## **Step 1 : Source Code**

#include <string>

#include <iostream>

#include <fstream>

std::string mal\_line = "I want to learn PE file format!"; // this is the malicious line which can be replaced with malicious code

bool fexists(const char \*filename) {

/\*\*

fuction to check if file exists

\*\*/

std::ifstream ifile(filename);

return (bool)ifile;

}

void filecreater(const char \*filename){

/\*\*

function to create file if it does not exist

\*\*/

std::ofstream fout; //object created \*\*fout\*\*

fout.open(filename);

fout<< mal\_line <<"\n";

fout.close();

}

bool checkline(const char \*filename){

/\*\*

fuction to check if malacious line already present in file

\*\*/

std::string line;;

std::ifstream myfile (filename);

if (myfile.is\_open())

{

while ( getline (myfile,line) )

{

if (line == mal\_line){

myfile.close();

return true;

}

}

myfile.close();

}

return false;

}

void fileupdater(const char \*filename){

/\*\*

function to call checkline and add malicious line if needed or print whats there in file

\*\*/

bool file\_flag = false;

file\_flag = checkline(filename);

if (file\_flag == true){

std::string line;

std::ifstream myfile (filename);

if (myfile.is\_open())

{

while ( getline (myfile,line) )

{

std::cout << line << '\n';

}

myfile.close();

}

}else{

std::ofstream fout; //object created \*\*fout\*\*

fout.open(filename,std::ofstream::app);

fout<< mal\_line <<"\n"; //adding malicious line

fout.close();

}

}

int main() {

char filename[30]= "D:/PE-1.txt"; // filename with the directory

bool flag = false;

flag = fexists(filename);

if (flag == true){

fileupdater(filename);

}

else{

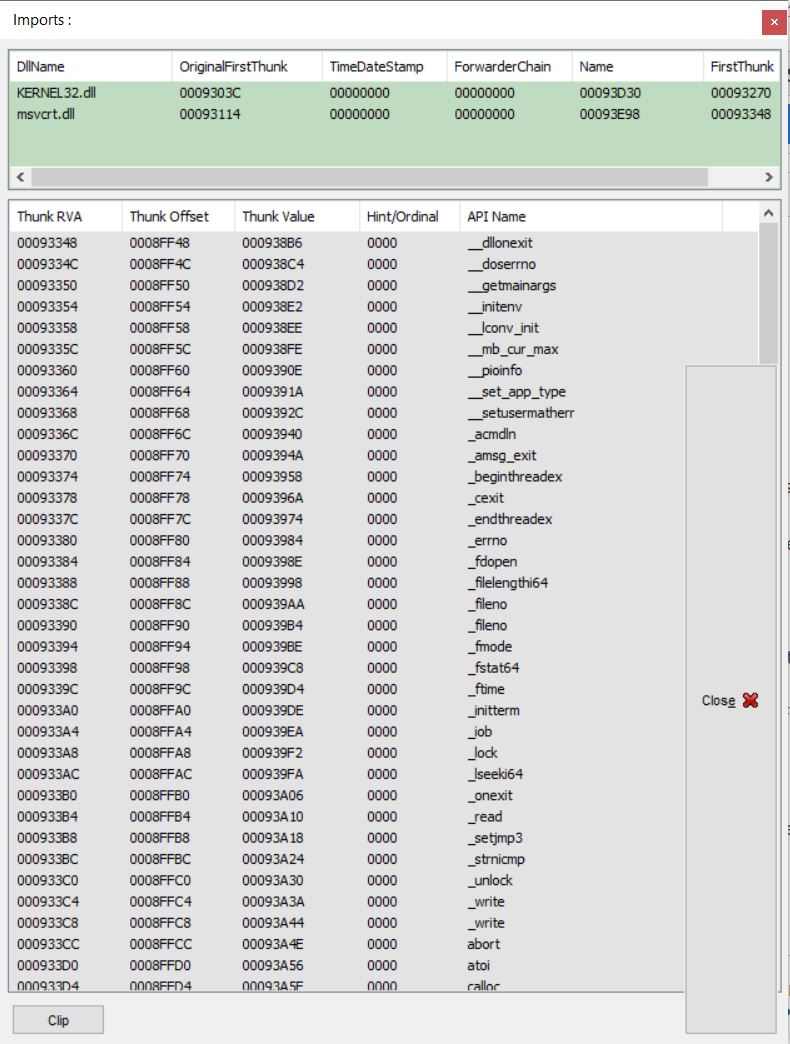
filecreater(filename);

