1999 – 2019: THE ANALYSIS & SURVEY OF MAJOR CYBER ATTACKS (The Impact of Cyber Attacks on Digitized World & Security Measures)

Suriya Gharib
Department of Computer Sciences, COMSATS University, Islamabad,
Abbottabad Campus, Pakistan
suri.rehman3@gmail.com

Somiya Zaman
Department of Computer Sciences, COMSATS University, Abbottabad
Abbottabad Campus, Pakistan
somiyazaman7@gmail.com

Syeda Roshana Ali Naqvi
National University of Sciences & Technology (NUST),
Islamabad, Pakistan
snaqvi.mscs17seecs@seecs.edu.pk

Abstract- **The rapid development in technology enabled the use of computer systems for communication in all the sectors including governance, military, education, energy, and finance etc. The adversaries are easily attracted towards these sectors for disrupting, spying, & steeling information worldwide. So, in this era of digitized world where information is communicated and shared via electronic means security and privacy are at risk. This paper is a survey of major cyber attacks from 1999-2019 and underlying motives behind those attacks. It also analyzes the attacks to understand the techniques, targets and motives of attacks. Furthermore, preventive measures to cyber security are also proposed in this paper.**

Keywords-- Cyber-attacks, cyber security, data breach, threat actors

I. INTRODUCTION

In the modern era of technical world information is stored, shared and processed digitally. Privacy and security of networks and personal information is of the major concern in this era. The tremendous increase in computer and network technology has resulted in large proportion of cybercrimes. Fifteen major data breaches in EU were resulted in 2016, leaking personal information of 41 million records including email, contacts and address [1]. The monetary loss due to cybercrime in United States of America was 1,070,000,000 $ in 2015. This loss has been expected to reach 2.1 trillion dollars by 2019[2]. In spite of the economic loss cyber-attacks are now targeting individuals and cooperate organizations. In order to prevent the digital world of cyberspace, cyber-attacks must be examined carefully. Cyber-attacks are difficult to cater due to cloaked identities of perpetrators. But counter actions can be taken that may avoid the occurrence of threats in future.

This paper has analyzed the major cyber-attacks and their impact on the digital world. The preventive strategies to avoid cybercrimes in future has also been discussed.

Organization: The paper is organized as follows. In Section II the related work carried in past regarding cybercrimes is covered. Section III highlights the objective of survey. Section IV describes threat actors in cyber security. Section V focuses on major cyber-attacks and section VI includes the analysis of those attacks. Section VII encompasses the precautionary measures to be taken to avoid these attacks. Finally, in section VIII we conclude our survey.

II. RELATED WORK

Many researchers by their research study have published the analysis of cybercrimes, investigations, discussions and preventive measures regarding past cyber-attacks that will help to encounter cyber threats in future.

E.K Maclean [3], established that effect of cyber space is the result of malevolent agents that spread and cause damage to critical infrastructure and human beings. Cyber weapon could open the doors for individuals having ill-intention such as criminals, foreign governments, hackers and cyber terrorists. These individuals scheme agents and spread cyber threats that are difficult to counter. These influences may uncover severe threats to homeland security due to responsiveness of citizens in cyberspace.

P. Paganini [4], observed that range of cybercrime is wide and cyber weapons may hit critical infrastructure of country. The major cyber-attacks target the defense system, hospitals, banks, educational sectors, automated system, water supply, transportation system and control systems. Cyber weapon is a device or tool that damages a computer system unlawfully. The information facilitates the interruption, its data or program having the nature of critical infrastructure.

Halevi et al. [5] and Alseadoon [6] have evaluated different human traits such as trust, demographics and email experience. They analyzed the human traits to predict email phishing by individual detection ability. Personality trait has been assumed to have direct influence on individual detection ability for email phishing.

In 2015, Amin Kharraz [7], has presented fully programmed approach called HELDROID which is fast and effective to recognize known and mysterious ransomwares from good wares. In 2016 Hiran V. Nath et.al [8], proposed machine learning technique based on statistical analysis used for malware.

Further in 2016 Jan Frick et.al [9], analyzed four types of common ransomwares and identified that prevention mechanism of infecting system relies on the recovery tools available in target system. System tools that handle shadow copies are helpful to counter ransomware attacks.

