IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Security Vulnerability Analysis

Chaitanya Vijay Parab, Kizhar Ahmed Arshad Katheem, Mohd Shoeb Shaikh, Amman Akhtar Sayed

Researcher, Researcher, Researcher, Researcher,
Computer Science of Engineering,
Rizvi College of Engineering, Mumbai, India

Abstract : This study has been undertaken to understand and fight against viruses using antivirus. Many antiviruses do remove the virus but take more memory, we are developing an antivirus that removes the virus without affecting the efficiency and speed of the computer. The antivirus also helps to show loopholes in computers.

***IndexTerms* – Virus, Antivirus, Computer, Program, Malicious Code.**

I. INTRODUCTION

A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document.

In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

Comprehensive virus protection programs help protect your files and hardware from malware such as worms, Trojan horses and spyware, and may also offer additional protection such as customizable firewalls and website blocking.

Data and Sources of Data

We have found from the study of a research paper made by Bhaskar V. Patil, Rahul J. Jadhav that, now a day’s computers are a very essential part of our life. In today’s world of extreme competition on the business front, information exchange and efficient communication is the need of the day. The internet is the highway that connects you to millions of computers together globally, forming networks in which any computer can communicate with any other computer as long as they are both connected to the internet. This fantastic world of computers and their worldwide network has been replete with incidences of malicious attacks of a virus created by people who get the thrills of spotting loopholes and making an entry into other computer systems. 'Virus' is a generic term for software that is harmful to your system. They spread via disks, a network, or via services such as email. Irrespective of how the virus travels, its purpose is to use or damage the resources of your computer. The history of the worst computer virus attacks dates back to 1998 and since then the world of computers has witnessed several computer attacks which were shocking in their times. Now (from 2010 onwards) computer attacks are not shocking anymore, the world of computers has learned to take into its stride computer attacks and has also learned to deal with malware. Viruses are classified as Compiled viruses, Boot Sector viruses, Interpreted viruses, Multi-partite Viruses, and Radio Frequency Identification [RFID] viruses. There are different computer viruses and their variants that are created and find their way into other computers through networks and media. But there is some mechanism to find particular viruses and their categories.

Theoretical framework

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are then said to be "infected" with a computer virus, a metaphor derived from biological viruses.

Computer viruses generally require a host program. The virus writes its code into the host program. When the program runs, the written virus program is executed first, causing infection and damage. A computer worm does not need a host program, as it is an independent program or code chunk. Therefore, it is not restricted by the host program but can run independently and actively carry out attacks.

Virus writers use social engineering deceptions and exploit detailed knowledge of security vulnerabilities to initially infect systems and spread the virus. The vast majority of viruses target systems running Microsoft Windows, employing a variety of mechanisms to infect new hosts, and often using complex anti-detection/stealth strategies to evade antivirus software. Motives for creating viruses can include seeking profit (e.g., with ransomware), desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, sabotage and denial of service, or simply because they wish to explore cybersecurity issues, artificial life and evolutionary algorithms.

Computer viruses cause billions of dollars’ worth of economic damage each year.

In response, an industry of antivirus software has cropped up, selling or freely distributing virus protection to users of various operating systems.

RESEARCH METHODOLOGY

Data and Sources of Data

We have found from the study of a research paper made by Muchelule Yusuf Wanjala & Neyole Misiko Jacob that, With the Internet as a major essential communication between billions of people and also a tool for commerce, social interaction, there are increasingly new threats in viruses as new unrecognized signatures are evolving for the antiviruses to detect during the scan. Anti-virus software uses a virus signature to find a virus in a computer file system, allowing to detect, quarantine and remove the virus. In the anti-virus software, the virus signature is referred to as a definition file or DAT file. Anti-virus software performs frequent virus signature, or definition, updates. These updates are necessary for the software to detect and remove new viruses. New viruses are being created and released almost daily, which forces anti-virus software to need frequent updates. The ability to detect heuristically or generically is significant, given that most scanners now include more than 250k signatures and the number of new viruses being discovered continues to increase dramatically year after year. Further, Landesman indicates that to maintain the highest level of protection, configure your antivirus software to check for updates as often as it will allow. Keeping the signatures up to date doesn't guarantee a new virus will never slip through, but it does make it far less likely.

Theoretical framework

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are then said to be "infected" with a computer virus, a metaphor derived from biological viruses.

Computer viruses generally require a host program. The virus writes its code into the host program. When the program runs, the written virus program is executed first, causing infection and damage. A computer worm does not need a host program, as it is an independent program or code chunk. Therefore, it is not restricted by the host program but can run independently and actively carry out attacks.

Virus writers use social engineering deceptions and exploit detailed knowledge of security vulnerabilities to initially infect systems and spread the virus. The vast majority of viruses target systems running Microsoft Windows, employing a variety of mechanisms to infect new hosts, and often using complex anti-detection/stealth strategies to evade antivirus software. Motives for creating viruses can include seeking profit (e.g., with ransomware), desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, sabotage and denial of service, or simply because they wish to explore cybersecurity issues, artificial life and evolutionary algorithms.

Computer viruses cause billions of dollars’ worth of economic damage each year.

In response, an industry of antivirus software has cropped up, selling or freely distributing virus protection to users of various operating systems.

Antivirus software, or antivirus software (abbreviated to AV software), also known as anti-malware, is a computer program used to prevent, detect, and remove malware.

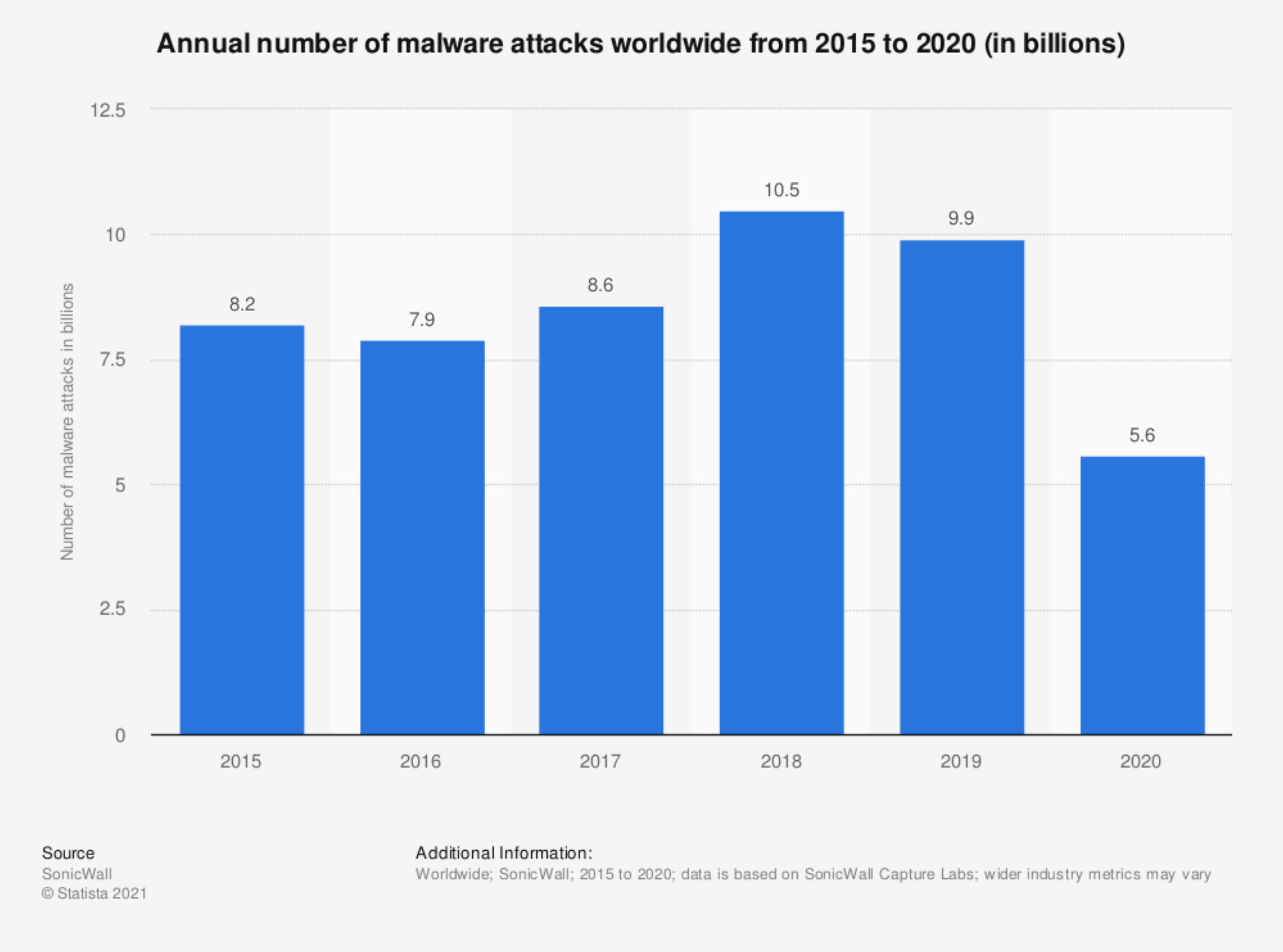
Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other malware, antivirus software started to protect from other computer threats. In particular, modern antivirus software can protect users from malicious browser helper objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, and worms, malicious LSPs, dialers, fraud tools, adware, and spyware. Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, advanced persistent threats (APT), and botnet DDoS attacks.

