Evolution of Antivirus software

A short survey

Shanika Perera *(Author)*
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
0.perera.hishi@gmail.com

Dilan Mel *(Author)*
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
dilanmel74@gmail.com

***Abstract* - This paper has been undertaken to introduce, analyze and summarize of the concept of antivirus software. It presents a general overview on evaluation of antivirus software. In order to stay far away from the antivirus scanners, computer viruses increased their codes to make them invisible. On the other hand, in order to guarantee effectiveness and maximum protection, antivirus software must be continually updated. This disquisition reveals how antivirus software work and what important criteria are, when choosing of such a solution.**

Keywords - virus; worm; malware; security; antivirus; scanners; machine learning; data mining; sandbox detection

I. INTRODUCTION

Modern day computer viruses are huge impact on Information and Communication Technology. A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions. It is designed to spread from host to host and has the ability to replicate itself. Viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document. A computer virus is something that needs to be avoided. Consequently, every computer requires a strong security application for protect its data and installed software. Because of that antivirus software has important position in Information and communication Technology.

An antivirus program is a software utility designed to protect computer or network against computer viruses. The first antivirus programs are appeared in 1987 with the introduction of an antivirus program from G Data Software for the Atari ST. Once an antivirus has been installed and is running the program on computer, it can detect new viruses or malware installing on the computer. Every antivirus program also has definitions that tell the antivirus program how to detect and clean any new viruses that may have been released.

II. OBJECTIVES

Broadly, this review paper aims to evaluate how anti-virus software work. This research is proposed,

- To identify what are the antivirus software features
- To evaluate its virus identification methods
- To discuss antivirus software evasion
- To assess the effectiveness of antivirus solutions

This paper reviews the literature surrounding how antivirus software perform, current trends in antivirus software and its drawbacks as well.

III. HISTORY

Pre-Anti-virus days

At first Antivirus product was simply called "scanners". Because they try to identified patterns in the program. AV programs furthermore don't use command line scanners. The base of the virus as early as 1949, first virus is published in 1971 and it called as a "Creeper virus". The "Creeper virus" programed by "Ray Tomlinson" and finally he eventually deletes the program, it called "The Reaper" Antivirus. someone consider that The Reaper is the first Antivirus Software Ever written.

The creeper Virus conducive to many other Viruses. Which is followed by "In the wild" was "Elk Cloner" is infected_Apple II computers in 1981.most viruses written in early and 1980's mid.

Early days (1980-1990)

There was competing among others to become innovator of the first Antivirus product. However, in 1987 Bernd Fix performed the first publicly documented removal of computer virus. There were many antivirus products released in those days such as in 1985 Andreas Lüning and Kai Figge, who found G Data software for the Atari ST platform, in 1987 Ultimate Virus Killer(UVK) was released.

In 1987 United States John McAfee found the McAfee company and released the first Virus Scan version end of the year. And also, in 1987 NOD antivirus was released by Peter Paško, Rudolf Hrubý, and Miroslav Trnka. Early Heuristic engines depends on dividing the binary sections (data sections, code sections).

In 1988 begin to growth AV companies. In Germany Tjark Auerbach produced the Avira, In Bulgaria Dr. Vesselin Bontchev released the first freeware and many of researchers found many products in those days. And also, in 1988 some were discussed the possibilities of eliminating and detecting viruses. In the end of those days United Kingdom Jan Hruska and Peter Lammer founded the security firm and begun to produce first encryption and antivirus products.

1990–2000 period

In 1990 also new arousal of the Antiviruses products, Such as Panda Security, Pasteur antivirus, Viral eXplorer antivirus and etc. Computer Antivirus Research Organization (CARO) also found in 1990.

In 19991 Norton Antivirus was founded by United states Symantec and jan Gritzbach and Thomas Hofer founded AVG Technologies, European Institute for Computer Research (EICAR) also founded in this year.

IV. ANTIVIRUS SOFTWARE FEATURES

Antivirus software programs are created to prevent, detect and take any necessary action to remove them from computers. Most of the antivirus products share a set of common features. There are many features to be found in antivirus products.

