Computest Security

DoNex Ransomware Decryptor Usage Manual

April 5th, 2024

Table of contents >>

01. Introduction >>

Computest Security's Research Division, Sector 7, is a team that was established to give back to society by improving the state of security through their work, either by finding and reporting vulnerabilities in commonly used software or through public service projects. In the course of their work, Team High Tech Crime (THTC) of the Dutch Police reached out to Sector 7 in March of 2024 to help develop a decryptor for the DoNex/DarkRace ransomware family after THTC had identified a cryptographic vulnerability in the ransomware's encryption process.

The decryptor associated with this manual is the result of this collaboration effort, which is publicly provided in partnership with the NoMoreRansom initiative lead by Europol and the Dutch Police.

You can find out more information about Computest Security at the end of this manual.

02. Before using the decryptor >>

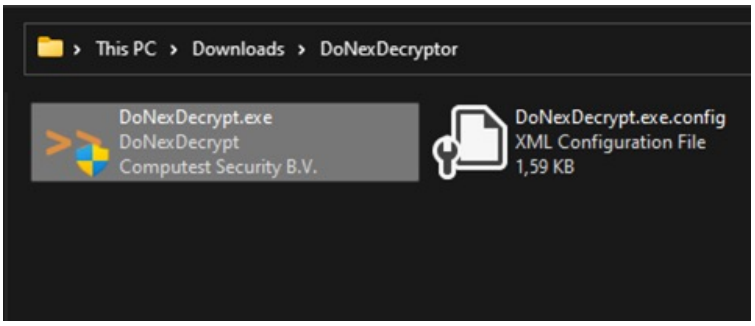
Please make sure to remove the malware from your system first to avoid any further re-encryption of your files. Any reliable antivirus or antimalware solution can do this for you. You may also extract the encrypted files from the infected computer and use the decryptor from a clean, uninfected computer.
This decryptor requires you to provide it with a file sample consisting of an encrypted file and the original version of the same file before it was encrypted by the malware. Please ensure that you can provide files that satisfy this criterion and do not rename the encrypted nor the original file, the decryptor will use the file names to identify the extension that was added by the ransomware to your encrypted files. More information about the file sample selection process is provided in the how-to section of this manual.

In case there are files that were encrypted by the malware remotely on network-attached systems that were accessible to the infected device at the time of infection, please consult the advanced options section in this manual.

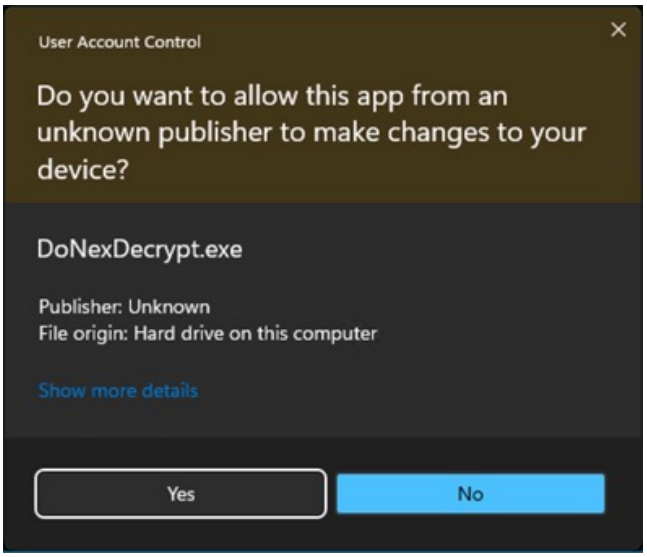
03. How to use decryptor >>

1 Download the decryptor from the DoNexDecryptor.zip file from the same website that provided this manual.

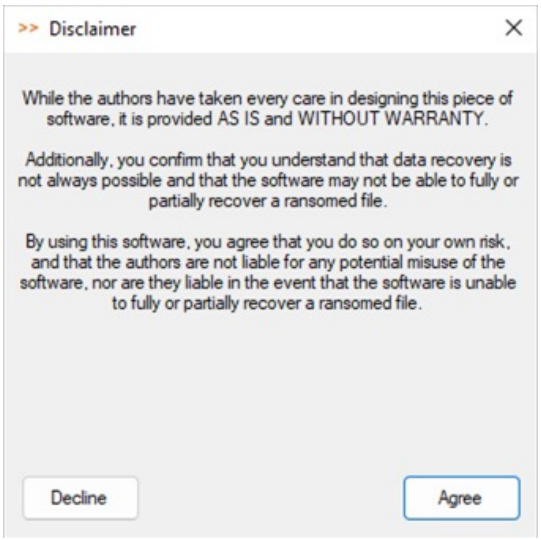
2 Extract the downloaded file, you should find the decryptor program DoNexDecrypt.exe in the extracted files list:



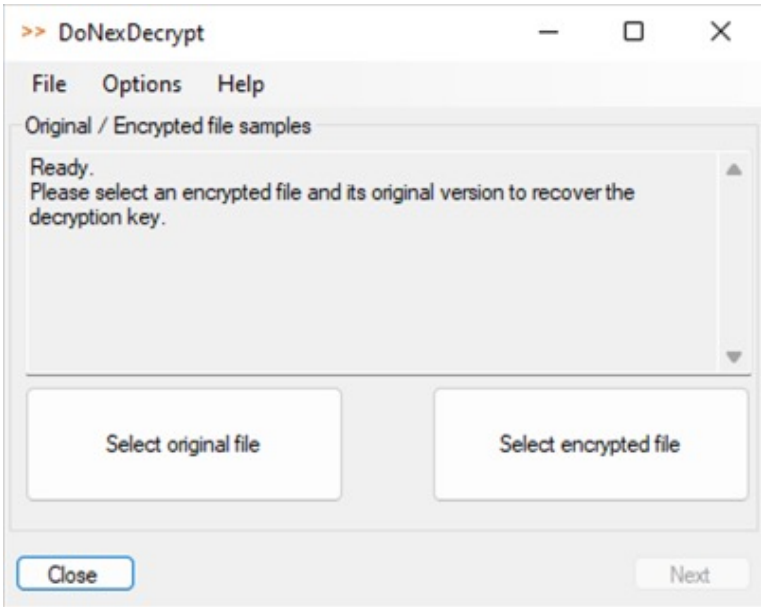
3 Once double-clicked, the decryptor will request permission to run as an administrator user. This is necessary to make sure that the decryptor can decrypt as many files as possible. Allow the decryptor to run by accepting the UAC prompt:



4 Read the disclaimer and click on “Agree” to continue:



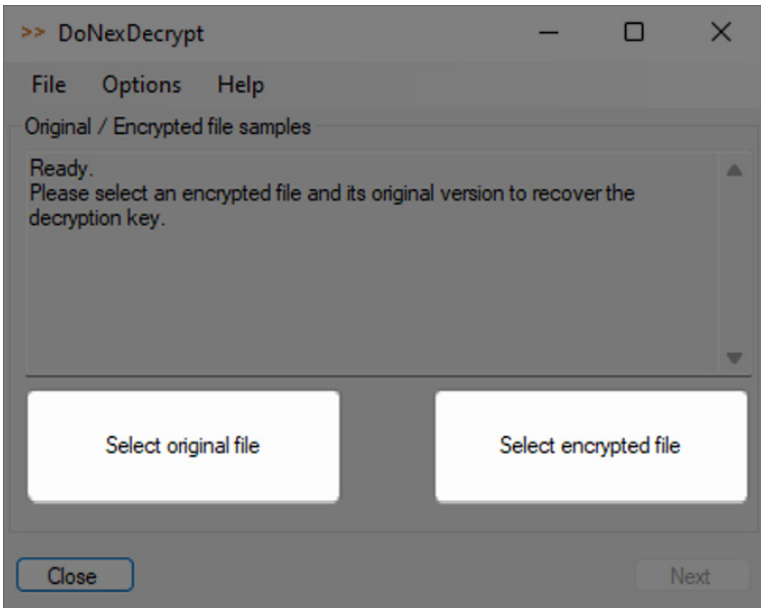
5 Once you agree to the disclaimer, the decryptor’s main screen will appear:



6 On the first screen, you are given the option to select a file sample for key recovery. This file sample consists of a file that was encrypted by the malware and the original version of the same file prior to encryption. Make sure that you have at least one such sample at hand. You may use any available files that satisfy these conditions, but it is recommended to use a sample where the original unencrypted version is at least 1MB in size. By doing so, the decryptor can decrypt all the files that were encrypted by the malware using the same key as the sample files. Otherwise, the decryptor will not be able to decrypt files that are larger in size than the original unencrypted file in the given sample.

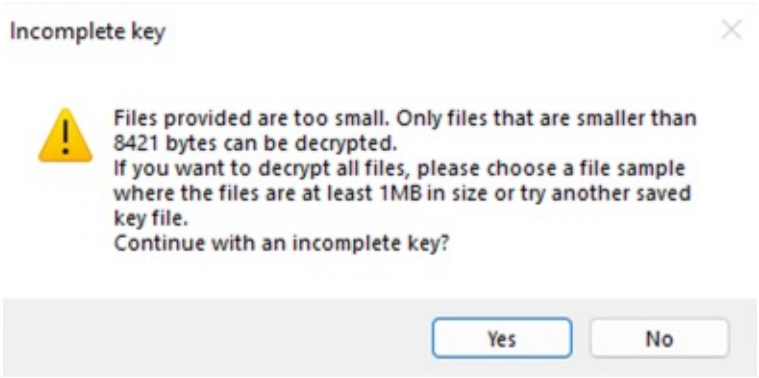
7

Select the original unencrypted file by clicking on “Select original file” button and picking the right file from the file selection screen. Do the same for the encrypted file by clicking on the “Select encrypted file” button:



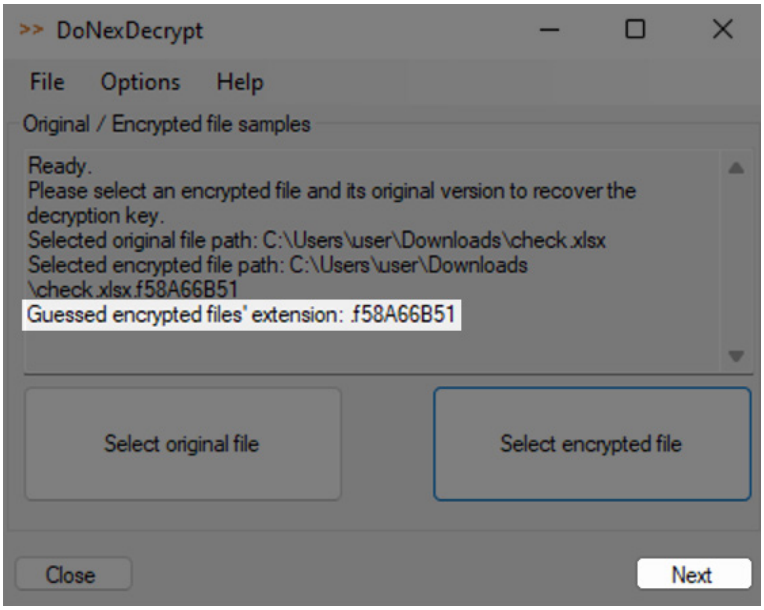
8

If the selected file samples will produce a key that is not sufficient to decrypt all files, the decryptor will prompt you with the maximum size in bytes of files that it can decrypt. You may click “Yes” to continue with the incomplete key, or otherwise pick a sample where the original file version is at least 1MB in size:



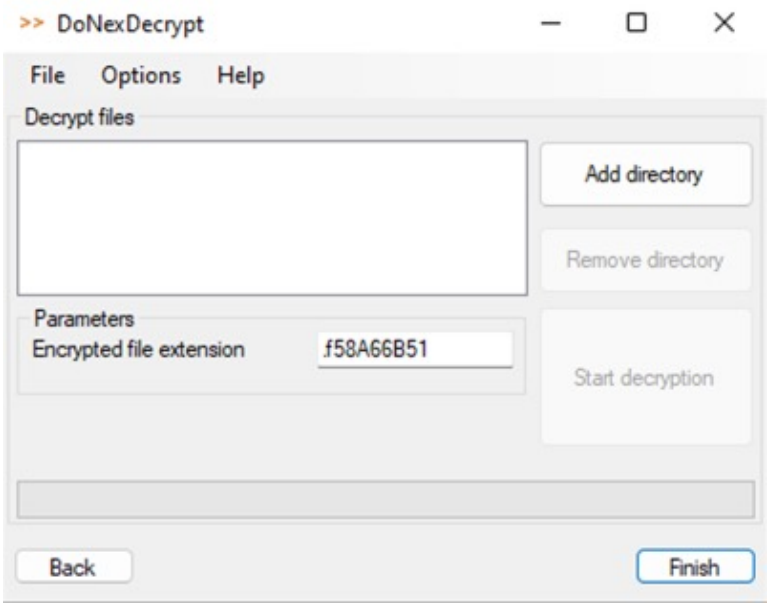
9

Once the key has been recovered, the decryptor will guess the encrypted files' extension and the "Next" key will be available to continue to the decryption screen:



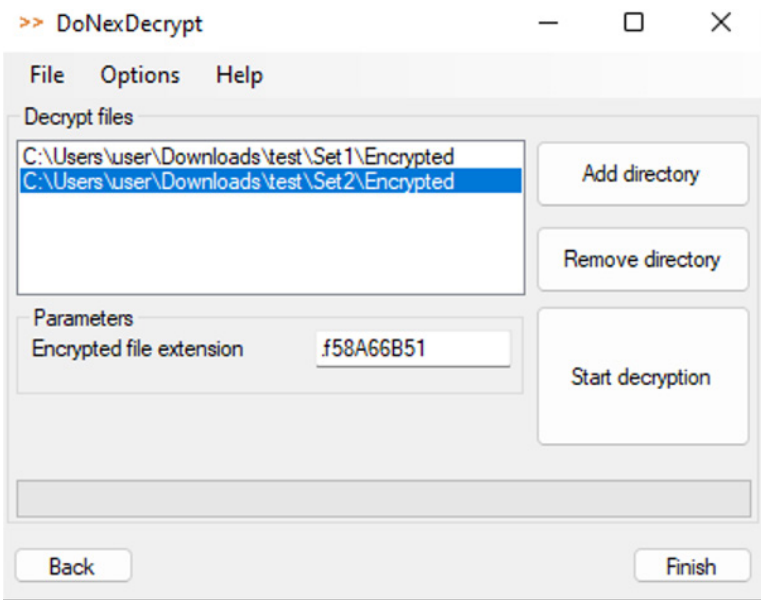
10

After pressing next, the decryption screen is shown:



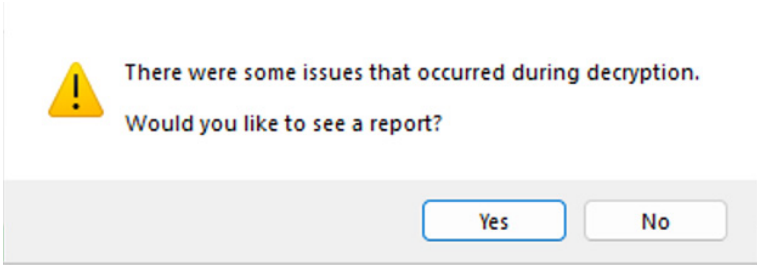
11

On the decryption screen, you can change the encrypted file extension in case it does not match the encrypted files in your directories. Press “Add directory” to add a directory to the directories that the decryptor will scan for encrypted files and “Remove directory” to remove a highlighted entry in the directory list. Once there is at least one directory in the scan list, the “Start decryption” button will be enabled and can be pressed to start decryption:

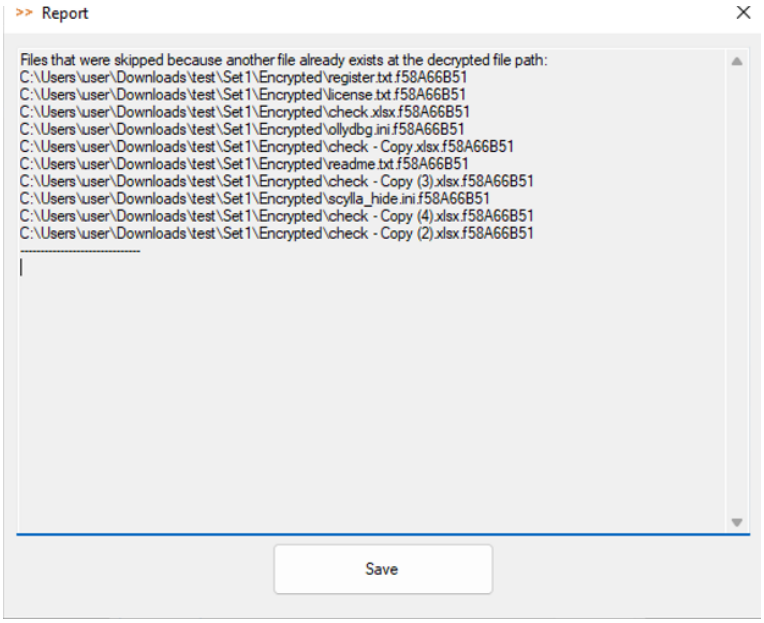


12

When decryption starts, the “Start decryption” button changes to a “Stop decryption” button, which can be pressed to stop the process. After decryption is stopped or finished, the decryptor will inform as to whether all files have been successfully decrypted and if there were any issues that were encountered during decryption, a prompt will appear asking if you would like to view a report of the issues:



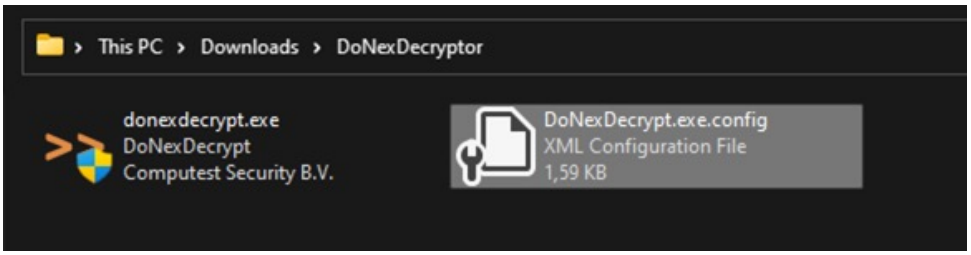
13 Selecting “Yes” reveals a window listing out the issues that were encountered and the affected encrypted files. A .txt report of the report can be saved on the same window:



14 At this step, the files have been decrypted and further directories may be decrypted. When done, you can simply press “Finish” or exit the decryptor.

04. Advanced options >>

In the case that files on a network-attached device or share were encrypted by the ransomware from the infected computer, these may be decrypted using the key recovered from files that were encrypted from a local disk. However, remotely encrypted files follow a different process for decryption, which the decryptor can be instructed to use by changing its configuration file. The file is provided in the DoNexDecryptor.zip file and is named DoNexDecrypt.exe.config:



Edit the file in notepad or another text editor, and change the following line from:
<add key="UseNetworkDecryptionMode" value="false"/>
to:
<add key="UseNetworkDecryptionMode" value="true"/>
Then run the decryptor again and follow the same process to decrypt files that were encrypted on a network share.

About us

Computest Security is the most client, people, and tech focused IT security company in The Netherlands. We are here to enhance the long-term resilience of our clients and help them overcome their most pressing security threats.

We have a solid background in the areas of code-, application-, network-, infrastructure and cloud security, both from an offensive and defensive security perspective. Our specialists support our clients throughout the entire security cycle: they help with preventing, detecting, and responding to modern-day security threats from a technical, process-oriented, and human perspective.

By means of our specialised high-quality work and our advanced security research, we actively contribute to the security of the European communities our clients are navigating through.

Contact:

www.computest.nl

info@computest.nl

Signaalrood 25, 2718 SH Zoetermeer

+31(0)88 733 1337

Independent. Security. Partner. >>