### **Network Analysis — Ransomeware**

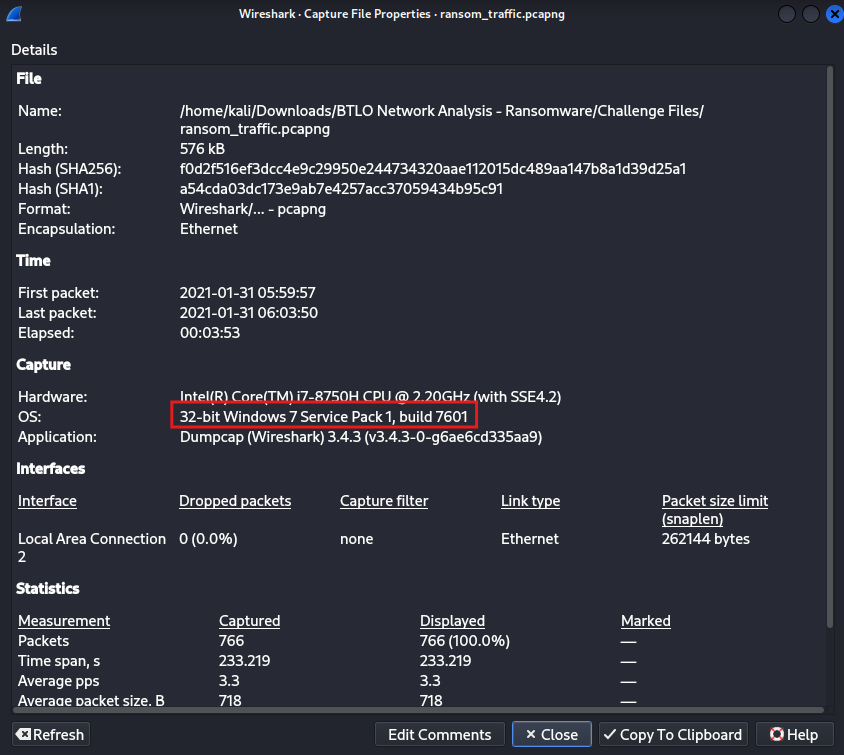
Scenario: ABC Industries worked day and night for a month to prepare a tender document for a prestigious project that would secure the company’s financial future. The company was hit by ransomware, believed to be conducted by a competitor, and the final version of the tender document was encrypted. Right now they are in need of an expert who can decrypt this critical document. All we have is the network traffic, the ransom note, and the encrypted ender document. Do your thing Defender!​

**Note: All actions performed in an isolated environment.**

Tasks:

1. What is the operating system of the host from which the network traffic was captured? (Look at Capture File Properties, copy the details exactly)

Let us look at the capture file properties, statistics -> capture file properties or ctr+alt+shift+c.

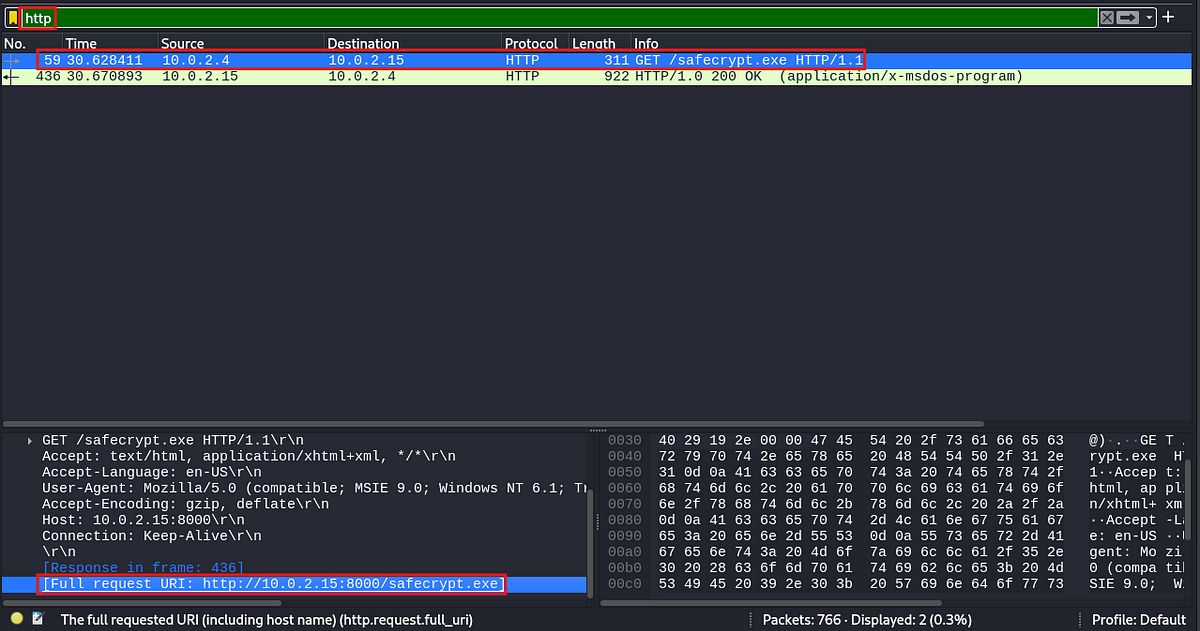


Answer: 32-bit Windows 7 Service Pack 1, build 7601

2. What is the full URL from which the ransomware executable was downloaded?

Let us check the http traffic for this

filter: http



Answer: http[:]//10[.]0[.]2[.]15[:]8000/safecrypt[.]exe (defanged for safety)

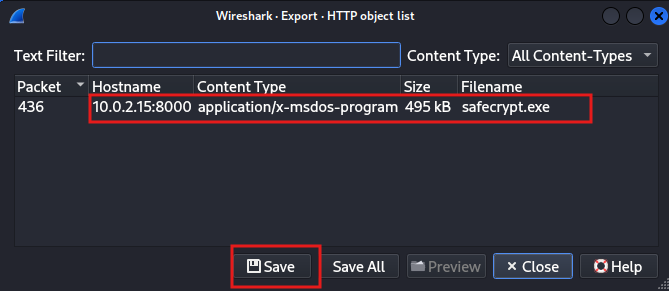
3. Name the ransomware executable file?

Answer is in the above screenshot.

Answer: safecrypt.exe

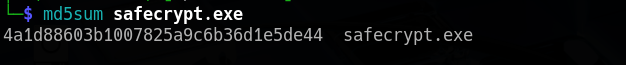
4. What is the MD5 hash of the ransomware?

Let us export this file by going to File -> Export objects -> HTTP



Calculate the md5 hash for the downloaded file using the following commnad

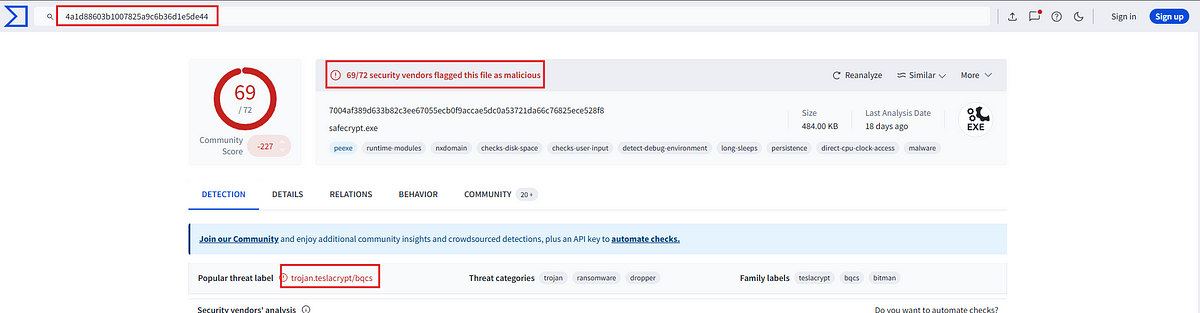
command: md5sum safecrypt.exe



Answer: 4a1d88603b1007825a9c6b36d1e5de44

5. What is the name of the ransomware?

Let us use Virustotal to find this out. Open<https://www.virustotal.com/gui/> and provide the calculated md5 hash to find out more info about this file.

