ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 3, May2012

"Impact of Malware in Cyber world"

"A Comparatively Study"

Pranay chauhan, Nihal gupta, Brajesh chaturvedi
pranaychauhan1985@gmail.com,

Abstract

The boom in the cyber world can be seen as that Various technologies has been developed and these technology has made a cyber life advanced the role of cyber is increasing day by day which has made easy the accessing of various commerce application. These technologies were quite effective but as the role of cyber technology is increasing similarly the role of malicious program is also increased. Various malicious code get Introduced day by day some of these code required a host program to execute and some of these execute independtly. The above paper would mainly focus over these different malicious code and different vulnerability and how these can be overcome.

Keywords*:* - Malware, Vulnerability, Attacks, tools

1. Introduction

The role of cyber world in human life can be seen easily. Internet and mobile are two application play an important role in our daily life the role of internet can be seen that at July 1993 they were around total 350 domains were registered. But today Internet grew by a million domain names in ending the quarter with a base of more than 200 million domain name registrations across all of the Top-Level Domains [1]. So as the cyber world is enhancing it has made things easier, the advantage of ecommerce application over traditional application is quite effective, but as the technology is enhancing some other factor were also Enhanced such as the malicious program, different vulnerability, different attacks over the cyber world they have made things unsafe and risky to use figure 1 shows the main categories of malicious code the malicious program can be easily divided into two forms such as those who required a host program and those who work independently

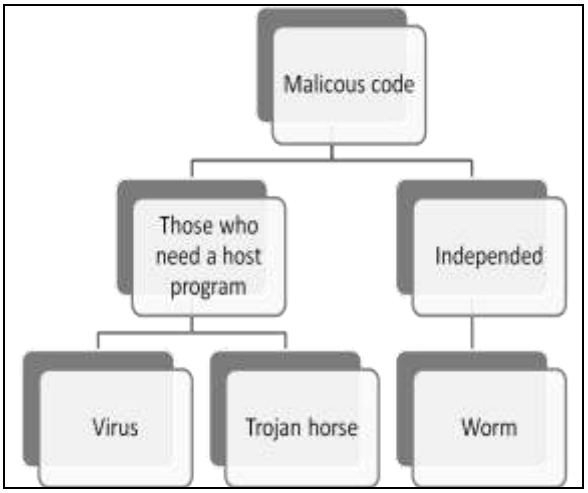

Figure 1: Categories of Common Malicious code

as the Virus is the main malicious code which mainly affects the application they always required a host program to execute and as they are different categories in which these virus were divided such as stealth virus parasitic virus , boot sector virus , memory resident virus , poly morphic virus these are certain categories In which these virus were divided some other virus

perform functioning in different application such as mailing application get affected by the email virus which mainly spread from email to email various action perform by these virus they modify data, destroy data, change content ,alter data, insert data, delete data etc these are the different action perform by these email virus. The development of Virus can been seen that first virus was created in 1980 and after that it has been increasing rapidly the figure shows the development of virus from 1980 these are some common virus which were quite harmful for the cyber world

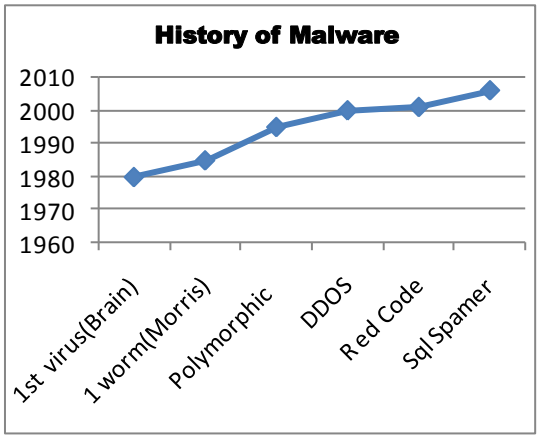

Figure 2: History of Malware

Viruses mainly perform working in four different phases figure 3 shows the working phases of virus

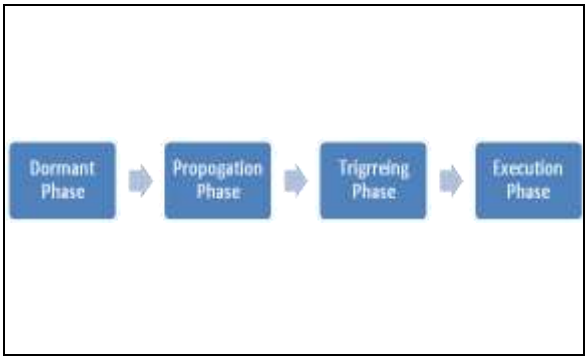

Figure 3: Working phases of virus

The different phase in which virus mainly performs the execution they start affecting the data. Other malicious code which need an host program is the Trojan horse which also need an host program to execute the Trojan horse mainly come from the internet these malicious code always required an host program to execute while some other malicious code such as Trap door, logic bomb which also required an host program to execute in the system. In case of logic bomb it build logically it mainly perform the action at particular time period or at particular condition i.e. when two or more condition were meet then it mainly perform the action. other malicious code which work independlty are Worm and Zombie ,Worm is also replicate program which mainly replicate from machine to machine they also make their copy and start replicating while in case of Zombie they used Botnet server by which they consume bandwidth of system various flooding has been done over the system by which they stop working it uses the D.O.S. attack in which mainly large amount of packet are sent over the server by which server stop working denial of service attack is an type of active attack in which flooding is done by TCP flood. UDP flood, ICMP flood, and HTTP GET flood these different types of flooding strategies by which attack is perform denial of service can be prevent by firewall but DDOS can be prevent by firewall in this again large amount of packet are sent.

2. Role of Vulnerability:

The other categories by which an cyber world can be get affected is the different vulnerability these vulnerability are the mainly loop hole in the system an attacker mainly sees these different

vulnerabilty and they manily make use of these vulnerability [2]. The windows based operating system are most vulnerable because they are totally GUI based operating sytsem and Intruder manily see the loop hole in the system and the mainly make use of them figure 4 shows the different common vulnerability

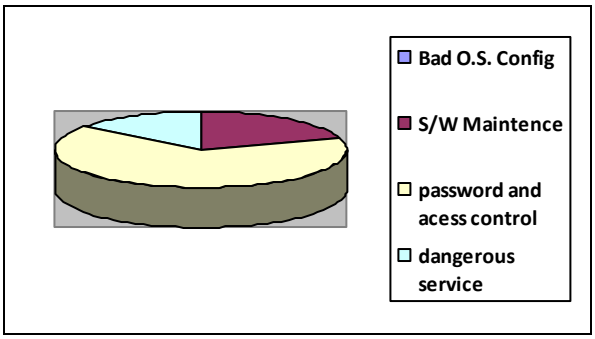

Figure 4: Different vulnerability in a system

These are the common vulnerability which is found in the system proper software maintence is the main vulnerability which can destroy the system these are the main loop hole in the system. Network Security assessment methodology can be in four level reconnaissance, enumeration, assessment, exploitation [2]. These are different level by which assessment can be perform first the reconnaissance which can be done by using various tools such as who is, dig, nslookup, tracert and the enumeration can be perform by using the nmap, nessus tools the various other tools such as TCP port scanning, UDP port scanning, ICMP Probing by these enumeration is perform and at last the exploitation can be done by using the metaspolit framework tool [2]. In which the vulnerability can be in used

Figure 5: Network security assessment methodology

3. Role of Malicious code in cyber worlds

The role of cyber world is enhancing regularly first internet application ecommerce [3]. was used for the purpose of selling and buying the ecommerce play an important role in the development of internet but the malicious code and different mode of attacks has easily targeted these application such as Trojan can easily destroy the privacy of data user carries it passwords and personal information for authentication but the Trojan can easily b used for the purpose of sniffing and other categories of malicious program such as Botnet and Zombie they also used for destroying the security of data other categories of malicious is Zeus which mainly uses the Botnet and the Zeus mainly perform attack over the financial data it mainly steel the personal information of data and make the data more vulnerable and other various malicious software were there which also act a harmful application for the internet [3]. then certain enhancement is done over the ecommerce application and to make it more feasible and comfortable for the user to used and easy to reach various mobile application were developed the role of M-Commerce increase but they are certain condition where these application were although not secure and privacy can't be maintain M commerce application can be easily use

from any location if the network exit and to make it more comfortable for user the various development has been done [4]. They are certain cases were M - commerce has been targeted. The first malicious worm for mobile devices, Caber, was developed and after that there is increase rate of development of Bot net and malicious codes [5].

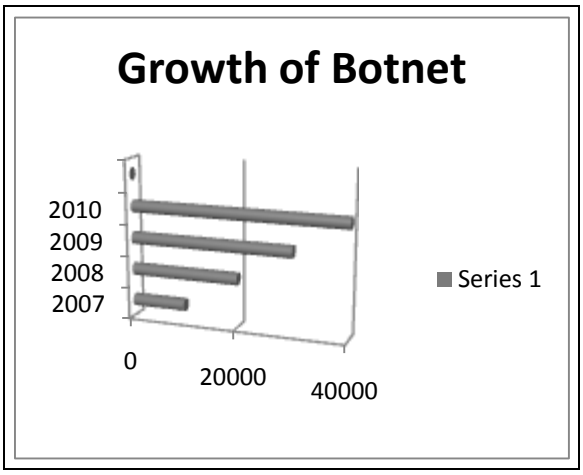

Figure 6: Growth of Botnet Annually [5]

The above figure shows the growth of botnet annually The role of this botnet server is increasing rapidly and they were infecting the M commerce application. Currently the Cloud Computing is an emerging area in the cyber world similarly to internet and mobile application cloud server also get affected by the malicious code and they easily destroy the privacy of data they were various threat to cloud computing such as

- Insecure API and interface
- Malicious insider
- Shared technological issues
- Data loss or leakage
- Account or service hijacking

Out of these various threats the malicious insider is the most common type of threat in the cloud computing server which destroys the privacy of data [6]. In order to provide protection in the cloud computing the concept of Cloud AV were given in these concept mainly the different antivirus engine were combine and then security is provided in the cloud environment two behavior detection engine were also used to prevent against the malicious code[6].

4. Conclusion

The above paper discussed about the role of malicious data in the cyber world different malicious program just destroy the system vulnerability and they are quite harmful for the cyber world different and the malicious just destroy the privacy of data in different application and these application were just struggling against these malicious program. And as various tools were developed in order to provide protection against these threat but these were not good enough to solve this problem of malicious program.

5. References

[1] Top level domain online available http://www.thewhir.com/web-hosting-news/060810_Total_Domain_Name_Registrations_Surpas. Accessed on 15 may2011

[2] Chris_McCabe, "network security assessment" Principles and practice" 3rd edition, Publisher: O'Reilly Media March 2004

[3] Malware spreading countries [Online] available at:http://www.spamfighter.com/News-13363-Kaspersky-Lab-%E2%80%93-China-Hosts-Highest-Malware-Laden-Websites.htm (accessed 29 March)

[4] *"Report on Cyber security: CERT VULNERABILITY NOTES"* CERT Gov. of India http://www.cert-in.org.in/
*(*Accessed 18 May)

[5]. Security report online available at: "http://www.symantec.com/press/2004/n040920b.html Accessed on 16 May2011

[6]. Cloud security and various tools to remove the malicious code online available at: "http://www.h-online.com/newssticker\new\item\update"accessed on 16 may2011

First Author

Pranay Chauhan
M.E. Student, Institute of Engineering and Technology,Davv
Indore, M. P., India,
Ph. +91 9754143398

Biography: Pranay Chauhan has receivable.(Bachelor of Engineering)Degree in Information Technology Engineering from Rishiraj Institute of Technology, Indore ,M.P.,India in2007. He has 4.years of teaching experience. His subjects of Interest include, Computer Networking, Biometric system, Security assessment, Securing E commerce Operating system, Network Management, Wireless network, Network security, he is M.E.(Information Technology) , from IET-Davv Indore M.P, India. He has published several researches Papers in National/International Conferences. .His research areas are Secure Email Application, Email authentication, Ecommerce role in wireless Network, Wireless network. Currently he is working as a Assistant Professor in Information Technology Dept. At SWAMI VIVEKANAND COLLEGE OF ENGINEERING, INDORE M.P.