Decrypted: BianLian Ransomware

Static analysis of BianLian ransomware

BianLian is a ransomware strain written in Go language and compiled as a 64-bit Windows executable. Due to the nature of the Go language, there are many strings directly visible in the binary, including details about the directory structure of the author's PC:

```
-gcflags=all=-trimpath=/home/jack/Projects/project1/crypt28
/home/jack/Projects/project1/common/crypt.go
/home/jack/Projects/project1/common/helpers.go
/home/jack/Projects/project1/common/scanFS_windows.go
/home/jack/Projects/project1/common/scanFS.go
```

There are references to asymmetric cryptography libraries in the sample (RSA and elliptic curves), but the ransomware doesn't do any of it. File data is encrypted with AES-256 in CBC mode. The length of the encrypted data is aligned to 16 bytes, as required by the AES CBC cipher.

BianLian ransomware behavior

Upon its execution, BianLian searches all available disk drives (from A: to Z:). For all found drives, it searches all files and encrypts all whose file extension matches one of the 1013 extensions hardcoded in the ransomware binary.

Interestingly enough, the ransomware doesn't encrypt the file from the start nor does it encrypt a file to the end. Instead, there is a fixed file offset hardcoded in the binary from which the encryption proceeds. The offset differs per sample, but none of the known samples encrypts data from the start of the file.

After data encryption, the ransomware appends the .bianlian extension and drops a ransom note called "**Look at this instruction.txt"** into each folder on the PC (see Figure 1).

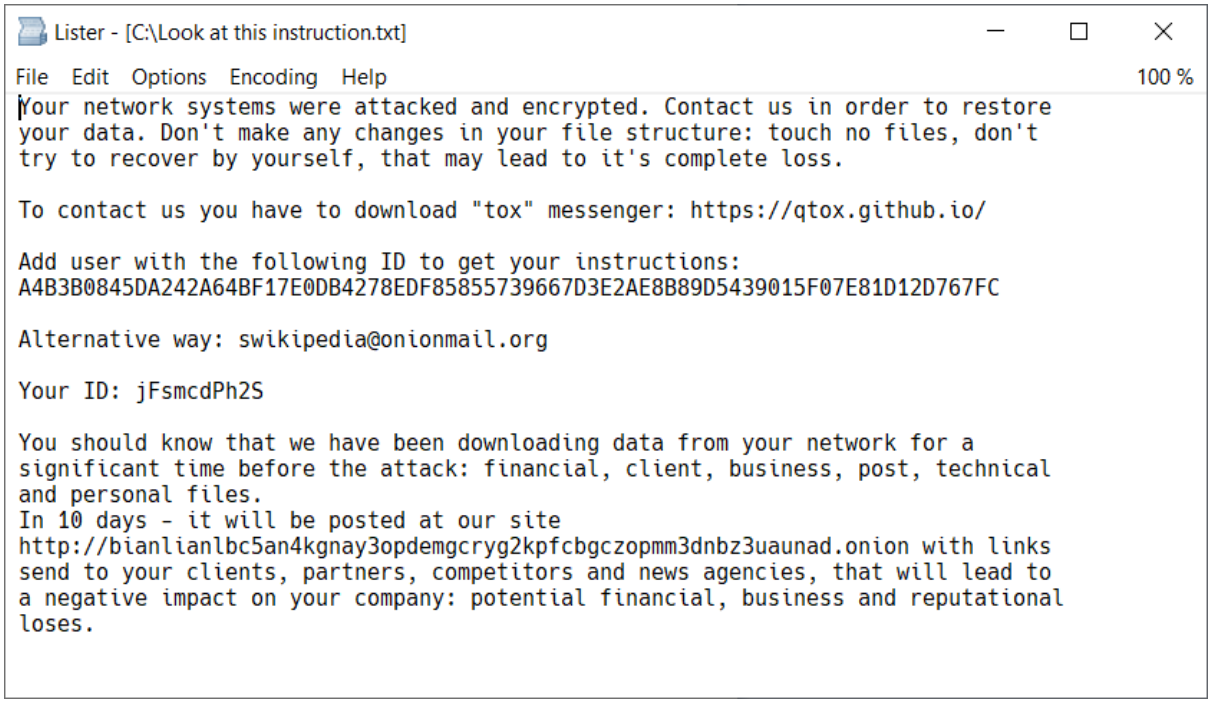


Figure 1: Screenshot of the ransom note

When the encryption is complete, the ransomware deletes itself by executing the following command:

