Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications

Journal homepage: www.akademiabaru.com/arca.html
ISSN: 2462-1927

Open Access

Experimental Analysis of Trojan Horse and Worm Attacks in Windows Environment

Abidah Mat Taib[1,*], Nurul Nabila Khairu Azman Azman[2]

[1] Department of Computer Science, Faculty of Computer and Mathematical Sciences Universiti Teknologi MARA, 40450 Shah Alam, Malaysia
[2] Faculty of Education, Universiti Teknologi MARA, 40450 Shah Alam, Malaysia

ARTICLE INFO

Article history:
Received 5 March 2018
Received in revised form 12 April 2018
Accepted 10 July 2018
Available online 4 August 2018

ABSTRACT

Trojan Horse is the most powerful malware that can produce an attack to penetrate into the network environment. Besides Trojan, another harmful malware known as Worm also can cause enormous damage to the computer system. Unfortunately, some users do not concern much on security because they thought there is not much valuable information can be obtained from them. The lack of awareness about computer and network security as well as misunderstanding of how malware attacks can occur, resulted in these users do not realize that their machines are at risk and they are exposed to several kind of potential cyber threats. Thus, this paper provides an insight on network vulnerability and presents some demonstrations of Remote Access Trojan (RAT) attack and worm file duplication attack via experimental tesbed. Then, Wireshark and some malware scanning tools such as Virus Total, MalwareBytes and Avast AntiVirus were also used for malware detection. The findings show that these attacks are possible and can be easily conducted to meet the purpose of the attackers. Therefore, educating the public to pay extra concern on malware vulnerabilities and to equip themselves with knowledge and skills to face the security challenges due to malware attacks is crucial.

Keywords:
Remote Access Trojan (RAT), vulnerability of operating system (OS), malware activity, worm attack, cyber threat

1. Introduction

1.1. Overview of Network and Computer Security

Network security and the computer security are two complementary elements that must be prioritize in a certain network [1]. In order to have a secure transmission of the information between one computer to another, the concept of network security must be applied. The computer users should concern about the levels of the security defense of their computer or personal computer (PC) so that their PC will always be in a good state. In addition, without the security aspects, there are many violent cases such as virus attacks may arise.

[*] *Corresponding author.*
E-mail address: Abida Mat Taib (abby4108@gmail.com)

The security of the computer includes the hardware, software and its internal. Thus, maintaining the physical scope such as the monitor, Central Processing Unit (CPU), keyboard, mouse and many more must be handled with care because without supervision, the culprits could easily took an advantage. On top of that, the supervision towards the software, the handling of input to the computer system, and an ethical usage of information over the internet must be considered.

However, many cases of computer security nowadays are related to the malware attacks [2]. The new technologies that have been developing years by years may not resistance to malwares that potentially introduce more new attacks towards the computer. Fewer defences towards computer will make the fraud or the culprit easy to take over the computer system. Threats such as malware will arise to exploit the vulnerabilities in the system that is seen as originally safe. Thus, with the rise of the digital shadow economy [3], malware is no longer used only to make the system going wrong, but now it is used as a tool for the criminals to make their own profit, as well as the opportunity to access to valuable digital, financial resources and/or databases.

The malware that break into the system can do many bad things such as steal the information, change the information of the file and also camouflage as a clean file. The malware types comprise of Ransomware, Adware, Spyware, Rootkits, Keylogger, Worms and also Viruses [4]. These different kinds of malware have their own kind of ways to intrude into the system [5]. Each of them also has their own strength and weaknesses [6]. However, Trojan malware has the highest rate of capability in attacking into the computer system.

Trojan attacks are the attacks that were commonly found in the computer system nowadays [7]. The Trojan can appear in many different types of file formats such as the document, applications, pictures or binary code. There are many types of Trojan that exists and each of them had their very own way of attacks [8]. The Trojan attack also may be in a silent mode until no one has noticed that there is an attack [9]. Trojan also can work by hiding itself inside a useful software program and can do many corruptions towards the computer system [10].

For instance, Remote Access Trojan (RAT) is capable to control the victim's computer system without being traced [11]. This is possible because RAT will act as a server and listened to the port that is not available to the internet attackers. These Trojans commonly hide in games or other programs, thus escape from being suspicious by the users. On the other hand, Worm is commonly used by the attackers to intrude into the computer system. Most worms send themselves through email, which cause fast spreading as they can email to every address in a particular mailbox. Moreover, the worm itself acts as an executable program that can infect the other file on the computer system.

Malware attacks are the problems that still exist because the new malware samples are being created by the malware's writer year by year [2]. Although there are some malware tools and also techniques that have been used by the researchers, it is still not enough to make sure that the computer users are free from malware infections [12]. Malware also have their own capabilities to do any illegal activities towards that infected PC. The infected PC may contain vulnerabilities such as buffer overflow, decoding errors, poor handling of malformed data and sabotaged configurations. Cases regarding the infected PC because of malware attacks are increasing enormously from time to time [13].

However, the users' ignorance towards the computer security makes the problem still continue and getting worse. Many previous researchers found that most of the security cases regarding malware infected PC was because of the user's attitude itself [9]. Most of the computer users do not care about their computer security, the antivirus they need to use and also their computer system.

If this malware attack problem is not being taken care with an effective way, many users will have problems regarding to the infected PC [14]. The user's personal data and information that stored in their PC also will be in danger. Therefore, it is crucial for the users to be aware of the impact of malware attack and be educated about detecting existence of malware and preventing its potential attacks. Hence, this paper presents an insight on the analysis of Trojan and Worm attacks in Windows environment, particularly due to RAT and worm that spread via email.

1.2 Related Work

Windows operating system has highest number of users rather than Mac OS, Linux and FreeBSD [15]. It is mostly chosen because it is user friendly, easy to use and quickly learned by the beginner. Unfortunately, Windows OS has some vulnerabilities that include lack of personal firewall and malware protection, weak Windows security policy as well as insecure files and share permission.

Besides detecting the presence of Trojans, preventing the Trojan attacks is also important. Prevention can be done via internal and external aspects. Internal aspect means the computer itself while the external aspect is the environment outside the computer [2]. Both of these aspects must be prioritized so that the Trojan attacks problem can be mitigated. However, according to [7], these two aspects are the users and the computer network. Users are responsible to maintain the computer’s system from being infected by any attacks especially the Trojan attacks.

Meanwhile, the security of computer network must be appropriately administered to ensure it is always ready to combat potential attacks. Thus, educating the users about malware attack and acquiring knowledge and skills to deal with it are vital. Hopefully, the presentation of this paper contributes to provide insight and create awareness among computer users. Consequently, the users will know the effects of Trojan and Worm on their PC and take prevention steps accordingly.

2. Methodology

The experimental testbed was setup to demonstrate the potential malware attacks in Windows environment and carried out the analysis. The conducted experiments include RAT attack and worm attack that are explained subsequently in the next section.

2.1 Experimental Setup

The experimental testbed setup consists of the hardware arrangement according to the topology created in Figure 1. The testbed comprises of two laptops connected to the LinkSys Wireless-G Broad Router using Cat6e UTP cable. The LinkSys Wireless-G Broad Router can be setup as a wired or wireless. In this experiment, wired medium had been chosen for the router setup because wired medium has higher speed and less interference compared to wireless medium. The router was connected to internet via UiTM Perlis network by using Cat6e UTP cable.

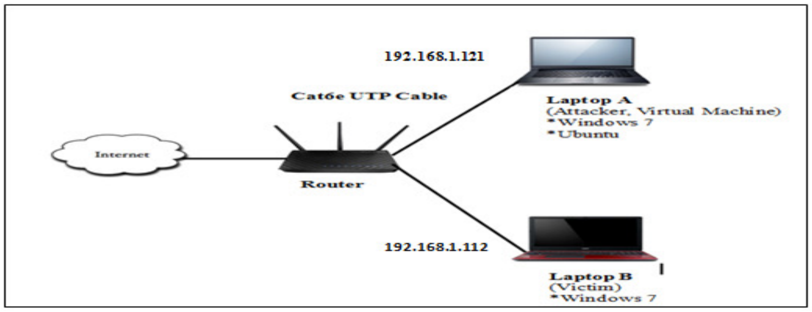


Fig. 1. Testbed Setup

A quick installation was done on the router to configure its basic functions. The router control panel's page was opened from the browser. The browser used is Google.com. The router control's panel can be opened by typing the IP default gateway in the web browser. Username and password were required to access into the configuration utility. After the log in process was successful, quick setup was chosen from the menu of the configuration utility in the router's control panel in the web browser.

