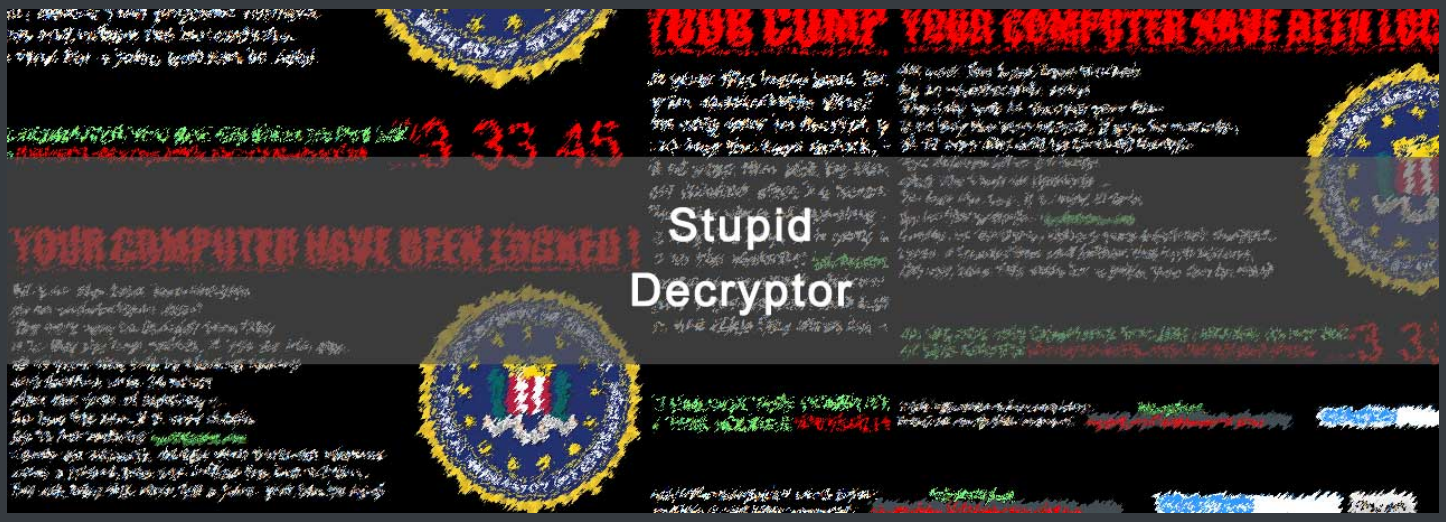
How to Decrypt the Stupid Ransomware Family with StupidDecrypter

By Lawrence Abrams

- December 21, 2018
- 10:17 AM
- 2



Stupid Ransomware is a family of ransomware infections that are typically utilized by less skilled developers and many utilize themes based on movies, pop-culture, or pretend to be law enforcement. This family of ransomware infections are created using an open source project that was posted to GitHub.

The good thing about this ransomware family is that they static encryption keys and thus are easy to decrypt. You can see an example of a Stupid Ransomware variant below.

Stupid Ransomware variant

Michael Gillespie has created a decryptor called StupidDecryptor that contains the decryption keys for all known Stupid Ransomware variants that were released. The currently supported variants are the ones that append the following extensions to the names of encrypted files.

bleepingcomputer

From a bleeping computer to a working computer

Top Articles

American

OOPS!

READ MOREYouTube down: Live streams hit byworldwide outage

```
.666, .adam, .alosia, .android, .ANNABELLE, .anon, .bycicle, .corrupted,
.crypted, .CYRON, .deria, .devil, .Doxes, .encrypt, .eTeRnItY,
.FailedAccess, .fucked, .fucking, .fun, .H34rtBl33d, .Harzhuangzi, .haters,
.iGotYou, .jeepers, .jigsaw, .killedXXX, .lock, .malki, .Malki, .MIKOYAN,
.Nazi, .powned, .purge, .slvpawned, .SnakeEye, .Tesla, .whycry, .WINDIE,
.XmdXtazX, .xncrypt, _crypt0, _nullbyte
```

Instructions on how to use StupidDecryptor are below.

