Help for Ukraine: Free decryptor for HermeticRansom ransomware

decoded.avast.io/threatresearch/help-for-ukraine-free-decryptor-for-hermeticransom-ransomware/

March 3, 2022

by Threat Research TeamMarch 3, 20223 min read

On February 24th, the Avast Threat Labs discovered a new ransomware strain accompanying the data wiper HermeticWiper malware, which our colleagues at ESET found circulating in the Ukraine. Following this naming convention, we opted to name the strain we found piggybacking on the wiper, HermeticRansom. According to analysis done byCrowdstrike's Intelligence Team, the ransomware contains a weakness in the crypto schema and can be decrypted for free.

If your device has been infected with HermeticRansom and you'd like to decrypt your files, click here to skip to the How to use the Avast decryptor to recover files

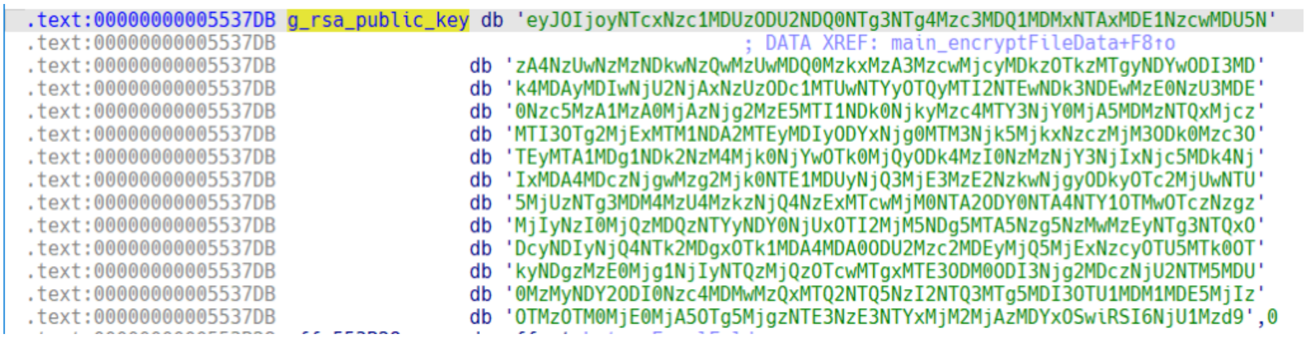
Go!

The ransomware is written in GO language. When executed, it searches local drives and network shares for potentially valuable files, looking for files with one of the extensions listed below (the order is taken from the sample):

```
 .docx .doc .dot .odt .pdf .xls .xlsx .rtf .ppt .pptx .one.xps .pub .vsd
.txt .jpg .jpeg .bmp .ico .png .gif .sql.xml .pgsql .zip .rar .exe .msi
.vdi .ova .avi .dip .epub.iso .sfx .inc .contact .url .mp3 .wmv .wma .wtv
.avi .acl.cfg .chm .crt .css .dat .dll .cab .htm .html .encryptedjb
```

In order to keep the victim's PC operational, the ransomware avoids encrypting files in Program Files and Windows folders.

For every file designated for encryption, the ransomware creates a 32-byte encryption key. Files are encrypted by blocks, each block has `1048576` (`0x100000`) bytes. A maximum of nine blocks are encrypted. Any data past `9437184` bytes (`0x900000`) is left in plain text. Each block is encrypted by `AES GCM` symmetric cipher. After data encryption, the ransomware appends a file tail, containing the `RSA-2048` encrypted file key. The public key is stored in the binary as a `Base64` encoded string:

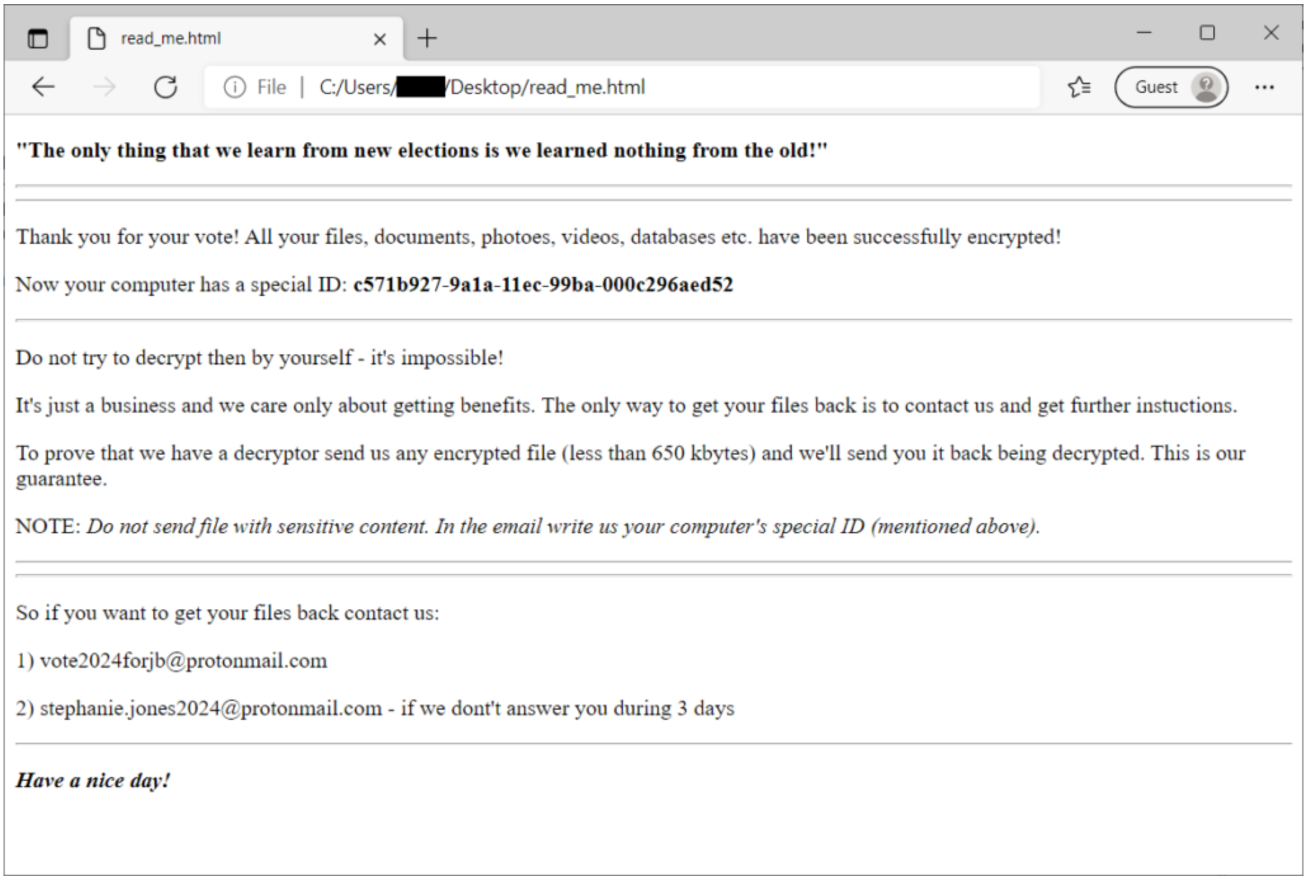


```
.text:00000000005537DB g_rsa_public_key db 'eyJOIjoyNTcxNzc1MDUzODU2NDQ0NTg3NTg4Mzc3MDQ1MDMxNTAxMDE1NzcwMDU5N'
.text:00000000005537DB                                          ; DATA XREF: main_encryptFileData+F8↑o
.text:00000000005537DB                  db 'zA4NzUwNzMzNDkwNzQwMzUwMDQ0MzkxMzA3MzcwMjcyMDkzOTkzMTgyNDYwODI3MD'
.text:00000000005537DB                  db 'k4MDAyMDIwNjU2NjAxNzUzODc1MTUwNTYyOTQyMTI2NTEwNDk3NDEwMzE0NzU3MDE'
.text:00000000005537DB                  db '0Nzc5MzA1MzA0MjAzNjg2MzE5MTI1NDk0NjkyMzc4MTY3NjY0MjA5MDMzNTQxMjcz'
.text:00000000005537DB                  db 'MTI3OTg2MjExMTM1NDA2MTEyMDIyODYxNjg0MTM3Njk5MjkxNzczMjM3ODk0Mzc3O'
.text:00000000005537DB                  db 'TEyMTA1MDg1NDk2NzM4MjkONjYwOTk0MjQyODk4MzI0NzMzNjY3NjIxNjc5MDk4Nj'
.text:00000000005537DB                  db 'IxMDA4MDczNjgwMzg2MjkONTE1MDUyNjQ3MjE3MzE2NzkwNjgyODkyOTc2MjUwNTU'
.text:00000000005537DB                  db '5MjUzNTg3MDM4MzU4MzkzNjQ4NzExMTcwMjM0NTA2ODY0NTA4NTY1OTMwOTczNzgz'
.text:00000000005537DB                  db 'MjIyNzI0MjQzMDQzNTYyNDY0NjUxOTI2MjM5NDg5MTA5Nzg5NzMwMzEyNTg3NTQxO'
.text:00000000005537DB                  db 'DcyNDIyNjQ4NTk2MDgxOTk1MDA4MDA0ODU2Mzc2MDEyMjQ5MjExNzcyOTU5MTk0OT'
.text:00000000005537DB                  db 'kyNDgzMzE0Mjg1NjIyNTQzMjQzOTcwMTgxMTE3ODM0ODI3Njg2MDczNjU2NTM5MDU'
.text:00000000005537DB                  db '0MzMyNDY2ODI0Nzc4MDMwMzQxMTQ2NTQ5NzI2NTQ3MTg5MDI3OTU1MDM1MDE5MjIz'
.text:00000000005537DB                  db 'OTMzOTM0MjE0MjA5OTg5MjgzNTE3NzE3NTYxMjM2MjAzMDYxOSwiRSI6NjU1Mzd9',0
```

