iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.47887

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 XII Dec 2022- Available at www.ijraset.com

Review on Malware, Types, and its Analysis

Jeff Chandy
Amity Institute of Information Technology (AIIT), Amity University (AUR), Jaipur, Rajasthan

Abstract: ***Malicious entities utilize malware as a tool to carry out their nefarious plans. Malicious software, sometimes known as malware or mal-ware, is a type of program with malicious intents. Malware and spam both pose severe hazards to the security of systems, raising complex system issues. Malware that compromises computers through a coordinated attack includes worms, trojan horses, botnets, and rootkits. It is challenging to compile convincing evidence because inadequate tools are available, and the system is still in its infancy. This study examined the challenges faced by investigators in their search for a missing person. The author emphasized the need for a novel approach to malware detection that focuses on a robust framework and offered a solution based on a thorough literature evaluation and market research analysis. While market research was carried out to ascertain the precise nature of the current problem, the literature review concentrated on various malware detection tests and methodologies to establish the parameters for developing a solution design.***
Keywords: Malware, analysis, forensics, risks, security, system

I. INTRODUCTION

Malware is a type of harmful software that targets remote computers to steal sensitive data and access them in order to harm their resources. Malware can operate in the background of the system in many different ways, including as.exe files, scripts, dlls, files, macros, etc. By obtaining illegal access to the network and dispersing malicious code throughout it, malware infects computer network security. At the moment, a number of malware problems are plaguing the internet, endangering the security of computer networks. Virtually every element of the computer business has been infected by malware, which is viewed as a global threat.

According to current data, global malware used nowadays is to blame for 80% of cyberattacks. Malware is shared widely online and targets businesses, wealthy individuals, and colleges and universities that are connected to the internet. This enables the cybercriminals to use internet-based services to their advantage in order to steal data from the affected targets.

In 2016, there were over nine mega breaches (a breach with more than 10 million records is considered a mega breach), and the overall number of identities exposed by malware increased by 23% to 429 million, according to Symantec's Internet Security Threat report from that year.

Not only businesses but also end users cannot ignore it. Over the past ten years, there have been significant changes in the types of computer devices available and in how they are used. Cell phones and personal computers are used to conduct bank transactions, make hotel and travel reservations, pay utility bills, serve as automobile key fobs, run home appliances, manage IoT devices, and more. A lot of sensitive information is stored on our personal devices, including usernames, passwords, and pictures. No one can afford to get hacked these days. Malware assaults in the past directly implicated a business or a government agency, but now they increasingly target and attack the computing devices of end users in order to monetize.

The purpose of the disguised payloads or attacks is to deceive the user into carrying out execution by making them appear friendly. The backdoor application installs a server component as part of the installation process that opens a specific port or service within the host secure channel, enabling the attacker to connect remotely using the client component.

Installing backdoors has a number of critical drawbacks, the most dangerous of which is that the attacker can return at any time and easily get access to the infiltrated network. Back doors are installed in every system in the target network to make sure the attacker can exploit other systems even if one system is cleaned up and the threat is taken away, resulting in a persistent attack.

The key component of a malware attack is to steal data from the host, which is the next significant step. The attacker gains access to every compromised system on the network and collects sensitive and vital data there. This could contain crucial information like bank account information, patent rights, personal information, etc. From the infected machines, the stolen data are forwarded to servers that belong to the attacker or to other computers on the same network. The attacker leaves the network for a while after completing the data movement. The attack leaves virtually no trace because it merely masquerades as normal data flow within trustworthy systems. Any of the back doors the attacker previously installed will allow him to subsequently resume his attack anytime he pleases.

Malware analysis's primary goals are to gather in-depth knowledge about a piece of malware's capabilities, to assess the potential harm it can cause to a target system, to plan for potential damage repair, and, if at all possible, to identify the attacker.

Most of the time, organised crime rings are responsible of malware threats with properly planned out schemes to automate crimes. Software companies have created strategies to trade, introduce, and stay informed about malicious codes in order to gain an advantage; however, the malware industry has created transmission and support systems to help criminals successfully deploy malware. Security workers need to learn more about malware analysis because it is an industry that is expanding. Several studies predict that the malware analysis industry will increase from 3 billion in 2019 to 11 billion in 2024. This growth forecast is based on the observation that malware is not only getting more prevalent every day but also getting more sophisticated with the introduction and application of new technology. Additionally, malware now has new attack surfaces to target and profit from thanks to the availability of new computing platforms like the cloud and IoT. Due to a lack of security specialists with the necessary expertise to combat malware, the defence remains mostly unmanned even if the attack surface and complexity have grown.

II. RESEARCH METHODOLOGY

The paper is organized as follows: Section 3 explains the various types of malwares followed by its functionalities, attack model, etc. Section 4 discusses the methodologies for the analysis of malwares. Section 5 mentions the challenges faced by the analysts in the present-day analysis of the malwares, followed by Section 6, i.e., Conclusion.

III. TYPES OF MALWARE

The field of malware analysis has developed a number of regularly used terminology for malware and its functionalities. Despite the fact that there are many different kinds of malware, the following are the most prevalent today:

1) *Virus:* A computer virus is a form of malware that accompanies another programme (such as a document) and has the ability to multiply and propagate once it has been run on a machine. For instance, you can unintentionally open a dangerous email attachment after receiving it, resulting in the infection of your machine with the virus. Viruses can damage data, absorb system resources slowly, and record keystrokes.
2) *Trojan:* This is a a kind of malware that usually finds its way onto a user's device by masquerading as an email attachment or a free download. Once downloaded, the malicious code will carry out the purpose for which it was created, such as gaining unauthorised access to business systems, monitoring users' internet activities, or stealing confidential information. Unusual behaviour on a device, such as unexpected changes to computer settings, is a sign that a Trojan is active on it.
3) *Worm:* A computer worm is a subset of Trojan horse malware that, once infiltrating a system, can spread or self-replicate from one computer to another without human activation. Your LAN (Local Area Network) or Internet connection is frequently used by worms to spread throughout a network.
4) *Spyware:* Spyware is often considered to be harmful software intended to infiltrate your computer system, collect information about you, and send it to a third party against your will. Spyware also refers to legitimate software that tracks your data for commercial purposes like advertising. However, malicious malware is created with the intention of profiting from stolen data. You are vulnerable to data breaches and the misuse of your personal information due to spyware's surveillance activities, whether it is honest or motivated by fraud. Due to the fact that malware slows down typical user activity, it also affects the performance of networks and devices.
5) *Ransomware:* An organisation or user's access to files on their computer might be restricted by ransomware, a type of malware. Cyberattackers lock up these files and demand a ransom in exchange for the decryption key, putting businesses in a situation where paying the ransom is the quickest and least expensive method to get back access to their files. To further entice victims of ransomware to pay the demanded ransom, several variants have included further capabilities, such as data theft.
6) *Rootkit:* This is intended to allow remote access to the system without the user being aware of it. If a rootkit is successful in running, it can carry out a variety of actions on the system, including uploading files, installing programmes, changing system files, or turning off tools like antivirus software.
7) *Bot:* This malware enables the attacker to take over the user's system or carry out a certain task without the user's knowledge. In large-scale attacks, bot malware is typically deployed to take advantage of the system's computing capability.
8) *Crypto-Malware:* This type of malware gives a threat actor the ability to engage in cryptojacking behaviour. While the method employed by hackers and legitimate cryptominers is fundamentally the same, crypto-malware makes use of another user's devices and processing capacity to obtain payment.

9) Fileless Malware: A type of memory-resident malware. As the name implies, this malware runs from the computer's memory rather than from data on the hard drive. It is more difficult to find than conventional malware because there aren't any files to scan. Additionally, because the infection disappears after the victim PC is restarted, it makes forensics more challenging.