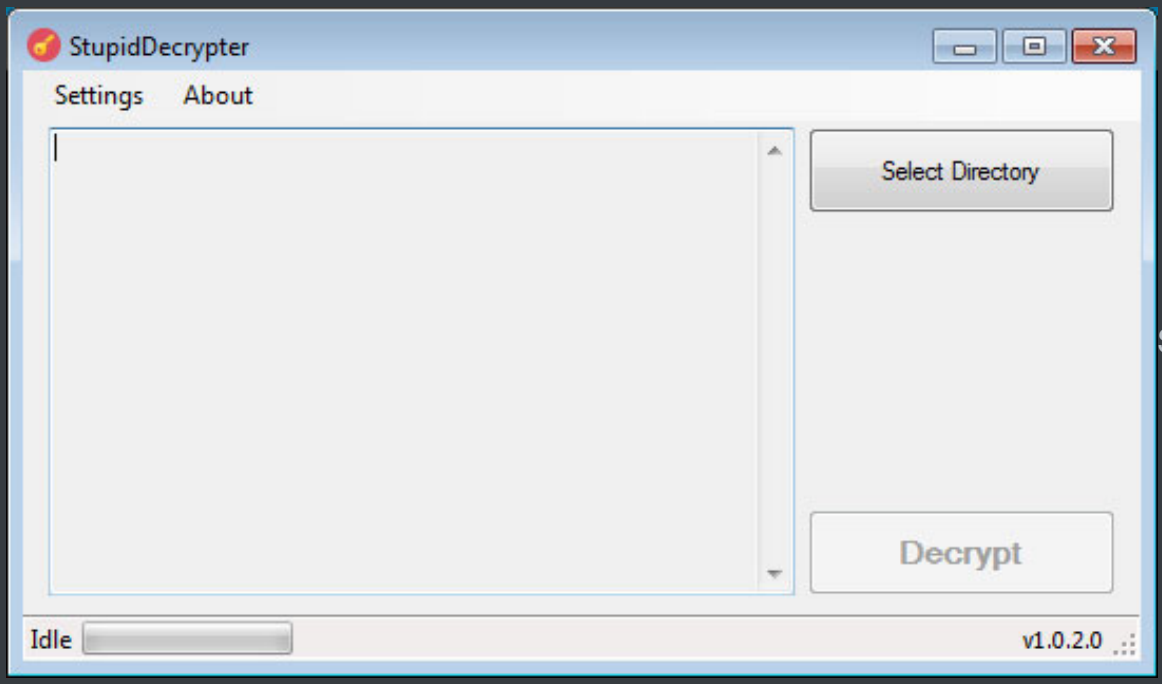
How to Decrypt Stupid Ransomware variants

To decrypt a Stupid Ransomware variant you can download the StupidDecryptor from the link below.

