Decrypted: Midnight Ransomware

In the ever-evolving landscape of cyber threats, a new ransomware strain known as *Midnight* has emerged, echoing the notorious tactics of its predecessor, Babuk. First detected by Gen researchers, Midnight blends familiar ransomware mechanics with novel cryptographic modifications – some of which unintentionally open the door to file recovery. This blog dives into the technical anatomy of Midnight, its lineage from Babuk, and the critical indicators of infection. Most importantly, it offers a practical guide to decrypting affected files, empowering victims with a rare opportunity to reclaim their data without paying a ransom.

Midnight’s Discovery and Roots

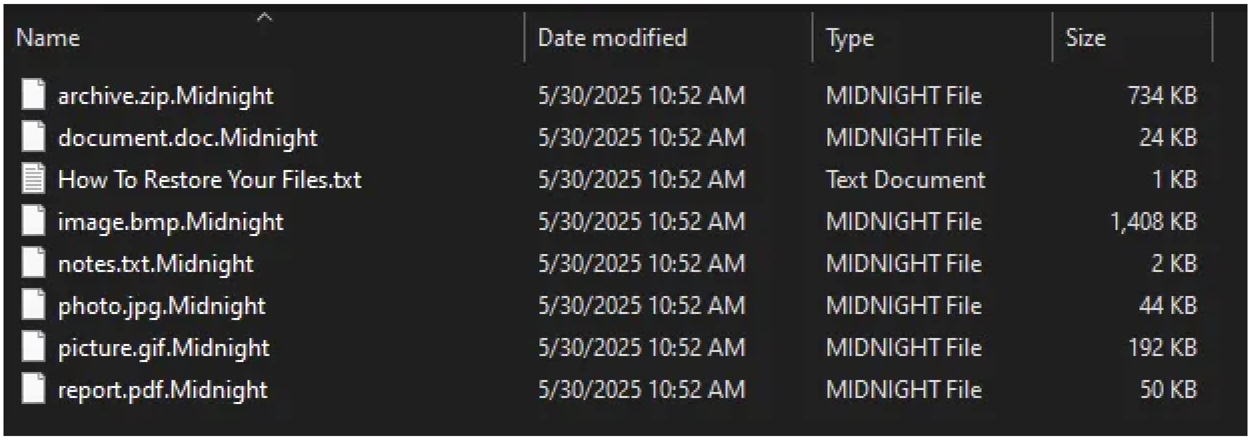
Gen researchers have identified a new ransomware strain, internally dubbed Midnight. It shows clear signs of being inspired by the Babuk ransomware family, which first appeared in early 2021 and quickly gained a reputation for its aggressive tactics and advanced technical aspects. Babuk operated as a Ransomware-as-a-Service (RaaS), targeting large organizations across healthcare, finance, government, and other critical infrastructure. The ransomware used strong encryption (HC256 and ECDH) and intermittent file encryption to maximize damage while maintaining speed.

In mid-2021, Babuk's operators abruptly shut down and leaked their full source code, including builders for Windows, ESXI and NAS variants. This leak led to a wave of inspired ransomware families, each modifying Babuk's original design to suit their own goals.

Midnight is one such evolution. While it retains much of Babuk's core structure, its authors introduced several changes - most notably in the cryptographic scheme used for file encryption. These changes, while likely intended to improve the ransomware's effectiveness, inadvertently introduced weaknesses that make file decryption possible under certain conditions.

