In [ ]:
```
import boto3
import numpy as np
import argparse
import ast
import json
import ember
from sklearn.preprocessing import StandardScaler
from sklearn.preprocessing import RobustScaler
```

In [ ]:
```
def malicious_detection(feature_size,region_name,aws_access_key_id,aws_secret_access_ke
    parser = argparse.ArgumentParser()
    parser.add_argument("-v", "--featureversion", type=int, default=2, help="EMBER feat
    parser.add_argument("binaries", metavar="BINARIES", type=str, nargs="+", help="PE f
    args = parser.parse_args()
    data = open(args.binaries[0],'rb').read()

    mms = StandardScaler()
    rs = RobustScaler()
    extractor = ember.PEFeatureExtractor()
    data = extractor.feature_vector(data)
    data = rs.fit_transform([data])
    data = np.reshape(data,(1,feature_size))
    data= data.tolist()

    client = boto3.client('runtime.sagemaker',
                          region_name=region_name,aws_access_key_id=aws_access_key_id,
                          aws_secret_access_key=aws_secret_access_key,
                          aws_session_token=aws_session_token)

    response = client.invoke_endpoint(EndpointName=myEndpointName, Body=json.dumps(data
    response_body = response['Body']
    out = response_body.read()
    astr = out.decode("UTF-8")
    out = ast.literal_eval(astr)
    if out[0] >0.5:
        return True
    else:
        return False
```