}

return 0;

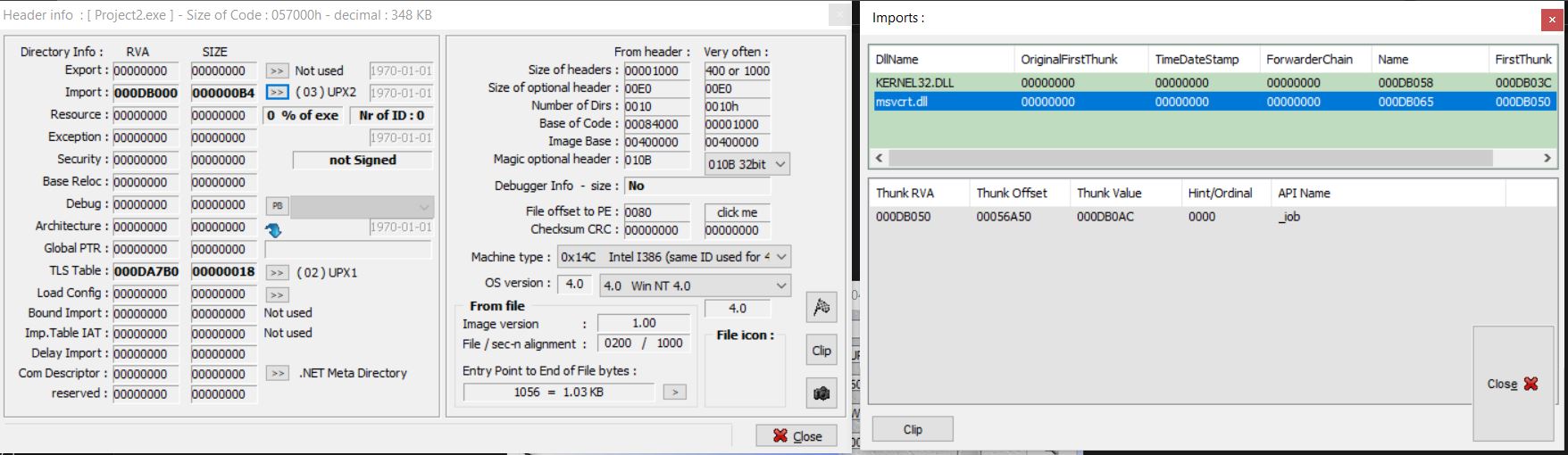
}

## **Step 2 : Import table**

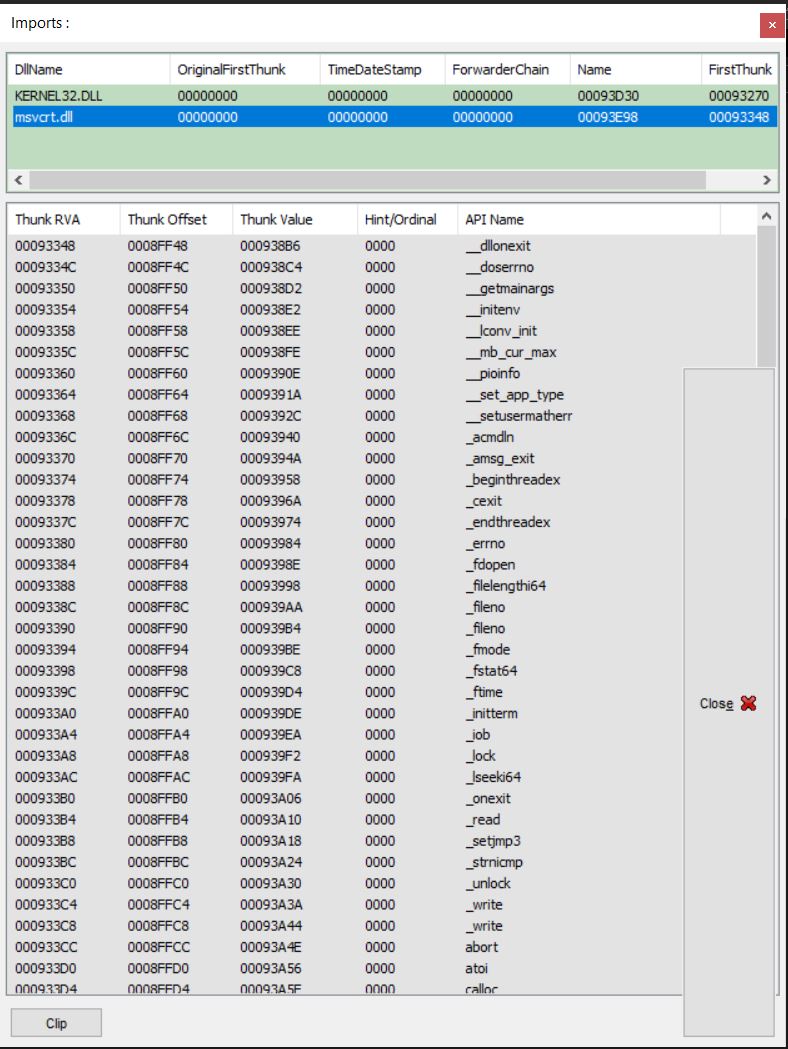


Above is the screenshot of the import table for the malware.

## **Step 3 : Compressed and Uncompressed Import table**

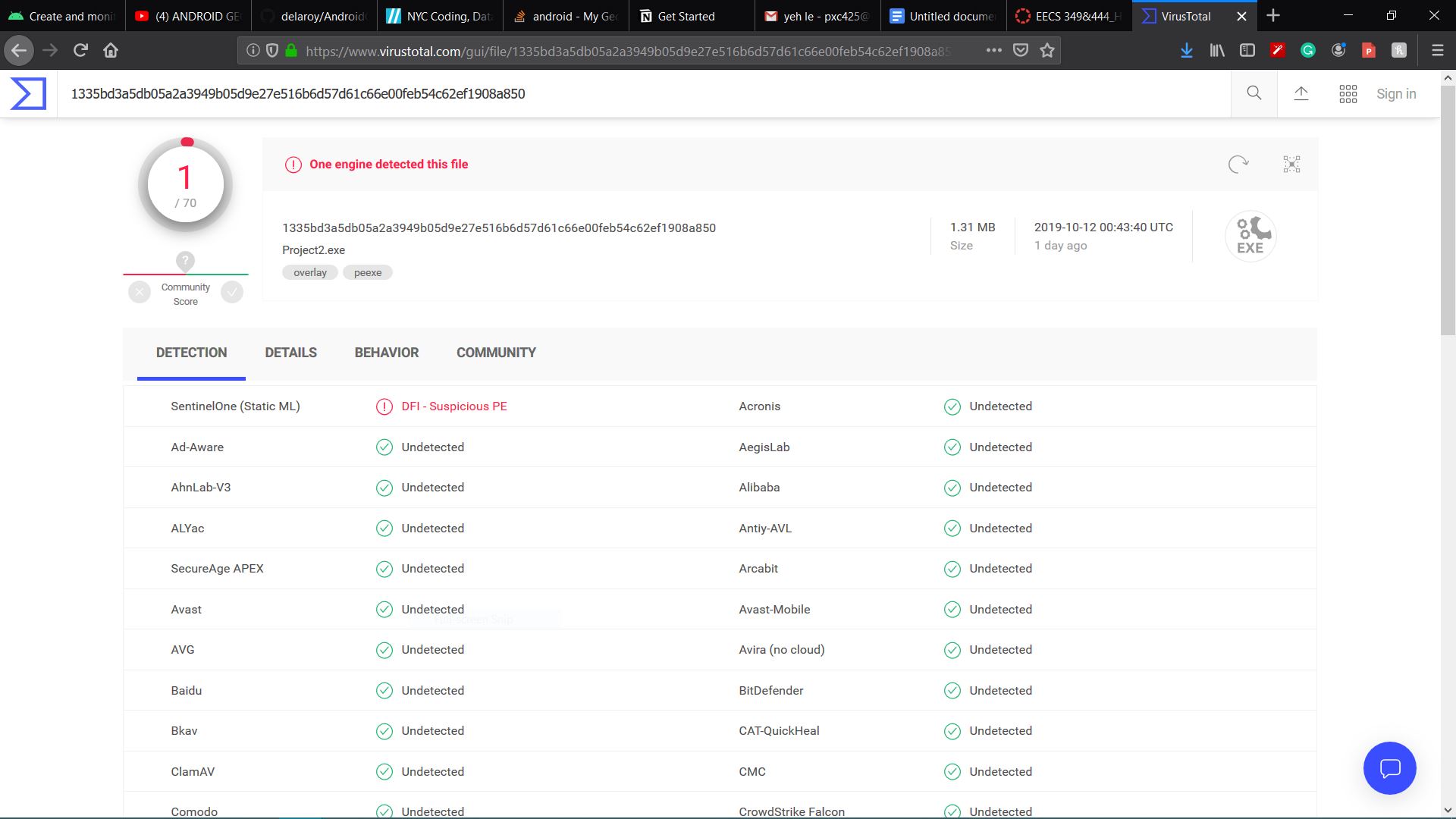


Above is Import table after packing the exe malware

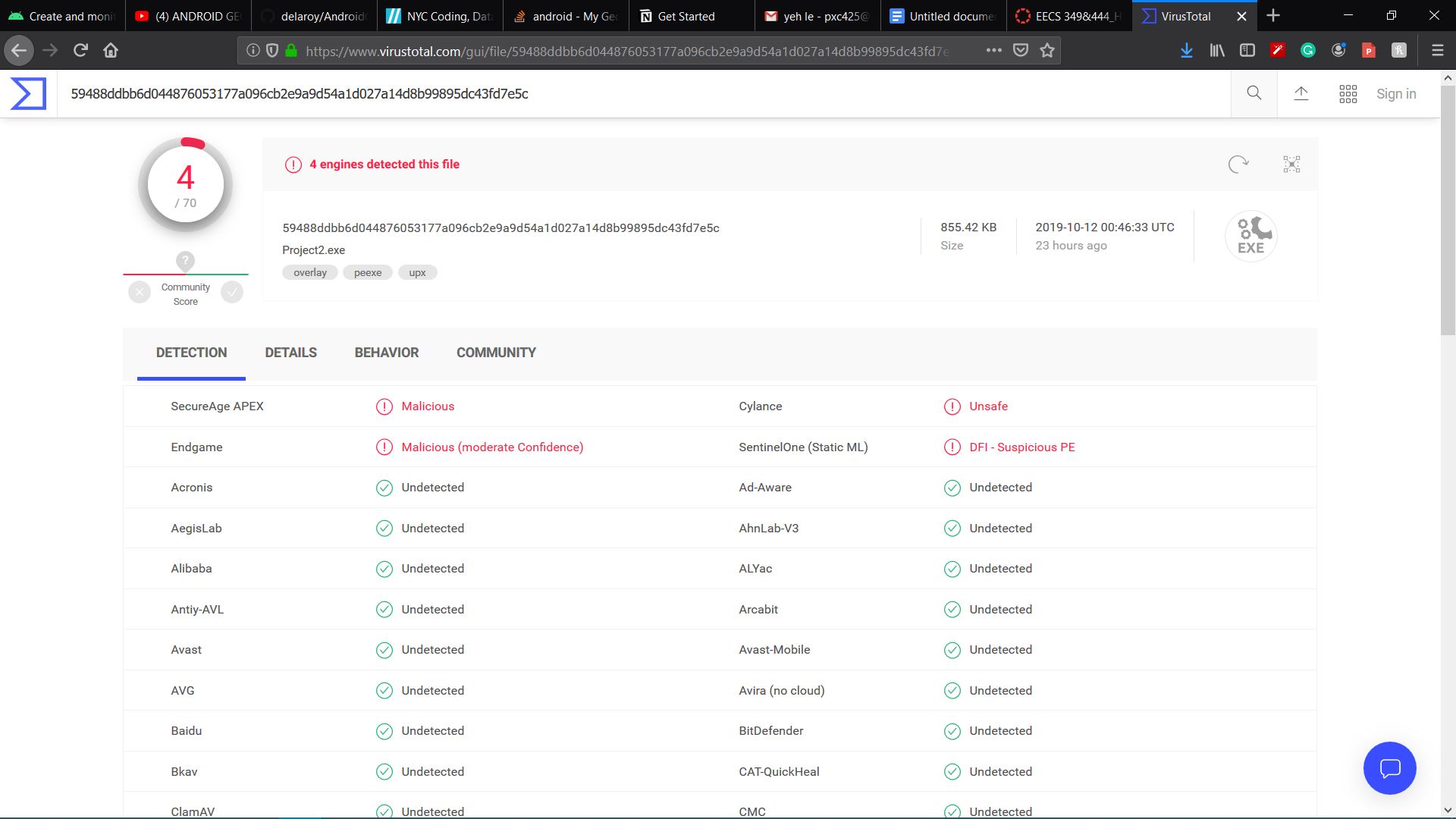


Above is the decompressed Import table

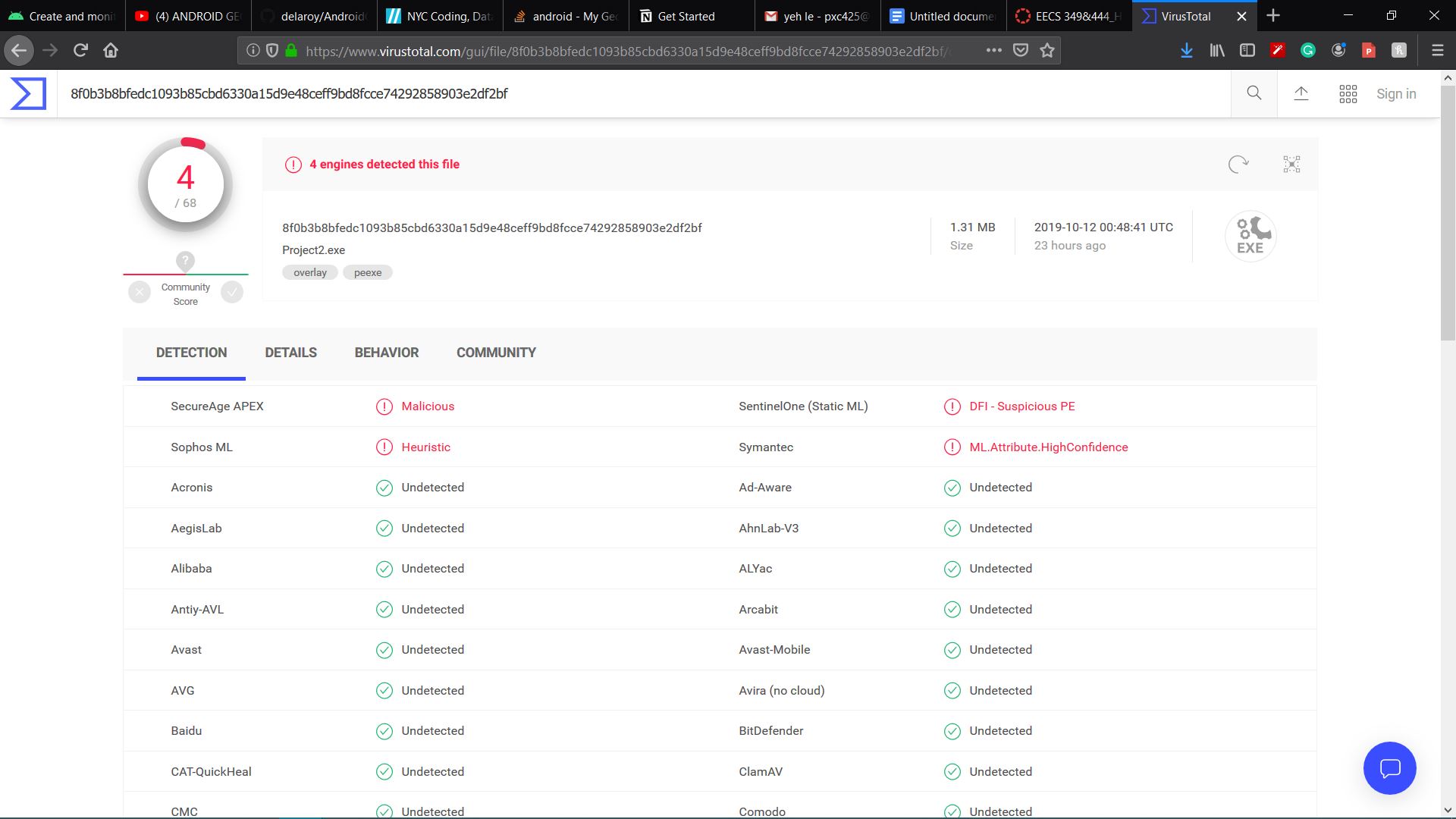
## **Step 3 : Virus scans**



Normal virus scan has only 1 detection



Compressed exe virus scan has 4 detections



Decompressed again also has 4 virus scans detections