Taxonomy of Malware: Virus, Worms and Trojan

Jasmeet Kaur
Assistant Professor, Computer Science, Innocent Hearts Group of Institutions, Jalandhar, India

Received: January 16, 2019 Accepted: February 24, 2019

ABSTRACT: *A computer Malware is a code that can be placed in a remote computer and can reproduce itself to other programs in the computer and other computers in the network, when executed. This paper aspires to discuss the modern situation of Malware, propose theoretically about latest categories of computer viruses, project potential in computer viruses and discover new capabilities in computer virus defense.*

Key Words: *Current viruses, new types of viruses, immune system, Malware threats etc.*

I. INTRODUCTION

The word 'malware' is an abbreviation of the term 'malicious software'. This includes such program code classes as computer viruses, computer worms, and Trojan horses. This list may not be exclusive [1]. Computer virus is a term on which there are no exact definitions, but computer anti-virus researchers have been generally known regarding every kind of program cipher and software. A program (set of instructions) that is designed can be deemed either as precarious or precious, depending on the use. Virus can lift user data, remove or change files & documents, records keystrokes & web sessions of a client. It can also lift or smash up hard disk space, and slowdown CPU processing.

II. TAXONOMY OF MALWARE:

<table>
<tr><th>S. No</th><th>Taxonomy of Malware</th><th colspan="2">Description</th></tr>
<tr><td rowspan="6">1</td><td rowspan="6"><b>Computer virus</b></td><td colspan="2">Refers to a program code which has a capacity to replicate recursively by itself. Computer viruses may include operations, which are typical for Trojan horses and malicious toolkits, but this does not make such viruses' Trojan horses or malicious toolkits [1]. A file virus connects itself to a file, which is typically an executable application. Generally, file viruses don't transmit infected files to data files. But, data files can enclose fixed executable code such as macros, which can be demoralized by computer virus or Trojan horse authors. Text files like postscript files, batch files, and source codes that hold commands which can be compiled or interpreted by another program are possible targets for malware [2][3].</td></tr>
<tr><td><b>Boot Sector Virus</b></td><td>A Personal Computer is infected with a boot sector virus if it is booted normally or by accidentally from an infected hard disk in hard disk drive. Boot sector virus could not usually spread across a network.</td></tr>
<tr><td><b>File Virus</b></td><td>When the infected file is opened or used the virus may overwrite the file and grounds everlasting smash up to the content of the overwritten file. These viruses target a large series of operating systems, like Macintosh, UNIX, DOS, and Windows. file virus could spread across a network</td></tr>
<tr><td><b>Multipartite virus</b></td><td>A multipartite virus infects both boot sectors and file sector. An infected file is often used to infect the boot sector; and could spread across a network.</td></tr>
<tr><td><b>Macro Virus</b></td><td>Macro viruses are macros which call it-self again and again. If a user works on a document that contains a macro virus and unsuspectingly executes this macro virus, then, it can copy itself into that application's set up files. If the infected PC is on a network, the infection is very much possible to extend quickly to other computers on the network.</td></tr>
<tr><td><b>E-Mail Worm</b></td><td>Viruses attached to email messages can infect a complete project in affair of minutes; estimate companies millions of dollars annually in lost efficiency and clean-up cost.</td></tr>
<tr><td>2</td><td><b>Computer worm</b></td><td colspan="2">An independent program code (does not have a host program) that has a capacity to replicate itself again and again. Computer worms are a subgroup of computer viruses.</td></tr>
</table>

		Computer worms may include operations which are typical for Trojan horses and malicious toolkits, but this does not make such worms trojan horses or malicious toolkits [4].
3	**Trojan horse**	**A** self-standing program code that performs something useful, while at the same time some kinds of destructive function performed intentionally, unknowingly to the user. The program code may be attached to any part of a systems' program code. Trojan horses may include operations which are typical for malicious toolkits [5].
4	**Adware**	The most common online nuisances are the example of adware. The programs that repeatedly send advertisements to host computers. It includes pop-up ads on Website and in-program advertising that often accompanies "free" software [6].
5	***Spyware***	It searches out on what user doing at computer. It collects data such as user press any keystrokes, browsing habits of the user and even login information of the client. This information is then sent to third parties, usually cyber criminals [6].
6	***Ransomware***	Ransomware attacks on your computer and then important data such as personal documents or photographs are encrypted and on the behalf demands a ransom for their release. If the owner of the data, refuses to pay, the data is deleted [6].

