2019-08-20 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to exercise: https://www.malware-traffic-analysis.net/2019/08/20/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

LAN segment data:

- LAN segment range: **10.8.20.0/24** (10.8.20.0 through 10.8.20.255)
- Domain: **spraline.com**
- Domain controller: **10.8.20.8** (Spraline-DC)
- LAN segment gateway: **10.8.20.1**
- LAN segment broadcast address: **10.8.20.255**

Src IP	SPort	Dst IP	DPort	Pr	Event Message
10.8.20.101	49202	94.103.87.160	80	6	ETPRO CURRENT_EVENTS MalDoc Requesting Ursnif Payload 2018-09-24
10.8.20.101	49206	172.217.6.174	80	6	ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1
10.8.20.101	49206	172.217.6.174	80	6	ETPRO TROJAN Ursnif Variant CnC Beacon 8 M2
10.8.20.101	49214	94.103.86.146	80	6	ETPRO CURRENT_EVENTS Ursnif Loader Activity 2018-09-25
185.193.141.166	443	10.8.20.101	49217	6	ETPRO TROJAN Zeus Panda Banker / Ursnif Malicious SSL Certificate Det...
191.37.181.152	449	10.8.20.101	49222	6	ETPRO TROJAN Observed Trickbot Style SSL Cert (Internet Widgets Pty Ltd)
89.105.203.184	443	10.8.20.101	49224	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dri...
185.117.75.41	447	10.8.20.101	49231	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dri...
185.183.98.232	80	10.8.20.101	49238	6	ET MALWARE Windows executable sent when remote host claims to sen...
185.183.98.232	80	10.8.20.101	49238	6	ET MALWARE Windows executable sent when remote host claims to sen...
185.183.98.232	80	10.8.20.101	49238	6	ET SHELLCODE Possible TCP x86 JMP to CALL Shellcode Detected
185.183.98.232	80	10.8.20.101	49238	6	ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile
170.238.117.187	8082	10.8.20.101	49241	6	ETPRO TROJAN Trickbot Checkin Response
10.8.20.101	49242	170.238.117.187	8082	6	ET TROJAN [PTsecurity] Trickbot Data Exfiltration
10.8.20.101	49244	185.183.98.232	80	6	ETPRO TROJAN Trickbot Requesting networkDll Module
10.8.20.101	49511	170.238.117.187	8082	6	ET TROJAN Suspicious POST with Common Windows Process Names - Po...
10.8.20.101	49511	170.238.117.187	8082	6	ETPRO TROJAN W32/Trickbot C2 (networkDll module)

Shown above: Alerts on the traffic from this exercise.

QUESTIONS:

- When did the infection happen (date and time in UTC)?
- What is the IP address, MAC address, and host name of the infected Windows host?
- What is the Windows user account name for the infected Windows host?
- Based on the alerts, what type(s) of malware was the victim infected with?

2019-08-20 - TRAFFIC ANALYSIS EXERCISE ANSWERS

ANSWERS:

Q: When did the infection happen (date and time in UTC)?
A: **2019-08-20 at 19:31 UTC**

Q: What is the IP address, MAC address, and host name of the infected Windows host?
A: **10.8.20.101, 00:18:F3:A6:01:92, TAMPA-OFFICE-PC**

Q: What is the Windows user account name for the infected Windows host?
A: **reginald.chandler**

Q: Based on the alerts, what type(s) of malware was the victim infected with?
A: **Urnsif (also known as Gozi) and Trickbot**

NOTES:

Ursnif will often retrieve follow-up malware. In this case, the malware was Trickbot. In this infection, there are 3 HTTP GET requests that end in ***.rar*** that retrieved 3 Trickbot binaries:

- http://activity.gingcloud.com/wp-content/uploads/2019/08/4antifreeze.rar
- http://idogoiania.com.br/wp-content/uploads/2019/08/3antifreeze.rar
- http://boozzdigital.com/wp-content/uploads/2019/08/antifreeze.rar

Unfortunately, the content returned from these URLs is encoded or otherwise encrypted, and we cannot extract those particular Trickbot EXE files from the pcap.

Uranif traffic:

- 94.103.87.160 port 80 - ***bh79sbu.com*** - GET /qtra/ttqr.php?l=csuv3.j12 (returned initial Ursnif EXE)
- google.com - GET /images/[long string].avi (decoy URL generated by Ursif)
- 94.103.86.146 port 80 - ***hne53brianaea.com*** - GET /images/[long string].avi

2019-08-20 - TRAFFIC ANALYSIS EXERCISE ANSWERS

- 185.193.141.166 port 443 - ***kjoanaxbrennan.top*** - HTTPS/SSL/TLS traffic caused by Ursnif
- 139.198.5.65 port 80 - ***activity.qingcloud.com*** GET /wp-content/uploads/2019/08/4antifreeze.rar
- 139.198.5.65 port 443 - ***activity.qingcloud.com*** - HTTPS traffic (redirect from previous URL)
- 206.189.74.47 port 80 - ***idogoiania.com.br*** - GET /wp-content/uploads/2019/08/3antifreeze.rar
- 206.189.74.47 port 443 - ***idogoiania.com.br*** - HTTPS traffic (redirect from previous URL)
- 68.183.185.221 port 80 - ***boozzdigital.com*** - GET /wp-content/uploads/2019/08/antifreeze.rar

Trickbot traffic:

- 89.105.203.184 port 443 - SSL/TLS traffic caused by Trickbot
- 185.117.75.41 port 447 - SSL/TLS traffic caused by Trickbot
- 191.37.181.152 port 449 - SSL/TLS traffic caused by Trickbot
- 185.248.87.88 port 443 - ***api.ip.sb*** - HTTPS traffic - IP address check by the infected Windows host
- 170.238.117.187 port 8082 - ***170.238.117.187*** - POST /leo3/TAMPA-OFFICE-PC_W617601.ED4782C345F87239758E6C1922A1FC2A/81/
- 170.238.117.187 port 8082 - ***170.238.117.187*** - POST /leo3/TAMPA-OFFICE-PC_W617601.ED4782C345F87239758E6C1922A1FC2A/83/
- 170.238.117.187 port 8082 - ***170.238.117.187:8082*** - POST /leo3/TAMPA-OFFICE-PC_W617601.ED4782C345F87239758E6C1922A1FC2A/90
- 185.183.98.232 port 80 - ***185.183.98.232*** - GET /samerton.png (returned a Trickbot EXE)
- 185.183.98.232 port 80 - ***185.183.98.232*** - GET /tablone.png (returned a Trickbot EXE)
- 185.183.98.232 port 80 - ***185.183.98.232*** - GET /wredneg2.png (returned a Trickbot EXE)

- mail.protonmail.com - HTTPS traffic generated by one of the Trickbot modules