Ragnarok ransomware releases master decryptor after shutdown

bleepingcomputer.com/news/security/ragnarok-ransomware-releases-master-decryptor-after-shutdown/

Ionut Ilascu

By
Ionut Ilascu

- August 26, 2021
- 06:36 PM
- 0

Ragnarok ransomware gang appears to have called it quits and released the master key that can decrypt files locked with their malware.

The threat actor did not leave a note explaining the move; all of a sudden, they replaced all the victims on their leak site with a short instruction on how to decrypt files.

Rushed exit

The leak site has been stripped of visual elements. All that remains there is the brief text linking to an archive containing the master key and the accompanying binaries for using it.

Looking at the leak site, it seems like the gang did not plan on shutting down today and just wiped everything and shut down their operation.

HOME

DECRYPT

JUL 11, 2021

paste your device id into id.txt run decode_deviceID.exe run decrypt.exe Decrypt

READ MORE

HOME

DECRYPT

paste your device id into id.txt

run decode_deviceID.exe

run decrypt.exe

Decrypt

source: BleepingComputer

Up until earlier today, the Ragnarok ransomware leak site showed 12 victims, added between July 7 and August 16, threat intelligence provider HackNotice told BleepingComputer.

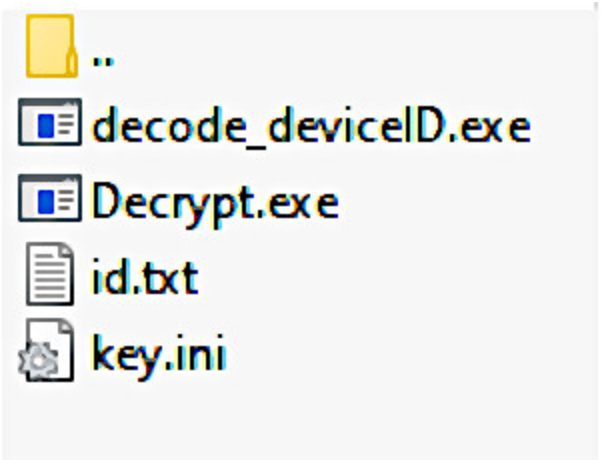
By listing victims on their website, Ragnarok sought to force them into paying the ransom, under the threat of leaking unencrypted files stolen during the intrusion.

The listed companies are from France, Estonia, Sri Lanka, Turkey, Thailand, U.S., Malaysia, Hong Kong, Spain, and Italy and activate in various sectors ranging from manufacturing to legal services.

Ransomware expert Michael Gillespie told BleepingComputer that the Ragnarok decryptor released today contains the master decryption key.

“[The decryptor] was able to decrypt the blob from a random .thor file,” Gillespie told BleepingComputer initially.

The researcher later confirmed that he could decrypt a random file, which makes the utility a master decryptor that can be used to unlock files with various Ragnarok ransomware extensions.



source: BleepingComputer

A universal decryptor for Ragnarok ransomware is currently in the works. It will soon become available from Emsisoft, a company famed for assisting ransomware victims with data decryption.

The Ragnarok ransomware group has been around since at least January 2020 and claimed dozens of victims after making headlines for exploiting the Citrix ADC vulnerability last year.

Ragnarok is not the only ransomware gang to release a decryption key this year

- Ziggy ransomware operation shut down in February, and its operator shared a file with 922 keys
- In May, Conti ransomware gave a free decryptor to HSE Ireland
- Avaddon ransomware shut down in June and released the decryption keys
- SynAck ransomware gang rebranded as El_Cometa and released the master decryption keys as part of this transition

Researchers also provided decryptors [1, 2, 3], and sometimes the provenance of these tools remained uncertain, as it happened with the Kaseya attack.

Related Articles:

Free decryptor released for Yanluowang ransomware victims

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

- Decryption Key
- Decryptor
- Ragnarok
- Ransomware

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

You may also like: