iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XI **Month of publication:** November 2022

DOI: https://doi.org/10.22214/ijraset.2022.47268

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XI Nov 2022- Available at www.ijraset.com

A Study on Analysis of Malware in Android Applications

Veeraj R Singh[1], Sharmila S P[2], Narendra S Chaudhari[3]
[1]*Department of Computer Science, PDA College of Engineering, Kalaburagi, India*
[2, 3]*Department of Computer Science, IIT, Indore, India*

Abstract: ***Malware is still a big problem around the world, but the nature of malware is changing. Malware is described as any malicious program designed to cause havoc or mischief in a computer system. the malware landscape changes every year, although long-term trends can be identified in year-on-year data reports. Despite numerous anti-malware measures, cybercriminals and hackers do not give up quickly, especially not when there is money to be made in malware. This study emphasizes the need to study malware and its effect on android applications. The primary objective is to infect an android application with malware and study the structural modifications that occur in the apk. This can be achievable by using Metasploit which is a frame work in Kali Linux. The structural changes are analyzed by an application called Virus Total. This study will help in preventing malware attacks and also bring awareness among users on malware.***
Index Terms: Malware, VirusTotal, Cuckoo sandbox, Android Apk, Software security, Kali linux, Metasploit.

I. INTRODUCTION

The security of systems, servers, portable devices, communication devices, network, & data against hostile assaults is known as cybersecurity. Also referred to as electronic information security or information security technology. The phrase may be used in a wide range of situations, including business to computers, which could be broken down in number of distinct categories. A computer network's security refers to actions used to keep out malicious or unwanted intruders.

Software & devices are protected against attacks via application security. Access to data that is meant to be private might nonetheless happen via the use of third-party applications. Prior to the deployment of any system or device, security should be included into the design from the outset. If you want your data to be secure while it is being stored and transported, you need information security measures. Steps and actions that are taken to secure information assets fall under operational security. The user's access credentials to network as well as process of selecting how, when, or where data must be stored all come under this umbrella phase. Disaster Recovery & Business Resilience refers to the procedures in place to ensure that your company's operations and data are not disrupted in event of a cyberattack or another calamity. In the case of a disaster, an organization's disaster recovery plans outline how it would restore activities and information to its pre-event capabilities. Returning when an organization is operating without certain resources constitutes business continuity

II. LITERATURE RVIEW

1) The term "malware" refers to malicious software. Computer systems may be harmed without the user being aware of it, and technological advances are creating major problems for academics in university and business alike. Malware analysis research has changed and progressed in terms of number, substance, and publication, motivated us to conduct. It’s impossible to grasp all of the intricacies of malware programs since they are so massive. Internet users need to be educated about malware assaults and the correct usage of anti-malware programs to safeguard their online identities against malware attacks.

2) Malware is a major threat to Internet users nowadays. Every day, a large number of malwares are tested by hostile to Virus companies. It is designed to damage PC frameworks without the user's knowledge, and approach advancements are posing huge problems for scientists in both the academic and corporate worlds. For further examination, malware tests have been organized and amassed. In this literature evaluation, we conducted a manual search of all papers published between 2014 and 2020. We used quality assessment criteria to choose roughly 27 publications out of 55 as main studies, and then derived research questions from those questions. The purpose of this SLR is to survey the state of malware analysis literature and report on the breadth, depth, and variety of related research, as well as the most prominent and relevant publications in the field.

3) Since Android operating system is free to use, Android devices are more popular than other smartphones. It is possible to install third-party programs on Android because of its open operating system. However, Android's security is a major problem. Since only developers may provide access to third-party software, the danger of rogue programs is on the rise. All or nothing is the principle on which applications are deployed. Because of this, attackers are able to infiltrate a regular program using rights that they obtained illegally. Various varieties of malware, as well as general methodologies and strategies for malware detection, are all presented in this study, which also includes literature analysis for android smartphone security issues.

III. OBJECTIVES

1) To analyze the architecture and structural details of the android application.
2) To study the modifications that the application undergoes by an adversary to steal the information of the user.
3) To demonstrate the analysis of malware by a working model.

