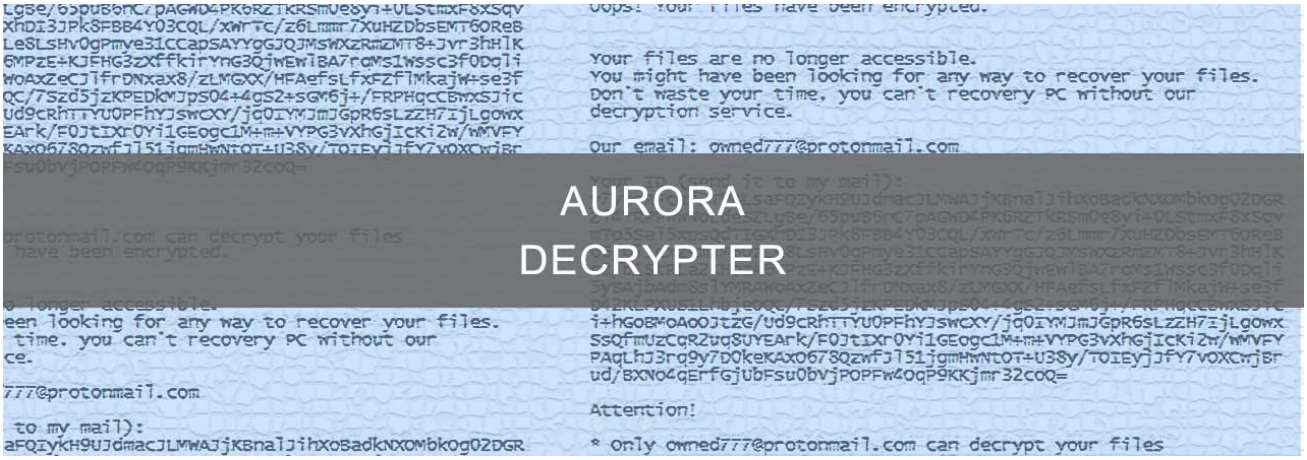
How to Decrypt the Aurora Ransomware with AuroraDecrypter

bleepingcomputer.com/ransomware/decryptor/how-to-decrypt-the-aurora-ransomware-with-auroradecrypter/

Lawrence Abrams

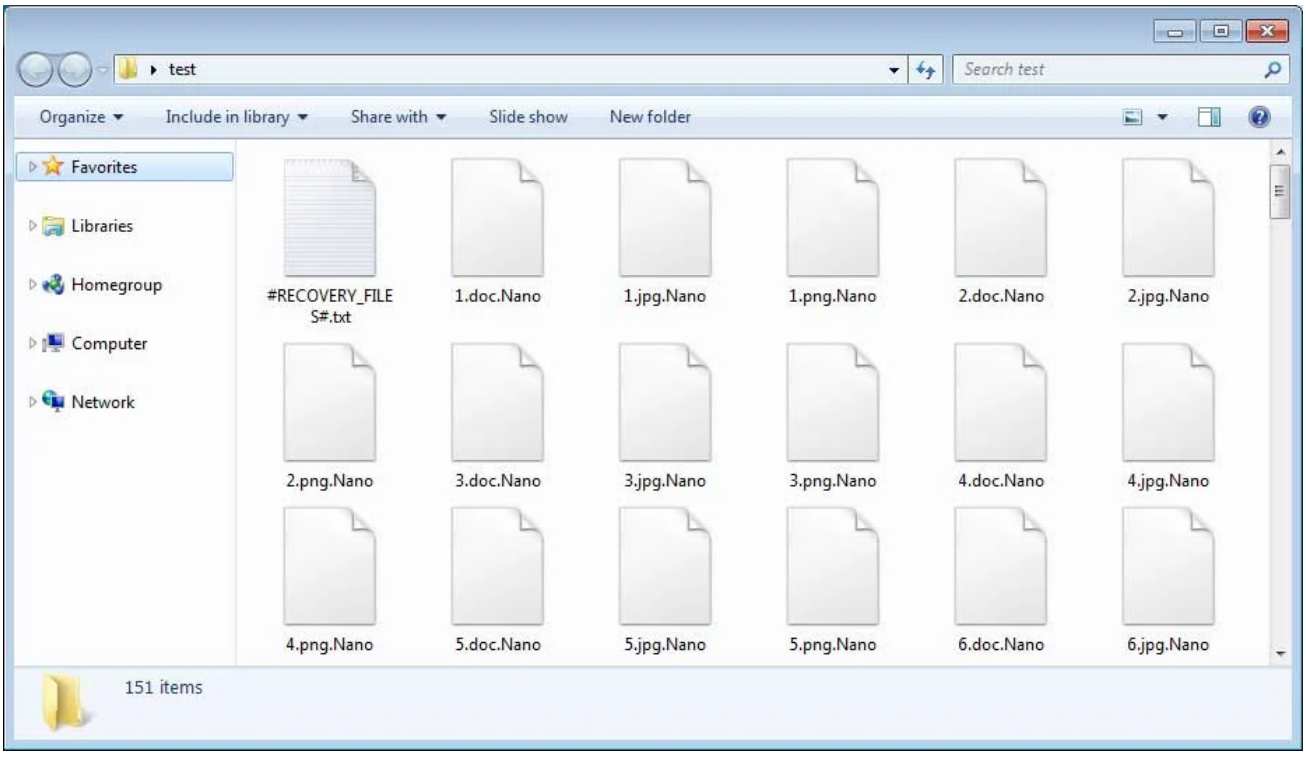
By
Lawrence Abrams

- January 4, 2019
- 11:35 AM
- 1



The Aurora Ransomware is a Windows infection that encrypts your files and then demands a ransom in bitcoins in order to get the decryption key. This ransomware has had numerous variants released with the most active current one being the one that appends the .Nano extension.

The Aurora Ransomware family is spread by attackers hacking into computers running Remote Desktop Services. Once they gain access to a computer, they install the ransomware and encrypt any files that they gain access to. Once files are encrypted they will have an extension appended to the file names and a ransom note will be created on the Windows desktop and in various folders on the computer.



Encrypted .Nano Files

The good news is that the variants of this ransomware family can be decrypted for free using a decryptor created by Michael Gillespie. In order to use the decryptor a victim just needs to have two encrypted files of a certain file type, which will be described later in the guide.

The currently supported variants are the ones that append the following extensions to the names of encrypted files.

```
.Nano
.animus
.Aurora
.desu
.ONI
.aurora
```

To learn how to decrypt files encrypted by the Aurora Ransomware, please use the guide below.

How to Decrypt the Aurora Ransomware

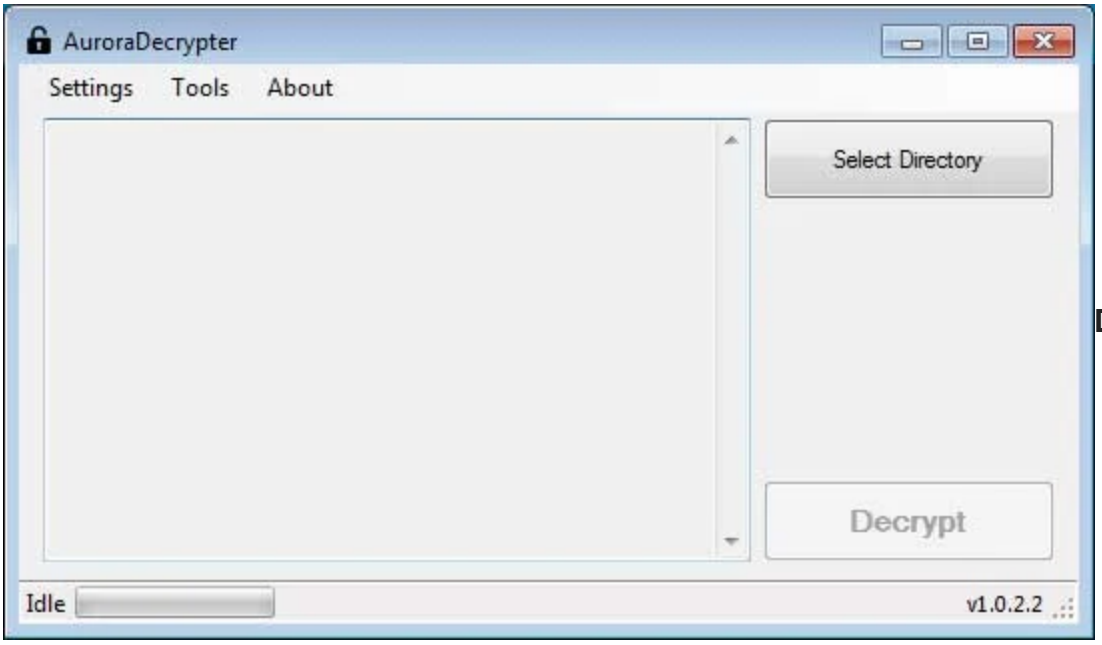
Victims of the Aurora Ransomware can be identified by having their files encrypted and renamed to have a .Nano, .animus, .Aurora, .desu, .ONI, or .aurora extension.

To decrypt files encrypted by the Aurora ransomware, you need to first download the Aurora Decryptor below.

AuroraDecrypter

Download Now

Once downloaded, simply double-click on the executable to start the decryptor and you will be greeted with the main screen.



Decryptor Screen

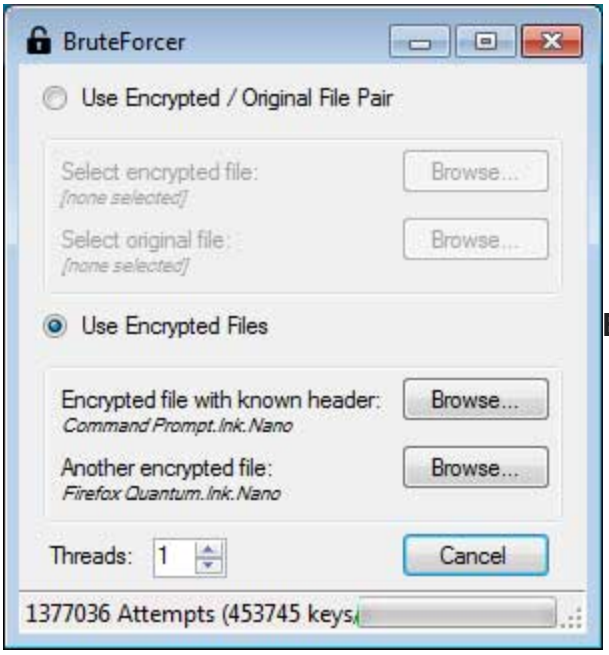
In order to brute force the decryption key, we need two encrypted files of a certain file types. The supported file types are:

```
.png, .gif, .pdf, .docx, .xlsx, .pptx, .doc, .xls, .ppt, .vsd, .psd, .mp3, .wmv,
.zip, .rar, .pst, .rtf, .mdb, .ico, .lnk, .fdb, .jar, and .idx
```

Once you have located two of one of the above file types, click on the **Settings** menu and select **Bruteforcer**. This will open a screen where you should select two encrypted files as illustrated below.

Select files to bruteforce

Once you have selected both files, click on the **Start** button to begin brute forcing the decryption key. This process can take quite a while, so please be patient.

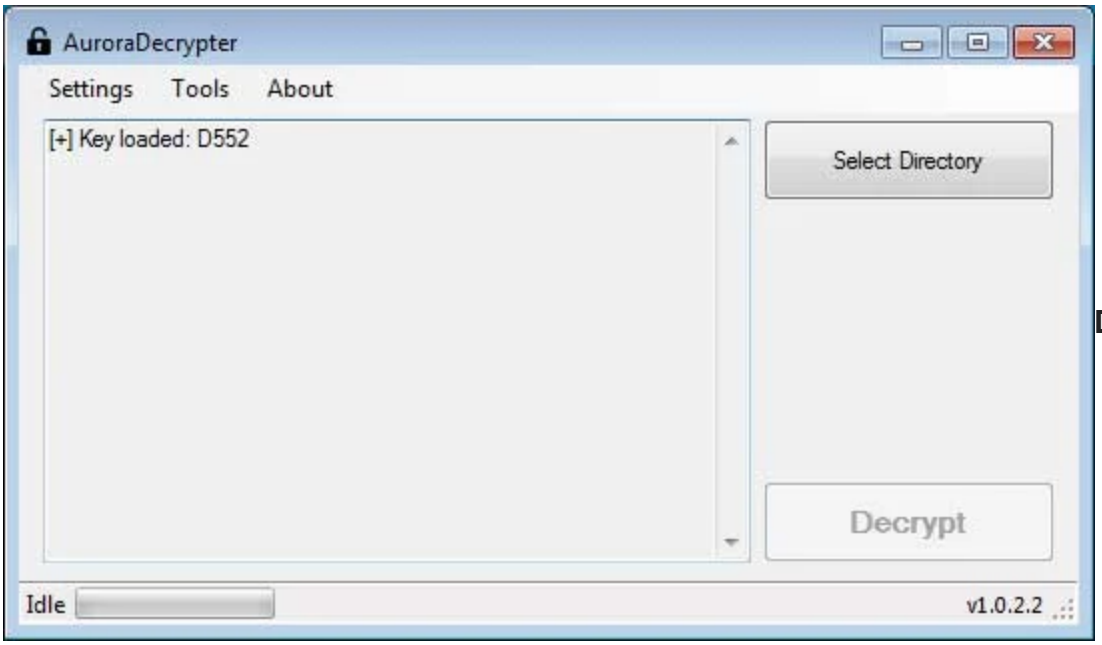


Bruteforcing Key

When finished, the decryptor will state that a decryption key has been found.

