Pylocky decryption tutorial

Your computer has been infected by the ransomware PyLocky.

You have, on your system, encrypted files and several identical files named LOCKY-README.txt have appeared as follows:

```
Please be adviced:

All your files, pictures document and data has been encrypted with Military Grade Encryption RSA AES-256.

Your information is not lost. But Encrypted.

In order for you to restore your files you have to purchase Decrypter.

Follow this steps to restore your files.


1* Download the Tor Browser. ( Just type in google "Download Tor" ).

2* Browse to URL : http://pylockyrkumqih5l.onion/index.php

3* Purchase the Decryptor to restore your files.


It is very simple. If you don't believe that we can restore your files, then you can restore 1 file of image format for free.

Be aware the time is ticking. Price will be doubled every 96 hours so use it wisely.


Your unique ID : 8ERA5C89S1VR27AT


CAUTION:

Please do not try to modify or delete any encrypted file as it will be hard to restore it.


SUPPORT:

You can contact support to help decrypt your files for you.

Click on support at http://pylockyrkumqih5l.onion/index.php


--------BEGIN BIT KEY---------

g+1h38goWCvhPPlc8P2vU/ClI0wus4fkemma7KtsAjoD/jQWwRRdlZHYhSflvNp/bgtqyMCbxIOF
TPfjtsKoFo4jO+1KSWH+b4pQe2G4EoyfEI39nVopqnYXzq9FGq/KtP70rLzk4T1rMR8fEDVATm61
Fe15aAfIOEeluD+Hc5cty3pDwCYddADhBxsqQt0W9nh9E0WH6cCY9yRV97EsFxH2kByFqZ9pupAK
PfeseKf4vlAuHO61G9M2ONW0FBRY0zLPhTlD4PeXJuoH+wBlL2zB8pFneOQtRH/ij5R3UouZitp5
qgGL/AiChNPS1V9i58ACs0pudO03k70MfBFgAA==
```

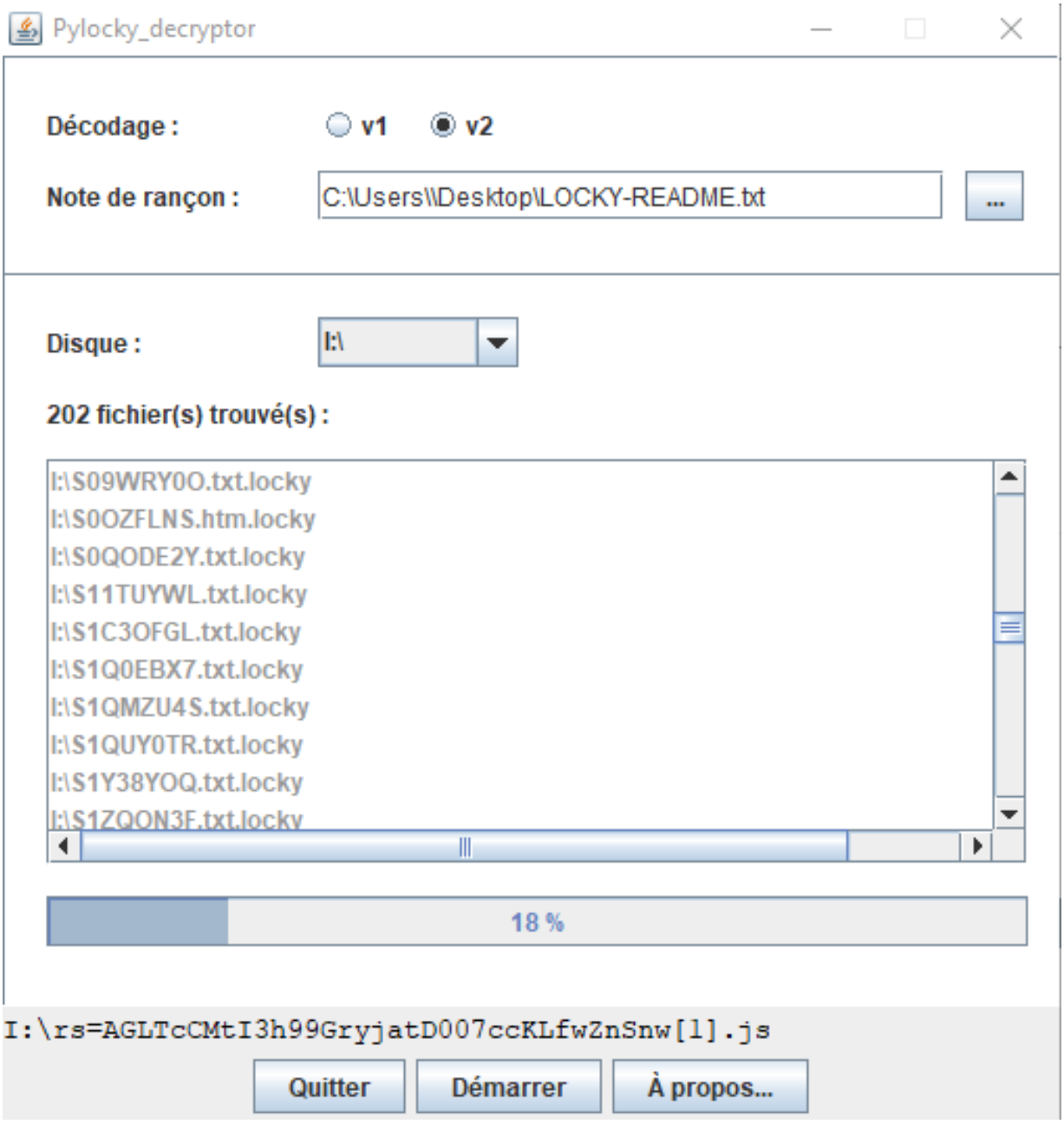
If the encrypted files have the extension:

- « .lockedfile” or « .lockymap »: it is the first version of Pylocky
- « .locky » : it is the second version.

In order to decrypt your files for free, without paying the ransom, please follow the steps below:

On a computer running the operating system Windows 7 or higher,

- Install Java Runtime Environment or JRE version 8, available for free on Oracle's website (https://www.java.com/download/)
- Connect the drive to the computer you are about to use for the analysis and whose hard drive's files have been encrypted.
- Download the program Pylocky_Decryptor.jar
- Run the program by double-clicking on it.
- The window below should appear:



Select the version of Pylocky (V1 : .Lockymap .Lockedfile / V2: .Locky)

Select, by clicking on the selection button, the ransom note LOCKY-README.txt copied on your external drive.

Select the drive's letter matching your external drive by clicking on the arrow:

Then click on « Démarrer ».

The program will automatically search for the encrypted files copied on the disk & proceed to their decryption.

If no encrypted file is detected, please make sure that:
- you have chosen the correct letter of the disk's drive;
- you have selected the right version of the malicious software then start again.

If you don't have the opportunity to connect the infected drive on a clean system with Pylocky_-Decryptor on it, you can also install it directly on the infected computer

We advise you, once all your files have been decrypted, to transfer them on a new system and not to use the infected computer's system as it might still contain malicious files.