Tutoriel de déchiffrement Pylocky

Votre ordinateur a été infecté par le Raçongiciel PyLocky.

Vous avez sur votre système des fichiers chiffrés et il est apparu plusieurs fichiers identiques intitulé LOCKY-README.txt de cette forme.

```
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==
```

Si les fichiers chiffrés comportent l'extension :
- « *.lockedfile* » ou « *.lockymap* » : Il s'agit de la version 1 de Pylocky
- « *.locky* » : Il s'agit de la version 2.

Pour déchiffrer gratuitement vos fichiers, sans payer la rançon, veuillez suivre les étapes suivantes.

Sur un ordinateur équipé d'un système d'exploitation Windows 7 ou plus,

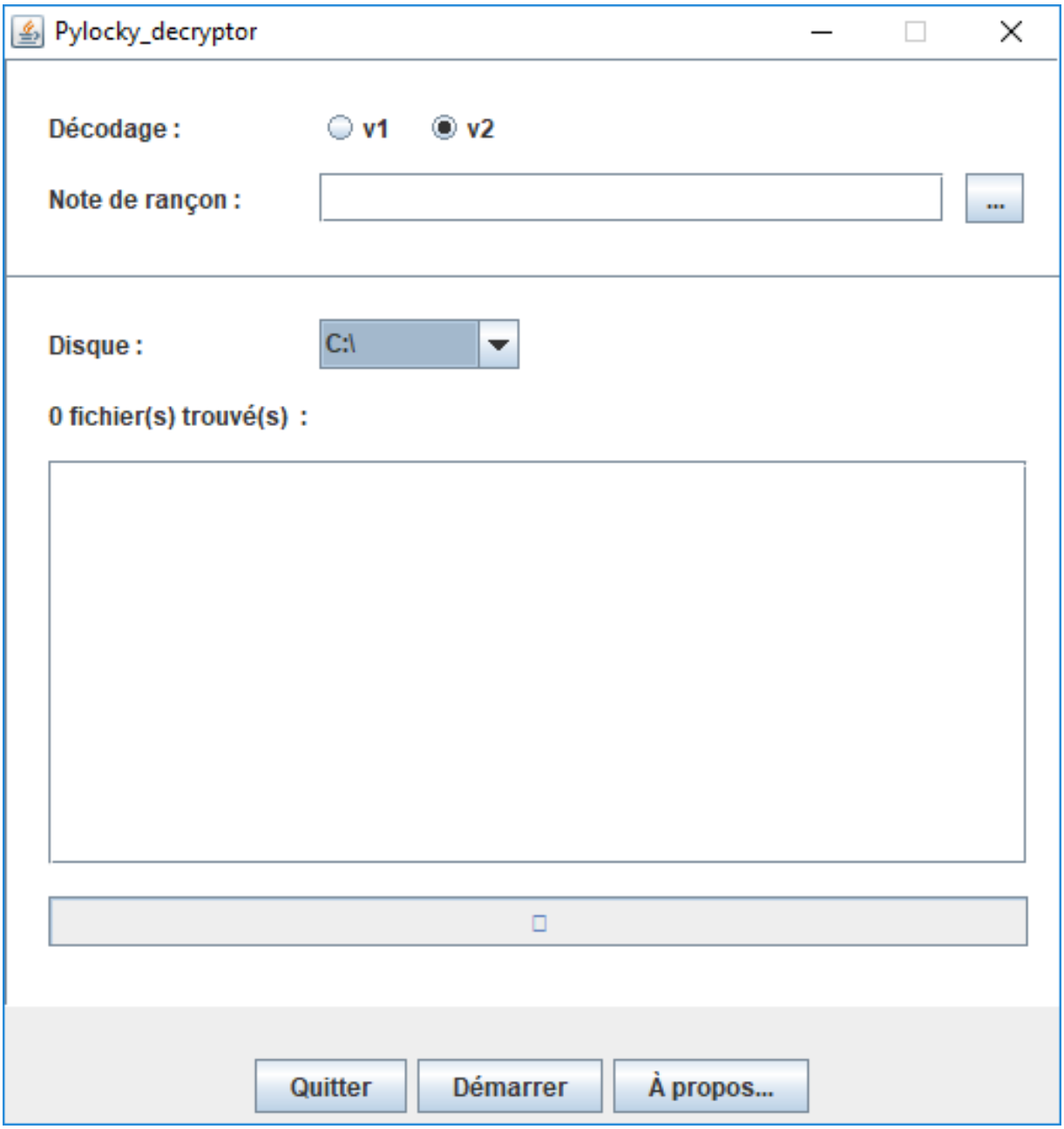
- Installer Java Runtime Environment ou JRE version 8, disponible gratuitement sur le site de Oracle (https://www.java.com/fr/download/)

