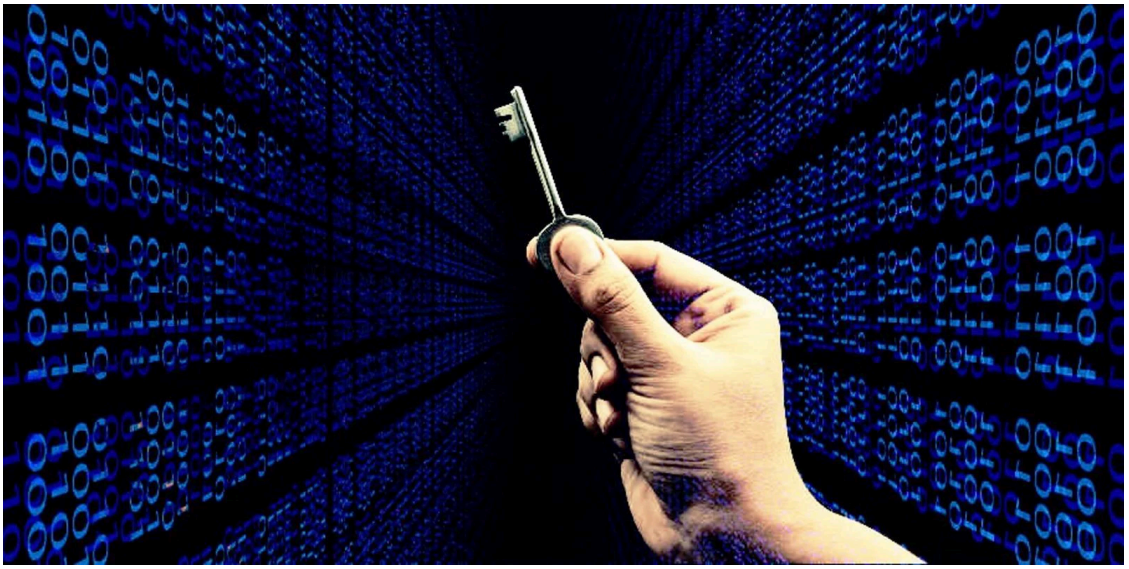
Babuk ransomware decryptor released to recover files for free

