Questions for Preliminary Selection of Fin Drill 2023

Your organization is concerned about the recent ransomware threat actors. Your leadership management has received a couple of threat intelligence reports from various sources and asked the SOC and Cyber Threat Intelligence Unit to collaborate to find any suspicious activities regarding two infamous ransomware group in particular, Lockbit 3.0 and CL0p ransomware. Your team is provided with the following threat intelligence reports for this activities-

1. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
2. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

You are now assigned to analyze the attached pcap and answer the following questions-

Q1. There are two prominent domain names in this pcap which are related to Lockbit 3.0 What are the names of those two domains?

Ans:

Q2. Which ip addresses were resolved for the two domains for Lockbit3.0 in Question 1?
Ans: **89.22.239.240** and **144.76.136.153**

Q3. There were '**failed attempts**' to connect with two IOC of CL0P ransomware which is captured in the pcap. What are the domain names of these two IOC?
Ans:

Q4. Which ip addresses were resolved for the two domains for CL0P ransomware in Question 3?
Ans:

From the same pcap there are several suspicious footprints which needs to be investigated but those are not related with the threat intelligence reports which are shared for Lockbit3.0 and CL0p ransomware. Answer the following to find out about those suspicious activities-

Q5: How many unique suspicious domains are found from the pcap for attempted downloads of files with the extension '.exe' or '.php'?
Ans:

Q6: There is an embedded ip address in one of the downloaded scripts from the suspicious domains of Question 5. This ip is used in http://x.x.x.x format inside the script. What is the value of this ip address?
Ans:

Q7: What is the name of the domain which was used to download the script in Question 6?

Q8: What was the duration for the entire HTTP communication to download the suspicious script for Q6?

Q9: In the provided pcap there is a suspicious ip address who is trying to perform network scans in stealth mode. What is this suspicious ip address?

Q10: How many packets are sent **ONLY** for the stealth scan by the suspicious ip address in Q9?