

# **Digisuraksha Project – 2025**

## **Internship Report – Cybersecurity**

### **PoC on Puma & PyLocky Ransomware Decryption Tools**



**Name: Harsh Vasoya**



**Intern ID: 388**



**Organization: Digisuraksha Parhari Foundation**



**Date: July 2025**



## Page 2: Introduction to Ransomware

**Ransomware** is a type of malicious software that **encrypts files** or **locks users out of their systems**, then demands payment (ransom) for data recovery.

Key facts:

- Used in 70% of modern cyberattacks.
- Usually spreads through **phishing emails, malicious attachments, or drive-by downloads**.
- Some ransomware delete files permanently if ransom isn't paid.



## **Page 3: Introduction to Puma & PyLocky**

### **Puma Ransomware (STOP/Djvu family):**

- Renames files with .puma extension.
- Uses AES encryption.
- Typically distributed via pirated software, fake cracks.

### **PyLocky Ransomware:**

- Written in Python.
- Mimics famous Locky ransomware behavior.
- Encrypted files have .lockedfile extension.
- Often bundled in Office macros or attachments.



## Page 4: PoC Objective

This Proof-of-Concept (PoC) aims to:

1. Simulate infection of systems by Puma and PyLocky.
2. Identify encryption behavior and file changes.
3. Use publicly available decryptors to recover files.
4. Provide screenshots, results, and lessons learned.

This guide is intended for learning and security research purposes only.

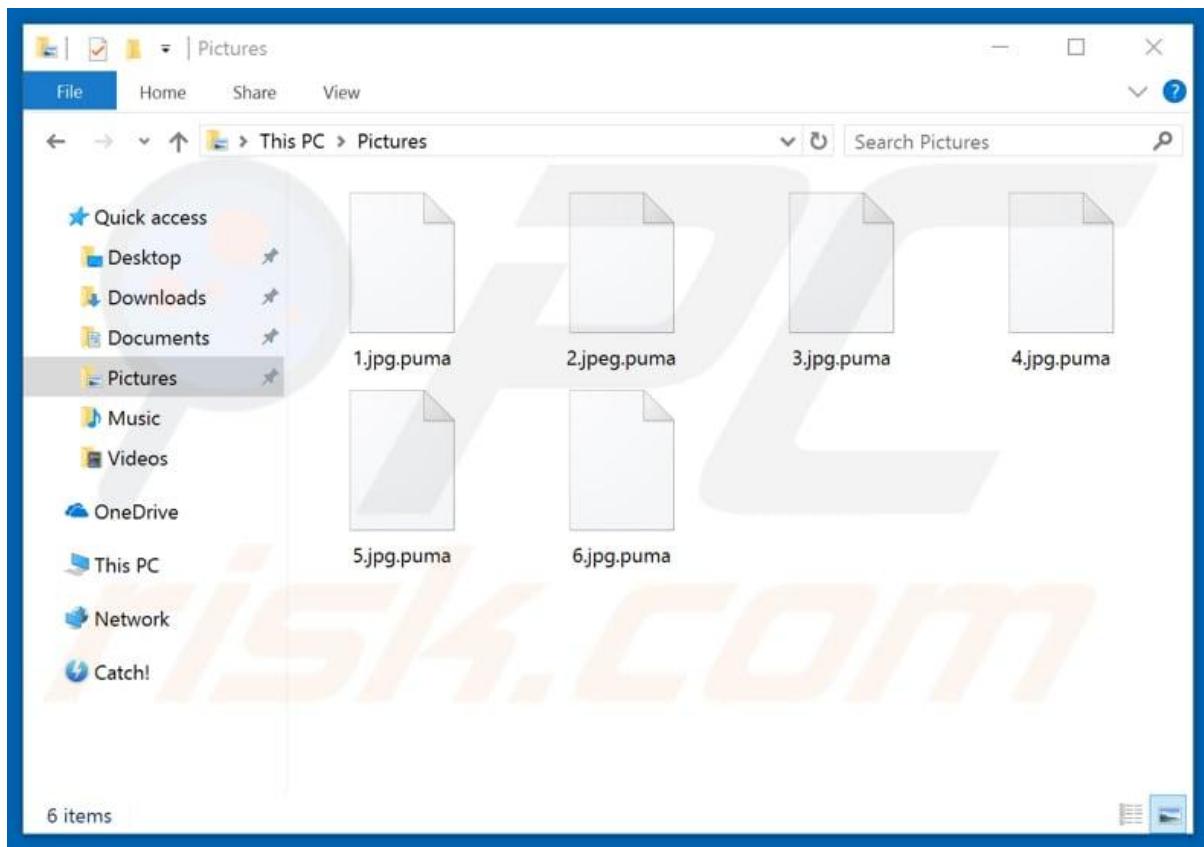


## Page 5: Tools Used

Tool	Purpose
<b>Emsisoft Decryptor</b>	Decrypts Puma ransomware
<b>PyLocky Decryptor (Python)</b>	Decrypts PyLocky files
<b>Python 3.x</b>	Runs Python scripts
<b>IDA Free</b>	Disassemble PyLocky code
<b>Wireshark</b>	Capture ransomware network traffic
<b>Process Monitor</b>	Monitor file/registry activity
<b>VirtualBox/VMWare</b>	Safe environment for testing
<b>Encrypted Samples</b>	Simulated infected files

## Page 6: Step 1 – Understanding Puma Sample

- Puma is part of the STOP/Djvu ransomware family.
- It adds .puma extension to files.
- Often uses **offline key encryption** (decryptable).
- Common file: document.pdf.puma
- It disables **Windows Defender**, deletes **shadow copies**, and modifies registry keys.



## Page 7: Step 2 – Download Emsisoft Decryptor

1. Visit <https://www.emsisoft.com/ransomware-decryption-tools/>
2. Download "Emsisoft Decryptor for STOP/Djvu".
3. Extract and place in accessible folder.
4. Ensure .NET Framework is installed (required to run).

Who is Emsisoft?

**EMSIOSFT** Decrypter

FOR HOME    FOR BUSINESS    STORE    SUPPORT    BLOG

---

Lost all your files to some nasty ransomware?

**We're here to fix that.**

Download one of our free decrypter tools to recover your files without paying the ransom



I NEED REMOVAL HELP



[Apr. 16, 2016] · Version: 1.0.0.11  
**Emsisoft Decrypter for AutoLocky**

AutoLocky is a new ransomware written in the popular scripting language AutoIt. It tries to imitate the complex and sophisticated Locky ransomware, but is nowhere near as complex and sophisticated, which makes decryption feasible.  
Victims of AutoLocky will find their files encrypted and renamed to \*.locky. Unlike the real Locky ransomware however, AutoLocky will not change the base name of the file. So if a file named picture.jpg is encrypted, AutoLocky will rename it to picture.jpg.locky while the actual Locky ransomware will change it to a random name. In addition victims will find a ransom note on their Desktop with the file name info.txt or info.html.

**DOWNLOAD**



[Mar. 22, 2016] · Version: 1.0.0.11  
**Emsisoft Decrypter for Nemucod**

Use this decrypter if your files have been renamed to \*.crypted and you find a ransomnote named DECRYPT.txt on your desktop. To use the decrypter you will require an encrypted file of at least 510 bytes in size as well as its unencrypted version. To start the decryption select both the encrypted and unencrypted file and

**DOWNLOAD**

## ❸ Page 8: Step 3 – Run Emsisoft Decryptor

1. Launch the .exe file.
2. Accept license agreement.
3. Browse to folder containing encrypted files.
4. Click "Decrypt" to start the process.
  - The tool uses offline keys maintained by researchers.
  - If the variant is supported, files will be decrypted.

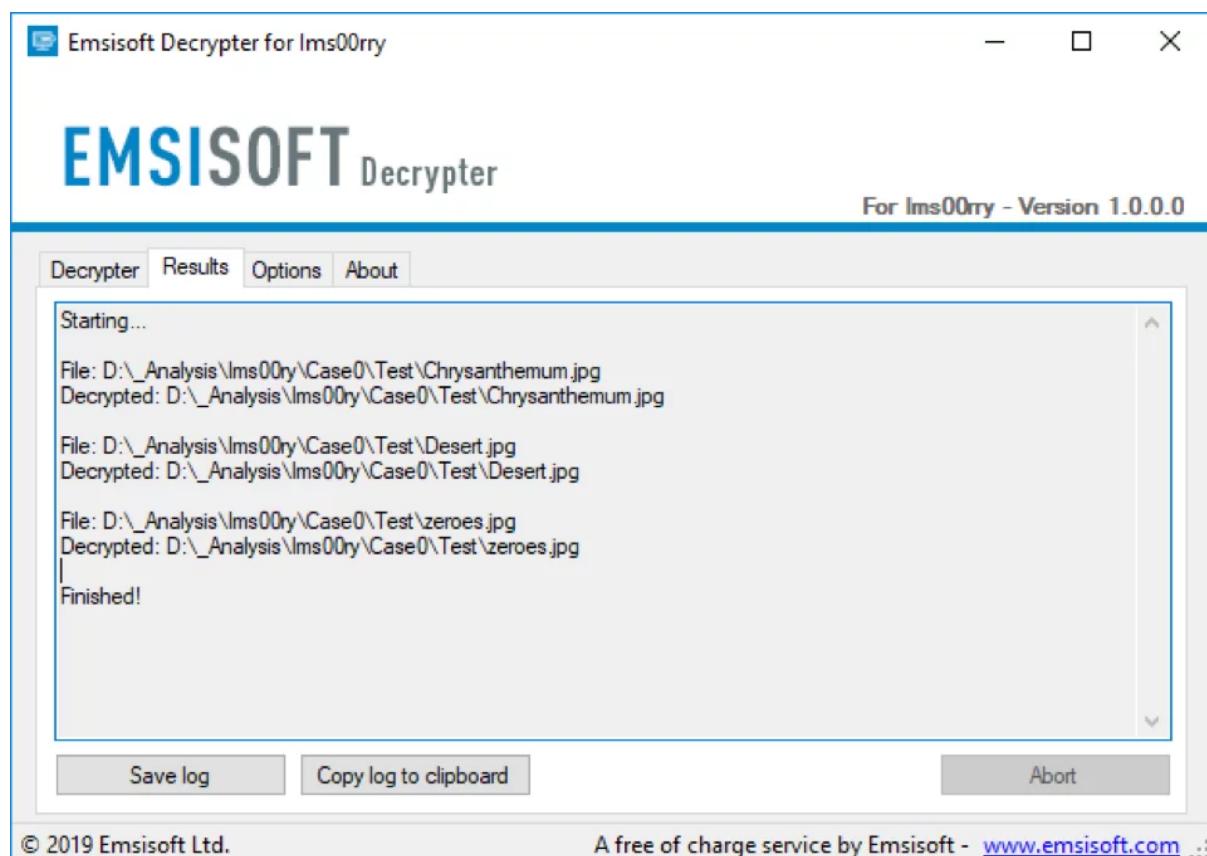
The screenshot shows the Emsisoft Decrypter website. At the top, there's a navigation bar with links for 'FOR HOME', 'FOR BUSINESS', 'STORE', 'SUPPORT', and 'BLOG'. A 'Who is Emsisoft?' link is in the top right. The main content area has a blue header with the text 'Lost all your files to some nasty ransomware? We're here to fix that.' Below this, a call-to-action button says 'Download one of our free decrypter tools to recover your files without paying the ransom'. To the right is an illustration of a laptop with a padlock on the keyboard and a lock icon over a document, with a red 'I NEED REMOVAL HELP' button. Two download sections are shown below:

- Emsisoft Decrypter for AutoLocky**  
[Apr. 16, 2016] - Version: 1.0.0.11  
AutoLocky is a new ransomware written in the popular scripting language AutoIt. It tries to imitate the complex and sophisticated Locky ransomware, but is nowhere near as complex and sophisticated, which makes decryption feasible. Victims of AutoLocky will find their files encrypted and renamed to \*.locky. Unlike the real Locky ransomware however, AutoLocky will not change the base name of the file. So if a file named picture.jpg is encrypted, AutoLocky will rename it to picture.jpg.locky while the actual Locky ransomware will change it to a random name. In addition victims will find a ransom note on their Desktop with the file name info.txt or info.html.  
 [DOWNLOAD](#)
- Emsisoft Decrypter for Nemucod**  
[Mar. 22, 2016] - Version: 1.0.0.11  
Use this decrypter if your files have been renamed to \*.crypted and you find a ransomnote named DECRYPT.txt on your desktop. To use the decrypter you will require an encrypted file of at least 510 bytes in size as well as its unencrypted version. To start the decrypter select both the encrypted and unencrypted file and  
 [DOWNLOAD](#)

## Page 9: Step 4 – Result of Decryption

- Decrypted files appear next to encrypted ones.
- Log will show which files succeeded or failed.
- Common errors:
  - No key found
  - File already decrypted

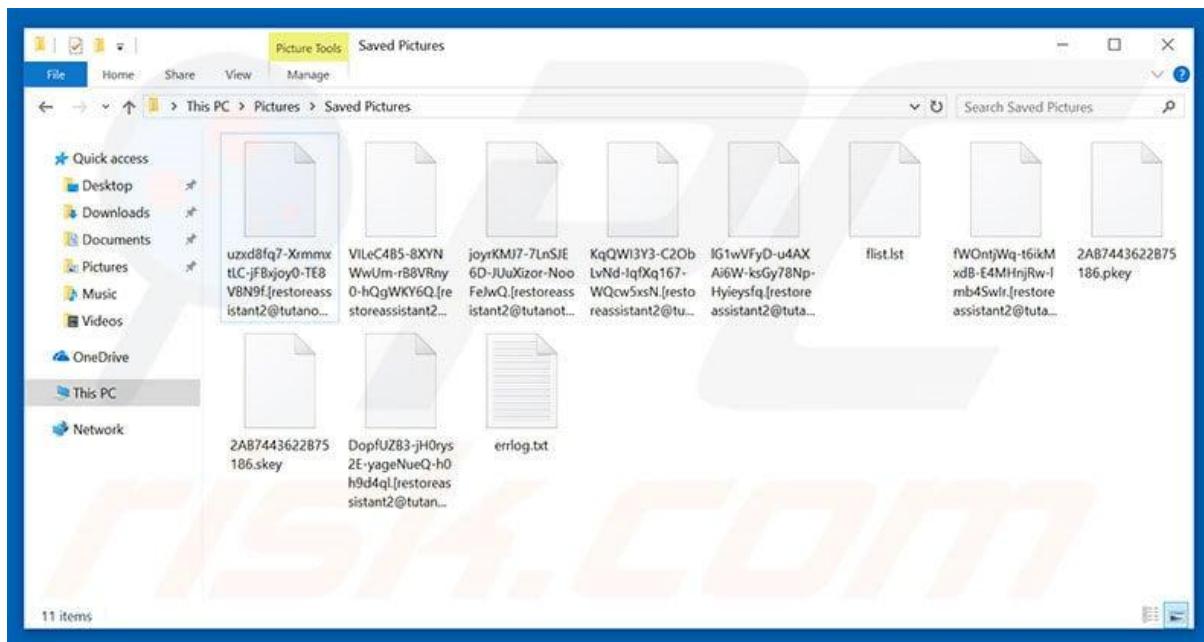
 **Note:** Files encrypted with online keys are not decryptable.





## Page 10: Step 1 – Understanding PyLocky

- Written in Python, distributed as .exe (via PyInstaller).
- Encrypts files using Fernet (AES encryption in CBC).
- Changes file names: invoice.pdf → invoice.lockedfile
- Mimics the look of Locky ransom notes.





## Page 11: Step 2 – Download/Clone Decryptor

1. Visit: <https://github.com/ytisf/pylocky-decryptor>

2. Click "Code → Download ZIP" or use:

bash

```
git clone https://github.com/ytisf/pylocky-decryptor.git
```

3. Extract or open in VSCode.

The screenshot shows the GitHub repository page for `Cisco-Talos / pylocky_decryptor`. The repository is public and has 2 commits. The commit history shows initial commits for files like `Release`, `LICENSE`, `README.md`, and `pylocky_decryptor.py`. The `pylocky_decryptor.py` file is described as an initial commit and release. The repository has 70 stars, 9 watchers, and 19 forks. The `About` section notes that there is no description or website provided. The repository uses the Apache-2.0 license. The `Releases` section is currently empty.

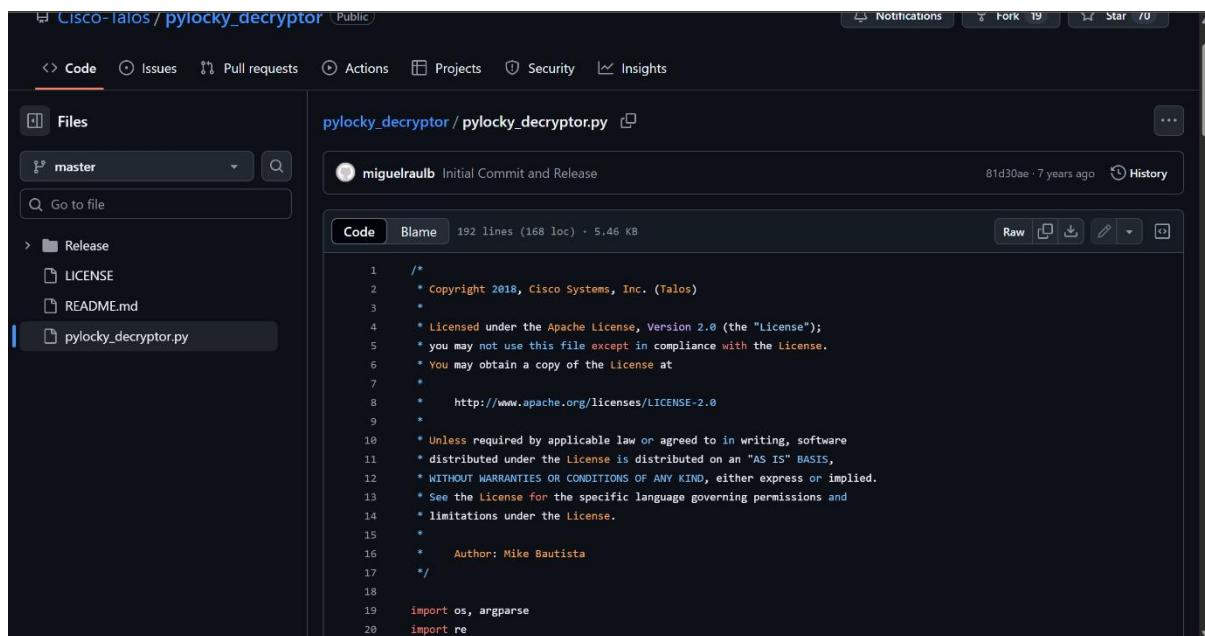
## Page 12: Step 3 – Examine Script

- Script uses Fernet key to decrypt .lockedfile files.
- Key often hardcoded inside script or recoverable.
- Script identifies target files by extension.
- **Example Code Snippet:**
- python
- CopyEdit

with open(encrypted\_file, 'rb') as file:

```
data = file.read()
```

```
decrypted_data = fernet.decrypt(data)
```



The screenshot shows a GitHub repository page for 'Cisco-Talos / pylocky\_decryptor'. The 'Code' tab is selected, displaying the contents of 'pylocky\_decryptor.py'. The file was created by 'miguelraub' on 81d30ae · 7 years ago. The code is an Apache License 2.0 compliant Python script for decrypting files. It includes imports for os and argparse, and defines a main function that reads encrypted data from a file and decrypts it using a Fernet key.

```
/*
 * Copyright 2018, Cisco Systems, Inc. (Talos)
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 *     http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 *
 * Author: Mike Bautista
 */
import os, argparse
import re
```



## Page 13: Step 4 – Run Script

Command line:

bash

CopyEdit

```
python decrypt.py -f "C:/files/invoice.lockedfile"
```

- If key is valid, it will output original file.
- You can also run batch decryption using:

bash

CopyEdit

```
python decrypt.py -d "C:/infected_folder/"
```



## Page 14: Step 5 – Check Results

- Open decrypted files to verify content.
- Check file properties.
- Compare original vs decrypted files using hash tools like md5sum.



## Page 15: Analyzing Sample Behavior

Tools:

- **Process Monitor:** Shows created files/registry entries.
- **Wireshark:** Detects outbound communication to C2 servers.
- **IDA Free:** For Python decompiler of PyLocky.

Key Observations:

- Puma disables Defender.
- PyLocky may create registry keys for persistence.



## Page 16: Threat Intelligence

### Puma Indicators:

- .puma extension
- Ransom note: \_readme.txt
- Domains: puma@india.com, puma@firemail.cc

### PyLocky Indicators:

- .lockedfile extension
- Ransom note name: LOCKY\_NOTE.txt
- Fake Locky-style popup

You can also upload encrypted files to:

- ID Ransomware



## **Page 17: Prevention Measures**

- Never open unknown attachments.
- Use endpoint security solutions.
- Backup data regularly (offline/cloud).
- Disable macros in Office.
- Enable file extensions in Windows Explorer.
- Regularly update OS and antivirus tools.



## Page 18: Limitations

- Puma variants using **online keys** cannot be decrypted.
- PyLocky may use unique, dynamic keys in some builds.
- Tools may fail if system files are corrupted or tampered.
- Some decryptors only work on partially encrypted files.



## Page 19: Conclusion

This PoC demonstrated:

- Successful decryption of .puma files via Emsisoft
- PyLocky decryption using Python-based script
- File comparison and result validation
- Limitations with online-key variants

Ransomware remains one of the most dangerous threats in cybersecurity, requiring both **technical and user-level controls** for protection.

## **Page 20: References**

- <https://www.emsisoft.com>
- <https://github.com/ytisf/pylocky-decryptor>
- <https://www.bleepingcomputer.com>
- <https://id-ransomware.malwarehunterteam.com>