



NioGuard analyzed the latest version of DeriaLock ransomware ([MD5: 0a7b70efba0aa93d4bc0857b87ac2fcb](https://md5.0a7b70efba0aa93d4bc0857b87ac2fcb)). This version is unique because of two reasons. First, it demands to pay the 30 USD/EUR ransom to the Skype account. Second, DeriaLock incorporates three types of functionality: SystemLocker, CryptoLocker, and FileKiller within a single attack.

If you managed to remove the DeriaLock infection and keep your encrypted files, you can start now decrypting your documents using the encryption key and initialization vector calculated by [our script](#) based on the password string extracted from the DeriaLock's body:

- AES 256-bit key:  
9c9e1ba2ee5b86494b7e1ebba6420ee6ab64ce6d678604eb5b5049b210693743
- IV: 9fa4ed4d89b04ee7f3b74c9b46588e18

There are three ways you can decrypt the files encrypted by DeriaLock:

1. Executing DeriaLockDecryptor.exe
2. Running the Python script DeriaDecryptor.py
3. Using OpenSSL or another crypto tool

**Caution:** Use the decryptor at your own risk. We are not responsible for any damage that it may cause.

**To decrypt the files encrypted by DeriaLock ransomware using the decryptor:**

1. Download the decryptor 'DeriaLockDecryptor.exe' from the GitHub:  
<https://github.com/AlexanderAda/Ransomware-Decryptors/blob/master/DeriaLock/DeriaLockDecryptor.exe>

MD5: a55f076837511a937c4cc420a6147f9e

SHA1: 2e7eb53d7abb91d3e249f52f8f12f2b658e259fa

2. Run the decryptor on an infected machine.

Note: The decryptor will scan the following locations for the presence of the files having the '.deria' extension:

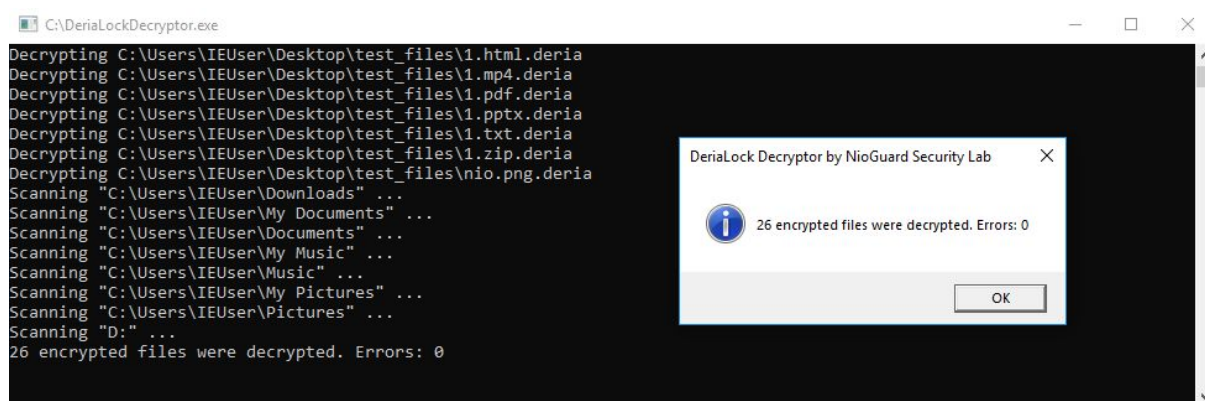
- Current folder
- Desktop
- Downloads
- Documents or My Documents
- Music or My Music
- Pictures or My Pictures
- D:\

Example of output:



