

Article 8

Digital Forensic Investigation of Trojan Attacks in Network using Wireshark, FTK Imager and Volatility

Muhamad Arif Hashim, Iman Hazwam Abd Halim, Mohammad Hafiz Ismail, Norfaizalfarid Mohd Noor, Mohd Faris Mohd Fuzi, Abdul Hapes Mohammed, Ray Adderley JM. Gining
Faculty of Computer Sciences and Mathematics
Universiti Teknologi MARA Perlis Branch, Malaysia

Abstract

Trojan attacks are the most common and serious threat to network users. It is a program that appears to be useful program but actually harmful one. It is difficult to detect Trojan attacks because it uses special techniques to conceal its activities from antiviruses and users. Thus, this research intends to retrieve and investigate of Trojan attacks on the network using digital forensic tools namely Wireshark, FTK Imager and Volatility. Two types of Trojan attacks called Remote Access Trojan (RAT) and HTTP Trojan (HT) are created and experimented in this research. These Trojans are sent to the targeted computer in the network through email. Wireshark is used to capture the network packets and then analyze the suspicious packets. FTK Imager is used to capture RAM data on targeted computer. Volatility is used to analyze the captured RAM data and extract suspicious process. This suspicious process is dumped into file and scanned using the Avast antivirus to check whether this process is running Trojan or otherwise. This research may benefit and contribute to the computer security and forensic domain. It can be extends to investigate other Trojan attacks such as Zeus, SubSeven or Back Orifice by using the same digital forensic tools.

Keywords: Digital forensic, Trojan attack, Wireshark, FTK Imager, Volatility

Introduction

The Trojan attack (Trojan) is one of the most notorious malware attacks (Al-Saadoon & Al-Bayatti, 2011). It is a program in which malicious code is contained inside the harmless program in such way that can control and cause some damage on the computer system (Al-Saadoon & Al-Bayatti, 2011). Trojan can cause massive harm to the computer system and can also crash computer system. **Mostly, Trojan infected the computer via the acts of downloading software, movie or music from unknown websites or an email attachment (Garcia, Reilly & Shorter, 2003).** Trojan operates by hiding itself inside a useful software program (Al-Saadoon & Al-Bayatti, 2011). Once it is installed or executed in the system, Trojan begins its work by infecting different files in the computer. The user will notice that the computer has becoming slower and a window pop up may suddenly appears on the desktop (Al-Saadoon & Al-Bayatti, 2011). This phenomenon happens because of Trojan has already spread its virus to the computer's user. Later, this would cause their computer to crash and the computer is eventually no longer usable. Trojan also capable of stealing crucial information from the user's computer (Kumar, Upadhyay & Kumar, 2012).

Related Works

The analyzing a Trojan attack is tricky and crucial. It must include forensics analysis processes. Thus, Podile, Gottumukkala, & Pendyala (2015) highlight that forensic analysis is important for

cases such as the analyzing of bank customer’s computer that has been infected with Trojan. Forensic analysis may use FTK imager (FTK) and Digital Evidence Forensic Toolkit (DEFT) to collect evidence on registry files, internet history and events log files from the infected bank customer computer. Other than that, Volatility is also used to analyze RAM dump on infected machine.

Heriyanto (2012) performed forensic analysis to find and collect the evidence from Trojan banking malware for instance Cridex, Zeus and SpyEye. The tools that were used are Volatility and Wireshark. Volatility is used to seek the existence of Cridex and Zeus on the virtual machine while Wireshark is used to examine and capture the network traffic on Cridex, Zeus and SpyEye for evidence.

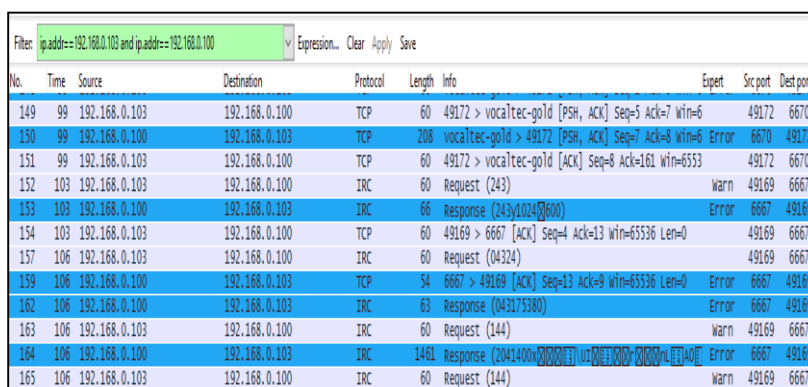
Analysis and Results

The result obtained from the analysis, which has been carried out are as follow:

i. Network Forensic Investigation

Network forensic performs analysis on network activities by collecting information associated with illegal activities(Xrysanthou& Apostolakis, 2006). Wireshark was used to captures network packet and analyses suspicious Trojan packet on the network.

Figure 1 and Figure 2 showed the results based on Wireshark after a RAT and HTTP Trojan attack on victim’s laptop. There was communication between attacker’s laptop and victim’s laptop when we filtered using the IP addresses 192.168.0.103 (attacker) and 192.168.0.100 (victim). This means that both attacks have already infiltrated the victim’s.



No.	Time	Source	Destination	Protocol	Length	Info	Espet	Src port	Dest port
149	99	192.168.0.103	192.168.0.100	TCP	60	49172 > vocaltec-go!d [PSH, ACK] Seq=5 Ack=7 win=6		49172	6670
150	99	192.168.0.100	192.168.0.103	TCP	208	vocaltec-go!d > 49172 [PSH, ACK] Seq=7 Ack=8 win=6	Error	6670	49172
151	99	192.168.0.103	192.168.0.100	TCP	60	49172 > vocaltec-go!d [ACK] Seq=8 Ack=161 win=6553		49172	6670
152	103	192.168.0.103	192.168.0.100	IRC	60	Request (243)	Warn	49169	6667
153	103	192.168.0.100	192.168.0.103	IRC	66	Response (243)(0240600)	Error	6667	49169
154	103	192.168.0.103	192.168.0.100	TCP	60	49169 > 6667 [ACK] Seq=4 Ack=13 win=65536 Len=0		49169	6667
157	106	192.168.0.103	192.168.0.100	IRC	60	Request (04324)		49169	6667
159	106	192.168.0.100	192.168.0.103	TCP	54	6667 > 49169 [ACK] Seq=13 Ack=9 win=65536 Len=0	Error	6667	49169
162	106	192.168.0.100	192.168.0.103	IRC	63	Response (043173380)	Error	6667	49169
163	106	192.168.0.103	192.168.0.100	IRC	60	Request (144)	Warn	49169	6667
164	106	192.168.0.100	192.168.0.103	IRC	1461	Response (2041400v00000E1 UT0EE000P 0000vLE1A0E	Error	6667	49169
165	106	192.168.0.103	192.168.0.100	IRC	60	Request (144)	Warn	49169	6667

Figure 1 Packet captured after RAT attack

No.	Time	Source	Destination	Protocol	Length	Info	Expet	Src port
2222	523	192.168.0.100	192.168.0.103	HTTP	1514	Continuation or non-HTTP traffic	Error	80
2223	523	192.168.0.100	192.168.0.103	HTTP	89	Continuation or non-HTTP traffic	Error	80
2224	523	192.168.0.100	192.168.0.103	HTTP	550	Continuation or non-HTTP traffic	Error	80
2225	523	192.168.0.103	192.168.0.100	TCP	60	50728 > http [ACK] Seq=407 Ack=2390 win=65536 Len=		50728
2226	523	192.168.0.100	192.168.0.103	HTTP	634	Continuation or non-HTTP traffic	Chat	80
2227	523	192.168.0.103	192.168.0.100	TCP	60	50728 > http [ACK] Seq=407 Ack=3502 win=64512 Len=		50728
2228	523	192.168.0.103	192.168.0.100	TCP	60	50728 > http [FIN, ACK] Seq=407 Ack=3502 win=64512 Chat		50728
2229	523	192.168.0.100	192.168.0.103	TCP	54	http > 50728 [ACK] Seq=3502 Ack=408 win=65536 Len=	Error	80
2230	524	192.168.0.103	192.168.0.100	TCP	66	50730 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 W Chat		50730
2231	524	192.168.0.100	192.168.0.103	TCP	66	http > 50730 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 Chat		80

Figure 2 Packet captured after HTTP Trojan attack

ii. *Memory Forensics Investigation*

Memory forensic performs analysis on memory image taken from the victim’s running computer (Sindhu & Meshram, 2012). Memory forensic is important in the investigation because it helps in extracting forensic artifacts from victim’s computer’s memory like network connection, running process and loaded module. Two memory forensic tools that was used to detect Trojan attacks are FTK Imager and Volatility.

