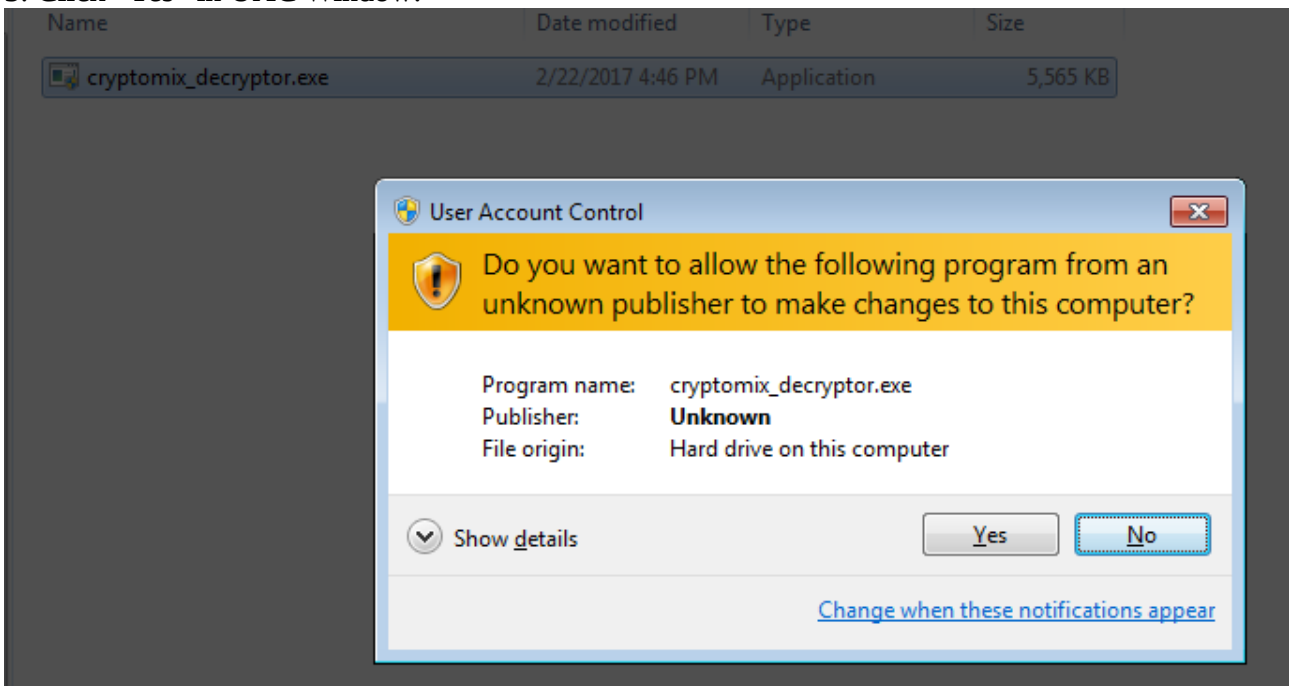


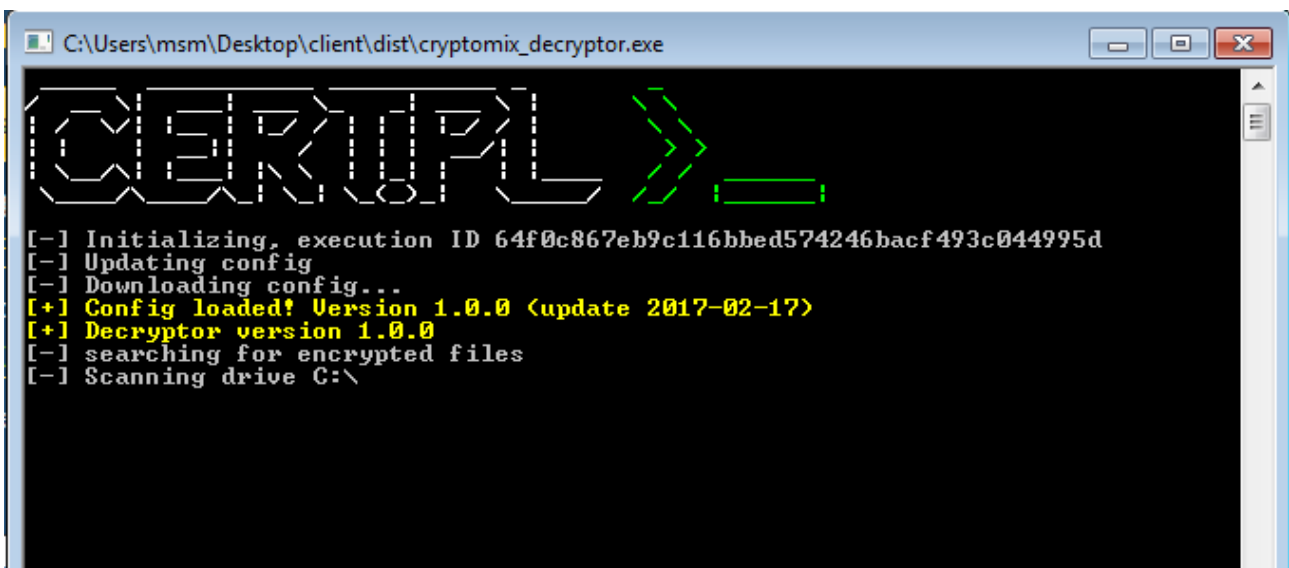
## CryptFile2/CryptoMix/CryptoShield How-to guide

**Make sure that you remove the malware from your system before running this tool – otherwise it will repeatedly encrypt your files.**

1. Download Cryptomix Decryptor ([https://nomoreransom.cert.pl/static/cryptomix\\_decryptor.exe](https://nomoreransom.cert.pl/static/cryptomix_decryptor.exe))
2. Run cryptomix\_decryptor.exe on the infected computer
3. Click “Yes” in UAC Window:



4. Scan should start automatically:



5. This should be enough – if you’re lucky, all your files will be decrypted:

```

C:\Users\msm\Desktop\client\dist\cryptomix_decryptor.exe

CERTPL >>>

[-] Initializing, execution ID 67991c9f2a5bdfaa56472cd2a32436fa1ea5a134
[-] Updating config
[-] Downloading config...
[+] Config loaded! Version 1.0.0 (update 2017-02-17)
[+] Decryptor version 1.0.0
[-] searching for encrypted files
[-] Scanning drive C:\
[+] Found encrypted files:
[-] C:\Users\msm\Desktop\files\0a54c430c3bb10c53ad0158fba541fd75caf9efcad9b3f0e5f369a322ea6b4b5.id_a87b6d32_email_enc10@dr.com_.lesli
[-] C:\Users\msm\Desktop\files\0ba2474bb207082e596652d25f88260f07eb9aa73d14a221502045e144fbad9d.id_a87b6d32_email_enc10@dr.com_.lesli
[-] C:\Users\msm\Desktop\files\0bd18e98d8d1a2e9d3bfa4d5a687de6dd55919866a978f86bfd5d4e8df19ee30.id_a87b6d32_email_enc10@dr.com_.lesli
[+] Trying hardcoded keys... (1/3)
[+] Decryption key found: 363e4e177960fb5fbc71ad0914ef3109443ef694e4cc51d6efa741255559099b
[-] Initiating decryption
[-] Scanning drive C:\
[-] Decrypting file: C:\Users\msm\Desktop\files\0a54c430c3bb10c53ad0158fba541fd75caf9efcad9b3f0e5f369a322ea6b4b5.id_a87b6d32_email_enc10@dr.com_.lesli
[+] Decrypted file: C:\Users\msm\Desktop\files\0a54c430c3bb10c53ad0158fba541fd75caf9efcad9b3f0e5f369a322ea6b4b5.id_a87b6d32_email_enc10@dr.com_.lesli
[-] Decrypting file: C:\Users\msm\Desktop\files\0ba2474bb207082e596652d25f88260f07eb9aa73d14a221502045e144fbad9d.id_a87b6d32_email_enc10@dr.com_.lesli
[+] Decrypted file: C:\Users\msm\Desktop\files\0ba2474bb207082e596652d25f88260f07eb9aa73d14a221502045e144fbad9d.id_a87b6d32_email_enc10@dr.com_.lesli
[-] Decrypting file: C:\Users\msm\Desktop\files\0bd18e98d8d1a2e9d3bfa4d5a687de6dd55919866a978f86bfd5d4e8df19ee30.id_a87b6d32_email_enc10@dr.com_.lesli
[+] Decrypted file: C:\Users\msm\Desktop\files\0bd18e98d8d1a2e9d3bfa4d5a687de6dd55919866a978f86bfd5d4e8df19ee30.id_a87b6d32_email_enc10@dr.com_.lesli

```

6. But sometimes we're not able to decrypt files. If you're unlucky, error message will be presented:

```

C:\Users\msm\Desktop\client\dist\cryptomix_decryptor.exe

[-] Initializing, execution ID 64f0c867eb9c116bbcd574246bacf493c044995d
[-] Updating config
[-] Downloading config...
[+] Config loaded! Version 1.0.0 (update 2017-02-17)
[+] Decryptor version 1.0.0
[-] searching for encrypted files
[-] Scanning drive C:\
[+] Found encrypted files:
[-] C:\Users\msm\Desktop\01 25 10 2012 kurs CNC\QFP00006.WCT.[RES_SUP@INDIA.COM].ID[001B7163A689A0F1].CRYPTOSHIELD
[-] C:\Users\msm\Desktop\01 25 10 2012 kurs CNC\QFP00007.WCT.[RES_SUP@INDIA.COM].ID[001B7163A689A0F1].CRYPTOSHIELD
[-] C:\Users\msm\Desktop\01 25 10 2012 kurs CNC\QFP00008.WCT.[RES_SUP@INDIA.COM].ID[001B7163A689A0F1].CRYPTOSHIELD
[+] Trying hardcoded keys... (1/3)
[+] Scanning registry... (2/3)
[+] Scanning filesystem... (3/3)
[!] Decryption key not found
[+] We're sorry, we can't currently decrypt your files
[-] Finishing
[+] In case of any inquiries, please email cert@cert.pl and attach generated log.txt file!
[-] Press 'Enter' to exit...

```

In this case, your files are encrypted with strong key, and we can't currently decrypt them – sorry.

7. If something didn't work, or not all files were decrypted, don't hesitate to contact [cert@cert.pl](mailto:cert@cert.pl). Please attach log.txt file, that should be generated next to cryptomix\_decryptor.exe.

8. After decryption you can safely delete encrypted files