III. Objectives

This survey has been carried out to meet the following objectives:

- ➢ To analyze the major cyber-attacks and their impact on humans, economy and cyberspace.
- ➢ To propose the preventive measures that may help to counter cyber threats in future.
- ➢ To identify the system vulnerabilities and criminal’s motivation towards cyber-attacks.
- ➢ To analyze the different research articles and deduce a result.

IV. Threat Actors In Cyber Security

To understand cyber security and prevent cybercrimes in future it is necessary to know your enemy. What they want and why they are targeting a specific system? Some of the threat actors involved in cybercrimes are listed as follow:

1. *Nation-state Actors:* This group of actors is usually funded by government and intelligent agencies to perform sophisticated attacks. They are motivated by economic, political, military or technical agendas. Their main purpose is to target organizations and users to measure their competency level through espionage.
2. *Hacktivists:* Their main purpose is to promote any political agenda. They either create a high-profile attack or cause damage to the opposed organizations.
3. *Insider Threat*: This threat is caused by the employees currently working in an organization or are ex-employees. These actors have the deep knowledge about the organizational structure and commit crime either to take revenge or financial gain. They also collaborate with other threat actors.
4. *Organized crime:* Cybercriminals engaged in targeted attacks for financial gain seek to exploit the weakness of targeted organization and systems. They attack either to hijack the resources of targeted system and organization and demand ransom amount or to capture personal identifiable information (PII) of employees such as contact information, email accounts, social security numbers, credit cards, banking information etc.
5. *Cyber espionage:* Cyber espionage is done to gain access to system resources of targeted organization to monitor their activities through a network. These actors are also hired by government agencies or organization to measure the competence level. Their target is to cause reputational damage.

Threat actors involved in cybercrimes to attack different systems and organization for different purpose. Their motivation differs on the basis of attack types. Threat actors along with their motivation and attack example with possible outcomes are clearly defined in Table 1.

TABLE 1: THREAT ACTORS

Threat Actors	Description	Attack Example	Motive	Outcome
Nation state	Hackers hired by the government to penetrate the commercial systems and government systems of other countries.	US attack on Iran via stuxnet, Iran attack on US Bank information.	• Cyber espionage. • Disable critical Infrastructure. • Political outcome disruption.	• Financial loss to victim. • Economic gain for the state and loss to victim.
Hactivist / hactivism	Individuals or group of individuals who by means of tools promote their political, social and ideological agendas.	Anonymous attacks on payment processors in defense of wiki leaks.	• Political gain. • Social change. • Reputational damage. • Thrill seeking.	• Service Disruption.
Third Party / Insider Threat	Service providers or vendors who have: • Access to data. • Access to system. • Access to facilities.	Misusing the credentials and system resources of organization.	• Competitive advantage. • Financial gain. • Information collected to be utilized for future.	• Reputation gain. • Assets damage. • Financial loss to target.
Organized Crime	Well-structured group of hackers or criminal organization that seek to exploit weakness by attacking defended targets.	Bank, government, intelligent agencies or other government sector systems takeover through malware and impersonation.	• Financial gain. • Revenge. • Personal grudges.	• Competitive level. • Economic loss for victim. • Reputational loss to victim.
Insiders	Former or current employees misusing the authorized access for cybercrimes.	Financial, political or economic attack.	• Personal advantage. • Monetary gain. • Malevolent behavior. • Blackmail. • Bribery. • Financial means.	• Financial loss disruption. • Monetary loss.
Cyber espionage	Gaining illicit access to confidential information by the use of computer networks, held by organization or government.	IP theft, Planting backdoors in firewalls, exploitation of identified vulnerabilities.	• Information gain. • Financial gain. • Economic gain.	• IP loss. • Financial loss to victim. • Economic loss.

V. MAJOR CYBER ATTACKS

Internet has become and attack vector for attackers. Various attacks are committed by cyber criminals; either for financial gain, to harm reputation, victim's defacement, targeting the competitive and well-known organization to destroy their identity and for various other means. Any action that threatens CIA (Confidentiality, Integrity and Availability) triad of a network resource falls under attack. The CIA has following explanation:

- **Confidentiality:** Information must not be made available or disclosed to unauthorized entity, individual, process or an organization.
- **Integrity:** Data should not be modified or tempered in unauthorized manner.
- **Availability:** Data must be available to authorized entities whenever demanded.

