2021-02-08 - TRAFFIC ANALYSIS QUIZ ANSWERS

SCENARIO:

- LAN segment range: 10.2.8.0/24 (10.2.8.0 through 10.2.8.255)
- Domain: ascolimited.com
- Domain Controller: AscoLimited-DC
- LAN segment gateway: 10.2.8.1
- LAN segment broadcast address: 10.2.8.255

TASK:

- Write an incident report based on the pcap and alerts.
- The incident report should contain the following:
- Executive Summary
- Details (of the infected Windows host)
- Indicators of Compromise (IOCs)

ANSWERS:

Executive Summary

On 2021-02-08 at approximately 16:00 UTC, a Windows host used by Bill Cook was infected with Hancitor, Cobalt Strike, and Ficker Stealer malware.

Details

MAC address: 00:12:79:41:c2:aa
IP address: 10.2.8.101
Host name: DESKTOP-MGVG60Z
Windows user account: bill.cook

Indicators of Compromise (IOCs)

Traffic for Hancitor:

- 45.124.85.55 port 80 - ***tonmatdoanminh.com*** - GET /uninviting.php
- port 80 - api.ipify.org - GET /
- 213.5.229.12 port 80 - ***satursed.com*** - POST /8/forum.php

Traffic for Cobalt Strike:

- 8.208.10.147 port 80 - ***roanokemortgages.com*** - GET /0801.bin
- 8.208.10.147 port 80 - ***roanokemortgages.com*** - GET /0801s.bin
- 198.211.10.238 port 8080 - ***198.211.10.238:8080*** - GET /6Aov
- 198.211.10.238 port 443 - HTTPS traffic
- 198.211.10.238 port 8080 - ***198.211.10.238:8080*** - GET /ca
- 198.211.10.238 port 8080 - ***198.211.10.238:8080*** - POST /submit.php?id=3275377518

Traffic for Ficker Stealer:

- 8.208.10.147 port 80 - ***roanokemortgages.com*** - GET /6lhjgfdghj.exe
- port 80 - api.ipify.org - GET /?format=xml
- 185.100.65.29 port 80 - ***sweyblidian.com*** - TCP traffic caused by Ficker Stealer

NOTES:

There is a malicious Word document for Hancitor you can get from this exercise pcap. It's encoded as base64 text in a web page. Export this page from the pcap, then open the extracted HTML page in a web browser. The Word doc is:

SHA256 hash: 3a5648f7de99c4f87331c36983fc8adcd667743569a19c8dafdd5e8a33de154d

- File size: 822,272 bytes
- File name: 0208_54741869750132.doc
- File description: Word document with macros for Hancitor malware

