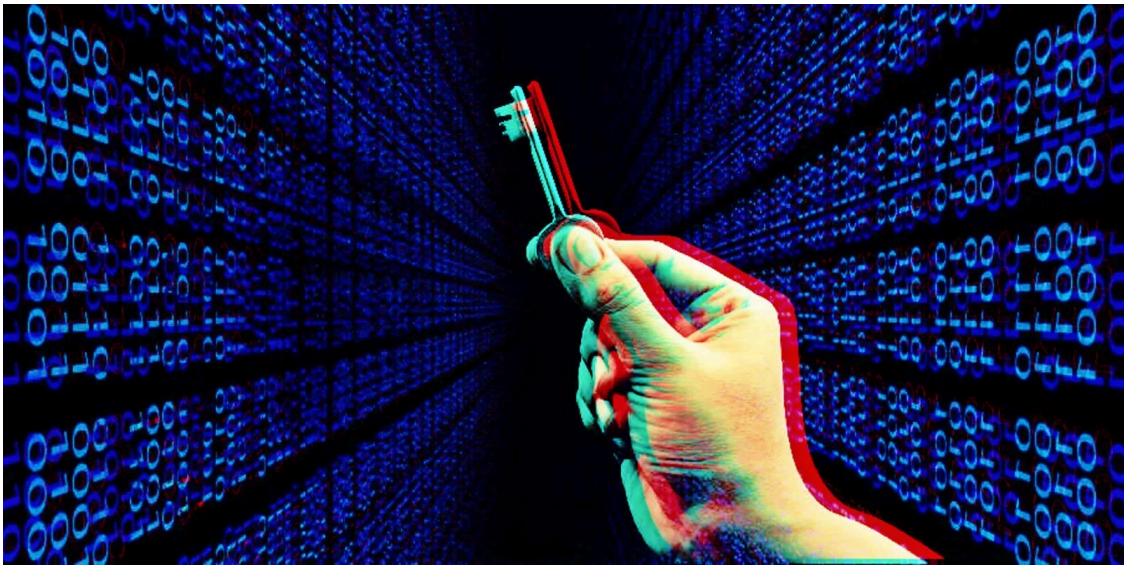
# Free decryptor released for TargetCompany ransomware victims

By Sergiu Gatlan

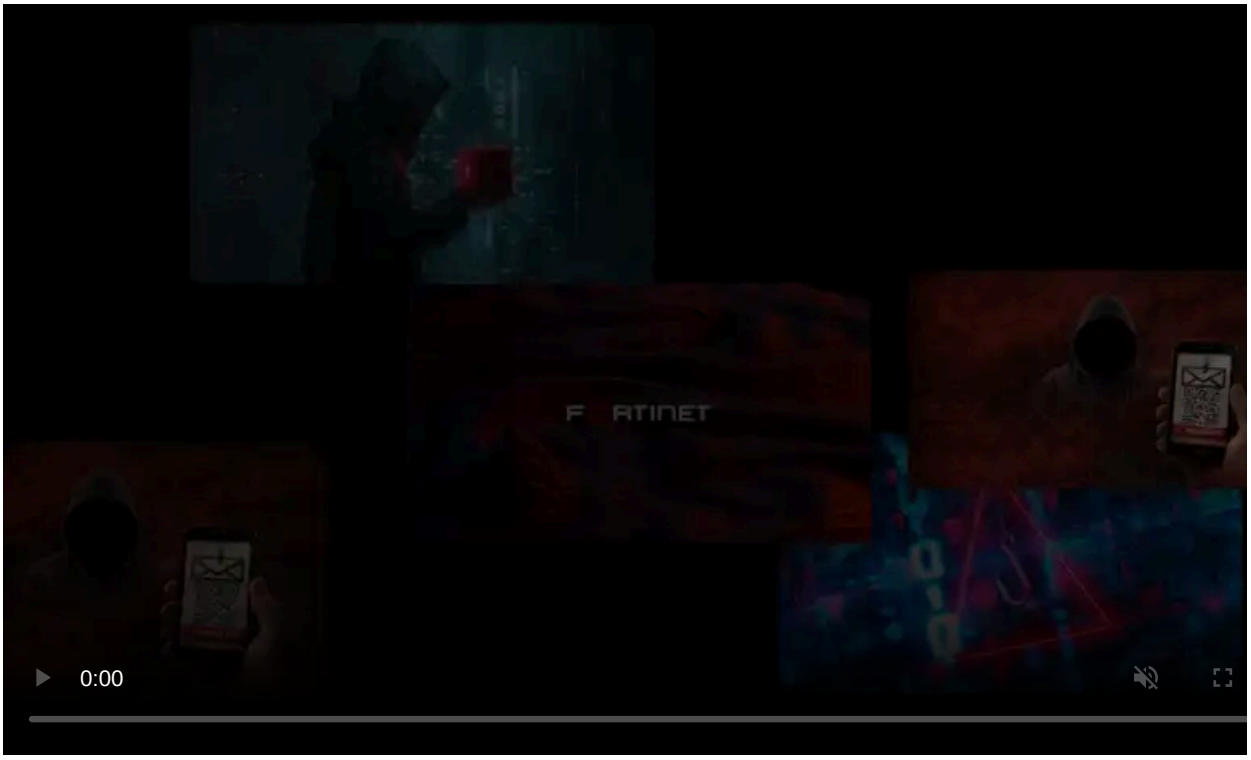
Published: 2022-02-07 · Archived: 2026-04-06 00:37:15 UTC



Czech cybersecurity software firm Avast has released a decryption utility to help TargetCompany ransomware victims recover their files for free.

However, as Avast warns, this decryptor can only be used to restore encrypted files "under certain circumstances."

Victims who want to recover their files using this decrypting tool should also be aware that this will likely be a resource-intensive and time-consuming process.

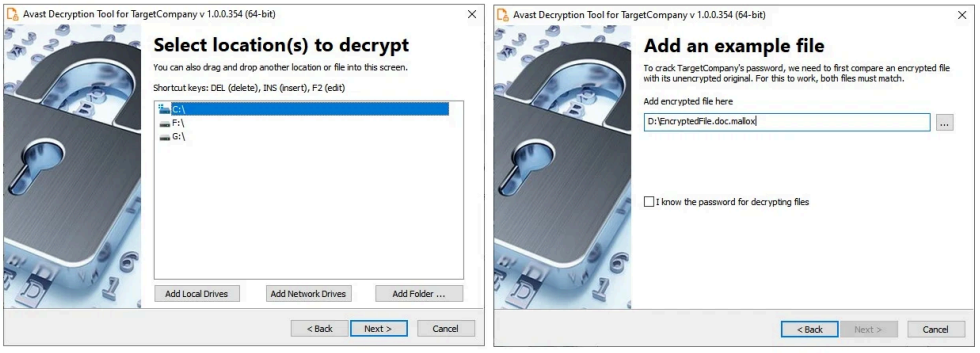

F RTINET
0:00

"During password cracking, all your available processor cores will spend most of their computing power to find the decryption password. The cracking process may take a large amount of time, up to tens of hours," Avast said.

"The decryptor periodically saves the progress and if you interrupt it and restart the decryptor later, it offers you an option to resume the previously started cracking process."

The TargetCompany ransomware decryptor works by cracking the password after comparing an encrypted file with its original unencrypted version.

Avast says this only has to be done once per each device encrypted by TargetCompany ransomware since the decryptor wizard will allow you to enter previously cracked encryption passwords by selecting the "I know the password for decrypting files."




*TargetCompany decryptor (BleepingComputer)*

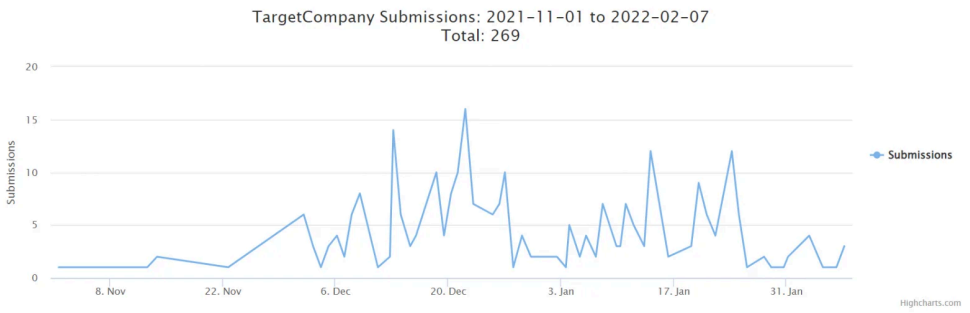
**TargetCompany ransomware victims can download the decryption tool from Avast's servers (64-bit or 32-bit) to decrypt entire disk partitions using the instructions displayed within the tool's user interface.**

"On the final wizard page, you can opt-in whether you want to backup encrypted files. These backups may help if anything goes wrong during the decryption process," Avast added.

"This option is turned on by default, which we recommend. After clicking 'Decrypt,' the decryption process begins. Let the decryptor work and wait until it finishes."

You can find additional instructions on how to use Avast's TargetCompany ransomware decryptor here.

TargetCompany is a relatively newly discovered ransomware strain, active since mid-June 2021, that will add a .mallox, .exploit, .architek, or .brg extension to all encrypted files.




*TargetCompany ransomware submissions (ID-Ransomware)*

It also drops a ransom note file named "HOW TO RECOVER !!.TXT" in all folders containing encrypted files.

This happens after it deletes volume shadow copies, reconfigures boot options, and kills processes that could lock databases of sensitive information (e.g., MySQL, Oracle, SQL Server).

Avast also released free decryptors for Babuk, AtomSilo, and LockFile ransomware in October 2021 to allow victims to recover their files without paying a ransom.



---

Source: https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-targetcompany-ransomware-victims/