Network Analysis- Ransomware

Contents

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!

Pre-requisites

- Load kali
- Run sudo apt update && sudo apt -y upgrade > reboot
- Change network to host only instead of NAT – to restrict network so malware inside the pcap is contained within the VM
- Load Wireshark and open the pcap file
- Review the challenge files that come in the zip file along with the pcap for clues/insight

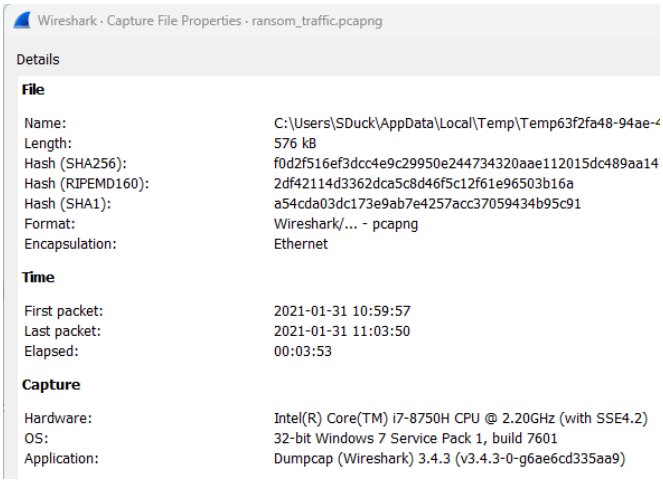
Initial thoughts from scenario/challenge files

- Scenario
    - Nothing really standing out to me besides the fact it's potentially a competitor, but that won't help with the pcap
- Challenge file:
    - Ransom notes
        - Files encrypted using RSA-4096

Challenge Questions

What is the operating system of the host from which the network traffic was captured?

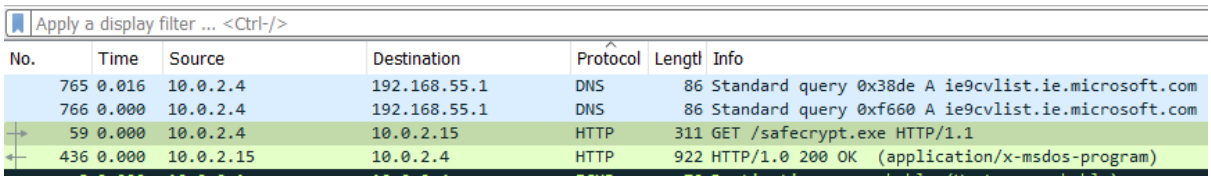
- Answer: 32-bit Windows 7 Service Pack 1, build 7601



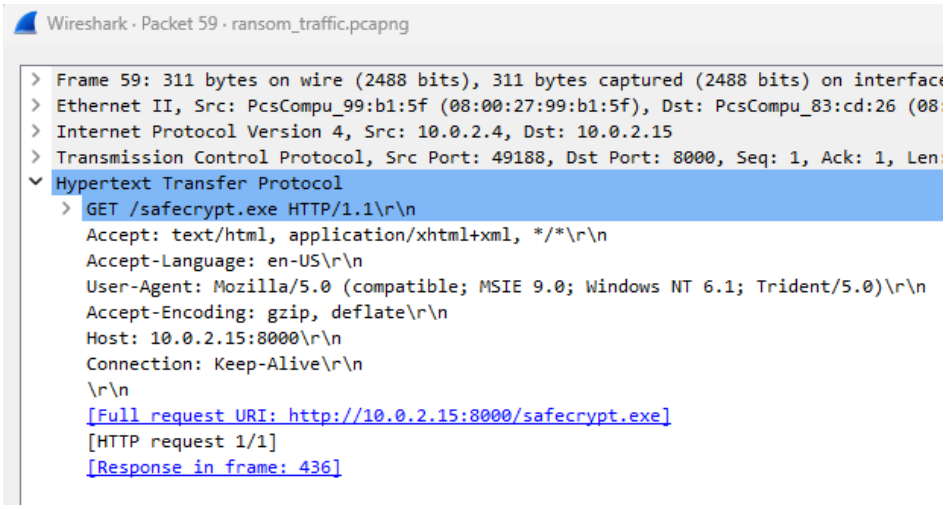
- Access the Capture File Properties through Wireshark by clicking the notepad icon in the bottom left hand side of the Wireshark window
- Then, review the newly opened window to retrieve the value associated with "OS:" in the first column