- Capability to scan compressed files as well as executables.
- Tools for performing real-time scanning
- Firewall and network inspection functionality
- Command line interface
- Graphical user interface
- A daemon
- A management console [1]

These features are briefly discussed in the following subsections.

A. Use of native languages

Antivirus(AV) engines must perform as quickly as possible in case of a malware detection without concerning the systems performance. To do that most of the antivirus engines are languages such as C, C++ or a mix of both these languages. These are known as native languages because it can run on any platform without converting it first. Making use of these native languages help to fulfill these requirements because when the code is compiled, they run natively on the host CPU at full speed without needing of any interpreters [1].

B. On-Access or Real-time scanning

With the use of this feature, it gives the ability to catch viruses as soon as they try to get into a system. On access scanners runs as a background process and scans the computer system continuously for any incoming viruses or other malware types. The On-Access scanner should be able to scan all areas of the system including the file system, boot records, memory and master boot record [2]. Real-time scanning runs until the user power off the computer.

C. On-Demand scanning

As described in the name itself, this scanner is to make sure that all the files in your system at the moment are virus free on the users' demand. This scanner scans the computer system only when provoked by the user or at a timely schedule. It is essential to check the current file system in case if a virus has gone undetected [2].

D. Ability to scan miscellaneous file formats

Harmful software can sneak into a system from a variety of different source. Even though a virus can't run when compressed, its righteous to detect them, before it enters to the system. Antivirus engines are able to decompress and steer through all the files inside including Word and Excel documents, HTML pages, XML documents, PDF files and other types of file formats [1].

E. Packet filtering and firewalls

Antivirus software tries to protect computers from all kind of malware. Network traffic analysis, packet filtering and firewalls was installed in AV software to block and detect malware types specially from worms. Because many worms, ransomware and spyware attacks use network resources to infect computers.

V. HOW IT WORKS?

An antivirus program consists of 5 major components. The kernel, command-line scanner, GUI scanner, network filter drivers and system services are the major elements of it. The kernel is the core of any antivirus software. All the procedures for relieving executable programs, compressors, cryptos, protectors etc. are stored in the kernel inside a library or so. The kernel is used by scanners, residents (or daemons), or by other programs and libraries.

An antivirus engine does not provide direct access to its core by any third-party developers. But it gives access to the command-line scanners. Some products give access to its GUI scanner instead of giving access to its command-line scanner. GUI scanners provide real time protection, handling malware identification and disinfection. Antivirus products are also combined with other security features such as browser toolbars for protection, network filtering, firewalls and so on. While scanners scan the files and directories and the kernel includes the core features offered to high level software components such as command-line or GUI scanners [1].

Any antivirus software works in a traditional way. It uses a database called "Virus dictionary" which has lots of codes of different viruses. A virus is also another program which is set to follow some commands. When antivirus scans a file, it takes some time to check that code and compare it with codes of that dictionary. If it matches, it informs the user telling a virus has been detected. The virus dictionary contains hashes of viruses such as MD5. That MD5 code will always match that virus no matter what unless the virus is encrypted. Encrypted viruses are further discussed in section VI.

Any effective antivirus software must have the ability to carry out several functions. First it must detect the viral code with minimal false positives or negatives. It must avert any unwanted behavior that comes with it and must remove that malicious code and fix any damage that it has caused. The software must perform these functions with minimal system resources and as fast as possible. It must not impact the performance of other applications which are running at the moment. To detect and identify, most software packages use different kind of identification methods [14]. Those methods will be further discussed in the following section.

VI. IDENTIFICATION METHODS

According to Frederick B. Cohen's 1987 demonstration, which is a solid theoretical study in computer viruses there are no algorithm that can perfectly detect possible viruses [6]. Using different layers of defense, you can detect these viruses up to some level.

There are 2 main methods that antivirus engines used to identify malicious codes.

- Sandbox detection

This is a behavioral-based detection technique. A sandbox is executed by implemented by executing the software in a restricted operating system otherwise known as virtualism. In a virtual environment, viruses and trojans have fewer opportunities of harming the computer. In this method it does not detect the fingerprint at run time. In fact, it runs virtually and logs all the actions. Based on the logged data, the antivirus engine checks whether the executed program is malicious or not. If it's not malicious it runs the program in the real environment [8].

