2022-02-23 - TRAFFIC ANALYSIS EXERCOSE ANSWERS

Link to quiz:

- https://www.malware-traffic-analysis.net/2022/02/23/index.html

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

- Wireshark Tutorial: Changing Your Column Display
- Wireshark Tutorial: Identifying Hosts and Users
- Wireshark Tutorial: Display Filter Expressions
- Wireshark Tutorial: Exporting Objects from a Pcap
- Wireshark Tutorial: Wireshark Workshop Videos Now Available

ENVIRONMENT:

- LAN segment range: 172.16.0.0/24 (172.16.0.0 through 172.16.0.255)
- Domain: sunnystation.com
- Domain Controller: 172.16.0.52 - SUNNYSTATION-DC
- File Server: 172.16.0.53 - SUNNYFILESERVER
- LAN segment gateway: 172.16.0.1
- LAN segment broadcast address: 172.16.0.255

TASK:

- What hosts/usernames are active on this network?
- What type of malware are they infected with?

ANSWERS:

Hosts/usernames

(Read: MAC address - IP address - host name - Windows account name)

- 2c:27:d7:d2:06:f5 - 172.16.0.131 - DESKTOP-VD151O7 - tricia.becker
- 00:12:f0:64:d1:d9 - 172.16.0.170 - DESKTOP-W5TFTQY - everett.french
- 00:1b:fc:7b:d1:c0 - 172.16.0.149 - DESKTOP-KPQ9FDB - nick.montgomery

Malware infections:

(Read: IP address - malware infection - start date/time)

- 172.16.0.131 - Formbook (XLoader) - 2022-02-23 at 18:29 UTC
- 172.16.0.170 - Emotet - 2022-02-23 at 18:25 UTC
- 172.16.0.149 - Emotet with spambot activity - 2022-02-23 at 18:24 UTC

2022-02-23 - TRAFFIC ANALYSIS EXERCOSE ANSWERS

Formbook/XLoalder Indicators of Compromise (IOCs):

HTTP GET request for Formbook/XLoader binary, returned the bytes in reverse order:

- 156.96.154.210 port 80 - 156.96.154.210 - GET /Ocklqc.jpg

The file returned from 156.96.154.210 is a binary that represents a Windows DLL file with the bytes in reverse order.

I found a Windows-based tool by Didier Stevens that reverses the byte order of a binary here. I used that tool to reverse the byte order and get the DLL file.

Couldn't get a positive ID on the DLL file from that binary, but the C2 traffic is definitely Formbook/XLoader.

Formbook/XLoader C2 traffic:

- 23.227.38.74:80 - www.katchybugonsale.com - GET /uar3/?*[base64 style string]*
- 72.167.191.69:80 - www.privilegetroissecurity.com - GET /uar3/?*[base64 style string]*
- 194.9.94.85:80 - www.hentainftxxx.com - GET /uar3/?*[base64 style string]*
- 198.54.117.210:80 - www.moonshot.properties - GET /uar3/?*[base64 style string]*
- 120.55.51.124:80 - www.nt-renewable.com - GET /uar3/?*[base64 style string]*
- 216.58.193.147:80 - www.elsiepupz.com - GET /uar3/?*[base64 style string]*
- 198.185.159.144:80 - www.jogoreviravolta.com - GET /uar3/?*[base64 style string]*
- 213.186.33.5:80 - www.seo-python.com - GET /uar3/?*[base64 style string]*
- 23.227.38.74:80 - www.db-propertygroup.com - GET /uar3/?*[base64 style string]*
- 216.58.193.147:80 - www.xn--pckwb0cye6947ajzku8opzi.com - GET /uar3/?*[base64 style string]*
- 154.206.65.249:80 - www.czzhudi.com - GET /uar3/?*[base64 style string]*
- 104.21.89.147:80 - www.hydrocheats.com - GET /uar3/?*[base64 style string]*
- 66.235.200.112:80 - www.riskprotek.com - GET /uar3/?*[base64 style string]*
- 198.54.117.215:80 - www.campdiscount.info - GET /uar3/?*[base64 style string]*
- 209.17.116.163:80 - www.mystore.guide - GET /uar3/?*[base64 style string]*
- 104.16.12.194:80 - www.theperfecttrainer.com - GET /uar3/?*[base64 style string]*
- 216.172.184.77:80 - www.globalsovereignbank.com - GET /uar3/?*[base64 style string]*
- 3.130.253.23:80 - www.keysine.com - GET /uar3/?*[base64 style string]*
- 173.231.37.114:80 - www.chinadqwx.com - GET /uar3/?*[base64 style string]*
- 184.168.99.26:80 - www.awridahmed.com - GET /uar3/?*[base64 style string]*
- 66.29.145.216:80 - www.ban-click.com - GET /uar3/?*[base64 style string]*

2022-02-23 - TRAFFIC ANALYSIS EXERCOSE ANSWERS

DNS queries for Formbook/XLoader C2 traffic:

- www.byaliciafryearson.com - response: No such name
- www.krpano.pro - response: No such name
- www.barrcoplumbingsupply.com - response: No such name
- www.32342240.xyz - response: No such name
- www.jmtmjz.com - response: No such name
- www.freedomteaminc.com - response: No such name
- www.centroimprenta.xyz - response: Server failure
- www.e-scooters.frl - response: No such name
- www.klassociates.info - response: No such name

Emotet IOCs from 172.16.0.170:

Traffic to download Emotet DLL:

- 178.211.56.194 port 443 - dalgahavuzu.com - HTTPS traffic
  Note: URLhaus indicates this is Emotet from its epoch 5 botnet (link).

Emotet C2:

- 27.254.174.84 port 8080 - HTTPS traffic
- 37.44.244.177 port 8080 - attempted TCP connections
- 37.59.209.141 port 8080 - attempted TCP connections
- 45.71.195.104 port 8080 - attempted TCP connections
- 54.37.106.167 port 8080 - HTTPS traffic
- 54.37.228.122 port 443 - attempted TCP connections
- 54.38.242.185 port 443 - HTTPS traffic
- 59.148.253.194 port 443 - HTTPS traffic
- 61.7.231.226 port 443 - HTTPS traffic
- 61.7.231.229 port 443 - HTTPS traffic
- 68.183.93.250 port 443 - attempted TCP connections
- 78.46.73.125 port 443 - attempted TCP connections
- 85.214.67.203 port 8080 - attempted TCP connections
- 103.41.204.169 port 8080 - attempted TCP connections
- 103.42.57.17 port 8080 - attempted TCP connections
- 104.131.62.48 port 8080 - attempted TCP connections
- 118.98.72.86 port 443 - attempted TCP connections

- 128.199.93.156 port 8080 - HTTPS traffic
- 128.199.192.135 port 8080 - HTTPS traffic
- 139.196.72.155 port 8080 - HTTPS traffic
- 159.69.237.188 port 443 - attempted TCP connections
- 162.144.76.184 port 8080 - HTTPS traffic
- 168.197.250.14 port 80 - HTTPS traffic
- 180.250.21.2 port 443 - HTTPS traffic
- 185.148.168.15 port 8080 - attempted TCP connections
- 185.148.168.220 port 8080 - attempted TCP connections
- 185.184.25.78 port 8080 - HTTPS traffic
- 190.90.233.66 port 443 - attempted TCP connections
- 191.252.103.16 port 80 - attempted TCP connections
- 194.9.172.107 port 8080 - attempted TCP connections
- 195.154.146.35 port 443 - attempted TCP connections
- 198.199.98.78 port 8080 - HTTPS traffic
- 210.57.209.142 port 8080 - attempted TCP connections

Emotet with spambot IOCs from 172.16.0.149:

Emotet DLL:

- www.ajaxmatters.com - GET /c7g8t/zbBYgukXYxzAF2hZc/

SHA256 hash for Emotet DLL:

- 14b57211308ac8ad2a63c965783d9ba1c2d1930d0cafd884374d143a481f9bf3

Emotet C2:

- 135.148.121.246 port 8080 - HTTPS Emotet C2 traffic
- 144.217.88.125 port 443 - HTTPS Emotet C2 traffic
- 134.209.156.68 port 443 - HTTPS Emotet C2 traffic

Spambot traffic:

- various IP addresses over TCP ports 25, 465, and 587 - spambot traffic

Note: There is an email from the spambot traffic over unencrypted SMTP you can export from the pcap in Wireshark by using ***File --> Export Objects --> IMF***