2023-01-Unit42-Wireshark-quiz-pcap

Sunday, June 16, 2024 7:46 PM

Challenge Introduction

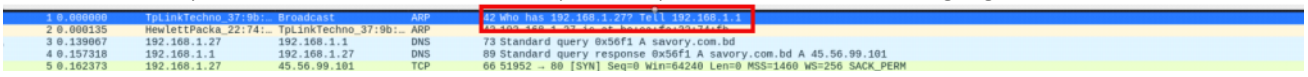
This challenge involves analyzing a packet capture (pcap) of malicious activity, focusing on understanding and interpreting network traffic associated with potential malware infections. It tests us by answering the following questions on the analysis.

Questions to answer

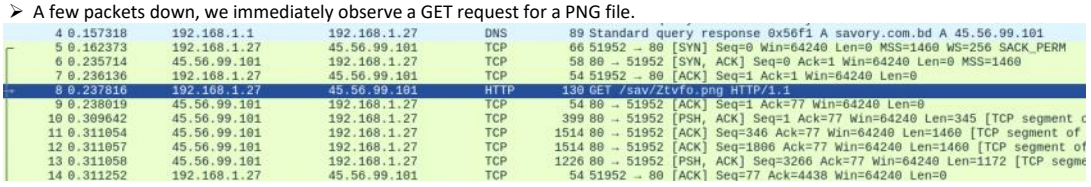
- When did the malicious traffic start in UTC?
- What is the victim's IP address?
- What is the victim's MAC address?
- What is the victim's Windows host name?
- What is the victim's Windows user account name?
- How much RAM does the victim's host have?
- What type of CPU is used by the victim's host?
- What is the public IP address of the victim's host?
- What type of account login data was stolen by the malware?

Network traffic analysis

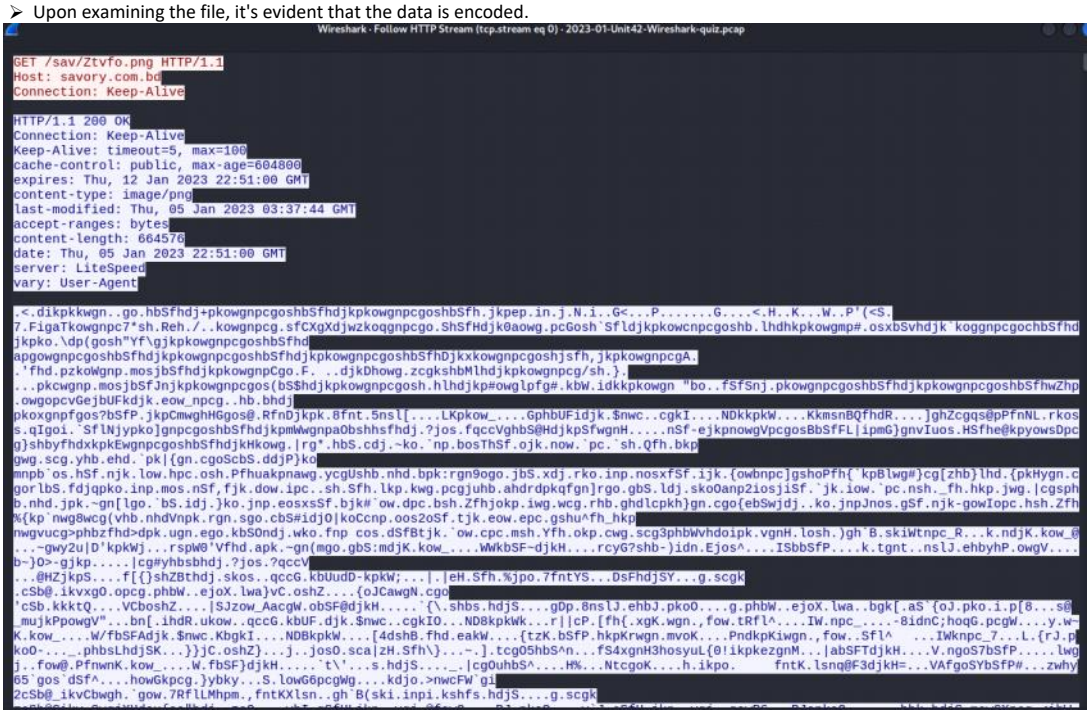
Upon initial inspection of our pcap file, we observe that the first line begins with a broadcast asking "who has 192.168.1.27," followed by the router's response providing the associated MAC address. We must verify that this IP address and MAC address correspond to the potential victim data we are investigating.



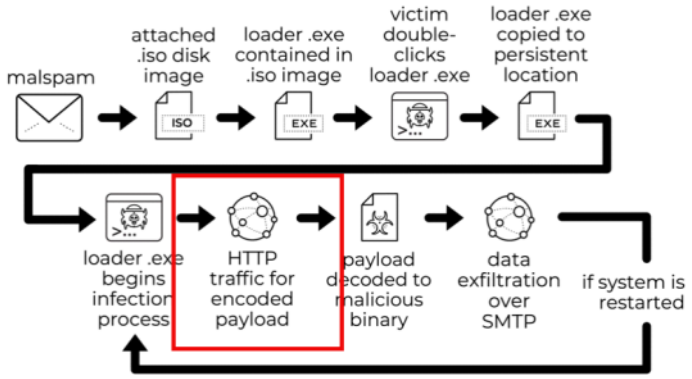
- A few packets down, we immediately observe a GET request for a PNG file.



- Upon examining the file, it's evident that the data is encoded.



- When we research a bit further into the flowchart of this malware from the image provided below.
  We can see the infection process of a variant of Agent Tesla malware, detailing HTTP traffic for encoded payload delivery.



➢ From this information we can derive that the source IP address 192.168.1.27 requested this PNG file, confirming it as our infected host. We can document the information provided, noting that the victim's IP address is 192.168.1.27, and the MAC address can be copied from this request.

```
    7 0.236136    192.168.1.27    45.56.99.101    TCP     54 51952 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
    8 0.237816    192.168.1.27    45.56.99.101    HTTP    130 GET /sav/Ztvfo.png HTTP/1.1
    9 0.238019    45.56.99.101    192.168.1.27    TCP     54 80 → 51952 [ACK] Seq=1 Ack=77 Win=64240 Len=0
```

✓ This discovery answers the following questions:

- What is the victim's IP address? **192.168.1.27**

```
      Protocol  Length Info
      ARP         42 Who has 192.168.1.27? Tell 192.168.1.1
37:9b:… ARP       42 192.168.1.27 is at bc:ea:fa:22:74:fb
      DNS         73 Standard query 0x56f1 A savory.com.bd
      DNS         89 Standard query response 0x56f1 A savory.com.bd
```

- What is the victim's MAC address? **bc:ea:fa:22:74:fb**

➢ Our next task is to determine when the malicious traffic started. To find this information, we can inspect the payload request and examine the headers to locate the time and date.

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2023-01-Unit42-Wireshark-quiz.pcap

```
GET /sav/Ztvfo.png HTTP/1.1
Host: savory.com.bd
Connection: Keep-Alive

HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
cache-control: public, max-age=604800
expires: Thu, 12 Jan 2023 22:51:00 GMT
content-type: image/png
last-modified: Thu, 05 Jan 2023 03:37:44 GMT
accept-ranges: bytes
content-length: 664576
date: Thu, 05 Jan 2023 22:51:00 GMT
server: LiteSpeed
vary: User-Agent

.<.dikpkkwgn..go.hbSfhdj+pkowgnpcgoshbSfhdjkpkowgnpcgoshbSfh.jkpep.in.j.N.i..G<...P.......G....<.H..K...W..P'(<S.
7.FigaTkowgnpc7*sh.Reh./..kowgnpcg.sfCXgXdjwzkoqgnpcgo.ShSfHdjk0aowg.pcGosh`Sfldjkpkowcnpcgoshb.lhdhkpkowgmp#.osxb
jkpko.\dp{gosh"Yf\gjkpkowgnpcgoshbSfhd
apgowgnpcgoshbSfhdjkpkowgnpcgoshbSfhdjkpkowgnpcgoshjsfh,jkpkowgnpcgA.
.'fhd.pzkoWgnp.mosjbSfhdjkpkowgnpCgo.F. ..djkDhowg.zcgkshbMlhdjkpkowgnpcg/sh.}.
...pkcwgnp.mosjbSfJnjkpkowgnpcgos(bS$hdjkpkowgnpcgosh.hlhdjkp#owglpfg#.kbW.idkkpkowgn "bo..fSfSnj.pkowgnpcgoshbSfh
.owgopcvGejbUFkdjk.eow_npcg..hb.bhdj
pkoxgnpfgos?bSfP.jkpCmwghHGgos@.RfnDjkpk.8fnt.5nsl[....LKpkow_....GphbUFidjk.$nwc..cgkI....NDkkpkW....KkmsnBQfhdR.
s.qIgoi.`SflNjypko]gnpcgoshbSfhdjkpmWwgnpaObshhsfhdj.?jos.fqccVghbS@HdjkpSfwgnH.....nSf-ejkpnowgVpcgosBbSfFL|ipmG}
g}shbyfhdxkpkEwgnpcgoshbSfhdjkHkowg.|rg*.hbS.cdj.~ko.`np.bosThSf.ojk.now.`pc.`sh.Qfh.bkp
```

- When did the malicious traffic start in UTC? **05 Jan 2023 22:51:00**

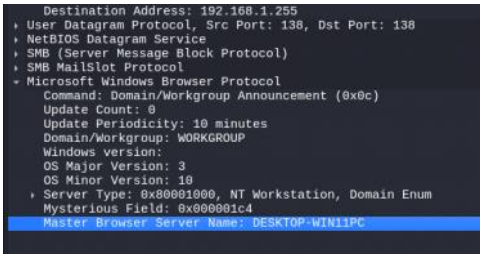
➢ Our next question asks us about the victim's Windows host name and user account name, so our first step is to filter for Windows traffic, such as NBNS and SMB, on the network. This will allow us to identify commonly generated Windows communications, including host names and user account names.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

nbns or smb or smb2

No.	Time	Source	Destination	Protocol	Length	Info
677	36.406254	192.168.1.27	192.168.1.1	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>
678	37.920864	192.168.1.27	192.168.1.1	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>
679	39.436389	192.168.1.27	192.168.1.1	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>
699	156.418779	192.168.1.27	192.168.1.1	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>
700	158.028798	192.168.1.27	192.168.1.1	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>
701	159.653669	192.168.1.27	192.168.1.1	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>
704	197.201989	192.168.1.27	192.168.1.255	BROWSER	258	Domain/Workgroup Announcement WORKGROUP,
786	276.420884	192.168.1.27	192.168.1.1	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>
787	277.935782	192.168.1.27	192.168.1.1	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>
816	279.436262	192.168.1.27	192.168.1.1	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>

➢ If we examine the packet under the Microsoft Windows Browser Protocol, the "Master Browser Server Name" field indicates the name of the computer currently acting as the Master Browser on the network, is "DESKTOP-WIN11PC".

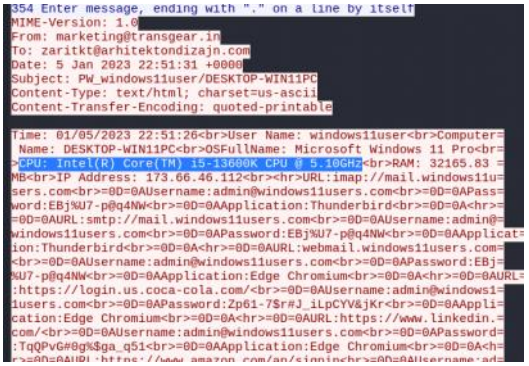


- What is the victim's Windows host name? **DESKTOP-WIN11PC**

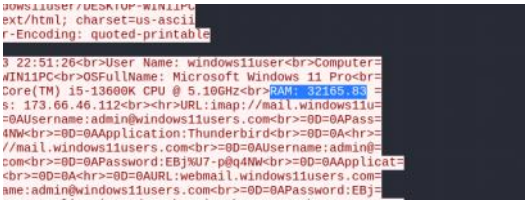
➢ Our next question is asking us to find the victim's Windows user name, to do this we look at SMTP traffic and by following the TCP stream, we can see exfiltrated data from the email includes the infected PC's username, "Windows11user," which we can use as the user account name.

- What is the victim's Windows user account name? **windows11user**

➢ Our next question asks us about what type of CPU is used by the victims host and how much RAM does the victim have.
This information can be found in this same exfiltrated data from the email in the TCP stream.

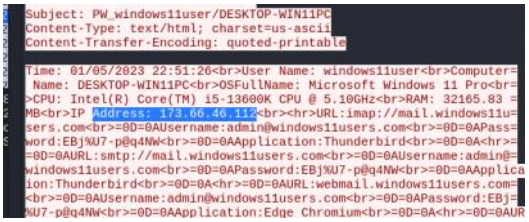


- What type of CPU is used by the victim's host? **Intel® Core™ i5-13600K CPU @ 5.10GHz**



- How much RAM does the victim's host have? **32GB**

Then it asks us what is the public IP address of the of the victim's host. This can also be found in the email.



- What is the public IP address of the victim's host? **173.66.46.112**

➢ Our final question pertains to the type of account login data that the malware has acquired.

- What type of account login data was stolen by the malware? **The malware stole usernames and passwords from multiple accounts, including email, social media, and shopping websites.**

🏁 Conclusion

This real-world example demonstrates the importance of analyzing packet captures (pcap) to understand and interpret network traffic associated with potential malware infections.