pyLocky Decryptor Released by French Authorities

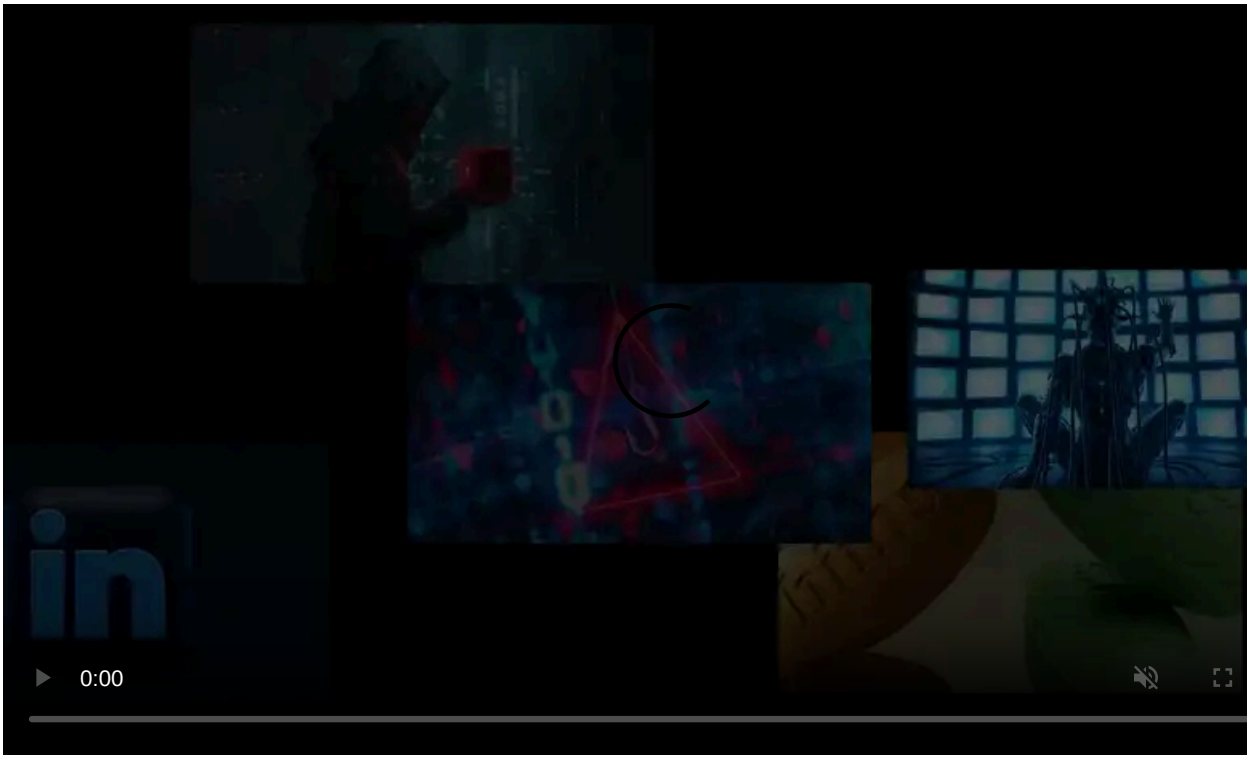
By Lawrence Abrams

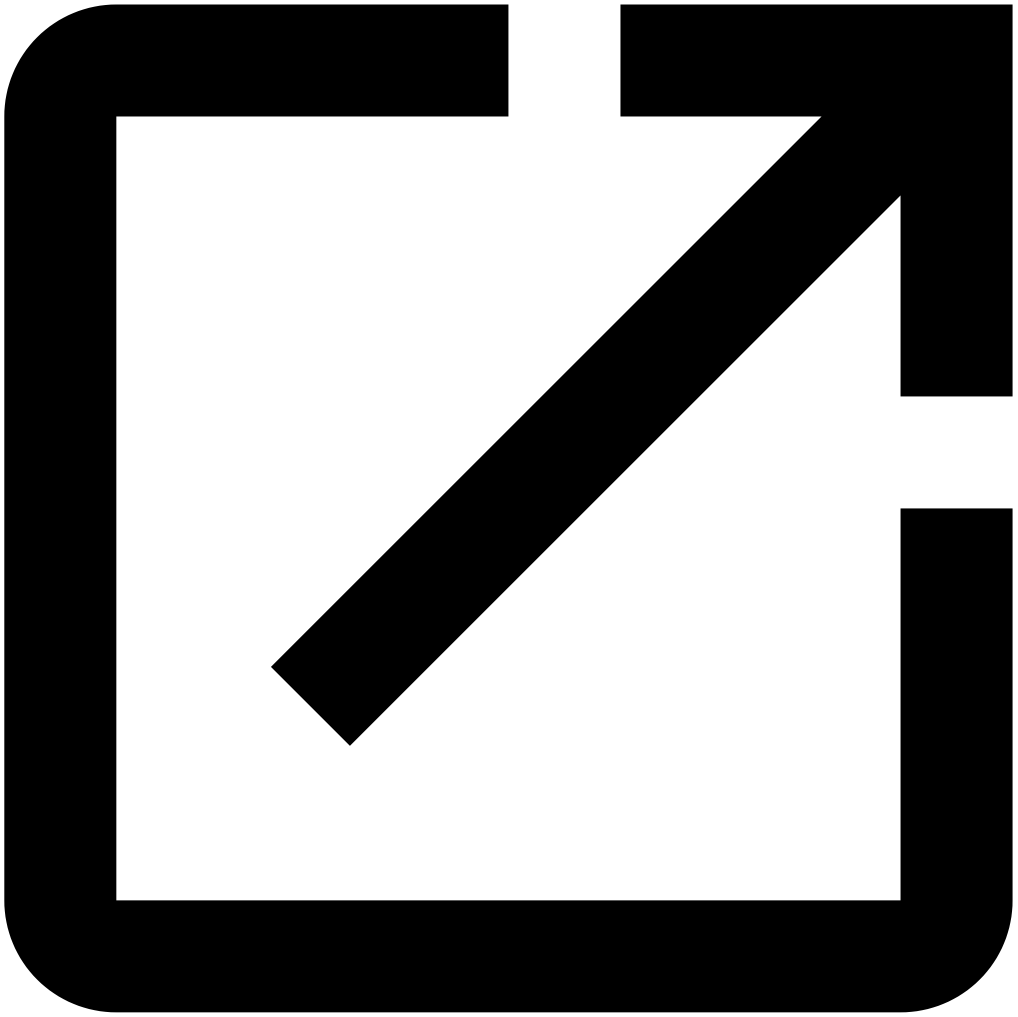
Published: 2019-06-13 · Archived: 2026-04-05 18:15:15 UTC

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."


0:00



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

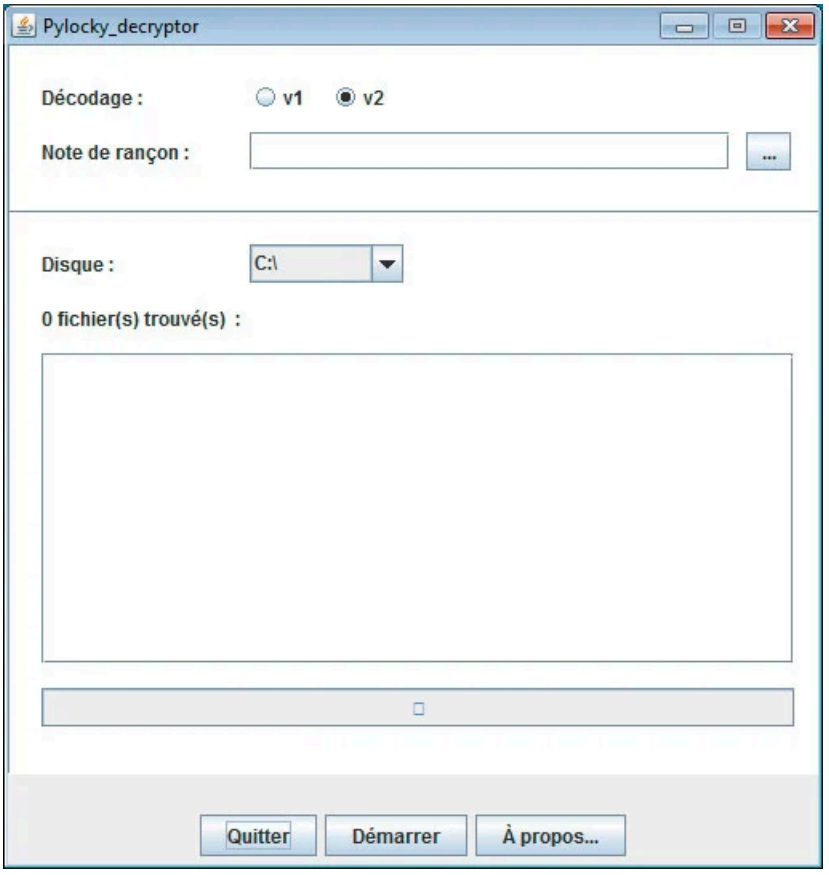
"PyLocky is very active in Europe and there are already many victims in France, both within the professional environment (SMEs, large businesses, associations, etc.) as well as at home."

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.

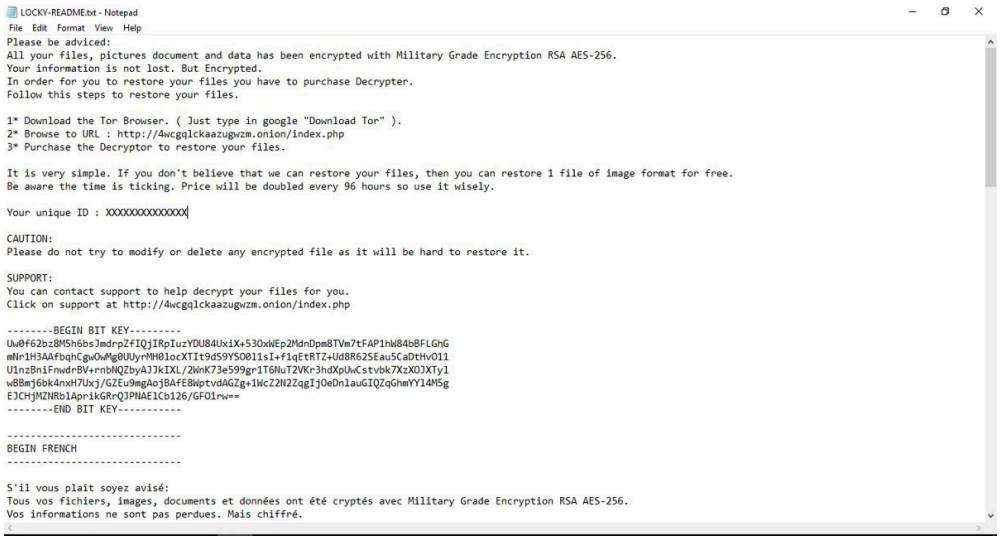
To use this decryptor, victims will need to have the Java Runtime installed. Once installed, victims can double-click on the PyLocky_Decryptor_V1_V2.jar file to launch the decryptor.



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.