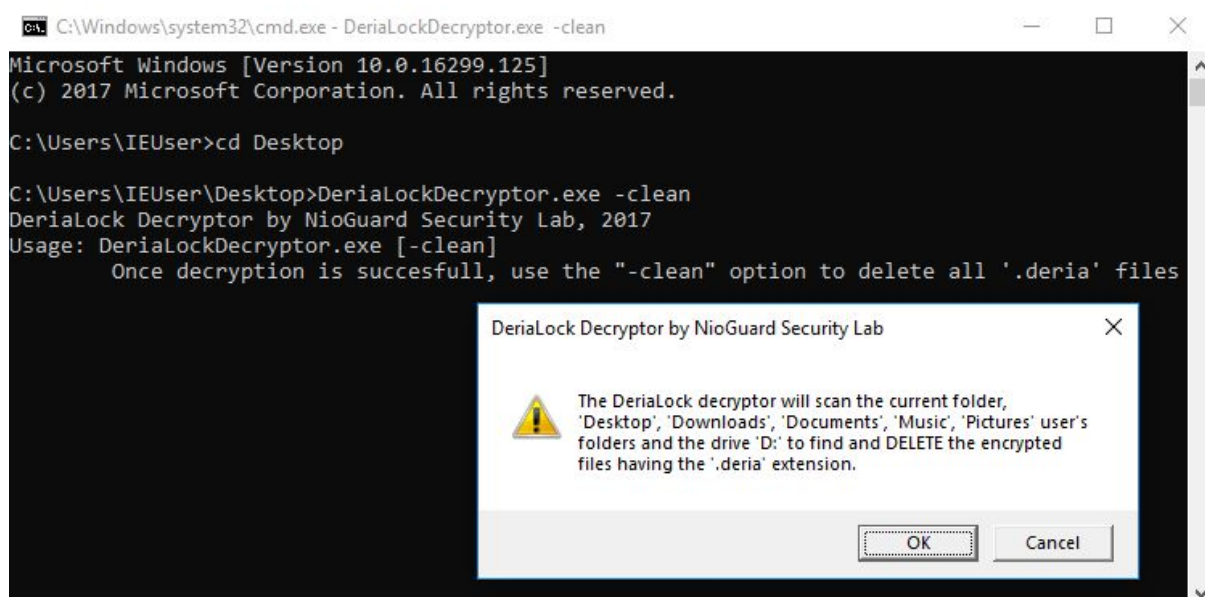
3. Click 'Ok' and wait until the decryptor finishes the decryption process.

Example of output:



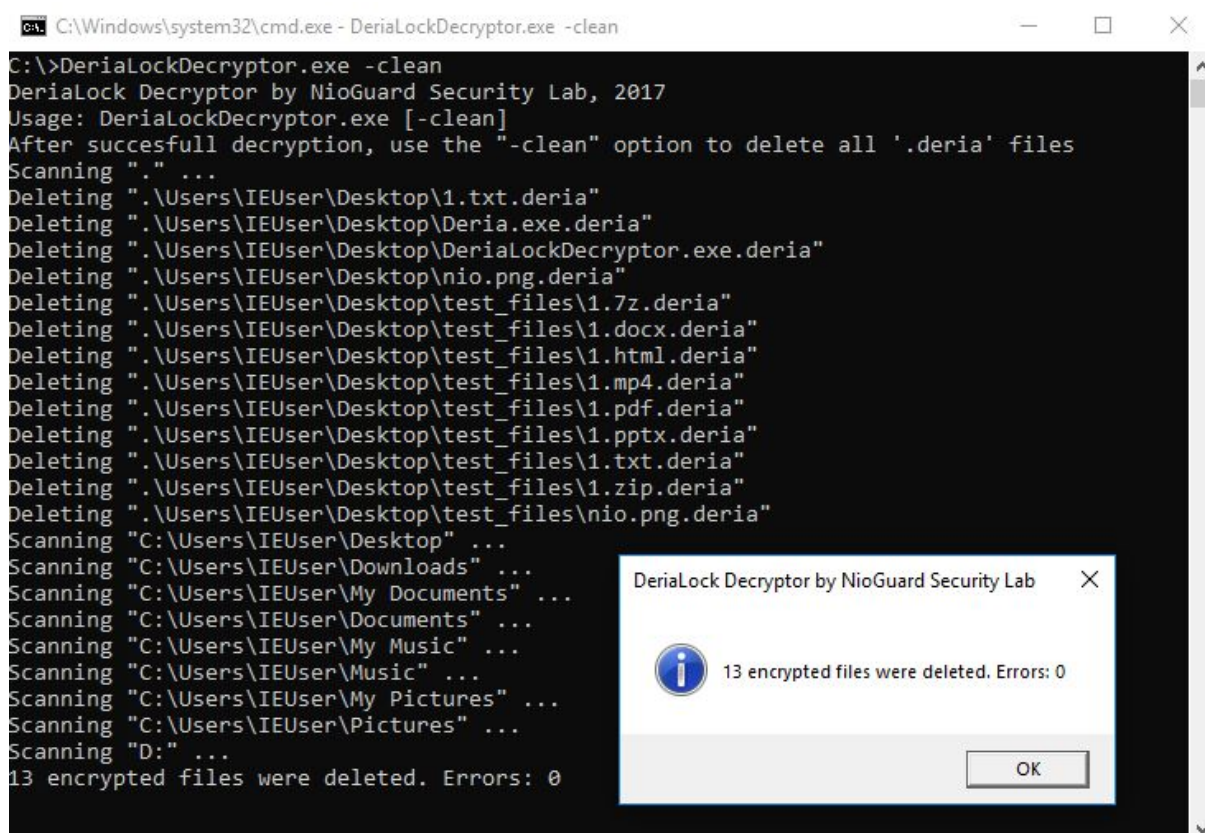
4. Verify that the files were successfully decrypted.
5. Remove the encrypted files having the '.deria' extension by running the following command from the command line:  
*DeriaLockDecryptor.exe -clean*

Example of output:



6. Click 'OK'.

Example of output:



```
C:\Windows\system32\cmd.exe - DeriaLockDecryptor.exe -clean
C:\>DeriaLockDecryptor.exe -clean
DeriaLock Decryptor by NioGuard Security Lab, 2017
Usage: DeriaLockDecryptor.exe [-clean]
After succesfull decryption, use the "-clean" option to delete all '.deria' files
Scanning "." ...
Deleting ".\Users\IEUser\Desktop\1.txt.deria"
Deleting ".\Users\IEUser\Desktop\Deria.exe.deria"
Deleting ".\Users\IEUser\Desktop\DeriaLockDecryptor.exe.deria"
Deleting ".\Users\IEUser\Desktop\nio.png.deria"
Deleting ".\Users\IEUser\Desktop\test_files\1.7z.deria"
Deleting ".\Users\IEUser\Desktop\test_files\1.docx.deria"
Deleting ".\Users\IEUser\Desktop\test_files\1.html.deria"
Deleting ".\Users\IEUser\Desktop\test_files\1.mp4.deria"
Deleting ".\Users\IEUser\Desktop\test_files\1.pdf.deria"
Deleting ".\Users\IEUser\Desktop\test_files\1.pptx.deria"
Deleting ".\Users\IEUser\Desktop\test_files\1.txt.deria"
Deleting ".\Users\IEUser\Desktop\test_files\1.zip.deria"
Deleting ".\Users\IEUser\Desktop\test_files\nio.png.deria"
Scanning "C:\Users\IEUser\Desktop" ...
Scanning "C:\Users\IEUser\Downloads" ...
Scanning "C:\Users\IEUser\My Documents" ...
Scanning "C:\Users\IEUser\Documents" ...
Scanning "C:\Users\IEUser\My Music" ...
Scanning "C:\Users\IEUser\Music" ...
Scanning "C:\Users\IEUser\My Pictures" ...
Scanning "C:\Users\IEUser\Pictures" ...
Scanning "D:" ...
13 encrypted files were deleted. Errors: 0
```

DeriaLock Decryptor by NioGuard Security Lab

13 encrypted files were deleted. Errors: 0

OK

### To decrypt the encrypted files using our Python script:

1. Download the Python script 'DeriaDecryptor.py' from the GitHub:  
<https://github.com/AlexanderAda/Ransomware-Decryptors/blob/master/DeriaLock/DeriaDecryptor.py>

MD5: 61d6336332a8cd904a8c9fd2f78de062

SHA1: 1b651efcedbaae51f12a343b526ee22c8c86eab

2. Download and install Python 2.7 on an infected machine from  
<https://www.python.org/downloads/>

3. Run the script on the infected machine:

```
python DeriaDecryptor.py
```

### To decrypt the encrypted file using OpenSSL tool:

1. Download OpenSSL source code available by the link and compile it:  
<https://www.openssl.org/source/>

2. Run in the command line:



```
openssl aes-256-cbc -d -in photo.png.deria -K  
9c9e1ba2ee5b86494b7e1ebba6420ee6ab64ce6d678604eb5b5049b210693743 -iv  
9fa4ed4d89b04ee7f3b74c9b46588e18 -out photo.png
```

Should you have any questions, please email to: [ada@nioguard.com](mailto:ada@nioguard.com)

## References

- <https://nioguard.blogspot.com/2017/02/decrypting-derialock.html>
- <https://www.acronis.com/en-us/blog/posts/derialock-demands-victims-pay-ransom-sky>
- <https://www.bleepingcomputer.com/news/security/new-derialock-ransomware-active-on-christmas-includes-an-unlock-all-command/>
- <https://twitter.com/struppigel/status/813741939690442756>
- <http://id-ransomware.blogspot.com/2016/12/derialock-ransomware.html>