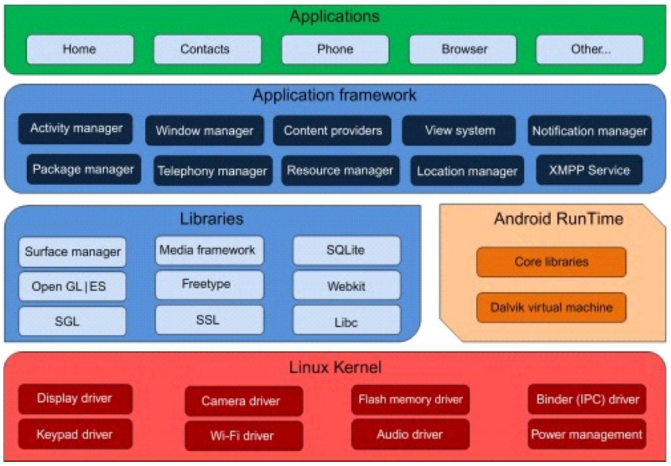
IV. METHODOLOGY

A. Android Architecture

Software components are arranged in stack in Android architecture. Runtime environments are a subset of software that includes anything from OS to middleware to native library to web services.

It's separated in five sections, as:

1) Linux Kernel
2) Native Libraries
3) Android Runtime
4) Application Framework
5) Applications



Following diagram shows architecture of Android Application respectively.

a) *Linux Kernel:* The Android operating system is based on Linux. The Linux kernel is foundation of Android operating system. Different device drivers are handled by Linux kernel, like the ones that control camera or display or Bluetooth or a keyboard and memory or processes or power in general.
b) *Native Libraries:* Media, Web Kit, SQLite so Runtime Library will be included in Linux Kernel's native libraries. Free Type fonts support, Web Kit browser compatibility & more are provided by Media Library.
c) *Android Runtime:* This is third component of architecture, and it is located at 2nd level. Runtime libraries and Android apps are handled by Dalvik virtual machine (DVM) included in the Android runtime. Similar to Java Virtual Machine (JVM), DVM is tailored formobile devices, unlike JVM.
d) *Application Framework:* The application framework goes on top of Android runtime and the native libraries. Class interface for Android app development and also higher level functions for Java classes, are provided by Android framework in Java. Apps like activity administrators, content producers & telephone managers are included in this category. Managing all parts of app life span & activities stack is responsibility of the Activity Manager (AM).

e) Applications: Top of application frame is application. Apps like as home, contacts, alarm, calendar, webcams, and browsers are all included in this section. Utilize the Android runtime & libraries with an Android framework. The Linux kernel powers the Android operating system and its native libraries. It is possible for users to construct apps which could only be used by users who have reached this level.

f) Structure of Android Application: The figure above shows the basic components of an Android application. An Android application in Eclipse or any developmenttool has a predefined structure with code and resources organized in a set of folders.

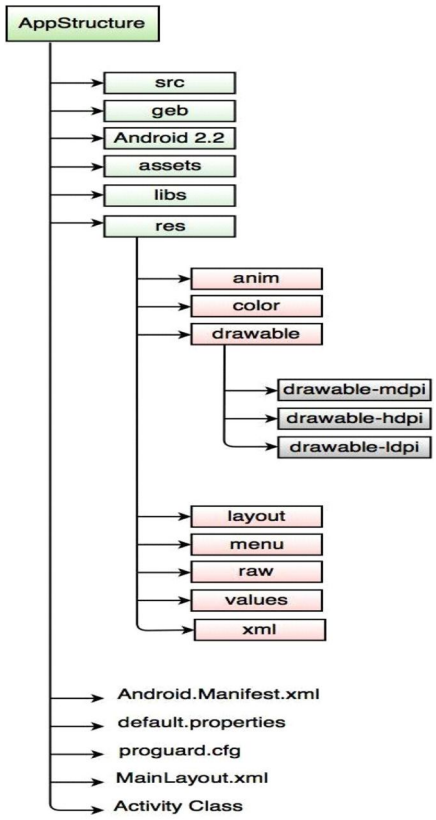


Fig. Structure of Android Application

B. Malware in Android Applications

Malware can be created using an application in Kali Linux which is known as Metasploit . But before we discuss about metasploit, let's have a quick overview on Kali Linux.

1) Metasploit Module

The main modules of Metasploit are:

a) Helper Module: Among the tools in the aid module are scanners, SQL injection utilities, as well as other applications that maybe utilized to gather information about target system..

b) Encoders: Encoders encrypt payloads / exploits to protect them from signature-based antivirus solutions. Payloads or exploits contain invalid or malformed characters that are more likely to be detected by antivirus solutions.

c) Exploits: As mentioned earlier, exploits are code that exploits target vulnerabilities to ensure system access through the payload.Payload: As mentioned above, the payload aids in achieving anticipated aim of attacking targeted system.

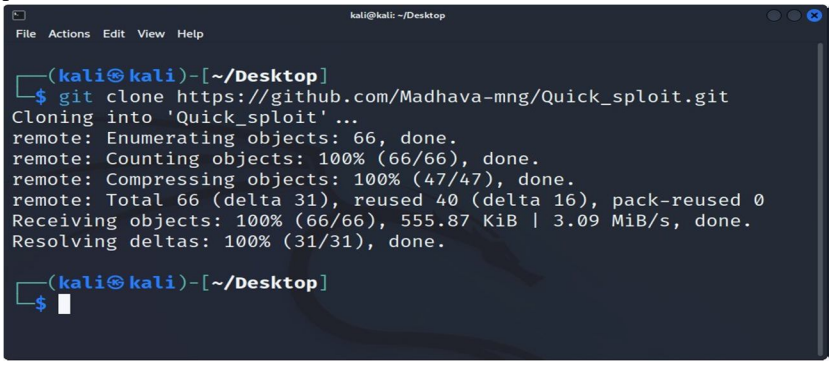
d) Payload: As mentioned above, the payload helps in achieving anticipated aim of attacking targeted system. It's useful for getting an interactive shell, waiting for a backdoor, executing commands, and loading malware. Metasploit offers two types of payloads: step less payloads and stepped payloads.

e) Post: Post-Abuse Modules Help Gather More Information About Your System. For example, When seeking for password hashesand login information for lateral migration or privileges elevation, it might be beneficial.

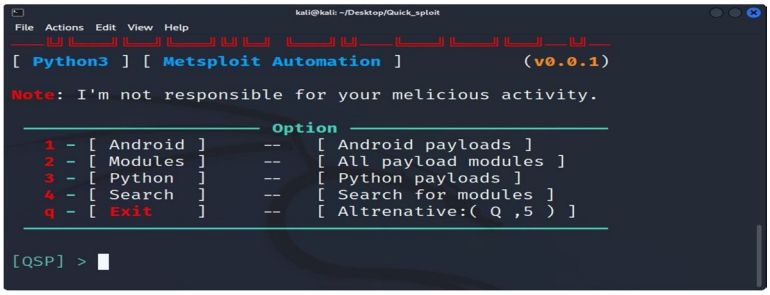
2) *Steps For Installation Of Metasploit And The Malware Attack On The Device Which Needs To Be Accessed*

a) *Step1:* Installing Quicksploit.

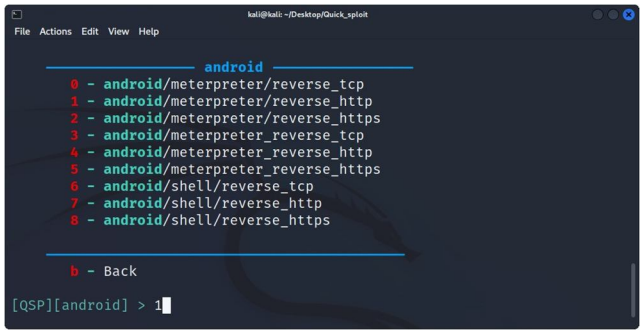
-



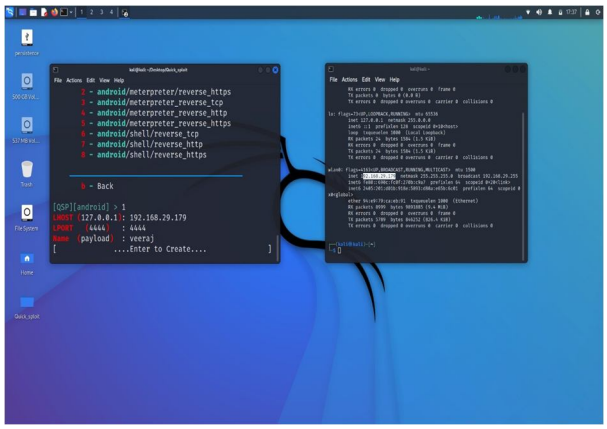
b) *Step 2:* Running Quickspolit .



c) *Step 3:*Using android/meterpreter/reverse HTTP

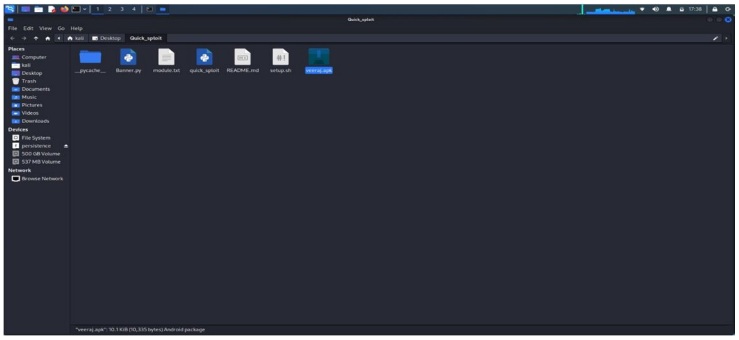


d) *Step 4:* Adding host IP address, port and naming the apk.

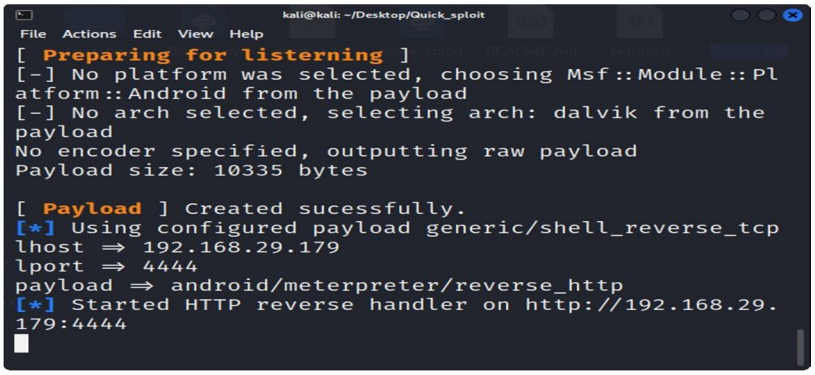


e) Step 5: Creating a Malware using Metasploit for testing.

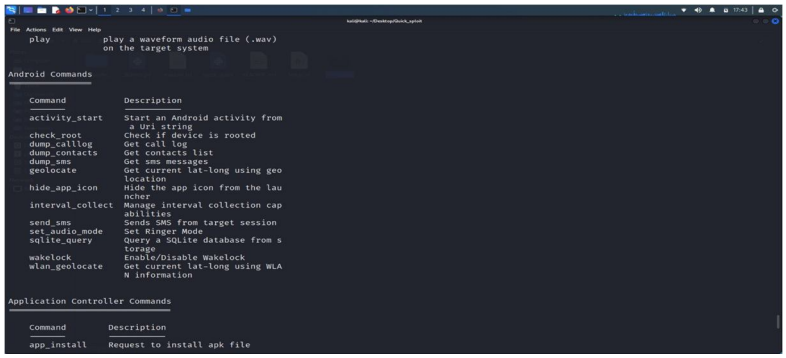
.



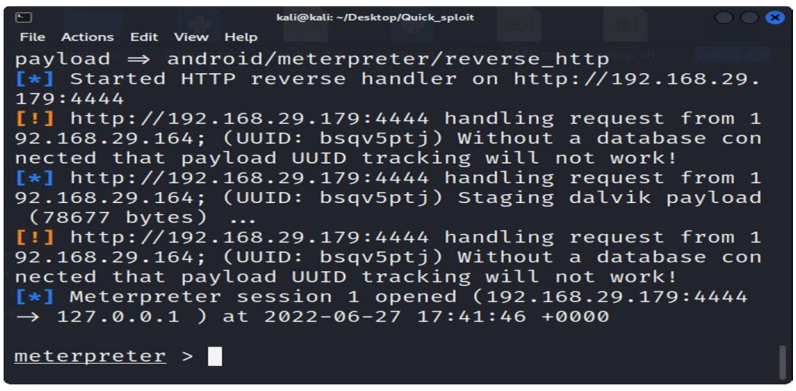
f) Step 6: Started listener.



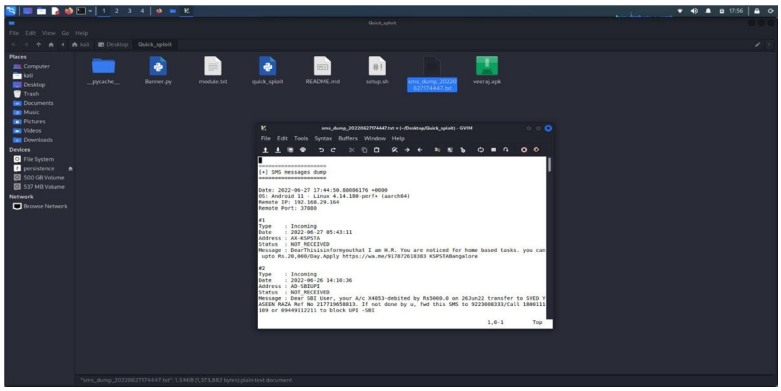
g) Step 7: Gained Access to Victim's Phone



h) Step 8: Type help menu. List of every possible command we could run.



i) Step 9: Contents of text file showing SMS Details.



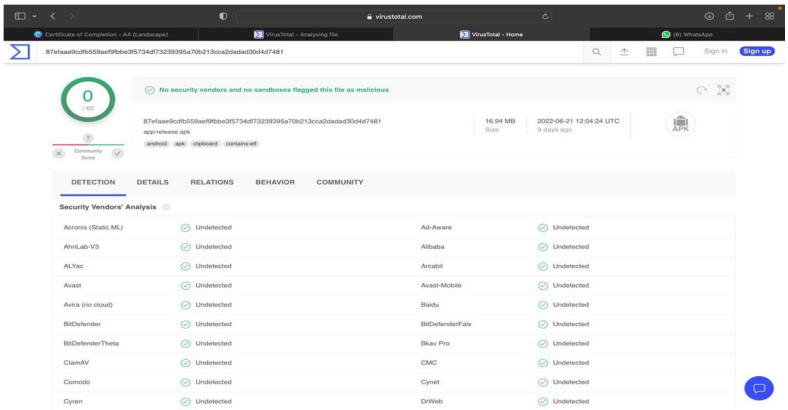
V. RESULTS

A. Analysis of Structural details of Android Apk

Files detected by other scans may be sent to anti-virus software makers who then run them by their own algorithm to enhance the product and subsequently VirusTotal. VirusTotal data may also be found by scanning suspicious URLs. The Cuckoo sandbox is used by VirusTotal to analyze dynamic malware. PC World picked VirusTotal as one of the top 100 products of 2007.

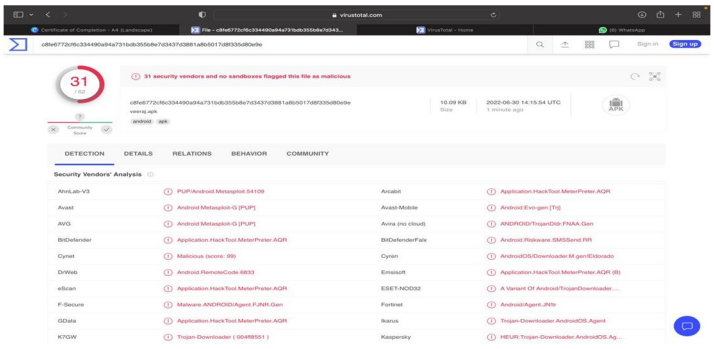
Virus Total score is an indication of the Structural changes that occur in the android application when it is attacked by malware. This indicators is used as a tool to study the minimal structural changes that occur in the files of the application before and after it is infected by malware.