Descriptive Statistics

Key Malware Statistics

- 560,000 new pieces of malware are detected every day.
- There are now more than 1 billion malware programs out there.
- Every minute, four companies fall victim to ransomware attacks.
- Trojans account for 58% of all computer malware.

No lesson in the history of malware is complete without mentioning ILOVEYOU. This worm is considered the most destructive computer virus of all time. It did one very simple thing: It renamed all files "iloveyou" until the system crashed. While the exact scope of this attack was never revealed, analysts said it affected roughly 10% of all PCs around the world. The infamous ILOVEYOU virus caused $10 billion of damage when it struck in 2009.



Source
SonicWall
© Statista 2021

Additional Information:
Worldwide; SonicWall; 2015 to 2020; data is based on SonicWall Capture Labs; wider industry metrics may vary

The cybersecurity market has grown rapidly over the last few years. Annual revenues for security software across the globe reached an estimated $40 billion in 2020, with that number expected to reach $42 billion in 2021.

Cybersecurity software makes up a large percentage of total information security spending. Norton and McAfee, for example, generated $2.49 billion and $2.635 billion of revenue respectively in 2020.

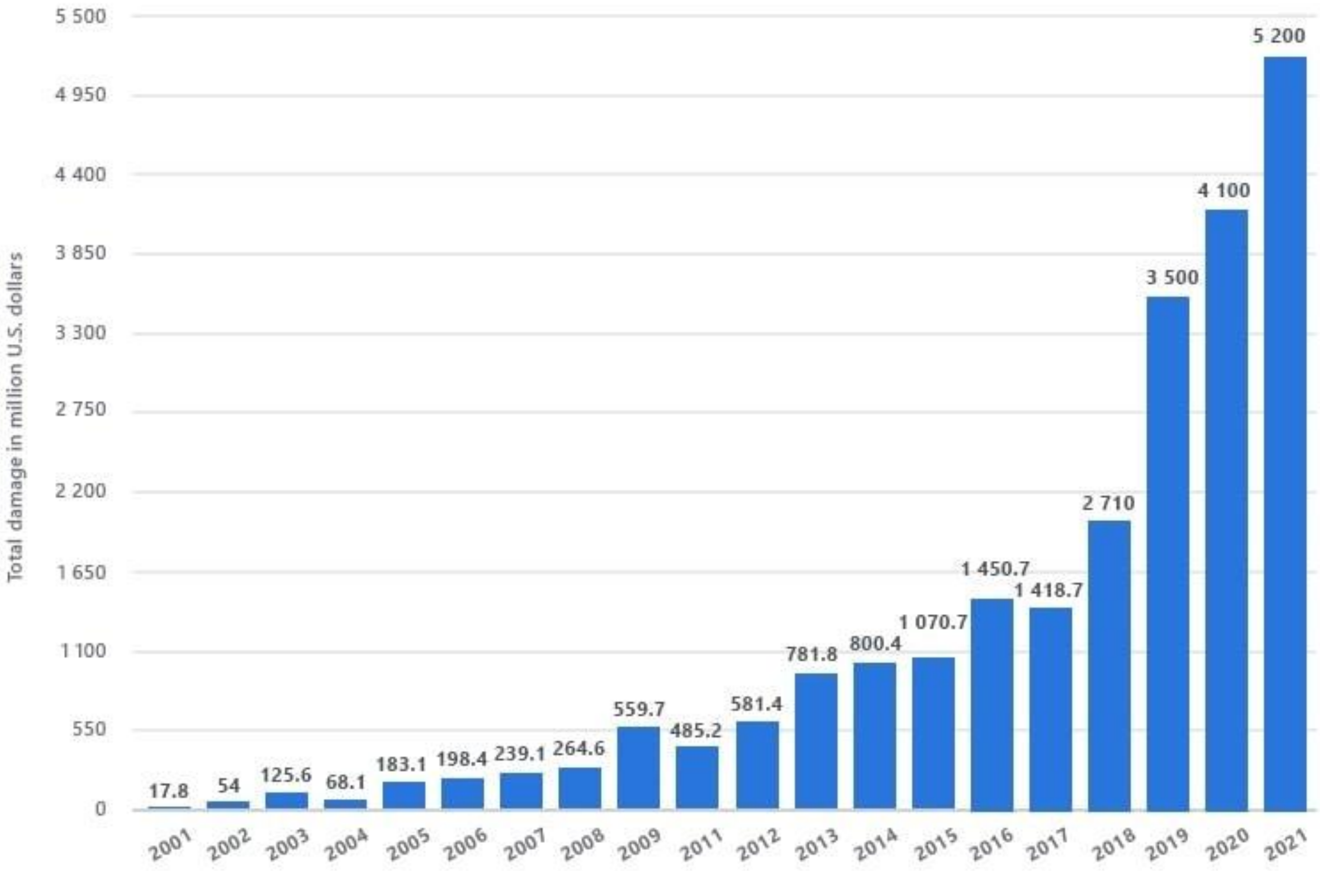
In terms of profit growth, however, most companies have plateaued in recent years, including names like Norton and Trend Micro. While IBM has shown a noticeable rise in profit in the past five years, the antivirus market is now taken up with free solutions like Microsoft Security Essentials, which collectively make up 30% of the market.