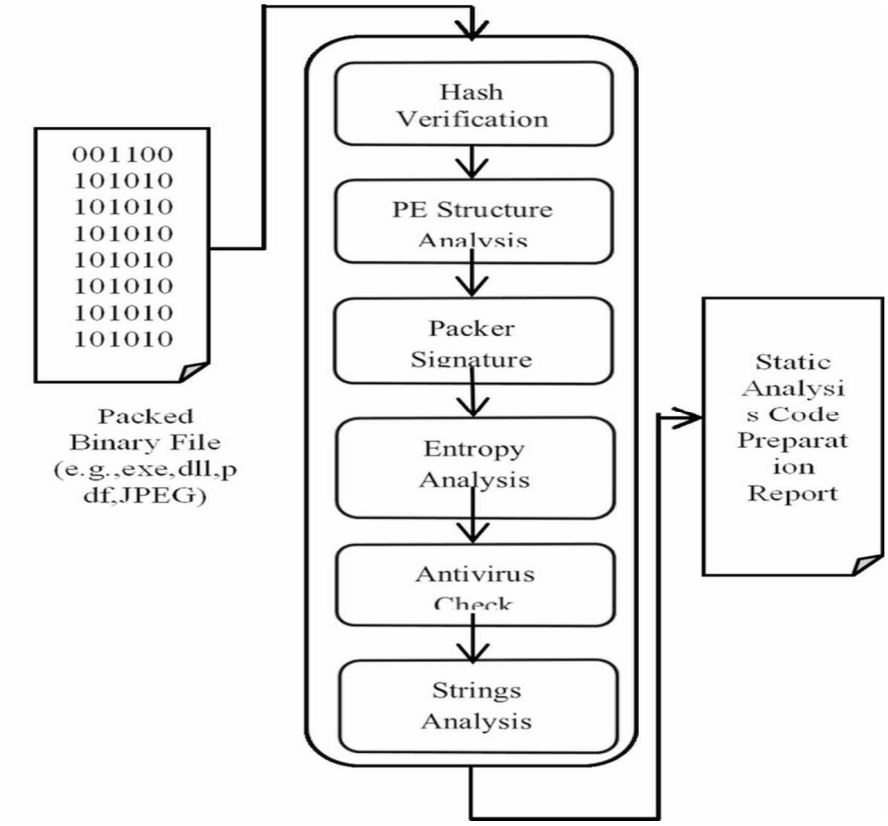
IV. ANALYSIS AND METHODOLOGIES

Malware analysis is a procedure used to look at the components and behaviours of malware and, if possible, pinpoint the attacker. Through a variety of tools and approaches, malware that has infected the target system can be found and examined.

Malware analysis can roughly be divided into two types:

A. Static Analysis (Code Analysis)

This is a quick and easy analytical method. Analysis of malware is possible both with and without execution. As opposed to running a sample and studying its behaviour, which is known as dynamic analysis, static analysis examines a sample without running it. This investigation decompiles the virus and uses a number of tools to examine its source code. Since the source code of the virus can openly expose its destructive intent, it can provide crucial information such as DLLs called by the infection, URLs viewed, etc. Therefore, malware authors strive to conceal the malware's dangerous code by utilising the packers discussed before. The major focus of static analysis technique is the identification and unpacking of such packers. Static analysis has played a significant role as a preliminary analysis technique throughout the history of malware investigation.

