Malware Traffic Analysis

Source of the sample file: Malware traffic analysis

Scenario:

- LAN segment range: 10.0.19.0/24 (10.0.19.0 through 10.0.19.255)
- Domain: burnincandle.com
- Domain Controller: 10.0.19.9 - BURNINCANDLE-DC
- LAN segment gateway: 10.0.19.1
- LAN segment broadcast address: 10.0.19255

Task:

- Write an incident report based on traffic from the sample pcap
- The incident report should contains 3 sections:

    - **Executive Summary**: State in simple, direct terms what happened (when, who, what).
    - **Details**: Details of the victim (hostname, IP address, MAC address, Windows user account name).
    - **Indicators of Compromise (IOCs)**: IP addresses, domains and URLs associated with the infection. SHA256 hashes if any malware binaries can be extracted from the pcap.

Answers:

Executive summary:

On Monday 2022-03-21 at around 20:58 UTC, a Windows host used by Patrick Zimmerman was infected with IcedID (Bokbot) malware that led to Cobalt Strike.

Details:

- Host name: DESKTOP-5QS3D5D
- IP address: 10.0.18.14
- MAC address: 00:60:52:b7:33:0f
- Windows user account name: Patrick zimmerman

Domains and IP addresses for Cobalt Strike:

- 23.227.198.203 port 757 - bupdater.com - HTTPS traffic

Indicators of Compromise (IOCs):

Domains and IP addresses for IcedID (Bokbot):

- 188.166.154.118 port 80 - oceriesfornot.top - GET/
- 157.245.142.66 port 443 - antnosience.com - HTTPS traffic
- 160.153.32.99 port 443 - suncoastpinball.com - HTTPS traffic

- 157.245.142.66 port 443 - otectagain.top - HTTPS traffic
- 91.193.16.181 port 443 - seaskysafe.com - HTTPS traffic
- 91.193.16.181 port 443 - dilimoretast.com - HTTPS traffic

Suspicious traffic to file sharing domains:

- Port 443 - filebin.net - HTTPS traffic
- Port 443 - situla.bitbit.net - HTTPS traffic