2019-12-03 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to exercise: https://www.malware-traffic-analysis.net/2019/12/03/index.html

Links to some tutorials I've written that should help with this exercise:

- Customizing Wireshark - Changing Your Column Display
- Using Wireshark: Identifying Hosts and Users
- Using Wireshark - Display Filter Expressions
- Using Wireshark: Exporting Objects from a Pcap

ENVIRONMENT FOR THE PCAP:

- LAN segment range: 10.18.20.0/24 (10.18.20.0 through 10.18.20.255)
- Domain: icemaiden.com
- Domain controller: 10.18.20.08 - Icemaiden-DC
- LAN segment gateway: 10.18.20.1
- LAN segment broadcast address: 10.18.20.255

QUESTIONS:

- What is the IP address, MAC address, and host name of the infected Windows host?
- What is the Windows user account name of the victim on this infected Windows host?
- What type of malware was the victim infected with?
- Based on traffic from the pcap, where did the malware possibly come from?
- After the initial infection, what type of web page/website did the victim appear to visit?

ANSWERS:

Q: What is the IP address, MAC address, and host name of the infected Windows host?
A: **10.18.20.97, 00:01:24:56:9b:cf, JUANITA-WORK-PC**

Q: What is the Windows user account name of the victim on this infected Windows host?
A: **momia.juanita**

2019-12-03 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Q: What type of malware was the victim infected with?
A: **Ursnif**

Q: Based on traffic from the pcap, where did the malware likely come from?
A: **Possibly from email, since the user went to mail.aol.com shortly before getting infected.**

Q: After the initial infection, what type of web page/website did the victim appear to visit?
A: **Looks like the victim went to a banking website, because of several domains in the HTTPS traffic ending in bankofamerica.com.**

NOTES:

Q: What is the IP address, MAC address, and host name of the infected Windows host?
A: 10.18.20.97, 00:01:24:56:9b:cf, JUANITA-WORK-PC

You can identify the IP address based on the pcap itself. All traffic is going to or from IP address 10.18.20.97. You can find the MAC address as described in this tutorial. You can also find the host name by filtering on ***kerberos.CNameString*** as described in the same tutorial.

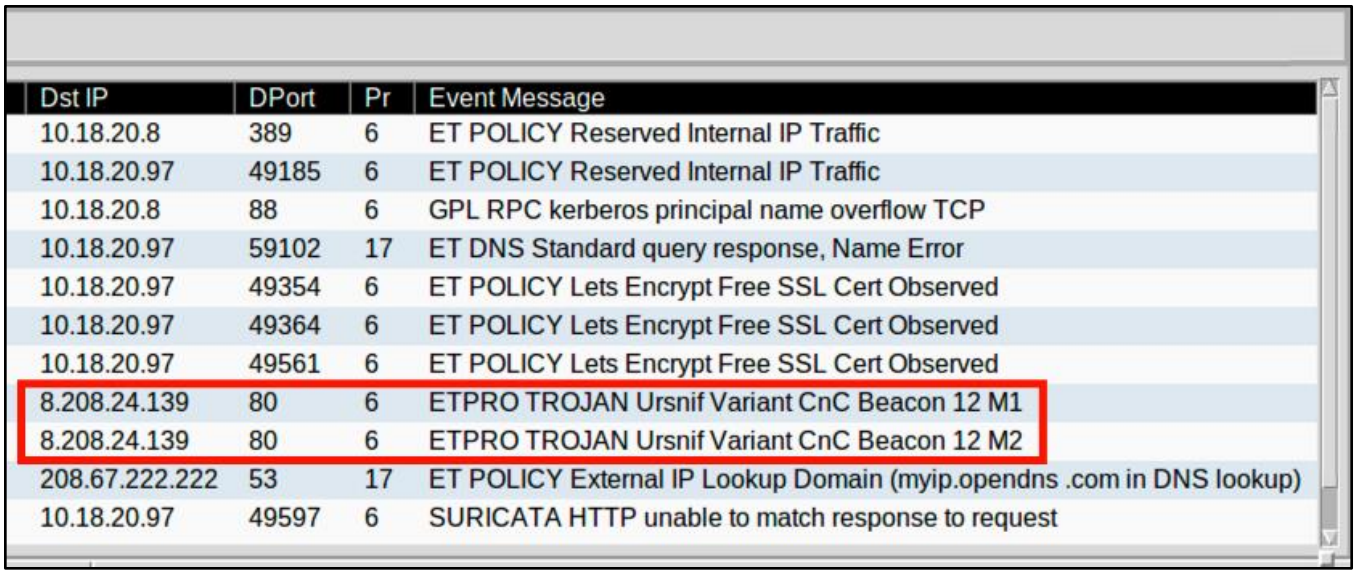
Q: What is the Windows user account name of the victim on this infected Windows host?
A: momia.juanita

You can also find the host name by filtering on ***kerberos.CNameString*** as described in the tutorial I mentioned in the last question.

