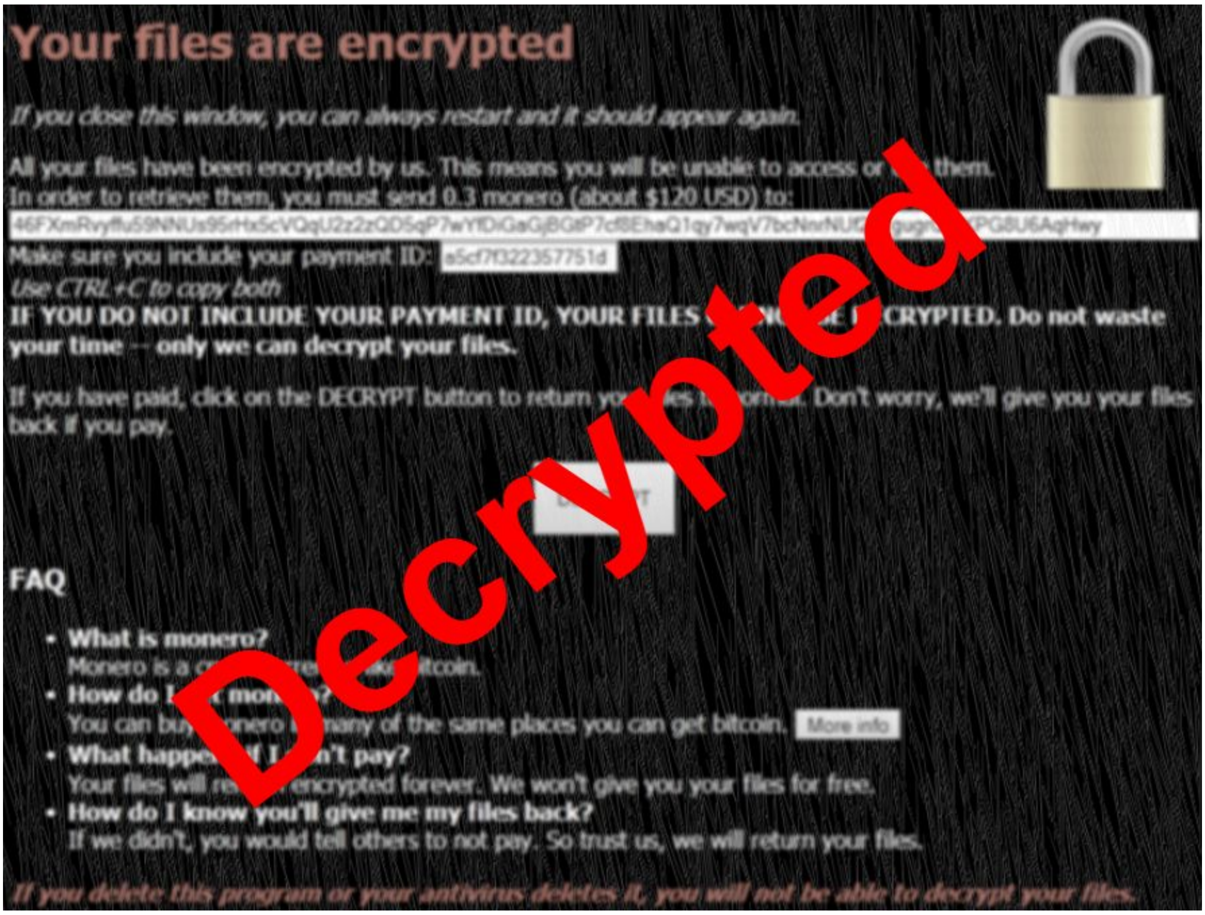


Your files are encrypted

If you close this window, you can always restart and it should appear again.

All your files have been encrypted by us. This means you will be unable to access or [illegible] them.
In order to retrieve them, you must send 0.3 monero (about $120 USD) to:
46FXmRvyffu59NNUs95rHx5cVQqU2z2zQD5qP7wYfDiGaGjBGtP7cf8EhaQ1qy7wqV7bcNnrNU[illegible]gugn[illegible]PG8U6AqHwy
Make sure you include your payment ID: a5cf7f3223577751d
Use CTRL+C to copy both
IF YOU DO NOT INCLUDE YOUR PAYMENT ID, YOUR FILES [illegible] CRYPTED. Do not waste your time -- only we can decrypt your files.

If you have paid, click on the DECRYPT button to return yo[illegible] [illegible] Don't worry, we'll give you your files back if you pay.

FAQ

- **What is monero?**
  Monero is a c[illegible] re[illegible] itcoin.
- **How do I [illegible] mon[illegible]?**
  You can buy [illegible]onero [illegible] many of the same places you can get bitcoin.
- **What happe[illegible] if I [illegible]n't pay?**
  Your files will re[illegible] encrypted forever. We won't give you your files for free.
- **How do I know you'll give me my files back?**
  If we didn't, you would tell others to not pay. So trust us, we will return your files.

If you delete this program or your antivirus deletes it, you will not be able to decrypt your files.

After analysis of the MoneroPay ransomware, we managed to patch the binary to turn it into decryptor.

The ransomware and password stealer in one detected as MoneroPay impersonates itself as the SpriteCoin cryptocurrency. The fraud was discovered by on January 13, 2018.

The original ransomware uses the Salsa20 crypto algorithm to encrypt files. The MoneroPay generates 128-bit key based on C&C address ‘jmqapf3nflatei35.onion’, %COMPUTERNAME%, %USERNAME%, and %USERPROFILE% strings. Therefore, it is essential to run the MoneroPay decryptor on the same computer from where the files have been encrypted.

To decrypt the files encrypted by MoneroPay ransomware follow the steps below:

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

1. Backup copies the encrypted files that have the extension ‘.encrypted’.

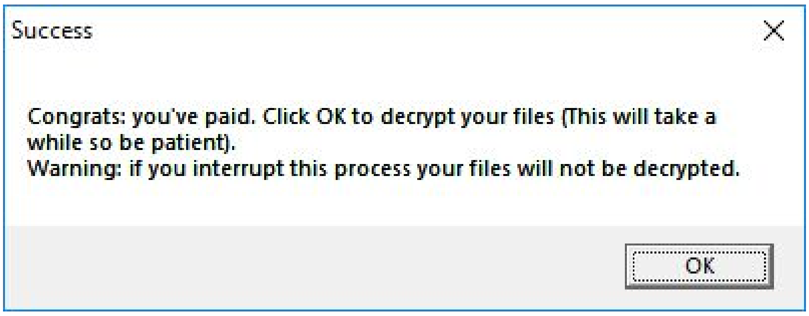
2. Download the archive with the decryptor from the GitHub: https://github.com/AlexanderAda/Ransomware-Decryptors/tree/master/MoneroPay

3. Unpack the archive using the password ‘infected’.

   <u>Note</u>: The decryptor is the patched version of the cryptolocker and can be detected as the MoneroPay ransomware by your antivirus.

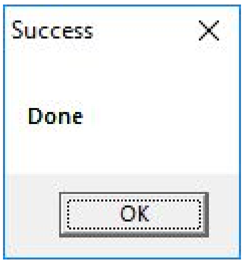
4. Run the decryptor ‘spritecoind_decryptor.exe’ (MD5: 3749d56abd58dff3d248b91b24da76d7) on an infected machine.

   a. Once executed, the decryptor shows the message to notify you about starting the decryption process.

   Congrats: you've paid. Click OK to decrypt your files (This will take a while so be patient).
   Warning: if you interrupt this process your files will not be decrypted.

   b. After successful decryption, it shows the message with the status ‘Done’.

   Done

To clean up the computer that was previously infected by the MoneroPay ransomware:

1. Delete the ‘MoneroPay’ autorun reference in the Windows System Registry:

   [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
   ‘MoneroPay’ = ‘C:\Users\<USER>\AppData\Roaming\MoneroPayAgent.exe’

2. Delete the ransomware file:

   C:\Users\<USER>\AppData\Roaming\MoneroPayAgent.exe

Should you have any questions, please email to: ada@nioguard.com

References

- https://www.acronis.com/en-us/blog/posts/spritecoin-new-ransomware-not-cryptocurrency

- https://blog.fortinet.com/2018/01/22/spritecoin-another-new-cryptocurrency-or-not
- https://www.bleepingcomputer.com/news/security/moneropay-ransomware-disguised-as-wallet-for-fake-spritecoin-cryptocurrency/
- http://id-ransomware.blogspot.com/2018/01/moneropay-ransomware.html
- https://sensorstechforum.com/remove-moneropay-virus-spritecoin-restore-encrypted-files/