This survey focuses on the major cyber-attacks that are discussed below:

1) *Denial of Service:*

This attack is accomplished by an attacker against intended user which may prevent the legitimate users to access the system and network resources. Denial of service (DOS) attack flood the servers, networks or systems with traffic to overwhelm system resources and making it impossible for the legitimate users to use them. Some of the common types of DOS attacks are:

- Ping of death attack.
- SYN attack.
- Buffer overflow.
- Mail bomb.
- Teardrop.
- Distributed denial of service attack (DDOS).

2) *Ransomware:*

In the recent years' ransomware has spread like a cyclone wind in cyber world. The data is kept secure in computer systems by users and this data can be hijacked. Ransomware is a software virus that hijacks system data. Ransomware locks the user system in such manner that it cannot be reversed by knowledgeable person. The data is encrypted and cannot be decrypted by the user [10]. This attack not only targets the personal computers at home but also targets the systems in business sectors and other organizations. To get the data back victim has to pay some ransome amount. The motive behind this attack is usually financial gain.

3) *R2L - Remote to Local (User) Attack:*

In this class of attack an attacker sends packet to target machine over a network. The vulnerability of the system is exploited to gain local access illegally.

This attack occurs when user has ability of sending packet to targeted machine and he exploits the vulnerability to gain local access on the system. Some of the methods to gain authorized access on a system are Ftp write, Dictionary, Xsnoop and guest etc. These all attempts exploit the vulnerable and misconfigured systems. Social engineering can be made successful through Xlock attack which spoofs human operator to provide passwords to screensaver that is actually Trojan horse.

4) *Probing:*

In this type of attack attacker scans the network to gather information and to find known vulnerabilities. An attacker creates architecture of scanned system can identify the vulnerabilities and exploit them. The ports scan is used to determine open ports and services running on the target system. This scan is useful for the system auditors to improve the security. On the other side attackers use the gained information for compromising the security of target system. Port scanning provide the value able information of hosts that are live on the network, topological details, IP address, MAC address, gateway and router filters and firewall rules etc.

5) *U2R- User to Root Attack:*

In this class of attack an attacker accesses user account on system and exploit the vulnerability to gain root access on the system. The normal access to account is gained by attacker through sniffing, social engineering or dictionary attack. There various types of U2R attack. The most common is buffer overflow attack. In buffer overflow attack program copies the data in buffer without checking that data will fit or not.

TABLE 2: MAJOR CYBER ATTACKS

Major Cyber Attacks				
Attacks	**Year**	**Exploits Techniques**	**Motives behind attacks**	**Impact**

Massive Cyber Attack	October, 2019	Encryption of files and restricting the access	Disruption	Hospitals of Arkanas were affected by massive cyber-attack. This attack encrypted the files on the systems and limited the access. This affected the whole management system of hospitals which resulted in shifting to manual mode.
Ransom Cyber Attack	May, 2019	Ransom	Financial	Baltimore city wat attacked by hackers and $76,000 were demanded in bitcoins as ransom. The city denied paying ransom which resulted in 18 million loss impacting critical systems. This includes disruption, halting of network systems, and even real estate transactions were suspended.
Massive Cyber Attack	24 Apr 2018	Through command: ping-ping-ping-pew-pew-pew	Disruption	The country of “Berylia” is under a cyber-attack: Internet service providers and military air bases have been breached and the nation’s security is deteriorating Electricity Supplies, 4G network and drone operations have been disrupted and internet systems are under intense pressure.
GitHub Website Attack	28 Feb 2018	DDOS	Disruption	Memcached severs compromised because of misconfiguration.
WanaCry	May 2017	Encrypt Data	Financial	200,000+ system affected and more than 150 countries
WikiLeaks Vault 7	7 March 2017	Data leakage	Disclose data	Detail activities and capabilities of the United States Central Intelligence Agency to perform electronic surveillance and cyber warfare. The files, dated from 2013–2016, include details on the agency's software capabilities, such as the ability to compromise cars, smart TVs, web browsers, operating systems
Dyn DDOS Attack	Oct 2016	Distributed denial of services	Disruption	It is estimated to have generated more than 40 to 50 times of the normal traffic volume and the expected number of involved botnets during the attack amounts to 100,000
Heartbleed	April 2014	Known vulnerability And buffer overflow	Data Theft	Infected vulnerable OpenSSL instance for TLS. It results from improper input validation (due to a missing bound check) in the implementation of the TLS heartbeat extension, thus

				the bug's name derives from "heartbeat”
29+ Axis bank accounts hack in India	2013	Phishing/Spear phishing	Financial	30 lac rupees withdrawn. Money withdraw in Euro from Greece 30 account Mumbai police
Snowden Leaks	2013	Data leakage	Disclose data	Reports in the international media have revealed operational details about the United States National Security Agency and its international partners' global surveillance of foreign nationals and U.S. citizens.
Flame, sky Wipe	May 28, 2012		Cyber Espionage	Middle east countries that run on Microsoft windows as their OS. Affected 1000 machine from different institutes. It also recorded audio, including Skype conversation, keyboard activity, screenshots, and network traffic
Attacking a Car	2011	Relay Attack	Financial	300 BMW cars stolen
Sony PlayStation Attack	2011	Phishing/Spear phishing	Financial	77 million of PlayStation Network and Sony Online Entertainment accounts, including credit and debit card information users were stolen. Estimated damage at $1 to $2 billion dollars;
Citigroup	2011	Phishing/Spear phishing	Financial	In 2011, over 200,000 customer information from contact details to account numbers were compromised, which resulted in $2.7 million loss for the company.
Sony PlayStation Attack	2011	Phishing/Spear phishing	Financial	77 million of PlayStation Network and Sony Online Entertainment accounts, including credit and debit card information users were stolen. Estimated damage at $1 to $2 billion dollars;
Citigroup	2011	Phishing/Spear phishing	Financial	In 2011, over 200,000 customer information from contact details to account numbers were compromised, which resulted in $2.7 million loss for the company.
Canadian Government Hacking	February 2011		Data theft	China infiltrate three departments and transmitted classified information back to themselves. Canada eventually cut off internet access of compromised department
WikiLeaks	2010	Exfiltration on CDs	Disclose data	Publish all secrets of US
Stuxnet	June 2010	Worm	Disruption/damage	infected over 60,000 computers
Operation Aurora	mid-2009 to	Advance		Attack originated from China on

	December 2009	persistent threat		Yahoo and others
July 2009 Cyber Attacks	2009	DDOS	financial	numbers of hijacked computers: 50,000 from the Symantec's Security Technology Response Group 20,000 from the National Intelligence Service of South Korea 166,000 from Vietnamese computer security
Operation Buckshot Yankee	2008	Thumb drives	Data Theft	A variant of a three-year-old relatively benign worm began infecting U.S. military networks via thumb drives.
Heart Land payment system	2008	Phishing	Financial	Phishing out over 100 million individual card numbers, costing Heartland more than $140 million dollars in damages
Melissa virus	March 26, 1999		Automatically send mails on first 50 outlook contacts	Targeted MS office word document. This attack costs $80 million

Table. 1 describes the major cyber-attacks that are being faced by the various countries' computing world. The details of the attacks along with the name, year, exploited techniques, motives behind and impact is illustrated in the table chronologically. It is being seen that in the early computing enhancement era, the attacks being reported were in 1999 and the latest being in April, the current year. Similarly, it is also seen that previously the motives behind attacks were data or financial theft, but today more attacks are being done to disrupt/ damage the information. The resulted attacks have affected the individuals, servers, and others sensitive information resources equally. The information regarding these attacks is taken from the online source[1].

VI. Analysis

Analyzing the above data for motivations behind attacks and Techniques used for attacks, following is the ratio of motivations and techniques being pictorially represented in the pie charts. Seeing the chart in Fig. 1, it can be clearly seen that the ***Financial Theft*** and intrusion is the main motivation behind cyber-attacks estimating about 43%. As far as Attacks techniques are being considered; it is the ***Phishing/ Spear Phishing*** technique that is used almost 32% to initiate the cyber-attacks from 1999-2019.

