### **HoneyBOT — CyberDefenders**

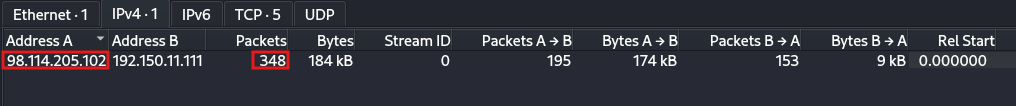
Scenario: A PCAP analysis exercise highlighting attacker’s interactions with honeypots and how automatic exploitation works.. (Note that the IP address of the victim has been changed to hide the true location.)

As a soc analyst, analyze the artifacts and answer the questions.

Tasks:

1. What is the attacker’s IP address?

Check the conversations tab in wireshark and see which IP is sending the most amount of traffic.



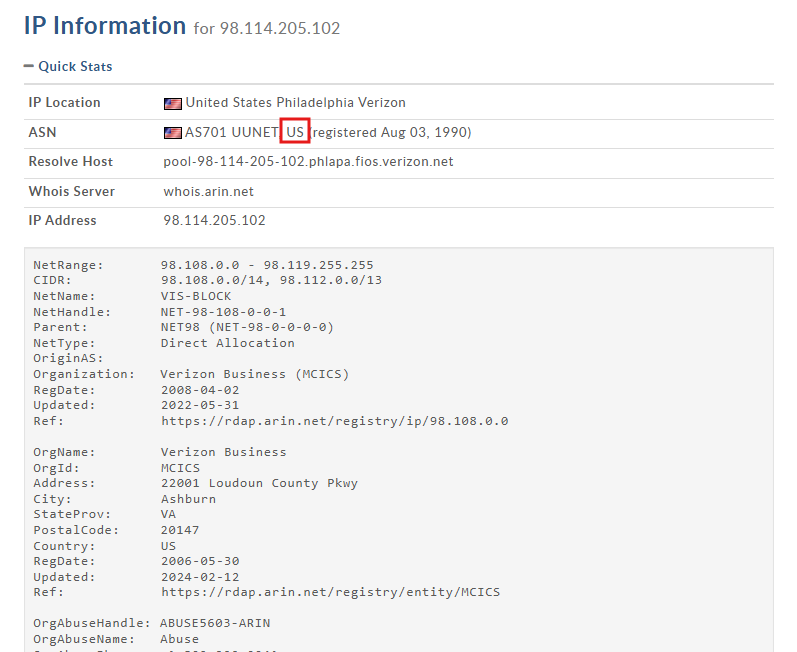
Answer: 98.114.205.102

2. What is the target’s IP address?

From the above screenshot we can see the answer to this question.  
Answer:192.150.11.111

3. Provide the country code for the attacker’s IP address (a.k.a geo-location).

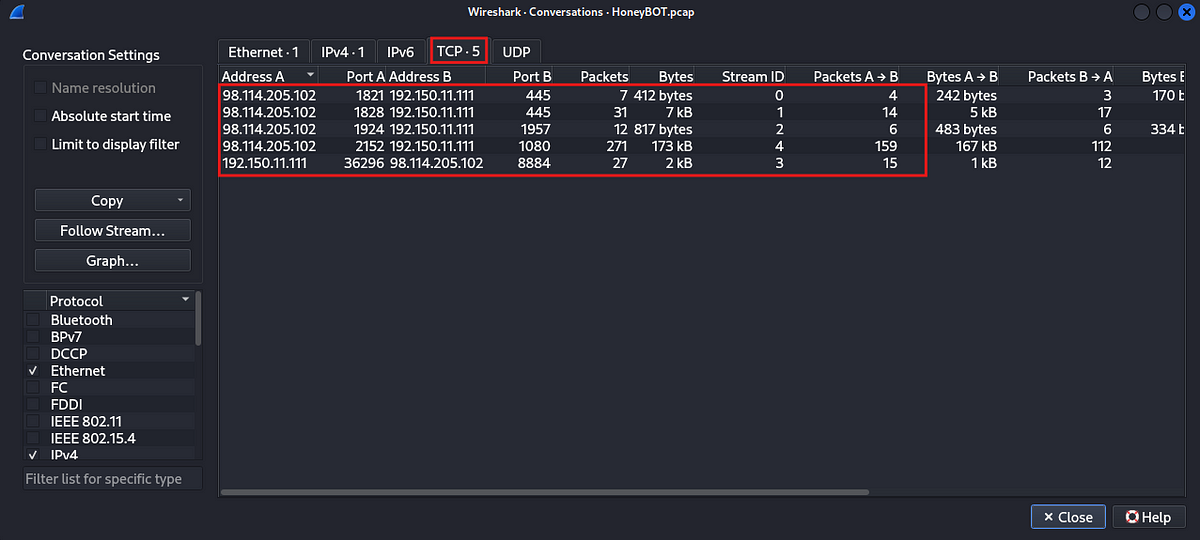
Open Whois domain tools and search for the particular IP.



