Decryptor for Rhysida ransomware is available!

helpnetsecurity.com/2024/02/12/rhysida-ransomware-decryptor/

February 12, 2024

Zeljka Zorz, Editor-in-Chief, Help Net Security
February 12, 2024

Files encrypted by Rhysida ransomware can be successfully decrypted, due to a implementation vulnerability discovered by Korean researchers and leveraged to create a decryptor.

Rhysida and its ransomware

Rhysida is a relatively new ransomware-as-a-service gang that engages in double extortion.

First observed in May 2023, it made its name by attacking the British Library, the Chilean Army, healthcare delivery organizations, and Holding Slovenske Elektrarne (HSE).

According to Check Point Research, the Rhysida ransomware group may simply be the Vice Society hacking group armed with new ransomware.

“The [Rhysida] ransomware encrypts data using a 4096-bit RSA encryption key with a ChaCha20 algorithm. The algorithm features a 256-bit key, a 32-bit counter, and a 96-bit nonce along with a four-by-four matrix of 32-bit words in plain text,” the Cybersecurity and Infrastructure Security Agency noted in a cybersecurity advisory published in November 2023.

Making the Rhysida ransomware decryptor

“Decrypting data encrypted using a symmetric-key cryptographic algorithm requires the encryption key used in the process. Since encryption keys can be generated in various methods, it is important to identify the factors used by ransomware in the key generation process during data encryption,” researchers Giyoon Kim, Soojin Kang, Seungjun Baek and Jongsung Kim from Kookmin University in Seul and Kimoon Kim from the Korea Internet & Security Agency (KISA) explained.

As other researchers before them, they established that Rhysida ransomware uses the open-source cryptographic library LibTomCrypt for its encryption routine, and its pseudorandom number generator (PRNG) functionalities for both key and initialisation vector (IV) generation.

After a thorough analysis of the ransomware, they found that:

- The random number generated by the PRNG is based on the execution time of the Rhysida ransomware
- They could determine the (randomized) order of files for encryption
- Rhysida's encryption thread generates 80 bytes of random numbers when encrypting a single file, the first 48 bytes of which are used as the encryption key and the IV

With that information in hand, they were able to create a recovery tool.

"To the best of our knowledge, this is the first successful decryption of Rhysida ransomware. We aspire for our work to contribute to mitigating the damage inflicted by the Rhysida ransomware," the researchers noted.

More about

- Check Point
- CISA
- decrypter
- enterprise
- KISA
- ransomware