- Data mining techniques

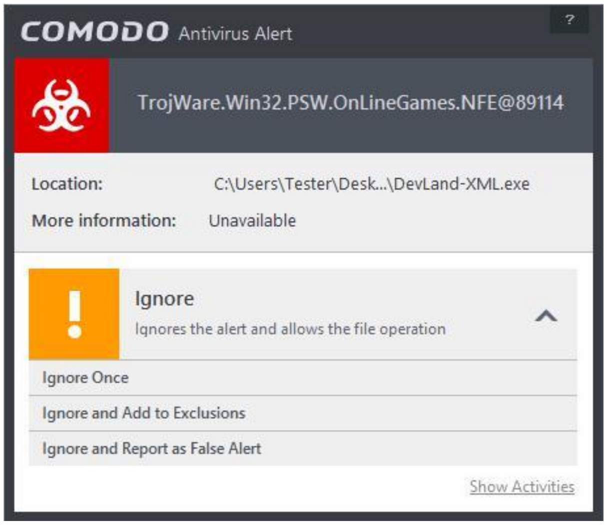
This is one of the latest approach in malware detection. Machine learning and data mining techniques are used to analyze the behavior of a file given a series of file features that are extracted from the file itself. Data mining is used to get information from available files and machine learning teaches the computer to learn and understand the given instructions [6][7][9] [10].

Instead of these two methods, virus detection methods can be categorized into 4 major parts.

A. *Signature based detection*

Most of the antivirus software rely on this technique to identify malware. The scanner of any antivirus product searches files using a set of signatures and assign a name to it. These signatures are known as patterns of malicious files. They are digested with simple pattern matching techniques, CRCs, or MD5 hashes [1]. It requires exact match between infection and signature. This technique can identify only known viruses, once that have been analyzed and categorized. There are viruses called "oligomorphic", "polymorphic" and most recently "metamorphic" which are one step ahead of bypassing the signature-based approach [20]. These viruses encrypt part or all of themselves or reform themselves as a method of disguise so that it won't be detected in the virus signatures in the dictionary [19].

Signature scanning are highly effective in discovering and disinfecting known viruses and has a low rate of occurrence of false positive and false negative reporting and requires frequent updates [14].



COMODO Antivirus Alert

TrojWare.Win32.PSW.OnLineGames.NFE@89114

Location: C:\Users\Tester\Desk...\DevLand-XML.exe

More information: Unavailable

Ignore

Ignores the alert and allows the file operation

Ignore Once

Ignore and Add to Exclusions

Ignore and Report as False Alert

Show Activities

Fig. 1. A false positive generated with Comodo antivirus software

B. *Heuristics*

Heuristic scanners are same like signature scanners. It runs as an on-demand scanner and diverge widely in their scope and complexity [2]. Heuristic scanners can be arranged into two categories as static and dynamic.

1) *Static scanners* - Static scanners also known as passive scanners, make use of signatures rather than scanning for byte sequences. With simple viruses, these scanners scan for byte sequences or take a look at the binary code and checks whether it is associated with virus behaviors. Heuristic scans are associated with positive, negative heuristics and other form of byte sequence non-virus behaviors. By applying both positive and negative heuristic analysis programs are able to reduce the incidence of false positives.

2) *Dynamic scanners* - Dynamic heuristic scanners (active scanners) load suspicious executable files into a virtual environment and emulate their execution. It scans for signatures in a file while it's running actively. It does not have a 100% detection rate. The viruses are made to evade dynamic scanners. Dynamic scanning is time consuming and resource concentrated than static scanning.

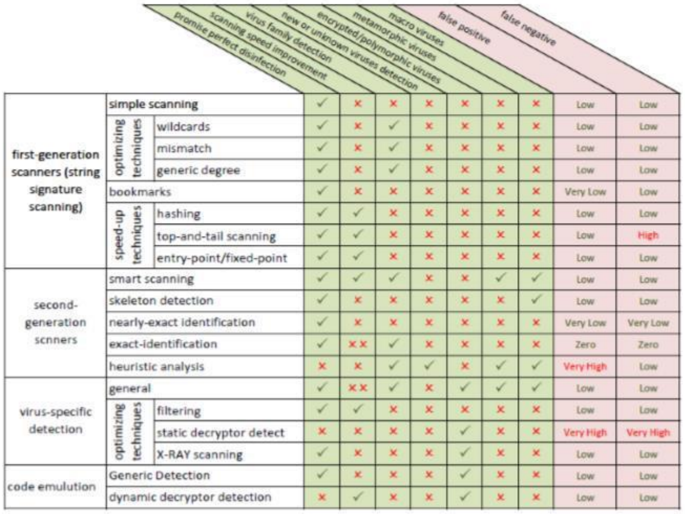
Heuristic scanners have higher rate of producing false positives than signature scanners but they are remarkable of detecting unknown viruses [14].