By Sergiu Gatlan

Published: 2021-10-27 · Archived: 2026-04-05 14:08:43 UTC

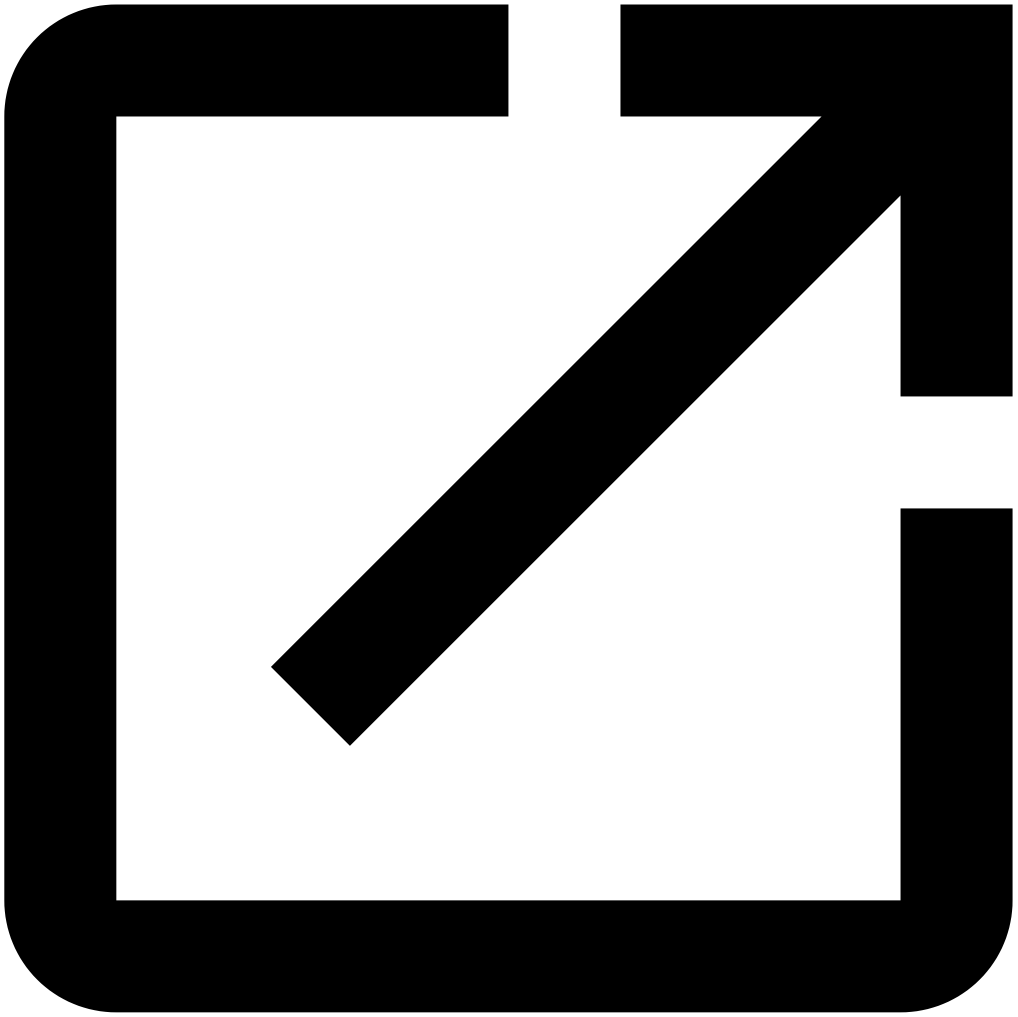


Czech cybersecurity software firm Avast has created and released a decryption tool to help Babuk ransomware victims recover their files for free.

According to Avast Threat Labs, the Babuk decryptor was created using leaked source code and decryption keys.

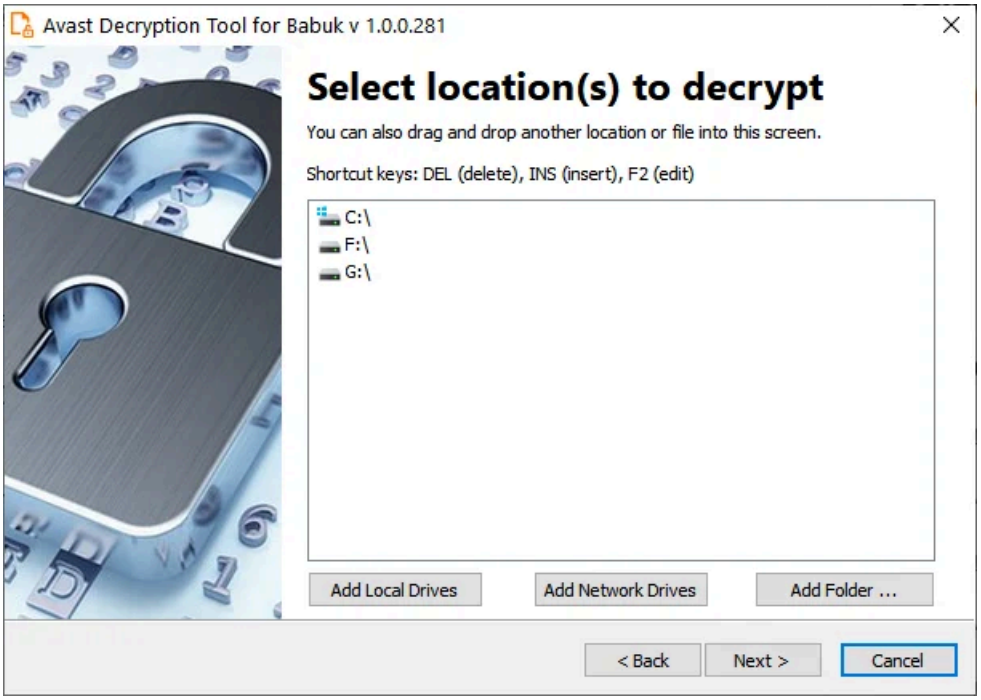
The free decryptor can be used by Babuk victims who had their files encrypted using the following extensions: .babuk, .babyk, .doydo.


