An improved traditional worm attack pattern

Conference Paper · July 2010

DOI: 10.1109/ITSIM.2010.5561572 · Source: IEEE Xplore

6 authors, including:

Y. Robiah
Technical University of Malaysia Malacca
32 PUBLICATIONS **110** CITATIONS
SEE PROFILE

S. Siti Rahayu
Technical University of Malaysia Malacca
29 PUBLICATIONS **108** CITATIONS
SEE PROFILE

Zaki Masud
Technical University of Malaysia Malacca
16 PUBLICATIONS **36** CITATIONS
SEE PROFILE

Mohd Faizal Abdollah
Technical University of Malaysia Malacca
58 PUBLICATIONS **66** CITATIONS
SEE PROFILE

An Improved Traditional Worm Attack Pattern

Robiah Y., Siti Rahayu S., Shahrin Sahib, Mohd Zaki M., Faizal M. A., Marliza R.
Faculty of Information and Communication Technology
Univeristi Teknikal Malaysia Melaka,
Durian Tunggal, Melaka,
Malaysia

Abstract—**The significant threats of traditional worms such as Blaster, Sasser, Code Red and Slammer are still continuing due to their hasty spreading nature on the internet. The worms attack pattern from three different scenarios have been extracted from various logs at different OSI layers such as victim logs, attacker logs and IDS alert log. These worms attack pattern are further analyzed to form the general worms' attack pattern which describes the process of worms' infection. This paper proposes a general attack pattern for worm in three different perspectives which is attacker, victim and victim/attacker or multi-step attack using only Blaster variant. Thus, the general attack pattern can be extended into research areas in alert correlation and computer forensic investigation.**

Index Terms — **worm attack pattern, log, blaster attack**

I. INTRODUCTION

It is important to understand on how the current worms' infection propagates dynamically to protect us against the attack of the future worms. The most well-known traditional worms such as Blaster, Sasser, Code Red and Slammer, are the major threats to the security of the internet. Their quick distribution in exploiting the vulnerability of the operating system has threatened the services offered on the internet. Hence, there is a need to find a solution to detect and predict the propagation of the worm and for this reason this paper propose the general worm attack pattern for detecting and predicting the worm by examining the various OSI layer's log from the worm source and the other machine that are infected with it and investigate the trace leave by the attacker which is considered as the attack pattern.

For the purpose of this paper, the researchers only select three scenarios: scenario A, B and C; and used Blaster variants during the experiment. This attack pattern is based on the fingerprint of Blaster attack on victim's logs, attacker's logs and Intrusion Detection System (IDS) alert's log.

II. RELATED WORK

A. Blaster Worm

The Blaster worm launch on August, 11th 2003 infected at least 100,000 Microsoft Windows systems and cost millions in damage. In spite of cleanup efforts, an anti-worm, and a removal tool from Microsoft, the worm persists [1]. This worm's impact was not bounded to a short period in August 2003 as according to [2], a published survey of 19 research universities showed that during a five-week period of recovering from the Blaster worms and its variants, an average of US$299,579 is consumed. In addition the blaster worms have the potential to generate the multi-step attack which can increase the recovery cost of the infected system and would initiate serious cyber crimes.

Blaster worms spreads by exploiting DCOM RPC vulnerability in Microsoft Windows as described in Microsoft Security Bulletin MS03-026. The worms scan *port 135* on random subnets in sequential or random order, and the target are the discovered systems. The exploit code opens a backdoor on *TCP port 4444* and instructing them to download and execute the file *MSBLAST.EXE* from a remote system via *Trivial File Transfer Protocol (TFTP)* on UDP *port 69* to the *%WinDir%\system32* directory of the infected system and execute it. The goal of the Blaster attacker is to make the system unstable by terminating the RPC services and causes the system to reboot.

Normally an exploit would only target a single operating system for example; *Windows XP* or *Windows 2000*, due to the location of certain files in the memory on each platform is usually different. These Blaster worms will semi-randomly tries and infect machine with 20% probability on *Windows 2000* and 80% probability on *Windows XP* as in [3].

B. What Is Attack Pattern?

An attack pattern is a systematic description of the attack goals and attack strategies for defending against attack. According to [4], an attack pattern is described as the steps in a generic attack, while [5] explain the term attack pattern as the attack steps, attack goal, pre-conditions and post-conditions of an attack. Subsequently, [6] has clarify an attack pattern is a method to cause an exploit against software used by attackers. Hence, an attack pattern is identified as one of the important component to protect from any potential attack.

The study from [4], [5] and [6] discussed the concept of attack patterns as a mechanism to capture and communicate at the attacker's perspective that shows the common methods for exploiting software, system or network while [7] and [8] discussed on the attack pattern on how the attack is performed, the attack goals, how to defences against the attack and how to trace once it has occurred. Software developers and network administrator can mitigate the impact of these attacks, detect and block any vulnerability in their network by applying the knowledge of potential attacks represented by the attack pattern.

978-1-4244-6716-7/10/$26.00©2010 IEEE

Based on the study, the victim's perspective is omitted by focusing on the attacker's perspective only. Consequently, the attack patterns by focusing on the attacker's, victim's and attacker/victim's (multi-step) perspectives are proposed to provide logical perception on how the attack is accomplished and the effect caused by the attack.

III. ATTACK SCENARIO

In this experiment, three attack scenarios: scenario A, scenario B and scenario C are designed using the framework which consists of four phases: Network Environment Setup, Attack Activation, Log Collection and Log Analysis as described in [9]. Each attack scenario is attained through thorough log analysis. The diverse logs involve in this analysis are divided into two categories which are host logs and network logs. The host logs categories: personal firewall log, security log, system log, application log and network logs categories: alert log by IDS

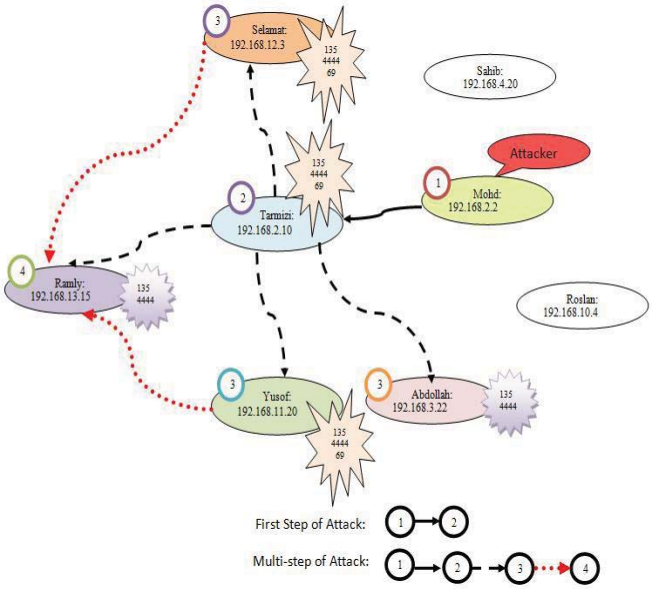

Fig. 1 Blaster attack in scenario A which consists of first step and multi-step of attack

In Fig. 1, the analysis of scenario A shows that the worms attack is activated in *Mohd* and this host has successfully exploited all hosts except for hosts *Sahib* and *Roslan*. Subsequently, hosts *Tarmizi* which has been previously exploited by *Mohd* has organized attack on host *Selamat*, *Ramly, Yusof* and *Abdollah* which called multi-step attack. Later on host *Yusof* and *Selamat* which has been exploited by *Tarmizi*; is trying to exploit Ramly.

In this attack scenario, those host that mark with *135, 4444* and *69* is indicated as successfully exploited by the attacker and this host has been infected. On the other hand, those marks with *135* and *4444* shows the attacker has already open the backdoor but has not successful transfer the exploit code through port *69*

Consequently, in scenario B, as depicted in Fig. 2, the analysis shows that the worms attack is activated in *Mohd* and this host has successfully exploited all hosts except for hosts *Abdollah*. Subsequently, hosts *Roslan* which has been previously exploited by *Mohd* has organized attack on host *Selamat* and *Yusof* which called multi-step attack. Later on host *Selamat* which has been exploited by *Roslan* is trying to exploit Ramly.