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

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



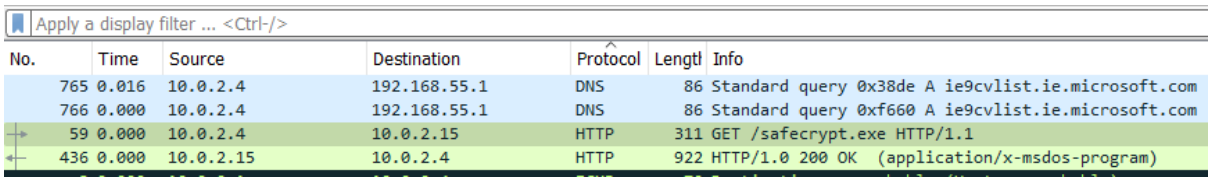
- Ransomware is commonly downloaded via HTTP GET requests from a C2 server
- Filter the pcap by Protocol A > Z and then scroll to HTTP traffic
    - Only two packets of HTTP which are 59 and 436
    - Packet 59 is requesting /safecrypt.exe which is the name of the executable that was most likely used to encrypt the tender document, based on the "crpyt" part of the name



- Double click on packet > expand the HTTP dropdown menu > read the full URL > http://10.0.2.15:8000/safecrypt.exe

Name the ransomware executable file?

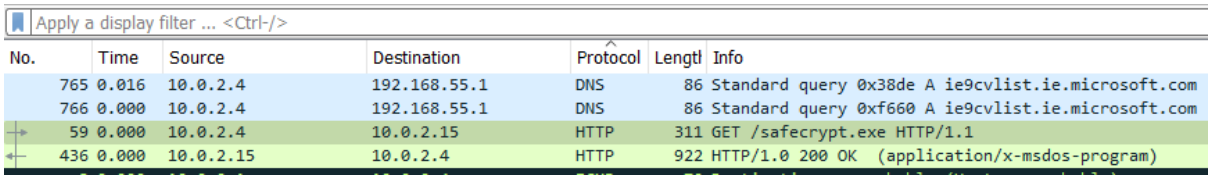
- Answer: safecrypt.exe



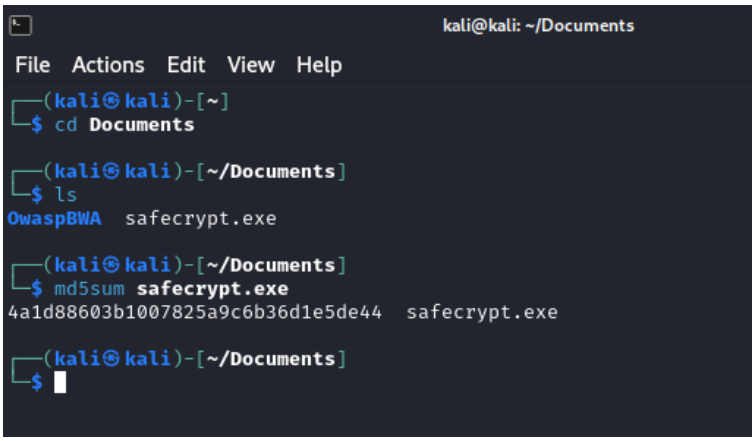
- We discovered packet 59 in the previous task, which is requesting the file safecrypt.exe via HTTP GET from the victim machine on IP address 10.0.2.4

What is the MD5 hash of the ransomware?

- Answer: 4a1d88603b1007825a9c6b36d1e5de44

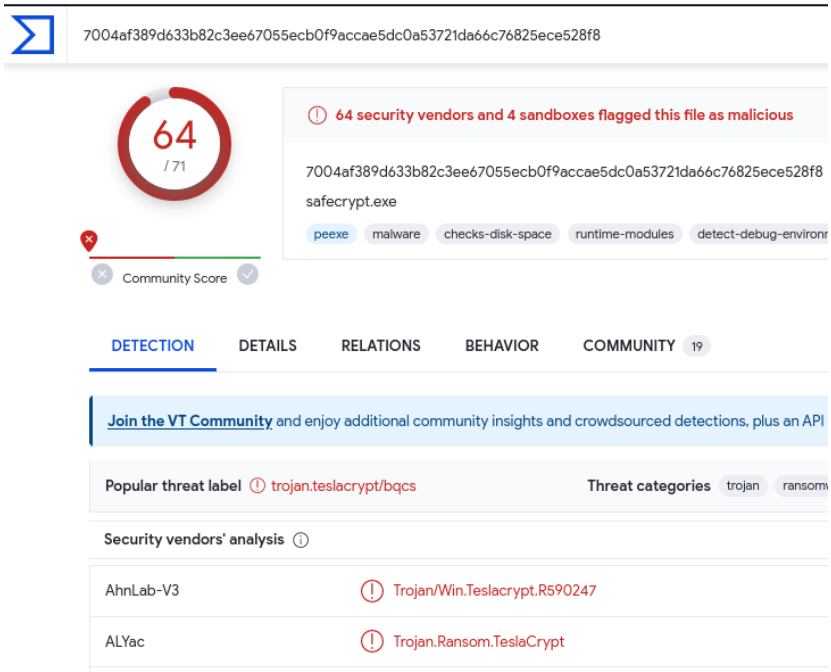


- Select packet 59 > File > Export objects > HTTP > select the safecrypt.exe file > save
- Open either a terminal or powershell depending if you're on Linux/Windows in the directory where safecrypt.exe is **securely** stored, and run either:
    - Md5sum safecrypt.exe
    - Get-Filehash safecrypt.exe -Algorithm MD5



What is the name of the ransomware?

- Answer: TeslaCrypt



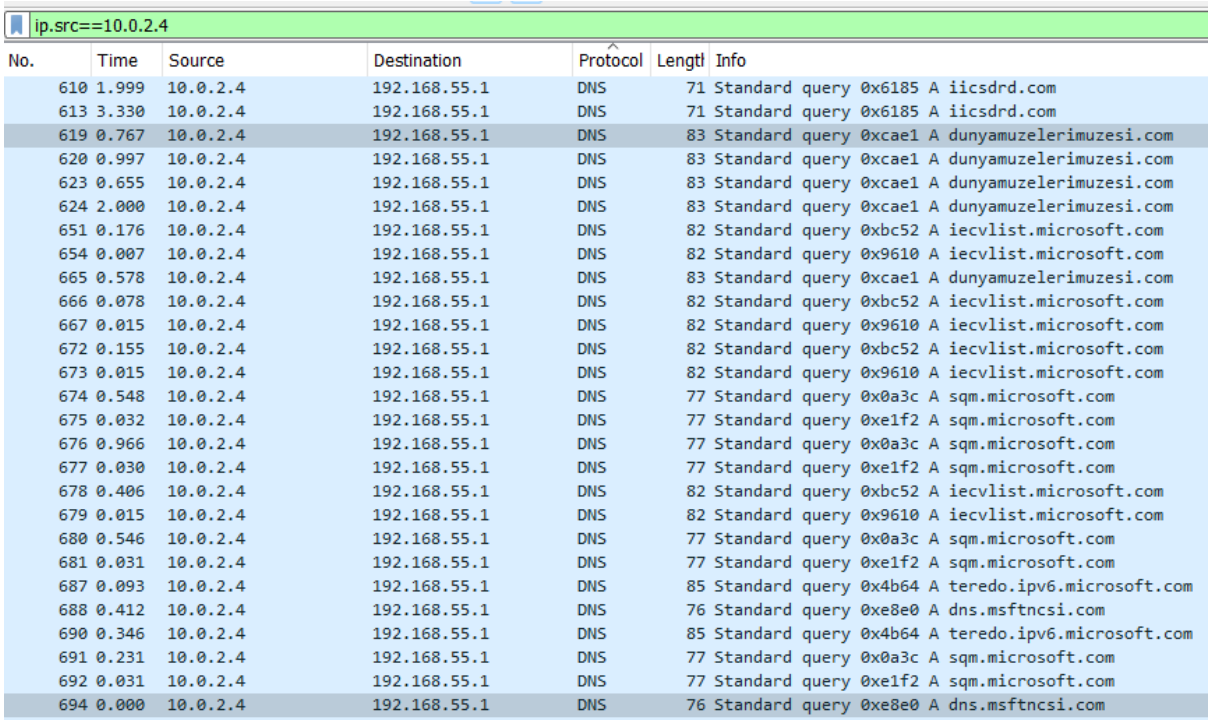
- Take the MD5 hash generated and search it in Virus Total
- Reviewing the results confirms it is malicious ransomware. And in the "Security Vendor's Analysis" section of Virus Total, the first two vendors label this file hash associated with TeslaCrypt

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

- Answer: RSA-4096
- Due to reviewing all the challenge files before beginning the tasks, we are prepared and already know the algorithm used (or claimed to have been used by the attacker)