C. *Activity blockers*

Activity blockers are memory resident programs that observes and check for distrustful behavior such as modification of executable files. It requires user interaction to decide whether the suspicious activity should be allowed to run on the system or not. The decision to avert a suspected or unwanted viral behavior rests upon with the user and not the antivirus software. Activity blockers are ineffective against macro viruses, trojan horses and worms including tunneling viruses [14].

D. *Integrity checkers*

Antivirus software use checksums to add extra element to signature scanners. After a scanner discovered a virus signature, a checksum is run against the file and endorsed against checksum for the known virus. By using this technique, it reduces the possibilities of making false positives. Integrity checkers themselves cannot detect the viral code. What they do is that they reveal the changes in files and disks against a baseline measure. By using these changes, the program alerts the users. User intervention is required and there is no repairing of programs with integrity checkers. Integrity checkers do not require time to time updates. But they produce a significant number of false positives [14].



			Promise perfect disinfection	scanning speed improvement	virus family detection	new or unknown viruses detection	encrypted/polymorphic viruses	metamorphic viruses	macro viruses	false positive	false negative
first-generation scanners (string signature scanning)	simple scanning		✓	✗	✗	✗	✗	✗	✗	Low	Low
	optimizing techniques	wildcards	✓	✗	✓	✗	✗	✗	✗	Low	Low
		mismatch	✓	✗	✓	✗	✗	✗	✗	Low	Low
		generic degree	✓	✗	✓	✗	✗	✗	✗	Low	Low
	bookmarks		✓	✗	✗	✗	✗	✗	✗	Very Low	Low
	speed-up techniques	hashing	✓	✓	✗	✗	✗	✗	✗	Low	Low
		top-and-tail scanning	✓	✓	✗	✗	✗	✗	✗	Low	High
		entry-point/fixed-point	✓	✓	✗	✗	✗	✗	✗	Low	Low
second-generation scnners	smart scanning		✓	✓	✓	✗	✗	✓	✓	Low	Low
	skeleton detection		✓	✗	✗	✗	✗	✗	✓	Low	Low
	nearly-exact identification		✓	✗	✗	✗	✗	✗	✗	Very Low	Very Low
	exact-identification		✓	✗✗	✓	✗	✗	✗	✗	Zero	Zero
	heuristic analysis		✗	✗	✓	✓	✗	✓	✓	Very High	Low
virus-specific detection	general		✓	✗✗	✓	✗	✓	✓	✓	Low	Low
	optimizing techniques	filtering	✓	✓	✗	✗	✗	✗	✗	Low	Low
		static decryptor detect	✗	✗	✗	✗	✓	✗	✗	Very High	Very High
		X-RAY scanning	✓	✗	✗	✗	✓	✗	✗	Low	Low
code emulution	Generic Detection		✓	✗	✗	✗	✓	✗	✗	Low	Low
	dynamic decryptor detection		✗	✓	✗	✗	✓	✗	✗	Low	Low

Fig. 2. Comparison table of virus detection methods according to their features

VII. TYPES AND COMPARISON OF ANTIVIRUS PROGRAMS

A. *Different Types of Antivirus Software*

1) *Stand-Alone Antivirus Software*

This is basic antivirus software that keep track on database of the known viruses which are called signatures. Signatures are value of hash or byte streams so it is used to check the buffer or file included malicious payloads, Signatures are significant part of the antivirus engine. When basic scan happens, the data contained on the disk and the memory of the computer, then it does comparison of the available signatures and the data.