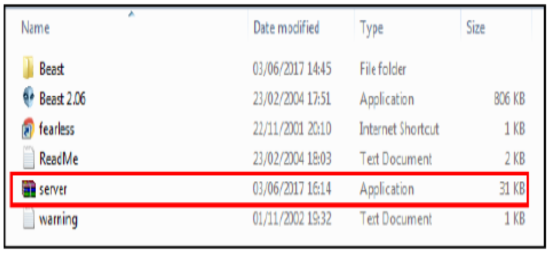
After configuring the router, Virtual Box installation was done on Laptop A. Laptop A operated as guest in Microsoft Windows 7 and acts as an attacker. Laptop B operated in Microsoft Windows 7 and acts as a victim. The connectivity testing was successful since Laptop A can ping to Laptop B and vice versa. IP address 192.168.1.121 owned by attacker's laptop and IP address 192.168.1.112 owned by victim's laptop.

As for malware detecting purposes, several tools including Wireshark, Virus Total, Malwarebytes and Avast antivirus were also installed on the victim's laptop. Wireshark is needed because it can capture the packet and analyse the traffic. Wireshark and WinPcap were installed and run in Laptop A and Laptop B in order to capture live network data. Virus Total is an online virus scanner that allows the user to pick any file that they want to scan. The file will be scanned whether it contains any harmful virus or not. VirusTotal scanner can be used by using webpage from www.virustotal.com. MalwareBytes is an anti-malware software that is built for Microsoft Windows, MacOS and Android OS. This software can be used to find and remove the malware detected. Avast AntiVirus is a software that can detect any unwanted virus or malware in the computer. It will block the virus, malware or Trojan from entering the computer system. Avast AntiVirus has built-in Apps for Windows, MacOS and also Android.

Two scenarios that were performed in this experiment are the Remote Access Trojan (RAT) attack and Worm attack.

2.2 RAT Attack

For this experiment, Beast which is a Remote Access Trojan (RAT) is used as a Trojan's attacking tool in Windows. Beast was installed in Laptop A which is the attacker's laptop so that the Trojan attacks can be sent to the Laptop B. Beast installer has been downloaded from https.connect-trojan.net/2009/10/beast-2.05.html. Beast formed the RAT Trojan and launched an attack by using the created RAT itself. Figure 2 shows the RAT file, named "server", that had been created in the attacker's laptop. The attacker will send the created RAT file to the victim via email. Before the attacker sends the Trojan via the email, the attacker must convert the RAT file "server" into jpg file. Figure 3 shows the RAT file "server" that had been renamed into "application" and in jpg file format.



Name	Date modified	Type	Size
Beast	03/06/2017 14:45	File folder	
Beast 2.06	23/02/2004 17:51	Application	806 KB
fearless	22/11/2001 20:10	Internet Shortcut	1 KB
ReadMe	23/02/2004 18:03	Text Document	2 KB
server	03/06/2017 16:14	Application	31 KB
warning	01/11/2002 19:32	Text Document	1 KB

Fig. 2. Trojan File

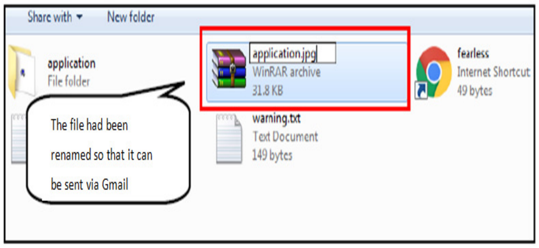
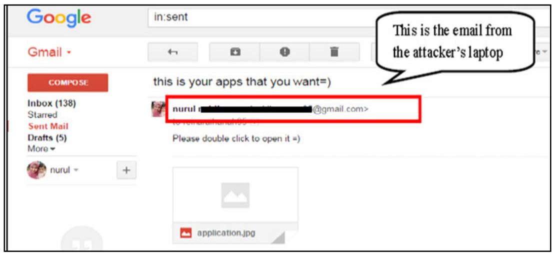


Fig. 3. Rename the Trojan file

By renaming and converting the RAT file into jpg file format, Gmail will not block the sending of the attachment file to the victim's laptop and the victim will not feel doubt to open the file received. Figure 5 shows the RAT file that has been sent from the attacker's laptop and Figure 6 shows the email that was opened by using the victim's laptop and the RAT file that had been received. If the receiver knew the sender of the email, she might not be hesitated to open the file by double clicking it. When the victim runs the Trojan file, the attacker's laptop can connect directly to the victim's laptop. As a result, the RAT file was executed and the connection between victim and attacker would be established. Since the attacker's laptop and the victim's laptop are now connected, the attacker now can monitor the victim's laptop activity such as the webcam, files registry, shut the machine off, services, clipboard and also the password.



