Cyber Defense Organization

Network Forensics with Wireshark - Jonathan Matza - 02/21/2020

Wireshark (check if installed)

1. Go to this link https://www.wireshark.org/download.html
2. Click on the stable release and download Windows installer 64 bit
3. Leave everything at the defaults and click through
4. Reboot if prompted :)))

Telnet

1. Download on https://tinyurl.com/CDONetworkForensics
2. Looking for telnet: type in telnet on Wireshark0
3. Check out the IP Address and type this in ip.addr == 10.0.2.7
4. Now right click on the telnet data and say "follow tcp stream"

Making sense of basic packet information:

1. Go to this link:// https:www.joesandbox.com/analysis/209050/0/html#network in Kali and download the filtered pcap (you can do full to, it is a difference of 32 packets).
2. Keep that report open, it should help you process what you are seeing and give you context
3. Open the pcap in wireshark (double click on the pcap or go into wireshark and press file open)
4. Let's walk through the first 20 packets (this won't give you anything close to the answer but it is good to understand the communication to apply it to future cases)
    a. So first you have a DNS query from victim machine (The second is a DNS response with an A record, click on the 2nd packet and really dive into it (look for where it says the record type, the ip address, etc)
    b. Then you will notice a TCP handshake indicated by flags SYN, SYN ACK, ACK dive into those packets on wireshark and see the flag settings, source ip, destination ip, port info, etc. (only do 5 packets worth of these max)
    c. The TCP data is encrypted using TLS v1 (Transport Layer Security). It is a method of encrypting TCP connections.
    d. Notice the different steps of the TLS connection. Go to this link for more info on TLS:

Let's start investigating the Malware:

https:www.joesandbox.com/analysis/209050/0/html#network

1. First thing I like to do is filter by DNS records to see where it is trying to reach out to
    a. Type in dns in the filter box and hit enter

    b. Do you see anything suspicious? What looks out of place?
2. Google the subdomain. For example, for drive.google.com only lookup google.com.
3. What service does it provide? Why is that potentially malicious?
4. Another useful tool for looking up ip addresses is: http://cqcounter.com/whois/
5. Based on the DNS query, what is the malicious IP?

Next Steps

1. Great, You found the potentially malicious IP! Now let's filter based on that IP address.
2. Do you see a similar pattern to the initial packets I had you analyze at the beginning?
3. It is doing the same SYN, SYN ACK, ACK handshake as before, but this time there is some HTTP data in there.
4. Really take some time and dig into that HTTP data , expand everything and skim through it. Notice how some Hex characters indicate certain information: highlight cursor over the words
5. Now, recall how I said to keep that sandbox report? Pull it up now. Look for Snort NIDS (Network Intrusion Detection System). These use signatures to identify malicious behavior.
6. Now google the SID # (Stands for Search ID…. I think) for the rule. Start with the client checkin SID
7. Read the rule, what does it indicate (think about this before reading next step)?
8. Notice how it is really specific with the HTTP status code (200), the HTTP data content to look for, & the HTTP method (POST). The theory is that this string of Hex is always consistent in this type of malware's communications & that this specific combo of factors will point to malware communications
9. Now go back to Wireshark, do you see any packet that looks like it could match this rule description?
10. Right click on the packet and say "Follow TCP stream". This would allow you to view the entire conversation between the victim and malicious host
11. Go to **show and save data as**: and click Hex Dump
12. See that string of Hex gibberish from the Alert? Copy and paste the first 14 Hex values only and hit enter. Double click on the match and it should highlight the packet that contains it. Congrats! You found a malicious trojan checking into the c2 server.
13. Now see if you can find the server response using the same methodology. At the time of writing I was having trouble searching for it, but if you find it let me know.

MISC

1. If you have extra time explore more of the sample sandbox report. Networking only tells part of the story.