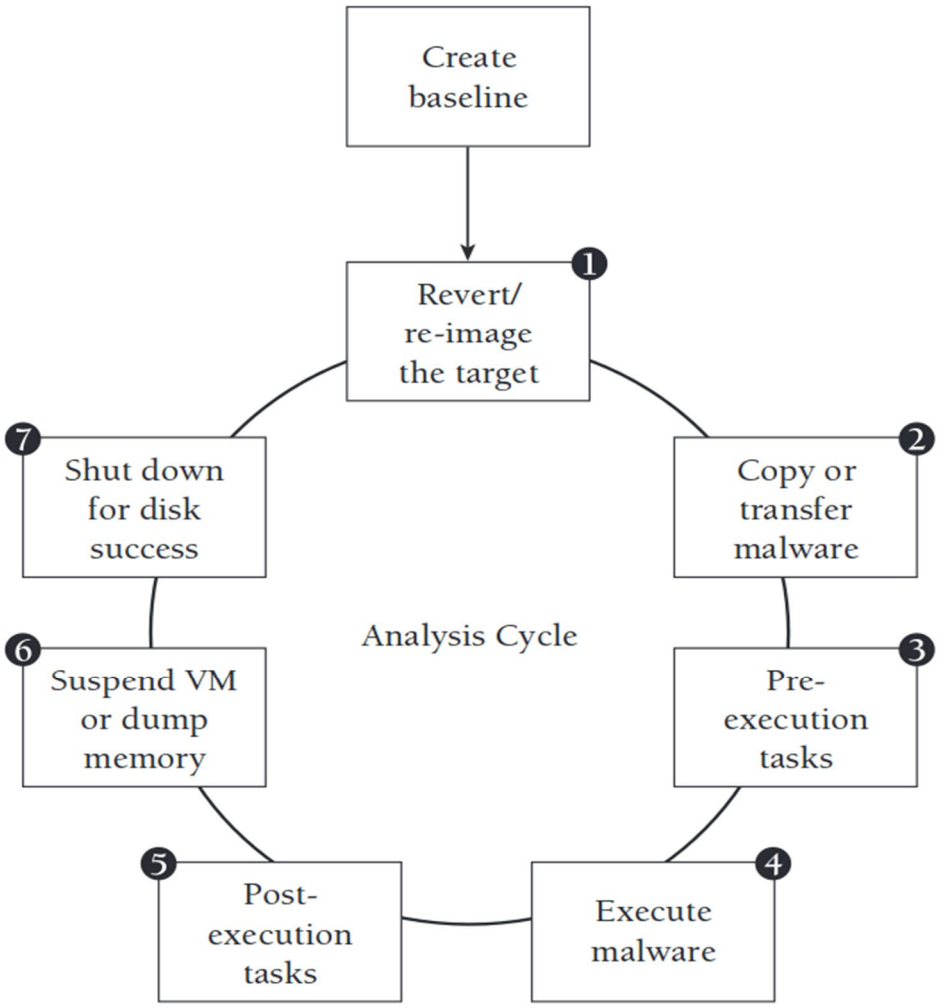


Source:https://www.researchgate.net/figure/Structure-of-static-malware-analysis_fig2_332215777

A solid grasp of programming and x86 assembly language concepts is needed to do static analysis. You don't need to run the malware during the static analysis procedure. Malware sample source codes are typically not easily accessible. After successfully completing reverse engineering, you must first disassemble and decompile the target code before you can examine the low-level assembly code. Because static analysis is safer than dynamic analysis, the majority of malware analysts execute it sooner in the malware analysis process. Modern malware is complex, and some of it uses anti-debugging systems to prevent malware analysts from analysing the code, which makes static analysis difficult.

B. Dynamic Analysis (Behaviour analysis)

In the process of analysing malware, dynamic analysis, also known as behaviour analysis, executes the malware and keeps track of its activity. Additionally, it tracks any adjustments made as the malware is executed. It entails running a sample through a number of tools, logging the behaviour, and observing the numerous artefacts that the malware's execution produces. When combined, they can aid in more accurate analysis and judgments about the sample.



Source: https://www.researchgate.net/figure/Dynamic-malware-analysis-34_fig1_316446553

Static analysis can identify straightforward malware. Malware can becoming more complicated and sophisticated, and simple static analysis cannot find them. These malware programmes hide their code in order to avoid static detection methods. When examined, such sophisticated malware frequently presents as harmless, but when it is executed, it calls malicious code stored elsewhere. Only after they have been used can these malwares be detected. A sandbox is a secure environment where suspected dangerous code is run in dynamic malware analysis. Security professionals can closely monitor the virus in activity in this closed, isolated virtual machine without worrying about infecting the machine or the network. The threat and its genuine nature are more clearly seen thanks to this strategy.

As a side advantage, automated sandboxing saves time that would have otherwise been spent on reverse engineering a file to find dangerous code. Dynamic analysis can be difficult, especially when facing intelligent adversaries who are aware that sandboxes would eventually be exploited. Therefore, opponents hide their code so that it is inactive until a set of circumstances is met as a sort of deception. Only then will the code run.

