Review on Types of Computer Viruses and Their Impacts

[1]Dr. Manjunath CR, [2]Gadug Sudhamsu, [3]Shashikala H K
[1, 2, 3]Department of Computer Science and Engineering
Jain (Deemed-to-be University), Ramnagar District, Karnataka - 562112.
Email Id: cr.manjunath@jainuniversity.ac.in

ABSTRACT: The virus is something of software that severely permeates the machine, but now large companies include batch processing that is spread across the world. Safety is, therefore, an important problem today for all businesses. Intelligence has now become the greatest weapon for everybody. It requires different measures to ensure certain properties secure. As the prevalence of different kinds of viruses such as ransomware, trojans, attackers and bugs grows that, managing the network is a major challenge. With rising internet penetration in our everyday lives, we are constantly at risk of multiple kinds of threats every day. In this paper, there are a few surveys of different virus monitoring systems, along with their implications for the structure, that assist to comprehend the benefits and drawbacks of each virus during the questionnaire. Throughout the end, there is indeed a conclusion as well as some details about what can be done.

KEYWORDS: Viruses, Virus Identification, Virus Identification, Fingerprint, Irregular Warning Systems, Trojan Virus.

INTRODUCTION

The computer virus is an arrangement that can reproduce on its own despite any interference, then the replication software will duplicate and resume the same process. The dangerous code is, therefore, a script that corresponds to something that operates against this requirement. There are also many varieties of malicious software or applications capable of performing such unlawful or unintended operations that are very risky to the structure [1]. There are several forms of ransomware, generally known as worms, Trojan, spyware, etc. A new virus comprises three forms. Like a traditional virus, the illness often makes the body to spread malicious software into the environment by having the infection in the network [2].

The malware influences the machine by connecting it to other device systems, including programs. Thus, when the device starts, it reaches the machine and impacts the hard drive or boot disk. The term "virus" is also misused by extension to refer to different kind of malware. The "Malware," around each other with several other aspects of malicious code, includes computer viruses, like "worms," spyware, ransomware, Trojan horses, adware, rootkits, key loggers, bots, and malicious browsers help objects (BHOs). In fact, most active ransomware warnings are Trojan horses or computer worms instead of a piece of malware [3].

The worst consequence is that some program such as window keys alters the configuration and changes the Program date, which makes it more difficult for a consumer to trace the bug, often viruses even erase vast amounts of information [4]. Viruses function as viruses infecting the processes that are in the shape of a.exe file or a.com file that runs another application when somebody selects the.exe file on a device, it can interrupt the whole machine that has to be re-formatted. The system often fails. The functioning of the virus is illustrated in figure 1.

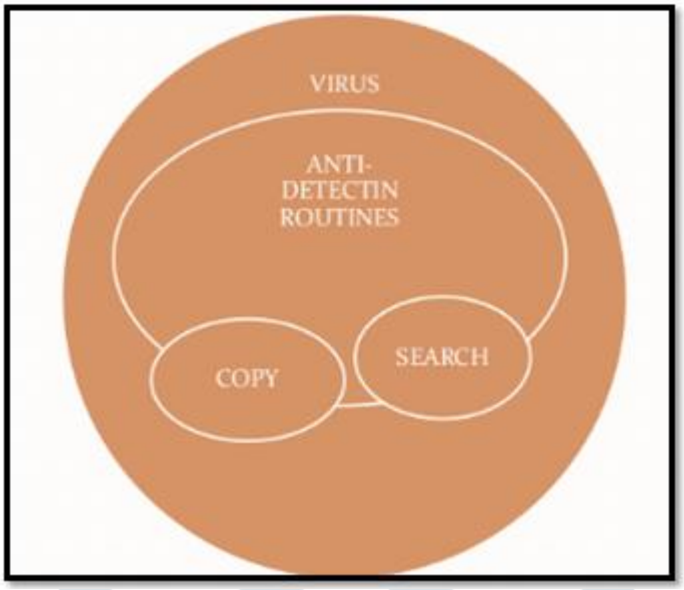
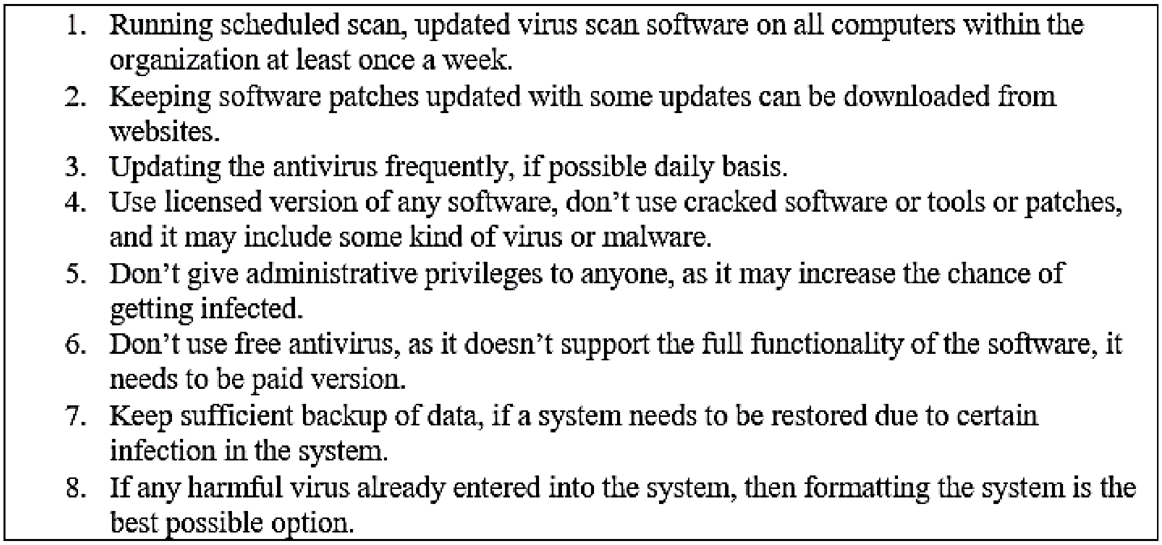


Figure 1: Finctioning of the virus

Security software is a software or application to deter, scan, discourage and delete malware from apps as well as other malicious code, such as worms, trojans, spyware and more [5]. Whether you are detecting a virus, your desktop exhibits a notification asking you what intervention to do, providing you the possibility of quarantining, removing, ignoring or moving the document to your void. Anti-virus systems are designed to safeguard your desktop or connection toward malicious software. Figure 2 shows some antivirus programs and their associated companies [6].

