An Investigation of the Efficacy of the Off-the-Shelf Malware Scanners and Combination Techniques

Ibrahim Ejdayid A. Mansour

***Abstract*—I was intrigued by the Antivirus term, how it works„ whether its designers understand the operating system more than the operating system vendors or not as well as the big question of how safe we are in practice because we are really rely on this term to protect all sort of businesses including web servers in which the eGovernment website is hosted, and many more questions I asked at the time. Also, Tanebaum in 2009 describes the contemporary operating systems as massive, inflexible, unreliable, unsecured and loaded with bugs, and that has been happening with the very presence of antivirus and their vendors who claim 100% protection against the variously clever malware. [4]**

All of that was the real motive behind conducting this paper to evaluate the practical level of protection that the commercial antivirus provides by designing an empirical test. Not only testing them generally, but also, making a design-based comparison between them, but calling it antivirus should have been changed for a while because it does not quite cover the contemporary malicious software, which includes more than just viruses. On account of this, this project will call it on a malware scanner as many professionals do so.

To conclude, it was found that there is remarkable disparity between the malware scanners' capabilities and the advertised ones. Also, the conventional design of the malware scanner was proved to be ahead of the combination technique that many security vendors have been using to design their own scanners. The other interesting fact according to today experts is that even security vendors are selling pitches because it is mere business, so they cannot be trusted blindly.

***Index Terms*— Malware scanners, combination techniques, DDOS**

I. Introduction

Recently, the growing malware number has reached frightening statistics. Therefore, it is crucial to work out the practical ability of the presence day malware scanners, then only we can surf the internet and provide our private information in a more confident way without being rather paranoid.

This paper not only evaluates the scanners generally, but also looks at the relatively new design of combing various scanners'engines to come up with a possibly better defending technique, also, the evaluating test is designed to be applicable to different scanners as well as being robust, repeatable and universal. Furthermore, Silberschatz et al said in 2009, "a properly designed operating system must ensure that an incorrect or malicious program cannot cause other programmes to execute incorrectly". [5]
Basically, this search aims to:

Manuscript received August 10, 2012; revised September 25, 2012.
Ibrahim Ejdayid A.Mansour is with The College of Electronics Technology, Libya (e-mail:ibraheem_1887@yahoo.com).

- Designing the testing methodology and referenced it to the AV-Comparative methodology.
- Defining the combination technique used in designing the scanner.
- Putting forward the scanners' scores and ordering them from the best to the less.
- Summarising the project outcome to the normal reader by generating a free-jargon article.

Finally, Modern businesses rely heavily on their digitized data and computer systems, and protecting them is essential. The digital world can be a dangerous place.

According to the 2008 Computer Crime and Security Survey, 50% of the surveyed organizations have been affected by a malware attack at least once during the previous twelve months [1]. A 2008 study by the UK government revealed that it took large British companies about two days as well as an average cost of £80000 - £130000 [2] to recover from security breaches - about 40% of the breaches caused by malware or malicious software. Yet, 97% of those organizations have Anti-virus software installed [1].

II. The Preparation Stage

This experiment has to be universal and repeatable to give it credibility and make it a robust test, but before going into details, I will mention the Malware Scanners (Antivirus), which were tested:

1) Avast Free Antivirus 5.0.462
2) AVG Antivirus 9.0.829
3) BitDefender Antivirus 2010
4) eScan Antivirus Edition 10.0.1058.677
5) F-Secure Antivirus 2010
6) G Data Antivirus 2010
7) TrustPort Antivirus 2010 5.0.0.4111
8) ESET NOD32 Antivirus 2010
9) Kaspersky Antivirus 2010
10) Symantec Norton Antivirus 2010

The different approach in testing those malware scanners which might give the edge over some previous research that carried out an evaluating test is comparing the multi-engine scanners to the single-engine scanners, but first of all, what those two terms mean:

The single engine scanner which has had its own engine since the scanner was profound, for example:

- Avast, AVG, Avira, Kaspersky, ESET, BitDiffender, McAfee, Norman, Mirosoft Essentials, Kingsoft and there are still more of them, but they are less known.