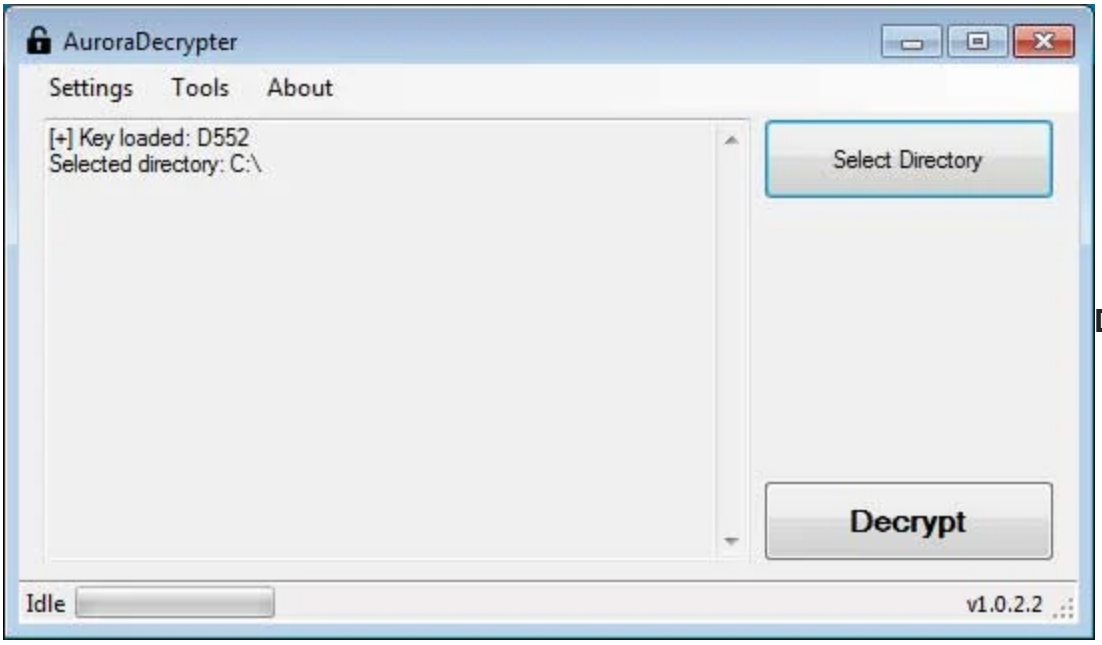
Decryption Key Found

Now click the **X** button to close the BruteForcer window and the key will be loaded into the decryptor as shown below.



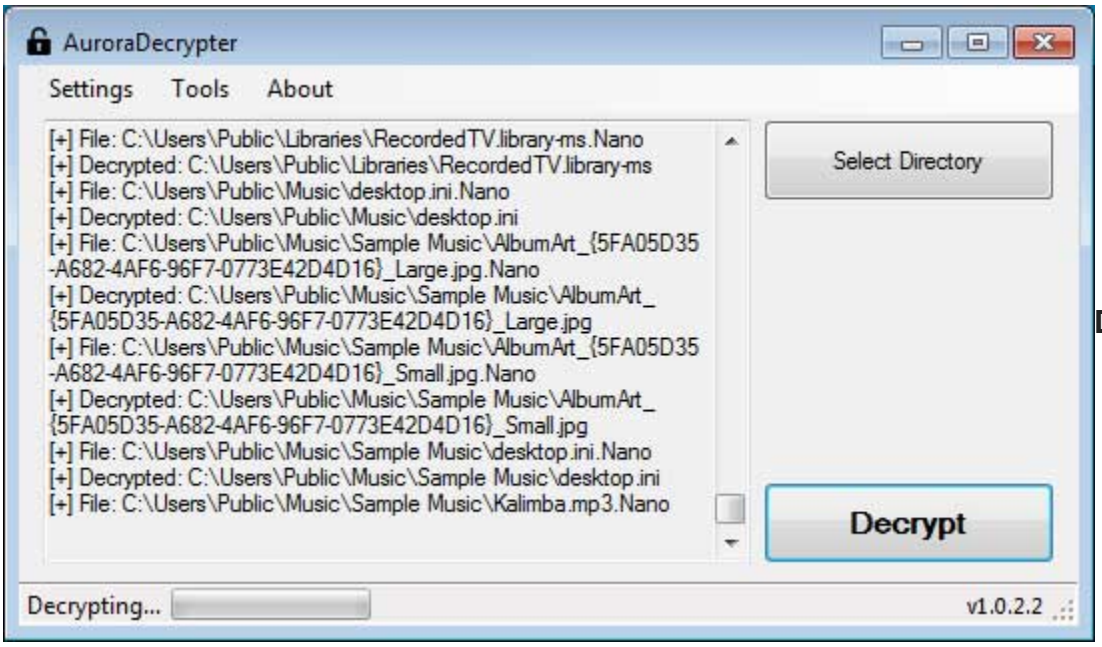
Decryption Key Loaded

We now need to select a directory to decrypt by clicking on the **Select Directory** button. If you wish to decrypt an entire drive, simply select the drive letter itself. For example, in the image below you can see that we selected the C:\ drive.



Drive Selected

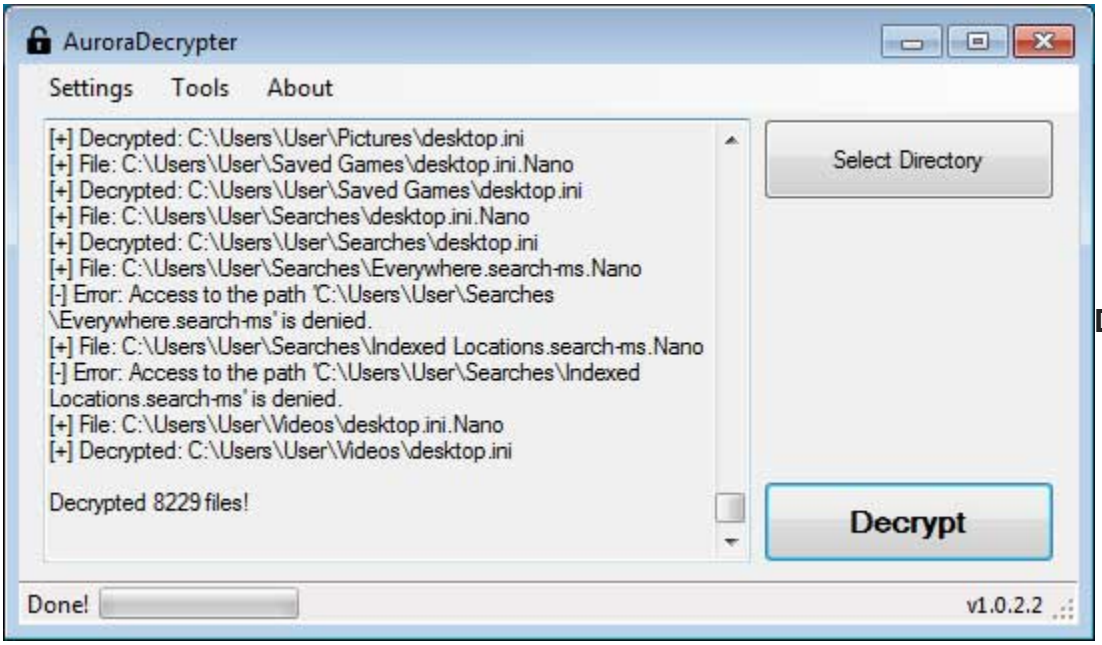
When ready, click on the **Decrypt** button to begin decrypting the Aurora Ransomware encrypted files. Once you click Decrypt, the program will decrypt all the encrypted files and display the decryption status in the window. This is illustrated below where you see files encrypted by the Nano variant of Aurora being decrypted.



Decrypting

Aurora Encrypted Files

When it has finished, the decryptor will display a summary of the amount of files that have been decrypted. If some of the files were skipped it may be due to permissions to the files.



Decryption

Finished

Though your files are now decrypted, the original encrypted files will still be on your computer. Once you confirm that your files have been properly decrypted, you can use CryptoSearch to move all the encrypted files into one folder so you can delete or archive them.

You can now close the decryptor and use your computer as normal. If you need help using this decryptor, feel free to leave a comment.

Related Articles:

Free decryptor released for Yanluowang ransomware victims

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

- Aurora
- AuroraDecrypter
- Decrypted
- Decryptor
- Nano
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

achzone - 3 years ago

Great news and article Lawrence! This once again lends credence to what I've always maintained about Ransomware. Backups should always be kept because one should never say never and assume their files are lost to these criminals.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: