

Disable malicious HiddenTear Ransomware with HT Brute Forcer

If your system has been infected with HiddenTear malicious code, don't worry because a program called HT Brute Forcer (developed by Michael Gillespie) can allow you to recover your encryption key without paying ransom.

If your system has been infected with HiddenTear, do not worry because a program called HT Brute Forcer (developed by Michael Gillespie) can allow you to recover your encrypted files but Don't pay ransom.

HiddenTear is the name of a family of full-source extortion software released on GitHub. This allows an attacker to download the source code and create their own ransomware variants, and these variations can be used to infect large-scale.

1. How to remove / fix ransomware WannaCry



Due to the huge availability of source code, there are many ransomware variants developed under different names but still use the same HiddenTear code base. However, it is also the use of the same platform code that makes these types of malicious code more easily decoded. We can completely use a single decoding method to deal with many different HiddenTear variants.

Some HiddenTear variants are supported by this decoding tool including:

8lock8, AnonCrack, Assembly, Balbaz, BankAccountSummary, Bansomqare Wanna, Blank, BloodJaws, Boris, CerberTear, CryptConsole2, CryptoKill, CyberResearcher, Data_Locker, Dev-Nightmare 2xx9, Diamond, Domino, Donut, dotRansom, Executioner, Executioner2, Executioner3, Explerer, FlatChestWare, Frog, Fuck_You, Gendarmerie, Horros, JobCrypter, Jodis, J-Ransomware, J-Want-To-Cry, Karmen, Kraken 2.0, Kratos, LanRan, Lime, Lime-HT, Luv, Matroska, MireWare, MoonCrypter, MTC, Nobug, Nulltica, onion3cry, OpsVenezuela, Paul, PayOrDie, Pedo, PGPSnippet, Poolezoor, Pransomware, Predator, Qwerty, Random6, Random6 2, Randion, RansomMine, Rootabx, Saramat, Shrug, ShutUpAndDance, Sorry, Symbiom, TearDr0p, Technicy, The Brotherhood, TheZone, tlar, TotalWipeOut, TQV, Ton, VideoBelle, WhiteRose, WhiteRose2,

Zalupaid, ZenCrypt, Zenis, ZeroRansom, Zorro

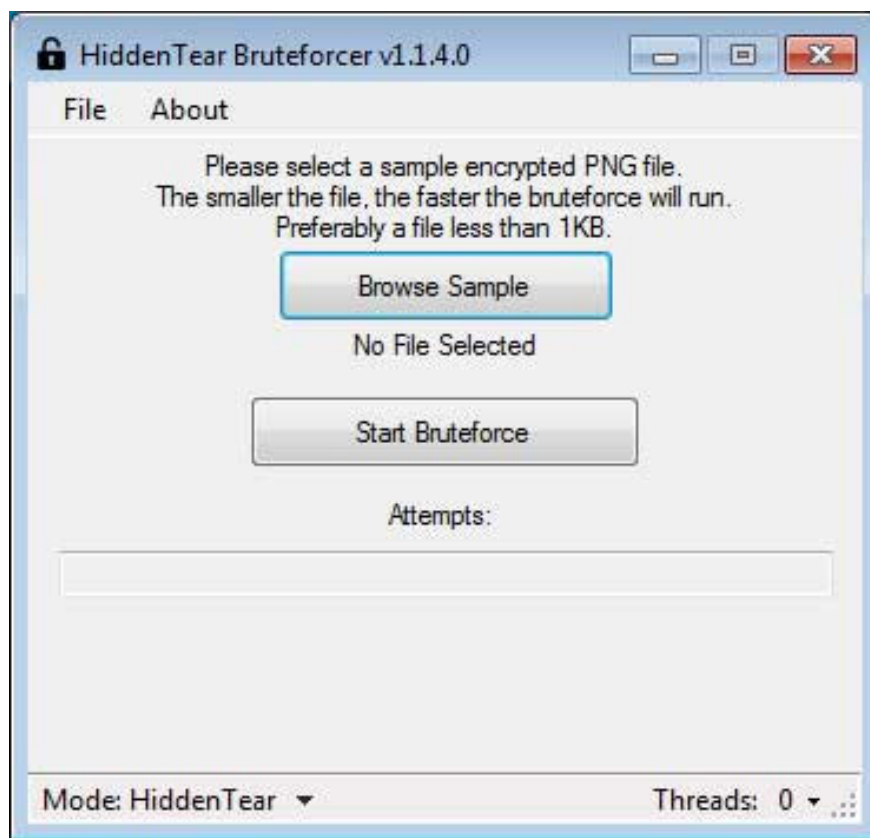
If your computer is infected with HiddenTear extortion software, you can use the following instructions to proceed to decrypt your files for free.

How to decrypt the file is encrypted by HiddenTear

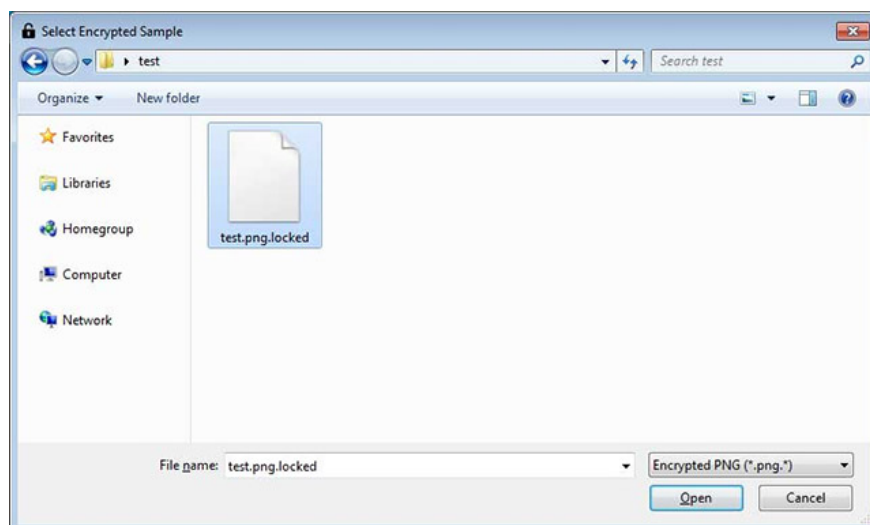
If you do not have HT Brute Forcer please download this software first by clicking the download link below and save the software to your Windows screen right away.

Download HT Brute Forcer

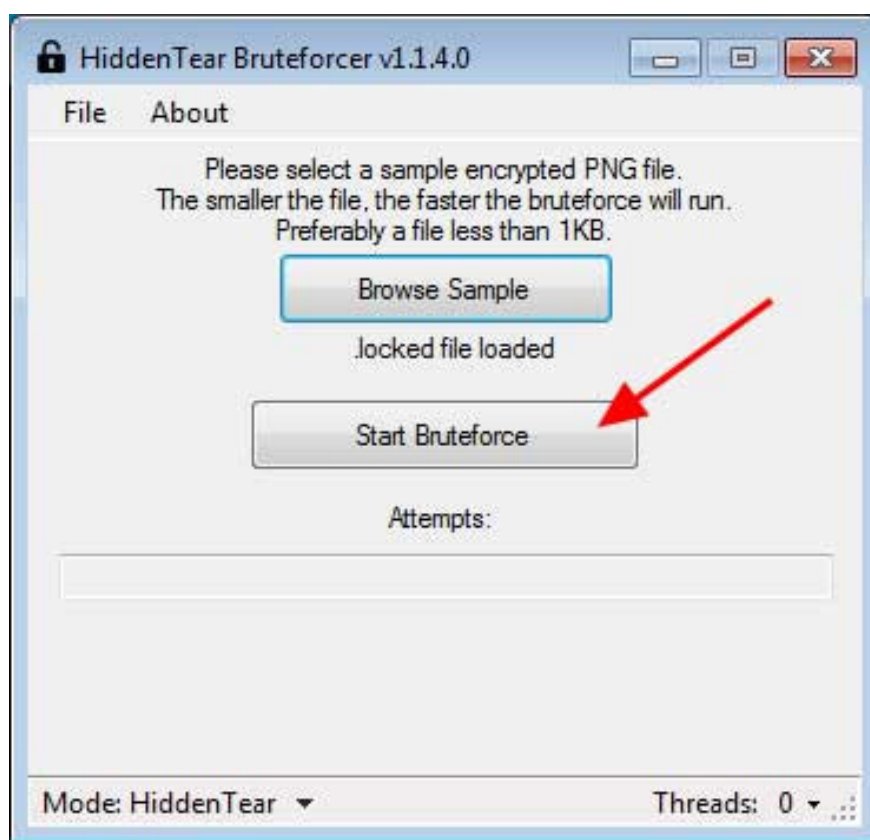
After downloading, you will have to unzip the file hidden-tear-bruteforcer.zip and then, a file named HiddenTear Bruteforcer.exe will be extracted. Now double-click the HiddenTear Bruteforcer.exe executable file to start the program launch.



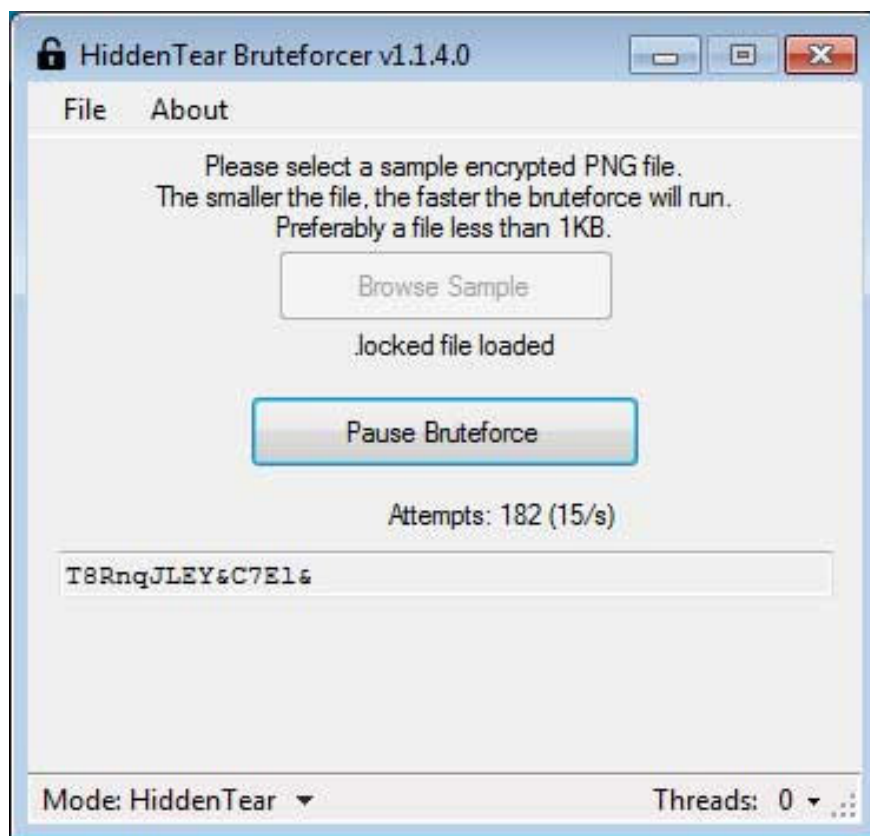
After the program has been launched, click the **Browse Sample** button and the program will ask you to find the encrypted PNG file. The smaller the better.



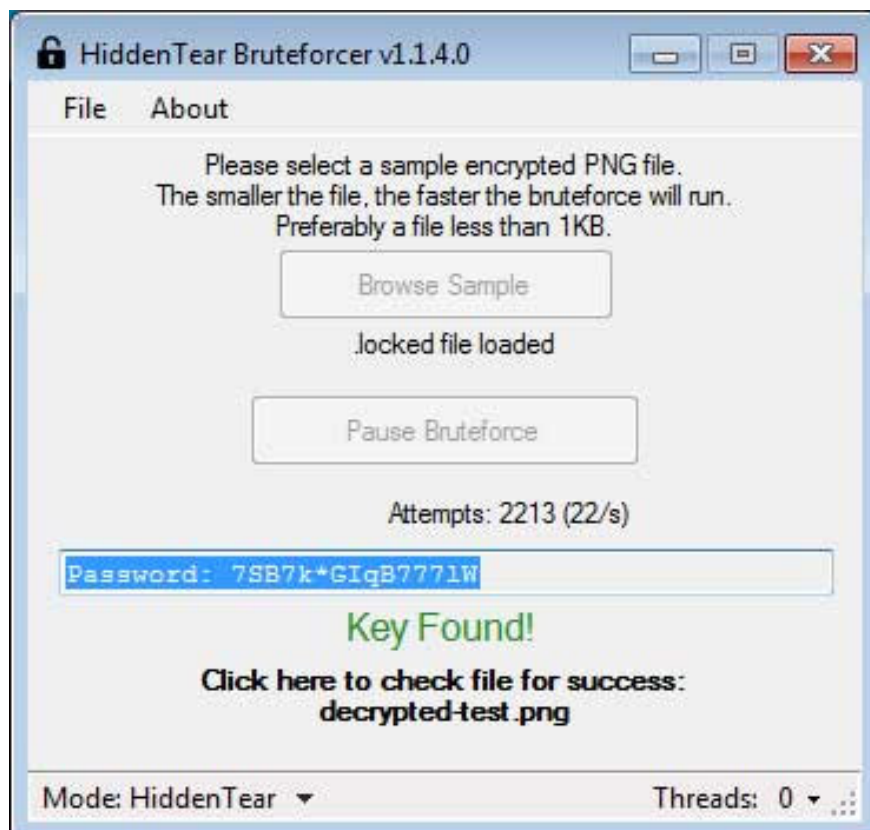
After you have selected an encrypted file, the tool will indicate that the file has been uploaded. Now, click on **Start Bruteforce** button to start decoding as shown below.