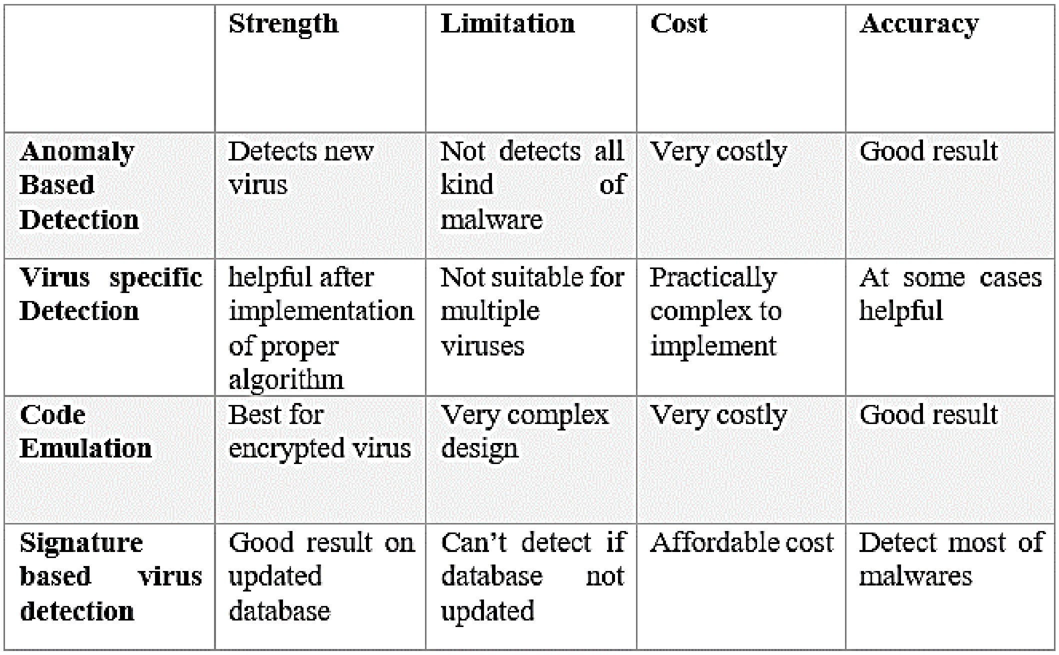
Figure 2: Some antivirus programs and their associated companies

Certain strategies can guard against Virus in addition to the usage of anti-virus software, including:



1. Running scheduled scan, updated virus scan software on all computers within the organization at least once a week.
2. Keeping software patches updated with some updates can be downloaded from websites.
3. Updating the antivirus frequently, if possible daily basis.
4. Use licensed version of any software, don't use cracked software or tools or patches, and it may include some kind of virus or malware.
5. Don't give administrative privileges to anyone, as it may increase the chance of getting infected.
6. Don't use free antivirus, as it doesn't support the full functionality of the software, it needs to be paid version.
7. Keep sufficient backup of data, if a system needs to be restored due to certain infection in the system.
8. If any harmful virus already entered into the system, then formatting the system is the best possible option.

COMPARISON STUDY



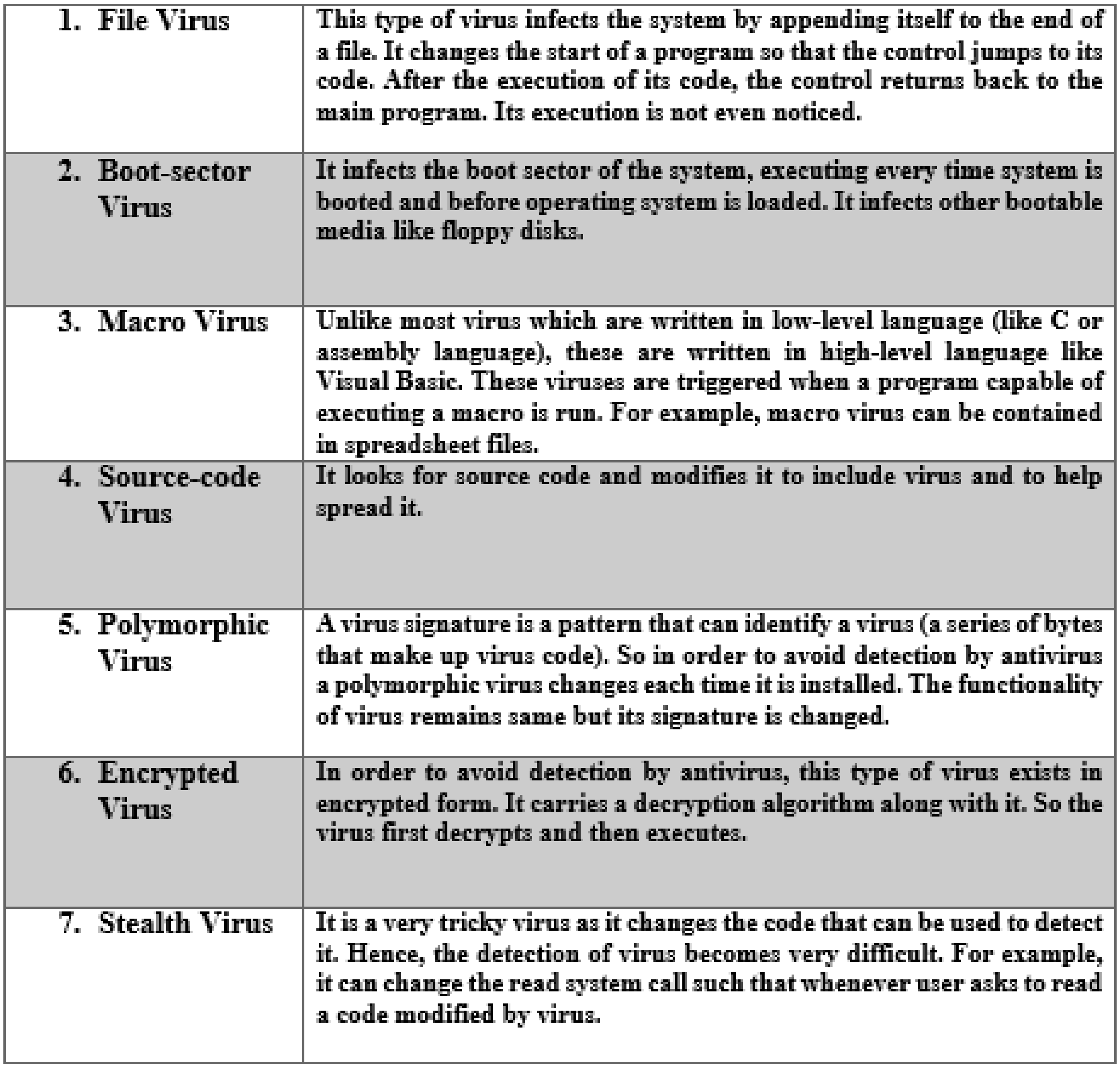
	Strength	**Limitation**	**Cost**	**Accuracy**
Anomaly Based Detection	Detects new virus	Not detects all kind of malware	Very costly	Good result
Virus specific Detection	helpful after implementation of proper algorithm	Not suitable for multiple viruses	Practically complex to implement	At some cases helpful
Code Emulation	Best for encrypted virus	Very complex design	Very costly	Good result
Signature based virus detection	Good result on updated database	Can't detect if database not updated	Affordable cost	Detect most of malwares

This review paper is divided into various sections, where the type of virus are described in the below section, review section talks about the reviewed cases and types of viruses along with some antivirus systems available in the market. The conclusion section of this paper focuses on the conclusion drawn after the review.

TYPES OF COMPUTER VIRUS

Virus has a plurality of types and every type is used for a specific intent and have a different- different mechanism. The types are presented in Table 1.

