IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 02, 2022

Analysis of Recent Malware, Mitigation methods and Future Research

Dr C Ramakristanaiah, Associate Professor Dept of CSE, KLEF, Vaddeswaram
K.chandrasekhar,Assistant Professor(Adhoc),CSE Department,JNTUACEP
P Namratha, Associate Professor Dept of CSE GATES institute of Technology
K.Bala Chandra Reddy,Assistant Professor (Adhoc),CSE Department,JNTUACEP

Abstract: In recent days, malwares known as malicious software, are advanced, and systematically developed to attack the target. Most of such advanced malwares are highly persistent and capable of escaping from the security systems. Malware affects the user's computer system or mobile devices by exploiting the system's vulnerabilities. It is the major threat to the security of information in the computer systems. Some of the types of malware that are most commonly used are viruses, worms, Trojans, etc. Nowadays, there is a widespread use of malware which allows intruder to get sensitive information like bank details, contact information, which is a serious threat in the world. Most of the malwares are spread through internet because of its frequent use which can destroy large information in any system. Malwares from their early designs which were just for propagation have now developed into more advanced form, stealing sensitive and private information. This work focuses on analyzing the recent malware attacks and threats which had a huge impact on the cyber world . This work is concluded by with malware mitigation strategies which can help us protect our system's information and future research directions which are emerged to protect from cyber attacks.
Keywords: Malware life cycle, Analysis, Recent malwares, Emotet, wannacry.

I. Introduction:

Everyday new malware are coming over the internet into many personal computers in various forms such as Trojan horses, spyware etc., The aim of malware always would be precious information, ransom demand, taking control away from the owner etc., Usually malware codes are completely different fromone malware to another and are very difficult to understand and analyze. The need of analysis and understanding the malware in a precise way to find its functionalities and signatures and the way they can affect the computer has been raised since they are more effective in internet era. In other way, malware analysis most emerging need for all internet applications. With the malware analysis, the applications will be able to identify malware entry into system and/or will be able to prevent such miscellaneous codes. Prevention of such code is emerging need in current days as thousands of internet applications are being used, and many of them are used to have most sensitive data. Every day more than half of the world's population is connecting to the internet[1]. To provide a safe environment for web applications to run on internet, quick response should be given on any malware on its arrival or on smell.

Everyday new malware and zero day attacks are mushrooming. Due to pandemic COVID-19 and lockdown in the world, online users are increased exponentially. Of course, more sensitive data has been shared and being shared over un-trusted channels. Pandemic forced organization have unprotected data and failed in practicing cyber security policies.

Surprising fact is 95% of cyber Attacks are happening due to human error. Only 5% of companies have protected data with them. 86% security attacks were financially motivated and 10% are towards other reasons[2]. This paper presents most recent malware attacks, targets and their motivations. This paper also presents countermeasures are to be taken and provided some research directions. The rest of the paper is organized as follows. The section II Presents Malware propagation and life cycle. Section III Presents various categories of malware. Section IV Presents most recent malware attacks and targets and its impact followed Conclusion and Future Work.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 02, 2022

II. Malware propagation and life cycle

How malware enters into a computer:

Broadly discussing, there are six most commonly used ways that a malware can enter into a system. i) Compromised nodes: Systems which have minor or major defects in its software/hardware but still working are referred to as compromised nodes or systems. These systems are more vulnerable to the malware to enter into any computer. ii)Back Doors: If the user click on any link or network or any other application intentionally or unintentionally, the malware penetrate into the system. iii) Downloads: A Malware can enter upon download a file from unknown source. iv) Homogeneity: Homogeneous computers running same network and most vulnerable to the worm attacks. Since the worms can spread on homogeneous networked computers, all computers would be in threat of worms. v) Escalation of privileges: If an intruder successfully escalates the privileges of the network and entering by, the entire network or system get hijacked by the malware. vi) Malware Packages: Malware packages are formed by combining various properties of various malware upon entering into systems. These malware are very hard to detect and prevent.

There are two methods for malware analysis. One is static analysis and another one is dynamic analysis. Earlier, Static analysis had been deployed widely for malware analysis. In this, malware program is analyzed without running it on computer. This analysis is based on statistical features and data flow of the code. Static analysis is also known as signature based analysis. In dynamic analysis of the malware, the malware program will be run on the virtual machine environment, to monitor the runtime behavior of the malware. This type of analysis is known as behavior based analysis[3]. The static analysis is not suitable for advanced malware techniques, such as encrypted malware code, inserting garbage code, transposition of code, permutation of the code [4]. In view of this, the need of using dynamic malware analysis is insensitive to the mutations of the malware. The dynamic malware analysis has been carried out in various directions.

