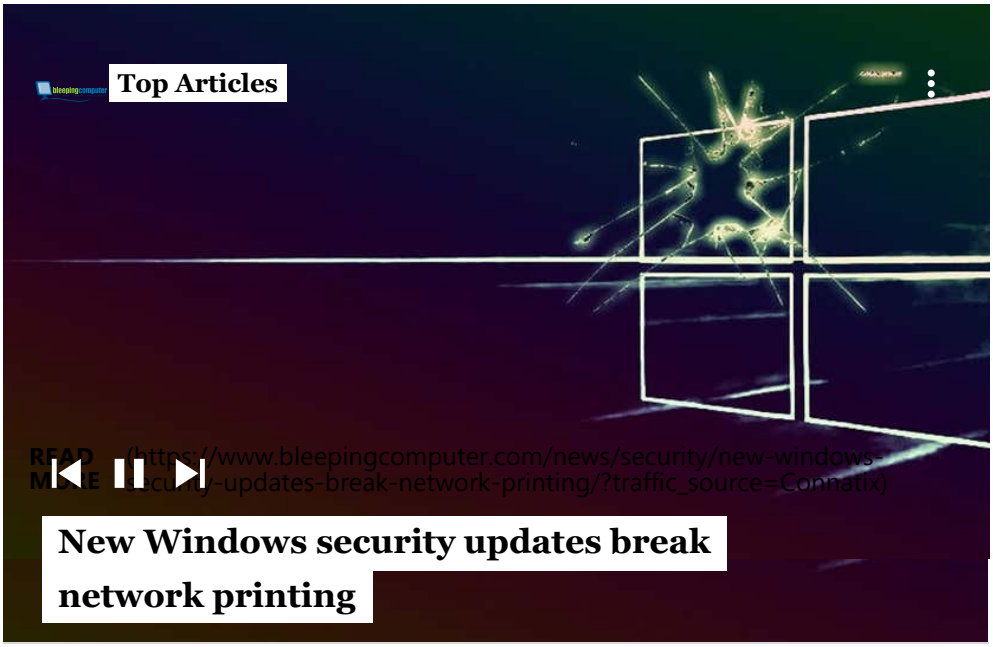
Free REvil ransomware master decrypter released for past victims

By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)** September 16, 2021 09:00 AM **5**

A free master decryptor 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 decryptor 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.

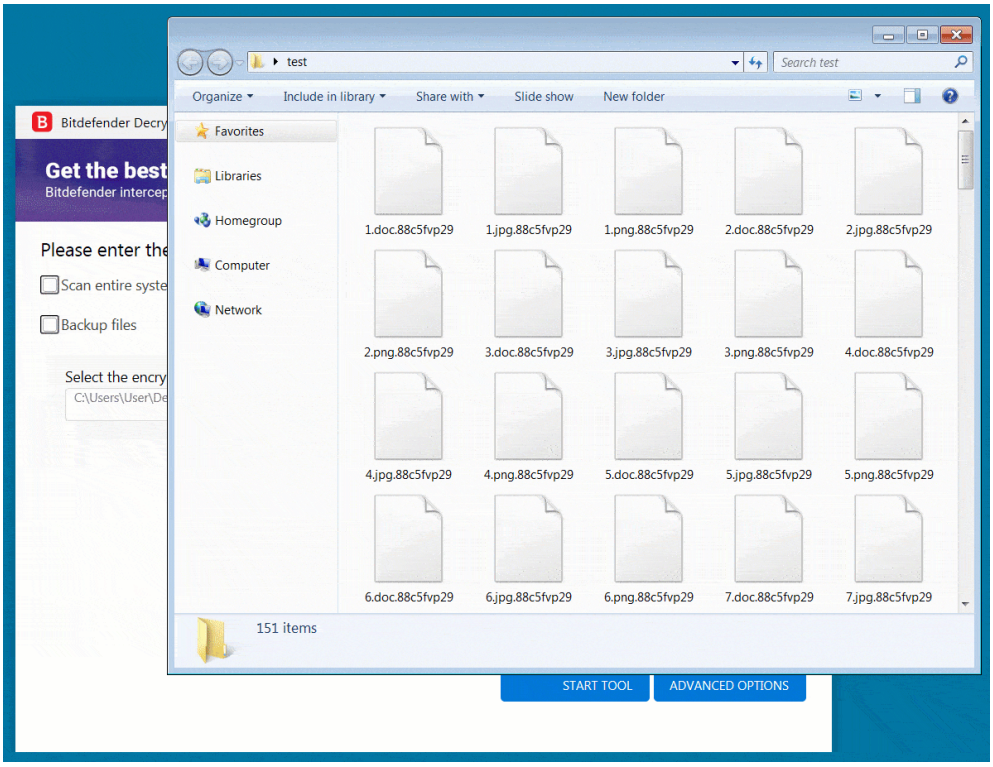


"As per our blog post, we received the keys from a trusted law enforcement partner, and unfortunately, this is the only information we are at liberty to disclose right now," Bitdefender's Bogdan Botezatu, Director of Threat Research and Reporting, told BleepingComputer.

"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 (http://download.bitdefender.com/am/malware_removal/BDREvilDecryptor.exe) from Bitdefender (instructions (https://www.nomoreransom.org/uploads/REvil_documentation.pdf)) 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.



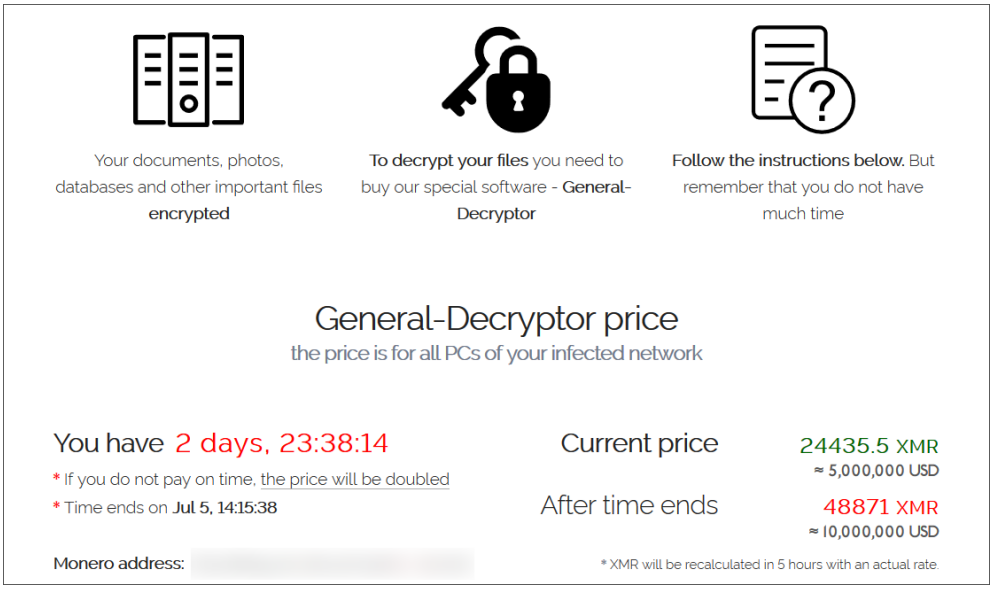
Decrypting REvil encrypted files with decryptor

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 (https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-shutting-down-after-claiming-to-earn-2-billion/).

Since launching in 2019, REvil has conducted numerous attacks against well-known companies, including JBS (https://www.bleepingcomputer.com/news/security/fbi-revil-cybergang-behind-the-jbs-ransomware-attack/), Coop (https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/), Travelex (https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-says-travelex-will-pay-one-way-or-another/), and Grupo Fleury (https://www.bleepingcomputer.com/news/security/healthcare-giant-grupo-fleury-hit-by-revil-ransomware-attack/).

Finally, in a massive July 2nd attack (https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-1-000-plus-companies-in-msp-supply-chain-attack/) using a Kaseya zero-day vulnerability, the ransomware gang encrypted sixty managed service providers and over 1,500 businesses worldwide.



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 (https://www.bleepingcomputer.com/news/security/revil-ransomware-gangs-web-sites-mysteriously-shut-down/) its operation on July 13th and disappeared.

While REvil was shut down, Kaseya mysteriously received a master decryptor (https://www.bleepingcomputer.com/news/security/kaseya-obtains-universal-decryptor-for-revil-ransomware-victims/) 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 (https://www.bleepingcomputer.com/news/security/revil-ransomware-is-back-in-full-attack-mode-and-leaking-data/) 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.