Table 1: Type of virus



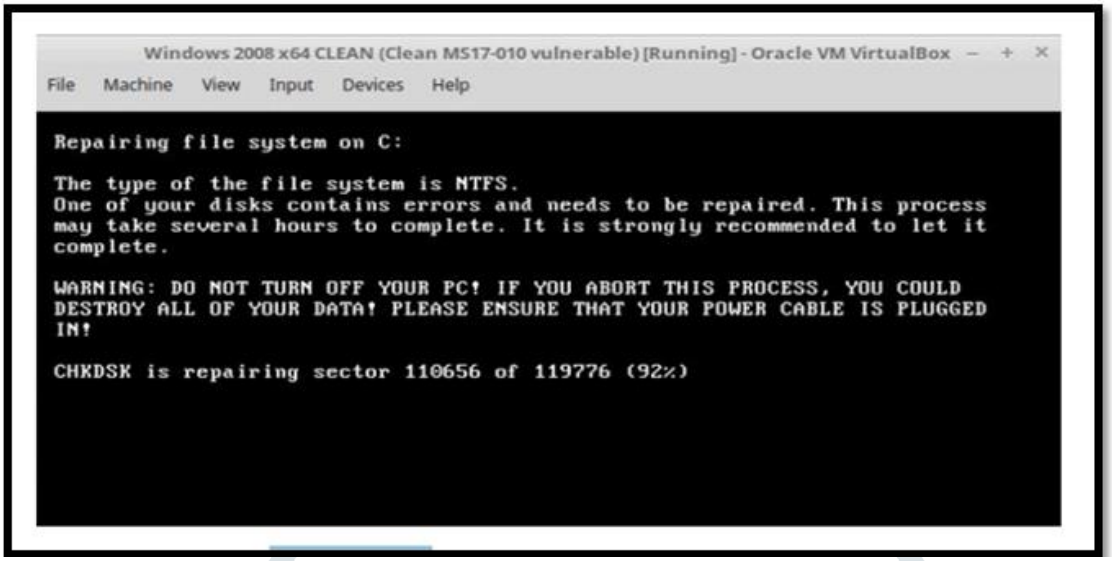
1. File Virus	This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed.
2. Boot-sector Virus	It infects the boot sector of the system, executing every time system is booted and before operating system is loaded. It infects other bootable media like floppy disks.
3. Macro Virus	Unlike most virus which are written in low-level language (like C or assembly language), these are written in high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, macro virus can be contained in spreadsheet files.
4. Source-code Virus	It looks for source code and modifies it to include virus and to help spread it.
5. Polymorphic Virus	A virus signature is a pattern that can identify a virus (a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of virus remains same but its signature is changed.
6. Encrypted Virus	In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.
7. Stealth Virus	It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of virus becomes very difficult. For example, it can change the read system call such that whenever user asks to read a code modified by virus.

REVIEW OF COMPUTER VIRUSES

Petya-Ransomware Attack

In the background, cyber-attacks have increased exponentially. The ransomware attack, which corrupts and decodes data as well as robes knowledge from the network, is among the most devastating attacks in this cyber-attack. The Petya-Ransomware attack has been one of the biggest ransomware assaults in modern times. Petya-malware techniques and risks will be addressed. Sensitivity and prevention are also discussed. This also utilizes that same flaw used for ransomware WannaCry. The first outbreak in Europe started, primarily with Ukraine. The intrusion was documented in Petya ransomware, first seen in March 2016 and once again targeted with the hybrid version in June 2017. Certain 64 nations, including Brazil, Germany, Russia, India and the United States, were influenced. Figure 3 depicts the screen of the computer after the attack.

Petya's malware coding is AES-128 with an RSA that varies from the prior SALSA20 versions. If permissions are not wide enough, data can even be secured without the need for a computer reload. The ransomware encrypts even the MBR and MFT if the administrator permissions are open. The ransomware downloads its software from either the MBR whenever the system is recharged and authenticates hard disk data. If the device is closed down without reloading, MBR will restart the operation using the order "bootrec /FixMbr." Ransomware threats are unique to the planet, so the ransomware mitigations are not understood. The leading cause of the attack is the decision to send off the ransomware e-mail containing the victim's malicious software. The assault is therefore effective when the individual who has endured the attack installs the application and activates it, as the user immediately tries to start the malicious software and provides exposure to the central network when the annex is opened.


Windows 2008 x64 CLEAN (Clean MS17-010 vulnerable) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help

```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 110656 of 119776 (92%)
```