V. CHALLENGES IN MALWARE ANALYSIS

The behaviour heuristics of improved malware types frequently change in order to achieve better levels of avoidance and avoid detection. When using automated systems, inside code might change and appear different to any detection tool, leading to malware being disregarded or what appears to be a never-ending stream of viruses attacking the system before flooding it.

Large amounts of information from malware analysis studies have been gathered, yet the findings are frequently unclear. Additionally, data is frequently not well recorded for referencing needs. Most malware analysis companies focus on antivirus algorithms and technologies, thus they don't want to share their knowledge or experiences in this area to protect their trade secrets (Neelakantanand & Rao, 2008)

Signatures are straightforward patterns seen in malware that take the form of bytes with hash information in an executable format. They are compiled in a well-known database and usually used in tandem with algorithms or techniques for spotting questionable files (Demme et al., 2013). The issue with this tactic is that malware frequently alters its functionality or characteristics on its own, as noted by Vinod & Laxmi in 2009.

VI. DISCUSSION AND CONCLUSION

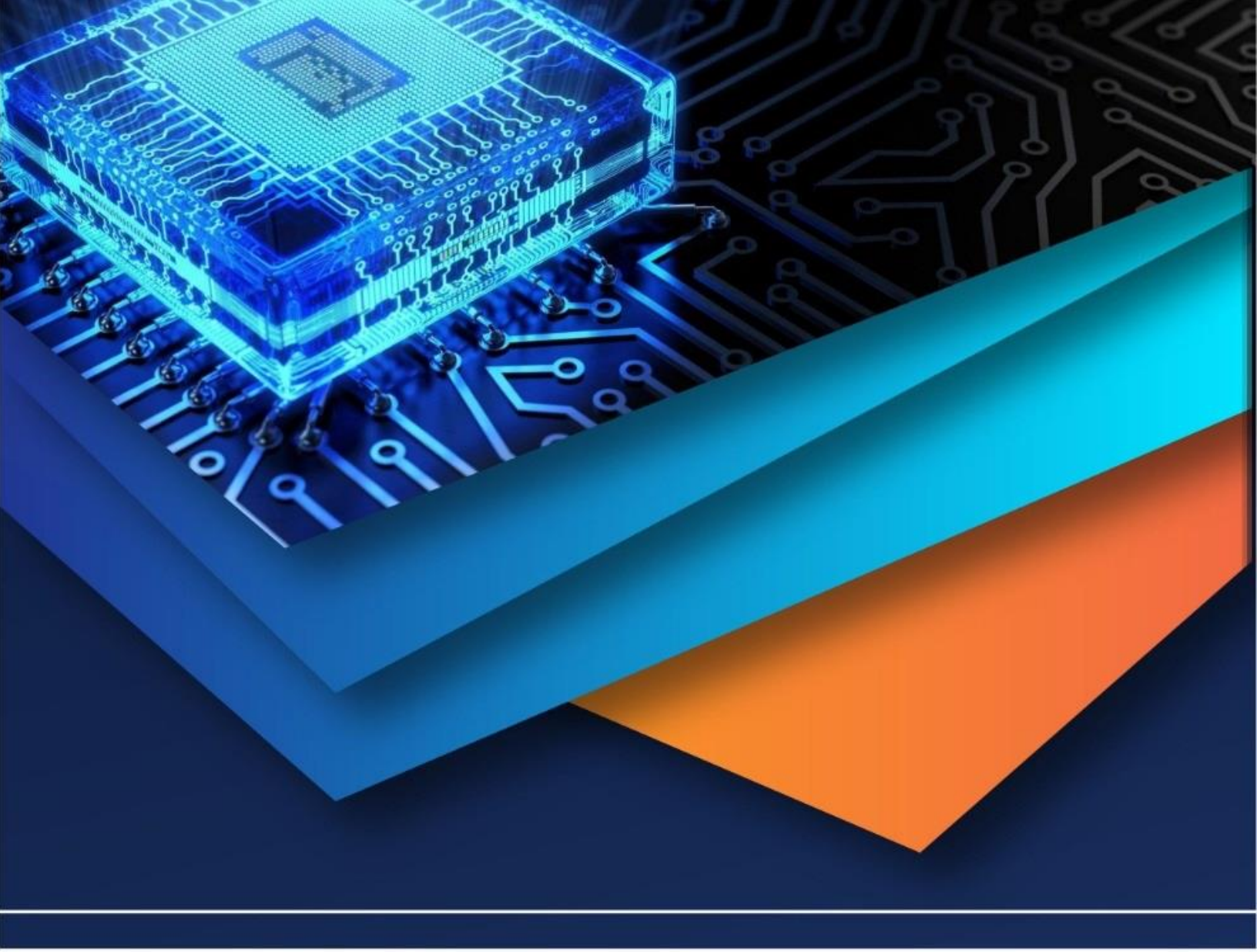
The steep increase in malware attacks over the past few years demonstrates that many businesses, from huge multinational firms with substantial security budgets to small businesses and individual users, are unable to adequately defend their systems from these cunning cyber attackers. Systems grow more open to attack due to rising security flaws and technological advancements, which also make them more appealing targets. Every day, new varieties of malware are created and disseminated in an effort to take advantage of this as a means of income. The small number of studies in this area and the inadequate recognition of the issue both contribute to an increase in malware victims. Without a doubt, victimisation will remain a severe issue for a very long time.

