ISSN No. 0976-5697

Volume 6, No. 7, September-October 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

The Best Antivirus, Antimalware Solution for Home Owners And Corporates

Nishant Patnaik

Editor-in-Chief,BiochemistryBlog.com,NeurophysiologyBlog.com
BiochemistryBlog.com.NeurophysiologyBlog.com
Varanasi,India

Abstract: This intends to analyse the best antivirus and antimalware for homeowners and corporates. To attain this goal, this paper will do an in-depth analysis on Kaspersky Anti-Virus/anti malware software that has been used to fight cyber threats for close to ten years now.

Keywords: Kaspersky Anti-Virus; Cyber threats; Virus; Malware; Computers.

I. INTRODUCTION

The increased use of computers and the internet has increased the number of cyber attacks experienced today. Since the advent of the internet age in the early 1980s, people are concerned with keeping the internet free from cyber attacks because they cause great damage when they can pass from one computer to another like a biological virus, thus infecting the system. Thus, a computer malware can be regarded as the undesirable embodiment of human intelligence to interrupt and to create a vacuum in the constant flow of internet information.

These attacks are as a result of malicious files and or threats such as virus, malware or Trojan horses [1]. For this reason, homeowners and organizations need to have antivirus and anti malware to help them protect their data from these malicious files. It is important to note that these attacks can cause huge losses when important data is breached by unauthorized persons or entities. They utilize various techniques to put their products out of sight of the scanners, because if antivirus programs can easily find their viruses, they cannot sufficiently spread far in the wild. Hence, there is a growing struggle to create new code evolution tactics to beat against the detectors.

However, there are many antivirus software that can be freely downloaded from various websites in the internet. These free antivirus software can help prevent a number of attacks from happening. Nevertheless, to fully protect computers and networks from these attacks, one needs to go for the best antivirus software in the market. One of the best antivirus in the market today is Kaspersky Anti-Virus. This software has been used for close to ten years now and it has proved to be reliable in protecting computers from viruses and malware [2].

II. EVOLUTION OF COMPUTER VIRUSES

Since the advent of the internet age in the late 1980's, traditional computer viruses were mostly first seen. The first and the most important reason was due to the spread of personal computers which had become common in homes and organizations. Another reason that led to the evolution of computer viruses in the late 1980s was the use of bulletin boards on the computer which led to the creation of more viruses and is now famously known as the Trojan horse. Moreover, the use of floppy disk at the time led to the rise of computer viruses. All kinds of data could easily fit on a single floppy disk and become transferred to other computers, subsequently leading to the spread of computer viruses.

Technical experts have tried to make an economic, ethical and moral sense of the worm unleashed by Robert Morris that invaded ARPANET computers. The small program that Morris created disabled about 6,000 computers on the network by flooding their memory banks with copies of itself. This and all other similar attacks on the internet has helped “to generate a moral panic that has all but transformed the everyday “computer culture”[3].

III. CONCEALMENT CLASSIFICATIONS

Computer malwares can be classified according to their different characteristics, such as classification by target, infection mechanism among others. One of these classification types is according to concealment techniques employed.

Encrypted Viruses

Encryption is practically the most primitive approach to take cover the operation of the virus code [4]. The ultimate aim of encrypted viruses is change of the virus body binary codes with some encryption algorithms to hide it from simple view and make it more difficult to analyze and detect [5]. The first encrypting virus, CASCADE, appeared in 1988 [6].

Normally, encrypted viruses are made of two key parts: the encrypted body of the virus, and a small decryption code piece [7]. When the infected program code gets to run, firstly, the decryption loop executes and decrypts the main body of the virus. Then, it moves the control to the virus body. In some viruses, decryption loop performs something more, in addition to its main task. For instance, it may calculate the checksum to make sure that the virus code is not tampered, but as a general principle, the decryptor should be created as small as possible to avoid the anti-virus software, which is trying to exploit the decryptor loop's string pattern for scanning purpose.