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

- Answer: dunyamuzelerimuzesi.com



ip.src==10.0.2.4

No.	Time	Source	Destination	Protocol	Lengtl	Info
610	1.999	10.0.2.4	192.168.55.1	DNS	71	Standard query 0x6185 A iicsdrd.com
613	3.330	10.0.2.4	192.168.55.1	DNS	71	Standard query 0x6185 A iicsdrd.com
619	0.767	10.0.2.4	192.168.55.1	DNS	83	Standard query 0xcae1 A dunyamuzelerimuzesi.com
620	0.997	10.0.2.4	192.168.55.1	DNS	83	Standard query 0xcae1 A dunyamuzelerimuzesi.com
623	0.655	10.0.2.4	192.168.55.1	DNS	83	Standard query 0xcae1 A dunyamuzelerimuzesi.com
624	2.000	10.0.2.4	192.168.55.1	DNS	83	Standard query 0xcae1 A dunyamuzelerimuzesi.com
651	0.176	10.0.2.4	192.168.55.1	DNS	82	Standard query 0xbc52 A iecvlist.microsoft.com
654	0.007	10.0.2.4	192.168.55.1	DNS	82	Standard query 0x9610 A iecvlist.microsoft.com
665	0.578	10.0.2.4	192.168.55.1	DNS	83	Standard query 0xcae1 A dunyamuzelerimuzesi.com
666	0.078	10.0.2.4	192.168.55.1	DNS	82	Standard query 0xbc52 A iecvlist.microsoft.com
667	0.015	10.0.2.4	192.168.55.1	DNS	82	Standard query 0x9610 A iecvlist.microsoft.com
672	0.155	10.0.2.4	192.168.55.1	DNS	82	Standard query 0xbc52 A iecvlist.microsoft.com
673	0.015	10.0.2.4	192.168.55.1	DNS	82	Standard query 0x9610 A iecvlist.microsoft.com
674	0.548	10.0.2.4	192.168.55.1	DNS	77	Standard query 0x0a3c A sqm.microsoft.com
675	0.032	10.0.2.4	192.168.55.1	DNS	77	Standard query 0xe1f2 A sqm.microsoft.com
676	0.966	10.0.2.4	192.168.55.1	DNS	77	Standard query 0x0a3c A sqm.microsoft.com
677	0.030	10.0.2.4	192.168.55.1	DNS	77	Standard query 0xe1f2 A sqm.microsoft.com
678	0.406	10.0.2.4	192.168.55.1	DNS	82	Standard query 0xbc52 A iecvlist.microsoft.com
679	0.015	10.0.2.4	192.168.55.1	DNS	82	Standard query 0x9610 A iecvlist.microsoft.com
680	0.546	10.0.2.4	192.168.55.1	DNS	77	Standard query 0x0a3c A sqm.microsoft.com
681	0.031	10.0.2.4	192.168.55.1	DNS	77	Standard query 0xe1f2 A sqm.microsoft.com
687	0.093	10.0.2.4	192.168.55.1	DNS	85	Standard query 0x4b64 A teredo.ipv6.microsoft.com
688	0.412	10.0.2.4	192.168.55.1	DNS	76	Standard query 0xe8e0 A dns.msftncsi.com
690	0.346	10.0.2.4	192.168.55.1	DNS	85	Standard query 0x4b64 A teredo.ipv6.microsoft.com
691	0.231	10.0.2.4	192.168.55.1	DNS	77	Standard query 0x0a3c A sqm.microsoft.com
692	0.031	10.0.2.4	192.168.55.1	DNS	77	Standard query 0xe1f2 A sqm.microsoft.com
694	0.000	10.0.2.4	192.168.55.1	DNS	76	Standard query 0xe8e0 A dns.msftncsi.com

- Start by applying a filter of ip.src==10.0.2.4 as we know this is the IP address of the compromised machine that is running the malware
- Then sort the Protocol column A > Z and scroll to DNS packets
- Review the Info column for A records beginning with the letter d
    - There are only 2 which are "dunyamuzelerimuzesi.com" and "dns.msftncsi.com"
    - We can take an educated guess at the second domain being related to Microsoft as it is often abbreviated to msft. This, in addition to the first domain being highly irregular, and unreadable confirms it is the suspicious domain we are after

What is the flag inside the encrypted tender document?

- Answer: BTLO-T3nd3r-Fl@g
- Download and install TeslaDecrypt program, follow the steps provided to decrypt the tender document from .micro to .pdf