STUPIDDECRYPTOR

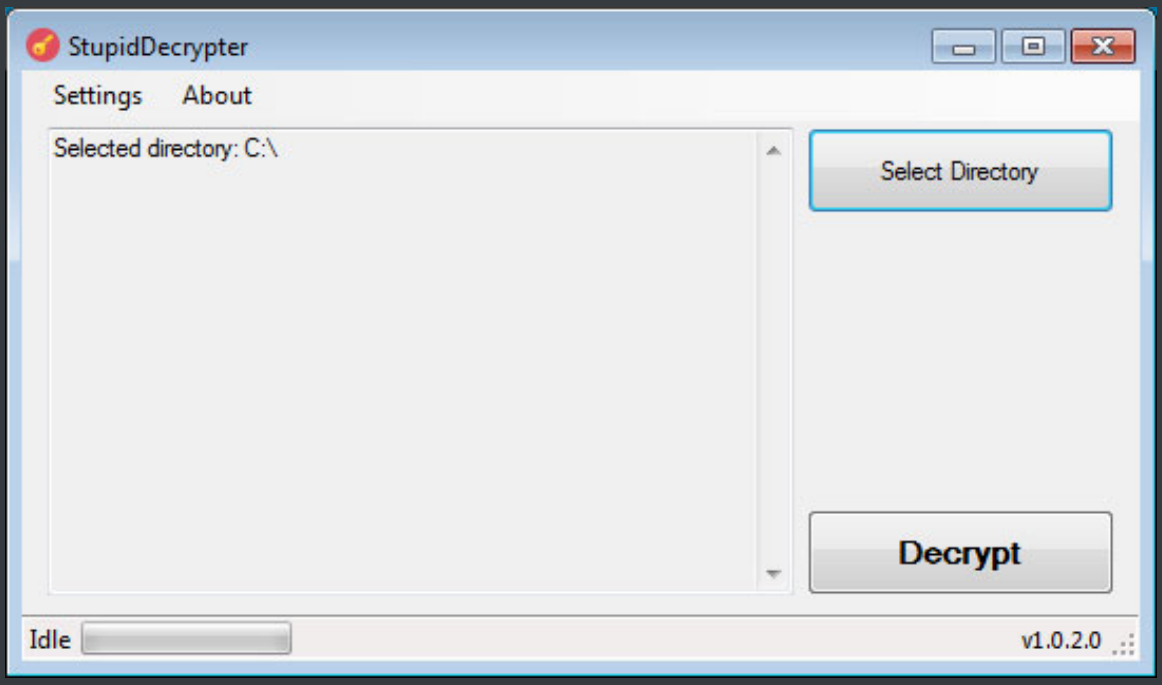
DOWNLOAD NOW

Once downloaded, simply double-click on the executable to start the decryptor and you will be greeted with the main screen.

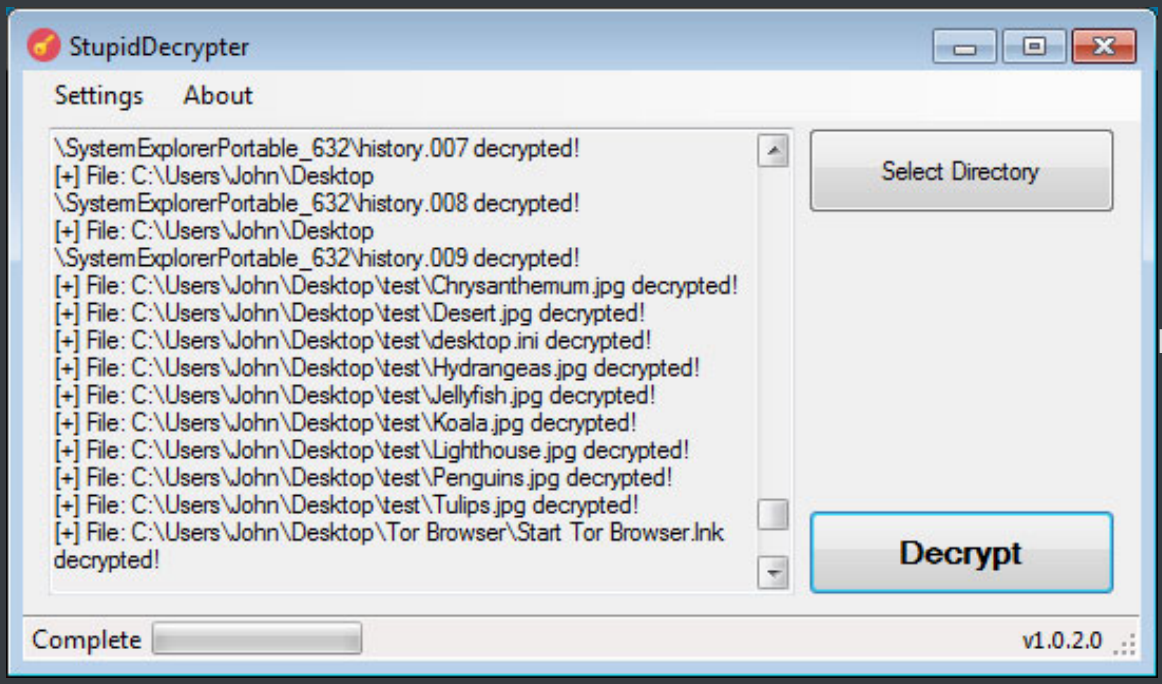


StupidDecryptor

Now click on the **Select Directory** button and select the drive you would like to decrypt, such as the C:\ drive. Once you select a drive, the Decrypt button will become available.

