Kaseya's universal REvil decryption key leaked on a hacking forum

bleepingcomputer.com/news/security/kaseyas-universal-revil-decryption-key-leaked-on-a-hacking-forum/

Lawrence Abrams

By
Lawrence Abrams

- August 11, 2021
- 02:01 AM
- 8

The universal decryption key for REvil's attack on Kaseya's customers has been leaked on hacking forums allowing researchers their first glimpse of the mysterious key.

On July 2nd, the REvil ransomware gang launched a massive attack on managed service providers worldwide by exploiting a zero-day vulnerability in the Kaseya VSA remote management application.

This attack encrypted approximately sixty managed service providers and an estimated 1,500 businesses, making it possibly the largest ransomware attack in history.

After the attack, the threat actors demanded a $70 million ransom to receive a universal decryptor that could be used to decrypt all victims of the Kaseya ransomware attack.

However, the REvil ransomware gang mysteriously disappeared, and soon after, the gang's Tor payment sites and infrastructure were shut down.

The gang's disappearance prevented companies who may have needed to purchase a decryptor now unable to do so.

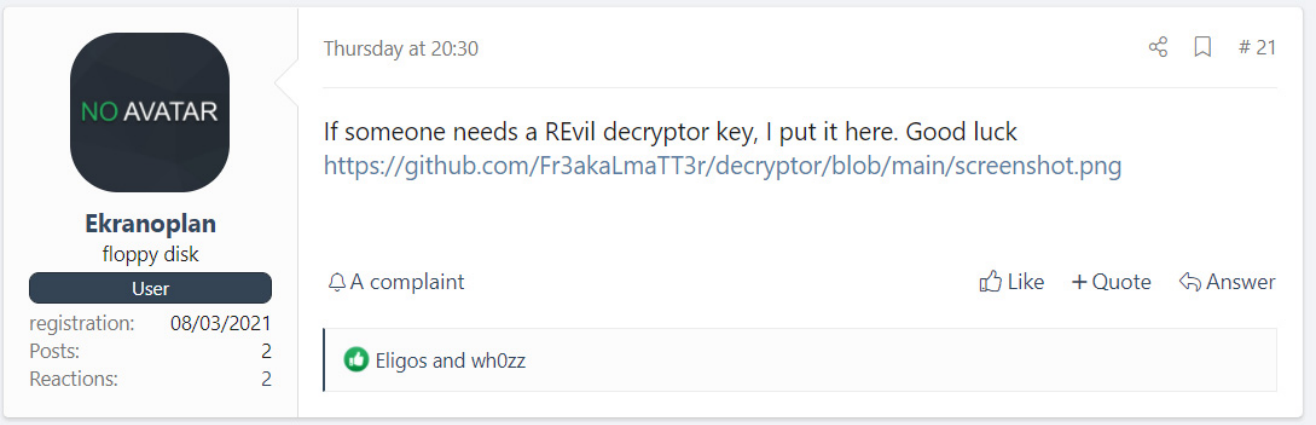
On July 22nd, Kaseya obtained a universal decryption key for the ransomware attack from a mysterious "trusted third party" and began distributing it to affected customers.

Before sharing the decryptor with customers, CNN reported that Kaseya required them to sign a non-disclosure agreement, which may explain why the decryption key hasn't shown up until now.

It is generally believed that Russian intelligence received the decryptor from the ransomware gang and shared it with US law enforcement as a gesture of goodwill.

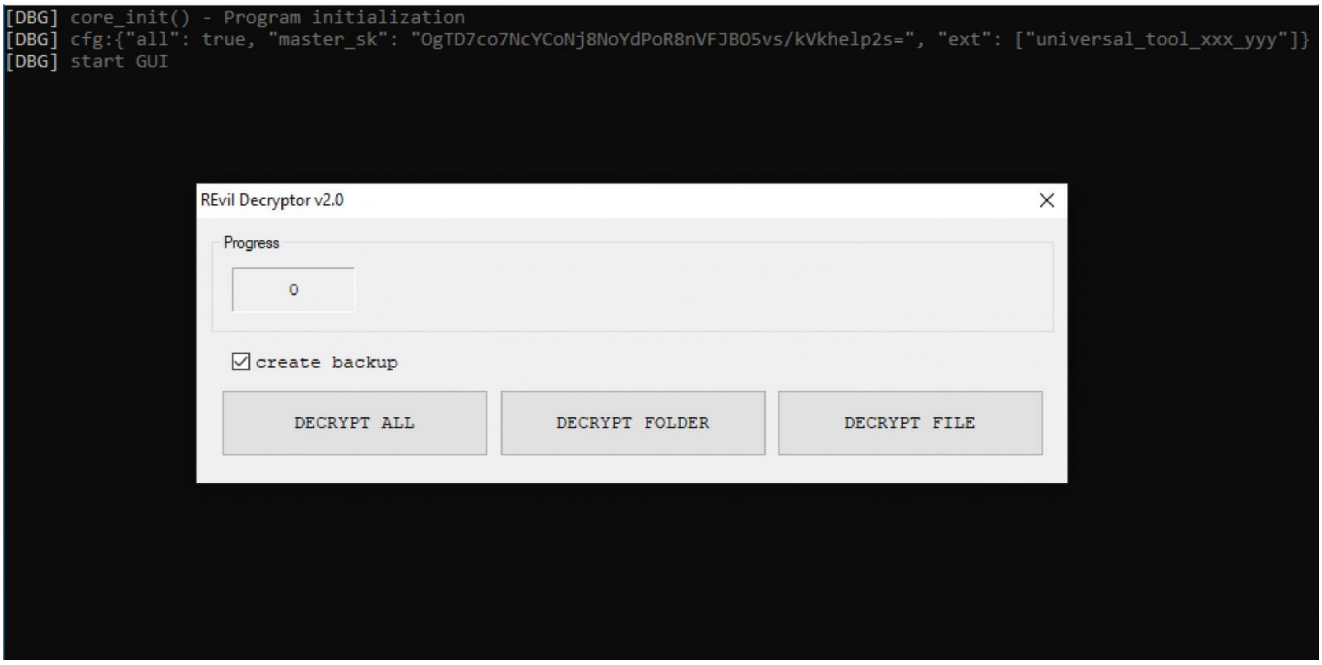
Decryption key leaked on a hacking forum

Yesterday, security researcher Pancak3 told BleepingComputer that someone posted a screenshot of what they claimed was a universal REvil decryptor on a hacking forum.



Forum post about Kaseya decryptor on a hacking forum

This post linked to a screenshot on GitHub that showed an REvil decryptor running while displaying a base64 hashed 'master_sk' key. This key is 'OgTD7co7NcYCoNj8NoYdPoR8nVFJBO5vs/kVkhelp2s=', as shown below.



Screenshot of alleged Kaseya REvil decryptor

When REvil ransomware victims pay a ransom, they receive either a decryptor that works for a single encrypted file extension or a universal decryptor that works for all encrypted file extensions used in a particular campaign or attack.