Virus Total score of the APK before infection by malware:

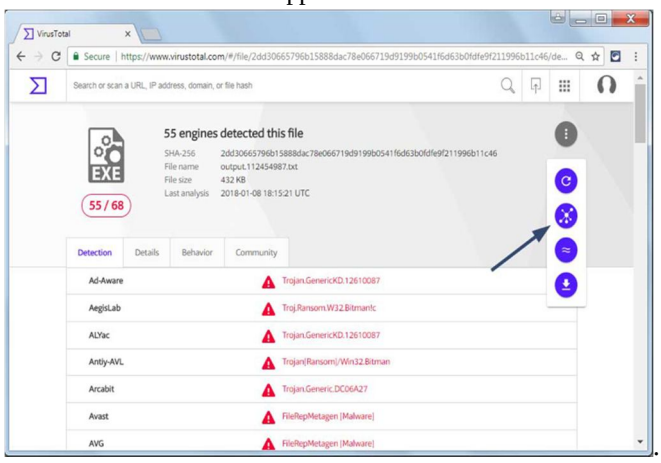


The score is Zero which indicates that the android application and the device in which it is installed both are free from the Malware.

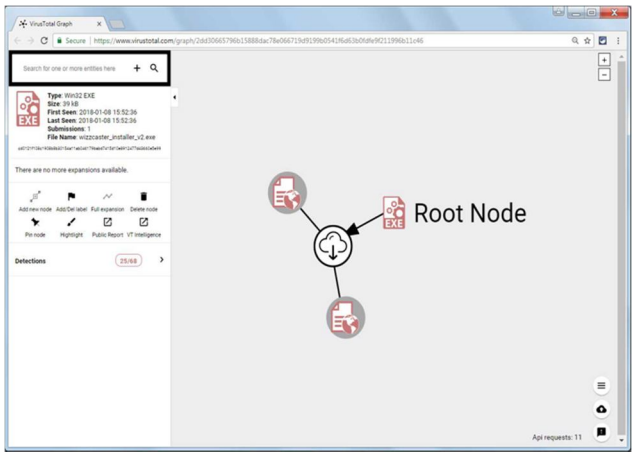
Virus Total score of the APK after infection by malware:



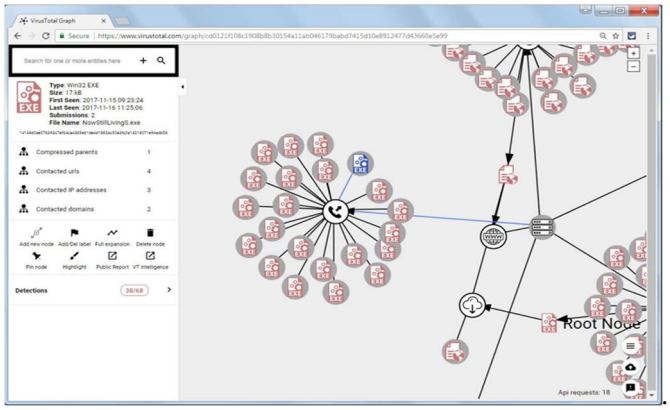
The score is now 31 which indicates that the malware Metasploit which was used to infect the Apk file has made the changes in the files which is by creating duplicate copies of preexisting files. This is an indication of the structural change that can be induced by malware in an Android application.