in:sent

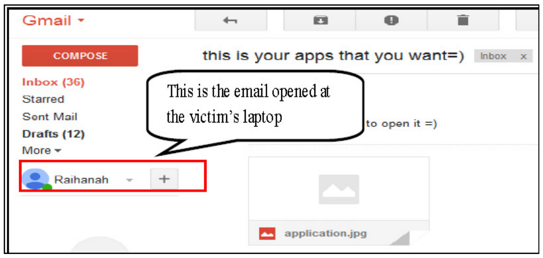
this is your apps that you want=)

nurul [redacted]@gmail.com>

Please double click to open it =)

application.jpg

Fig. 4. Email from attacker's laptop



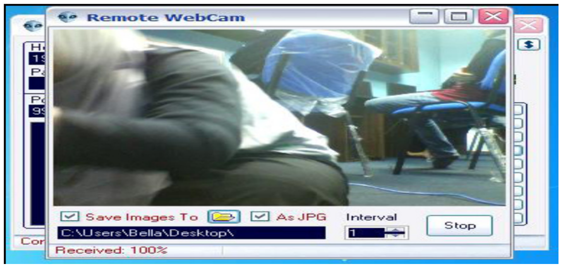
this is your apps that you want=)

to open it =)

application.jpg

Fig. 5. Email received at victim's laptop

Since the attacker's laptop is now connected to the victim's laptop, he may now do anything he wants to the victim from the attacker's laptop. In this experiment, the attacks that had been conducted were webcam hacking, screen hacking and also files registry hacking. As shown in Figure 6, the webcam of the victim's laptop had been hacked by the attacker's laptop. The attacker's laptop also can save the image of the webcam from the victim's laptop. Thus, by having this ability, the attacker will take advantage on the user of the victim's laptop by asking for ransom money if there were any inappropriate image were captured. Figures below showed the results on the victim's laptop when the attacks took placed.



☑ Save Images To ☑ As JPG

C:\Users\Bella\Desktop\

1

Received: 100%

Fig. 6. Successful Webcam Hacking

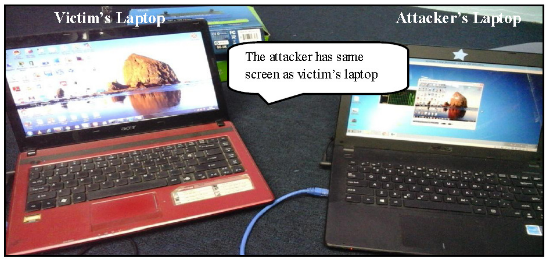


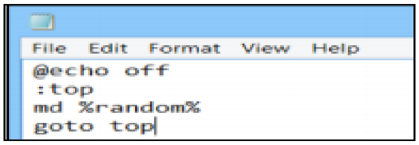
Fig. 7. Successful Screen Hacking

Figure 7 shows the result of screen hacking. The attacker can monitor the screen of the victim's laptop by using Beast tool. The attacker also can add or change the screen of the victim's laptop. It is believed that from the demonstration, readers can figure out the negative impact due to Trojan attack. Besides webcam hacking and screen hacking, the attacker also can do the files registry hacking. The built in registry file hacking that is included in the Beast tool has features such as uploading any foreign file to the victim's laptop or erasing any important data in the victim's laptop.

Hence, the attacker capable of uploading or erasing any file without the consent of the victim's laptop.

2.3 Worm Attack

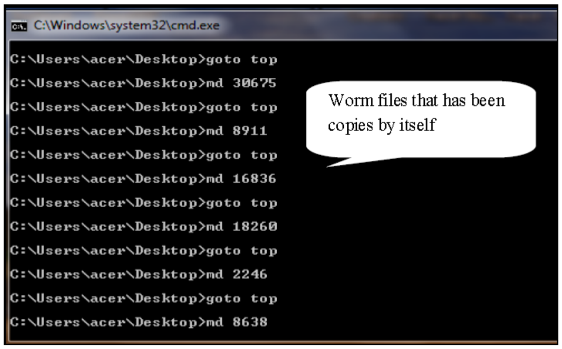
The worm attack was launched by using the command that must be used to create the worm file. As shown in Figure 8, the command for worm attack was written in the notepad and saved as a batch file named "1000.bat".



```
@echo off
:top
md %random%
goto top
```

Fig. 8. Command for Worm Attack

After the worm file has been created, the file was sent to the attacker's laptop by using Gmail account. As shown in Figure 9, when the user of the victim's laptop double click the file, the worm was executed and continue being reproduced, and would be spread into the computer system. Figure10 shows that the successful attack caused duplication of folder towards infinity and made the computer system going slower than usual.