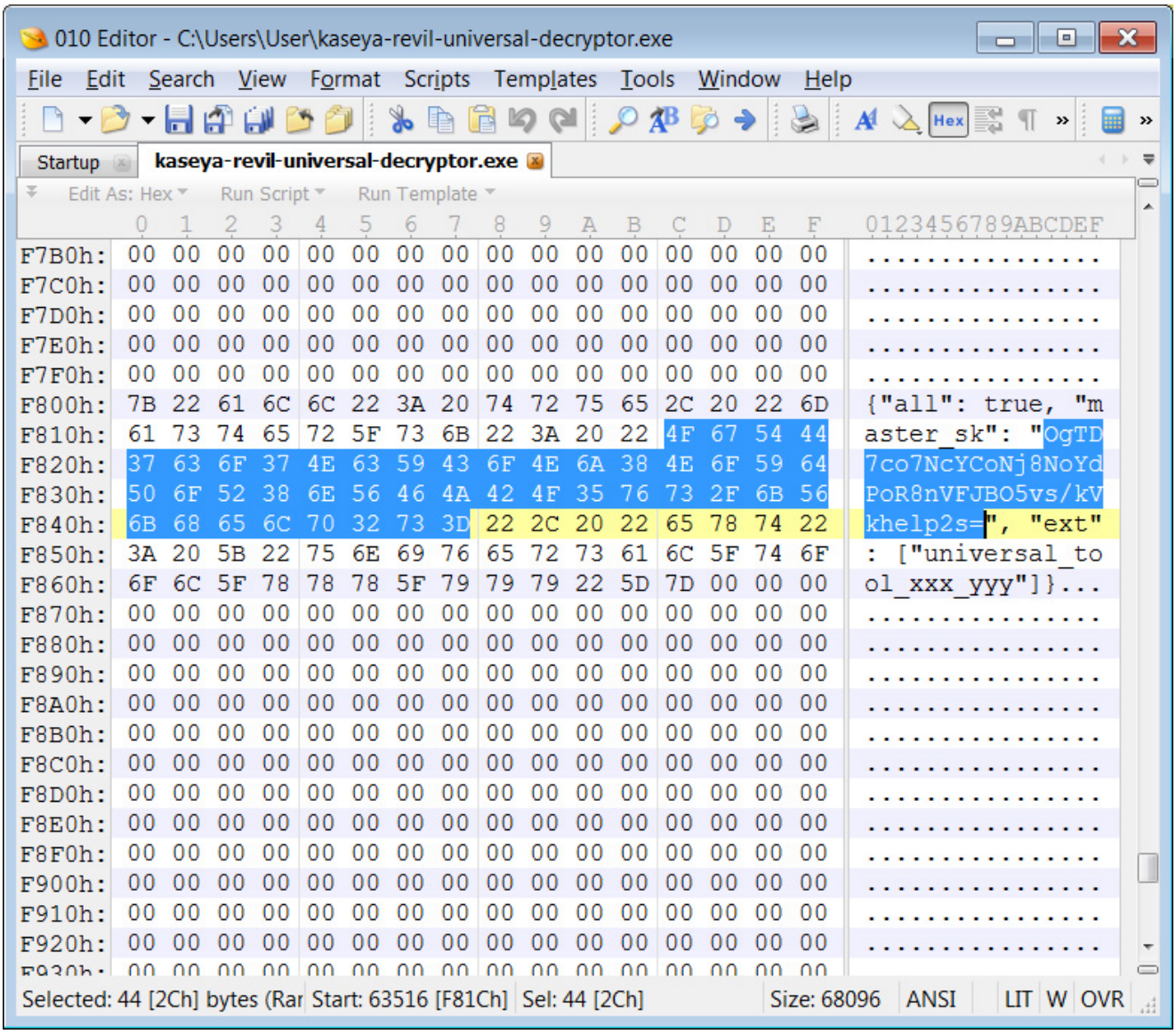
The screenshot above is for a universal REvil decryptor that can decrypt all extensions associated with the attack.

To be clear, while it was originally thought that the decryption key in this screenshot might be the master 'operator' key for **all** REvil campaigns, BleepingComputer has confirmed that it is only the universal decryptor key for victims of the Kaseya attack.

This was also confirmed by Emsisoft CTO and ransomware expert Fabian Wosar.

> The REvil hardcoded operator public key is 79CD20FCE73EE1B81A433812C156281A04C92255E0D708BB9F0B1F1CB9130635. The leaked key generates public key F7F020C8BBD612F8966EFB9AC91DA4D10D78D1EF4B649E61C2B9ADA3FCC2C853. Therefore, the leaked key is not the operator private key.
>
> — Fabian Wosar (@fwosar) August 11, 2021

BleepingComputer tested the leaked key by patching an REvil universal decryptor with the decryption key leaked in the screenshot.



Patching an REvil universal decryptor

After patching the decryptor, we encrypted a virtual machine with REvil ransomware samples used in the Kaseya attack.

As shown in our video below, we then used our patched REvil Universal Decryptor to decrypt the encrypted files successfully.

Security firm Flashpoint also confirmed that they could decrypt files encrypted during the Kaseya ransomware attack using this decryption key.

We also tried the decryptor on other REvil samples we have accumulated over the past two years. The decryptor did not work, indicating it is not the master decryption key for all REvil victims.

It is not clear why the Kaseya decryptor was posted on a hacking forum, which is an unlikely place for a victim to post.

However, BleepingComputer was told by numerous sources in the cybersecurity intelligence industry that they believe that the poster is affiliated with the REvil ransomware gang rather than a victim.

Regardless of the reasons for it being posted, for those following the Kaseya ransomware attack, this is our first access to the universal decryptor key that Kaseya mysteriously received.

Related Articles:

The Week in Ransomware - May 6th 2022 - An evolving landscape

Conti, REvil, LockBit ransomware bugs exploited to block encryption

REvil ransomware returns: New malware sample confirms gang is back

Austin Peay State University resumes after ransomware cyber attack

REvil's TOR sites come alive to redirect to new ransomware operation

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.