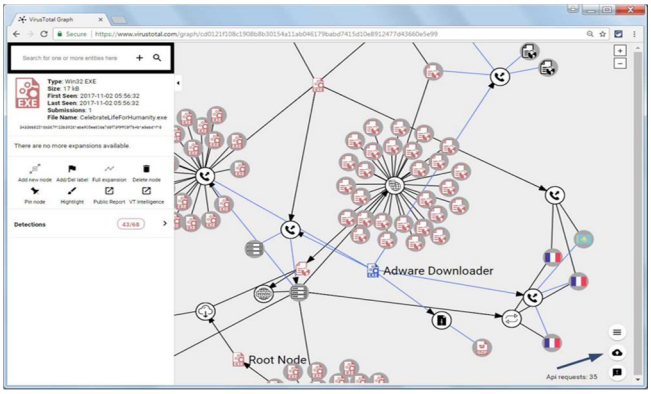


Accessing a Submission's graph.



VirusTotal Graph





Graph showing a file downloaded by the Root Node and object label.

VI. CONCLUSION

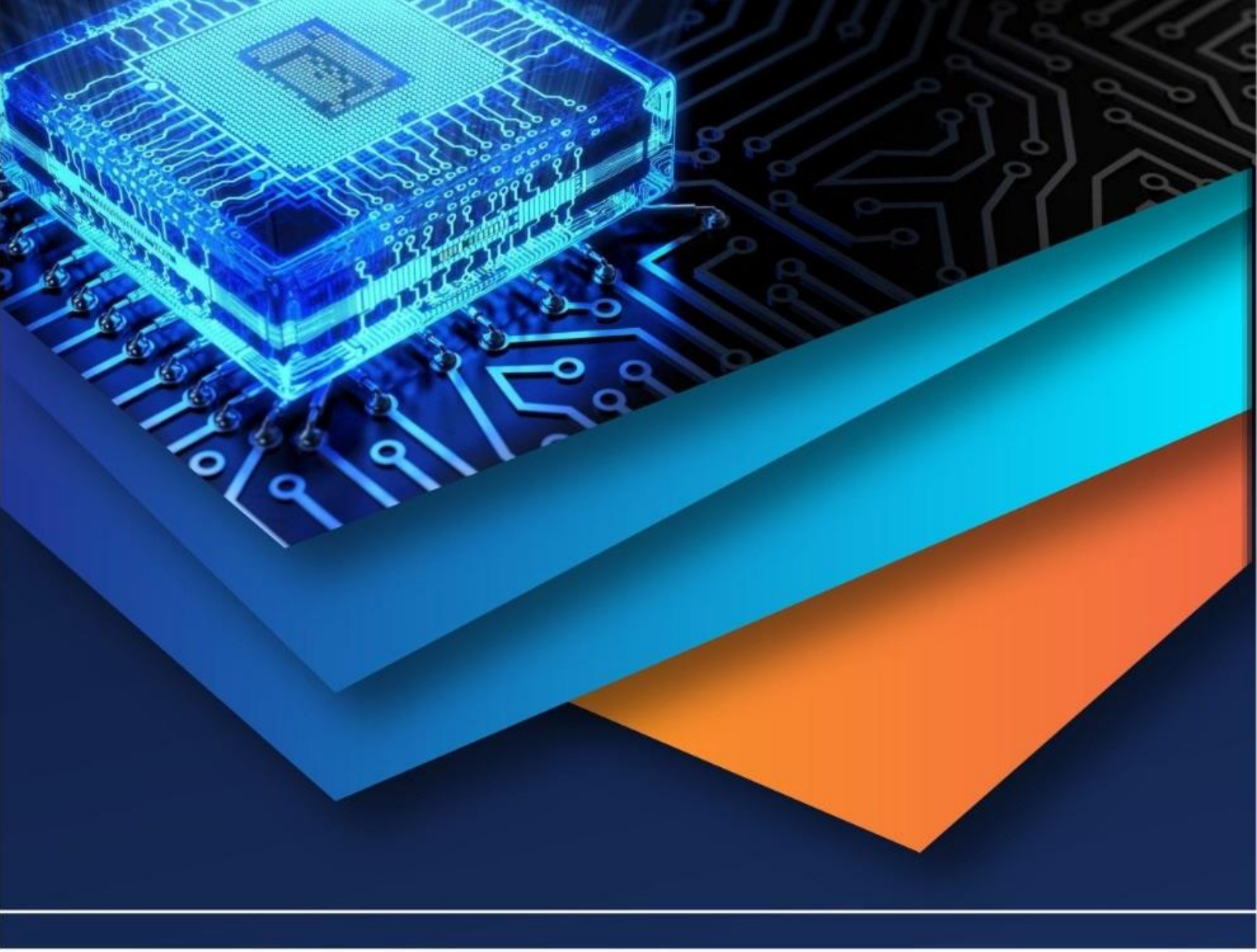
A user may notice information on an uploaded file graphically with the help of the VirusTotal Graph generated. This utility makes it simple to see data like hosts connected to, files created, and more. This is a data visualization tool that was constructed on top of the VirusTotal database. It offers a simple interface for pivoting and navigating between files, URLs, domains, and IP addresses, and it knows how they are related. We created the network and observed the relationships among the samples by selecting each node in the graph. Selecting the nodes, we can show the important details of each object instantly. We can add labels and get a detailed report by analyzing the VirusTotal public and VirusTotal Intelligence report. In the Graph page, there is an item called the Root Node. This is the object associated with the file that was submitted to VirusTotal. From this node, arises various arrows showing the information related to the sample.