This study provided a thorough explanation of what malware is. We've quickly explored a few types of malware that can harm a computer system as well as their impacts and effects in the cyber world. Examples of these categories include Trojans, worms, backdoor programmes, botnets, malicious software, and viruses.

The features that can be used to identify patterns of malware vulnerabilities in a system have been discussed in relation to various malware detection techniques. Static analysis and dynamic analysis, two of the main types of detection, were covered.

REFERENCES

[1] Crabtree, B.F., Miller, W. L. (eds.) (1992). Doing Qualitative Research. Newbury Park,
[2] CA: Sage. Curtis, K.R. (2008) Conducting Market Research Using Primary Data. Whitepaper by the Department of Resource Economics, University of Nevada.
[3] Damodaran, A. (2015). Combining Dynamic and Static Analysis for Malware Detection, Unpublished Master's dissertation, San Jose State University.
[4] Dickens, P., Thakur, R. (2000) An Evaluation of Java's I/O Capabilities for High Performance Computing. San Francisco, CA: Java. Dilkina, B.,Gomes, C.P., Sabharwal, A. (2009) 'Backdoors in the context of learning', in Proceedings of the 12th International Conference on Theory and Applications of Satisfiability Testing (SAT 2009)(pp. 73–79). Swansea, UK.
[5] https://www.theguardian.com/small-business-network/2016/feb/08/
[6] huge-rise-hack-attacks-cyber-criminals-target-small-businesses.
[7] A. Vance, Flow based analysis of APTs detecting targeted attacks in cloud
[8] computing, in: 2014 First International Scientific-Practical Conference Problems of Info communications Science and Technology, Kharkov, 2014, pp.173–176.
[9] https://www.scalar.ca/en/blog/major-cyber-attacks-on-financialservices-firms- illustrate-the- importance-of-data-security/.
[10] https://www.fisglobal.com/Solutions/Banking-and-Wealth/Risk-andCompliance/-/media/FISGlobal/Files/Report/2016-Risk-PracticesSurvey.pdf.
[11] www.virustotal.com.
[12] A Threat-Aware Signature Based Intrusion-Detection Approach for Obtaining Network-Specific Useful Alarms S. Neelakantan, S. Rao Published 29 June 2008
[13] Vinod, P., Laxmi, V. and Gaur, M.S. (2009) Survey on Malware Detection Methods. Proceedings of the 3rd Hackers' Workshop on Computer and Internet Security, Kanpur, 17-19 March 2009, 74-79.
[14] Coviello, A.W. (2011) RSA Written Testimony. US House of Representatives, the Security Division of EMC, CA USA



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY