Quick and painless - reversing deathransom /

By f0wL

Published: 2019-11-19 · Archived: 2026-04-05 15:26:13 UTC

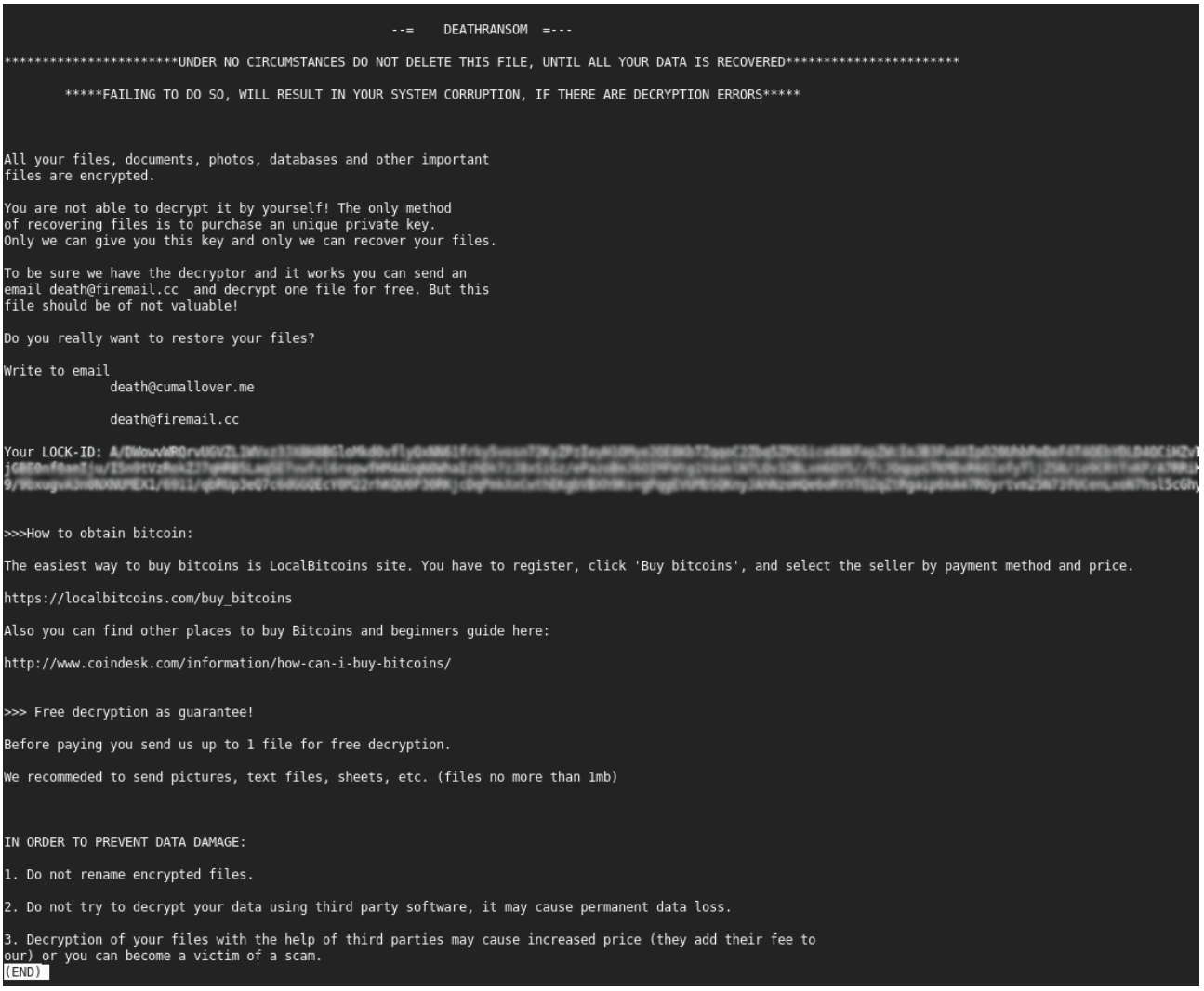
Tue 19 November 2019 in Ransomware

No flashy wallpapers or other bells and whistles, but if you aren't careful and maintain backups as you should DeathRansom will take your data with it to its grave. Or will it ?

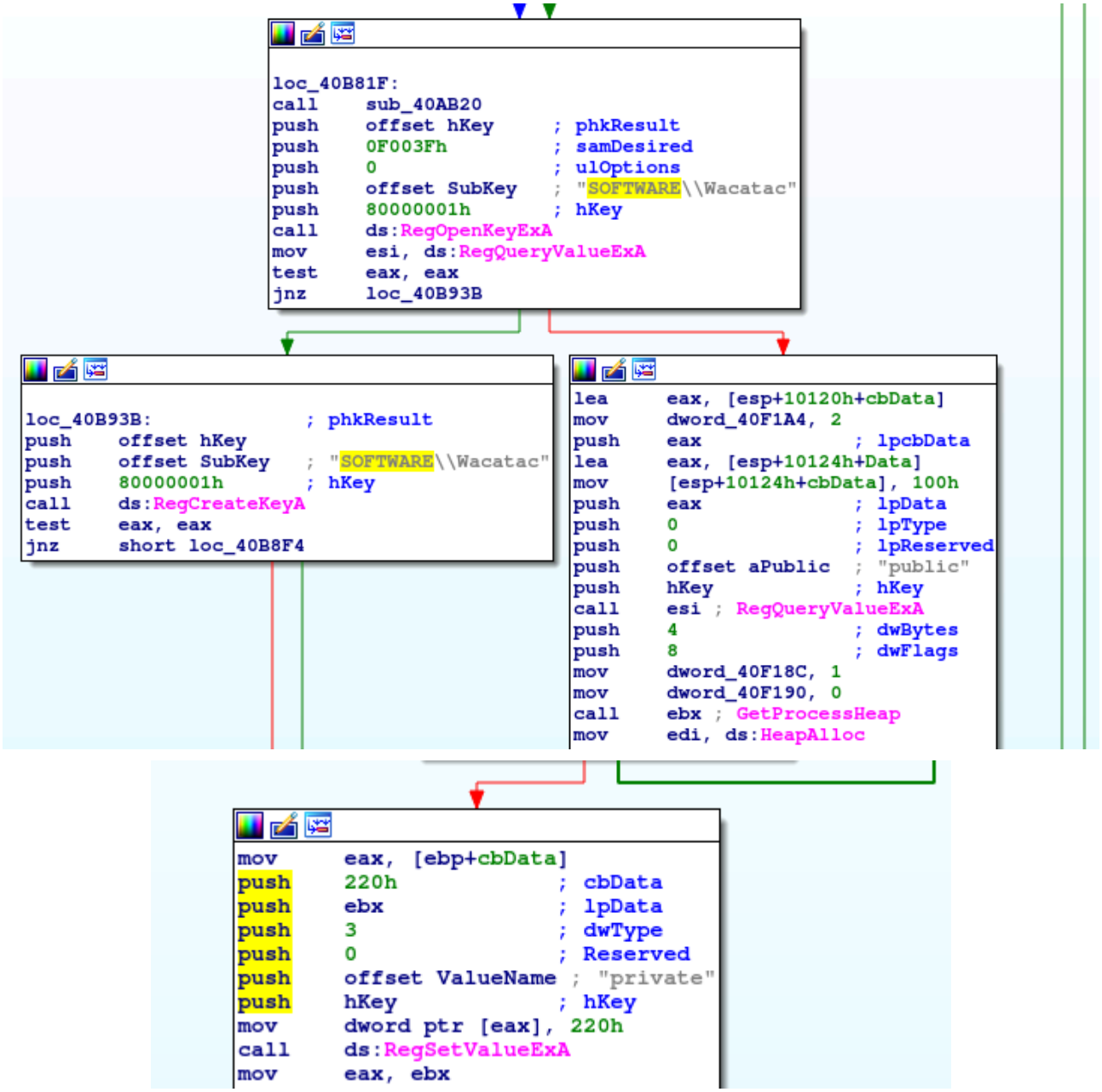
A general disclaimer as always: downloading and running the samples linked below will lead to the encryption of your personal data, so be f$cking careful. Also check with your local laws as owning malware binaries/ sources might be illegal depending on where you live.

DeathRansom @ AnyRun | VirusTotal | HybridAnalysis --> `sha256 3a5b015655f3aad4b4fd647aa34fda4ce784d75a20d12a73f8dc0e0d866e7e01`

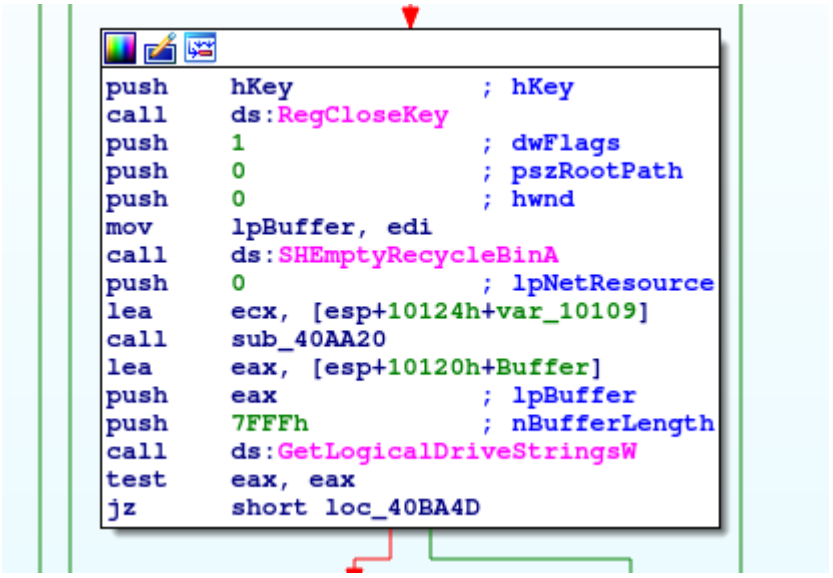
The plain text note doesn't look that special. I'll be refering to this strain as Deathransom, since the Wacatac Trojan doesn't seem to be affiliated with the sample.



The "Wacatac" Registry Keys are most likely an attempt at a false flag manouver. The Ransomware will set three Regkeys in total: The main Key **HKEY_CURRENT_USER\SOFTWARE\Wacatac** and two sub keys called **private** and **public**. The hex value set in the "private" acutally corresponds to the Lock ID referenced in the Ransomnote. Analysing the encryption loop will probably present the relation between these values, so I'll keep going.

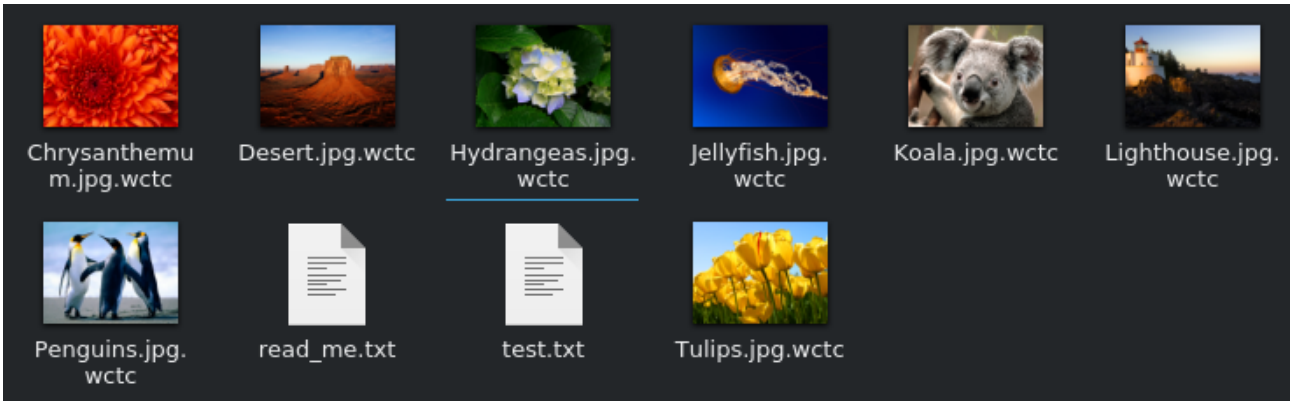


Somewhat of a rare occurance, but Deathransom will actually take out the trash for you by clearing the recycling bin.



Generally this sample seems to be very limited in features, but let's see how they implemented the encryption routine. Looking for *CreateFileW* we can see that it appends the *.wctc* extension to the name of the current file. But where's the encryption happening? Either they hid it very well or they just plainly forgot about it 🤔

Let's just fire up a VM and see what happens to the files after the encryption takes place so we have a better idea of what to look for. I got no UAC prompt upon running the sample and the ransom process seemed a bit fast. Checking out the sample files we can see what actually happened:

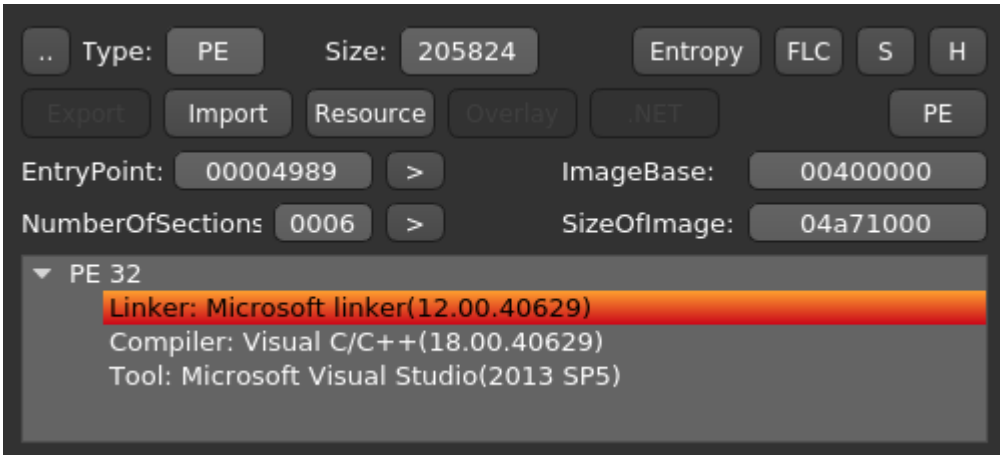


Exactly, nothing. I don't want to jump to conclusions here, but this strain might still be in the testing stage or is just a plain hoax. Regardless it is still possible that another variant turns up that will actually encrypt the files.

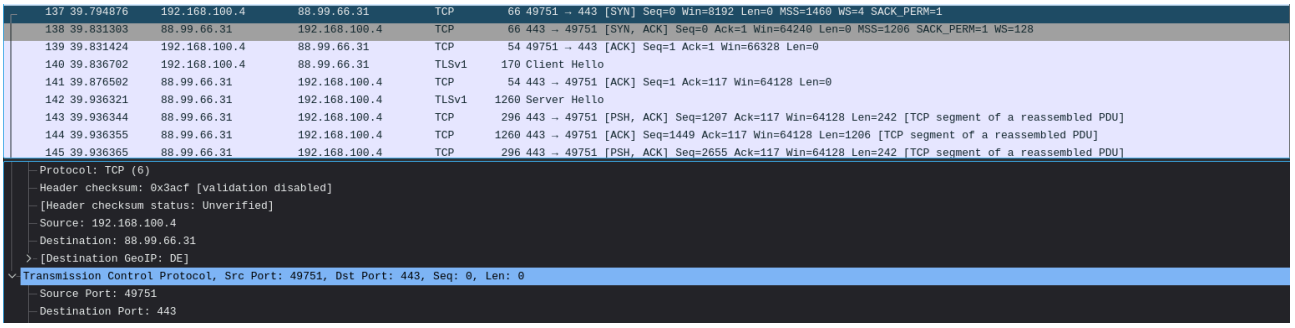
Update 25.11.2019:

As predicted there is another version of the Ransomware available now and it seems to do its job a lot more thorough than its predecessor. The new build doesn't seem to append a new suffix to the file and the ransomnote has been adapted slightly because it now features a Bitcoin wallet address and a new E-Mail contact.

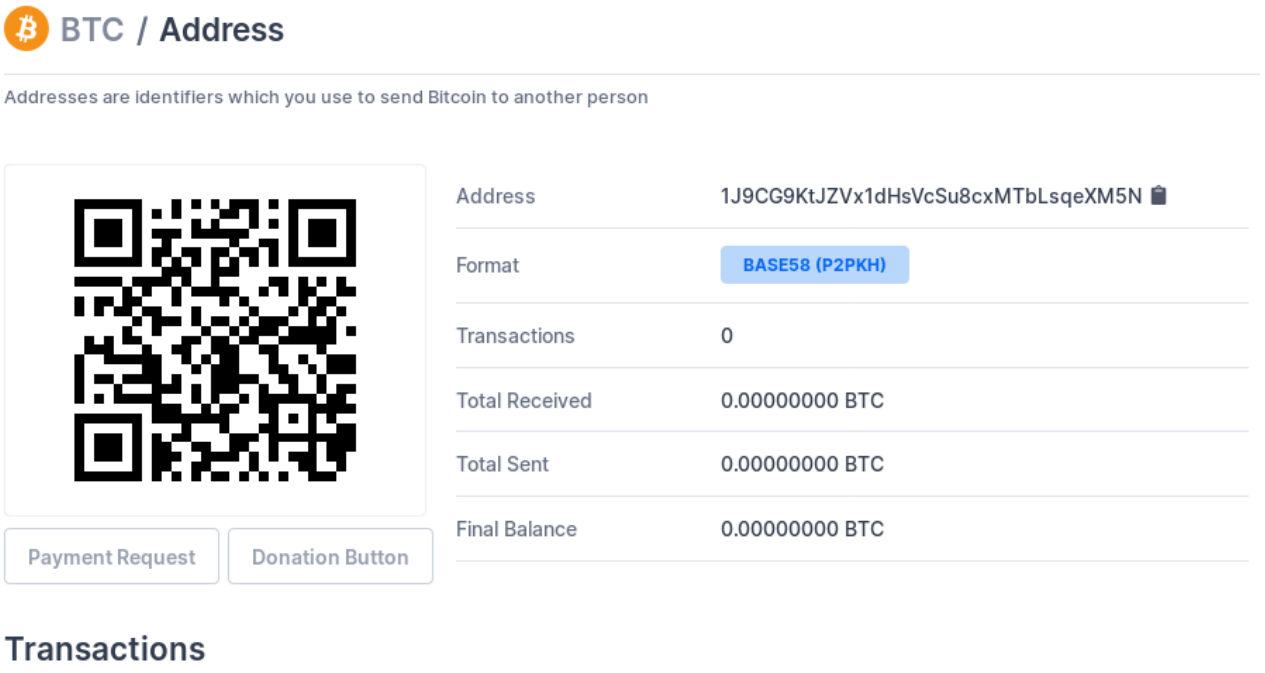
DeathRansom V2 @ AnyRun --> `sha256`
`fedb4c3b0e080fb86796189ccc77f99b04adb105d322bddd3abfca2d5c5d43c8`



Entropy-wise the sample doesn't seem to be packed and nor are there any weird sections or paddings. Compiler and Linker Versions point towards Visual Studio 2013 being utilized by the creators.



Looking at the packets captured during the dynamic analysis we notice a DNS request plus TCP traffic to iplogger[.]org which was not present in the first Version of the Ransomware. Looks like the criminals are trying to track infections over time.



According to Blockchain.com the Bitcoin Wallet mentioned in the V2 Ransomnote doesn't have any transactions on it as of the 30th of November, which is really good news :)

IOCs

DeathRansom

```
deathransom.exe --> SHA256: 7c2dbad516d18d2c1c21ecc5792bc232f7b34dadc1bc19e967190d79174131d1
                    SSDEEP: 1536:gZVYb2bbBisyEcPC00h7sBvvKk+jTc7+T8l7RJV62CzVDL+oWB27evMCUQ:EV+GiVEc

fyukfuyk.exe    --> SHA256: ab828f0e0555f88e3005387cb523f221a1933bbd7db4f05902a1e5cc289e7ba4
                    SSDEEP: 6144:f849/IB5jZozuL1itPJAOsF0l+t5Dn0ChC:f8kIB5jZyNVJWF0AHDC

2p1km7pr6l.exe  --> SHA256: fedb4c3b0e080fb86796189ccc77f99b04adb105d322bddd3abfca2d5c5d43c8
                            3072:ou1DaA5w1KmC5RjPquqavANItF2rv8ojAjAD5m9:Kb6Lq8wHUoe
```

E-Mail Addresses

```
death@firemail[.]cc
death@cumallover[.]me
```

```
deathransom@airmail[.]cc
```

Registry Keys

```
HKEY_CURRENT_USER\SOFTWARE\Wacatac

HKEY_CURRENT_USER\SOFTWARE\Wacatac\public
FA DE 13 AA 52 43 DF 85  B2 62 A5 88 1D 17 D0 59 99 BF 6B 69 5F 71 1C 76  D4 4A 36 86 B6 47 CA D4 A2

HKEY_CURRENT_USER\SOFTWARE\Wacatac\private
03 F0 D6 A3 0B D6 45 0A  EF 50 65 59 2F 55 95 C7 3D C9 5F C1 FC 04 69 68  32 47 74 BD F9 72 43 13 4D
```

Ransomnote Version 1

```
                                                --=    DEATHRANSOM  =---

**********************UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVE

    *****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****



All your files, documents, photos, databases and other important
files are encrypted.

You are not able to decrypt it by yourself! The only method
of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recover your files.

To be sure we have the decryptor and it works you can send an
email death@firemail.cc  and decrypt one file for free. But this
file should be of not valuable!

Do you really want to restore your files?

Write to email
              death@cumallover[.]me

              death@firemail[.]cc

Your LOCK-ID: [Redacted Base64]

>>>How to obtain bitcoin:

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', a
```

```
hxxps://localbitcoins[.]com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

hxxp://www.coindesk[.]com/information/how-can-i-buy-bitcoins/


>>> Free decryption as guarantee!

Before paying you send us up to 1 file for free decryption.

We recommeded to send pictures, text files, sheets, etc. (files no more than 1mb)



IN ORDER TO PREVENT DATA DAMAGE:

1. Do not rename encrypted files.

2. Do not try to decrypt your data using third party software, it may cause permanent data loss.

3. Decryption of your files with the help of third parties may cause increased price (they add their
our) or you can become a victim of a scam.
```

Ransomnote Version 2

```
????????????????????????????
??????DEATHRansom ???????
????????????????????????????
Hello dear friend,
Your files were encrypted!
You have only 12 hours to decrypt it
In case of no answer our team will delete your decryption password
Write back to our e-mail: deathransom@airmail[.]cc


In your message you have to write:
1. YOU LOCK-ID: PUmZiYT3OkC9IpVXHpZFOFzZ5Y7+dLuV9cYUSZ30UyPLeMPEPO4TZ79CCCbiTpSltqKKBv3oFqgH0O6lyre7
2. Time when you have paid 0.1 btc to this bitcoin wallet:
1J9CG9KtJZVx1dHsVcSu8cxMTbLsqeXM5N


After payment our team will decrypt your files immediatly
```

```
Free decryption as guarantee:
1. File must be less than 1MB
2. Only .txt or .lnk files, no databases
3. Only 1 files


How to obtain bitcoin:
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', a
hxxps://localbitcoins[.]com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
hxxp://www.coindesk[.]com/information/how-can-i-buy-bitcoins/
```

Gallow Icon made by [Freepik](#) from www.flaticon.com