The multi-engine scanner which is not very known, even though many people have been buying them and what more even many security professionals have not heard of this term. Basically, those scanners either use single engine scanners'

engines beside their own engines or they just use others' engines only. For instance:

- F-Secure: it is a multi-engine security product, it uses a range of engines including BitDefender and it used to incorporate Kaspersky's engine into their own engine.
- G Data: it combines Avast and BitDefender engines to strengthen its detection rate and gives it the edge over the other products.
- TrustPort: another multi-engine scanner which incorporates other scanners' engines, yet it does not have its own engine. This product by default uses BitDefender as well as AVG and there are other engines that available and can be chosen by the user.
- Lastly, eScan: it uses a combination of engines as well, but the vendor repeatedly refused to give away any information concerning which engines they employ.

On account of this, the criteria in choosing the products that it is needed to test was comparing four multi-engine scanners with the single scanners that incorporated into the multi ones as well as comparing both of them with the top three scanners in 2009 according the AV-Comparative Organization, consequently, the products are:

- eScan Antivirus Edition 10.0.1058.677 (Multi-engine)
- F-Secure Antivirus 2010 (BitDefender)
- G Data Antivirus 2010 (Avast and BitDefender)
- TrustPort Antivirus 2010 5.0.0.4111 (AVG and BitDefender)
- And the top three winners in 2009 [3] were:
- Symantec Norton Antivirus 2010
- Kaspersky Antivirus 2010
- ESET NOD32 Antivirus 2010

III. The Malware Samples Used

Those are the malicious software samples used to test the malware scanners efficiency to catch up the potential threats.

Backdoors:

- Backdoor.BAT.Comlabat.04.zip
- Backdoor.Win64.BotNet.a.zip
- Backdoor.VBS.Cimv.a.zip
- Backdoor.Win16.Intruder.zip

Rootkits:

- Rootkit.FreeBSD.Agent.a.zip
- Rootkit.Win32.Fu.zip
- Rootkit.Win32.Delf.aj.zip
- Rootkit.Win32.kernelBot.a.zip

Spam tools:

- SpamTool.Win32.Agent.af.zip
- SpamTool.Win32.Blen.ab.zip
- SpamTool.ICQReg.b.zip
- SpamTool.Win32.Mailbot.bj.zip

Trojans:

- Trojan.Lotus123.Winstart.zip
- Trojan.Win32.AF.20.zip
- Trojan.OLE2.FormatC.a.zip
- Trojan.ZIP.Fakecmos.zip
- Trojan-Spy.VBS.Liorra

Viruses:

- Eicar.com
- Eicar_com.zip
- Eicarcom2.zip
- Virus.1C.Tanga.a.zip
- Virus.BeOS.Kate.zip
- Virus.Script.ASX.Conp.zip

Worms:

- IM-Worm.BAT.Venez.a.zip
- IM-Worm.VBS.Skypper.a.zip
- IM-Worm.Win32.Silewar.zip
- IM-Worm.Win32.Vizim.a.zip

Using samples of Potentially Unwanted Applications (PUA) an unknown threats and observe how each scanner will behave in such instance. In the following list, there are the samples of PUA used in the test:

- Aik_trail
- EUE.5.50.2136
- fdminst
- Himalaya1973
- Sdsetup
- Siinst
- STOPzilla_Setup
- UniVerShieldv4.2
- Everestultimate550
- Norton_Utilities_14.5.0.118_Portable
- Fortiengia_Portable.Everest.Ultimate. .v5.00.1673
- Everestultimate.4.60.build.1639.Incl.key.7z

Turning to how many false alarms a particular scanner generates, a set of Hoaxes employed to achieve this target. Obviously, the false alarm in computer security is just as destructive as the real ones. The approach here to find out how those scanners will react and categorize hoaxes. Here is list of six different hoaxes (jokes or not viruses) that used in the evaluation:

- Hoax.MSWord.BadJoke.Auge.zip
- Not-virus_BadJoke.Win32.Agent.zip
- Not-virus_BadJoke.Win32.SwapMouseButton.b.zip
- Not-virus_BadJoke.Win32.Wall.a.zip
- Not-virus_Hoax.Win32.BadJoke.Delf.bd.zip
- Not-virus_Hoax.Win32.VB.ad.zip

IV. The Test Outcomes

The test was carried out on four stages and summarised the results to know the top three winners and then compare them to AV-Comparative results of 2009.

The first stage was measuring the computer performance before and after having the scanner installed and the test includes, benchmarking the machine memory (RAM), converting audio files, copying large files and installing certain applications.

The second stage was exploring the scanner to know its

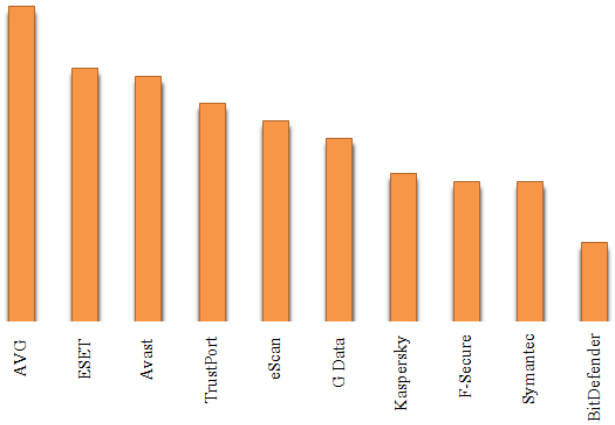
features, which areas it protects, does it have a real time protection and whether it offers any additional free utilities, such as online free removal or not .

The third stage was evaluating the scanner speed by measuring how fast the scanner to perform, a quick scan, a full scan, customised scan and whether it scans a specific areas and has a boot scan or not.

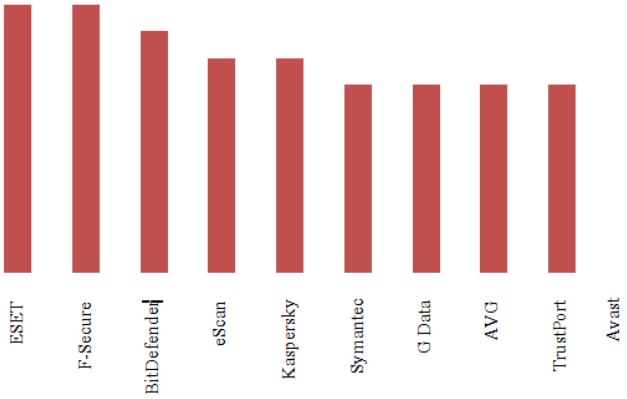
The fourth stage was evaluating the scanner effectiveness by testing its detection ability, how accurate it describes the sample and whether it deletes the sample or quarantine or repairs the infected files or it can do nothing.

Now, it is time to see how well those scanners did in the evaluating test and the result was in awarded points, so the higher is the better.

- Performance:

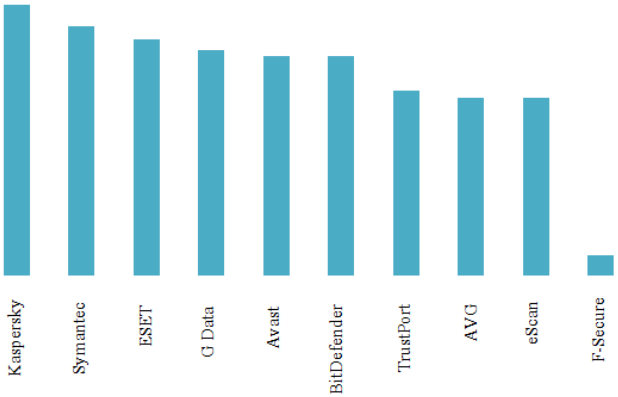


- Scanner's feature and its additional free utilities:

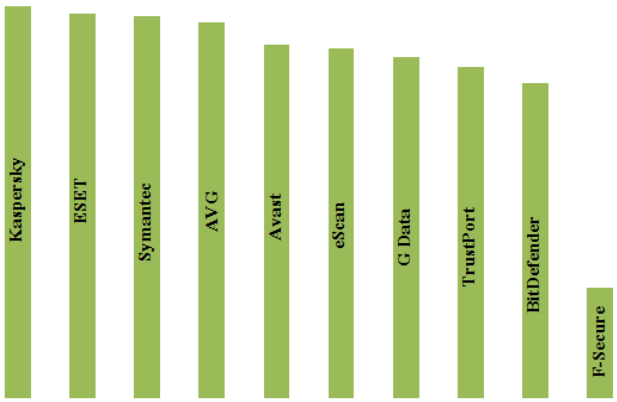


- Scanning speed

- Effectiveness



- The overall score



The scanner	The score achieved
Kaspersky	*124*
ESET	*122*
Symantec	*121*
AVG	*119*
Avast	*112*
eScan	*111*
G Data	*108*
TrustPort	*105*
BitDefender	*100*
F-Secure	*35*

V. Conclusion

Having seen the outcomes of the test, it would be advisable to the end user to become more cautious and rather paranoid when it comes to dealing with the internet and removal storage media, personally speaking, the computer users should be so because you never know whether your computer is a part of botnet or even your computer is a zombie used in conducting a distributed denial of service attack (DDOS) and that makes any eGovernment at real risk. There is no such a thing as 100% level of protection and there are more:

1) Many scanners have features that are not default, whereas the internet security versions of the same scanners have them as default, they only need to be reconfigured.

2) The security product vendors not only are designing the scanners, but also they are selling pitches.
3) The scanners always need to reconfigured for a reason or another, so I am wondering to what extent the home user can cope with activating a missing feature or setting up a password for the scanner, for example.
4) Many scanners missed many malware samples, yet those samples are pretty well-known. Therefore, can those scanners deal effectively with the unknown?
5) Many experts do not know why they are using a certain scanners as well as they do not know much about a combination technique, so how the end user would know how to choose the best scanner.
6) The novel comparison between the various scanners' design might give the enhancement and the uniqueness to this paper.
7) It has also proved that the multi-engine scanners among the good one, yet they are not among the best.

REFERENCES

[1] 7safe (n. d.) 7safe.com. [Online]. Available: http://www.7safe.com/breach_report/.
[2] GFI Software (n. d.) GFI.com. [Online]. Available: http://www.gfi.com/whitepapers/why-one-virus-engine-is-not-enough.pdf.
[3] AV-Comparatives (n. d.) comparativesreviews. [Online]. Available: http://www.av-comparatives.org/comparativesreviews.
[4] VX Heavens (n. d.) VX Heavens. [Online]. Available: http://vx.netlux.org/.
[5] A. Tanenbaum, *Modern Operating Systems*, 2nd edn.. Upper Saddle River NJ: Prentice Hall, 2009.
[6] A. Silberschatz, *Operating System Concepts*, 8th edn , Hoboken, N.J: John Wiley and Sons, 2010.

Ibrahim Ejdayid A. Mansour became a lecturer assistant at the College of Electronics Technology in Bani Walid, Libya. He was born in Zamem Valley, Sirte in September, 1979 and having had finished his secondary education at the local village high school, he moved to the College of Electronics Technology and achieved an BSc degree in computer engineering in 2002. In November, 2010, he earned a master degree in nework computing at Coventry University in the UK with a Distinction level and won the faculty special prize. From 2002 to 2004, he worked as a Lab engineer at the Electronics technology as well as having taught computer science at the village high school, starting from mid 2004, he assigned as a IT technician at the major electricity company in Libya, which abbreviated as Gecol and very soon in 2005, he had promoted as the Heaed of IT Documentation Department, but in the remarkable change in his career was to be positioned as the Manager of IT bureau in Sirte city area. Granting a scholarship from the Gecol Company in late 2008, he finished off his master degree in the UK, from 2008 until 2010. For the sake of pursuing his interest in Networking Security and Cloud Computing, Ibrahim has become a Cisco Computer Network Associate Instructor in Bani Walid Cisco Academy in June, 2012 as well as his CCNA Security and CCDA in progress and hopefully will get them very soon. Working in many places has given him the solid experience in various Microsoft systems, database applications and CompTIA A+, Network+ and security+.