Additionally ,we can keep our mobile device safe from hackers by following these instructions from Web root.

1) *Turning off Bluetooth:* If you don't use Bluetooth, keep it off. Leaving Bluetooth on and hibernating can open other backdoor for computer hacker.
2) *Do not Utilize Indiscreet Public WiFi:* Widespread WiFi networks which give access without passwords are not secure. They are a major target for computer hacker.
3) *Download the Security Application:* Install the security application on your phone in the same way you install firewalls, antivirus software & packages in your PC.Prevalent choices comprise Kaspersky Mobile Antivirus, Avast & Bit defender.
4) *Turn off Auto Completion of Typing:* When you're typing, your computer may figure out what you're looking for or fill in blanks. Hackers may get your mail address,phone number, & other personal information by using the program erase facility.

REFERENCES

[1] Literature Analysis on Malware Detection Parmjit Kaur and Sumit Sharma International Journal of Electronic and Electrical Engineering. ISSN 0974-2174 Volume 7, Number 7 (2014)
[2] B. Arief and D Bernard "Technical and human issues in computer-based systems security" University of Newcastle upon Tyne2010.
[3] Nwokedi Idika and Aditya P. Mathur "A Survey of Malware Detection Techniques" Department of Computer Science PurdueUniversity 2007.
[4] Nur Syuhada Selamat, Fakariah Hani Mohd Ali, N. A. Othman Computer Science 2016 6th International Conference on IT Convergence and Security (ICITCS)
[5] A Threat to Cyber Resilience: A Malware Rebirthing BotnetJuly 2011 Conference: 2nd International Cyber ResilenceConference Murray Brad
[6] Bonab, R.H.; Can, F. A Theoretical Framework on the Ideal Number of Classifiers for Online Ensembles in Data Streams. In Proceedings of the 25th ACM International on Conference on Information and Knowledge Management, Indianapolis, IN, USA, 24–28 October 2016; p. 2053.
[7] Webb, G.I.; Zheng, Z. Multistrategy ensemble learning: Reducing error by combining ensemble learning techniques. IEEE Trans. Knowl. Data Eng. 2004, 16, 980–991.
[8] Sagduyu, E.; Ephremides, A. A Game-Theoretic Analysis of Denial of Service Attacks in Wireless Random Access. In Proceedings of the 2007 5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks and Workshops, Limassol, Cyprus, 16–20 April 2007; pp. 1–10.
[9] Tsiropoulou, E.E.; Baras, J.S.; Papavassiliou, S.; Qu, G. On the Mitigation of Interference Imposed by Intruders in Passive RFID Networks. In Decision and Game Theory for Security; Zhu, Q., Alpcan, T., Panaousis, E., Tambe, M., Casey, W., Eds.; GameSec 2016; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2016; Volume 9996.
[10] Almubayed, A.; Hadi, A.; Atoum, J. A Model for Detecting Tor Encrypted Traffic using Supervised Machine Learning. Int. J. Comput. Netw. Inf. Secur. 2015, 7, 10–23.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY