

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. ».

LockBit 3.0 the world's fastest ransomware since 2019

>>>> Your data are stolen and encrypted

The data will be published on TOR website if you do not pay the ransom

Links for Tor Browser:



Links for the normal browser:



>>>> What guarantees that we will not deceive you?

We are not a politically motivated group and we do not need anything other than your money.

If you pay, we will provide you the programs for decryption and we will delete your data.
Life is too short to be sad. Be not sad, money, it is only paper.

If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.
Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.

You can obtain information about us on twitter <https://twitter.com/hashtag/lockbit?f=live>

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 détailés par Microsoft dans le maliciel de chiffrement, et susceptibles d'endommager les fichiers MSSQL.

>>>> Advertisement

Would you like to earn millions of dollars \$\$\$?

Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.

You can do it Both using your work computer or the computer of any other employee in order to divert suspicion of being in collusion with us.

Companies pay us the fareclosure for the decryption of files and prevention of data leak.

You can contact us using Tox messenger without registration and SMS <https://tox.chat/download.html>.
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.

If you want to contact us, write in jabber or [tox](#).

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.

12.03.2022

LOCKBIT

LockBitSupp
Преміум

Регистрація: 08.03.2021
Собщання: 384
Реакція: 807

This bug is due to the fact that some of the processes that control the MYSQL database, called by unique names, and the locker at runtime can not kill the process. As a consequence, the database file may be encrypted at the same time as filling, in my memory is the second time it happens. Thanks Kelly Bissell from Microsoft (write me a tox, I'll give you the money), now if someone complains that after buying a decryptor they can't decrypt the database, we'll send these customers to you. In the next update of LockBit 3.0 you can specify the list of processes to kill yourself when creating the build of the locker and the chance of damaging the database is greatly reduced, but even if the database gets damaged in some way, you can always contact Kelly Bissell.

Не шифруйте пожалуйста переписку, я не сохраняю ключи.

Жалоба Like + Цитата Orset

oikos, scarlett, berin и ещё 2

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 « bêta testeurs ». À moins qu'ils n'utilisent des victimes bien réelles pour des tests, ceux-ci semblent aujourd'hui terminés.

Actualités

Télécharger Information Sécurité

INFORMATION SÉCURITÉ

FÉVRIER 2022
N° 21

ÉDITO:
REMETTONS L'UTILISATEUR
À SA PLACE

FORMER SES EMPLOYÉS
À LA CYBERSÉCURITÉ :
COMMENT CONSTRUIRE
UN PROJET ROBUSTE

DALILA BEN ATTAL,
TERRANOVA SECURITY :
« LA FORMATION EST UN
PROCESSUS CONTINU »

E-MAILS MALVEILLANTS :
COMMENT SENSIBILISER
SES UTILISATEURS

PHISHING : MANTRA JOUE
LA CARTE DE LA MISE
EN CONDITIONS RÉELLES

CYBERZEN MISE SUR
LA RÉALITÉ VIRTUELLE
POUR SENSIBILISER
À LA CYBERSÉCURITÉ

CYBERSÉCURITÉ :
LA VISION « OFFENSIVE »
DE MANOMANO

SEPT CONSEILS POUR
CONSTRUIRE UNE SOLIDE
CULTURE DE LA SÉCURITÉ

LES CLÉS POUR FORMER
SES COLLABORATEURS À LA CYBERSÉCURITÉ

Techtarget | LeMAGIT

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](#)