The program will now start taking the decryption key. This process may take some time, so please wait patiently while Bruteforcer works.



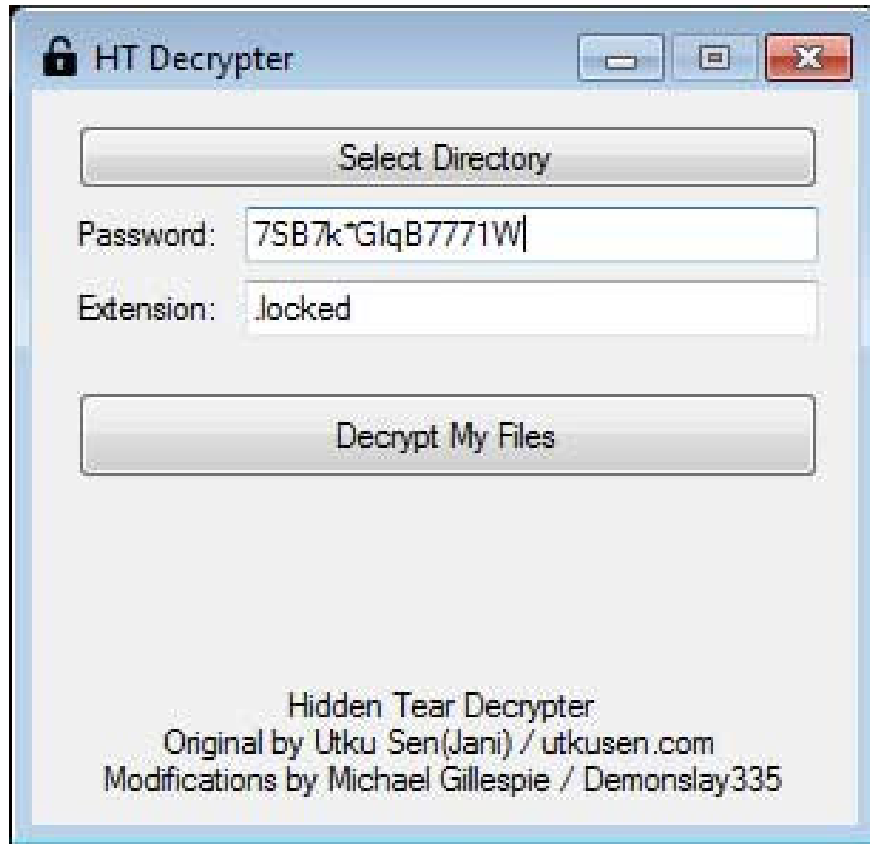
When you find a successful encryption key, the program will automatically decrypt the encrypted file that you have uploaded, and ask you to determine if it has been properly decrypted.



If the file has been properly decoded, you should record the detected key / password and save it for use with the HiddenTear decoder that you will have to download now.

Now you need to download the HiddenTear standalone decoder.

Once you have downloaded the HiddenTear decoder, you double-click the hidden-tear-decrypter.exe file to start the program. Once the program has been launched, enter the key detected above.



After entering the key, click the **Decrypt My Files** button to start decrypting the files encrypted by HiddenTear on your computer. When the decoding process is completed, the program will display a screen showing how many files have been successfully decoded.



At this point, you can close the program because your files are now decoded.

Above is how to disable malicious HiddenTear Ransomware with HT Brute Forcer. Good luck!

See more:

1. How to protect yourself from phishing attacks via mobile phones
2. How to use Trend Micro RansomBuster blocks ransomware
3. 3 types of virus scans and the right time to use
4. How do I know if a file is mistakenly identified as containing malicious code?

You finished reading the article "**Disable malicious HiddenTear Ransomware with HT Brute Forcer**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.