III. CHRONOLOGY OF MALWARE THREATS

In 1949, the idea of a computer virus extends, when early computer scientist John von Neumann wrote a paper on self-reproducing automata that suggests how a computer program could reproduce itself. But Modern Malware is developed for commercial purpose. In this paper, we discuss about the chronology of malware threats [6].

Year	**Developed By**	**Virus Name**	**Description**
The early Years			
1971	Bob Thomas	The Creeper Worm	It was a program which infected DEC PDP-10 computers of TENEX O.S.
1974		Wabbit	It made number of copies of itself again and again that clog the full system. After that the system would crash.
1974/75	John Walker	Non-Malicious Trojans (ANIMAL)	It was developed for UNIVACs. When users sharing tapes this virus spread quickly.
1981	Richard skrenta	EIK Cloner	It was developed for Apple II systems. It infected the Apple DOS 3.3 and after that transfer to other devices by the use of floppy disks.
1983	Frederick Cohen	Dissertation	Computer virus written and distributed over to the internet. Computer viruses were spread because viruses were capable of recall itself.
1986	Two programmers of Pakistan	Brain Virus	They developed code which replaces the executable code in boot sector of floppy disk. It was the first IBM PC virus.
1987	Yale University / Jerusalem	Lehigh/ Jerusalem virus	It infects command.com files and stop there working immediately. / It destroyed all the executable files on a computer that was activated only on Friday (13th).
1988	Robert Morris	Morris Worm	Computers connected to the internet were infected by this virus. It infects DEC VAX and SUN machines.
1991	unknown	Michelangelo Virus	This virus was designed on March 6th (the birthday of Renaissance artist) to remove data from hard drives.
1999	Smith	Melissa Virus	This was the first group-emailed virus; it used address books from infected machines of outlook, and e-mailed automatically to 50 people at a time.
Astonishing Rates of viruses			
2000	Reonel Ramones, Onel de Guzman	ILOVEYOU Worm	This worm damaged around 50 million (approx.) computers. It shut down the email servers of Major corporations and government bodies (the Pentagon and British Parliament).

2001	Jan de Wit	Anna Kournikova	Email spread the virus; contain pictures of the very attractive female tennis player but actually it was a virus.
2003	David Litchfield	SQL Slammer Worm	By using this virus, programmer infected around 75,000 computers. It slows down the worldwide Internet traffic via denial of service.
2004	29A, a hacker group	Cabir Virus	It was the first mobile phone virus.
2005	Unknown	Koobface	It infects Personal Computers after that broadcast to websites (social networking MySpace, Twitter and Facebook). Koobface is the reverse "Facebook".
2008	Unknown	Conficker	It is the combination of configure and flicker. It is just like slammer worm.
Impact of virus between 2010 to present			
2010	Sergey Ulasen	Stuxnet Worm	It is a Windows Trojan, the first worm to attack scada systems.
2011	Hackers in Eastern Europe	Zeus Trojan	By using this virus programmer steal banking information. They did this by taking the keystroke logging and form grabbing.
2013	Unknown	CryptoLocker	This malware encrypt the hard drive (all data), in order to receive the decryption key the developer of virus demand to pay a ransom.
2014	Unknown	BackOff	This virus steals the credit card information on the time of shopping.
2017	Unknown	WannaCry Ransomware	The virus damaged at least 150 countries, including hospitals, banks, telecommunications companies, warehouses, and industries.
2018	Unknown	Bitcoin	This virus was developed to accept the ransom money [7].
2019	Platinum	Titanium	Backdoors are used for securing computer on remote access, or getting access to plaintext in cryptographic systems [8].

IV. NEW TYPES OF MALWARE THREATS IN THE NEAR FUTURE

S.No	Type of Virus	Description
1	Wireless Virus	In new era, wireless communications provides novel probability for hackers, discontented workers, and others to show their proficiency in scattering computer viruses and harmful code. When the procession between mobile phones and personal digital assistants distorts, this provides an attractive recreational area for hackers and e-vandals to spread harmful code and virus [9]. Such type of threats can be categorized into three classes: • Application-based threats • Content-based threats • Mixed threats
2	Malware threats to Peer-to-peer networking	The use of peer-to-peer networks permits not only the capability for malicious software to extend, but also deployment of the protocols for communication by malicious software. Peer-to-peer networking introduces new vector of delivery that is email. Harmful software is usually found as email attachments.
3	Combined Attacks	These are very composite attack, which in some cases goes outside the common possibility of antivirus software. Pooled threats are defined as malware which merges the uniqueness of computer viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to activate, transmit, and increase an attack.
4	Instant Messaging	Instant messaging networks provide the potential to not only transfer text mails, but also relocate files. Hackers can use instant messaging to acquire backdoor access to computers without breach a notable port, successfully avoiding desktop and outer limits firewall completions.
5	File-less malware	File-less malware attacks are mostly commenced with an already infected

		existing legitimate program or by using existing legitimate tools that are built into the OS (for example, Microsoft's Powershell). These malware infect the computer using 'non-file' OS objects, like APIs, registry keys etc.
6	The hybrid attack	Malware that could be a mixture of more than one stream of traditional malware. This type of malware, some malware is part virus, part Trojan, and part worm. Such a malware during the initial stage might appear as a Trojan, after that it would be spread like a worm.

V. NEW PROMISING TRENDS IN MALWARE THREATS DEFENSE

Virus events in the future will increase more than what the Internet Worm and the Melissa virus did. Every latest virus will have the prospective to wrath out of control, if a remedy is not made available quickly and scattered extensively. The main source for this paper is IBM Thomas J. Watson Research Center [10].

S.No	New Trends in Computer Virus Defense	Description
1.	Immune System Architectural	To solve this kind of virus, IBM has built a front computer resistant system which can locate, investigate and treat formerly unidentified viruses faster than the viruses themselves can multiply. A virus study center is able to investigate most viruses without human intervention, with greater speed and accuracy than what human analysts can.
2.	An Active Network to Handle Epidemics and Floods	Administrator systems send virus tasters to the resistant system; form absconds of the active network. Tasters travel through a chain of commands of filters, which handle the taster if it has already been examined as pure or as a recognized infected file. Otherwise, they promote it to the examination center for analysis, consequential in reorganized virus definitions which are scattered downward to the gateways, to the administrator systems, and finally to the clients. Active networks launch samples up, after that these samples send back status information and virus description files. The gateways database will seize 10 million outcomes in 1 GB of disk.
3.	Automated Virus Analysis Center	The analysis center is self-possessed of a network of computers, which are remote from the rest of the world by a firewall for defense purposes. An administrator system is responsible of coordinating all actions surrounded by the analysis center. A supervisor system follows priorities and status, passing on tasks to groups of worker systems, until study is complete and updated virus definition files are returned to the active network through the firewall. A server stores virus duplication environments and contains records of everything prepared in the analysis center. The groups of worker systems can be expanded automatically to extent the analysis center to bigger workloads. Currently, the input file in the analysis center is proficient of holding roughly 8,000 samples which are pending analysis. By increasing the total disk space on the supervisor system it can be expanded easily.
4.	Handle Average Loads	The protected system is designed to easily hold the stack of new viruses, and insist for virus explanation updates to deal with submitted tasters. The active network and analysis center are deliberate to be strong, fault-tolerant systems which activate full day.

VI. CONCLUSION

The unexpected growth of the Internet and the rapid coming out of applications that ignore the traditional boundaries between computers intimidate to amplify the global spread rate of computer malware by several orders of extent. The new optimistic immune system is likely to be an essential tool to control their spread for the predictable future. Government, Home users and corporations' entities need to seriously think again their security policies, and anti-virus companies required to start working on the next generation of anti-virus protection.

REFERENCES

1. A System to Support the Analysis of Antivirus Products' Virus Detection Capabilities, Marko Helenius, 2002.
2. http://www.faqs.org/faqs/computer-virus/
3. http://www.wildlist.org/WildList/
4. "A Short Course on Computer Viruses"; Fred Cohen; ASP Press Pittsburg 1990.
5. Cohen, Fred; Establishing a Computer Security Incident Response Capability; 1992
6. https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/
7. Abrams, Lawrence (February 26, 2018). "Thanatos Ransomware Is First to Use Bitcoin Cash. Messes Up Encryption". Bleeping Computer. Retrieved June 25, 2019.
8. Linthicum, David. "Caution! The cloud's backdoor is your datacenter". InfoWorld. Retrieved 2018-11-29.
9. Virus and Malicious Code Protection for Wireless Devices, Trend Micro, February 2001.
10. Anatomy of a Commercial-Grade Immune System, Steve R. White, Morton Swimmer, Edward J. Pring, William C. Arnold, David M. Chess, John F. Morar, IBM Thomas J. Watson Research Center.