2021-02-08 - TRAFFIC ANALYSIS QUIZ ANSWERS

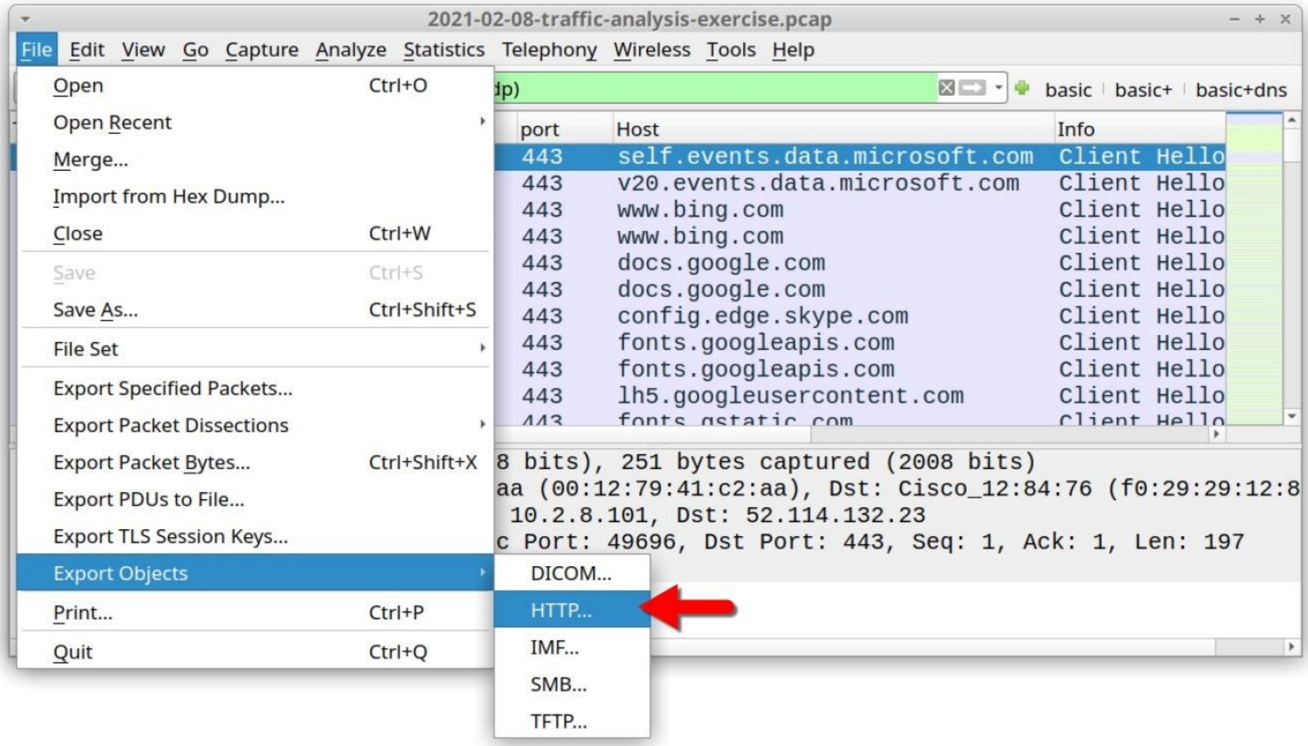
- Any.Run analysis: https://app.any.run/tasks/4a9eaf6f-1727-4636-99f15d677456213f

To get the Word doc from the pcap, do the following:

Step 1: export HTTP objects
Step 2: type ***uninviting.php*** in the text filter from the Export HTTP object list
Step 3: export the entry from ***tonmatdoanminh.com*** that's 1,097 kB
Step 4: save that entry as a web page (any name with an ***.html*** file extension)
Step 5: open your saved ***.html*** file in a web browser
Step 6: you should immediately see a pop-up window asking you if you want to save or open a Word document named ***0208_54741869750132.doc***.

NOTE: This Word document is Windows-based malware, and it will infect a Windows computer if given the chance. I strongly recommend you do these procedures in a non-Windows environment.

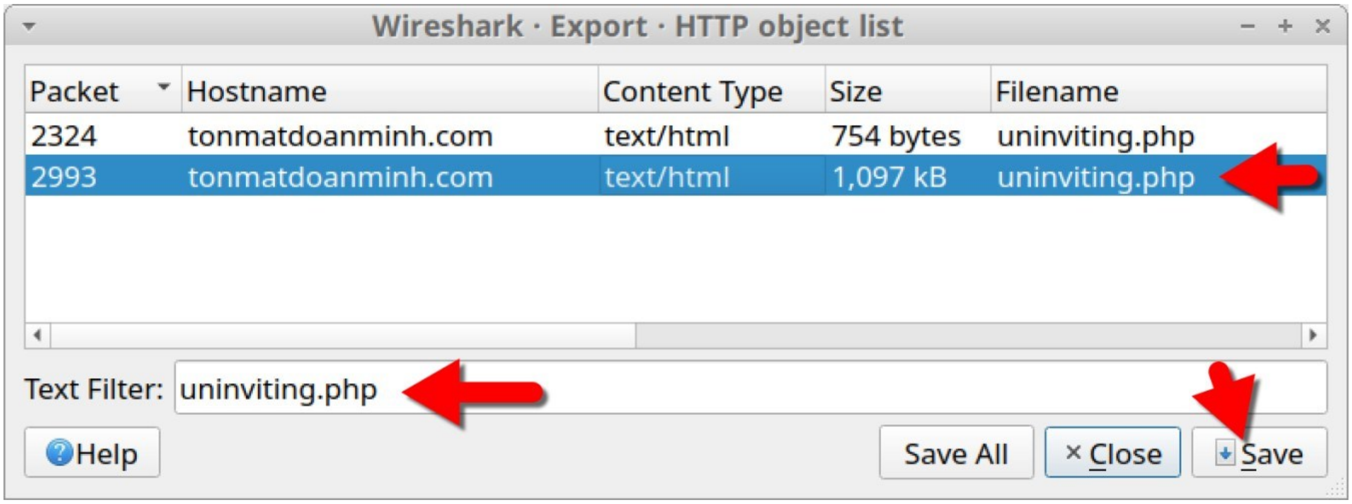
Step 1:



