2020-08-21 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to exercise: https://www.malware-traffic-analysis.net/2020/08/21/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

ENVIRONMENT:

- LAN segment range: 10.08.21.0/24 (10.08.21.0 through 10.08.21.255)
- Domain: pizza-bender.com
- Domain controller: 10.08.21.8 - Pizza-Bender-DC
- LAN segment gateway: 10.08.21.1
- LAN segment broadcast address: 10.08.21.255

INCIDENT REPORT:

Executive summary:

On Friday, 2020-08-21 at approximately 15:04 UTC, a Windows 10 host used by Matthew Jones was infected with IcedID malware.

Victim details:

IP address: 10.8.21.163
MAC address: 10:c3:7b:0a:f2:85 (ASUSTekC_0a:f2:85)
Host name: DESKTOP-OF4FE8A
User account name: matthew.jones

Indicators of compromise (IOCs):

SHA256 hash: 054ff4620aaa40928ca67a2c364bedf71d79672874d75ba50ff82
31069ad74d9

- File size: 176,692 bytes
- File type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
- File location: http://ncznw6a.com/dujok/kevyl.php?l=ranec11.cab
- File description: DLL malware file - installer for IcedID

2020-08-21 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Malicious HTTP traffic:

- 45.12.4.190 port 80 - ncznw6a.com – GET /dujok/kevyl.php?l=ranec11.cab

Suspicious domains using HTTPS traffic:

- 5.147.231.132 port 443 - ldrbravo.casa
- 89.44.9.186 port 443 - siesetera.club
- 89.44.9.186 port 443 - ciliabba.cyou
- 89.44.9.186 port 443 - ubbifeder.cyou

NOTES

Related to this infection:

- https://urlhaus.abuse.ch/url/438584/
- https://bazaar.abuse.ch/sample/054ff4620aaa40928ca67a2c364bedf71d79672874d75ba50ff8231069ad74d9/
- https://app.any.run/tasks/c1c0bb00-f446-4921-a33e-31b899eb5ae3/
- https://capesandbox.com/analysis/49597/

Possibly related to this infection:

- https://app.any.run/tasks/996a7aaf-e62c-44ec-a3c9-9af72b99f222/

Other notes:

You can export an item of malware from the pcap, the binary returned in response to the HTTP GET request to ncznw6a.com. This is a DLL file.

Beware of any domains ending in uncommon TLDs like (but not limited to) ***.top***, ***.casa***, ***.club***, ***.cyou***, or ***.xyz***.