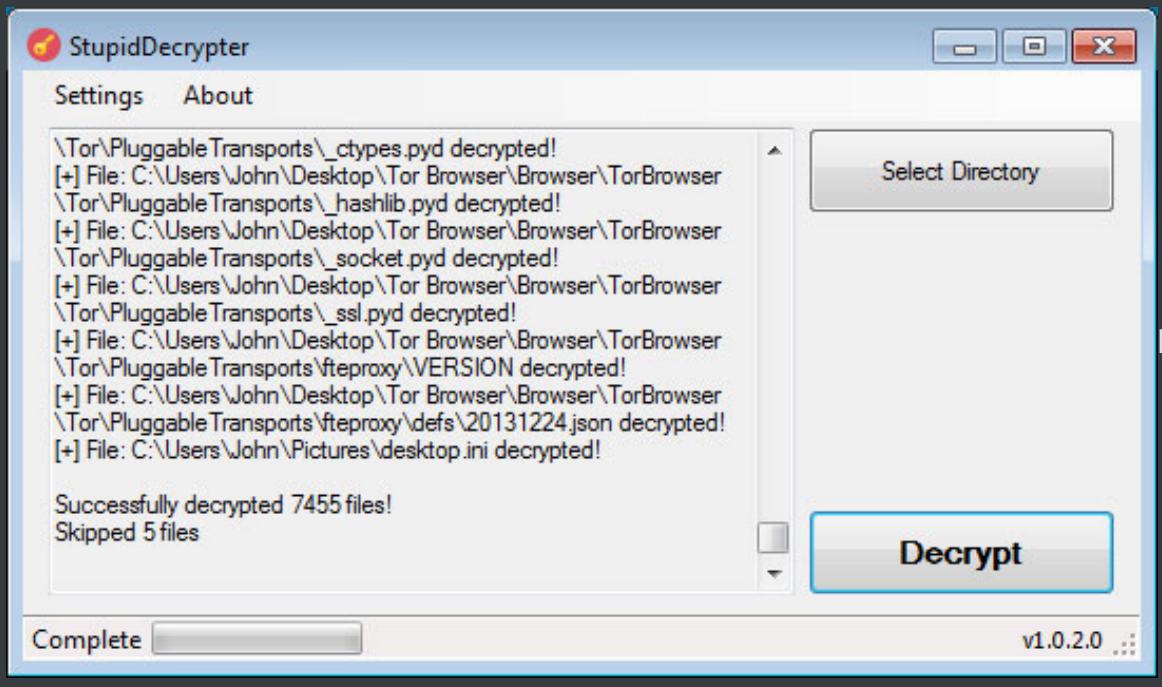


Now click on the **Decrypt** button to begin decrypting the selected folder. Once you click Decrypt, the program will decrypt all the encrypted files and display the decryption status in the window.



Decrypting Files

When it has finished, the decryptor will display a summary of the amount of files that have been decrypted. If some of the files were skipped it may be due to permissions configured on those files.



Decryption Finished

Though your files are now decrypted, the original encrypted files will still be on your computer. Once you confirm that your files have been properly decrypted, you can use CryptoSearch to move all the encrypted files into one folder so you can delete or archive them.

You can now close the decryptor and use your computer as normal. If you need help using this decryptor, feel free to leave a comment.

Related Articles:

No More Ransom helps millions of ransomware victims in 6 years

Microsoft SQL servers hacked in TargetCompany ransomware attacks

The Week in Ransomware - September 23rd 2022 - LockBit leak

BlackCat ransomware's data exfiltration tool gets an upgrade

LockBit ransomware builder leaked online by “angry developer”