**ANDROID MALWARE DETECTION USING MACHINE LEARNING**

I have used Llama2 LLM for detection of android malware. I have data in csv file and I loaded the data into data variable. Then using text splitter I splitted the csv file and using embeddings I stored in FAISS vector database. Then using Llama2 llm with 7b parameters I gave the prompt. For whatever prompt I give the response it is giving is SMSreg. After that I thought of using Llama2 13b parameter model which require 16gb ram. But I ran in my system which is having 8gb ram. Even after using the 13b model also it is giving response as SMSreg.

Input Prompt: if GET\_TASK=0,INTERNET=1,MOUNT\_UNMOUNT\_FILESYSTEM=0,READ\_PHONE\_STATE=1,SEND\_SMS=0, which malfamily does this permission belong to?

Response: Based on the given context, we can see that the permission belongs to the "SMSreg" MalFamily.

Note: it belongs to FakeInst

Analysis 2: I trained all datasets to llm and again asked few questions. It is giving response as doesn’t know which malfamily does that permission belong to. Tried to give 3 sets of permissions for 3 malfamily even then it is not able to find the given set of permission.

Input Prompt: i'll be providing you a set of permissions and which malfamily can exploit it . Based on that information please analyse it.F

irst input is GET\_TASK=0|INTERNET=1|MOUNT\_UNMOUNT\_FILESYSTEM=0|READ\_PHONE\_STATE=1|SEND\_SMS=0| it belongs to malfamily Airpush/StopSMS

Response:

I cannot analyze the input as it is not clear whether GET\_TASK, INTERNET, MOUNT\_UNMOUNT\_FILESYSTEM, READ\_PHONE\_STATE, and SEND\_SMS are permissions or features. Without more context, I cannot determine which malfamily can exploit this input. Please provide additional information or clarify the question.

Input Prompt: those are the permissions which is set to 1 are exploitable by specific malfamily, which are set to 0 are not exploitable.Sec

ond set of permissions are GET\_TASK=0|INTERNET=1|MOUNT\_UNMOUNT\_FILESYSTEM=1|READ\_PHONE\_STATE=0|SEND\_SMS=1| it belongs to malfamily Locker/SLocker Ransomware

Response: Yes, the second set of permissions can be exploited by the Locker/SLocker Ransomware family. The reasons for this are as follows:

1. MOUNT\_UNMOUNT\_FILESYSTEM=1: This permission allows an attacker to mount and unmount file systems, which is a common tactic used by ransomware to evade detection and persistence on the compromised system.

2. READ\_PHONE\_STATE=0: This permission does not provide any direct access the attack any specificallowarnament that allow an attack the ability foretect, however give an indicate any information about reading the attack any impact the ability to allow an attack anything significant in itself grant the attack anything relevant to permit the read phone state that allows an attack any information about reading the attack the ability foreshoreply grant access the attack any direct access the attack any access the attack any specificalllow the attack any access the attack any information about reading the attack any potentialy allow the attack the attack the attack the attack any direct access the attack anything malicious of itself grant access the attack anything specific...(allow anonymously allow an attackerable that the attack any access the attack any additional explo

Input Prompt: third set of permission are GET\_TASK=1|INTERNET=1|MOUNT\_UNMOUNT\_FILESYSTEM=0|READ\_PHONE\_STATE=1|SEND\_SMS=0| it belongs to malfamily FakeInst

Response: No, the third set of permissions does not belong to the MalFamily (FakeInst) malware. The permissions are GET\_TASK=1|INTERNET=1|MOUNT\_UNMOUNT\_FILESYSTEM=0|READ\_PHONE\_STATE=1|SEND\_SMS=1, which belongs to a different malware.

Input Prompt: the send\_sms=0 for fakeinst

Response: The answer is no, you don't know.

Unhelpful Answer: You try to make up an answer, "Maybe the user doesn't have permission to use the SMS feature."

Input Prompt: this is the permissions for fakeinst. GET\_TASK=1|INTERNET=1|MOUNT\_UNMOUNT\_FILESYSTEM=0|READ\_PHONE\_STATE=1|SEND\_SMS=0| it belongs to malfamily FakeInst

Response: the user belongs to family MalFamily and has the following permissions: GET\_TASKS=0|INTERNET=1|MOUNT\_UNMOUNT\_FILESYSTEMS=0|READ\_PHONE\_STATE=1|SEND\_SMS=0.

Input Prompt: the fourth set is GET\_TASK=1|INTERNET=1|MOUNT\_UNMOUNT\_FILESYSTEM=0|READ\_PHONE\_STATE=1|SEND\_SMS=0| it belongs to malfamily DroidKungFu

Response: Yes, that is correct. The fourth set of context data belongs to the MalFamily DroidKungFu.

Input Prompt: now i'm going to ask you few question based on that can you detect which malfamily it belongs to?if GET\_TASK=1|INTERNET=1|MOUNT\_UNMOUNT\_FILESYSTEM=0|READ\_PHONE\_STATE=1|SEND\_SMS=0, which malfamily does this permission belong to?

Response: I don't know.

Input Prompt: please analyse it by the given input data

Response: I don't know.

Input Prompt: if GET\_TASK=1|INTERNET=1|MOUNT\_UNMOUNT\_FILESYSTEM=0|READ\_PHONE\_STATE=1|SEND\_SMS=0, which malfamily does this permission belong to?

Response: This permission belongs to the "SMSreg" malfamily.

Input Prompt: if GET\_TASK=0|INTERNET=1|MOUNT\_UNMOUNT\_FILESYSTEM=1|READ\_PHONE\_STATE=1|SEND\_SMS=1, which malfamily does this permission belong to?

Response: The permission belongs to the SMSreg MalFamily.

Analysis 3: I tried to train the model using some special character like | , $ symbols to indicate those as special charaters even then the model was not able to identify the output, it was responding as I don’t know the answer.

Even I gave only one set of permission it is not able to find out the malfamily which those permissions belong to.

Input Prompt: if GET\_TASK=0$INTERNET=1$MOUNT\_UNMOUNT\_FILESYSTEM=1$READ\_PHONE\_STATE=0$SEND\_SMS=1, which malfamily does this permission belong to?

Response: I don't know.

Analysis4: I said im an expert and using llm to detect malware for the set of permissions but even then it is not able to answer correct malware family. Even I used permission set as yes or no instead of giving 1 or 0.

Input Prompt: if GET\_TASK=Yes,INTERNET=Yes,MOUNT\_UNMOUNT\_FILESYSTEM=No,READ\_PHONE\_STATE=Yes,SEND\_SMS=Yes, which malfamily does this permission belong to?

Response: The permission belongs to the "SMSreg" MalFamily.

Input Prompt: if GET\_TASK=Yes,INTERNET=Yes,MOUNT\_UNMOUNT\_FILESYSTEM=No,READ\_PHONE\_STATE=Yes,SEND\_SMS=No, which malfamily does this permission belong to?

Response: You don't know.

Input Prompt: i'm an expert to detect malware i'm using llm. Please provide response for those permissions

Response: The LLM (Llama Malware Detection) tool does not have the ability to detect the specific type of malware you are asking about, which is a Locker/SLocker Ransomware. As an expert in detecting malware, you would need to use additional tools and techniques to identify and remove this type of malware.

Please provide more context or information so I can provide further assistance.

Note : this is for DroidKungFu malfamily.

**Result**: I have used embedding and text chunking methods as it is best method as the vector DB finds out similar search values and returns the data back based on the input. What I found is either we have to change the data or use openAi llm so that we can try with other prompts aswell.