Q: What type of malware was the victim infected with?
A: Ursnif

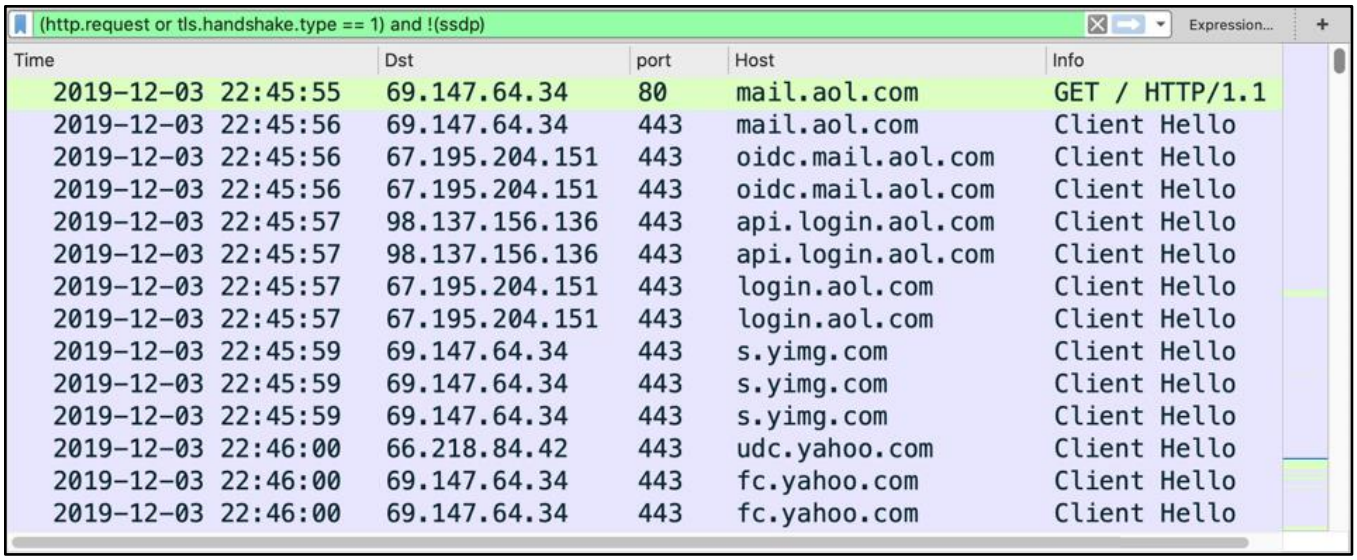
You can find this in the alerts from the image or the text file.

2019-12-03 - TRAFFIC ANALYSIS EXERCISE ANSWERS



Dst IP	DPort	Pr	Event Message
10.18.20.8	389	6	ET POLICY Reserved Internal IP Traffic
10.18.20.97	49185	6	ET POLICY Reserved Internal IP Traffic
10.18.20.8	88	6	GPL RPC kerberos principal name overflow TCP
10.18.20.97	59102	17	ET DNS Standard query response, Name Error
10.18.20.97	49354	6	ET POLICY Lets Encrypt Free SSL Cert Observed
10.18.20.97	49364	6	ET POLICY Lets Encrypt Free SSL Cert Observed
10.18.20.97	49561	6	ET POLICY Lets Encrypt Free SSL Cert Observed
8.208.24.139	80	6	ETPRO TROJAN Ursnif Variant CnC Beacon 12 M1
8.208.24.139	80	6	ETPRO TROJAN Ursnif Variant CnC Beacon 12 M2
208.67.222.222	53	17	ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)
10.18.20.97	49597	6	SURICATA HTTP unable to match response to request

Q: Based on traffic from the pcap, where did the malware likely come from?
A: Possibly from email, since the user went to ***mail.aol.com*** shortly before getting infected.

