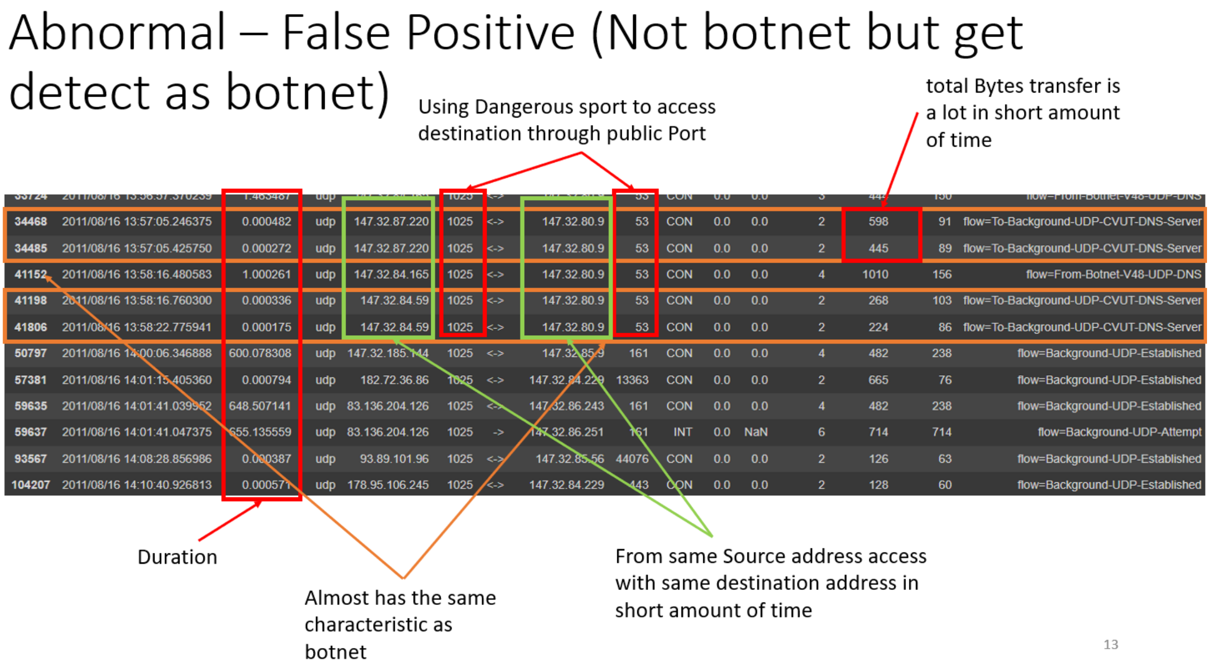
Weekly report Week 6 (26/6/2023 - 30/6/2023)

This week I have continue analyzing the dataset and found out the false positive and false negative characteristics that it will look similar to the botnet characteristics that I have showed last week



Abnormal – False Positive (Not botnet but get detect as botnet)

Using Dangerous sport to access destination through public Port

total Bytes transfer is a lot in short amount of time

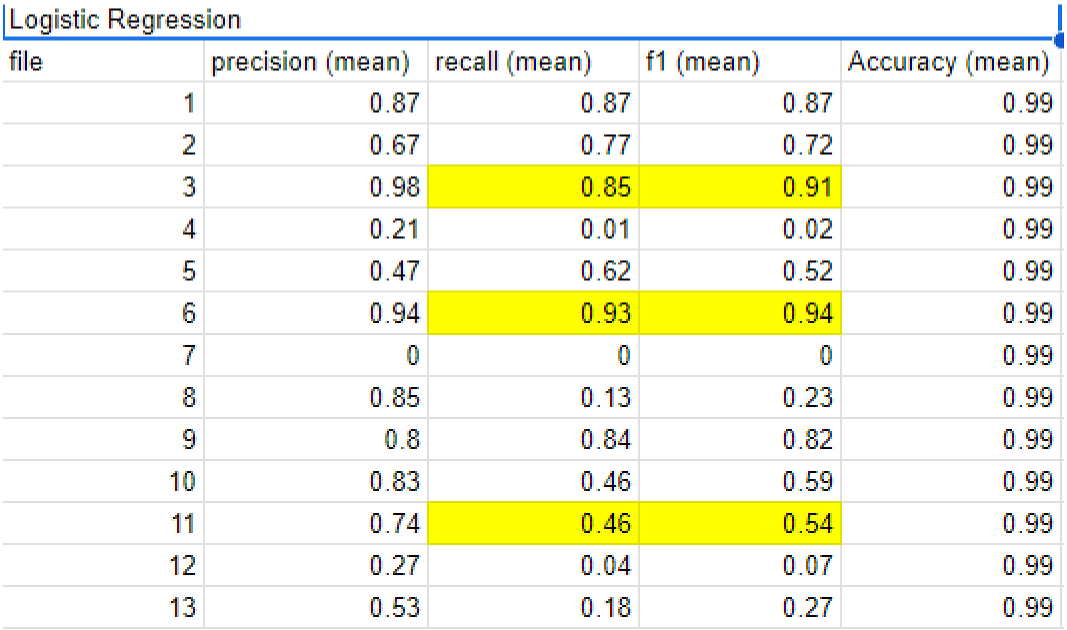
33724	[illegible]	1.463487	udp	[illegible]	1025	<->	[illegible]	53	CON	0.0	0.0	3	[illegible]	150	flow=From-Botnet-V48-UDP-DNS
34468	2011/08/16 13:57:05.246375	0.000482	udp	147.32.87.220	1025	<->	147.32.80.9	53	CON	0.0	0.0	2	598	91	flow=To-Background-UDP-CVUT-DNS-Server
34485	2011/08/16 13:57:05.425750	0.000272	udp	147.32.87.220	1025	<->	147.32.80.9	53	CON	0.0	0.0	2	445	89	flow=To-Background-UDP-CVUT-DNS-Server
41152	2011/08/16 13:58:16.480583	1.000261	udp	147.32.84.165	1025	<->	147.32.80.9	53	CON	0.0	0.0	4	1010	156	flow=From-Botnet-V48-UDP-DNS
41198	2011/08/16 13:58:16.760300	0.000336	udp	147.32.84.59	1025	<->	147.32.80.9	53	CON	0.0	0.0	2	268	103	flow=To-Background-UDP-CVUT-DNS-Server
41806	2011/08/16 13:58:22.775941	0.000175	udp	147.32.84.59	1025	<->	147.32.80.9	53	CON	0.0	0.0	2	224	86	flow=To-Background-UDP-CVUT-DNS-Server
50797	2011/08/16 14:00:06.346888	600.078308	udp	147.32.185.144	1025	<->	147.32.85.9	161	CON	0.0	0.0	4	482	238	flow=Background-UDP-Established
57381	2011/08/16 14:01:15.405360	0.000794	udp	182.72.36.86	1025	<->	147.32.84.229	13363	CON	0.0	0.0	2	665	76	flow=Background-UDP-Established
59635	2011/08/16 14:01:41.039952	648.507141	udp	83.136.204.126	1025	<->	147.32.86.243	161	CON	0.0	0.0	4	482	238	flow=Background-UDP-Established
59637	2011/08/16 14:01:41.047375	655.135559	udp	83.136.204.126	1025	->	147.32.86.251	161	INT	0.0	NaN	6	714	714	flow=Background-UDP-Attempt
93567	2011/08/16 14:08:28.856986	0.000387	udp	93.89.101.96	1025	<->	147.32.85.56	44076	CON	0.0	0.0	2	126	63	flow=Background-UDP-Established
104207	2011/08/16 14:10:40.926813	0.000571	udp	178.95.106.245	1025	<->	147.32.84.229	443	CON	0.0	0.0	2	128	60	flow=Background-UDP-Established

Duration

Almost has the same characteristic as botnet

From same Source address access with same destination address in short amount of time

And also I have recheck and retrain and test the model again this week with different condition because last week the model seem weird and also the code something is wrong with it so I have recheck it and run the model again the only model that is finished now is the logistic regression that got the result as below



Logistic Regression

file	precision (mean)	recall (mean)	f1 (mean)	Accuracy (mean)
1	0.87	0.87	0.87	0.99
2	0.67	0.77	0.72	0.99
3	0.98	0.85	0.91	0.99
4	0.21	0.01	0.02	0.99
5	0.47	0.62	0.52	0.99
6	0.94	0.93	0.94	0.99
7	0	0	0	0.99
8	0.85	0.13	0.23	0.99
9	0.8	0.84	0.82	0.99
10	0.83	0.46	0.59	0.99
11	0.74	0.46	0.54	0.99
12	0.27	0.04	0.07	0.99
13	0.53	0.18	0.27	0.99

this week I will focus on writing the research proposal only while waiting for other model to run