectés et analysés.

par **Valéry Rieß-Marchive,** Rédacteur en chef

Publié le: **03 févr. 2025**

Après plusieurs mois de pause plus ou moins forcée et plus ou moins complète, l'enseigne LockBit a repris ses activités. La revendication d'une cyberattaque contre Topackt IT Solutions, entreprise de services numériques (ESN) allemande, le confirme : elle est survenue le 2 février, mais l'attaque elle-même a été rapportée par la presse locale et remonte à la mi-janvier.

Affecté par l'opération Cronos, mais manifestement déterminé à continuer son œuvre, l'opérateur de la franchise mafieuse a lancé, en décembre dernier,

la version 4.0 de son rançongiciel, conformément à son annonce deux mois plus tôt.

Les premiers échantillons ont pu en être collectés et étudiés. Les analystes de Microsoft font ainsi état d'améliorations des capacités de prévention de la détection, de la rétro-ingénierie, et encore de chiffrement.

En particulier, le ransomware est doté d'un mode « silencieux » qui, selon Microsoft, « permet aux acteurs malveillants de lancer des attaques dans le cadre desquelles les extensions de fichiers et leurs dates de modification sont préservées après le chiffrement ». Dans ce mode-là, aucune note de rançon n'est par ailleurs déposée sur les machines affectées, de quoi générer de nouveaux « défis de détection et d'investigation ».

Lorsque ce mode n'est pas activé, la note de rançon prend la forme d'un fichier baptisé « Restore-My-Files.txt » qui, comme fréquemment, ne contient pas de demande financière explicite, mais des liens vers les sites vitrines de LockBit ainsi que des instructions sur la manière d'engager la discussion. Il est déposé dans chaque dossier contenant des fichiers explicitement chiffrés. Ceux-ci sont là aisément identifiables par leurs extensions à douze caractères alphanumériques.

L'échantillon que nous avons observé précisait la version du ransomware : LockBitGreen4.0-rc-577. Cette référence renvoie au début 2023, lorsque les opérateurs de la franchise ont annoncé ajouter à leur arsenal LockBit Green, basé sur le code Conti. Le code source de différentes versions du ransomware utilisé par cette enseigne et ses membres a été diffusé par l'un d'eux, en mars 2022.

Avec « Green », LockBit proposait une option additionnelle à ses affidés venant compléter LockBit Red (à savoir, LockBit 2.0), et LockBit Black (issu du code de BlackMatter).

Fin décembre dernier, le ministère américain de la Justice a rendu public l'acte d'inculpation de Rostislav Panev, qui serait l'un des développeurs des outils de LockBit.

Selon ce document, la franchise cherche à s'attaquer aux systèmes Proxmox et Nutanix, en plus des environnements virtualisés avec VMware ESXi.

Pour approfondir sur Menaces, Ransomwares, DDoS

Ransomware : arrestation d'un développeur de LockBit en Israël

Par: Valéry Rieß-Marchive

Ransomware : 2024, l'année Cronos

Par: Valéry Rieß-Marchive

Opération Cronos, exit-scam Alphv : lequel a le plus affecté l'écosystème ransomware ?

Par: Valéry Rieß-Marchive

Coup dur pour LockBit 3.0 : le FBI trouve 7 000 clés de déchiffrement

Par: Alex Scroxton