C:\Windows\system32\cmd.exe
Worm files that has been copies by itself

```
C:\Users\acer\Desktop>goto top
C:\Users\acer\Desktop>md 30675
C:\Users\acer\Desktop>goto top
C:\Users\acer\Desktop>md 8911
C:\Users\acer\Desktop>goto top
C:\Users\acer\Desktop>md 16836
C:\Users\acer\Desktop>goto top
C:\Users\acer\Desktop>md 18260
C:\Users\acer\Desktop>goto top
C:\Users\acer\Desktop>md 2246
C:\Users\acer\Desktop>goto top
C:\Users\acer\Desktop>md 8638
```

Fig. 9. Duplication of Worm File

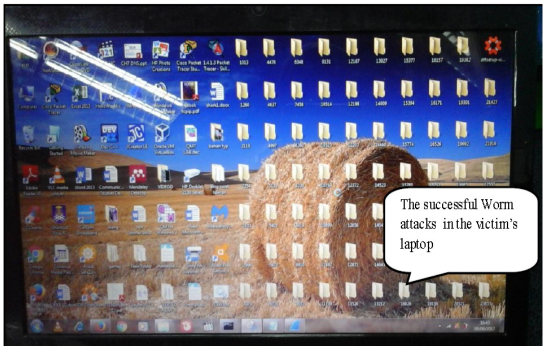
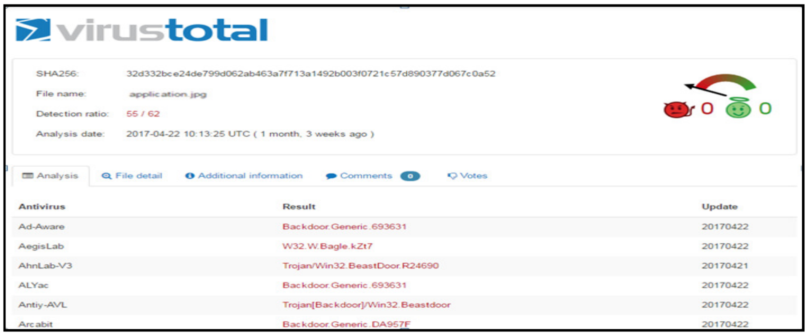


Fig. 10. Successful Worm Attack on Victim's Laptop

Tools to detect the presence of attack were executed before and after the attacks were performed. The observations are presented and discussed in the next section.

3. Results and Discussion

As some of the immediate results regarding the experiment have been presented in the previous section, this part will focus only on detecting the presence of malwares. The tools used for this purpose include Virus Total, MalwareBytes, Avast AntiVirus and Wireshark. The online scanning of the RAT file "application.jpg" using VirusTotal showed that it contains a high list of detected malwares. Hence, this file may cause huge damage if it runs into the computer system.



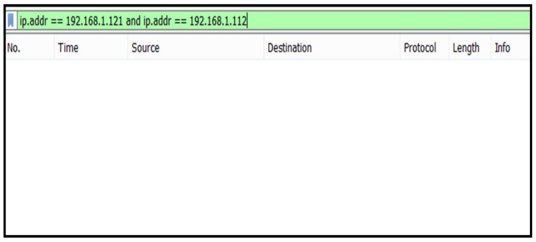
virustotal

SHA256:	32d332bce24de799d062ab463a7f713a1492b003f0721c57d890377d067c0a52
File name:	application.jpg
Detection ratio:	55 / 62
Analysis date:	2017-04-22 10:13:25 UTC (1 month, 3 weeks ago)

Antivirus	Result	Update
Ad-Aware	Backdoor.Generic.693631	20170422
AegisLab	W32.W.Bagle.kZt7	20170422
AhnLab-V3	Trojan/Win32.BeastDoor.R24690	20170421
ALYac	Backdoor.Generic.693631	20170422
Antiy-AVL	Trojan[Backdoor]/Win32.Beastdoor	20170422
Arcabit	Backdoor.Generic.DA957F	20170422

