


Avast Updates Babuk Ransomware Decryptor in Cooperation with Cisco Talos and Dutch Police

 decoded.avast.io/threatresearch/avast-updates-babuk-ransomware-decryptor-in-cooperation-with-cisco-talos-and-dutch-police/

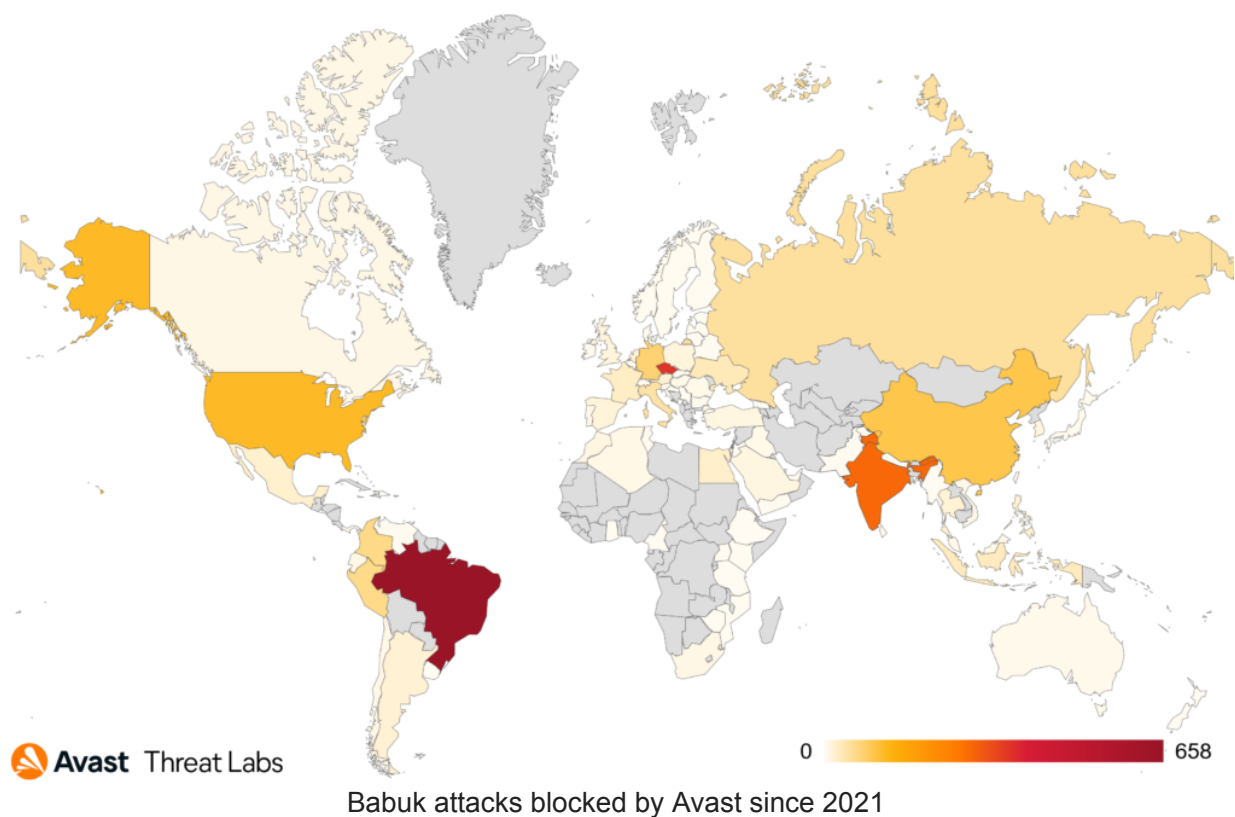
January 9, 2024



by [Threat Research Team](#) January 9, 2024 2 min read

Babuk, an advanced ransomware strain, was publicly discovered in 2021. Since then, Avast has blocked more than 5,600 targeted attacks, mostly in Brazil, Czech Republic, India, the United States, and Germany.

Today, in cooperation with Cisco Talos and Dutch Police, Avast is releasing an updated version of the Avast Babuk decryption tool, capable of restoring files encrypted by the Babuk variant called Tortilla. To download the tool, click [here](#).



Babuk Ransomware Decryptor

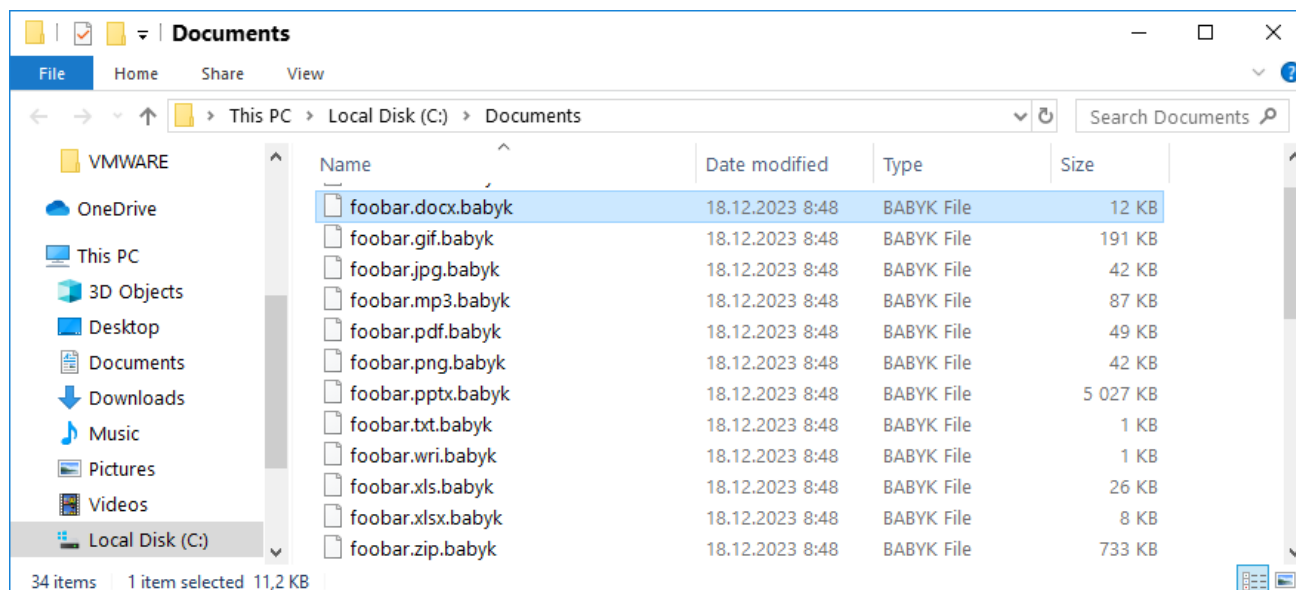
In September 2021, the source code of the Babuk ransomware was released on a Russian-speaking hacking forum. The ZIP file also contained 14 private keys (one for each victim). Those keys were ECDH-25519 private keys needed for decryption of files encrypted by the Babuk ransomware.

The Tortilla Campaign

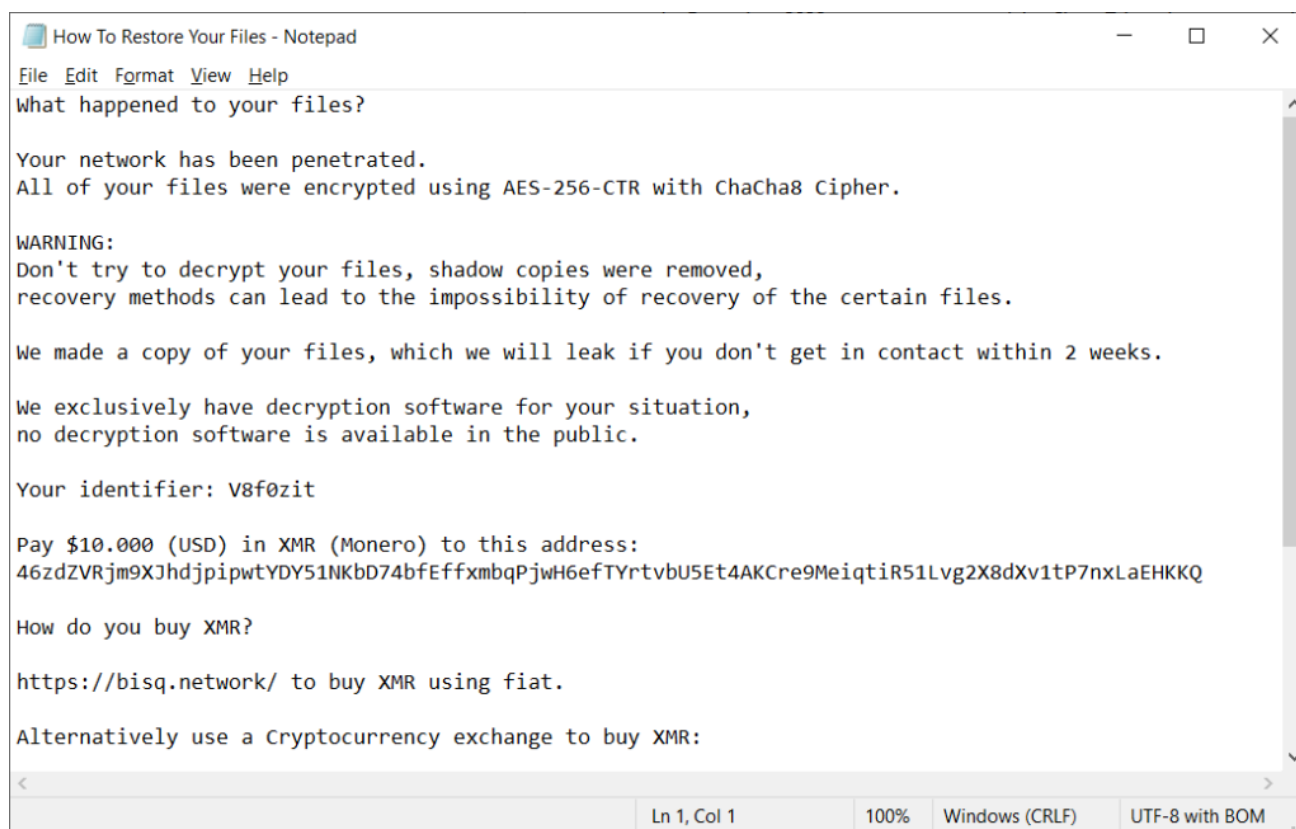
After brief examination of the provided sample (originally named `tortilla.exe`), we found out that the encryption schema had not changed since we analyzed Babuk samples 2 years ago. The process of extending the decryptor was therefore straightforward.

The Babuk encryptor was likely created from the leaked sources using the build tool. According to Cisco Talos, a single private key is used for all victims of the Tortilla threat actor. This makes the update to the decryptor especially useful, as all victims of the campaign can use it to decrypt their files. As with all Avast decryptors, the Babuk Ransomware Decryptor is available for free.

Babuk victims can find out whether they were part of the Tortilla campaign by looking at the extension of the encrypted files and the ransom note file. Files encrypted by the ransomware have the `.babyk` extension as shown in the following example:



The ransom note file is called **How To Restore Your Files.txt** and is dropped to every directory. This is how the ransom note looks like:



Babuk victims can download the Babuk Decryptor for free: https://files.avast.com/files/decryptor/avast_decryptor_babuk.exe. It is also available within the NoMoreRansom project.

We would like to thank Cisco Talos and the Dutch Police for the cooperation.

IOCs (indicators of compromise)

bd26b65807026a70909d38c48f2a9e0f8730b1126e80ef078e29e10379722b49
(tortilla.exe)

Tagged as decryptor, decryptors, ransomware

Share: X Facebook