Answer: US

4. How many TCP sessions are present in the captured traffic?

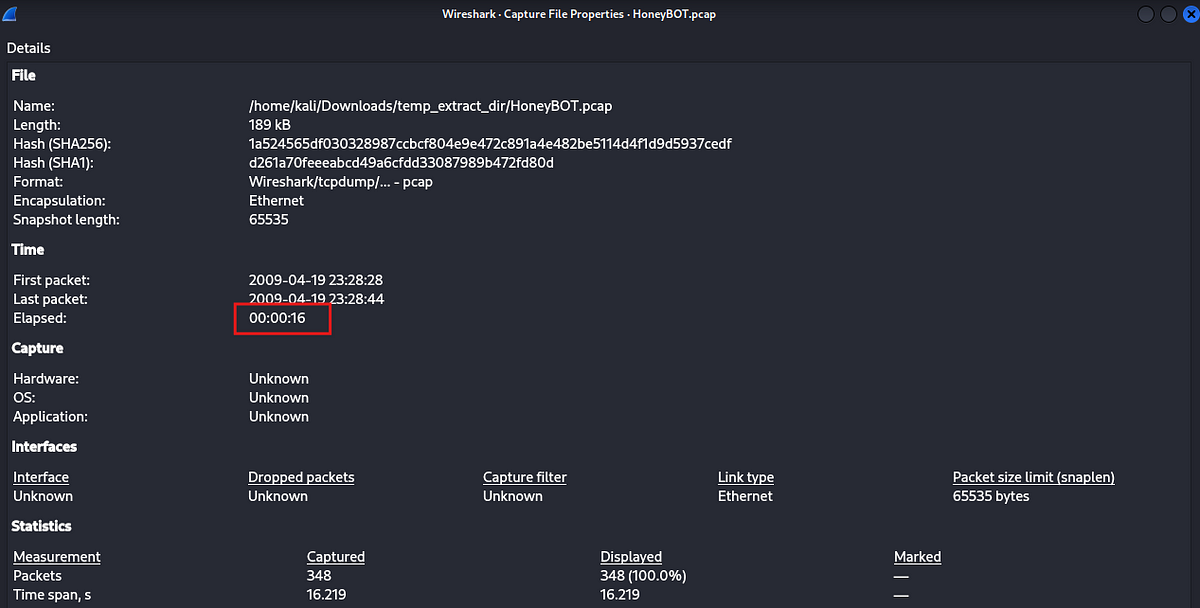
Go to the conversations tab and check the TCP tab.



Answer: 5

5. How long did it take to perform the attack (in seconds)?

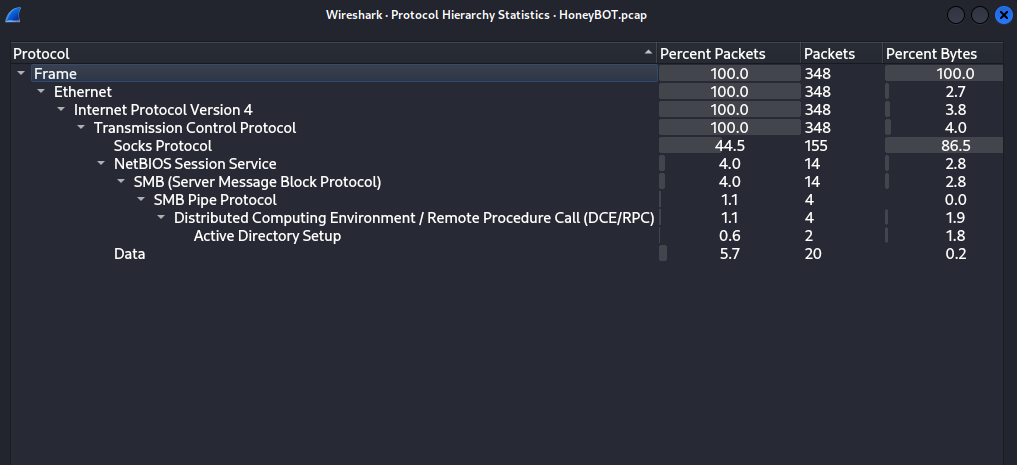
Check the capture file properties under the statistics menu.



Answer: 16

6. Provide the CVE number of the exploited vulnerability.

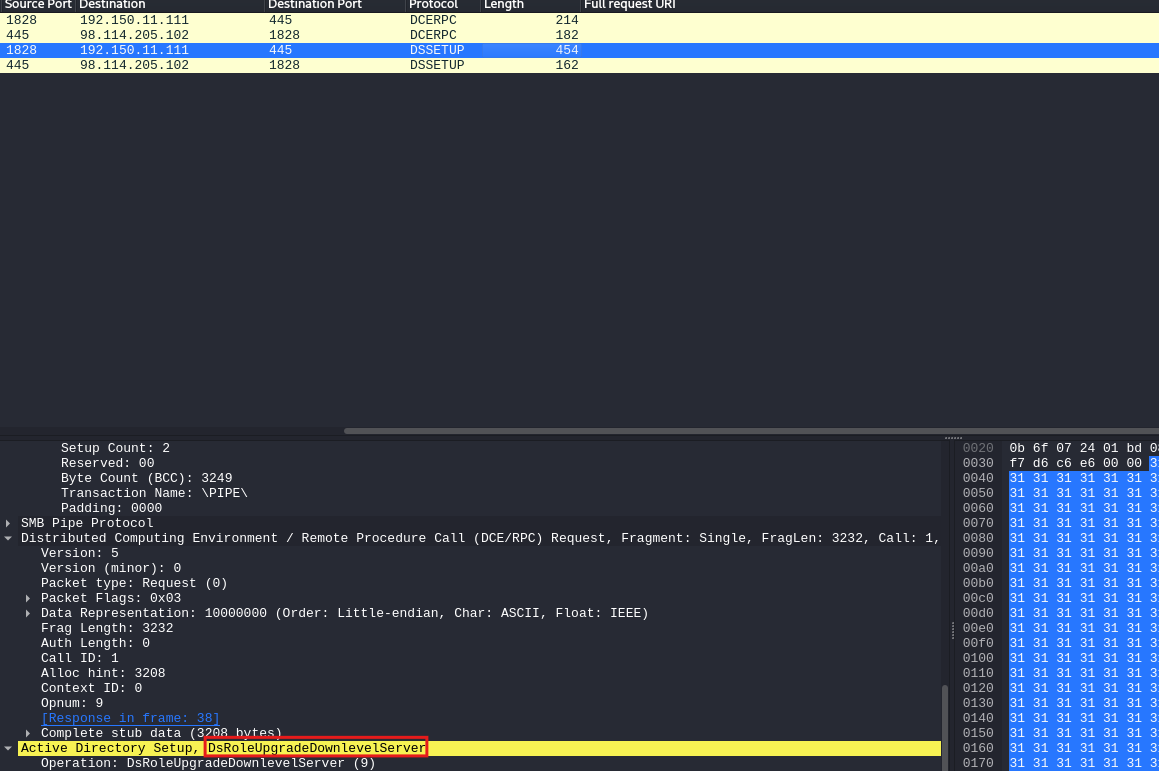
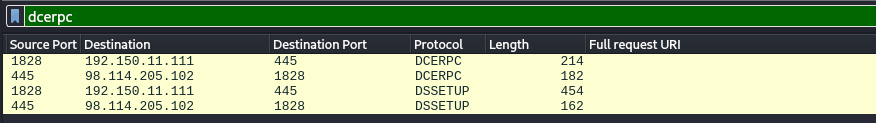
To find out the CVE, we need to first identify the kind of traffic that is being sent. Let us first check the protocol hierarch.



