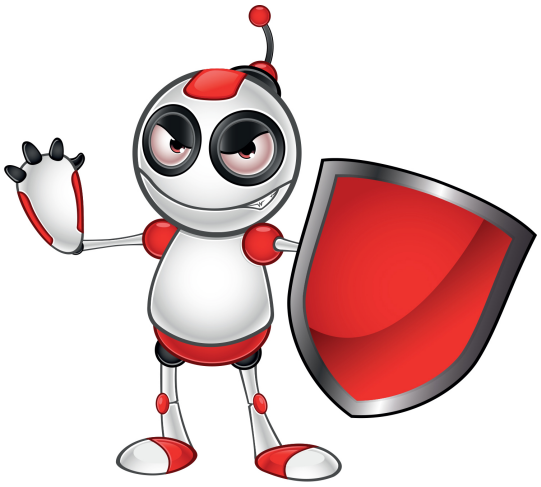


NO MORE RANSOM!

Incident response guidelines

- **Category:** Protect one's self and others

- **Activity Description:**
  Attempt to recover your files after falling victim of ransomware

- **Aims (What are you going to learn?):**

  At the end of this lesson you will be able to:

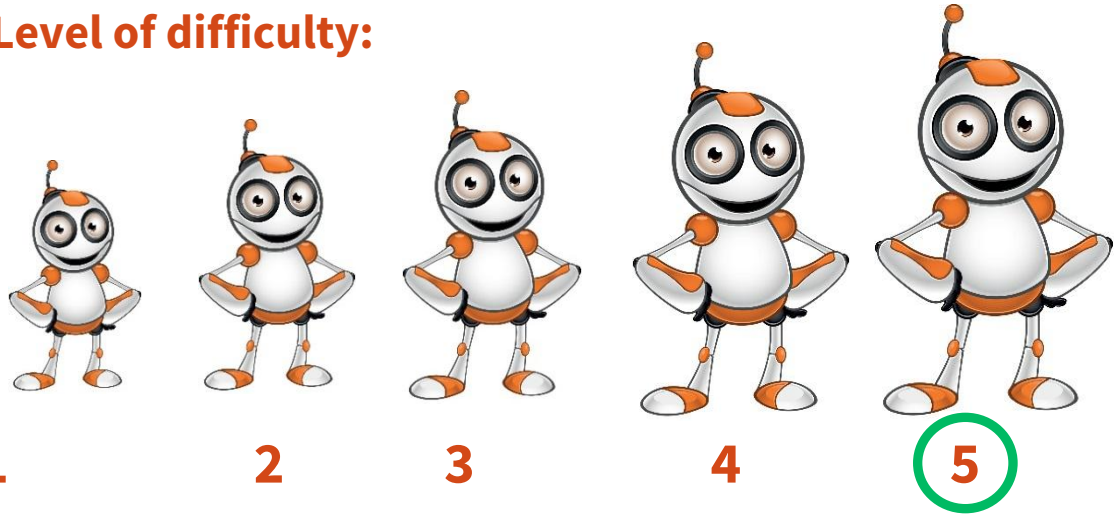
  - Identify encrypted (locked) files,
  - Use the nomoreransom service

- **What are you going to need?**

  Software:

  - Web browser

- **Audience/target group:** Adults
- **Time needed:** 5 minutes + time for decryption
- **Level of difficulty:**

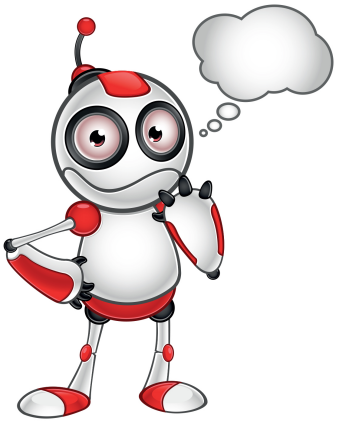


- **Before we start we need to ensure that the user has:**
  - good skills of web navigation,
  - confidence in navigating through their files and folders
  - ability to conduct google searches and follow step by step instructions of removing ransomware

- **Related antivirus platforms:**
  - Virustotal.com

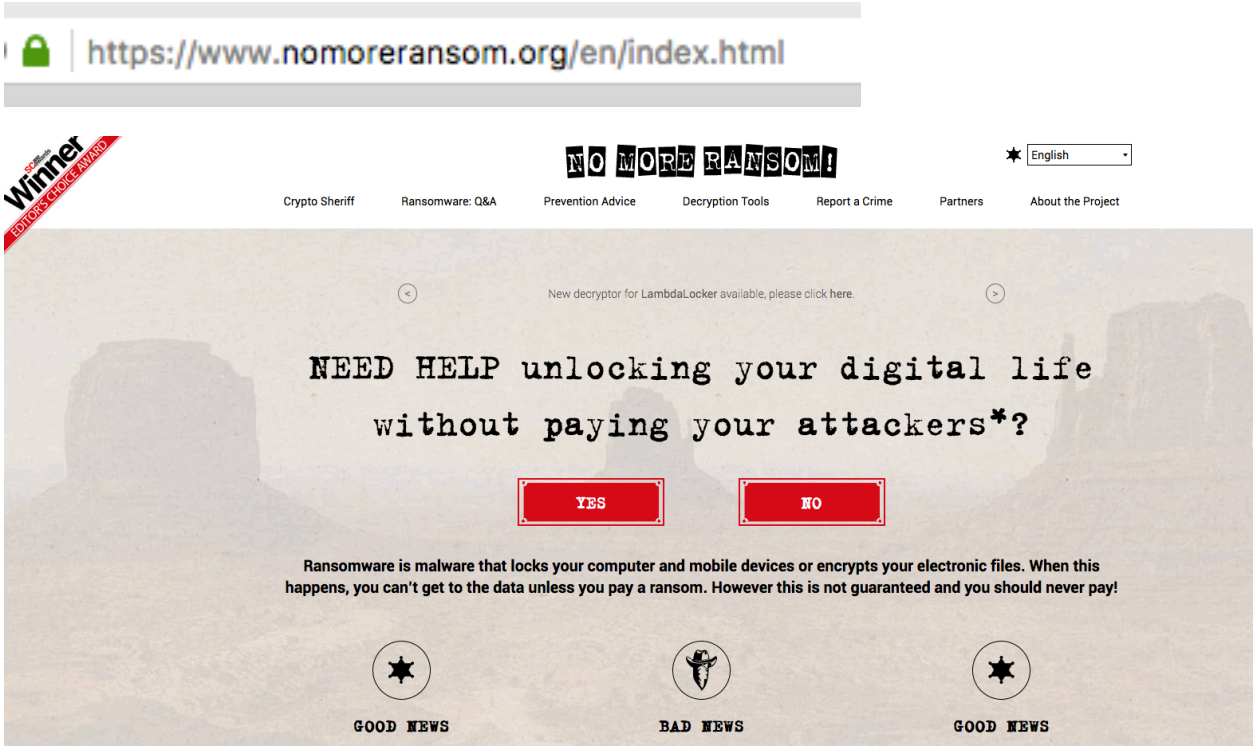
○ STEPS TO ATTEMPT FILE RECOVERY FROM RANSOMWARE

If your computer is infected, your screen will look something like this:

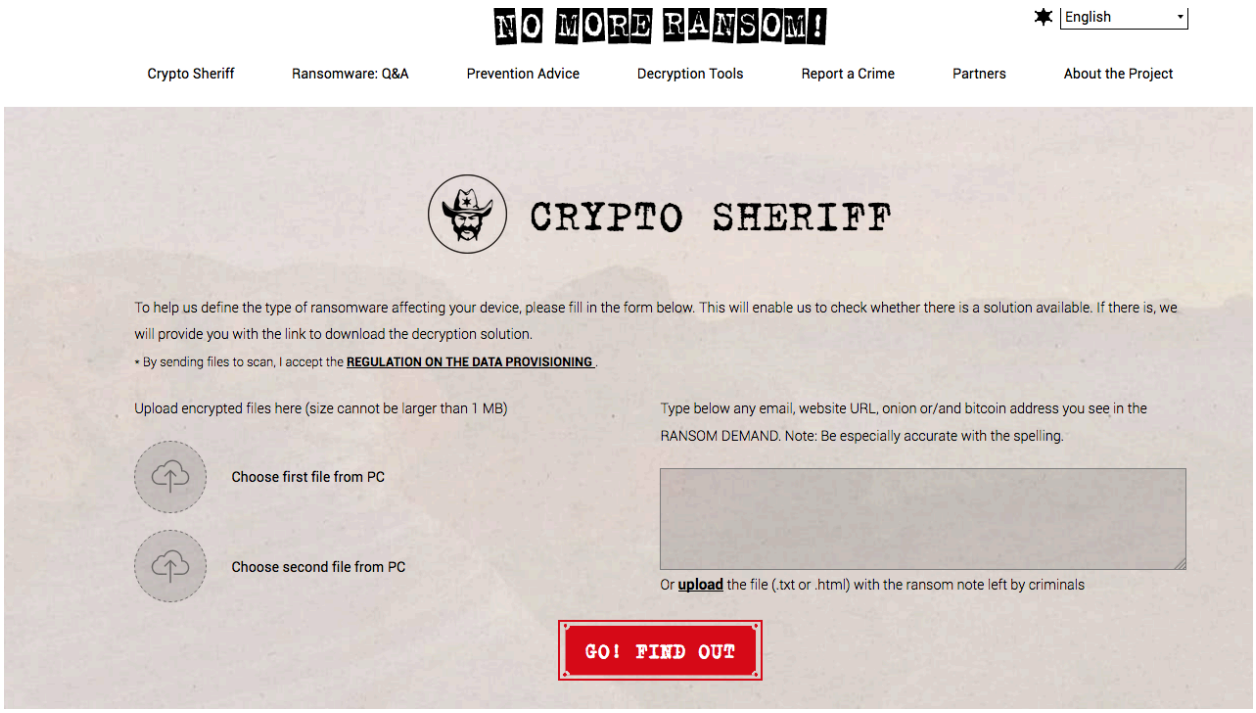


1. Ideally you need to remove the ransomware from the computer. This can be a complex task depending on the type of ransomware. If you are unsure about this, you should seek expert's assistance. If you wish to proceed you should copy **only** your encrypted files to a clean disk.

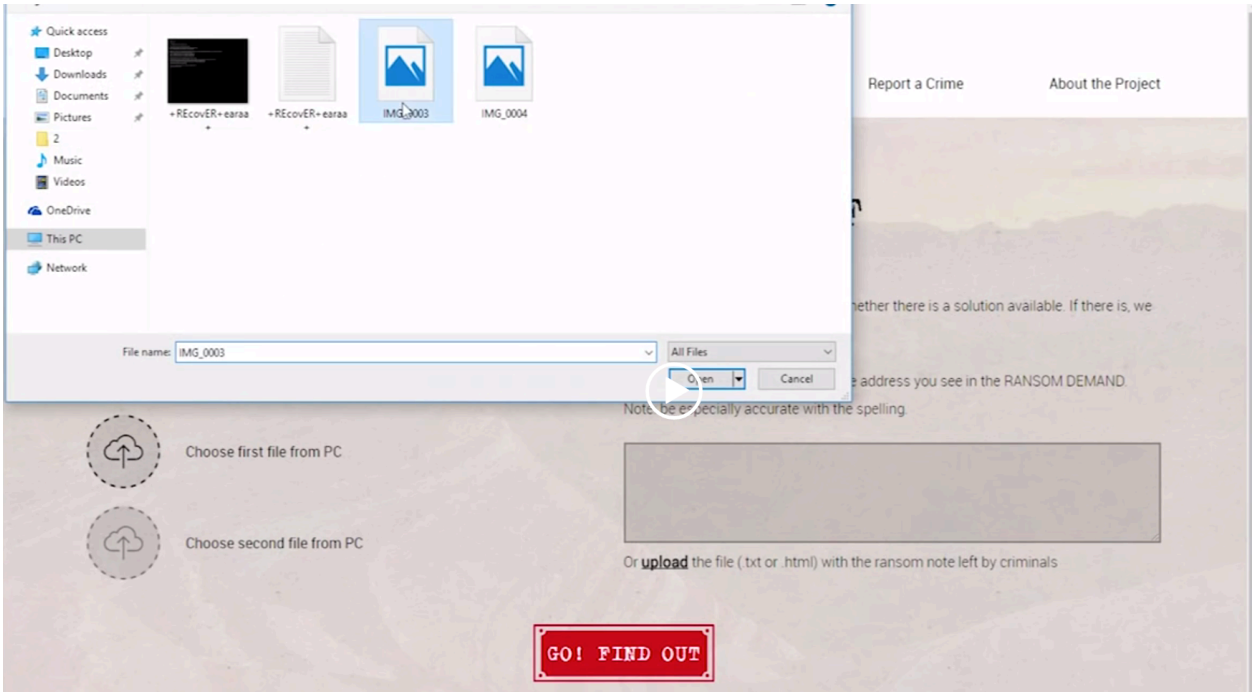
2. Open a web browser, e.g. Google Chrome and type the web address (link) nomoreransom.org to go to the site website, as shown in the image below.



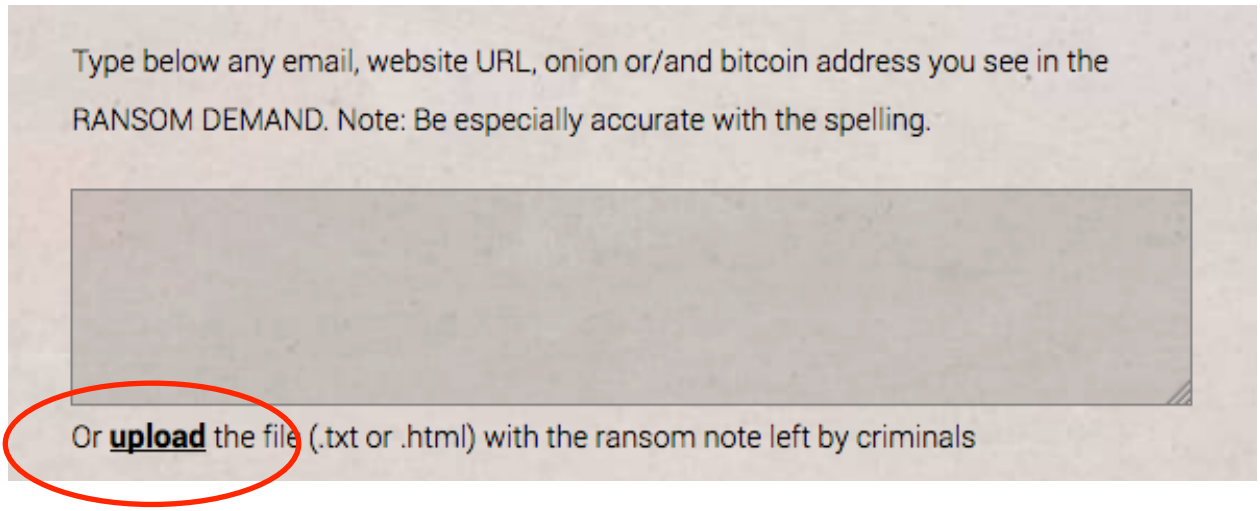
3. Click at the **Crypto Sheriff** tab, located at the top left of the page. The following page will appear:



4. Click on “Chose first file from PC” and select any encrypted file. This can be a picture (jpeg) or an MS document (doc, docx, xlsx, etc.). Do the same with a second file, by clicking on “Chose second file from PC”

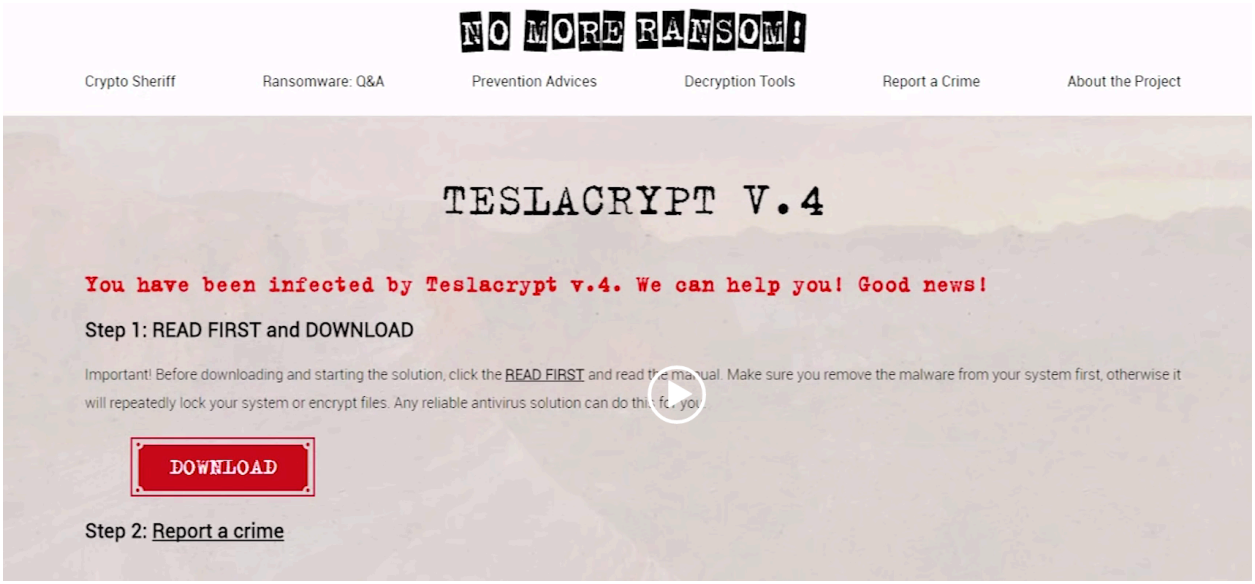


5. If possible, find a file with the description of the ransomware demand – this is not necessary:



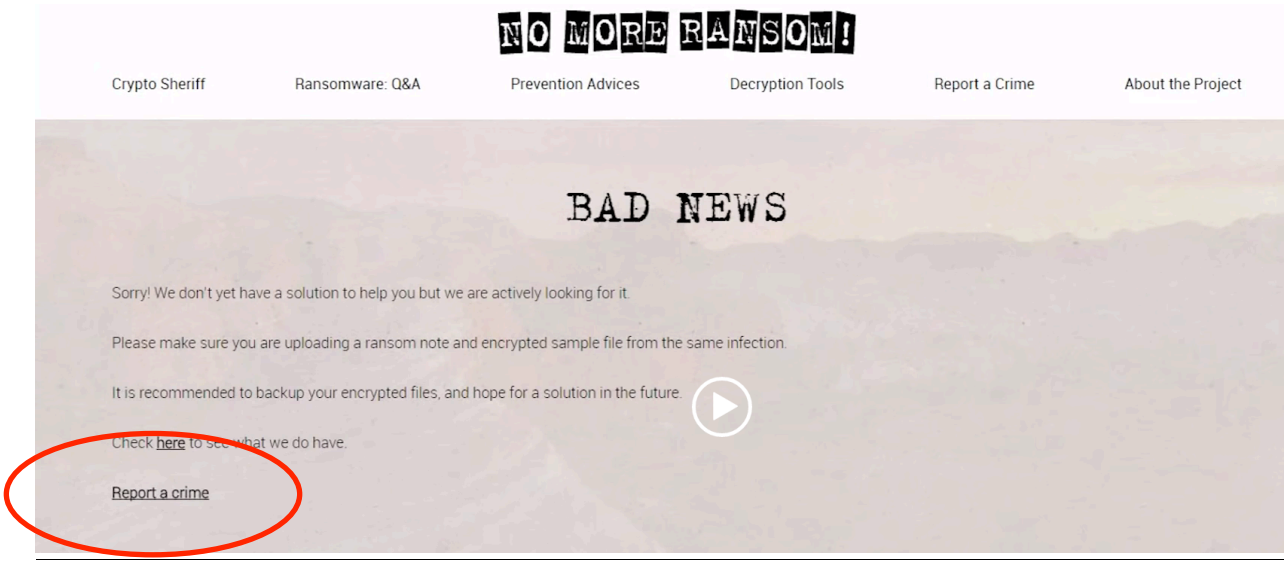
6. Click on 

7. if there is a decryptor available, you will get a screen like this:



8. Click on “Download” and follow the instructions of the respective descriptor.

9. If there is no descriptor available, you will get a screen like this. In this case you should click on “Report a crime”



Aims	Yes	No		
Do I regularly backup my files on a different PC/ storage medium?				
Do I know what process to follow in order to remove ransomware?				
Can I use confidently the nomoreransom service?				

Lesson Assessment