Encryption hides the virus body from those who like to view the virus code or tamper the infected files using code viewers or hexadecimal editors [8]. However, virus programmers use the encryption for some reasons. Four of the major motivations as described, as in [7] are:

1. **To avoid static code analysis:** Some programs try to analyze code automatically and generate warning if suspect code is found. Encryption is used to disguise suspicious codes and prevent static analysis.
2. **To delay the process of inspection:** It can make the analysis process a bit more difficult and time-consuming, however it usually can increase the time of process only a few minutes.
3. **To prevent tampering:** Many new variants of a virus can be produced with a minor change in the original virus code. Encryption makes it difficult to change the virus by non-experts.
4. **To escape from detection:** an encrypted virus cannot be detected through simple string matching before decryption, because only decryptor loop has identical string in all variants. Hence, signature for an encrypted virus is limited and must be selected precisely.

Oligomorphic viruses are willing to substitute the decryptor code in new offspring. The easiest method to apply this idea is to provide a set of different decryptor loops rather than one. Signature based detection depending on byte pattern of decryptor, though it is a achievable solution, but it is not a practical way, as in [4]. Therefore, oligomorphic viruses make the detection process more difficult for signature based scanning engines.

Polymorphic Virus

The most usual approach developed in anti-virus softwares and tools to identify the viruses and malwares is signature-based scanning [9]. It makes use of small strings, named as signatures, results of manual analysis of viral codes. A signature must only be a sign of a specific virus and not the other viruses and normal programs. Accordingly, a virus would be discovered, if the virus related signatures were found. To avoid this detection, virus can change some instructions in new generation and cheat the signature scanning. Polymorphic viruses exploit this concept. When the virus decides to infect a new victim, it modifies some pieces of its body to look dissimilar. As encryption and oligomorphism, scheme of polymorphism is to divide the code into two sections, the first part is a code decryptor, which its function is decryption of the second part and passes the execution control to decrypted code. Then, during the execution of this second part, a new different decryptor will be created, which encrypts itself and links both divisions to construct a new copy of the virus [10].

In fact, polymorphism is a newer and progressive variety of oligomorphism. Concerning of encryption, polymorphic virus, oligomorphic and encrypted viruses are similar, but the exception is the polymorphic virus has capability to create infinite new decryptors [11]. Polymorphic virus exploits mutation techniques to change the decryptor code. Furthermore, each new decryptor may use several encryption techniques to encrypt the constant virus body, as well.

Oligomorphic Virus

Although virus creators attempted to conceal the first generation of viruses with encryption methods, the decryptor loops were remained constantly in new infected files, so anti-virus software normally had no trouble with such virus that was inspected and for which a signature string was obtained. To overcome this vulnerability, virus writers employed several techniques to create a mutated body for decryptors. These efforts caused the invention of new type of concealment viruses, named as oligomorphic viruses.

Metamorphic Virus

Virus writers like to make the lifetime of their produced viruses longer, so they constantly challenge to make the detection as more difficult as possible for antivirus specialists. They have to spend a plenty of time to produce a new polymorphic virus that it may not be able to spread out broadly, but an anti-virus expert may handle the detection of such a virus in a short time [12].

Even for the most complicated polymorphic viruses, after code be emulated sufficiently, the original code will become visible and can be detected by a simple string signature scanning [13].

The shortest definition of the metamorphic virus, as in [11] defined by Igor Muttik, is "Metamorphics are body-polymorphics." Because metamorphic viruses are not encrypted, they do not require decryptor. Metamorphic virus is similar to polymorphic virus in aspect of making use of an obfuscation engine. Metamorphic virus mutate all of its body, rather it changes the code of decryption loop. All possible techniques applicable by polymorphic virus to produce new decryptor can be used by a metamorphic virus on whole virus code to create a new instance.

IV. HOW KASPERSKY WORKS TO PROTECT COMPUTERS

Kaspersky is developed to work in three ways to protect computers from malicious malware. These three methods include:

Full System Scans
Background Scanning
Virus Definitions

The Full System Scans occurs when the antivirus software scans all files and documents in a computer or a network. It involves going through all the files one by one in search of any virus or malware in the computer drives. Normally, full scans are not necessary when a computer has an on access virus scanning facility, as in [2]. These scans are normally essential when one installs the Kaspersky antivirus for the first time or when one updates the antivirus software. This procedure is generally done to ensure that there are no malicious files hidden somewhere in the system.

Background Scanning occurs when Kaspersky antivirus software scans all files that are opened from the back-end. Normally, this is referred to as an on access scan. The importance of this scanning is that it offers a real time protection thereby protecting a computer from malicious attacks.

Virus Definition is very important as it enables the antivirus software to define the malware or virus infecting the system. This is the main reason why Kaspersky software needs frequent updating to help the software to detect and define new threats to the system.

V. WHERE TO BUY KASPERSKY ANTI VIRUS

A. *Kasperskey shops:*

One can visit the nearest Kaspersky shop in town and buy a hard copy file. Generally, one is given a CD to use in installing the antivirus software into their computer system.

B. *Buy online*

One can visit the Kaspersky Lab website and purchase a copy of the antivirus online. After ones payment has been confirmed, one receives an installation link through their emails. This link enables one to install the software in their system.

VI. CONCLUSION

The above discussion shows that Kaspersky antivirus can be used by households and business organizations to protect their computer systems as well as other computer networks. This protection is very vital to any computer user in that it will enable them to protect their important data as well as information [14]. It is important to mention that Kaspersky software may have some drawbacks such as slowing the computer’s speed especially during the full scans. However, the advantages of the software outweigh the drawbacks.

VII. REFERENCES

[1] Bachaalany, E., & Koret, J. (2015). The Antivirus Hacker's Handbook. New York, NY: John Wiley & Sons. P 14-75.

[2] McBrewster, J. (2014). Kaspersky Anti-Virus: Antivirus Software, Kaspersky Lab, Malware, Computer Virus, Trojan Horse (computing), Computer Worm, Spyware, Adware, Keystroke Logging. New York, NY: Alphascript Publishing. P 25-98.

[3] A. Ross, "Hacking away at the Counterculture," http://www.3.iath.virginia.edu/pme/text-only/issue.990/ross-1.990.

[4] Szor, P. (2005). The Art of Computer Virus Research and Defense, Addison-Wesley Professional, Reading.

[5] Aycock, J. (2006). Computer Viruses and Malware, New York, NY, USA: Springer.

[6] Beaucamps, P. (2007). "Advanced Polymorphic Techniques", International Journal of Computer Science, **2(3)**, 194-205.

[7] Skulason, F. (1990). "Virus Encryption Techniques", Virus Bulletin. P 13-16.

[8] Johansson, K. (1994). Computer Viruses: The Technology and Evolution of an Artificial Life Form.

[9] Zhang, Q. (2008). "Polymorphic and metamorphic malware detection", Ph.D. Thesis, Graduate Faculty, North Carolina State University, Raleigh, NC, USA.

[10] Bonfante, G., M. Kaczmarek, and J.Y. Marion. (2005). "Toward an Abstract Computer Virology".

[11] Szor, P. and P. Ferrie. (2001). "Hunting for Metamorphic", 11th Virus Bulletin International Conference. P 123-144.

[12] Szor, P. (2000). "The new 32-bit medusa", Virus Bulletin. P 8-10.

[13] Jordan, M. (2002). "Dealing with Metamorphism", Virus Bulletin. P 4-6.

[14] Stelzhammer, P. (2015). Free Antivirus And Its Market Implementation: A Case Study Of Qihoo 360 And Baidu. Chicago, IL: BoD – Books on Demand. P.36-85