cmd /c del <sample_exe_name>

Parameters of the decryptor

The decryptor can only restore files encrypted by a known variant of the BianLian ransomware. For new victims, it may be necessary to find the ransomware binary on the hard drive; however, because the ransomware deletes itself after encryption, it may be difficult to do so. According to Avast telemetry, common names of the BianLian ransomware file on the victim's PC include:

C:\Windows\TEMP\mativ.exe

C:\Windows\Temp\Areg.exe

C:\Users\%username%\Pictures\windows.exe

anabolic.exe

When searching for the ransomware binary, we recommend looking for an EXE file in a folder which doesn't typically contain executables, such as %temp%, Documents or Pictures. It is also recommendable to check the virus vault of your antivirus. The typical size of the BianLian ransomware executable is around 2 MB.

Should you find a sample of the BianLian ransomware, you can inform us at decryptors@avast.com . We are actively looking for new samples and update the decryptor accordingly.

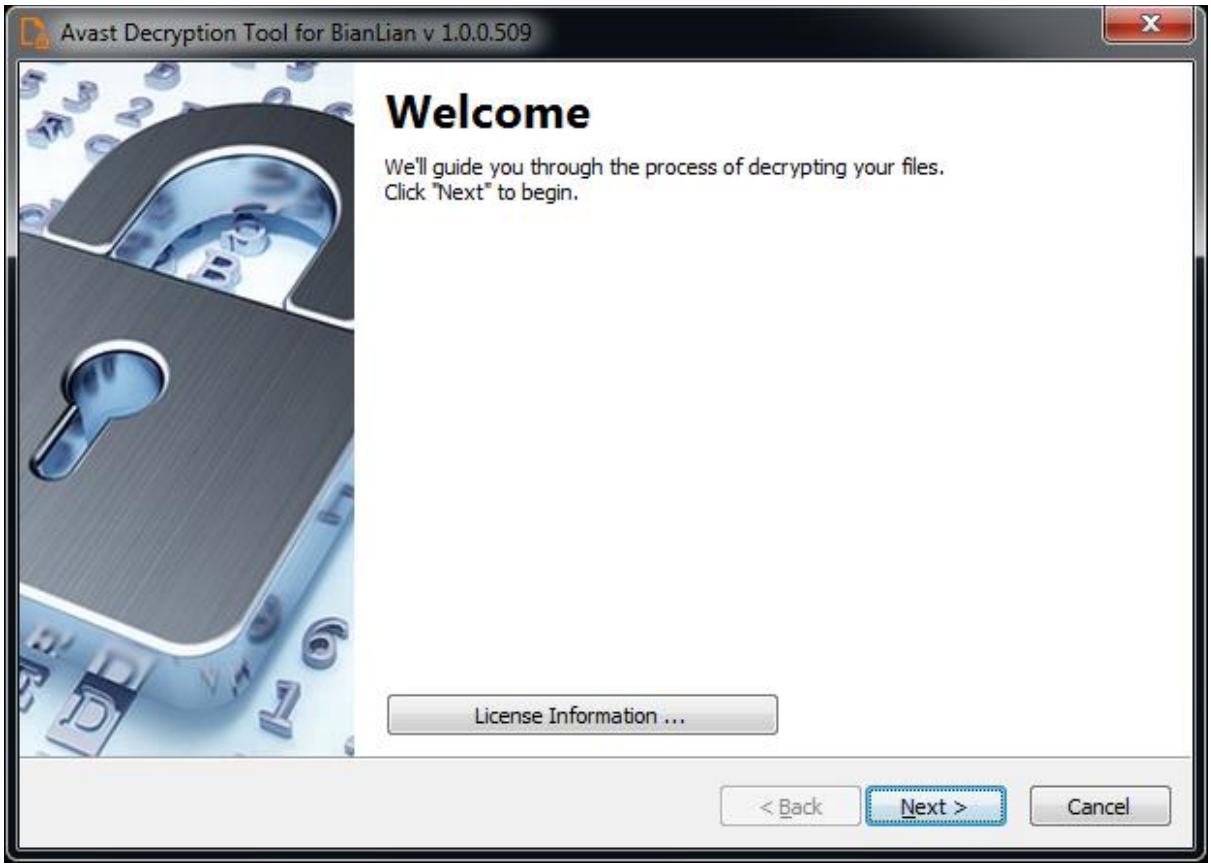
How to use the Avast decryption tool to decrypt files encrypted by the ransomware

Follow these steps to decrypt your files:

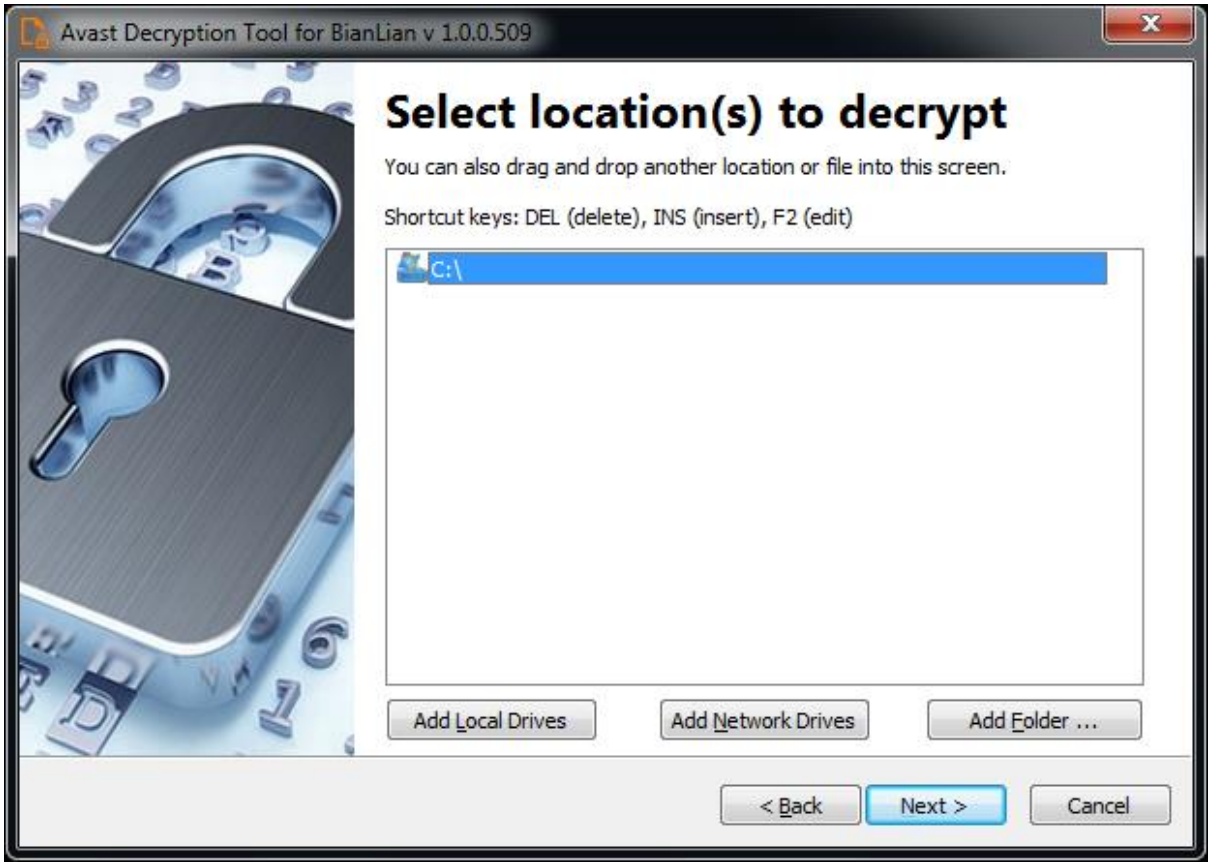
1) Download the free decryptor

2) Run the executable file. It starts as a wizard, leading you through the configuration of the decryption process.

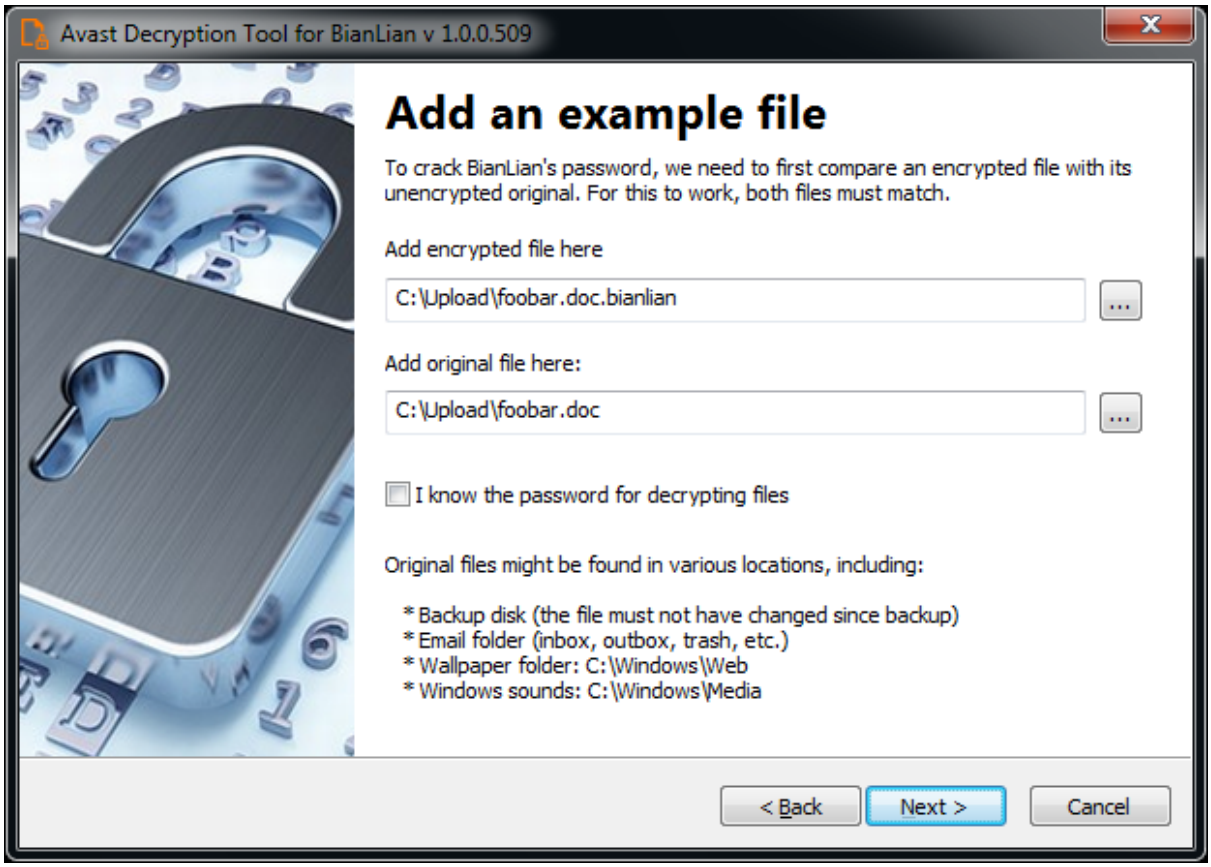
3) On the initial page, we have a link to the license information. Click the Next button, when you are ready to start.



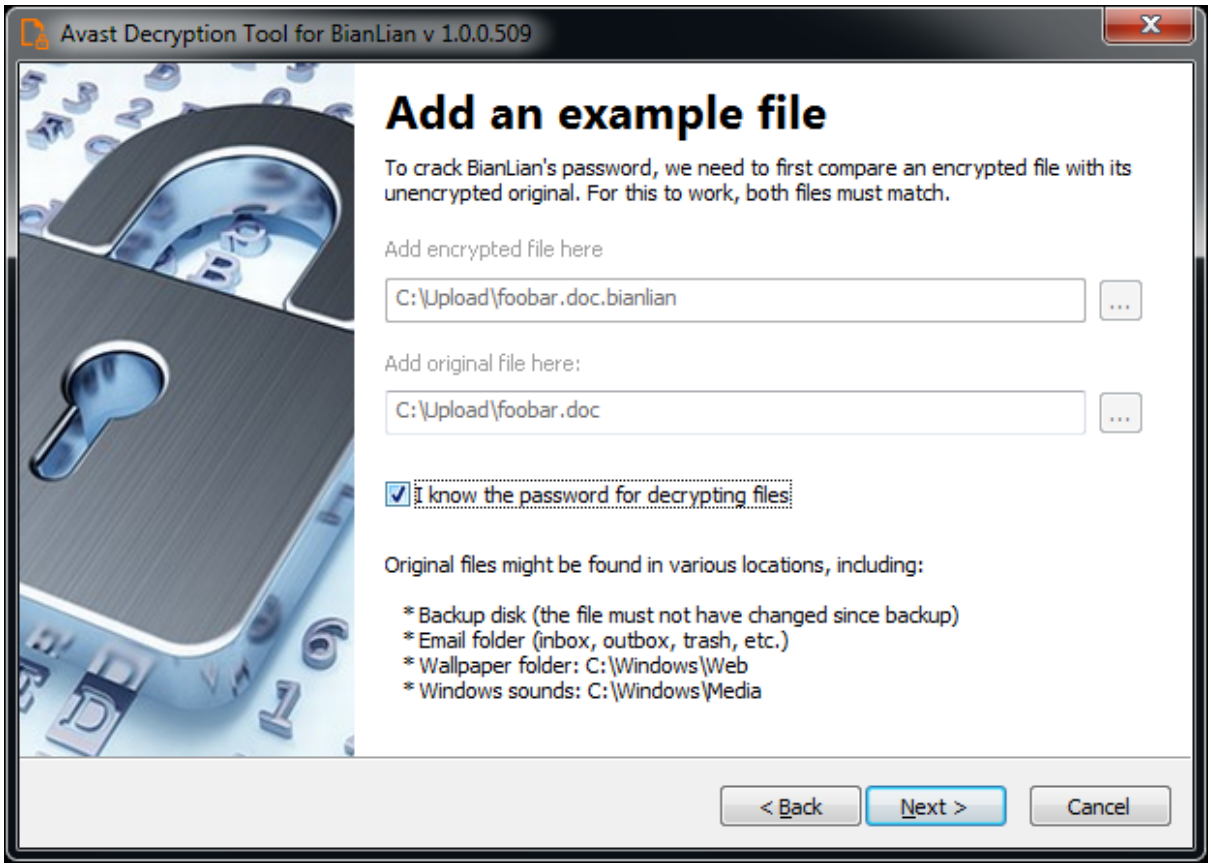
4) On the next page, select the list of locations you want to be searched and decrypted. By default, it contains a list of all local drives:



5) On the third page, you need to provide a file in its original form and encrypted by the BianLian ransomware. Enter both names of the files. You can also drag & drop a file from Windows Explorer to the wizard page.



6) If you have an encryption password created by a previous run of the decryptor, you can select I know the password for decrypting files option:



7) The next page is where the password cracking process takes place. Click Start when you are ready to start the process. The password cracking process tries all known BianLian passwords to determine the right one.

8) Once the password is found, you can proceed to decrypt all the encrypted files on your PC by clicking Next

9) On the final page, you can opt-in to back up your encrypted files. These backups may help if anything goes wrong during the decryption process. This option is on by default, which we recommend. After clicking Decrypt the decryption process begins. Let the decryptor work and wait until it finishes decrypting all of your files.

For questions or comments about the **Avast decryptor**, email decryptors@avast.com .

IOCs:

SHA256

1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43

3a2f6e614ff030804aa18cb03fcc3bc357f6226786efb4a734cbe2a3a1984b6f

46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b

3be5aab4031263529fe019d4db19c0c6d3eb448e0250e0cb5a7ab2324eb2224d

a201e2d6851386b10e20fbd6464e861dea75a802451954ebe66502c2301ea0ed

ae61d655793f94da0c082ce2a60f024373adf55380f78173956c5174edb43d49

eaf5e26c5e73f3db82cd07ea45e4d244ccb3ec3397ab5263a1a74add7bbcb6e2