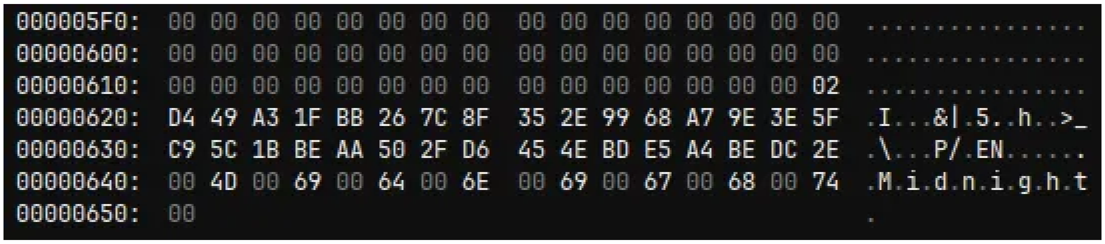
How to Recognize Midnight Ransomware

Midnight ransomware typically appends the .Midnight or .endpoint extension to encrypted files. In some cases, the ransomware is configured not to modify the file names. Instead, it appends the extension string directly to the end of the file content. This behavior can be observed in hex dumps and may affect file parsing.



Name	Date modified	Type	Size
archive.zip.Midnight	5/30/2025 10:52 AM	MIDNIGHT File	734 KB
document.doc.Midnight	5/30/2025 10:52 AM	MIDNIGHT File	24 KB
How To Restore Your Files.txt	5/30/2025 10:52 AM	Text Document	1 KB
image.bmp.Midnight	5/30/2025 10:52 AM	MIDNIGHT File	1,408 KB
notes.txt.Midnight	5/30/2025 10:52 AM	MIDNIGHT File	2 KB
photo.jpg.Midnight	5/30/2025 10:52 AM	MIDNIGHT File	44 KB
picture.gif.Midnight	5/30/2025 10:52 AM	MIDNIGHT File	192 KB
report.pdf.Midnight	5/30/2025 10:52 AM	MIDNIGHT File	50 KB

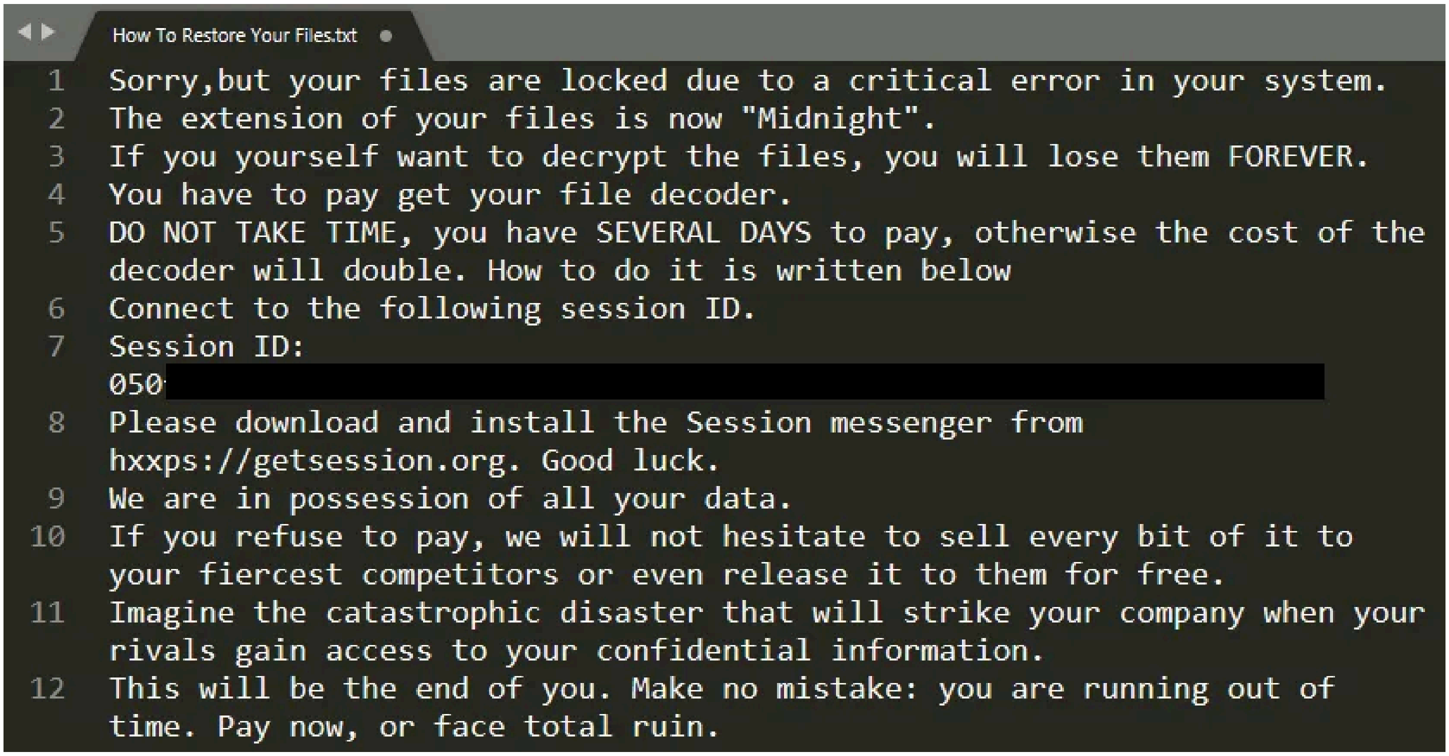
Folder listing showing files with the .Midnight extension



```
000005F0:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000600:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000610:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 02  ................
00000620:  D4 49 A3 1F BB 26 7C 8F  35 2E 99 68 A7 9E 3E 5F  .I...&|.5..h..>_
00000630:  C9 5C 1B BE AA 50 2F D6  45 4E BD E5 A4 BE DC 2E  .\...P/.EN......
00000640:  00 4D 00 69 00 64 00 6E  00 69 00 67 00 68 00 74  .M.i.d.n.i.g.h.t
00000650:  00                                                .
```

