Week 2 - Practical Task: The Suspicious Download

Objective

This task simulates the analysis of a packet capture (PCAP) file. Your goal is to use a *summary* of network traffic to identify a malicious event. This teaches you to "read" network conversations and identify attacker TTPs.

Scenario

You are a Tier 1 Analyst. At 14:30:05 UTC, an IDS (Intrusion Detection System) alert fires:

"IDS Alert: [1] Potential EXE Download over HTTP from Known-Bad Domain"

You are given a summary of the 15 "key" packets from around that time. The user's machine is 192.168.50.10 (DESKTOP-C7G3P2).

Key Packet Summary

Pkt	Time	Source IP	Dest. IP	Protocol	Info
1	14:30:01	192.168.50.10	1.1.1.1	DNS	Standard query for freetoolz-archive.com
2	14:30:01	1.1.1.1	192.168.50.10	DNS	Standard query response: freetoolz-archive.com A 185.12.33.4
3	14:30:02	192.168.50.10	185.12.33.4	TCP	[SYN]
4	14:30:02	185.12.33.4	192.168.50.10	TCP	[SYN, ACK]
5	14:30:02	192.168.50.10	185.12.33.4	TCP	[ACK]
6	14:30:03	192.168.50.	185.12.33.4	HTTP	**GET**

		10			/downloads/installer.exe HTTP/1.1 Host: freetoolz-archive.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)...
7	14:30:03	185.12.33.4	192.168.50.10	HTTP	HTTP/1.1 200 OK Content-Type: application/x-msdownload Content-Length: 512000
8	14:30:04	185.12.33.4	192.168.50.10	TCP	[TCP segment data]... (This is the file being sent)
9	14:30:05	185.12.33.4	192.168.50.10	TCP	[FIN, ACK] (Server is done sending)

10	14:30:05	192.168.50.10	185.12.33.4	TCP	[FIN, ACK] (Client acknowledges)
--- 5 seconds later ---					
11	14:30:10	192.168.50.10	198.51.100.5	TCP	[SYN]
12	14:30:11	192.168.50.10	198.51.100.5	TCP	[SYN] (Retransmission)
13	14:30:12	192.168.50.10	198.51.100.5	TCP	[SYN] (Retransmission)
14	14:30:13	192.168.50.10	45.1.8.22	TCP	[SYN]
15	14:30:13	45.1.8.22	192.168.50.10	TCP	[SYN, ACK]

Your Task

Analyze the packet summary and answer the following questions.

1. **The Download:**
   - What is the user's IP address?
   - What is the IP address of the server they downloaded the file from?
   - What is the *name* of the file that was downloaded?
   - What was the *size* of the file in bytes?
2. **The Connection:**
   - What packets (by number) show the TCP 3-Way Handshake for the *file download*?
   - What packet (by number) shows the *request* for the file?

- What packet (by number) shows the server *agreeing* to send the file?

3. **The "C2" (Command & Control):**
   - After the download, something *new* happens. What is the *first* "new" IP address the user's machine tries to contact?
   - Look at packets 11, 12, and 13. Is this connection succeeding? Why or why not? (Hint: Look at the 3-Way Handshake).
   - What happens in packet 14? Does this look like C2 "beaconing"?
4. **Tying it to the Kill Chain:**
   - In your opinion, what Kill Chain stage does Packet 6 (GET /downloads/installer.exe) represent?
   - What Kill Chain stage do Packets 11-15 represent?
5. **Final Recommendation:**
   - Is the IDS alert a True Positive or False Positive?
   - As a Tier 1 Analyst, what is your immediate next step?