[1] https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

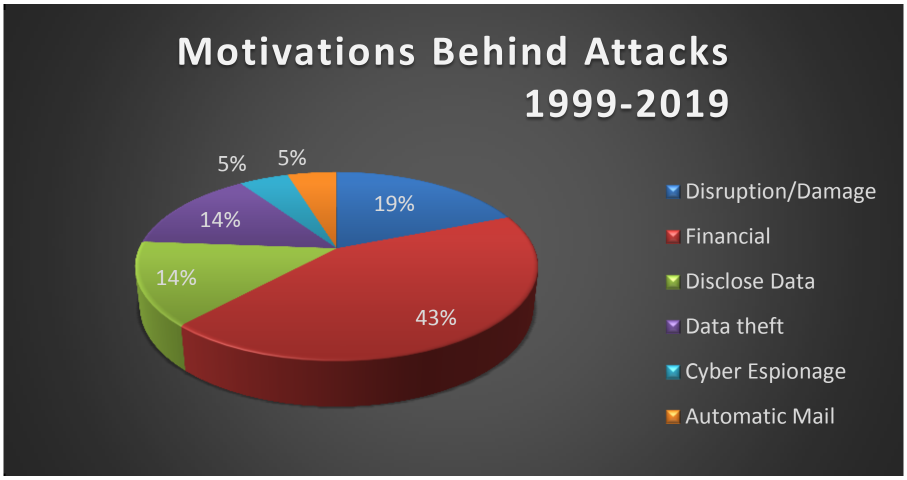

Fig.1. Analysis of Cyber Attacks Motivation (1999-2019)

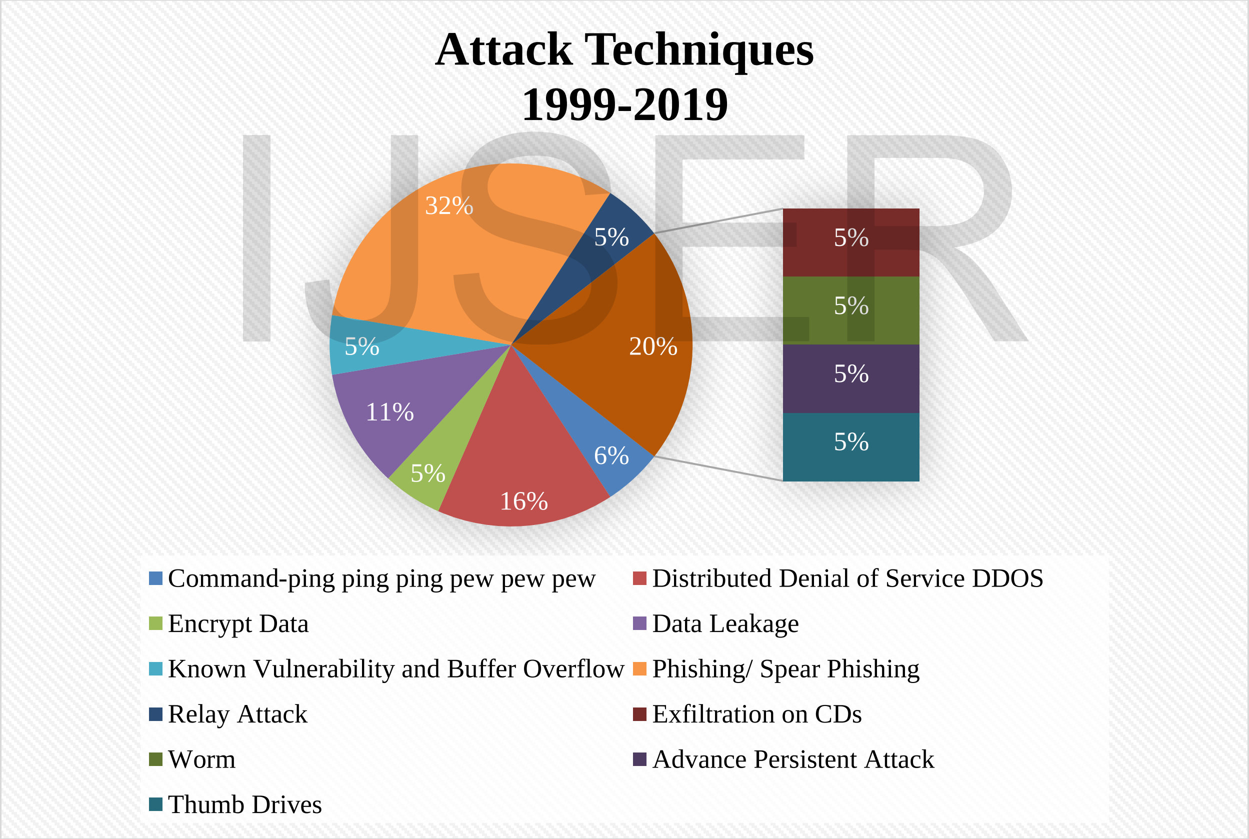

Fig. 1. Analysis of Attacking Techniques (1999-2019)

VII. PRECAUTIONARY MESAURES:

Protecting your vital data and information and staying safe from cyber-attacks is not an easy task. Organizations needs to employ some preventive measures to keep their system safe form possible threats. Following precautionary measures can be employed for system safety and integrity:

1) *Awareness:* Special awareness session must be conducted for the employees and stakeholders helping them to understand the need and importance of data fortification and employed security tools and techniques. Distributing flyers and hanging posters can also aid this process.
2) *Strong Passwords:* New tools have been introduced that helps to create two factor verification systems to authenticate a user access. Practice having strong and unique passwords complimenting them with two-factor, this would sturdily improve the authentication process.
3) *Employing modern tool:* Capitalize modern cybersecurity tools like firewall, antivirus software, and other security tools that routinely scan threats. Install and keep them updated for better protection.
4) *Backup:* Implement strong and routinely backup plan. It gives protection against ransomware attacks.
5) *Encryption:* Data must be encrypted before transmission. This keeps confidential files safe even after theft.
6) *Periodic Audits:* Make network and data security your priority. Evaluate and organize type of data transactions and required security protocols for its protection. Perform periodic security audits to keep your system safe.
7) *Try Hacking yourself:* Occasionally try hacking your own systems. This will help you detect the vulnerabilities and loopholes in the system. So, you can rectify them before someone else find and exploit them.

VIII. CONCLUSION

Cybersecurity is all about being up to date about the possible threats instead of handling them later. Over the past few years, the risk and adversity of cyber-attacks have evidently grown. In recent years, digital world has witnessed the most dreadful cases of cybercrimes related to cryptojacking, flaws in microchips, enormous data breaches and many others. In this era of digital revolution and globalization, cybercriminals are continually trying to find new exploits and show up with innovative plans to deceive and harm organizations. These criminals hugely take advantage of those individuals and companies who pay less attention to their security needs. Considering this fact, organizations should be aware of vulnerabilities in their system and novel cybersecurity threats that are being used by. Employ all the necessary check and security protocols to keep your system and data safe. Businesses need not to focus only on avoidance and preventive measures but also establish tolerance protocols, so that in case of attack its well know how to handle the situation and protect the underlying data.

REFERENCES:

[1]. Europol, “Internet organized crime threat assessment,” The Hague, 2016.

[2]. Juniper Research, “The future of cybercrime & security: Financial & corporate threats & mitigation 2015-2020,” Hampshire, United Kingdom, 2015. [Online].

[3]. E. K. MacLean, “Joseph e. davies: The wisconsin idea and the origins of the federal trade commission,” *The Journal of the Gilded Age and Progressive Era*, vol. 6, no. 03, pp. 249–284,2007

[4]. P. Paganini, “The rise of cyber weapons and relative impact on cyberspace,” *InfoSec Institute, Elmwood Park, Illinois¡ http://dx. doi. Org/resources. InfoSec institute. Com/the-rise-of cyber-weapons-and-relative-impact-on-cyber space*, 2012.

[4] T. Halevi, J. Lewis, and N. Memon, “Phishing, Personality Traits and Facebook,” *arXiv Prepr. arXiv1301.7643*. 2013.

[5] I. Alseadoon, M. F. I. Othman, and T. Chan, “What Is the Influence of Users’ Characteristics on Their Ability to Detect Phishing Emails?” in *Advanced Computer and Communication Engineering Technology*, Springer International Publishing, 2015, pp. 949–962.

[7]. Kharraz A., Robertson W., Balzarotti D., Bilge L., Kirda E.,”Cutting the Gordian knot: A Look under the Hood of Ransomware Attacks””. In: Almgren M., Gulisano V., Maggi F. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA. Lecture Notes in Computer Science, vol 9148. Springer, Cham, 2015.

[8]. Hiran V. Nath and Babu M. Mehtre, “Static Malware Analysis Using Machine Learning Methods”,International Conference on Security in Computer Networks and Distributed Systems, 2014.

[9]. MattiasWeckstén, Jan Frick, Andreas Sjöström, Eric Järpe, “A novel method for recovery from Crypto Ransomware infections”, Computer and Communications (ICCC), 2016 2nd IEEE International Conference.

[10]. Savita Mohurle and Manisha Patil, “A brief study of Wannacry Threat: Ransomware Attack 2017”, International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May-June 2017.