“Troldesh” – New Ransomware from Russia

blog.checkpoint.com/2015/06/01/troldesh-new-ransomware-from-russia/

June 1, 2015

Overview

“Troldesh”, aka Encoder.858 or Shade, is a Trojan and a crypto-ransomware variant created in Russia and spread all over the world.

Troldesh is based on so-called encryptors that encrypt all of the user’s personal data and extort money to decrypt the files. Troldesh encrypts a user’s files with an “.xtbl” extension. Troldesh is spread initially via e-mail spam.

A distinctive feature of the Troldesh attack is direct communication with the victim. While the most Ransom-Trojan attackers try to hide themselves and avoid any direct contact, Troldesh’s creators provide their victims with an e-mail address. The attackers use this email correspondence to demand a ransom and dictate a payment method.

In this report you’ll learn about the infection procedure, the primary symptoms, and you will find out how I ended up getting a discount from the hackers.

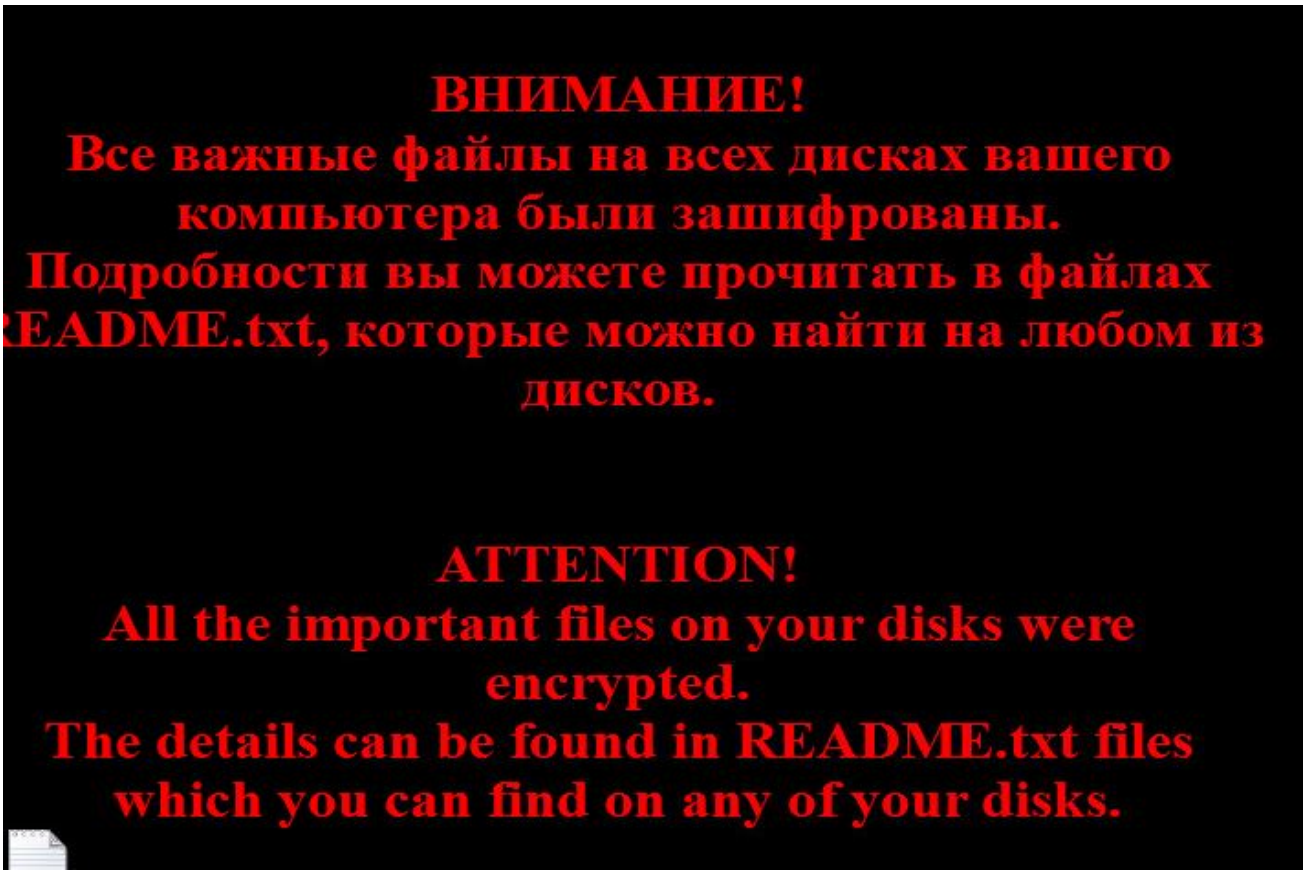
The Infection Process

As mentioned previously, Troldesh is a Trojan which encrypts all the user’s data and demands a ransom in exchange for decryption.

In my research, I used a malicious sample with this hash downloaded from VirusTotal:
a8b27aa4fe7df15a677f9ab9b62764d557525059a9da5f4196f1f15049e2b433

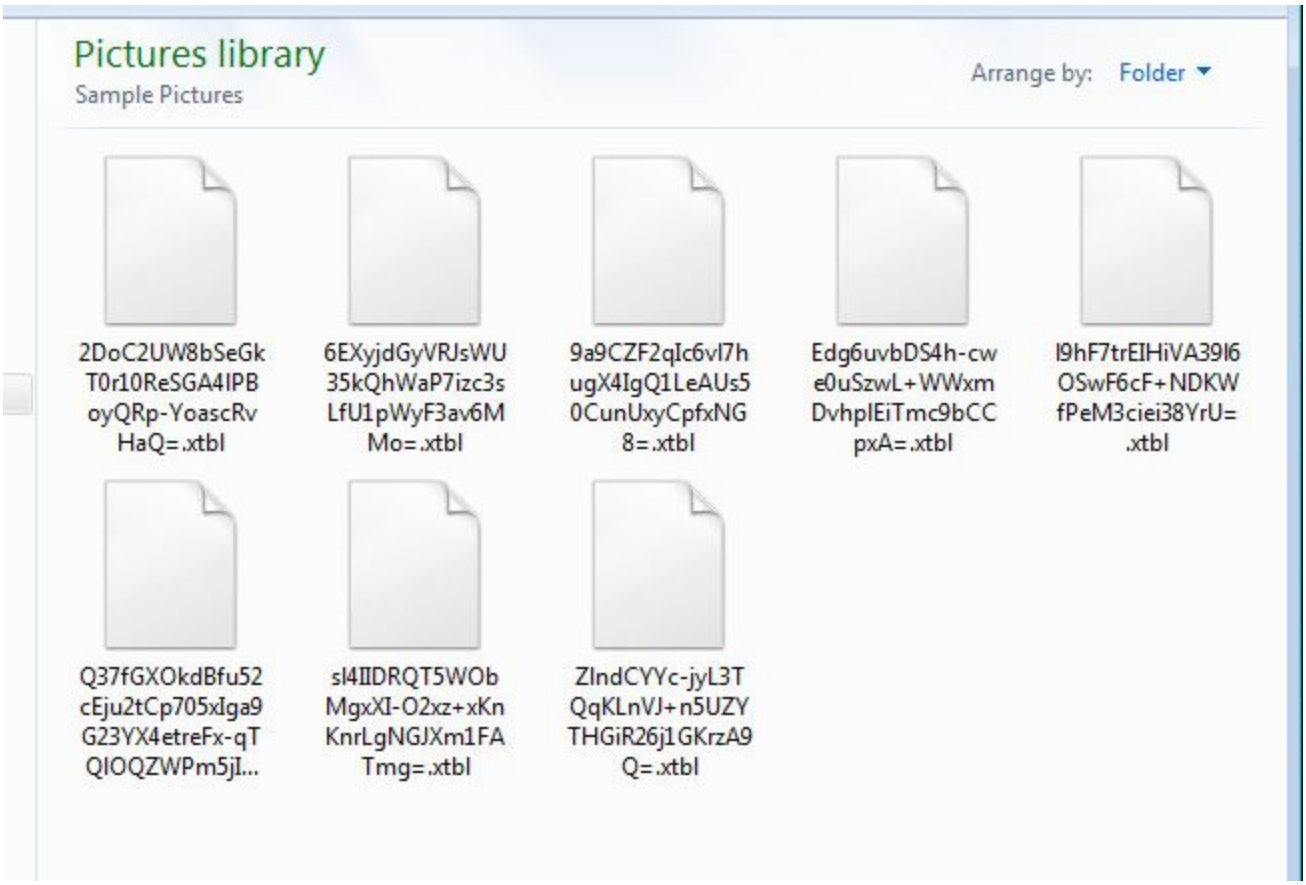
After execution, Troldesh encrypts all of the user's data and displays this message:

Additionally, it renames the encrypted files using this format: *[random characters]=.xbtl* For example, this is a screenshot of my machine's "Pictures" folder with the encrypted files:



Approximately 20 *txt* files were placed on my desktop. In other cases, a *txt* file was placed in each folder that had an encrypted file.

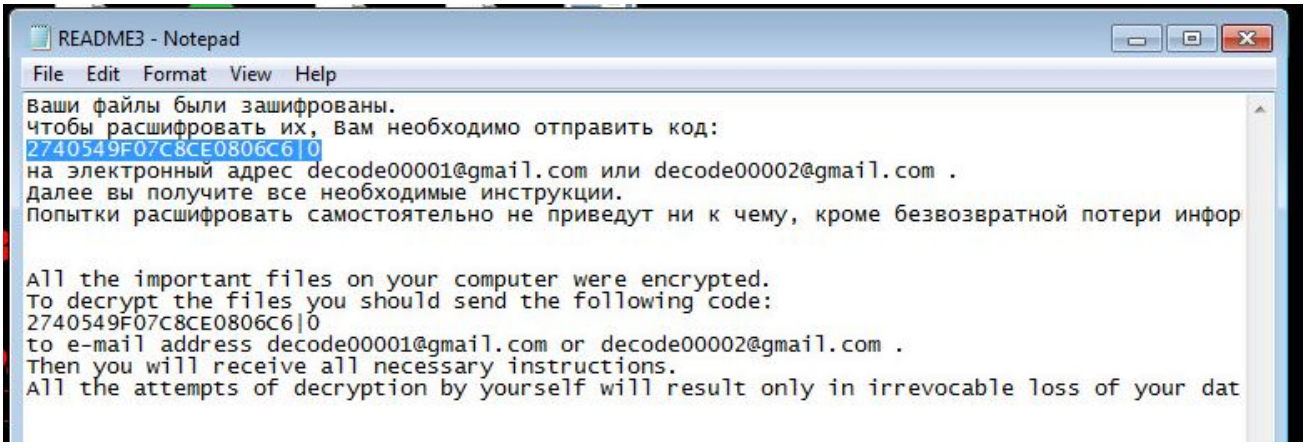
Each *txt* file has the filename in the format *README[number].txt* and looks like this:



The user is instructed to send a specified code to the e-mail address provided.

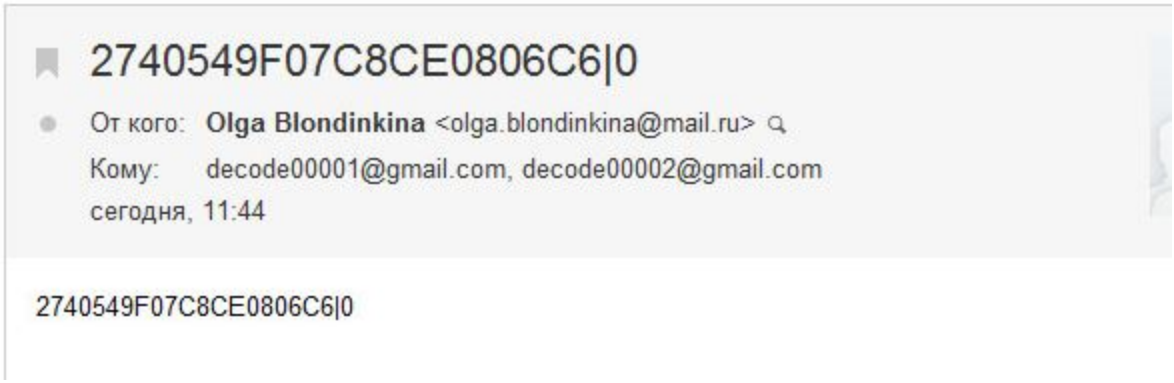
To summarize, a Troldesh infection displays these characteristics:

- A warning message on the user's screen
- Regular files replaced by the encrypted files with the *.xbtl* extension
- README[number].txt files for information and contact data



How I Got a Discount From the Hackers

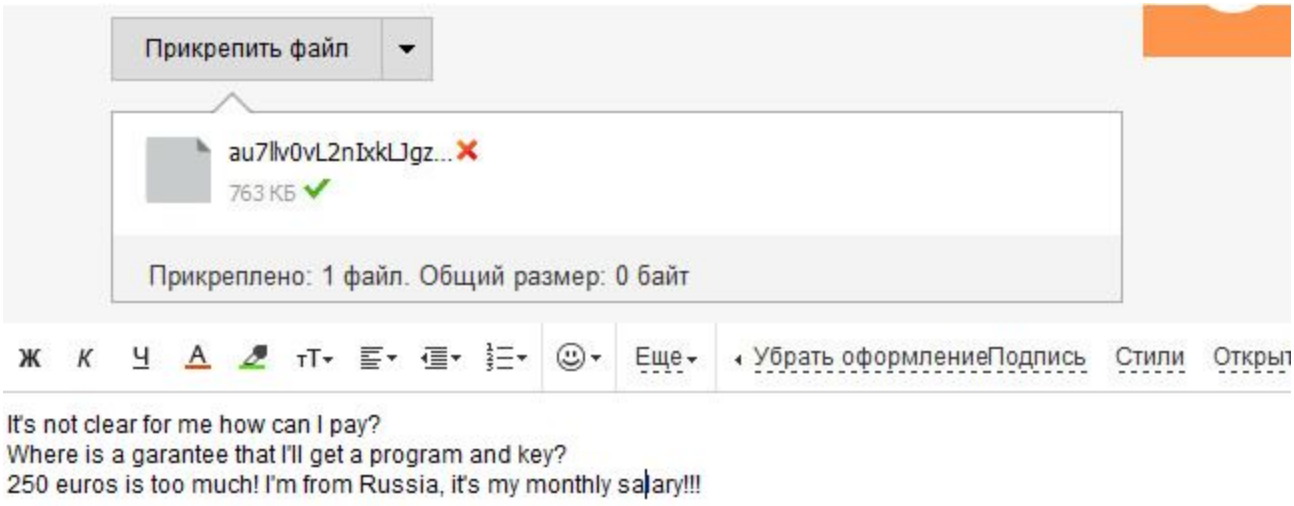
I was very interested to learn more about the ransom and tried to start a correspondence with the attackers. As required, I sent the specified code to the e-mail address provided, one that is registered on the most famous Russian domain.



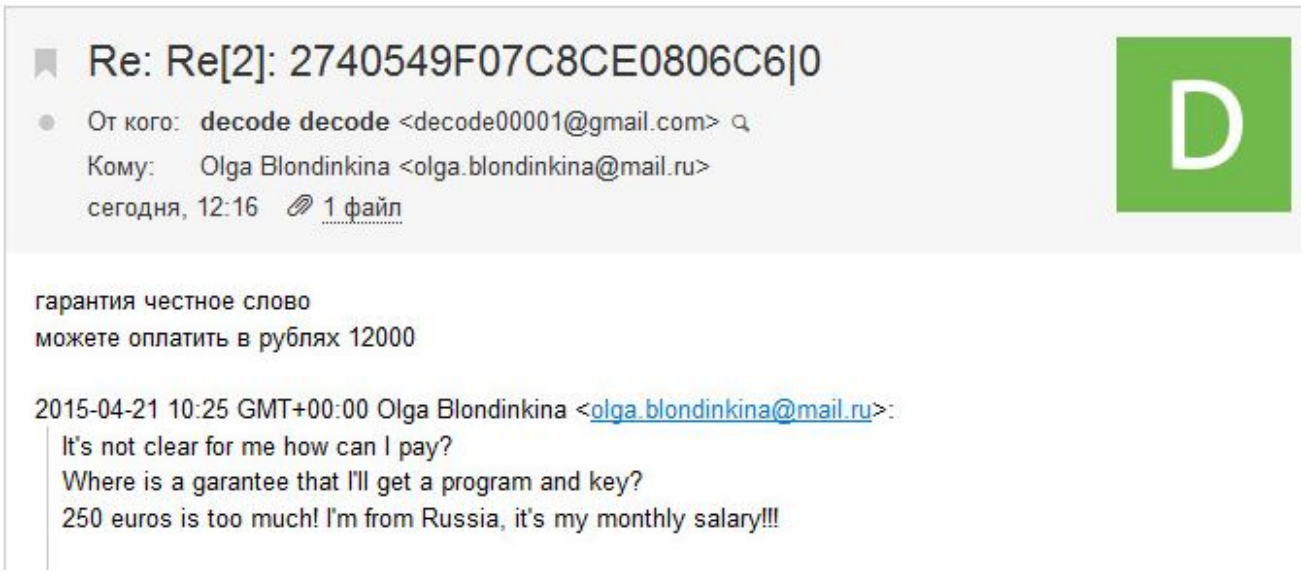
After several minutes I received an answer with my next instructions.

The extortionists said to send them one encrypted file to prove they could decrypt it. They demanded 250 euros to decrypt all of the files.

Something about this transaction bothered me. Was their answer generated automatically or was there a real person on the other end? To find out, I decided to accept the hackers' "generous" offer and send them an encrypted file for decryption. At the same time, I tried to start a conversation with them to see whether I could persuade them to give me the key for free, or at least get a decent discount.

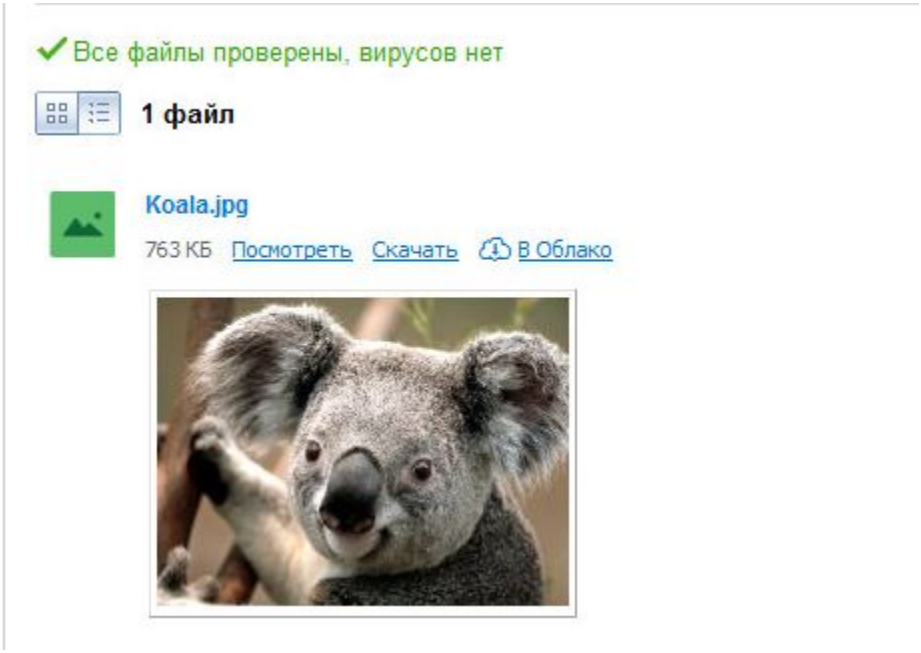


To my great surprise, after a minute I got an answer from a real person who was open to discussion! Since the answer and all of the following conversation were in Russian, a translation is provided under each screenshot.