Figure 3: System screen when reloaded after attack

Xafecopy Trojan

“Xafecopy” Trojan is malicious software that was originally recognized by the Information technology and Anti-virus Service “Kaspersky Lab” in September 2017 and that targets the Android operating system. In about 47 countries, “Xafecopy” contaminated 4,800 people within such a couple of weeks, as per the Kaspersky Lab. The main abusers of “Xafecopy” were consumers in India, accompanied by subscribers from Russia, Turkey and Mexico. In 2017, “Xafecopy” had first been detected in India by Kaspersky to hack hundreds of Android devices. It has been recorded that the malicious software is integrated into a wide range of applications, most often power supply optimizers. Unknown or unable to access malicious software to the device. The client taps on web pages using WAP monitoring and “Xafecopy” connects to a collection of providers paying money straight on the user's mobile telephone bill. The websites of the program are paid through WAP charging techniques. Captcha systems can also be bypassed by technological advances. It works by tapping on the WAP accounting program's webpages which would be a digital payment system that is specifically indicated to the mobile bill. “XAFecopy's” application is usually a battery optimization application. The malware is supported by the Ubsod-community on android phones that are powered by WAP throughout a GPRS or 3-G wireless links. “Xafecopy” provides a battalion-and-control system with WAP subscription URL addresses to web sites. Once you have done receive a URL address, you tap on WAP payment links that start a WAP meeting with the database, then continue receiving the MSISDN of a user and charged effectively to the mobile operator bill of the user and register into undesired pay-off services. “Xafecopy” seems to be using equipment that circumvents captcha technologies.

CONCLUSION

Even though the virus protection initiatives are updated regularly, it still helps virus developers to upgrade and modify codes every day which makes the process more vulnerable to exploitation. Only when the virus has been initiated will the anti-viruses be released on the industry with recent approaches. A wide infrastructure must now be supervised for raids by malware, viruses, Trojans etc. Such that the virus is first removed until any worthwhile data from an organization is removed. Even in the latest technology, time sophistication and hardware reliability must be decreased before decent quality software is implemented which immediately lessens the likelihood of being raised. This review paper firstly talks about the virus, what is it made up and what it can perform. This paper also analyzes the amount of damage the virus can do. Additionally, this paper discloses and discussed the types of the virus still present in the world. This review paper reviews two harmful viruses and discloses their mechanism.

REFERENCES

[1] M. Maliapen, “Computer Security,” in *Encyclopedia of Applied Ethics*, 2012.

[2] G. Serazzi and S. Zanero, “Computer virus propagation models,” *Lect. Notes Comput. Sci. (including Subsea. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, 2004.

[3] S. Mueller *et al.*, “Live attenuated influenza virus vaccines by computer-aided rational design,” *Nat. Biotechnol.*, 2010.

[4] S. Mohurle and M. Patil, “A brief study of Wannacry Threat: Ransomware Attack 2017,” *Int. J. Adv. Res. Comput. Sci.*, 2017.

[5] P. Eichhorn, “Computer virus,” *New Scientist*. 2013.

[6] J. O. Kephart and S. R. White, “Measuring and modeling computer virus prevalence,” in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, 1993.

[7] K. Mathur, M. T. Scholar, and S. Hiranwal, “A Survey on Techniques in Detection and Analyzing Malware Executables,” *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, 2013.

[8] E. Gandotra, D. Bansal, and S. Sofat, “Malware Analysis and Classification: A Survey,” *J. Inf. Secur.*, 2014.

[9] J. Chang, K. K. Venkatasubramanian, A. G. West, and I. Lee, “Analyzing and defending against web-based malware,” *ACM Comput. Surv.*, 2013.

[10] R. Veeramani and N. Rai, “Windows API based Malware Detection and Framework Analysis,” *Conf. Networks Cyber Secur.*, 2012.

[11] S. Alrabaee, L. Wang, and M. Debbabi, “BinGold: Towards robust binary analysis by extracting the semantics of binary code as semantic flow graphs (SFGs),” in *DFRWS 2016 USA - Proceedings of the 16th Annual USA Digital Forensics Research Conference*, 2016.

[12] J. Ming, D. Xu, Y. Jiang, and D. Wu, “BinSim: Trace-based Semantic Binary Diffing via System Call Sliced Segment Equivalence Checking,” *USENIX Secur. Symp.*, 2017.