Figure 3 and 4 showed the FTK imager has successfully captured RAM data on victim’s laptop.

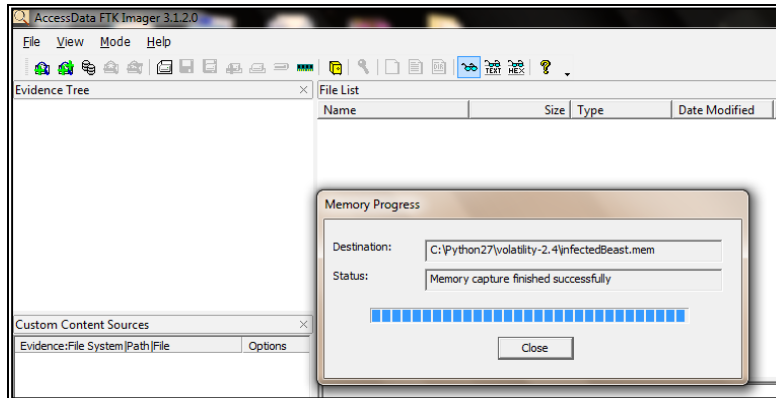


Figure 3 Successfully capture RAM data after RAT attack

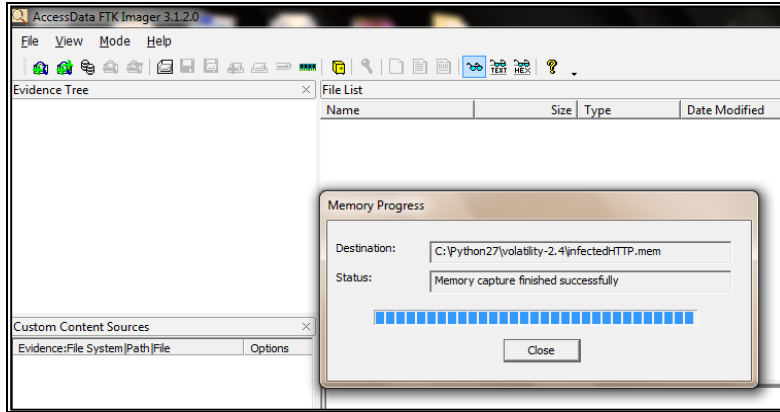


Figure 4 Successfully capture RAM data after HTTP Trojan attack

The memory files were saved as infectedBeast.mem for RAT and infectedHTTP.mem for HT. Once the RAM data has been captured, Volatility was used to perform memory forensic on the captured RAM data. Volatility analyzed the captured RAM data and extracted suspicious process from RAM data. Netscan plugin was used to extract information about the network connection held from and to the system with details included. Figure 5 showed the output of netscan plugin using the command “vol.py --profile=Win7SP0x86 netscan -f infectedBeast.mem” and Figure 6 showed the output of netscan plugin using the command “vol.py --profile=Win7SP0x86 netscan -f infectedHTTP.mem”.

0x1487db00	TCPv4	192.168.0.100:6667	192.168.0.103:50000	ESTABLISHED	2432	beastserver.exe
0x164e8830	UDPv6	:::1:55107	:::*		3344	svchost.exe
0x1d2c7850	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	572	lsass.exe
0x1d49ac40	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	948	svchost.exe
0x1d50ca18	TCPv6	:::1:27275	:::0	LISTENING	1376	AvastSvc.exe
0x1d719188	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	572	lsass.exe
0x1d719188	TCPv6	:::49154	:::0	LISTENING	572	lsass.exe
0x1d63d548	TCPv4	192.168.0.100:6674	192.168.0.103:50007	ESTABLISHED	2432	beastserver.exe
0x21bddb98	TCPv4	192.168.0.100:6671	192.168.0.103:50004	ESTABLISHED	2432	beastserver.exe
0x235822c6	UDPv4	0.0.0.0:0	:::*		948	svchost.exe
0x23fe4a88	TCPv4	127.0.0.1:43227	0.0.0.0:0	LISTENING	1784	MBAMService.exe
0x24166828	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	948	svchost.exe
0x24166828	TCPv6	:::49155	:::0	LISTENING	948	svchost.exe
0x23adec18	TCPv4	:::49581	10.0.7.12:443	CLOSED	3436	Wireshark.exe