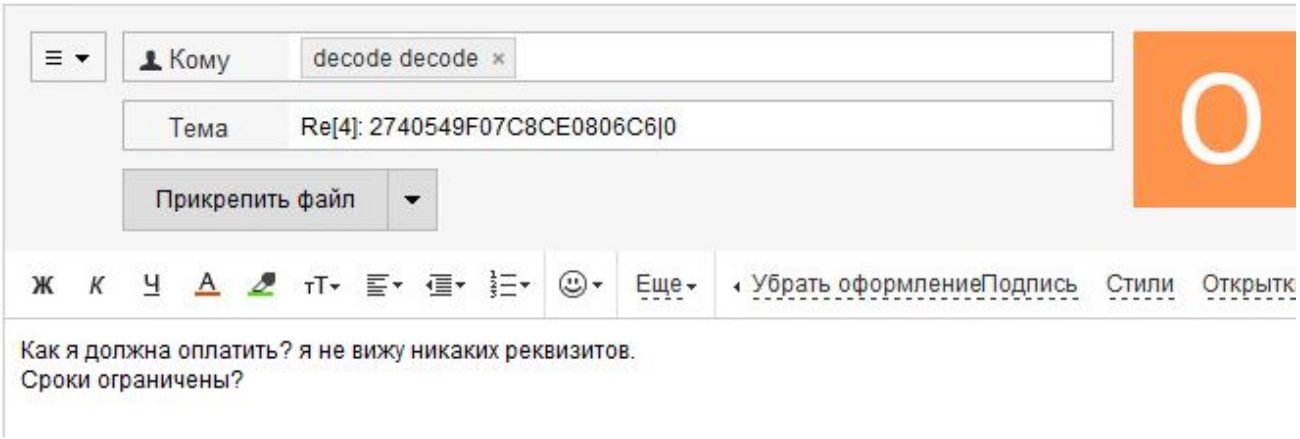


“The guarantee is our word of honor. You can pay in rubles, 12000 RUB.”

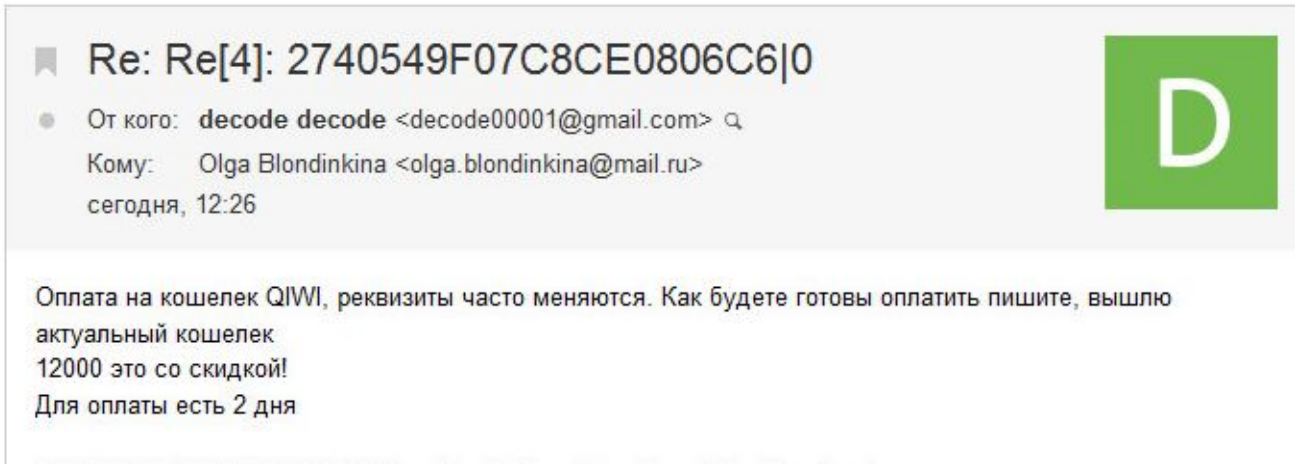
I checked the currency exchange rate and saw that I received a discount of approximately 15% (~35 euro). A decrypted version of the encrypted file I sent earlier was attached to the same e-mail.



I continued asking about payment methods and if there was a specific time frame.



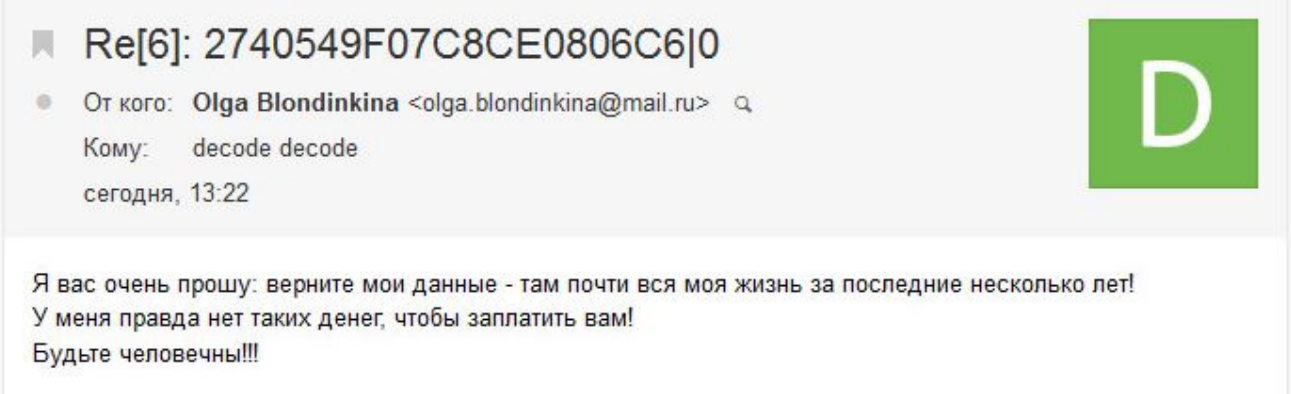
“How can I pay? I don’t see any requisites. Are there any time frames?”



“The payment should be done to the QIWI purse, requisites are changing frequently. As soon as you will be ready to pay, write me, and I’ll send an actual requisites.

12000 RUB is a sum with discount!
You have only 2 days to pay.”

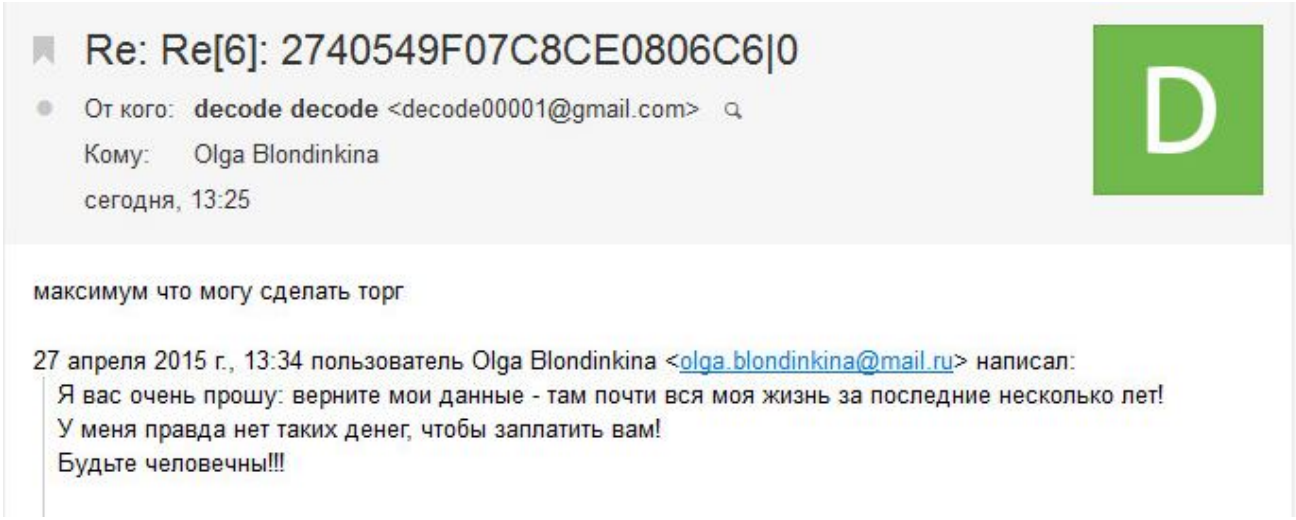
I took a break at this point and after almost a week wrote them again. I still had hopes of getting the key for free.



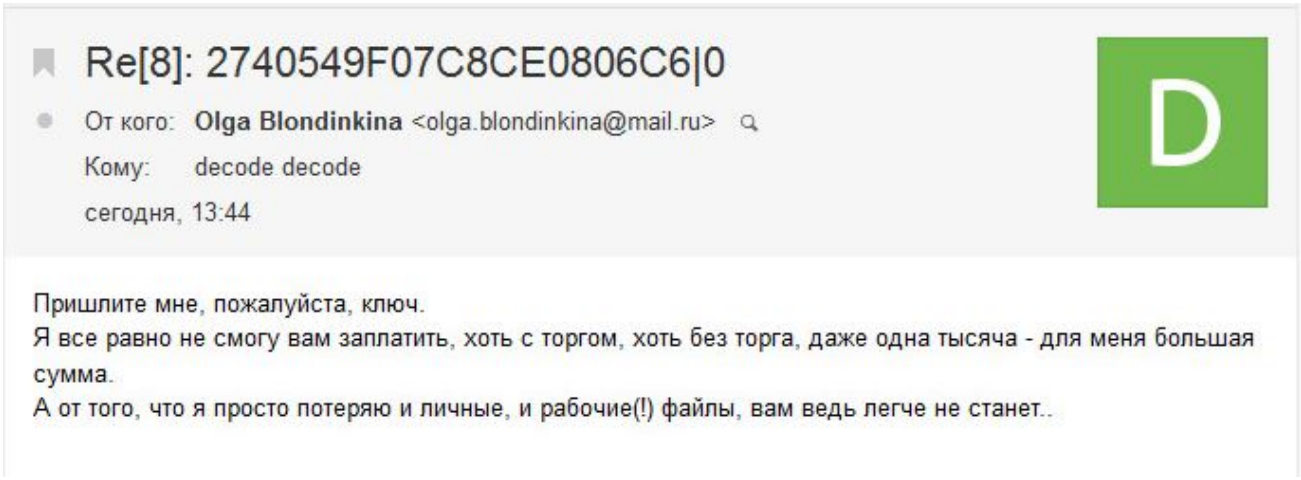
“I ask you: please, return my data – this is almost all of my life for the last several years!

I really don’t have much money to pay you!

Be humane!!!”



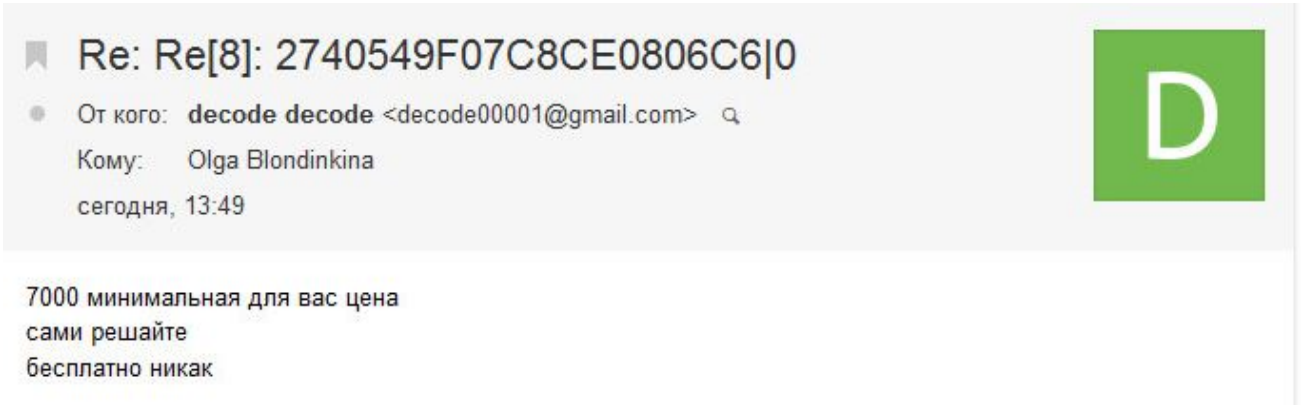
“The best I can do is to bargain”



“Please send me the key.

Anyway, I can’t pay, neither with bargain, nor without it. Even one thousand rubles is a big sum for me.

The case in which I’ll lose all of my personal and work(!) files will not make your life easier…”



“7000 is a minimal cost for you

Decide for yourself

There is no way to get the key for free”

By the end of our correspondence, I managed to get a discount of 50%. Perhaps if I had continued bargaining, I could have gotten an even bigger discount.