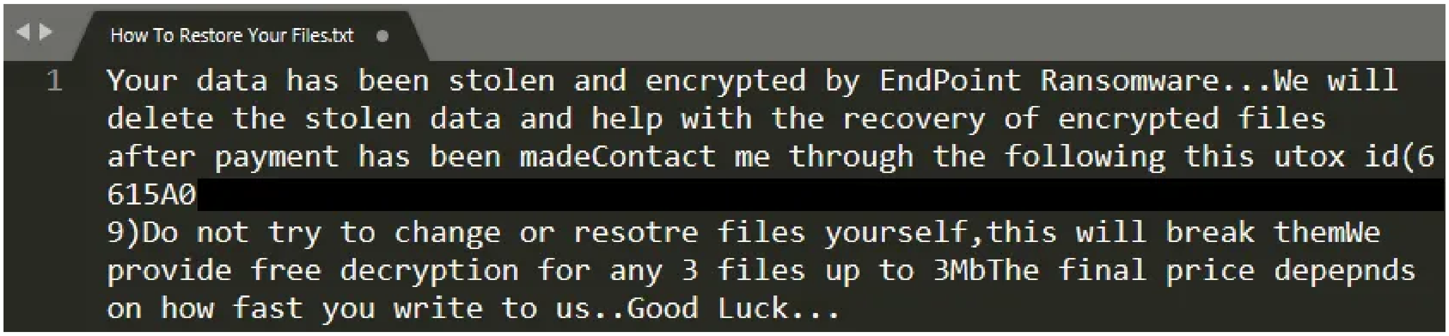
Hex view of an encrypted file with .Midnight appended to the file content

A ransom note named How To Restore Your Files.txt is dropped in the affected directories. It may look similar as on the following screenshots:



```
Sorry,but your files are locked due to a critical error in your system.
The extension of your files is now "Midnight".
If you yourself want to decrypt the files, you will lose them FOREVER.
You have to pay get your file decoder.
DO NOT TAKE TIME, you have SEVERAL DAYS to pay, otherwise the cost of the
decoder will double. How to do it is written below
Connect to the following session ID.
Session ID:
050[redacted]
Please download and install the Session messenger from
hxxps://getsession.org. Good luck.
We are in possession of all your data.
If you refuse to pay, we will not hesitate to sell every bit of it to
your fiercest competitors or even release it to them for free.
Imagine the catastrophic disaster that will strike your company when your
rivals gain access to your confidential information.
This will be the end of you. Make no mistake: you are running out of
time. Pay now, or face total ruin.
```

Ransom note of .Midnight variant



```
Your data has been stolen and encrypted by EndPoint Ransomware...We will
delete the stolen data and help with the recovery of encrypted files
after payment has been madeContact me through the following this utox id(6
615A0[redacted]
9)Do not try to change or resotre files yourself,this will break themWe
provide free decryption for any 3 files up to 3MbThe final price depepnds
on how fast you write to us..Good Luck...
```

Ransom note of .endpoint variant

Additional indicators include the creation of a mutex named Mutexisfunnylocal, which is used to prevent multiple instances of the ransomware from running simultaneously. Some samples also drop a debug log on the infected system, depending on the configuration. Known variants have been observed creating either Report.Midnight or debug.endpoint as log files.

A full list of discovered samples is available in the IoCs section at the end of this article.

Cryptographic Design and Flaws

While Midnight's core structure and execution flow is largely inherited from Babuk, its cryptographic implementation has been significantly reworked. These changes introduced flaws that make file decryption possible, which we leveraged to develop a working decryptor.

Midnight uses ChaCha20 for encrypting file contents and RSA for encrypting the ChaCha20 key. The RSA-encrypted key, along with its SHA256 hash, is appended to the end of each encrypted file. This format is consistent across known samples.

To improve performance, Midnight employs intermittent encryption, a technique also used by Babuk. However, Midnight refines this approach by applying a more granular file size-based logic to determine which portions of file to encrypt. This allows it to process large files faster while still rendering them unusable.

The ransomware accepts several command-line arguments to control its behavior:

- /e appends the extension string (e.g. .Midnight) directly to the file content instead of modifying the filename.
- /n enables encryption of network-mounted volumes.
- --paths=PATHS targets specific directories for encryption.

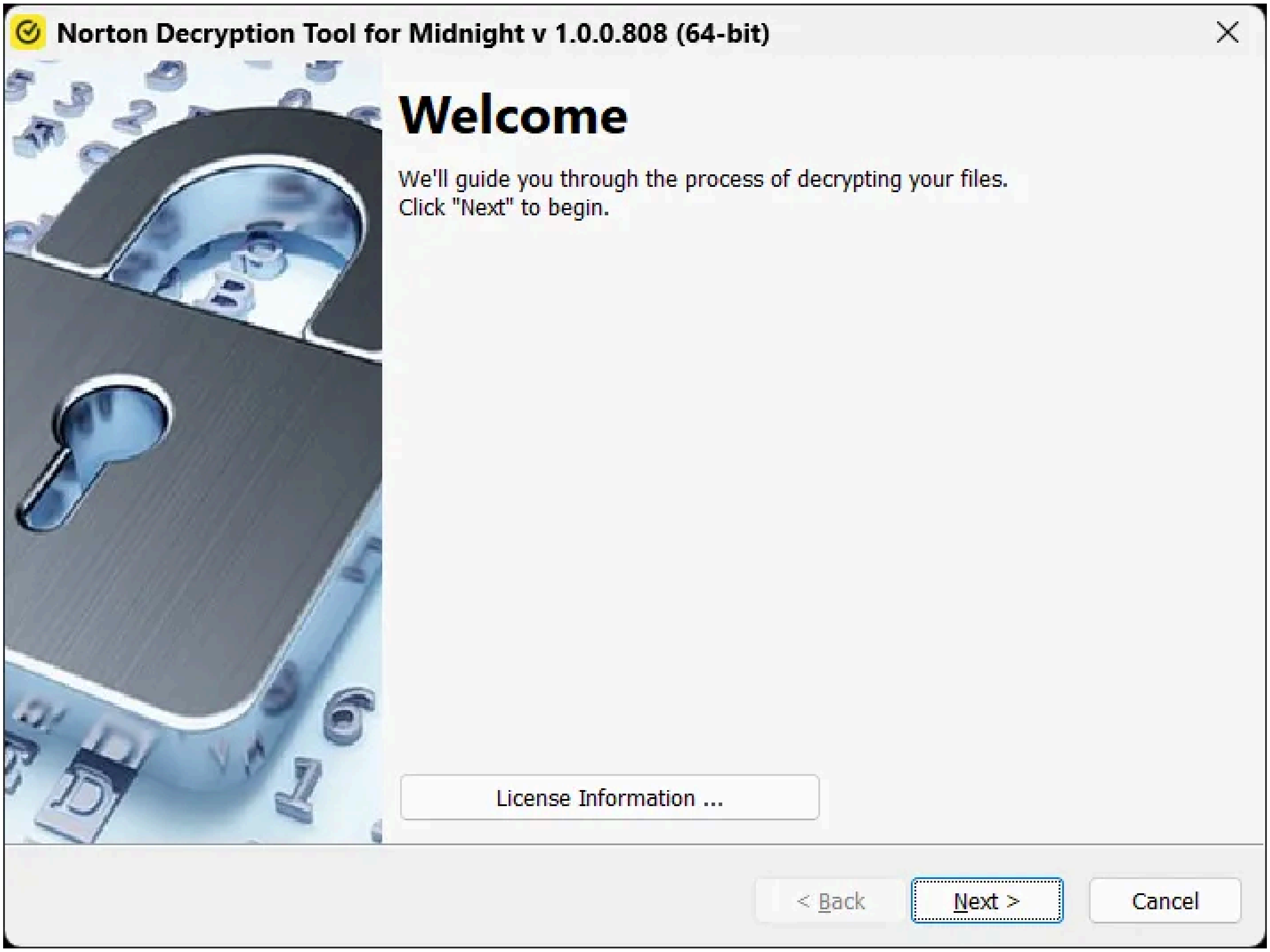
Earlier samples of Midnight primarily targeted high-value files such as databases, backups, and archives. These included the following extensions:

.mdf .ndf .bak .dbf .dmp .rman .frm
.ibd .myd .myi .sql .xbk .ldf .vbi
.vbk .ibdata .rar .md5 and .bitmap

More recent variants have broadened their scope and now encrypt nearly all file types, with the exception of executables such as .exe, .dll, and .msi.

How to Use the Ransomware Decryptor

1. Download the decryptor here. If you still use 32-bit Windows, you can also get the 32-bit version of the decryptor here.
2. Run the decryptor, preferably as an administrator. 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.

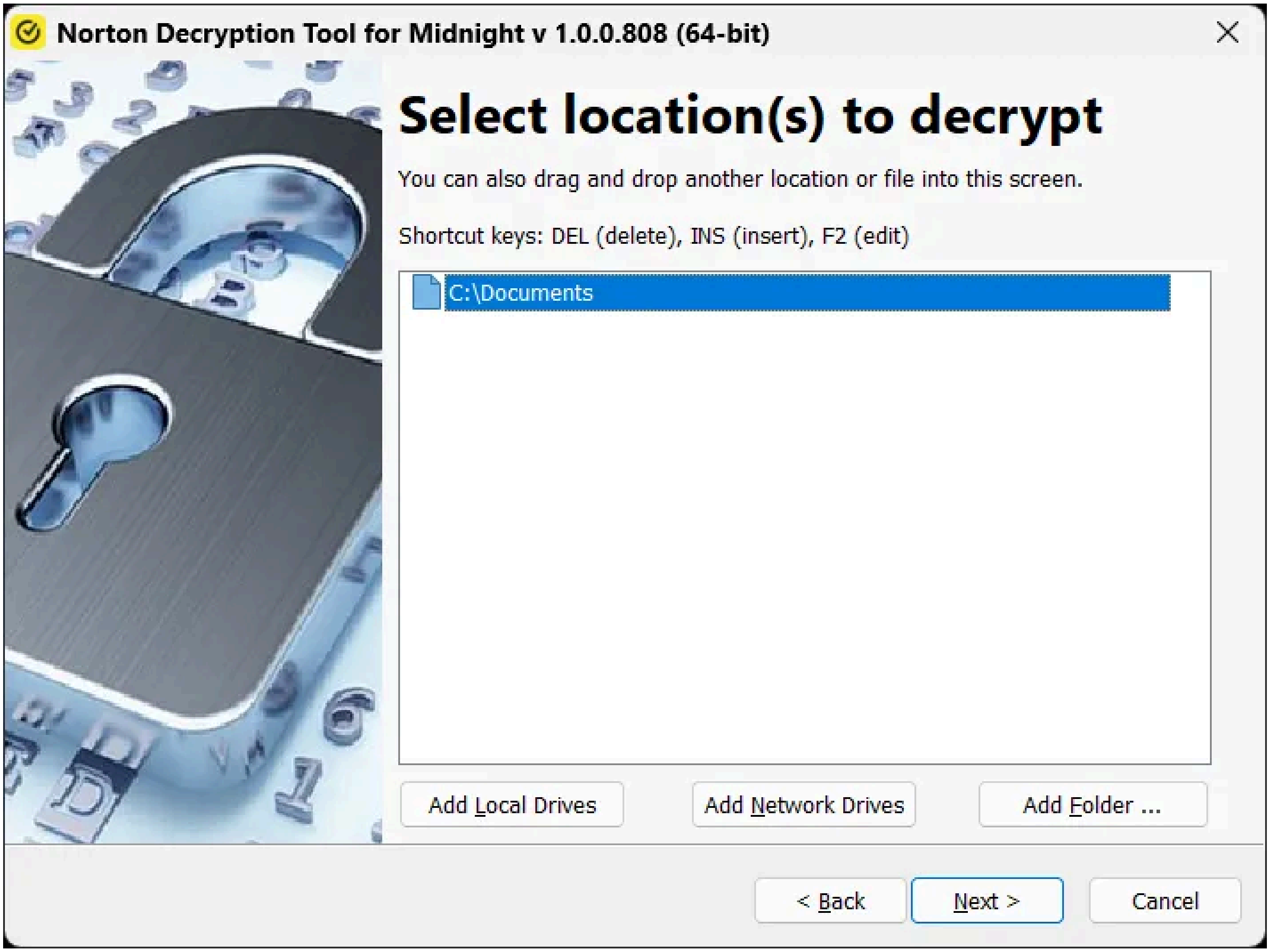


Norton Decryption Tool for Midnight v 1.0.0.808 (64-bit)

Welcome

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

4. On the next page, the user is asked to provide a list of locations (drives, folders, files) that are to be decrypted. By default, the decryptor provides a list of all local disk drives.



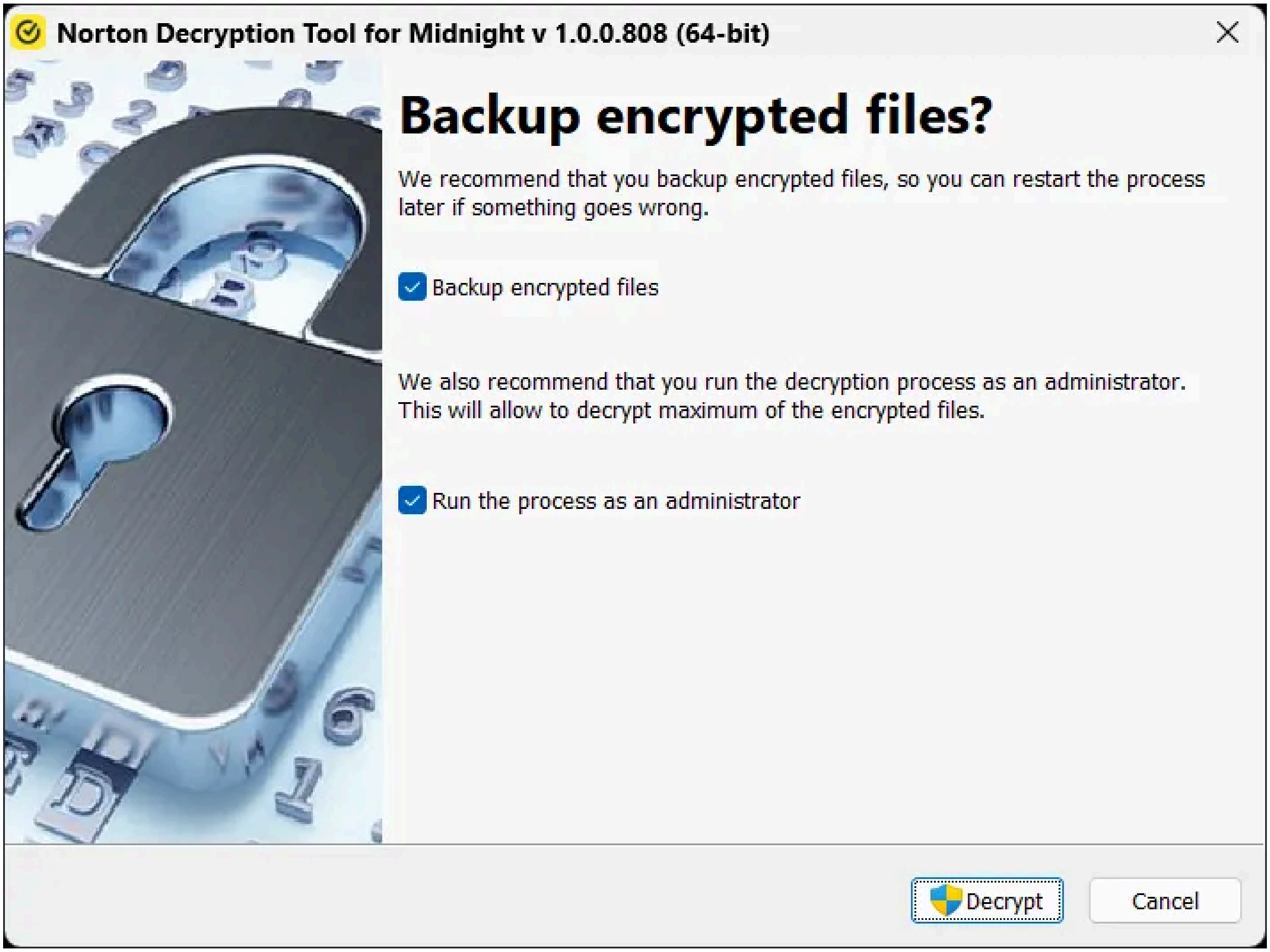
Select location(s) to decrypt

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

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

C:\Documents

5. 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 selected 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.



Backup encrypted files?

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

☑ Backup encrypted files

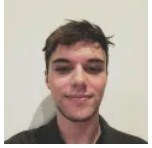
We also recommend that you run the decryption process as an administrator. This will allow to decrypt maximum of the encrypted files.

☑ Run the process as an administrator

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

IoCs: Ransomware Samples

dd9de77c6e17093b0b2150b3f0c66e8526369ba68fb7b9a5758ff9274d85342e
3d9a71cfec82fef531227465f40d9106e671ef162fa3ab21119e2ee08612e0aa
300c46bf17e8bd0cd5ac800a33e1d27ef9001aecef1f98965414bf9c33af19e0
1e58448808006de410ddb31a4d6ff8292aa70168f69f2b7e08144d6090d5084d
aa8a043fd3d64fc96864cf5361bbb82012cc4b2e1a909c747038edcf2b4369e7



Samuel Vojtáš

Malware Analyst at Gen