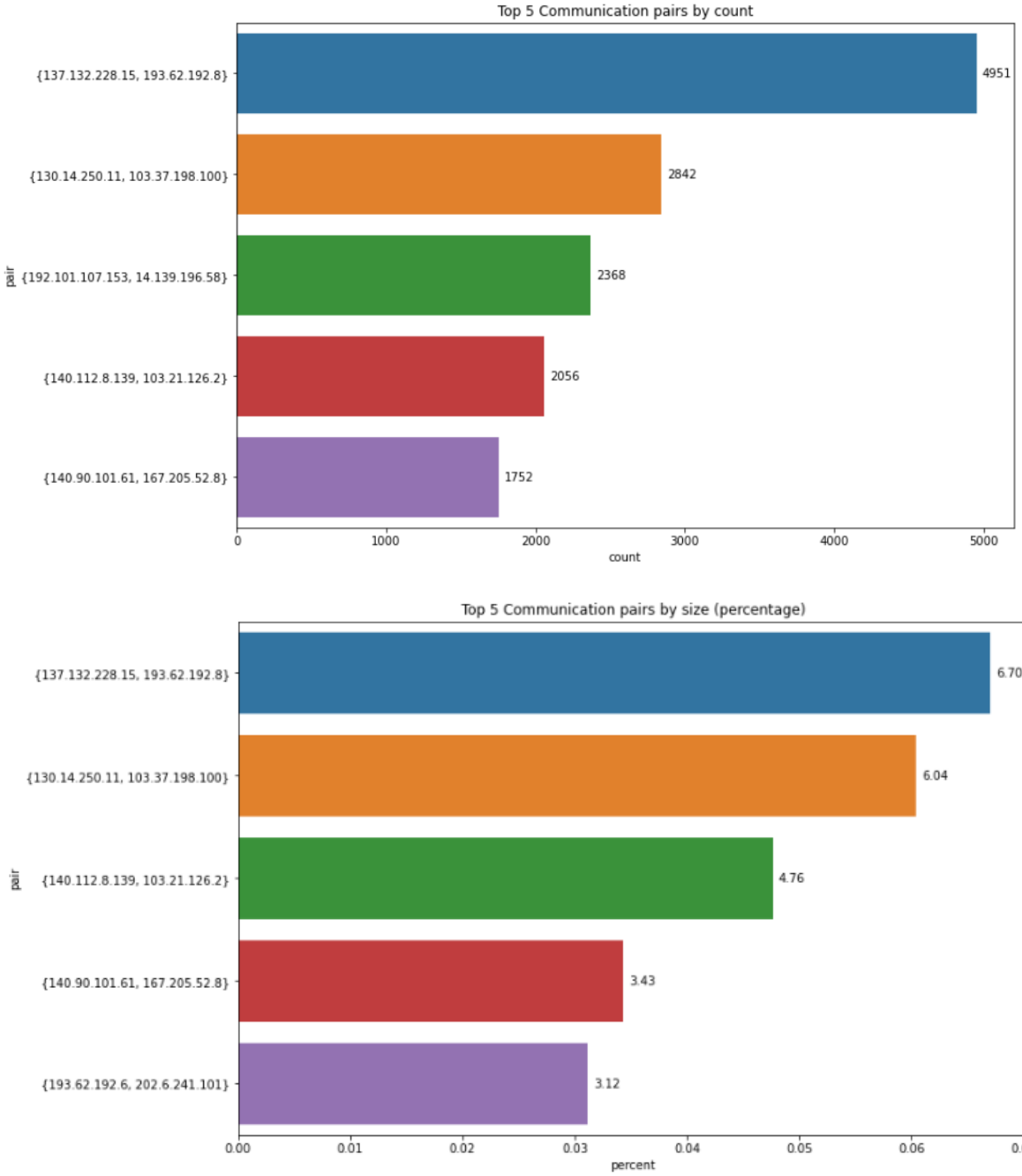
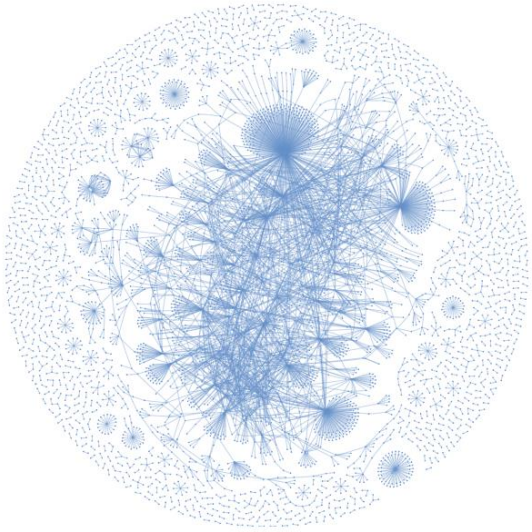
Top 5 communicating pairs:

