

## Free REvil ransomware master decrypter released for past victims

By Lawrence Abrams

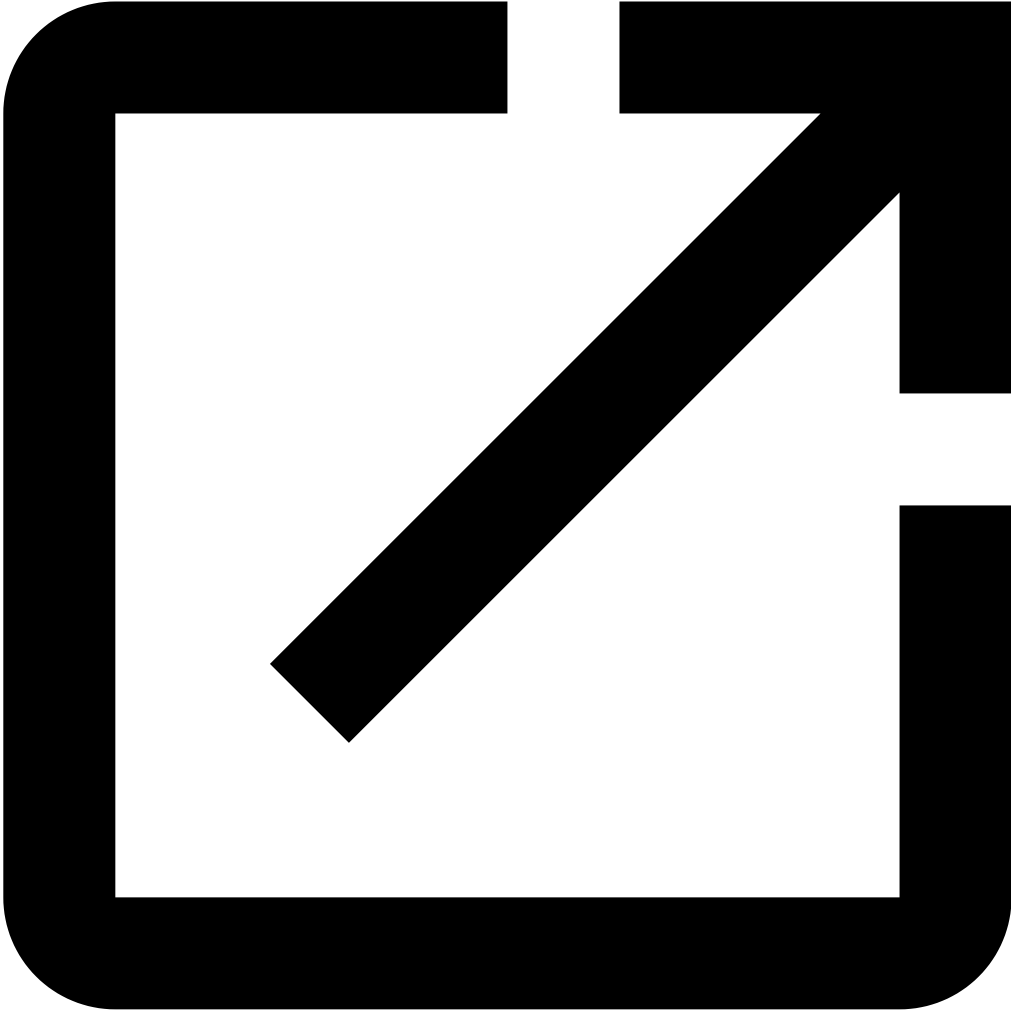
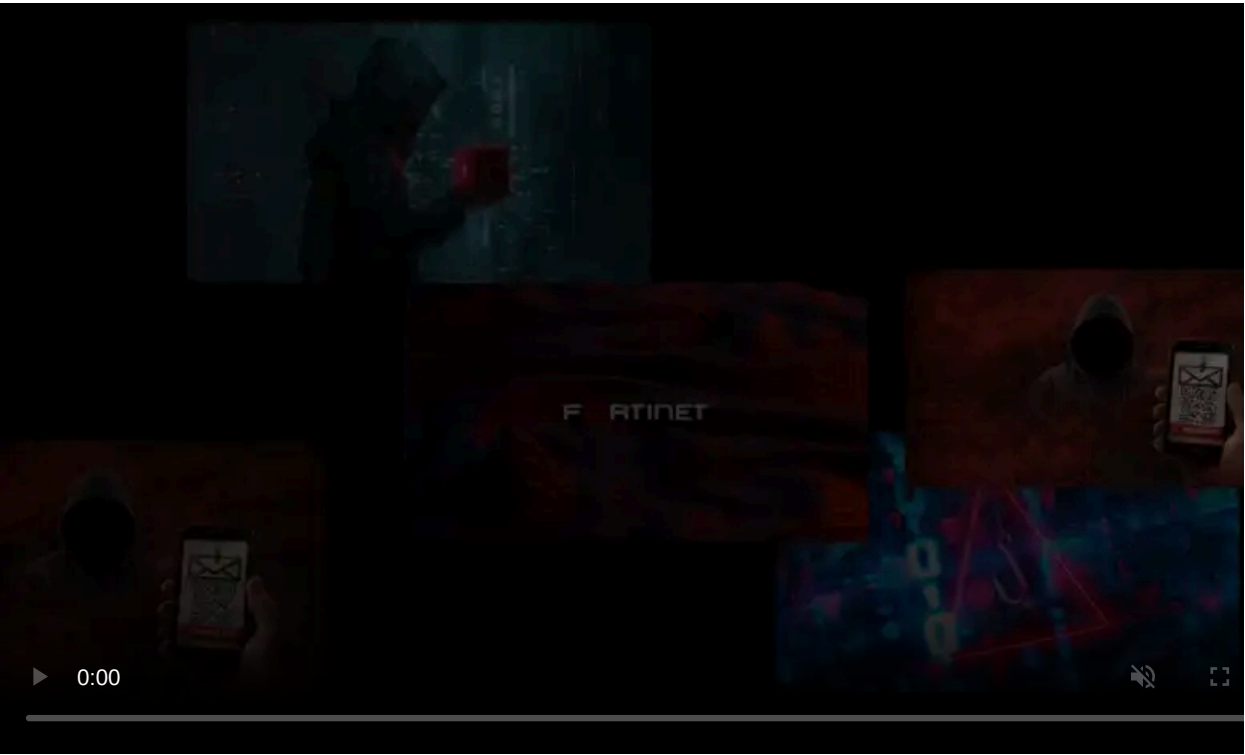
Published: 2021-09-16 · Archived: 2026-04-05 20:39:31 UTC



A free master decrypter for the REvil ransomware operation has been released, allowing all victims encrypted before the gang disappeared to recover their files for free.

The REvil master decrypter was created by cybersecurity firm Bitdefender in collaboration with a trusted law enforcement partner.

While Bitdefender could not share details about how they obtained the master decryption key or the law enforcement agency involved, they told BleepingComputer that it works for all REvil victims encrypted before July 13th.



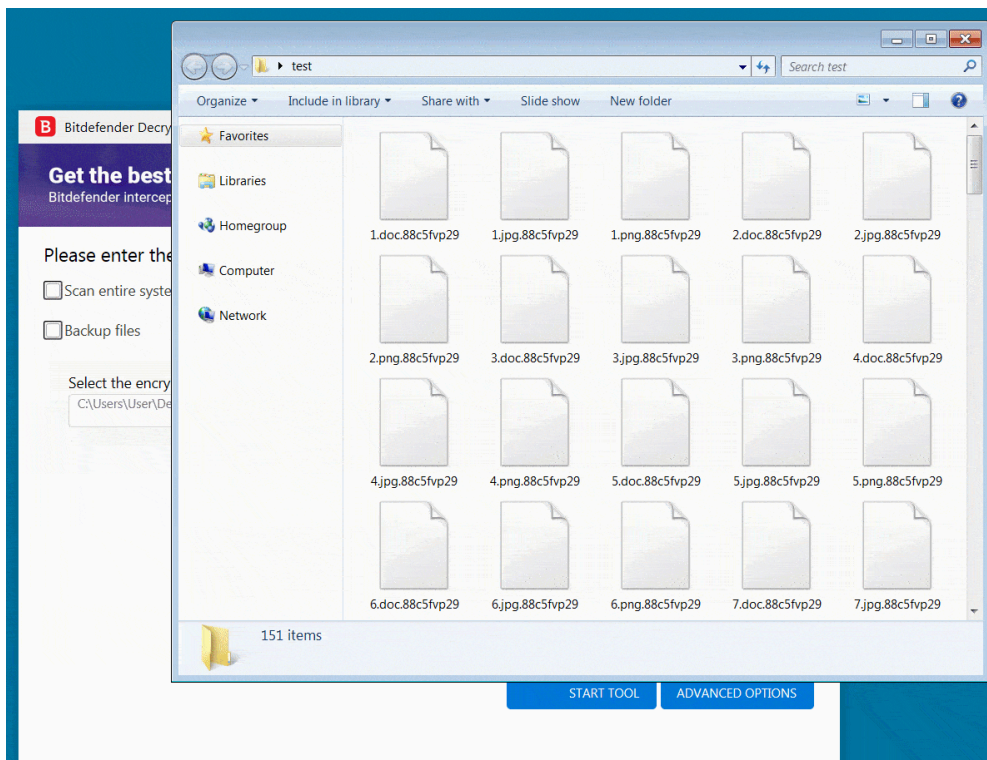
Visit Advertiser website [GO TO PAGE](#)

"As per our blog post, we received the keys from a trusted law enforcement partner, and unfortunately, this is the only information we are at liberty to disclose right now," Bitdefender's Bogdan Botezatu, Director of Threat Research and Reporting, told BleepingComputer.

"Once the investigation progresses and will come to an end, further details will be offered upon approval."

REvil ransomware victims can [download the master decryptor](#) from Bitdefender ([instructions](#)) and decrypt entire computers at once or specify specific folders to decrypt.

To test the decryptor, BleepingComputer encrypted a virtual machine with an REvil sample used in an attack earlier this year. After encrypting our files, we could use Bitdefender's decryptor to easily recover our files, as shown below.



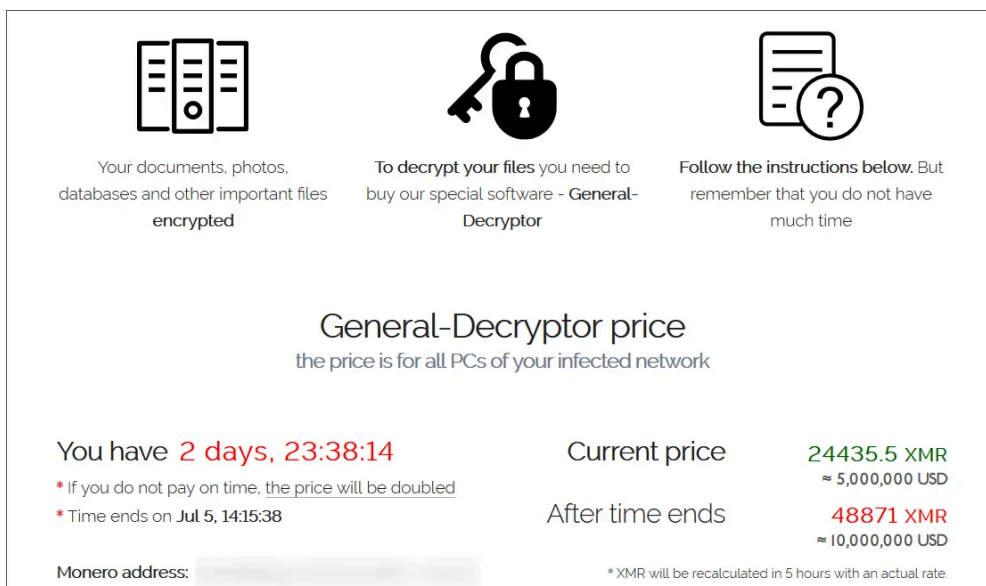
**Decrypting REvil encrypted files with decryptor**

## Law enforcement likely compromised REvil servers

The REvil ransomware operation, aka Sodinokibi, is believed to be a rebrand or successor to the now "retired" [ransomware group known as GandCrab](#).

Since launching in 2019, REvil has conducted numerous attacks against well-known companies, including [JBS](#), [Coop](#), [Travelex](#), and [Grupo Fleury](#).