DIE LINKE.
0:00



Babuk ransomware victims can download the decryption tool from Avast's servers and decrypt entire partitions at once using instructions displayed within the decryptor's user interface.

From BleepingComputer's tests, this decryptor will likely work only for victims whose keys were leaked as part of the Babuk source code dump.



Avast Babuk decryptor (BleepingComputer)

Ransomware and decryption keys leak

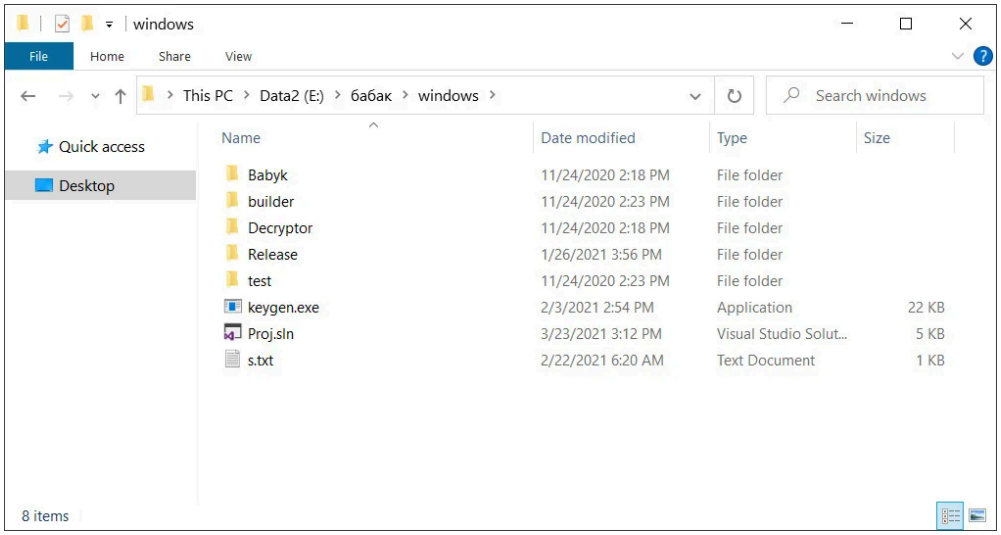
Babuk gang's full ransomware source code was leaked on a Russian-speaking hacking forum last month by a threat actor claiming to be a member of the ransomware group.

The decision to leak the code was motivated by the alleged Babuk member by his terminal cancer condition. He said in his leak post that he decided to release the source code while they have to "live like a human."

The shared archive contained different Visual Studio Babuk ransomware projects for VMware ESXi, NAS, and Windows encryptors, with the Windows folder contains the complete source code for the Windows encryptor, decryptor, and what looked like private and public key generators.

Included in the leak were also encryptors and decryptors compiled for specific victims of the ransomware gang.

After the leak, Emsisoft CTO and ransomware expert Fabian Wosar told BleepingComputer that the source code is legitimate and that the archive may also contain decryption keys for past victims.



Babuk Windows encryptor source code (BleepingComputer)

Babuk's troubled history

Babuk Locker, also known as Babyk and Babuk, is a ransomware operation that launched at the beginning of 2021 when it started targeting businesses to steal and encrypt their data as part of double-extortion attacks.

After their attack on the Washington DC's Metropolitan Police Department (MPD) they landed in U.S. law enforcement's cross hairs and claimed to have shut down their operation after beginning to feel the heat.

After this attack, the gang's 'Admin' allegedly wanted to leak the stolen MPD data online for publicity, while the other members were against it.

Following this, Babuk members splintered off, with the original admin launching the Ramp cybercrime forum and the others relaunching the ransomware under the Babuk V2 name, continuing to target and encrypt victims ever since.

Right after the Ramp cybercrime forum's launch, it was targeted by a series of DDoS attacks that eventually led to the site becoming unusable.

While the Babuk Admin blamed his former partners for third incident, the Babuk V2 team told BleepingComputer that they were not behind the attacks.

Source: https://www.bleepingcomputer.com/news/security/babuk-ransomware-decryptor-released-to-recover-files-for-free/