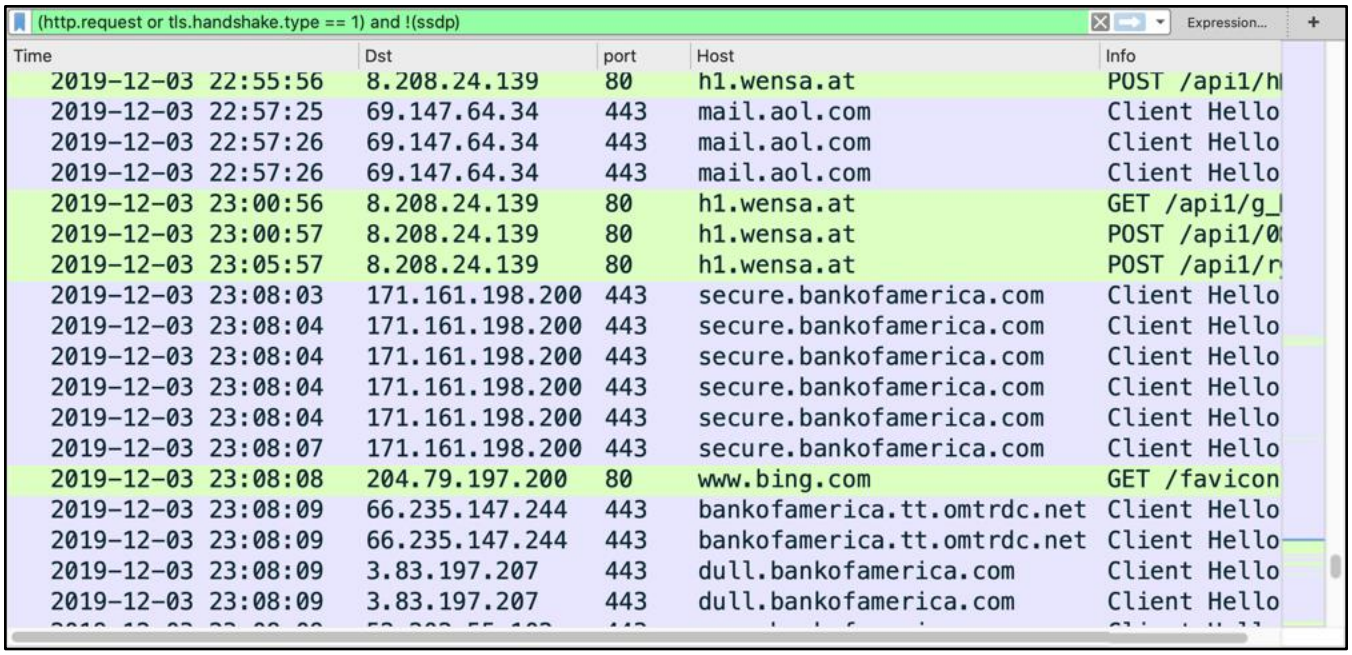


(http.request or tls.handshake.type == 1) and !(ssdp)

Time	Dst	port	Host	Info
2019-12-03 22:45:55	69.147.64.34	80	mail.aol.com	GET / HTTP/1.1
2019-12-03 22:45:56	69.147.64.34	443	mail.aol.com	Client Hello
2019-12-03 22:45:56	67.195.204.151	443	oidc.mail.aol.com	Client Hello
2019-12-03 22:45:56	67.195.204.151	443	oidc.mail.aol.com	Client Hello
2019-12-03 22:45:57	98.137.156.136	443	api.login.aol.com	Client Hello
2019-12-03 22:45:57	98.137.156.136	443	api.login.aol.com	Client Hello
2019-12-03 22:45:57	67.195.204.151	443	login.aol.com	Client Hello
2019-12-03 22:45:57	67.195.204.151	443	login.aol.com	Client Hello
2019-12-03 22:45:59	69.147.64.34	443	s.yimg.com	Client Hello
2019-12-03 22:45:59	69.147.64.34	443	s.yimg.com	Client Hello
2019-12-03 22:45:59	69.147.64.34	443	s.yimg.com	Client Hello
2019-12-03 22:46:00	66.218.84.42	443	udc.yahoo.com	Client Hello
2019-12-03 22:46:00	69.147.64.34	443	fc.yahoo.com	Client Hello
2019-12-03 22:46:00	69.147.64.34	443	fc.yahoo.com	Client Hello

Q: After the initial infection, what type of web page/website did the victim appear to visit?
A: A banking website, because of several domains in the HTTPS traffic ending in ***bankofamerica.com***.

2019-12-03 - TRAFFIC ANALYSIS EXERCISE ANSWERS



This exercise is dedicated to Mummy Juanita, also known as the ***Lady of Ampato***.