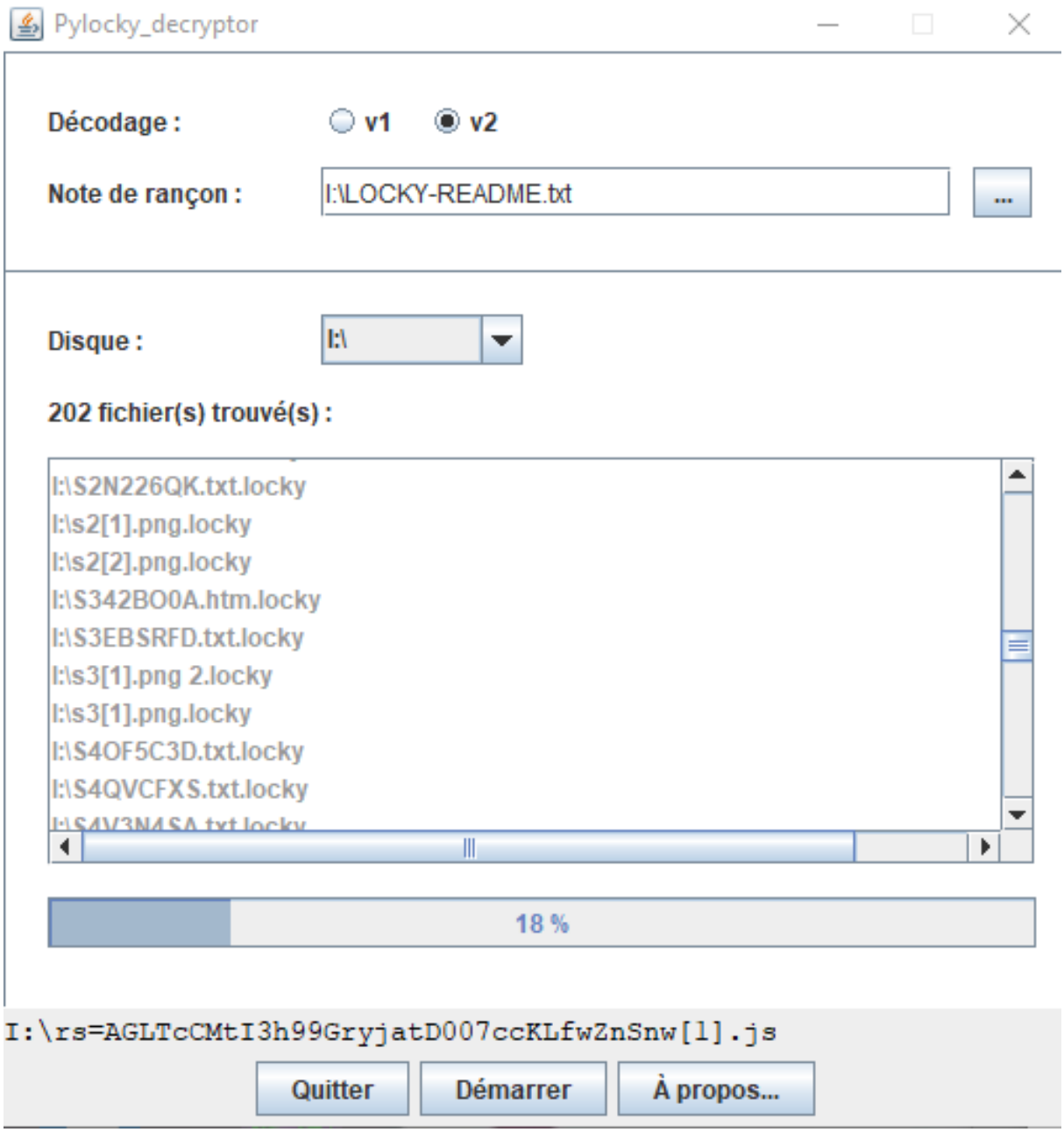
- Connecte, sur l'ordinateur que vous allez utiliser pour l'analyse, le disque dur dont les fichiers ont été chiffrés

- Télécharger le programme Pylocky_Decryptor.jar

- Exécuter le programme en double cliquant sur celui-ci.

- La fenêtre suivante devrait apparaître :





Sélectionnez la version de Pylocky (V1 : .Lockymap .Lockedfile / V2: .Locky)

Sélectionnez, en cliquant sur le bouton de sélection , la note de rançon LOCKY-README.txt qui se trouve sur votre disque externe.

Sélectionner la lettre du lecteur correspondant à votre disque externe en cliquant sur la flèche

Ensuite cliquez sur Démarrer

Le programme va rechercher automatiquement les fichiers chiffrés présents sur le disque, et procéder à leur déchiffrement

Si aucun fichier chiffré n'est détecté, vérifiez :
- que vous avez choisi la bonne lettre de lecteur de disque
- que vous avez bien sélectionné la version du programme malveillant puis recommencer .

Si vous n'avez pas la possibilité de connecter le disque infecté à un système sain comprenant le déchiffreur, vous pouvez également installer ce dernier directement sur l'ordinateur qui a été compromis par PyLocky.

Nous vous recommandons, une fois vos fichiers déchiffrés, de les transférer sur un nouveau système et de ne pas réutiliser celui de l'ordinateur infecté, celui-ci contenant probablement toujours les fichiers malveillants