Fig. 11. Result of online scanning of the RAT file “application.jpg”

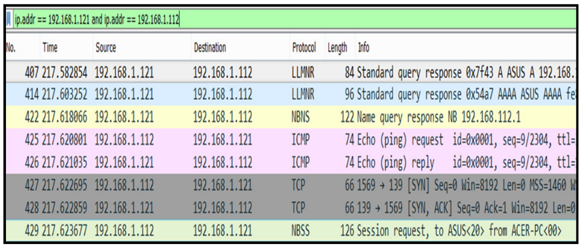
Meanwhile, Wireshark was used to detect the presence of attack between the attacker and the victim by analyzing the traffics that come from the attacker. Figure 12 shows the IP addresses of the attacker’s and victim’s laptops were filtered for easy analysis of the packets captured before and after the attacks. By analyzing the captured traffics, we can tell that some activities were happening between these two laptops. It is the evidence that Trojan attack has successfully occurred. Wireshark is helpful in detecting the malware activity as it can display the packet or exchange of packet traffic between server (attacker) and client (victim). Since Wireshark is a traffic analyzer or packet analysis tool, it is mainly used by the users to check the behaviour of their network or to monitor PC for any unwanted activity between his PC and the external network.



```
ip.addr == 192.168.1.121 and ip.addr == 192.168.1.112

No.   Time   Source   Destination   Protocol   Length   Info
```

Fig.12(a). No packets captured before the attack



```
ip.addr == 192.168.1.121 and ip.addr == 192.168.1.112

No.  Time        Source         Destination    Protocol  Length Info
 407 217.582854  192.168.1.121  192.168.1.112  LLMNR      84 Standard query response 0x7f43 A ASUS A 192.168.
 414 217.603252  192.168.1.121  192.168.1.112  LLMNR      96 Standard query response 0x54a7 AAAA ASUS AAAA fe
 422 217.618066  192.168.1.121  192.168.1.112  NBNS      122 Name query response NB 192.168.112.1
 425 217.620801  192.168.1.112  192.168.1.121  ICMP       74 Echo (ping) request  id=0x0001, seq=9/2304, ttl=
 426 217.621035  192.168.1.121  192.168.1.112  ICMP       74 Echo (ping) reply    id=0x0001, seq=9/2304, ttl=
 427 217.622695  192.168.1.112  192.168.1.121  TCP        66 1569 → 139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 W
 428 217.622859  192.168.1.121  192.168.1.112  TCP        66 139 → 1569 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
 429 217.623677  192.168.1.112  192.168.1.121  NBSS      126 Session request, to ASUS<20> from ACER-PC<00>
```

Fig. 12(b). Packets captured after the Trojan attack

Further scanning the laptops using MalwareBytes and Avast AntiVirus, both tools have successfully found the existence of malware on both devices. Avast detected the Trojan and categorized it as high severity. From the scanning result, the time elapsed to detect the malware was chosen to be presented here. For instance, MalwareBytes detected the Trojan in victim’s laptop within 17 seconds while the worm was found after 27 second (see Figure 13).

In addition, we also recorded the detection ratio of Trojan and Worm based on online VirusTotal scanner. The detection ratio value of Trojan file (“Application.jpg”) is 55 while Worm file (“1000.bat”) is only 2. This can be inferred that many Trojans were found in the file located in victim’s laptop, thus, they can be easily discovered by established scanners rather than Worm that has specific agenda and only discovered by certain scanners. The discovery of many Trojans in the file could indicate that they have higher ability to affect many programs rather than Worm. Nevertheless, a specific designed or dedicated worm could be harmful to users and possibly affect PCs or organizational networks.

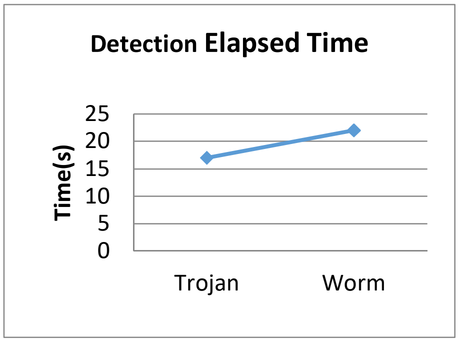


Fig. 13. The elapsed time to detect the malware

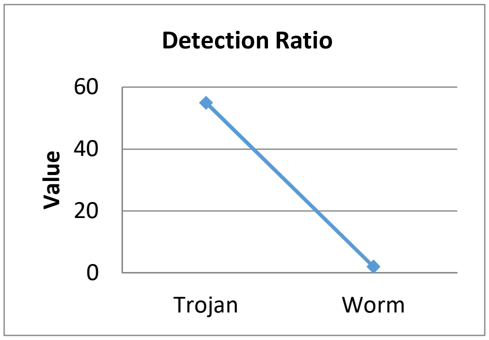


Fig. 14. Detection ratio of malware

4. Conclusion

This paper presents the effect of malware particularly Trojan and Worm attacks. The experiments were carried out to observe the Remote Access Trojan (RAT) and Worm attacks on PC. The detection of Trojan Horse and Worm attacks was done by using VirusTotal, Wireshark, Avast Anti Virus and MalwareBytes. From the results, it shows that Trojan and Worm can attack the PC and gain valuable information or do harm to the user. Besides, malwares can initiate other potential attacks that involved the unhealthy situation like the development of digital shadow economy. Thus, creating awareness to the computer users about the dangerousness of malware to their PC and digital gadgets is vital and must be done by the organization, schools, and parents to remind people under their supervision.

Acknowledgements

This research work was partially supported by Ministry of Higher Education (MOHE), Malaysia and Universiti Teknologi MARA, Malaysia under Research Acculturation Grant Scheme (RAGS), Project code: “600-RM1/RAGS 5/3 (9/2014)”.

References

[1] Golchha, Prakhar, Rajesh Deshmukh, and Palak Lunia. "A Review on Network Security Threats and Solutions." *International Journal of Scientific Engineering and Research* 3, no. 4 (2015): 21-24.
[2] Gostev, Alexander, Roman Unuchek, Maria Garnaeva, Denis Makrushin, and Anton Ivanov. "IT Threat Evolution in Q1 2016." *Kapersky 2015 Report, Kapersky L* (2016).
[3] Gaspareniene, Ligita, and Rita Remeikiene. "Digital shadow economy: A critical review of the literature." *Mediterranean Journal of Social Sciences* 6, no. 6 S5 (2015): 402.
[4] April, P. Internet Security Threat Report. 2014. 19(April).
[5] Lan, Kun-chan, Alefiya Hussain, and Debojyoti Dutta. "Effect of malicious traffic on the network." In *Passive and Active Measurement Workshop (PAM)*. 2003.
[6] Gaur, Chanakya. "Security Perspective in e-Commerce." *International Journal of Engineering Science* 4007 (2016).
[7] Zhenfang, Z. H. U. Study on Computer Trojan Horse Virus and Its Prevention, 8, (2015): 95–96.
[8] Abuzaid, Areej Mustafa, Madihah Mohd Saudi, Bachok M. Taib, and Zul Hilmi Abdullah. "An Efficient Trojan Horse Classification (ETC)." *IJCSI International Journal of Computer Science Issues* 10, no. 2-3 (2013).
[9] Gundu, T., and S. V. Flowerday. "Ignorance to awareness: Towards an information security awareness process." *SAIEE Africa Research Journal* 104, no. 2 (2013): 69-79.
[10] Al-Saadoon, Ghossoon, and Hilal MY Al-Bayatti. "A comparison of trojan virus behavior in Linux and Windows operating systems." *arXiv preprint arXiv:1105.1234* (2011).

[11] Security, C., & Report, I. Norton Cyber Security Insights Report 2016. Available from https://us.norton.com/cyber-security-insights-2016

[12] Teivāns-treinovskis, J., & Jefimovs, N. Journal of Security and Sustainability Issues www.lka.lt/index.php/lt/217049/ ISSN 2029-7017 / ISSN 2029-7025 online State National Security: Aspect of Recorded Crime, (Cho). 2012. 41–48.

[13] Solutions, E. S., & Heal, Q. Annual Threat Report 2017. 2017. Available from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[14] Rajesh, B., Reddy, Y. R. J., & Reddy, B. D. K. A Survey Paper on Malicious Computer Worms 3 no 2 (2015).

[15] Beaver, K. The 10 most common Widows security vulnerabilities. Retrieved July 2, 2017, from hhttp://www.searchenterprisedesktop.techtarget.com/tip/The-10-mostcommon-Windows-security-vulnerabilities. 2017. May 7.