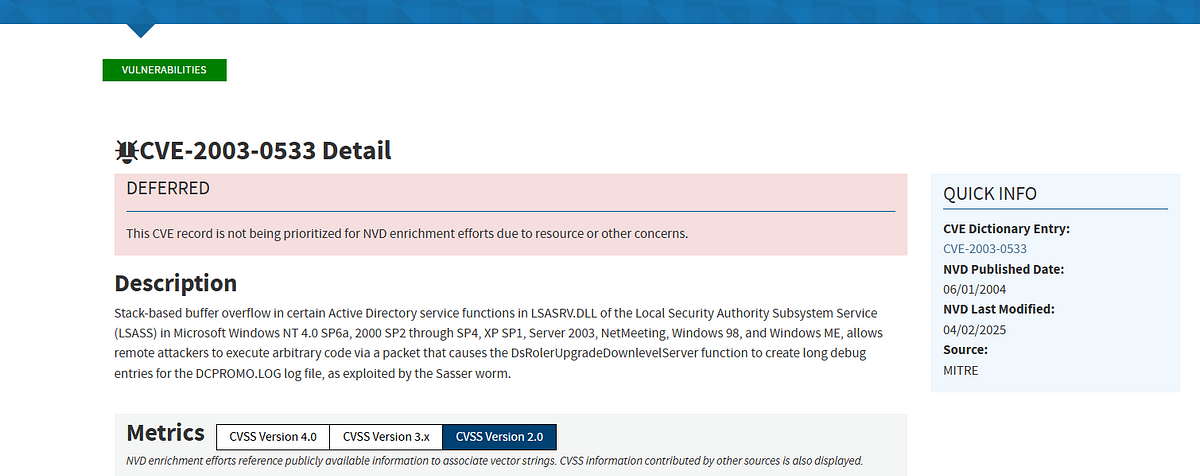
We can see how the attacker had accessed the system. They connected via socks protocol(Proxy), then opened an SMB connection, then initiated DCE/RPC call to AD Setup API.

Let us check the data in the DCE/RPC packets.

Filter: dcerpc



We can see above that a call to DsRoleUpgradeDownlevelServer was made. A quick google search revealed that this is an attempt to exploit the vulnerability CVE-2003–0533



Answer: CVE-2003–0533

7. Which protocol was used to carry over the exploit?

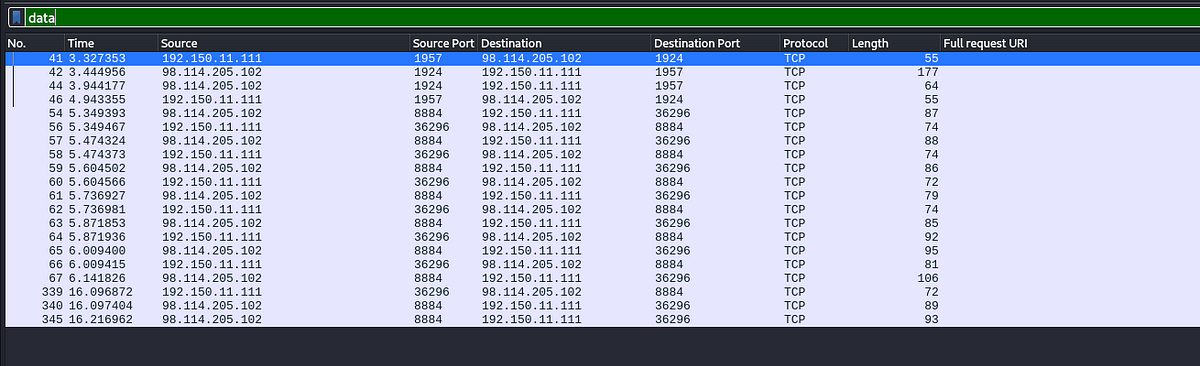
We saw in the protocol hierarchy that the attacker first connected over SMB and then used the SMB named pipes to communicate with DCE/RPC.

Answer: SMB

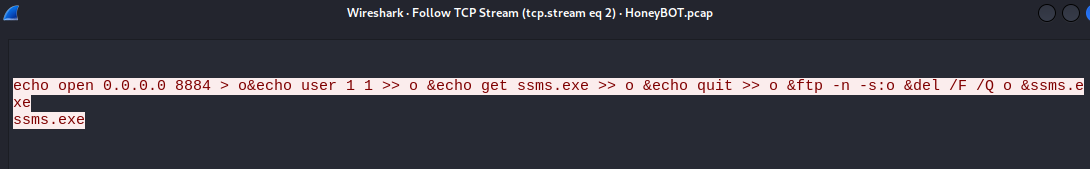
8. Which protocol did the attacker use to download additional malicious files to the target system?

In the protocol hierarchy, there was “data” which represents raw packet data, which Wireshark could not determine the exact protocol of. Let us check these packets to find out how the attacker sent over additional files.

Filter: data.



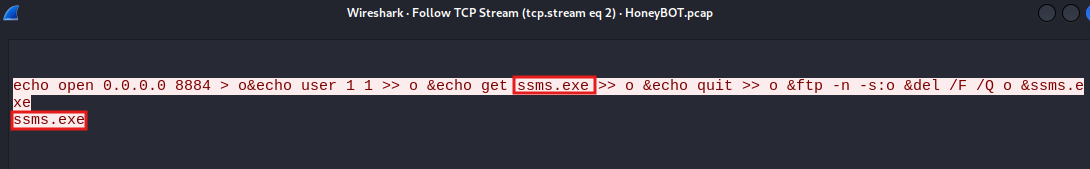
Let us examine these packets. Select a packet and hit follow TCP stream.



We can clearly see that this is FTP traffic.

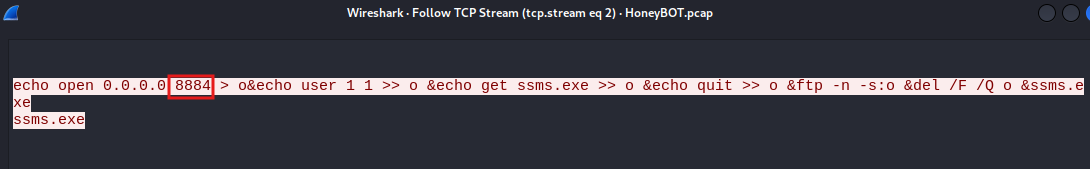
Answer: FTP

9. What is the name of the downloaded malware?



Answer: ssms.exe

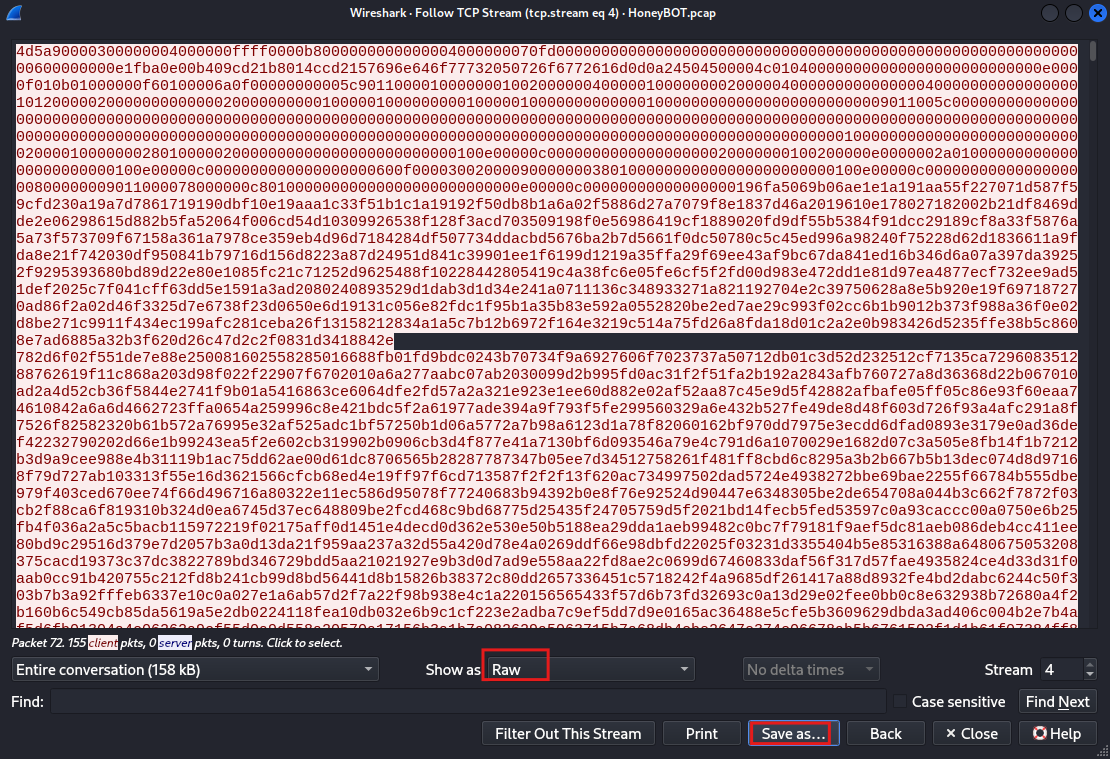
10. The attacker’s server was listening on a specific port. Provide the port number.