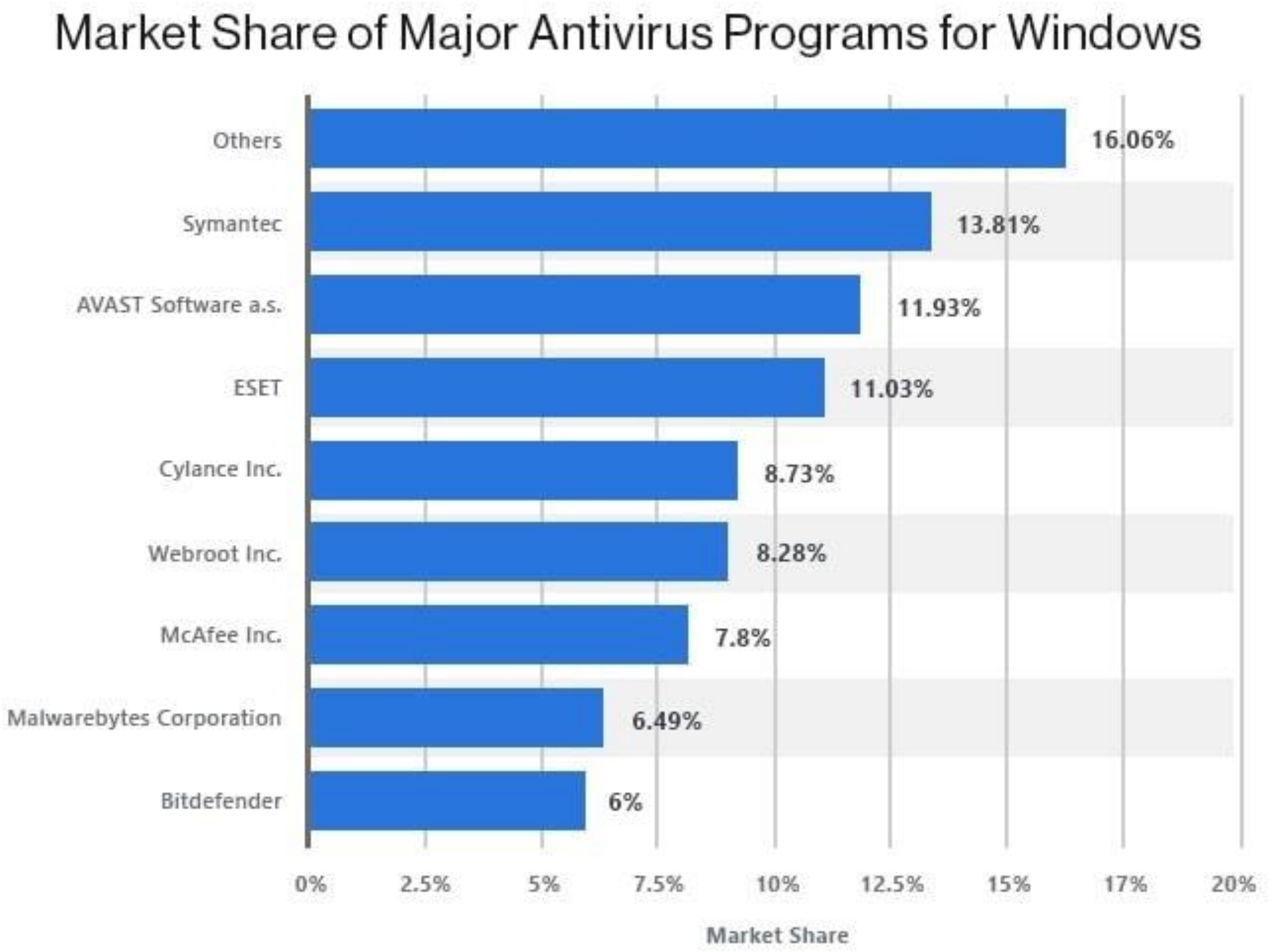
Many antivirus tests check for protection against:

- Zero-day attacks (viruses taking advantage of security holes before they are discovered and patched)
- Web and email threats
- Prevalent malware

Popular options like Bitdefender and Avira often combat as much as 100% against these attacks. Plus, most antivirus programs can run discreetly in the background without affecting the machine's performance.

Amount of Monetary Damage Caused by Reported Cybercrimes





II RESULTS AND DISCUSSION

In case your computer is attacked by a virus, it can affect your computer in the following ways:

- Slow down the computer
- Damage or delete files
- Reformat hard disk
- Frequent computer crashes
- Data loss
- Inability to perform any task on the computer or the internet

Antivirus software is like a ray of bright light in a world full of dark viruses. The number of advantages that they offer are countless. Some of the most prominent advantages are:

- Protection from viruses and their transmission
- Block spam and ads
- Defence against hackers and data thieves
- Ensures protection from removable devices
- Protects your data and files
- Supercharge your PC
- Firewall protection from spyware and phishing attacks
- Limit the access of websites to enhance web protection
- Keeping an eye on kids
- Protects your password
- Cost-effective

The following are time periods of evolution of Antivirus industry:

1949–1980 period	Pre-Antivirus days
1980–1990 period	Early days of Antivirus
1990–2000 period	Emergence of the Antivirus industry
2000–2014 period	Rise of Antivirus industry
2014–present	Rise of Next-Gen

III ACKNOWLEDGMENT

I would like to express my deep gratitude to Professor Nayna D., my research supervisor, for her patient guidance, enthusiastic encouragement and useful critiques of this research work.

I would also like to extend my thanks to the technicians of the laboratory of the Rizvi department for their help in offering me the resources in running the program.

Finally, I wish to thank my parents for their support and encouragement throughout my study.

REFERENCES

[1] Muchelule Yusuf Wanjala & Neyole Misiko Jacob. 2017. Review of Viruses and Antivirus Patterns. Global Journal of Computer Science and Technology.

[2] Bhaskar V. Patil, Rahul J. Jadhav. 2015. Computer Virus and Antivirus Software –A Brief Review. International Journal of Advances in Management and Economics.

[3] Martin C. Brown. 2018. Python: The Complete Reference.