Encrypted file names are given extra suffix:

```
.[vote2024forjb@protonmail.com].encryptedJB
```

When done, a file named "`read_me.html`" is saved to the user's `Desktop` folder:



"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: **c571b927-9a1a-11ec-99ba-000c296aed52**

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

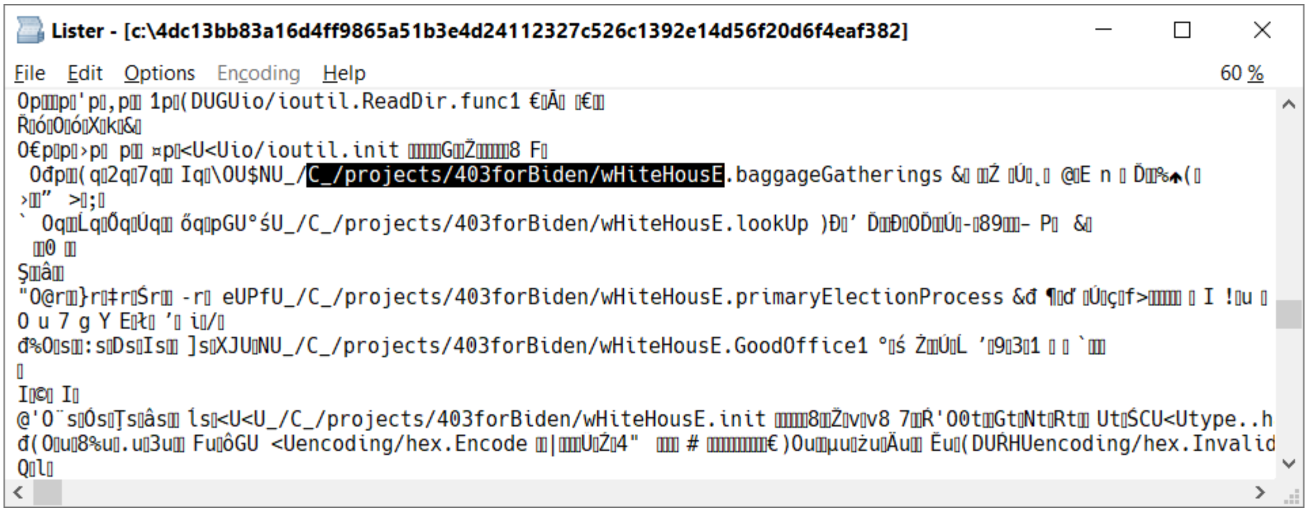
So if you want to get your files back contact us:

1) vote2024forjb@protonmail.com

2) stephanie.jones2024@protonmail.com - if we dont't answer you during 3 days

Have a nice day!

There is an interesting amount of politically oriented strings in the ransomware binary. In addition to the file extension, referring to the re-election of Joe Biden in 2024, there is also a reference to him in the project name:


Lister - [c:\4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382]
File
Edit
Options
Encoding
Help
60 %

```
Op▯▯p▯'p▯,p▯ 1p▯(DUGUio/ioutil.ReadDir.func1 €▯Ă▯ ▯€▯
Ř▯ó▯O▯ó▯X▯k▯&▯
O€p▯p▯›p▯ p▯ ¤p▯<U<Uio/ioutil.init ▯▯▯G▯Ž▯▯▯8 F▯
 Ođp▯(q▯2q▯7q▯ Iq▯\OU$NU_/C_/projects/403forBiden/wHiteHousE.baggageGatherings &▯ ▯Ż ▯Ú▯˛▯ @▯E n ▯ Ď▯%(▯
›▯” >▯;▯
` Oq▯Lq▯Őq▯Úq▯ őq▯pGU°śU_/C_/projects/403forBiden/wHiteHousE.lookUp )Đ▯’ Ď▯Đ▯OĎ▯Ú▯-▯89▯- P▯ &▯
 ▯0 ▯
Ş▯â▯
"O@r▯}r▯‡r▯Śr▯ -r▯ eUPfU_/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess &đ ¶▯ď ▯Ú▯ç▯f>▯▯▯ ▯ I !▯u ▯
O u 7 g Y E▯ł▯ ’▯ i▯/▯
đ%O▯s▯:s▯Ds▯Is▯ ]s▯XJU▯NU_/C_/projects/403forBiden/wHiteHousE.GoodOffice1 °▯ś Ż▯Ú▯Ĺ ’▯9▯3▯1 ▯ ▯ `▯
▯
I▯©▯ I▯
@'O¨s▯Ós▯Ţs▯âs▯ ĺs▯<U<U_/C_/projects/403forBiden/wHiteHousE.init ▯▯▯8▯Ž▯v▯v8 7▯Ŕ'O0t▯Gt▯Nt▯Rt▯ Ut▯ŚCU<Utype..h
đ(O▯u▯8%u▯.u▯3u▯ Fu▯ôGU <Uencoding/hex.Encode ▯|▯▯U▯Ž▯4" ▯▯ # ▯▯▯▯€)Ou▯µu▯żu▯Äu▯ Ëu▯(DUŔHUencoding/hex.Invalid
Q▯l▯
```

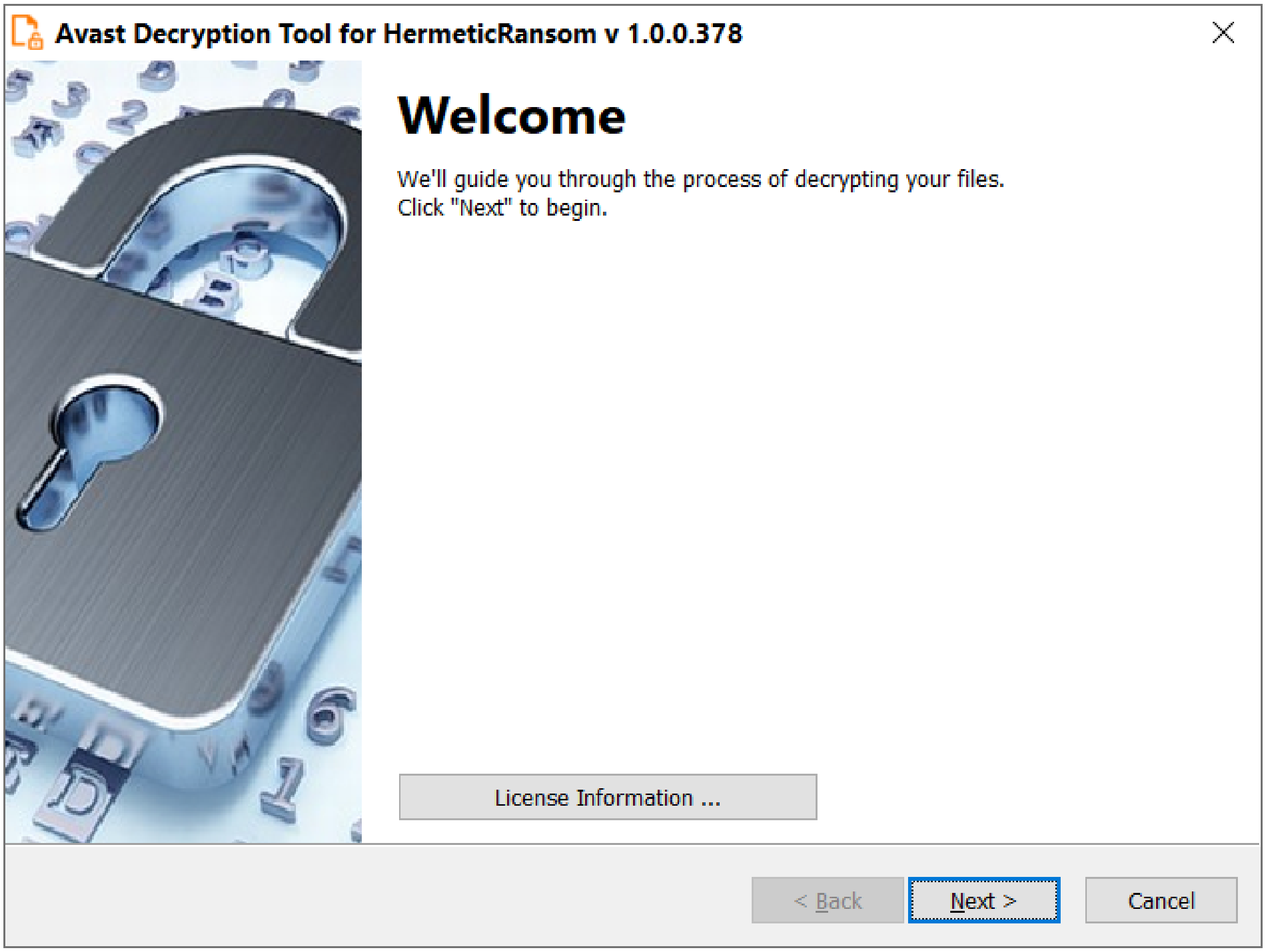
During the execution, the ransomware creates a large amount of child processes, that do the actual encryption:

```
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 8396a280-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 8299045b-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 824a7ce6-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 82d3941d-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 84389c43-9a72-11ec-b140-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 822a2702-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 820b2870-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 8241d860-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 8391b7a7-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 846da895-9a72-11ec-b140-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 8320ea65-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 82fc1c17-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 83b31893-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 82ce36d3-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 83fbf671-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 8327c527-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 834bd4b9-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 83a811b3-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 8497ae08-9a72-11ec-b141-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 82c5924d-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 823101c4-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 8362089f-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 8338032d-9a72-11ec-b13e-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 845ee808-9a72-11ec-b140-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 843ca23b-9a72-11ec-b140-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 844deb47-9a72-11ec-b140-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 8453bb03-9a72-11ec-b140-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 872c3f8f-9a72-11ec-b157-be069a07bcdf.exe
cmd /c copy C:\Users\[redacted]\AppData\Local\Temp\malware_sample.exe 82de74d8-9a72-11ec-b13e-be069a07bcdf.exe
```

How to use the Avast decryptor to recover files

To decrypt your files, please, follow these steps:

