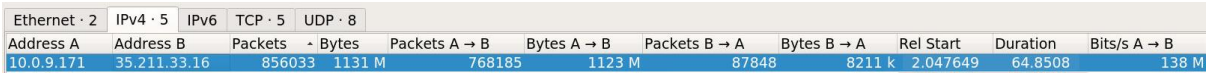
Blue Team Labs Online: Piggy

The following writeup is for Piggy on Blue Team Labs Online, it's an easy lab that involves analysing a series of pcap file. This investigation covers a lot of fundamental pcap analysis techniques, and also covers basic OSINT techniques. Anyone new to Wireshark that is trying to test their newly found knowledge of the tool should give this investigation a go.

Scenario: Investigate some simple network activity in Wireshark! You can launch Wireshark in a terminal with the command 'wireshark'. The questions are mapped to the four PCAPs on the Desktop.

PCAP One) What remote IP address was used to transfer data over SSH? (Format: X.X.X.X)

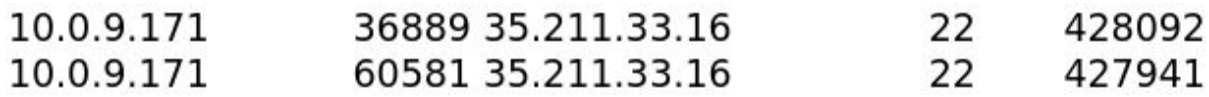
Typically when investigating a pcap file, I like to check out the conversations tab by navigating to Statistics > Conversations:



Ethernet · 2 | IPv4 · 5 | IPv6 | TCP · 5 | UDP · 8

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
10.0.9.171	35.211.33.16	856033	1131 M	768185	1123 M	87848	8211 k	2.047649	64.8508	138 M

If you also check the TCP tab, we can see that the destination port for these packets were port 22, which is the default SSH port:



10.0.9.171	36889 35.211.33.16	22	428092
10.0.9.171	60581 35.211.33.16	22	427941

Therefore, it is safe to assume that the remote IP address that was used to transfer data over SSH is 35.211.33.16.

PCAP One) How much data was transferred in total? (Format: XXXX M)

In the IPv4 tab for the Conversations statistics, we can see a Bytes column:

Bytes
1131 M

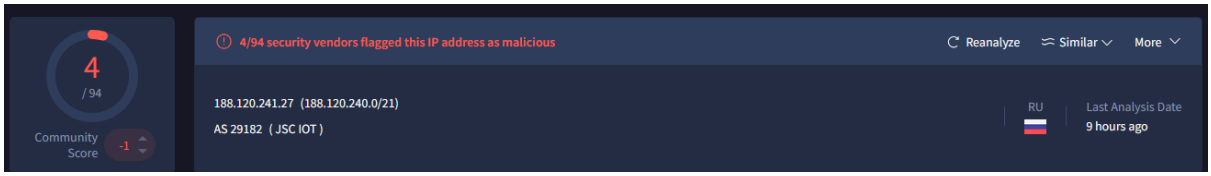
This indicates how much data was transferred in total, which in this case is 1131 M.

PCAP Two) Review the IPs the infected system has communicated with. Perform OSINT searches to identify the malware family tied to this infrastructure (Format: MalwareName)

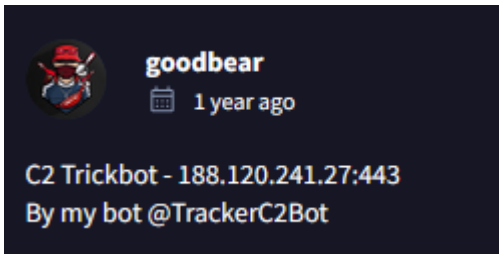
Following the same sort of methodology as the previous questions, let's take a look at the Conversations tab:

Address A	Address B	Packets
10.0.0.2	10.0.9.171	12
10.0.9.171	82.2.64.107	3754
10.0.9.171	34.110.209.165	46
10.0.9.171	188.120.241.27	1
10.0.9.171	195.161.41.93	6
10.0.9.171	92.53.67.7	1
10.0.9.171	31.184.253.37	6
10.0.9.171	78.155.206.172	1

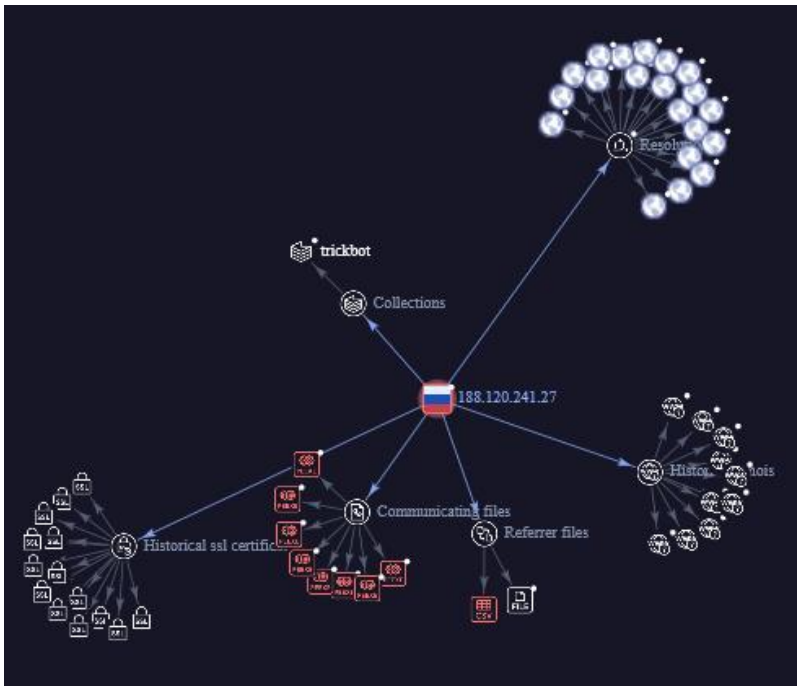
82.2.64.107 immediately pops out due to the number of packets, but after performing some basic OSINT, I found nothing indicating that it is associated with threat actor infrastructure. However, 188.120.241.27 does have a couple of results on VirusTotal:



The Community tab also provides a good indication that this IP address is associated with malicious infrastructure:



If you take a look at the threat graph, we can also see that this IP is associated with Trickbot:



PCAP Three) Review the two IPs that are communicating on an unusual port. What are the two ASN numbers these IPs belong to? (Format: ASN, ASN)

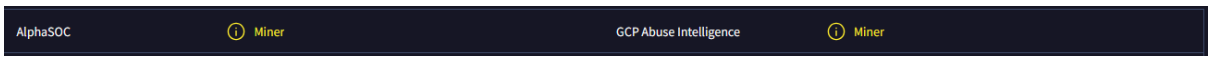
Address A	Port A	Address B	Port B
10.0.9.171	34825	194.233.171.171	8080
10.0.9.171	58651	104.236.57.24	8000
10.0.9.171	58032	34.110.209.165	443
10.0.9.171	58048	34.110.209.165	443
82.2.64.107	56171	10.0.9.171	443

I wouldn't consider port 8080 to be a very unusual port, however, based on the other ports that we can see (HTTPs), port 8080 is obviously the unusual port. We can use an ASN lookup tool to find the answer:

14061,63949.

PCAP Three) Perform OSINT checks. What malware category have these IPs been attributed to historically? (Format: MalwareType)

Both IP addresses have been flagged as potentially associated with Miners:

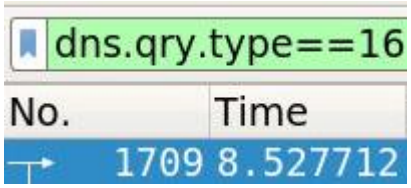


PCAP Three) What ATT&CK technique is most closely related to this activity? (Format: TXXXX)

After a quick google search, you can determine that mining is associated with the MITRE ATT&CK technique "Resource Hijacking" (T1496).

PCAP Four) Go to View > Time Display Format > Seconds Since Beginning of Capture. How long into the capture was the first TXT record query made? (Use the default time, which is seconds since the packet capture started) (Format: X.xxxxxx)

We can use a simple display filter to search for all TXT record queries made:



The answer is therefore, 8.527712.

PCAP Four) Go to View > Time Display Format > UTC Date and Time of Day. What is the date and timestamp? (Format: YYYY-MM-DD HH:MM:SS)

2024-05-24 10:08:50

PCAP Four) What is the ATT&CK subtechnique relating to this activity? (Format: TXXXX.xxx)

If you look at all of the DNS TXT record queries, we can clearly see that some sort of data exfiltration over DNS is occurring:

The subdomain is likely some sort of encoded data, but seeing as the question is only asking for the ATT&CK subtechnique, we don't need to decode it or make sense of it. After some basic research, you will come across T1071.004, aka Application Layer Protocol: DNS: