Ransomware : LockBit 3.0 commence à être utilisé dans des cyberattaques

lemagit.fr/actualites/252516821/Ransomware-LockBit-30-commence-a-etre-utilise-dans-des-cyberattaques

Valéry Rieß-Marchive

Actualites

Cette nouvelle mouture avait été évoquée mi-mars. Elle doit notamment corriger un bogue de chiffrement des bases de données MSSQL. Son utilisation dans le cadre de cyberattaques a commencé.

- Partager avec votre réseau:
-
-
-
-
-
-
-
-

par

Valéry Rieß-Marchive, Rédacteur en chef

Publié le: 06 mai 2022

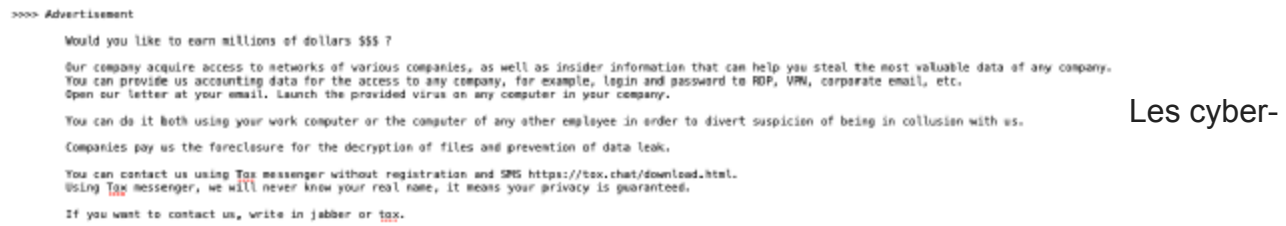
C'est l'une de ces notes déposées à l'issue du chiffrement d'un système attaqué qui nous a mis la puce à l'oreille. Sa première ligne est sans ambiguïté : « LockBit 3.0 le ransomware le plus rapide au monde depuis 2019 ». Cette mention est une première : avec les plus récents échantillons de LockBit que nous avons pu identifier à ce jour, la note commence par le plus prosaïque « LockBit 2.0 Ransomware ».

La note dont nous avons obtenu une copie présente d'autres spécificités. Là, il n'y a pas une adresse d'onion de site vitrine comme d'habitude, mais la liste de toutes les adresses miroirs. Un site Web accessible sans passer par Tor est également précisé, mais celui-ci ne semble plus utilisable depuis la fin mars.

Autre nouveauté, les cyberdélinquants invitent directement à travailler pour leur compte. « Voulez-vous gagner des millions de dollars ? », commence ainsi un paragraphe de la note de demande de rançon : « notre entreprise [sic] acquiert des accès aux réseaux de diverses entreprises, ainsi que des informations de sachants internes qui peuvent nous aider à voler les données les plus précieuses de n'importe quelle entreprise ». Que cherchent-ils ? Par exemple, les identifiants permettant de se connecter à des services de déport d'affichage (RDP), « VPN, courrier électronique d'entreprise, etc. ».

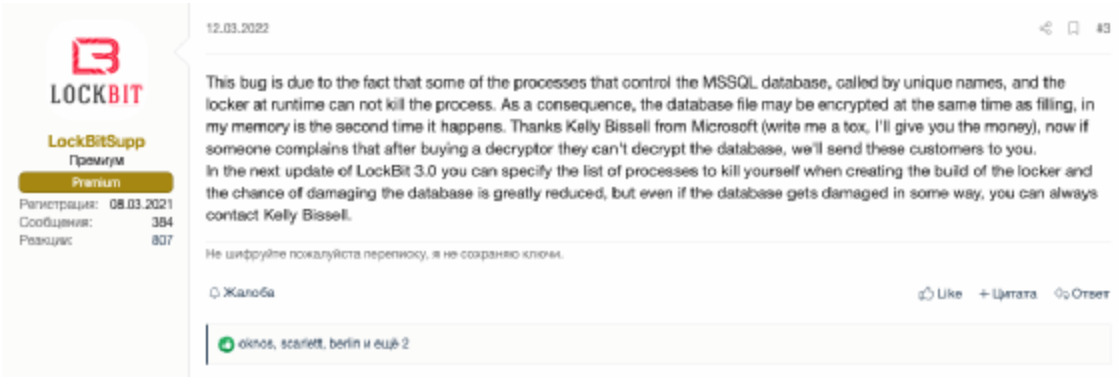
Note de rançon de LockBit 3.0.

La version 3.0 de LockBit a initialement été évoquée mi-mars, sur un forum fréquenté par les cyberdélinquants et, notamment, les opérateurs de la franchise de rançongiciel LockBit. La discussion portait sur des bogues détaillés par Microsoft dans le maliciel de chiffrement, et susceptibles d'endommager les fichiers MSSQL.



Les cyber-délinquants appellent à des complicités internes.

Les opérateurs de la franchise ont rejeté la faute sur « certains des processus contrôlant la base de données MSSQL » que leur logiciel de chiffrement ne parvient pas à interrompre. D'où la corruption des fichiers correspondants. En réponse à cela, LockBit 3.0 doit permettre à l'assaillant le déployant « de préciser la liste de processus » à arrêter, manuellement, lors de la création du ransomware.



Première évocation de LockBit 3.0.

Quelques jours plus tard, les opérateurs de la franchise LockBit indiquaient à *vx-underground* que LockBit 3.0 pourrait être prêt d'ici « une à deux semaines ». Fin avril, ils expliquaient chercher des « béta testeurs ». À moins qu'ils n'utilisent des victimes bien réelles pour des tests, ceux-ci semblent aujourd'hui terminés.

Actualités

Télécharger Information Sécurité

Dans ce numéro:

- Information sécurité no 21 – Cybersécurité : remettons l'utilisateur à sa place
- Former ses employés à la cybersécurité : comment construire un projet robuste
- E-mails malveillants : comment sensibiliser ses utilisateurs

Télécharger cette édition