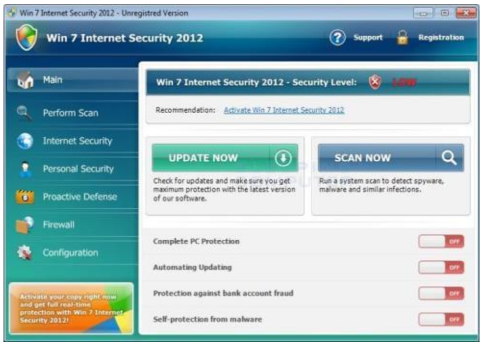
Some of the antivirus program procure "real time protection". These types of antivirus software monitors file sharing and internet connectivity, so AV senses recognize if there is an any computer virus or computer action that similar to virus it shut down or ignore the activity.
Ex. – Avira PC Cleaner

2) *Malware protection Antivirus Software*

These are combined antivirus detection with malware and spyware that are different from computer viruses. Spyware or malware do not target the PC files but tries to get sensitive data of the user. Some of Antiviruses contains protection to avoid this kind of behavior.

3) *Fake Antivirus Software*

As saying of the name these are fake, that catch only small piece of user unaware. These types of antiviruses display alerts to the user and saying "the computer has been compromised" and offer spurious button to getting rid of the threat. When the user tries to click the button, fake antivirus installs a virus in to the computer and damages the computer. Some of them even offer another solution by demanding a payment.



Win 7 Internet Security 2012 - Unregistred Version

Win 7 Internet Security 2012 - Security Level: LOW

Recommendation: Activate Win 7 Internet Security 2012

Check for updates and make sure you get maximum protection with the latest version of our software.

Run a system scan to detect spyware, malware and similar infections.

Complete PC Protection OFF

Automating Updating OFF

Protection against bank account fraud OFF

Self-protection from malware OFF

Activate your copy right now and get full real-time protection with Win 7 Internet Security 2012!

Fig. 2. Example of a fake antivirus software

4) *Antivirus Software security suits*

Most of the antivirus manufactures offer "Security Suits", because of the increasing over computer security and increasing of the types of security software programs. These are coming from bundle package of firewall and antivirus or combination of firewall, malware and antivirus protection. Firewall is a critical component of the security system, it monitors internet connectivity and activity that is block anything similar to virus. Antivirus software suits offer a better protection than the other antivirus software. They give the easier installation, security management, website filtering and spam blocking [3].

B. *Real world antivirus software*

- *AVG –*
  AVG is the most popular antivirus software in the industry. It is free and easy to download from the internet. AVG does not take appreciable space on a hard drive to store and can work many operating systems.

- *Avast –*
  It gives many features to end user, such as boot time scanning, email and network shield scanner. It can be easily installed in any Windows OS. In 2017, it's the most popular in the antivirus market.it has largest shares in the market. It provides anti-phishing, anti-spam, computer browser security among other services.

- *Avira -*
  Avira is a German multinational security software mainly known for the Avira antivirus software. It eliminates lots of malware including dialers, worms, rootkits. It provides many factures as the other antiviruses, such as system scanner that helps to prevent detect the viruses, worms and trojans. And additionally, it stops the new viruses before start it. Avira "cleans out" the its virus definition files and replace signature and increases the speed of the computer.

- *Bitdefender -*
  Bitdefender is a Romanian cyber security and antivirus software company. Bitdefender develops and sells antivirus software, internet security software, endpoint security software, and other cybersecurity products and services.

Bitdefender offers good protection to avoid rootkits.

- *Dr. Web* -
  Dr. Web is an anti-malware suite developed by Russian anti-malware company Dr. Web. It offers anti-spam solutions and is used by Yandex to scan email attachments. It also features an add-on for all major browsers which checks links with the online version of Dr Web.

- *McAfee* -
  This is the Second most popular antivirus program on the present market. Using one program it provides spyware and virus protection which other programs do separately.

- *Norton* -
  This program is produced by Symantec. There are various types of Norton Antiviruses programs available. Norton products are available in different range of electronic supply stores. There are two productions in the Norton programs, such as Norton Antivirus and Norton internet security either one search computer regularly and kill any viruses which they find.

- *Kaspersky* -
  Kaspersky is developed by Russians. It is a very effective antivirus, but most of them didn't know about it. It provides effective protection to avoid viruses, spyware and trojans [4].

C. *Comparison of antivirus software*

According to a survey conducted in Israeli Institute of Technology, the initial detection rate of detecting a newly created virus is less than 5%. Even though antivirus vendors try to update their detection mechanisms, they can't keep up with the virus propagation now a day. For certain vendors it takes up to 4 weeks to identify and detect a virus [16]. Third party antivirus engines are becoming popular in the antivirus industry. It means that the antivirus engine is made by another producer. A third-party producer is responsible for the core of the antivirus product. In spite of that, the malware signatures of the product are done by the owner of the product itself.

In this analysis, 8 main antivirus software are compared between according to their features.

TABLE I. COMPARISON OF ANTIVIRUS SOFTWARES

Anti-virus software	On demand scan	On access scan	Boot-time scan	Heuristic	Firewall	IPS/ IDS	Email security	Anti-spam	Web protection	Macro protection	Live protection
Avast	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
AVG	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes
Avira	Yes	Yes	Yes	Yes	No	No	No	Yes	No	Yes	Yes
Bitdefender	Yes	Yes	Yes	Yes	No	No	No	Yes	No	Yes	Yes
Dr. Web	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Kaspersky	Yes	Yes	Yes	Yes	No	No	No	Yes	No	Yes	Yes
MacAfee	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
Norton	Yes	Yes	Yes	Yes	No	No	Yes	No	No	Yes	Yes

VIII. CURRENT TRENDS OF ANTIVIRUS PROTECTION

This section discusses about the target audience for malware authors and what are the level of protection offered by the antivirus industry.

There are three main types of target audiences.

A. *Targeting home users*

When it comes to home users, attackers tend to care less about using their best technologies. Instead they focus on using simple techniques so that can attain quick results. The main motivation on targeting home users is to make money. For an example the infected computer can be monitored to capture banking details of that particular user and transfer any amount of money to attackers account.

B. *Targeting small to medium sized companies*

Attackers targeting small to medium sized businesses happened to use similar kind of techniques that are used for home users. It may involve social engineering techniques, zero-days bugs, exploit kits etc.

C. *Targeting governments*

Attacking governments and government like big companies requires much more complicated techniques. As it is a large-scale attack, the victims must protect themselves from zero-day vulnerabilities, spyware, trojan horses and all kind of malware [1].

When selecting the antivirus software, it is best choice to know the audience and select the best and most effective one which will protect you from these attackers.

IX. DRAWBACKS OF AV

A. *Computer performance*

Even though antivirus software plays a major role by defending malware, it impacts the computer's performance. It can slow down the computers performance.

B. *Unexpected renewal cost*

There are some Antiviruses made agreement between end-user it includes subscription will be automatically renewed. Since that user credit card billed automatically. Some AV always ask to user to get renewal the license, if they unable to pay it AV would stop detecting new viruses.

C. *Zero-day attacks*

Zero-day attacks are security bugs that are not yet fixed. It's called zero-day because there are zero days for antivirus developers to patch the flaw. Now a day's technology is becoming major development, sure enough the people who use it improperly finds malicious things, because of that antiviruses also need to update immediately unless it became a huge problem.

D. *False alarms*

This happens when the antivirus software identifies a non-malicious file as virus or malware. There can be false positive which is in spite of the fact that there is no virus, but it creates a false alarm and false negative which means that even though there is a virus infected, the antivirus software fails to identify it. If the antivirus program is configured to delete any infected file whenever it finds one, it can cause some serious problems in a false positive condition.

E. *Bypassing antivirus software*

There are many Antivirus evasion techniques and Tools. So that attackers can easily bypass antivirus techniques. This evasion techniques are not doing only malware writers, penetration testers also try to evasion the AV, penetration testers who are pen testing a company, they need to bypass Antivirus product. There are two evasion techniques. [1]

- *Static* - This technique put through by convert the content of the file, since that Antivirus can't detect it because input file hash value has been changed.
- *Dynamic* - This technique used when during the execution by running the malware, either in an emulated or real environment. The malware can change the procedure similarly of the Av software and fingerprint the AV software to evade to detect.

