


ZLab - LooCipher Decryption Tool

 github.com/ZLab-Cybaze-Yoroi/LooCipher_Decryption_Tool

CERT-Yoroi-Malware-ZLab

CERT-Yoroi-Malware-ZLab /...

Decryption tool for LooCipher Ransomware



2

Contributors



0

Issues



8

Stars



4

Forks



This tool does not work if you restart your computer after the infection

Decryption tool for the LooCipher Ransomware

1. Find the Process ID (PID) of the LooCipher ransomware
2. Open `cmd` (the tool does not require elevated (Administrator) privileges)
3. Move to the path where this tool was downloaded
4. In the `cmd` prompt, type `ZLAB_LooCipher_Decryptor.exe <PID>`

Disclaimer

Due to the continuing LooCipher infection campaign, we proceeded to release the decryptor in the shortest possible time in order to help the victims infected in the previous phase. So, the tool is a Beta release and it is still composed by an unsigned executable. We will provide to release some updates as soon as possible.

Thanks to Fortinet for their [analysis](#) about LooCipher obfuscation flaw. The tool embeds parts of Fortinet script.

New release!

The latest release and source code is available at: <https://www.yoroi.company/download.html>