Answer: 8884

11. When was the involved malware first submitted to VirusTotal for analysis? Format: YYYY-MM-DD

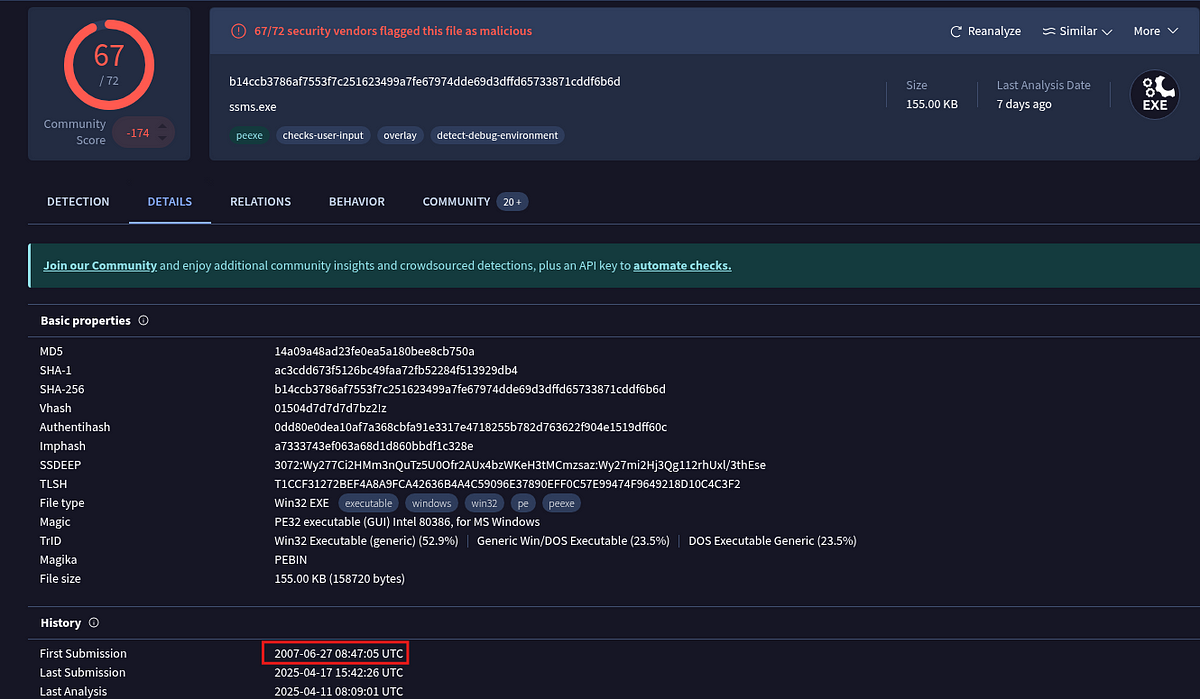
Go to the packet where the code for the malicious exe was sent over, then select save as and save the malicious code locally.



Now, calculate the hash for this file.



Submit this hash to Virustotal, and navigate to the details tab.



Answer: 2007–06–27

12. What is the key used to encode the shellcode?

Answer: 0x99

13. What is the port number the shellcode binds to?

Answer: 1957

14. The shellcode used a specific technique to determine its location in memory. What is the OS file being queried during this process?

Answer: kernel32.dll

This is the end of this walkthrough.