Figure 5 List of network connection extracted from infectedBeast memory

0x3e233488	UDPv4	0.0.0.0:0	:::*		1288	svchost.exe
0x3e233488	UDPv6	:::0	:::*		1288	svchost.exe
0x3e58f480	UDPv4	0.0.0.0:500	:::*		1000	svchost.exe
0x3e5ed7f8	UDPv4	127.0.0.1:49152	:::*		1376	AvastSvc.exe
0x3e257258	TCPv4	0.0.0.0:80	0.0.0.0:0	LISTENING	1180	HTTPSERVER.EXE
0x3e597888	TCPv4	0.0.0.0:554	0.0.0.0:0	LISTENING	1776	wmpnetwk.exe
0x3e700638	TCPv4	192.168.0.100:139	0.0.0.0:0	LISTENING	4	System
0x3f232c58	UDPv4	0.0.0.0:5355	:::*		1288	svchost.exe
0x3f25b2b8	UDPv4	0.0.0.0:5004	:::*		1776	wmpnetwk.exe
0x3f25b2b8	UDPv6	:::5004	:::*		1776	wmpnetwk.exe
0x3f25bbe8	UDPv6	:::1:50473	:::*		2264	svchost.exe

Figure 6 List of network connection extracted from infectedHTTP memory

0x00000003e551020	smss.exe	272	4	0x3e555020	2017-06-09	05:07:05	UTC+0000
0x00000003e6f3528	ScreenRecorder	4128	2576	0x3e5555a0	2017-06-09	07:13:01	UTC+0000
0x00000003e7b3440	svchost.exe	1660	528	0x3e555300	2017-06-09	05:07:28	UTC+0000
0x00000003e7c0aa8	taskhost.exe	1724	528	0x3e555320	2017-06-09	05:07:28	UTC+0000
0x00000003e7cd390	backup.exe	1796	1604	0x3e555340	2017-06-09	05:07:28	UTC+0000
0x00000003e978a50	beastserver.ex	2432	2352	0x3e555600	2017-06-09	07:14:39	UTC+0000
0x00000003f273030	wmpnetwk.exe	5944	528	0x3e5555e0	2017-06-09	05:10:12	UTC+0000
0x00000003f36bb90	svchost.exe	3344	528	0x3e555600	2017-06-09	05:10:22	UTC+0000
0x00000003f576bb0	System	4	0	0x00185000	2017-06-09	05:07:05	UTC+0000

Figure 7 List of hidden process extracted from infectedBeast memory

There was an active network connection between IP address 192.168.0.100 and 192.168.0.103 on victim's laptop. Network connection to the IP address 192.168.0.103 was made by the PID 2432 and the process that was associated with PID 2432 is beastserver.ex. PID 2432 was used as a cover process for some hidden processes which are being carried out on the victim's laptop. Figure 7 showed the output of psscan plugin using the command "vol.py --profile=Win7SP0x86 psscan -f infectedBeast.mem".

It showed that one of the processes beastserver.ex with the PID 2432 looked suspicious because the beastserver's extension was different from the other processes' extension whereas the other processes had the same .exe extension. These suspicious beastserver.ex process was dumped into files and was scanned using Avast antivirus to confirm that it is Remote Access Trojan (RAT). The result exhibited that Avast antivirus detected beastserver.ex process as Win32:BeastDoor-AA [Trj]. RAT used beastserver.ex process to hide its activity on victim's laptop so that victim cannot detect its present.

0x0000000271040f8	dumpcap.exe	4020	1952	0x3e5b5540	2017-05-23	00:35:43	UTC+0000
0x00000002eaca2d40	AvastUI.exe	1996	1932	0x3e5b5480	2017-05-23	00:16:50	UTC+0000
0x00000003cc36498	explorer.exe	1516	1456	0x3e5b52c0	2017-05-23	00:16:42	UTC+0000
0x00000003ccccf660	spoolsv.exe	1588	572	0x3e5b52e0	2017-05-23	00:16:44	UTC+0000
0x00000003cd45530	svchost.exe	1648	572	0x3e5b5320	2017-05-23	00:16:45	UTC+0000
0x00000003cd4a530	taskhost.exe	1668	572	0x3e5b5340	2017-05-23	00:16:45	UTC+0000
0x00000003cd4c030	HTTPSERVER.EXE	1180	316	0x3e5b56a0	2017-05-23	00:36:30	UTC+0000
0x00000003cd6fd40	wmpnetwk.exe	1776	572	0x3e5b5560	2017-05-23	00:18:57	UTC+0000
0x00000003cd9fd40	svchost.exe	2264	572	0x3e5b5280	2017-05-23	00:18:59	UTC+0000
0x00000003cdc5950	Wireshark.exe	1952	1516	0x3e5b51e0	2017-05-23	00:35:39	UTC+0000
0x00000003cde7c78	RtHDVCpl.exe	1884	1516	0x3e5b53c0	2017-05-23	00:16:48	UTC+0000

Figure 8 List of hidden process extracted from infectedHTTP memory

The result showed that there was no active network connection detected between IP address 192.168.0.100 and IP address 192.168.0.103 on the victim's laptop. Based on Figure 8, the HTTPSERVER.EXE process was running on victim's system but the source and destination IP address is 0.0.0.0. Figure 8 showed the output of psscan plugin using the command "vol.py --profile=Win7SP0x86 psscan -f infectedHTTP.mem".

It showed that HTTPSERVER.EXE process with the PID 1180 looks suspicious. This suspicious HTTPSERVER.EXE process had been dumped into files and was scanned using Avast antivirus to confirm that whether this process is a HTTP RAT. The result showed that Avast antivirus was unable to detect the HTTPSERVER.EXE process as a HTTP Trojan. This Trojan was considered dangerous because it uses a special technique to make their detection more difficult. Table 1 showed the result obtained from the Avast antivirus scanning.

Table 1 Avast Scanning Result

Trojan	Process ID	Dumped file	Avast antivirus
RAT	beastserver.ex 2432	2432.dmp	Win32:BeastDoor-AA[Trj]
HTTP Trojan	HTTPSERVER.EXE 1180	1180.dmp	No thread found

Conclusion

This research seeks to explain the importance of network forensic and memory forensic investigations on Trojan malware incidents. It has achieved its objectives to retrieve and investigate the evidence of Trojan attack using digital forensic tool like Wireshark, FTK Imager and Volatility. Based on the research results, it can be concluded that Wireshark is very useful in an investigation because it successfully detects both a RAT attack and a HTTP Trojan attack on the network. Volatility is a very powerful memory forensic tool that contains a great set of features and options which can help in detecting a Trojan attack. Volatility along with FTK Imager can be considered as a great memory forensic duo when performing an investigation of a Trojan attack. Both FTK Imager and Volatility can detect a RAT attack while the HTTP Trojan is quite difficult to be detected because Volatility cannot detect the communication between the IP address of the attacker and the IP address of the victim. It only shows the processes that are running on the victim's.

References

- Al-Saadoon, G. M. W. & Al-Bayatti, H. M. Y. (2011). A Comparison of Trojan Virus Behavior in Linux and Windows Operating Systems. *World of Computer Science and Information Technology Journal (WCSIT)*, 1(3), 56–62.
- Garcia, H. J., Reilly, R. & Shorter, J. D. (2003). Trojan horses: They deceive, they invade, they destroy, 136–142.
- Heriyanto, A. P. (2012). What is the Proper Forensics Approach on Trojan Banking Malware Incidents? In Proceedings of the 10th Australian Digital Forensics Conference, pp. 10-20. Edith Cowan University, Western Australia.
- Kumar, K., Upadhyay, H. & Kumar, R. (2012). Trojan: Infection and precaution. *BPR Technologia: A Journal of Science, Technology & Management*, 1(1), 54–61.
- Mabuto, E. K. & Venter, H. S. (2011). State of the art of Digital Forensic Techniques. Conference : Information Security South Africa Conference 2011. South Africa
- Podile, A., Gottumukkala, K. & Pendyala, K. S. (2015). Digital Forensic Analysis Of Malware Infected Machine - Case Study. *International Journal of Scientific & Technology Research*, 4(9).
- Sindhu, K. K. & Meshram, B. B. (2012). Digital Forensic Investigation Tools and Procedures. *I. J. Computer Network and Information Security*, (4), 39–48.
- Xrysanthou, A. & Apostolakis, I. (2006). Network Forensics : Problems and Solutions. In Conference : E-Democracy: Challenge of the Digital Era, pp 307-318. Greece.