X. FUTURE RESEARCH

Now a day everything is competitive, when thinking about attacker side, there are many ways to add a malicious code attached to executable file which are often legitimate programs. So, Antivirus author have to be smarter than attackers, they need to be one step ahead.

Antivirus software aim is to give a better armor to the operating System. So, antivirus authors must know how the attackers attack first and antivirus software defense against the attack. Because of the new virus’s authors must do many researches to prevent those kind upcoming viruses.

There can be weakness in both viruses and antiviruses, usually viruses try to attack Achilles’ heels defense system, so there are many problems in detection methods. [1]

- Detection methods not enough powerful to detect new viruses
- More time consuming to scan
- If the user forgets to update the AV, it cannot be reliable [20]

So that researchers interested in virology and antivirus techniques must work on these errors in the future.

CONCLUSION

Overview In the above report, viruses are very destructive programs that can be devastating to companies and individuals. Upon completion of this project you should be able to have an understanding of these things, what viruses are, how viruses can be avoided using antivirus software, how does antivirus programs get rid of viruses and any kind of malware and the best type of software used to prevent viruses. For better and safe computation anti-virus software should be installed and be help full for global network system freely.

ACKNOWLEDGEMENT

The authors would like to thank Sri Lanka Institute of Information Technology for supporting to this review paper. We thank our colleagues who provided insight and expertise that greatly assisted the research. We thank Mr. Amila Senaratne for assistance with Introduction to Cyber Security module. We thank 3 “anonymous” reviewers for their so-called insight although, any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

[1] Antivirus hackers handbook

[2] Jacqueline Castelli (December 12, 2001). Choosing antivirus software 784.

[3] Different types of antivirus software. [ONLINE] http://typeslist.com/different-types-of-antivirus-software/

[4] Five types of antivirus programs. [ONLINE] https://www.doityourself.com/stry/5-types-of-antivirus-programs

[5] Cohen, Fred, An Undetectable Computer Virus (Archived), 1987, IBM

[6] *Data Mining Methods for Malware Detection*. ProQuest. 2008.

[7] *Dua, Sumeet; Du, Xian (April 19, 2016). Data Mining and Machine Learning in Cybersecurity.*

[8] Detecting Malware and Sandbox Evasion Techniques

[9] Data Mining: Concepts and Techniques

[10] Konrad Rieck, Phillip Trinius, Carsten Willems, Thorsten Holz. Automatic Analysis of Malware Behavior using Machine Learning.

[11] Deng, P.S.; Jau-Hwang Wang; Wen-Gong Shieh; Chih-Pin Yen; Cheng-Tan Tung (2003). *"Intelligent automatic malicious code signatures extraction”*

[12] Aditya Agrawal, Karan White (2016). Analyzing and Optimizing cloud-based antivirus paradigm

[13] Rafael Felder, Marcel Kulicke, Julian Schutte. An Antivirus API for Android Malware Recognition

[14] Lisa Galarneau, Anti-virus Software: The Challenge of Being Prepared for Tomorrow#39; s Malware Today

[15] Sarah Gordon, Richard Ford. REAL WORLD ANTI-VIRUS PRODUCT REVIEWS AND EVALUATIONS – THE CURRENT STATE OF AFFAIRS

[16] Imperva. 2012. Assessing the Effectiveness of Antivirus Solutions

[17] Jameel Haffejee, Barry Irwin. Testing antivirus engines to determine their effectiveness as a security layer

[18] "Antivirus Research and Detection Techniques". ExtremeTech.

[19] *Szor, Peter (2005).* The Art of Computer Virus Research and Defense

[20] Babak Bashari Rad, Maslin Masrom, Suhaimi Ibrahim. Evolution of Computer Virus Concealment and Anti-Virus Techniques

AUTHOR PROFILE

Shanika Perera currently a third year B. Sc. student of Sri Lanka Institute of Information Technology at faculty of computing. She will be completing her undergraduate degree majoring on Cybersecurity by March 2020 and is highly focused on research work and competent academic career.

Dilan Mel is a third-year undergraduate student of Sri Lanka Institute of Information Technology at faculty of computing. He will be finishing his Cybersecurity B. Sc. degree by March 2020. He is keen on research are and exploring information technology based areas.