Finally, in a [massive July 2nd attack](#) using a Kaseya zero-day vulnerability, the ransomware gang encrypted sixty managed service providers and over 1,500 businesses worldwide.



The screenshot shows a ransomware payment interface. At the top, there are three icons: a server rack, a key and padlock, and a document with a question mark. Below each icon is a line of text: 'Your documents, photos, databases and other important files encrypted', 'To decrypt your files you need to buy our special software - General-Decryptor', and 'Follow the instructions below. But remember that you do not have much time'. In the center, it says 'General-Decryptor price' and 'the price is for all PCs of your infected network'. On the left, a timer shows 'You have 2 days, 23:38:14' with two asterisks below it: '\* If you do not pay on time, the price will be doubled' and '\* Time ends on Jul 5, 14:15:38'. On the right, it shows 'Current price 24435.5 XMR ≈ 5,000,000 USD' and 'After time ends 48871 XMR ≈ 10,000,000 USD'. At the bottom left, it says 'Monero address:' followed by a blurred grey box. At the bottom right, it says '\*XMR will be recalculated in 5 hours with an actual rate.'

### REvil ransom demand for MSP encrypted ion July 2nd

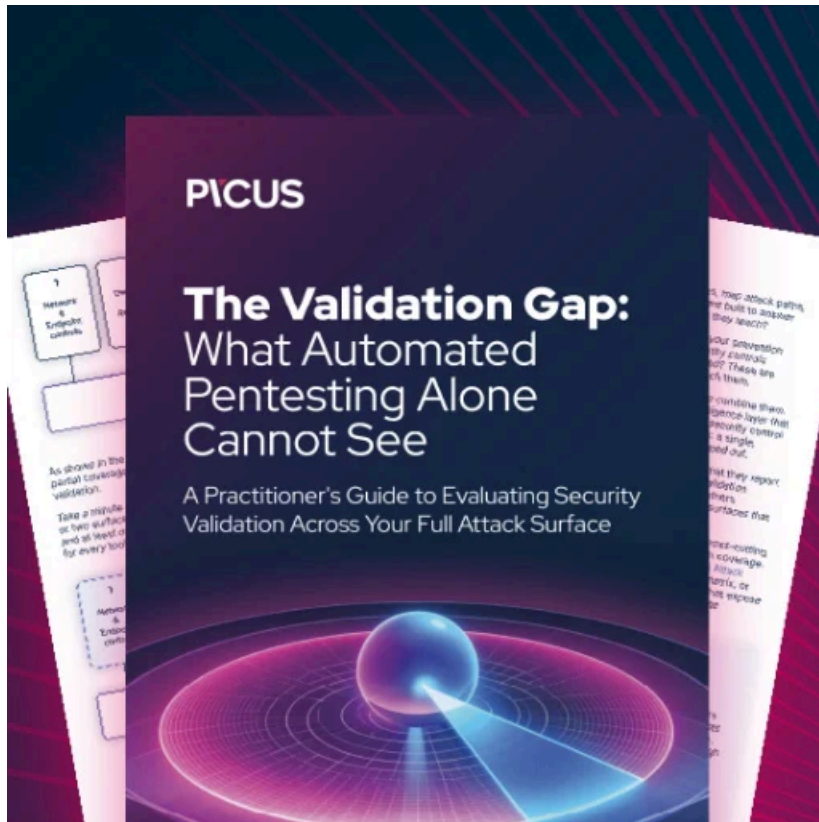
After facing intense scrutiny by international law enforcement and increased political tensions between Russia and the USA, [REvil suddenly shut down](#) its operation on July 13th and disappeared.

While REvil was shut down, [Kaseya mysteriously received a master decryptor](#) for their attack, allowing MSPs and their customers to recover files for free.

As Bitdefender states that victims who REvil encrypted before July 13th can use this decryptor, it is safe to assume that the ransomware operation's disappearance was tied to this law enforcement investigation.

It is also likely that Kaseya obtaining the REvil master decryption key for the attack on their customers is also tied to the same investigation.

While [REvil has returned to attacking victims](#) earlier this month, the release of this master decryptor comes as a massive boon for existing victims who chose not to pay or simply couldn't after the ransomware gang disappeared.



### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/free-revil-ransomware-master-decrypter-released-for-past-victims/>