Decryption Checker for Lockbit 3.0 Ransomware

This guide has been prepared to accompany a set of tools provided via the No More Ransom project, aimed at helping victims of the Lockbit ransomware retrieve their encrypted data.

It's important to acknowledge that, despite our best efforts, not all victims of Lockbit can be directly helped with decryption at this point. The two tools included in this download are specifically designed to determine the feasibility of decryption/recovery for your specific case (using two distinct techniques).

If the outcome of either tool indicates that decryption/recovery is feasible, you will be shown an email address to reach out to for further instructions.

Important: Please be aware that these tool binaries are not digitally signed, which means they might be mistakenly identified as potential threats by some antivirus programs. If your antivirus software flags our tools, we recommend temporarily disabling your antivirus protection.

Tool 1: Decryption ID checker

This script checks your unique decryption ID against a list of known decryption keys that have been recovered by law enforcement agencies. If a match is found, it indicates that a decryption key is available for your case, and you will be guided on how to proceed.

The tool provided (*check_decryption_id.exe*) is a commandline-utility and therefore features **no Graphical User Interface (GUI)**. *check_decryption_id.exe* can be executed directly from a windows command prompt and does not need to be installed. As it also does not rely on any remote services, it is fully functional in offline environments.

Tool 2: Check Decrypt for LockBit 3.0 - User Manual

Abstract

The purpose of this tool is to assess if there might be a chance of recovering a certain number of files that had been encrypted with the LockBit 3.0 ransomware. The chances of decryptability depend on a number of factors and cannot be predicted without access to Lockbit-encrypted files.

During the assessment process provided by the tool, none of the existing files scanned are being altered but diagnostic output is being gathered by the tool that would be potentially helpful during additional stages that (given certain conditions are met) could be applied in separate steps involving additional software. This manual focuses solely on the use of the Check Decrypt utility provided.

It is important to note this 2nd tool assesses the feasibility of a partial recovery procedure, it is not a comprehensive decryption solution.

Prerequisites

Please read the instructions provided in this document carefully as the rate of success depends on it.

The tool provided (*check_decrypt.exe*) is a commandline-utility and therefore features **no Graphical User Interface (GUI)**. *check_decrypt.exe* can be executed directly from a windows command prompt and does not need to be installed. As it also does not rely on any remote services, it is fully functional in offline environments.

In order to run this assessment, the tool provided needs to scan the files encrypted by the LockBit ransomware, ideally the entire set of encrypted files with the same 9-letter file extension and not just a subset/extraction of a few files.

Should several individual systems have been individually (!) encrypted, *check_decrypt.exe* can be run on each of them individually without affecting the likelihood of recoverable files. This does e.g. typically not apply to mounted file shares (at the time the ransomware encrypted them) as these were not encrypted individually.

check_decrypt.exe is able to assess the decryptability if the following conditions are met:

- User-generated files on the infected system (e.g. *.jpg*, *.docx*, …) have
  - their previous name (up to the extension part) scrambled, typically to a 7-character string, for example *pfSek8q*
  - the extension part of their filename such as *.jpg* replaced by a seemingly arbitrary 9-character string, for example *xE9thWXg6*
- The ransomware note based on this example, left in several locations on the system during the encryption process would be found in files named *xE9thWXg6.README.txt* but these notes are not needed by *check_decrypt.exe* .

Program invocation

In order to start an assessment on which of the encrypted files of the current fileset could potentially be decrypted, open either a traditional *windows command prompt* or alternatively a *powershell prompt*. Unless the path containing the encrypted files would require special user rights in order to be accessed, *check_decrypt.exe* can be run with a normal windows user able to run portable executables.

check_decrypt.exe expects two arguments during its invocation:

1. A fully qualified path to a location that contains the encrypted files,
2. The extension part common to all encrypted files.

Based on the examples provided in the previous section, the *check_decrypt.exe* which is assumed to be located in a folder *nomoreransom* on drive *E:* can be started to scan files in *D:\data\lockbit_encrypted* with the command:

```
E:\check_decrypt.exe "D:\data\lockbit_encrypted" "xE9thWXg6"
```

During its execution *check_decrypt.exe* provides several lines of status output, among it the number of files with the specified extension found as well as a progress on the calculations performed on the extracted data.

As one of the final steps, *check_decrypt.exe* creates a file containing summarizing information about all files analyzed to the current path from which the command was executed. That means that if this example command was executed from the default starting location of a command prompt, which is the current users home directory, opened by a user *nomoreransom,* that file would be created at:

C:\Users\nomoreransom\check_decrypt_filestatus_xE9thWXg6.csv

This csv-file would be overwritten by subsequent executions of *check_decrypt.exe* from the same location given the same extension is being specified, so take care to copy or rename the resulting *.csv* file if needed.

The *.csv* file allows to check which files have been assessed and could also be of help if decryptable files are being detected.

If decryptable files are being detected, the number of files where a decryption will likely be possible as well as further contact information is provided directly before the message mentioning the writing of the *.csv* file. In this case, please use the contact details provided to request additional information on how to proceed with the decryption process.

Should *check_decrypt.exe* not detect any decryptable files, *"No decryptable files found"* is printed instead. Unfortunately, this also means that the mechanisms used by *check_decrypt.exe* cannot be used to decrypt any of the files scanned.