uOttawa

ELG7186[EG] Ai For Cyber Security
" Malware classification using Malimg dataset"

Theme Selection

GROUP: 1

	Student Name	Student ID	Student E-Mail
1	Abdelrhman Gaber Youssef Saad Rezkallah	300327290	arezk095@uOttawa.ca
2	Abdulrahman Muhammad AbdulSalam Ahmed	300327218	aahme275@uOttawa.ca
3	Ali Amin El-Sayed Mahmoud El-Sherif	300327246	aelsh054@uottawa.ca
4	Basma Reda Shaban Abd-Elsalam Abd-Elwahab	300327209	babde014@uottawa.ca

Main problem:

Malware is any malicious code or a program that can be harmful to the computer. There are many types of malwares, and it's essential to detect these types to prevent their breaches to keep the data and the system private and secured.

Dataset:

The Malimg dataset consists of 9339 images and 25 classes. The following table represents the class and type of the included malwares:

	Family/Class	Type
0	Adialer.C	Dialer
1	Agent.FYI	Backdoor
2	Allaple.A	worm
3	Allaple.L	Worm
4	Alueron.gen!J	worm
5	Autorun.K	Worm.AutoIT
6	C2LOP.P	Trojan
7	C2LOP.gen!g	Trojan
8	Dialplatform.B	Dialer
9	Dontovo.A	Trojan Downloader
10	Fakerean	Rogue
11	Instantaccess	Dialer
12	Lolyda.AA1	PWS
13	Lolyda.AA2	PWS
14	Lolyda.AA3	PWS
15	Lolyda.AT	PWS
16	Malex.gen!J	Trojan
17	Obfuscator.AD	Trojan Downloader
18	Rbot!gen	Backdoor
19	Skinterm.N	Trojan
20	Swizzor.gen!E	Trojan Downloader
21	Swizzor.gen!I	Trojan Downloader
22	VB.AT	worm
23	Wintrim.BX	Trojan Downloader
24	Yuner.A	worm

Solution:

The main idea is to predict which Family/Class the malware belongs to by extracting the important features from the images using a Convolutional Neural Network (CNN), so this problem can be considered as a multiclassification problem.

References:

malimg_dataset.zip. (n.d.). Dropbox.
https://www.dropbox.com/s/ep8qjakfwh1rzk4/malimg_dataset.zip?dl=0