pyLocky Decryptor Released by French Authorities

bleepingcomputer.com/news/security/pylocky-decryptor-released-by-french-authorities/

Lawrence Abrams

By
Lawrence Abrams

- June 13, 2019
- 03:57 PM
- 2

A decryptor for pyLocky Ransomware versions 1 and 2 has been released by French authorities that allows victim to decrypt their files for free.

According to a post by the French Ministry of Interior, this decryptor was created in collaboration between French law enforcement, the French Homeland Security Information Technology and Systems Service, and volunteer researchers.

"This tool is a result of a collaboration among the agencies of the french Ministry of Interior, including first the Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) of the Direction régionale de la police judiciaire de Paris, on the basis of technical elements gathered during its investigations and the collaboration with volunteer researchers. Those elements allowed the Service des technologies et des systèmes d'information de la sécurité intérieure ST(SI)², part of the Gendarmerie nationale, to create that software."

While pyLocky has not seen a wide distribution, the post by the French Ministry of Interior states it is more active in Europe.

"PyLocky is very active in Europe and there are already many victims in France, both within the professional environment (SMEs, large businesses, associations, etc.) as well as at home."

Getting the pyLocky Decryptor

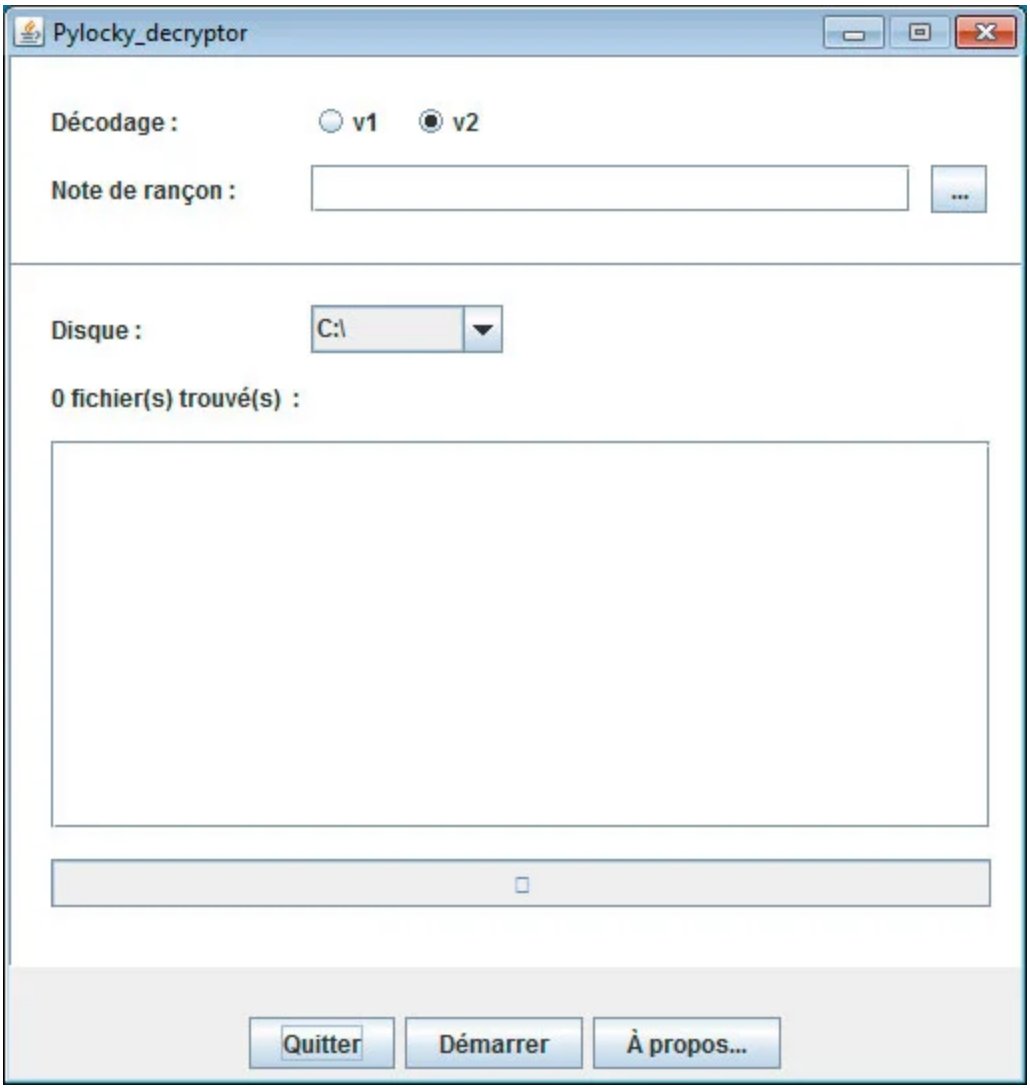
The pyLocky decryptor will decrypt files encrypted by version 1 and 2 of the ransomware. Supported encrypted file extensions for version 1 are **.lockedfile** or **.lockymap** and version 2 is **.locky**.