The authors in [5] had used APIs and features extracted dynamically to detect malwares. The combination of temporal features and spatial features of runtime APIs are considered in this work. In work [6], the dependency graphs are used to find the behavior malware. In the paper [7], register content based behavior, behavior of binary of malware etc.., are analyzed thoroughly. Their analysis concludes that dynamic analysis are having limitations. Behavioral analysis may not sufficient to observe the entire functionality of the malware because it is resource constrained, large volume of malware. In spite of its limitations, the dynamic analysis are out performed well to analyze the malware in current day technology.

Life Cycle of Malware

As of [8], there are 10,217 families of malware and 340246 entries in its database [9]. They have been used as sources of analysis by many researchers. All the malware specimens stated in above two sources have almost common life cycle [10].

1. Creation: Creation of malware needs proficient knowledge in programming and computers. However, Almost all malware are straight forward in its duties and designed on the basis of modularity and are capable of generating new strains.

2. Entry and Activation: A Malware can be entered into any system in any one of the activity of the user like opening a link or downloading or clicking etc.,. Once it enters into computers, malware will be activated by its own and replicated thousands of times to create new strains.

IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 02, 2022

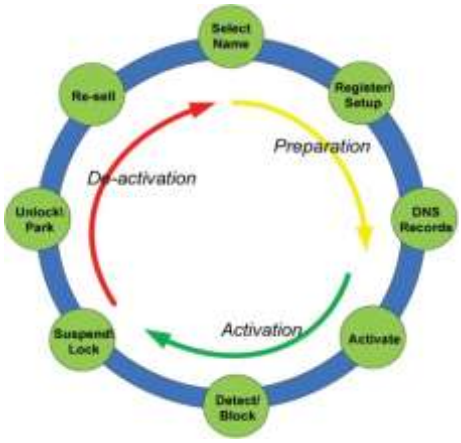

Figure 1: Life Cycle of Malware

3. Undetected, Self Resistant and Deactivation: Upon replication, it may propagate on its own and executes its functionality to accomplish the task. Some malware get deactivated once its task is done. Now a day's malware are not getting deactivated on its work done. They sit in the system and can infect other components of the system. Malware always try to be undetectable and can exhibit diverse behavior in its life cycle. Sometimes it looks no harm, sometimes extreme danger. The figure 1 shows the life cycle of malware.

III. Categories of Malware

Based on its behavior, malware are categorized into many groups. The table 1 shows the list of the categories.

S.No	Name	Description
1.	Trojan	A Program contains malware. It looks good software with hidden malware features
2.	Backdoor	A malware enters into system indirectly on user activity.
3.	File Infector	A malware attached to the executable files.
4.	Worm	A malicious program stays o network components and can replicate and propagate on its own.
5.	JavaScript	JavaScript Code in malware and can affect other software written in JavaScript
6.	VB Script	VB Script Code in malware and can affect other software written in VB Script
7.	HTML Script	Written in Scripting Languages supported by Web and Propagated using web.
8.	Macro	Malware developed in macro programming language and propagated with the help of other files.
9.	Boot virus	Loaded into Boot Records of the system. Execute when system gets on.
10.	Batch Virus	A malicious program replicating through other infected files ad boot records.
11.	Others	Includes mobile malicious codes, zero day attacks, attack tools.

The major malware type is Trojan horse which is widely being used by attackers. Trojan horse attack happens in four phases. The first phase is information Gathering. In this phase , the intruders collect the information about the protocols used by user to communicate with outside world. This information can be used to establish a two way communication channel between the server and intruder. This connection aims get the information to write or develop the malicious code. The second phase is creating to Reverse Trojan. The information get in the previous phase will be used here to write Trojan binary. This Binary will be inserted into genuine software, on inserting malicious code into software program, intruder can get control over the system or software. Finding various ways to attack is third phase of the attack. In this phase attack will be launched on the computer of the user by using any fake mail, website link or any other techniques. In final phase of the attack the Trojan which is

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 02, 2022

entered into the system can send the data of the user to any unauthorized destination , can make compromise other components of the system and can perform the communications with intruders choice.

Trojans are divided into two types.

i)Software Trojans

ii) Hardware Trojans

Software Trojans are malicious programs that can gain the complete access of the operating system and can take away the information or can damage the computer. Most of the Trojan programs are identified and be removed by the Anti Trojan programs [11]. The Hardware Trojans are injected into integrated circuit (IC) when it is fabricated. Hardware Trojans are impossible to delete from IC once it is fabricated. It is extremely difficult to provide remedy to such Trojans. Though, Research is continuing in this field.

Table shows brief description of Trojans

	Activation	Propagation	Elimination
Software Trojan	Can be activated on execution of the software in which Trojan Resides	It can be propagated on user action on the software in which Trojan sits.	Can be eliminated by deploying anti Trojan Program.
Hardware	Can be activated on operation of IC circuit since it resides in IC.	Can be inserted into chip by un-trusted chip design or fabrication organizations.	Cannot be eliminated from IC once it is fabricated.

Table 1: Description of Trojans

All Trojans may not be harm but security threat for sure. The general proverb “precaution is better than cure” comfortably fit to protect from Trojans. Precaution is the best option than eliminating the Trojan after it enters into system. As a prevention measure the user should not open or download any software or program from unknown source. Another prevention measure is update operating system timely. It is very important in case of Microsoft windows operating system.

The most dangerous Trojan in last five years in Emotet. Emotet was found in the year 2014 which had been used for stealing information across the devices particularly financial data [12]. Emotet also worked as carrier for other malware programs. Emotet was top threat for antivirus researchers in the year 2018 [13].

Backdoor Malware:

This is another type of Trojan. Backdoor attacks are top 4 attacks in last five years. Backdoors deploys at door step of the user machine something known as root kit. It is malware package designed to Escape from detection by any antivirus program or operating system.

Backdoors are of two types. One is Built in Backdoor and another one is proprietary backdoor. Built in Backdoors can be inserted into software where as proprietary Backdoors are can get entire control of the system and can act as owner of it. Backdoors are also used by investigation department as surveillance factor confirmed by united states of America’s National security Agency(NSA) in the year 2013.

Open source code Repositories had been used as carrier for backdoor attacks. Usually these repositories are supposed to have code for any problem. That code may be used by others. Intruders could place malicious code into repository which can be downloaded by innocent needy.

Such an attack in happened in the year 2018 and it was named as crypto mining malware.

File infectors:

File infector Malware can copy its code into executable files like .exe and .com etc. These file infectors spread through replication on its arrival at computer and can damage host software programs as well. Some file infectors can overwrite host files also. Some file infectors are usually destructive range from formatting hard drive to crashing Hardware component.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 02, 2022

Worms:

Worm malware usually resides in network components and steal valuable information from the network. Worm attacks can be deployed in following steps.

Step 1:

Worm program find the system to attack on the network with network credentials like IP address.

Step 2:

A copy of the worm will be created by its own and can be propagated towards that system on the network.

Step 3:

Worm can be executed on that machine if it was undetected by that computer.

Interoperable systems are more vulnerable to worm attack. All interoperable systems accepts the programs of the same network and executes them quickly. This would have become Loop hole for the attackers.

Creation of Network firewall could become a solution for worms, unfortunately not yet developed such a firewall that can stop all worms. Off course it is not guaranteed by the research community that a firewall can prevent all worms.

Scripting Attacks Vulnerable to SQL Insertion Attacks. Scripting Attacks can be Launched in 2 Steps.

1) Malicious Script will get Execute in user's browser after injecting payload into it.
2) User must open the webpage or web Browser. If attack is identified by Anti Virus software the attacker may use social Engineering or punishing to Escape from detection.

The following is scripting attacks code to steal cookie information on web browser.

```
<script>
window.location="http://evil.com/?cookie=" +
 document.cookie
</script>
```

Macro virus:

A malware which infects an application and sequence of movements to be caused when it is opened or Executed. Most of the surveys are research works have already clarified that Macros are surprises but are harmless.

Batch Virus, Boot Virus:

The Virus can affect Boot sector of the Hard drive. These Virus can be inserted into Boot sector of the hard drive area by using Dos attacks. The most widely deployed Boot sector files are .exe, .com, .bat etc. These are proved to Dos attacks. Drastic changes occurs in the behavior of the loading of OS without knowing details like signature of the virus etc.

IV. Recent Malware Attacks

The most stunning and sensational cyber attack happened in the last decade is wannacry[14] cyber attack. It was a worm type of attack. Upon entering into computer, all the data of the computer was encrypted. Upon paying some ransom, those files were decrypted. There were around 2 lakhs victims across 150 countries over the world. Due to nature of this attack some health organizations, manufacturing companies, telecom companies closed offices temporarily. This virus could cause $8 billion economic costs around the world.

Notpetya another Ransomware attack happened in the year 2017 in Ukraine. This is a backdoor attack came into picture as an update of app called medoc.

Surprisingly, these back doors were deployed by some organizations in their products and components. NASA of USA had confirmed its back door malware existence. Bloomberg story is another incident happened which was connection of some organization in US and china command and control.

Some Organization had refused to insert backdoor code into products even requests comes from investigation and justice departments of US after one terrorist attack in US.

As per Emsis of IS 2020 research papers US government, health care and educational institutions expended 7.5 Billion dollars in the year 2019 itself. Brookfield attack, Costs limited, colarado city of Lafayette costs $40,000, university of Utah costs $457059, university of California, Michigan state university , cognizant a fortune 500 company,

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 02, 2022

Travelex are most significant attacks happened in the year 2020. In [15] various malwares or bugs found in world's most famous organizations products or applications like Google , Tiktok , Microsoft etc.

Samsam 2015 malware attacks by escaping from privileges. It runs a gambit by en-cashing the vulnerabilities in IIS Server.

RYUK 2018 and 2019 attack disabled the windows system restore option on victims computer. It was very difficult to retrieve information back.

PURELOCKER 2019 can be installed on machines which are compromised and encrypt the data. The IBM and intezer organizations had not disclosed more information on purelocker 2019

ZEPPELIN is also known as vegaslocker. Researchers and experts trusted that this malware is particularly developed to do not attack machines running in Russia, Berkeley or khazhakstan.

Zeppeline can be spread in many ways such as .exe or a power shell loader to a compromised computers.

REVIL/Sodunokibi:

This malware also had been prevented by Russian and Syria also. This attack used bad holes in oracle web logic servers or some VPN's to propagate.

Kaspersky Laboratory had released a report on number of users being affected from the malware. The 40% of Internet connected systems are being attacked by malware in many forms in a year.

The average amount of Ransom paid to attackers in 2020 is $111,605 which 30% higher than paid in 2019 (fintech news). As per Cisco reports about 60% of malware are associated with spam mails and 94% of malware delivered by general Emails.

Can Cyber World prevent any new malware?

Absolutely No. Number of internet users is huge. Scope for cyber attacks is huge. Cyber security Experts are limited. The knowledge of attackers would be unpredictable. An 17 year old boy deployed cyber attacks stated in literature. Unfortunately, organizations are unable to practice security policies strictly which would become weapons to the attackers.

V. Conclusion and Future Work

As attackers are keep on attacking the cyber world, it should be ready to accept challenges of attackers and should follow some procedures. Every organization should have an immediate response team for any cyber attack. That team must be expertise in many aspects including zero day attacks. Maintaining backups of Multiple copies in different sources is most important to prevent collapse of organization. Organizations should have updated antivirus software to stop various attacks. Every organization must follow security privileges issued by local governments. System access must be restricted to limited users and applications underlying to security policies and configurations.

Prominent reserarch direction in malware prevention is developing system patches for bugs. One cannot find when bug will be detected once bug Encountered that system should be patched. This development of patch and identifying bugs should be a continuous research.

There is an emerging need of next generation firewalls to be developed to make suitable for any security threat. The research must be carried in this direction at least to Enhance the features of existing firewalls. Since all firewalls proprietary firewalls , organization research is being carried on it.

To ensure and provide effective prevention of malware, malware analysis such as malicious signature, malicious binary, target etc should be done effectively. This is most significant research direction.

References:

[1]. Internet usage worldwide – statistics & facts Published by J. Clement, Oct 26, 2020.

[2]. Cyber Statistics websites.

[3]. Rabek, Jesse C., et al. "Detection of injected, dynamically generated, and

obfuscated malicious code." Proceedings of the 2003 ACM workshop on Rapid malcode. 2003.

[4]. Brand, Murray. (2007). Forensic Analysis Avoidance Techniques of Malware. ECU Publications.

[5]. Siddiqui, Muazzam & Wang, Morgan & Lee, Joohan. (2008). Data mining methods for malware detection using instruction sequences. Artificial Intelligence and Applications. 358-363.

[6]. Karbalaie, F. et al. "Semantic Malware Detection by Deploying Graph Mining." (2012).

[7]. Galal, H.S., Mahdy, Y.B. & Atiea, M.A. Behavior-based features model for malware detection. J Comput Virol Hack Tech 12, 59–67 (2016). https://doi.org/10.1007/s11416-015-0244-0

[8]. Symantec 2009 Annual Report.

[9]. Trend Micro 2011 Threat Predictions.

[10].Chen, Zhongqiang & Roussopoulos, Mema & Liang, Zhanyan & Zhang, Yuan & Chen, Zhongrong & Delis, Alex. (2012). Malware characteristics and threats on the internet ecosystem. Journal of Systems and Software. 85. 1650–1672. 10.1016/j.jss.2012.02.015.

[11]. Trojan Hunter Help File.

[12]. National Cyber Awareness System Alerts Emotet Malware, Alert (AA20-280A), Emotet Malware

[13]. 2019 State of Malware powered by malware labs.

[14]. Mohurle, Savita, and Manisha Patil. "A brief study of wannacry threat: Ransomware attack 2017." International Journal of Advanced Research in Computer Science 8.5 (2017): 1938-1940.

[15]. cyware.com