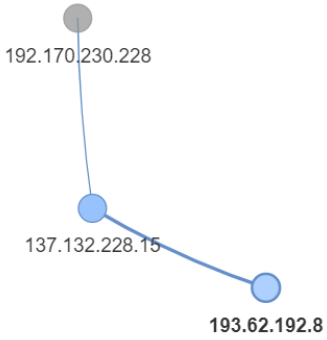


These graphs show the activity of the top 5 communicating pairs. The top graph lists the activity of the top 5 conversing pairs by count, while the bottom graph shows the top five conversing pairs by percentage of traffic. This information can be useful to check whether a certain pair is “hogging” up the network, or if there is any abnormal activity between communication pairs. (For example, in a data breach, it is likely that one host will communicate a lot with another, leading to a large spike in packets sent and proportion of traffic used. Real-time detection of such anomalies can be used prevent more data from being stolen during data breaches.)

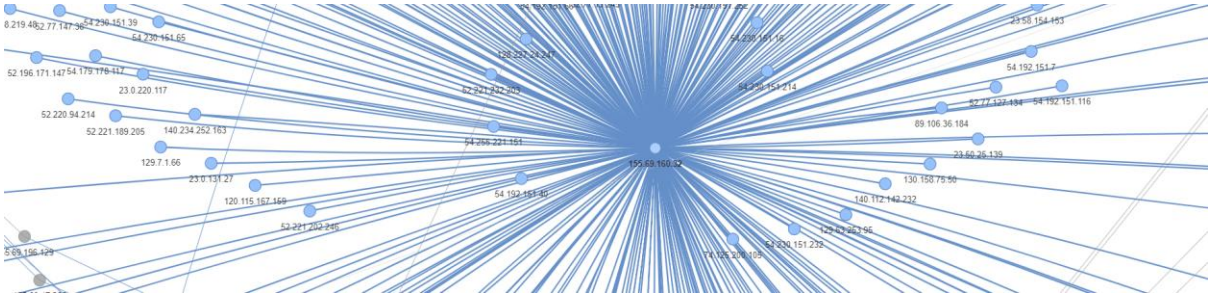
Network Visualisation



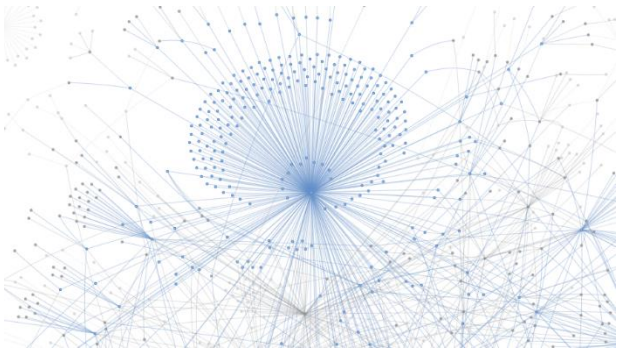
Here is a visualization of the whole network in the dataset. Each node represents an IP address, and each edge represents a connection between 2 networks. This just gives an overview of the whole network: how many nodes and connections there are, and how the nodes are generally connected.



We can use the visualisation to look up the behaviour of specific IP addresses. For example, we can look at the behaviour of the top talker: 193.62.192.8. We can see that the only connection that 193.62.182.8 has is with 137.132.228.15, which it makes up the top communication pair with, at 4951 packets sent between them and 6.7% of total network traffic in size.



Another example the NTU network, 155.69.130.32, in the centre. As expected, we can see that it acts as a hub.



A more zoomed out view of the nodes that are linked to the NTU network. Directly linked nodes are highlighted in blue. We can see that the NTU node is connected to a large number of unique end-users, and even other smaller hubs.