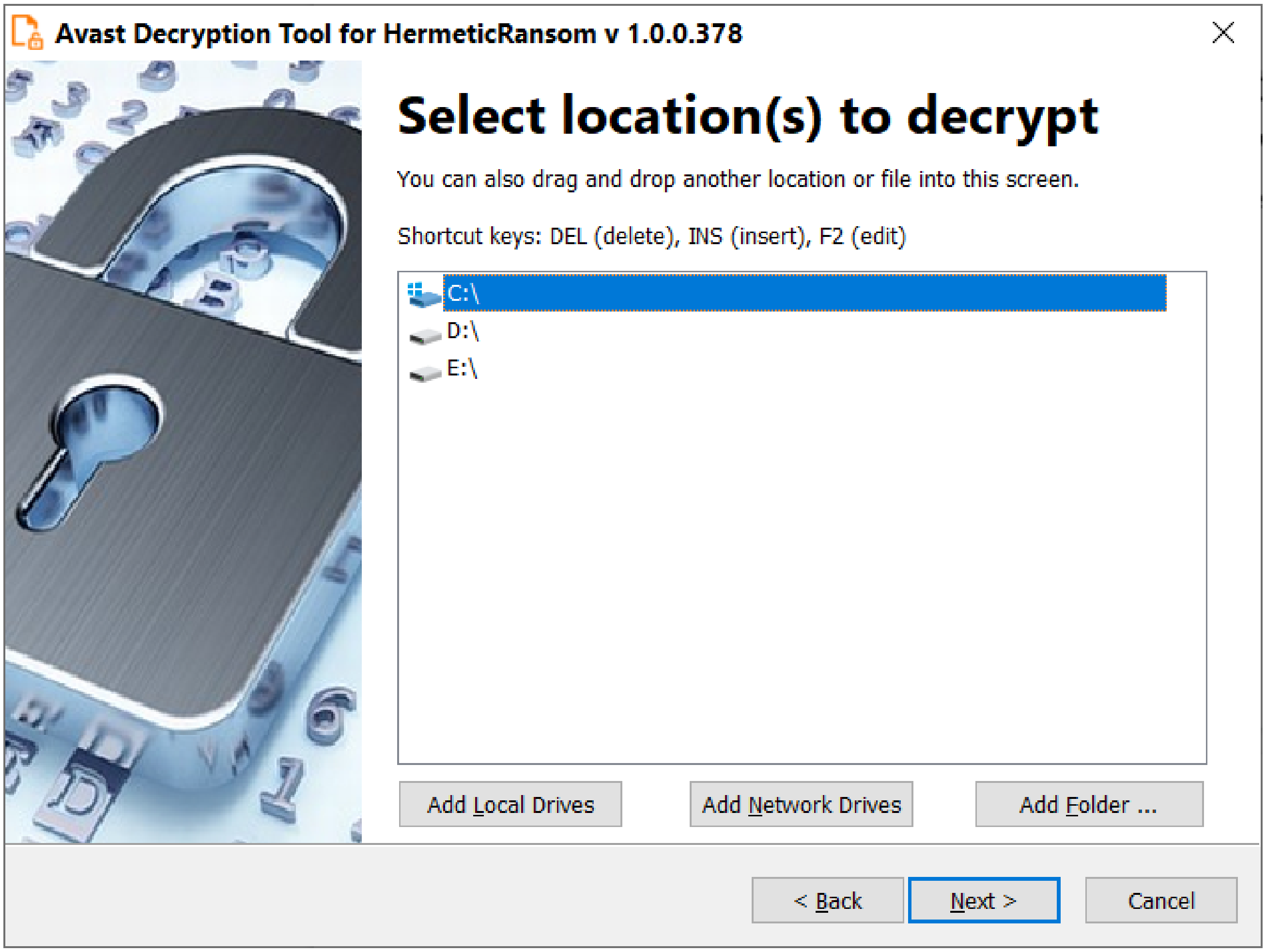
1. Download the free Avast decryptor.
2. Simply run the executable file. It starts in the form of a wizard, which leads you through the configuration of the decryption process.
3. On the initial page, you can read the license information, if you want, but you really only need to click “ `Next` “


Avast Decryption Tool for HermeticRansom v 1.0.0.378

Welcome

We'll guide you through the process of decrypting your files.
Click "Next" to begin.