For those who were encrypted, you can download the pyLocky Decryptor from the following link.

pyLocky Decryptor

Download Now

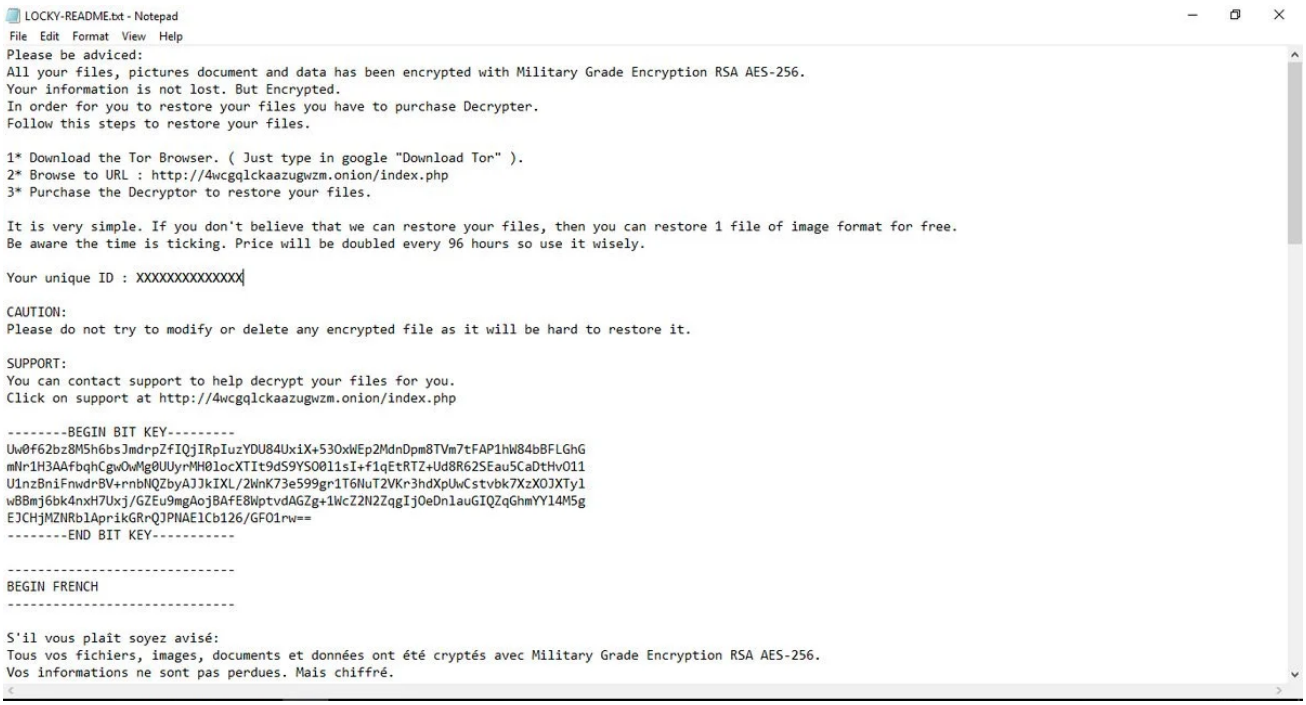
To use this decryptor, victims will need to have the Java Runtime installed. Once installed, victims can double-click on the PyLocky_Decryptor_V1_V2.jar file to launch the decryptor.



Instructions on how to use the decryptor are included in the downloaded zip file or can be read online.

Possible Command & Control server takeover

The pyLocker Ransomware utilizes Command & Control servers on the Tor network. These Tor servers are provided in the ransom notes created on a victim's computer as shown below.



pyLocky Ransom Note

Based on analysis by Michael Gillespie, the decryptor contains 2 hard coded private RSA keys.

This could mean that French law enforcement or security researchers were able to gain access to a command and control server and retrieve the master private encryption keys for versions 1 and 2 of the ransomware.

It would also indicate that this is not a flaw in the encryption algorithm used by the ransomware.

Related Articles:

Free decryptor released for Yanluowang ransomware victims

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

- Decryptor
- pyLocky
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

- 

  sunnykumar - 2 years ago

  -
  -

  my all file encrypted with FORDAN extension please help me
  No key for ID: qOYn1VNGsvBEwqldLg6QzqQVTpWLpN9U0xdyJC4n (.fordan)
  Unidentified ID: qOYn1VNGsvBEwqldLg6QzqQVTpWLpN9U0xdyJC4n (.fordan)
  MACs: 00:11:22:98:76:54, 0C:9D:92:80:F0:3E

- 

  FastCode - 2 years ago

  -
  -

  https://www.bleepingcomputer.com/forums/t/608858/id-ransomware-identify-what-ransomware-encrypted-your-files/
  https://www.bleepingcomputer.com/forums/t/671473/stop-ransomware-stop-puma-djvu-promo-drume-help-support-topic/

  Please read the moderator advice there and avoid making duplicate posts or comments in inappropriate places.
  Good luck.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: