ATHANASIUS J.K GADOSEY

Week 2

Practical Task: The Suspicious Download

The following answers below are the analysis packet summary for the task:

1. The Download:

    - **The user's IP address**: 192.168.50.10
    - **The Evil server IP address:** .185.12.33.4
    - **The file downloaded:** installer.exe.
    - **The file size**: 51200 bytes

2. The Connection:

    - **The TCP 3-way handshake file download with the packet number**: SYN = 3, SYN–ACK = 4, ACK = **5**
    - **Packet requesting file**: PKT 6
    - **Server agrees to send the file:** Pkt 7

3. The "C2" (Command & Control):

    - **The first new IP address contacted after download**: 192.51.100.5
    - **Is the connection succeeding?:** No, because the connection isn't going through. Packets 11, 12, and 13 show the computer sending SYN requests over and over, but it never gets a reply back. Since there's no SYN/ACK coming from the other side, the handshake never completes, and the connection fails.
    - **What happens in packet 14?**
      In packet 14, the client device tries a new IP (45.1.8.22), and this time the server replies in packet 15. This looks like C2 beaconing

4. Tying it to the Kill Chain:
    - **Packet 6 (file download) represents:** This is the Delivery stage, the malicious installer.exe is downloaded to the victim's machine.
    - **Packet 11-15 represents**: These fall under Command and Control (C2), the host then starts reaching out to external IPs, which looks like beaconing.

5. Recommendations:
   This is a **true Positive**. The user downloaded an EXE from a known-bad domain, and right after that, the machine tried connecting to suspicious IPs.:

   Next Step:
   I will immediately isolate **DESKTOP-C7GP2** from the network and escalate to Tier 2 for malware analysis