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



Avast Decryption Tool for HermeticRansom v 1.0.0.378

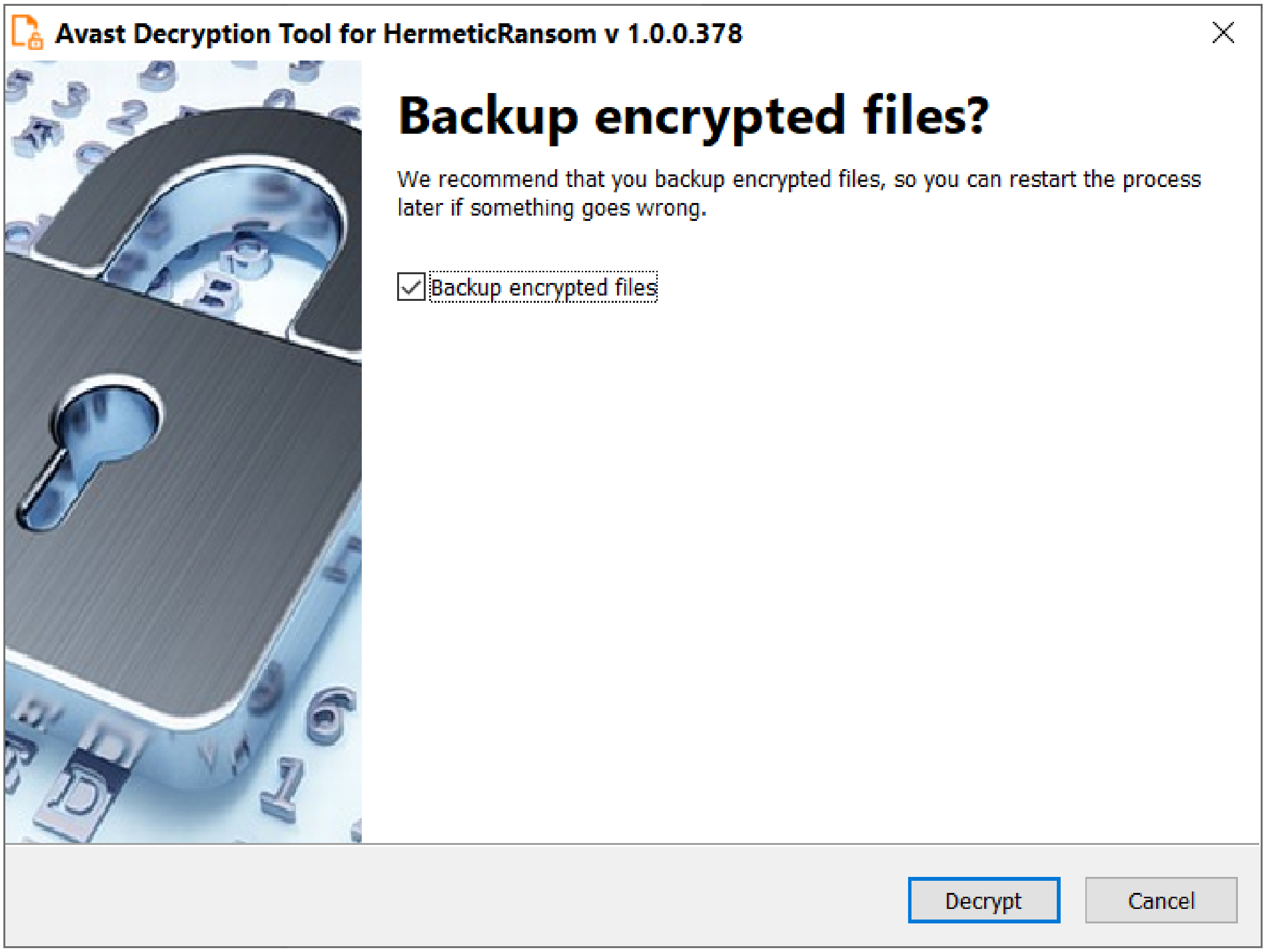
Select location(s) to decrypt

You can also drag and drop another location or file into this screen.

Shortcut keys: DEL (delete), INS (insert), F2 (edit)

C:\
D:\
E:\

1. On the final wizard page, you can opt-in whether you want to backup encrypted files. These backups may help if anything goes wrong during the decryption process. This option is turned on by default, which we recommend. After clicking “ `Decrypt` ”, the decryption process begins. Let the decryptor work and wait until it finishes.



Avast Decryption Tool for HermeticRansom v 1.0.0.378

Backup encrypted files?

We recommend that you backup encrypted files, so you can restart the process later if something goes wrong.

☑ Backup encrypted files

IOCs

SHA256: `4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382`

Tagged asanalysis, decryptors, malware, ransomware, reversing