Blue Team Labs Online: Network Analysis - Ransomware

The following writeup is for Network Analysis - Ransomware on Blue Team Labs Online, it's a medium difficulty lab that involves investigating a PCAP using Wiresharl

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!

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

To find the operating system of the host where the network traffic was captured, you can navigate to Statistics > Capture File Properties within Wireshark:

Capture

Hardware:	Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz (with SSE4.2)
OS:	32-bit Windows 7 Service Pack 1, build 7601
Application:	Dumpcap (Wireshark) 3.4.3 (v3.4.3-0-g6ae6cd335aa9)

Here you can find the OS and version information.

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

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

If you apply the "http" display filter, we can see one GET request made to /safecrypt.exe:

```
GET /safecrypt.exe HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, */*\r
Accept-Language: en-US\r\n
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0;
Accept-Encoding: gzip, deflate\r\n
Host: 10.0.2.15:8000\r\n
```

Answer: http://10.0.2.15:8000/safecrypt.exe

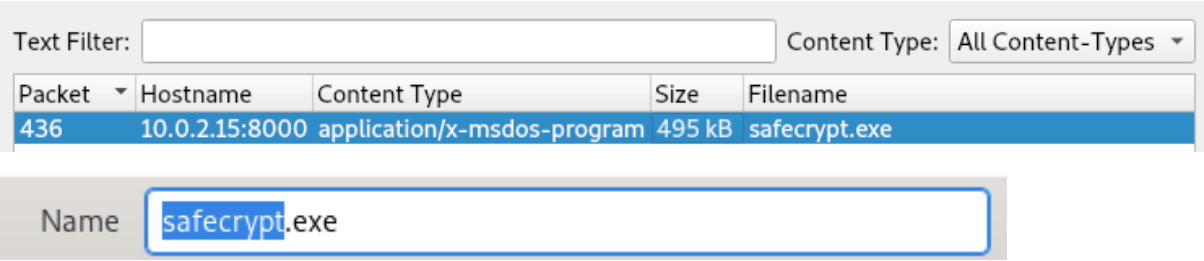
Name the ransomware executable file?

We found this in the GET request.

Answer: safecrypt.exe

What is the MD5 hash of the ransomware?

To generate the MD5 hash of the ransomware, let's first export the safecrypt.exe binary. We can do so by navigating to File > Export > HTTP Object:



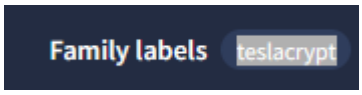
You can then use the md5sum command to generate the MD5 hash:

```
remnux@remnux:~/BTLO Network Analysis - Ransomware/Challenge Files$ md5sum safecrypt.exe
4a1d88603b1007825a9c6b36d1e5de44  safecrypt.exe
```

Answer: 4a1d88603b1007825a9c6b36d1e5de44

What is the name of the ransomware?

If you search for the MD5 hash of the ransomware binary using VirusTotal, you can see that it is associated with teslacrypt:



Answer: teslacrypt

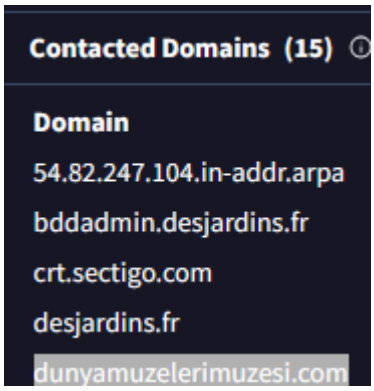
What is the encryption algorithm used by the ransomware, according to the ransom note?

```
remnux@remnux:~/BTLO Network Analysis - Ransomware/Challenge Files$ cat help_recover_instructions.TXT

 __!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!

NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files ?
All of your files were protected by a strong encryption with RSA-4096.
```

Answer: RSA-4096

What is the domain beginning with 'd' that is related to ransomware traffic?

On VirusTotal, we can see that the uploaded binary has contacted 15 domains:



If you look at the DNS requests in the pcap file, we can see a request for this domain:

```
Standard query 0xcae1 A dunyamuzelerimuzesi.com
Standard query 0xcae1 A dunyamuzelerimuzesi.com
Standard query 0xcae1 A dunyamuzelerimuzesi.com
Standard query 0xcae1 A dunyamuzelerimuzesi.com
```

Answer: dunyamuzelerimuzesi.com

Decrypt the Tender document and submit the flag

Download tesladecyptors to decrypt the file and find the flag.

Answer: BTLO-T3nd3r-Fl@g