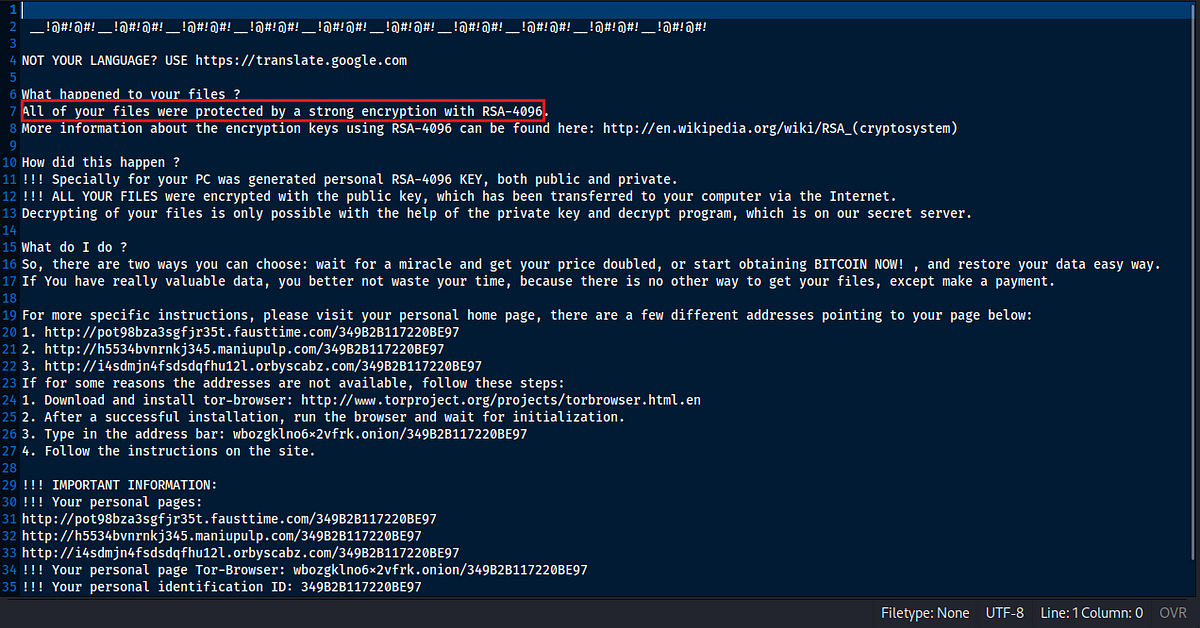


We can see under the popular threat label that it is a trojan called teslacrypt.

Answer: teslacrypt

6. What is the encryption algorithm used by the ransomware, according to the ransom note?

Along with the capture file we were given a text file which the attacker had left for us. Le us see the contents of this note.

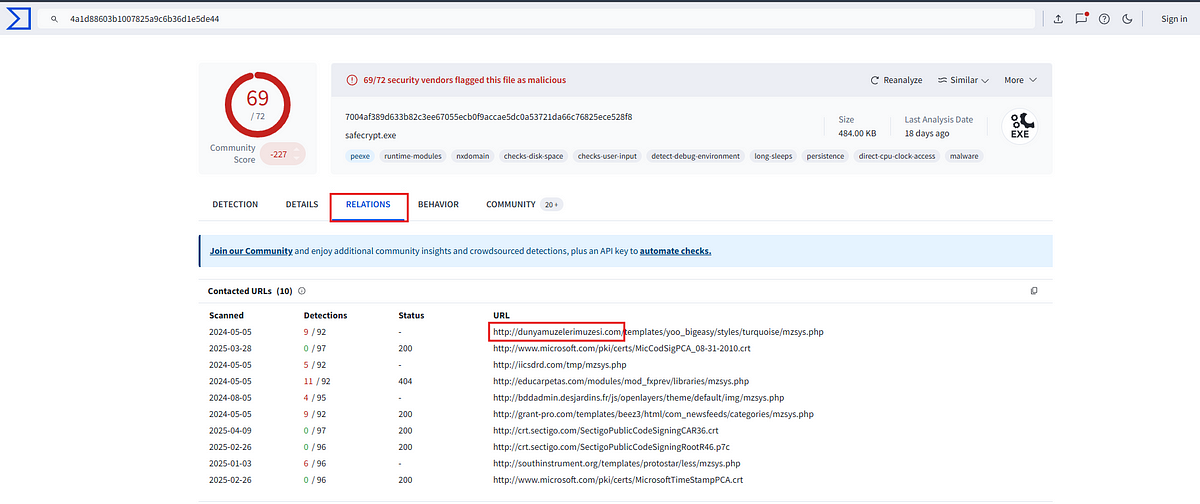


We can see from the above screenshot that the attacker had used RSA algorithm for encryption with a key length of 4096.

Answer: RSA-4096

7. What is the domain beginning with ‘d’ that is related to ransomware traffic?

Let us go back to Virustotal, and check the relations tab.



Answer: dunyamuzelerimuzesi.com

8. Decrypt the Tender document and submit the flag

BloodDolly, a security researcher had released a decryptor to decrypt the files encrypted by the Teslacrypt ransomware, It can be downloaded from [here](https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/). Using this we can decrypt the file to find the contents of the file.

Answer: BTLO-T3nd3r-Fl@g



This is the end of the walkthrough.