port	Host	Info
443	self.events.data.microsoft.com	Client Hello
443	v20.events.data.microsoft.com	Client Hello
443	www.bing.com	Client Hello
443	www.bing.com	Client Hello
443	docs.google.com	Client Hello
443	docs.google.com	Client Hello
443	config.edge.skype.com	Client Hello
443	fonts.googleapis.com	Client Hello
443	fonts.googleapis.com	Client Hello
443	lh5.googleusercontent.com	Client Hello
443	fonts.gstatic.com	Client Hello

```
8 bits), 251 bytes captured (2008 bits)
aa (00:12:79:41:c2:aa), Dst: Cisco_12:84:76 (f0:29:29:12:8
 10.2.8.101, Dst: 52.114.132.23
c Port: 49696, Dst Port: 443, Seq: 1, Ack: 1, Len: 197
```

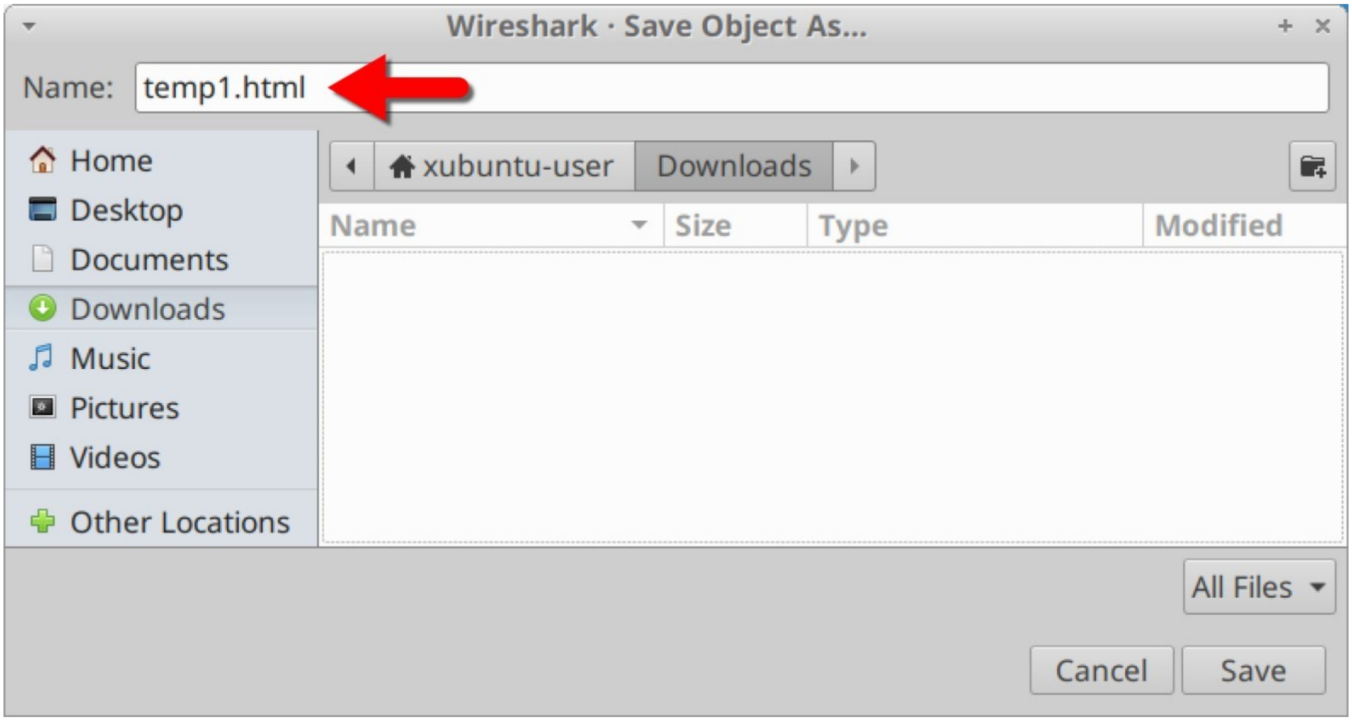
Step 2 and 3:



Packet	Hostname	Content Type	Size	Filename
2324	tonmatdoanminh.com	text/html	754 bytes	uninviting.php
2993	tonmatdoanminh.com	text/html	1,097 kB	uninviting.php

Text Filter: uninviting.php

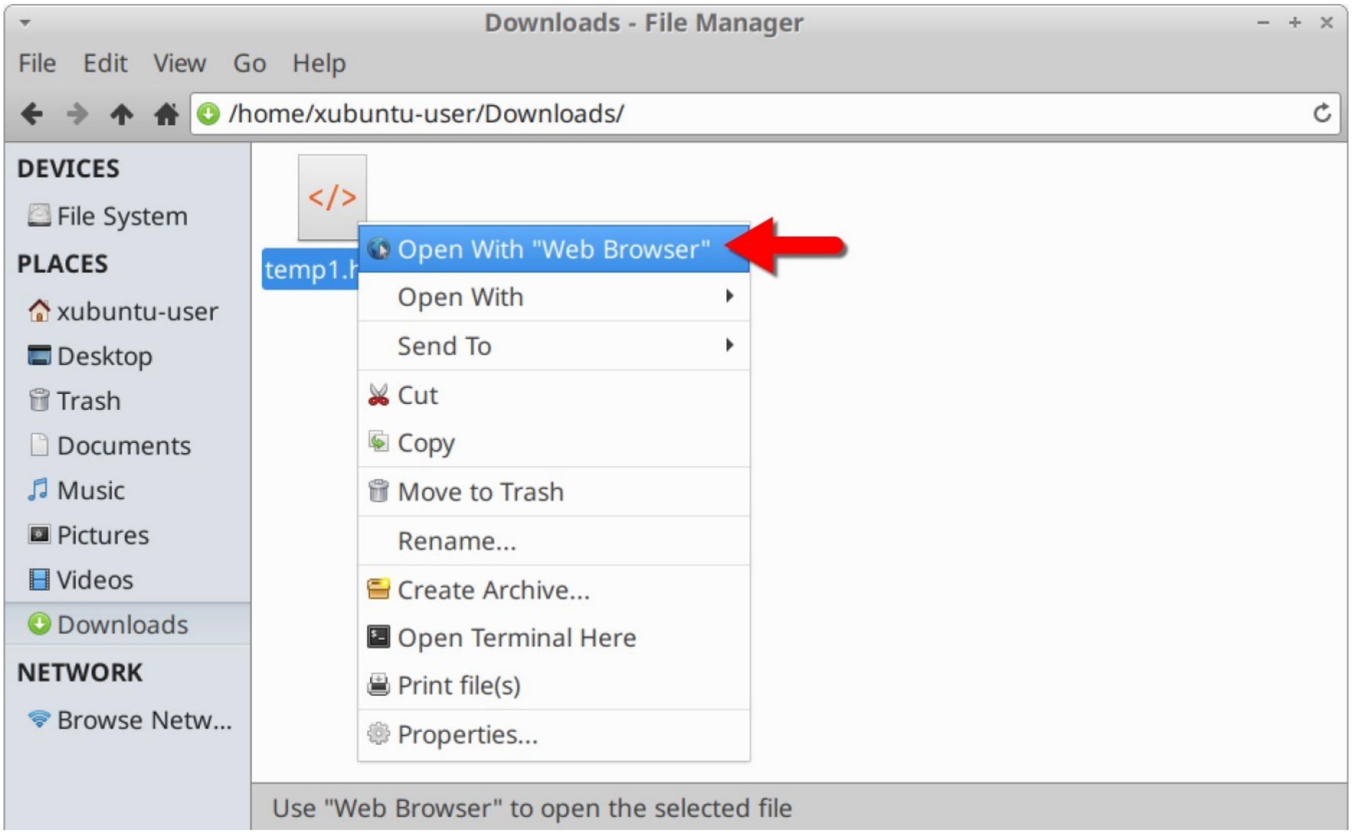
Step 4:



Name: temp1.html

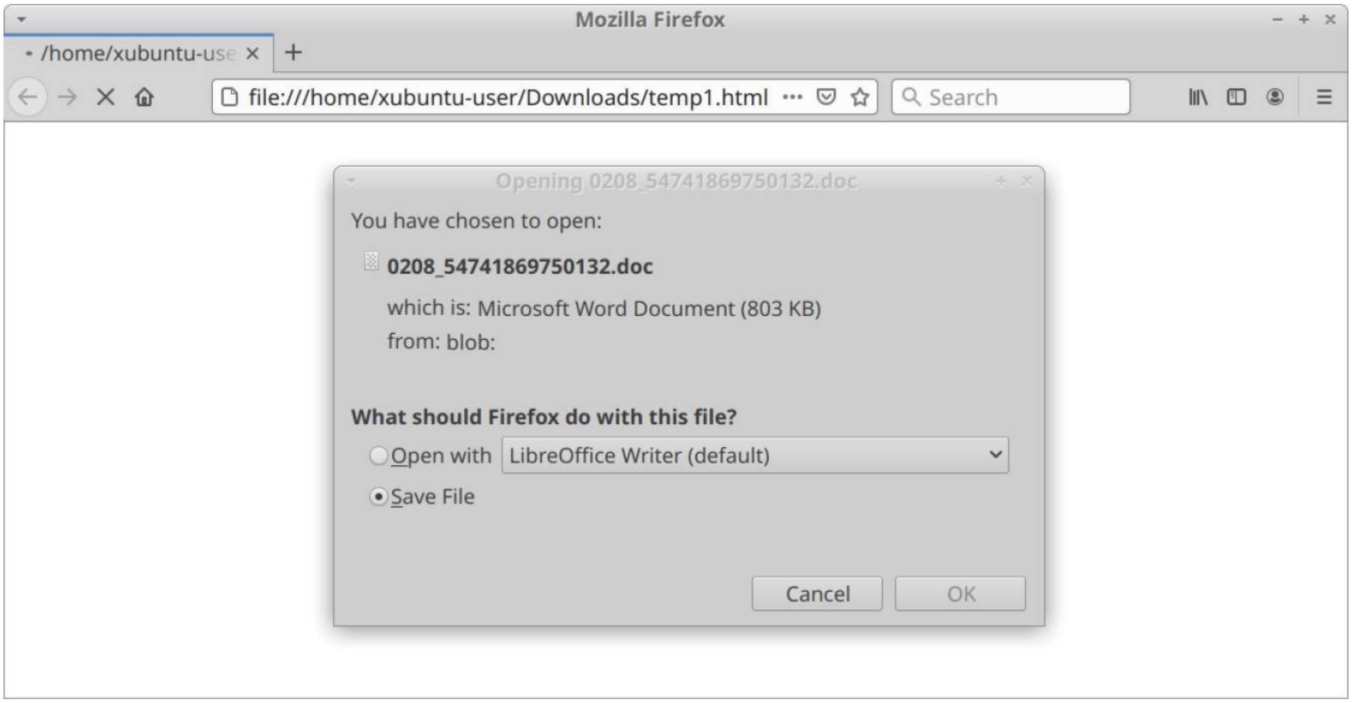
Step 5:

2021-02-08 - TRAFFIC ANALYSIS QUIZ ANSWERS



Step 6:

2021-02-08 - TRAFFIC ANALYSIS QUIZ ANSWERS



file:///home/xubuntu-user/Downloads/temp1.html

Opening 0208_54741869750132.doc

You have chosen to open:

0208_54741869750132.doc

which is: Microsoft Word Document (803 KB)
from: blob:

What should Firefox do with this file?

○ Open with LibreOffice Writer (default)

● Save File