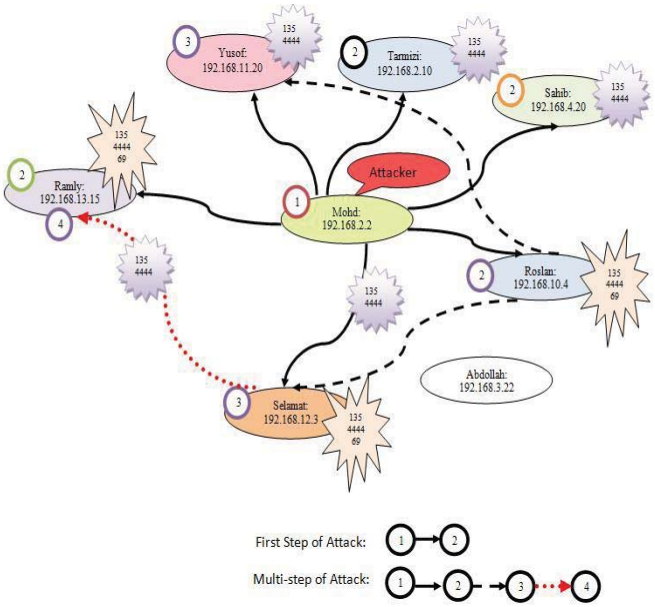

Fig. 2 Blaster attack in scenario B which consists of first step and multi-step of attack

Meanwhile in scenario C, the analysis as illustrated in Fig. 3; shows that the worms attack is activated in *Mohd* and this host has successfully exploited all hosts except for hosts *Abdollah*. Consequently, host *Sahib* which has been previously exploited by *Mohd* has organized attack on host Yusof, Ramly, *Selamat* and *Roslan* which called multi-step attack.

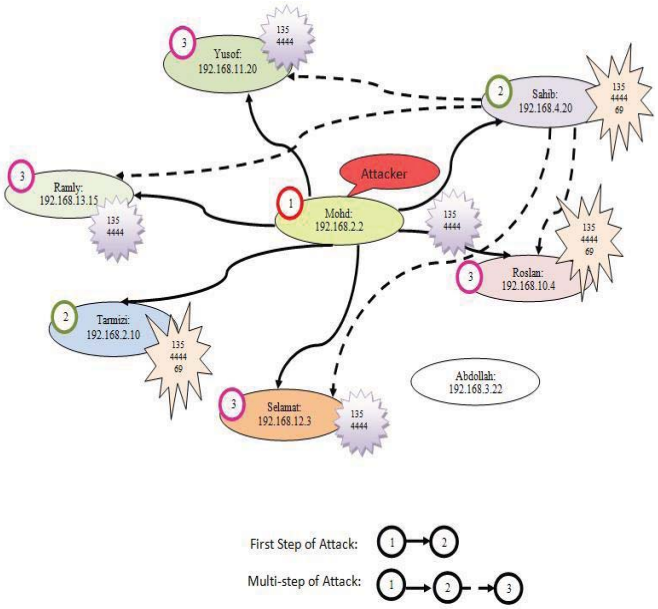

Fig. 3 Blaster attack in scenario C which consists of first step and multi-step of attack

IV. ANALYSIS AND FINDINGS

The three attack scenarios are further analysed and the findings from this analysis are used as the primary guideline

in developing the general worm attack pattern. These attack patterns are constructed in three different perspectives: attacker, victim and victim/attacker or multi-step attack. The details of these perspectives are elaborated in the following sub-sections.

A. Analysis Of Worm Attack Pattern In Attacker Perspective

In attacker perspective, the analysis found that there are significant attack pattern in all scenarios and the summary of the Blaster attacker pattern for these three scenarios are shown in TABLE I. The proof of the pattern are analyse in personal firewall log, security log, system log, application log and IDS alert log; and the details of the attacker pattern are discussed.

TABLE I
Summary On Blaster's Attacker Pattern For Scenario A, B And C
(Item Found=√, Item Not Found=×)

Perspective	Attack Steps	Log Name	Attributes	Scenario A	Scenario B	Scenario C
Attacker	Scan	Personal firewall	135 open tcp	√	√	√
	Exploit	Personal firewall	4444 open tcp 69 open-inbound udp	√	√	√
	Impact/Effect	Security	Event ID: 592 Image Filename: ~\blasterA. exe	√	√	√
		System	Nil	×	×	×
		Application	Nil	×	×	×
	Activity	IDS Alert	(Portscan) TCP Portsweep	√	√	√
	Alarm	IDS Alert	Source IP: Attacker	√	√	√

In all scenarios, the data in attacker's *Personal Firewall Log* shows the vulnerable ports that are used by the attacker to exploit the system-level command shell on its victims. As referred to [10], [3] and [11], the attack patterns are *135 OPEN TCP, 4444 OPEN TCP* and *69 OPEN-INBOUND UDP*. The local host will primarily scan the vulnerable ports and opened an outbound session to the remote host which allows it to transmit the payload (worm codes) to the remote host by exploiting the vulnerable ports open.

Meanwhile, there is a new process created (*Event ID: 592*) from the *security log* shows that the blaster worm is activated and fingerprint is shown on the *image file name*. Consequently, there is no significant fingerprint found in both *system log* and *application log*.

In the *alert IDS log*, *(Portscan) TCP Portsweep* presents the pattern of scanning activity which shows the behavior of worm attack in general and blaster worm attack in specific [12] and the alarm shows that the *Source IP* is the attacker. Therefore, this fingerprint discovers that this local host is a potential attacker who launched the worm.

B. Analysis Of Worm Attack Pattern In Victim Perspective

The victim's fingerprints are extracted from the logs at the victim's host and network log. The fingerprints of these three scenarios are analysed in *personal firewall log, security log, system log, application log* and *IDS alert log*. The summary of the victim pattern are shown in TABLE II and the details are discussed.

TABLE II
Summary On Blaster's Victim Pattern For Scenario A, B And C
(Item Found=√, Item Not Found=×)

Perspective	Attack Steps	Log Name	Attributes	Scenario A	Scenario B	Scenario C
Victim	Scan	Personal firewall	135 open-inbound tcp	√	√	√
	Exploit	Personal firewall	4444 open-inbound tcp 69 open udp	√	√	√
	Impact/Effect	Security	Event ID: 592 Image Filename: %WINDIR%\System32\ tftp.exe Event ID: 592 Image Filename: %WINDIR%\System32\ msblast.exe	√	√	√
		System	Event ID: 1074 Windows Restart RPC Service terminated	√	√	√
		Application	Nil	×	×	×
	Activity	IDS Alert	TFTP Get	√	√	√
	Alarm	IDS Alert	Source IP: Victim Destination IP: Attacker Destination Port: 69	√	√	√

In these three scenarios, as mentioned by [10], [3] and [11] *135 OPEN-INBOUND TCP, 4444 OPEN-INBOUND TCP* and *69 OPEN UDP* in *Personal Firewall log* are considered as part of victim's attack pattern which consists of scanning and exploiting steps. In these steps, the malicious codes use vulnerable ports *135, 4444* and *69* to exploit the system-level command shell on its victims which provide an inter-process communication mechanism. These exploits allow programs running on one host to execute code on remote hosts.

A complete sequence of blaster worm communication consists of *OPEN-INBOUND, OPEN-INBOUND* and *OPEN* action used to gain access and upload the malicious codes to be exploited as described by [13]. The *OPEN-INBOUND* action shows that an inbound session was opened to the local host and *OPEN* action shows that an outbound session was opened to a remote host.

The *Security* and *System log* contained the fingerprint of the worm's exploitation impact. The existence of *event id: 592* leave in *security log* can proved that there is a new process created by the system. The *TFTP* service has been initiated and used to download and upload the blaster worm code as well as executing the remote blaster worm code (*msblast.exe*). This fingerprint is capture in *Image File Name* as *%WINDIR%\System32\tftp.exe* and *%WINDIR%\ System32\ msblast.exe*.

System log shows the fingerprint of the Blaster-infected machine stops its *TFTP* daemon after a transmission or after 20 seconds of *TFTP* inactivity by showing the new process created on *event id:1074* that indicates the *windows restart and RPC service terminated unexpectedly*. Subsequently,

there is no significant fingerprint found in *application log*. The addition fingerprint of *TFTP Get* on *port 69 UDP* can also be found in *alert IDS log*. These fingerprints identify that there is a pattern exists on how the blaster worm initiates the client to download the worm code using *port 69* where the *source IP address* is the victim and the *Destination IP address* is the attacker.

C. *Analysis Of Worm Attack Pattern In Multi-Step (Victim/Attacker) Perspective*

The multi-step (victim/attacker)'s attack fingerprint is identified in these three scenarios. The summary of the fingerprint on the multi-step and network logs are represented in TABLE III and the details of the attack pattern of the multi-step's logs are discussed.

TABLE III
Summary On Blaster's Multi-Step (Victim/Attacker) Pattern For Scenario A, B And C
(Item Found=√, Item Not Found=×)

Perspective	Attack Steps	Log Name	Attributes	Scenario A	Scenario B	Scenario C
Victim/ Attacker	Scan	Personal firewall	**VICTIM** 135 open-inbound tcp **ATTACKER** 135 open tcp	√	√	√
	Exploit	Personal firewall	**VICTIM** 4444 open-inbound tcp 69 open udp **ATTACKER** 4444 open tcp 69 open-inbound udp	√	√	√
	Impact/ Effect	Security	**VICTIM/ATTACKER** Event ID: 592 Image Filename: %WINDIR%\System32\ tftp.exe Event ID: 592 Image Filename: %WINDIR%\System32\ msblast.exe	√	√	√
		System	**VICTIM** Event ID: 1074 Windows Restart RPC Service terminated	√	√	√
		Application	Nil	×	×	×
	Activity	IDS Alert (Activity)	**VICTIM** TFTP Get **ATTACKER** (Portscan) TCP Portsweep	√	√	√
	Alarm	IDS Alert (Alarm)	**VICTIM** Source IP: Victim Destination IP: Attacker Destination Port: 69 **ATTACKER** Source IP: Attacker	√	√	√

Referring to TABLE III, there are two different patterns existing in *personal firewall log* that discover attacker and victim fingerprint. From the victim perspective (*OPEN-135 INBOUND TCP, 4444 OPEN-INBOUND TCP and 69 OPEN UDP*), the patterns indicate that the local host has permitted the *TFTP* service which then initiate the incoming traffic from the remote host.

Meanwhile, from the attacker perspective (*135 OPEN TCP, 4444 OPEN TCP and 69 OPEN -INBOUND UDP*), the patterns show that the local host has opened an outbound session to the remote host which allow the local host transmit the payload (worm codes) to the remote host. These communication activities used the vulnerable open ports that permit all exploitation. The fingerprints found show it's significant to the multi-step attack (victim/attacker) in which this host was infected (act as victim). Subsequently, as long as the computer was infected with the worm code (*msblast*), it is considered as an attacker and it continue to generate traffic which attempt to infect other vulnerable computers [14].

The fingerprint in the *security log* shows there is a new process created by the system which initiates the *TFTP* service in order to receive and sent the blaster worm code. Then it executes the blaster worm code (*msblast.exe*) remotely. Both processes has new event id created (*Event ID: 592*). Based on the fingerprint it indicates that this host is a victim of blaster worm attack. However, this host was infected previously and automatically generating traffic to exploit other vulnerable computers by transferring the worm code.

The fingerprint found in *System log* shows the Blaster-infected machine halt by showing the new process created on *event id:1074* which indicates the *windows restart and RPC service terminated*. Hence it indicates the host is infected by blaster worm and this is comparable to the victim pattern.

In TABLE III, the IDS alert log shows that there are alerts found on *TFTP Get* and *(Portscan) TCP Portsweep* activities for victim and attacker respectively. Both alerts indicate that there is a pattern exists on the blaster worm attack activities and shows that the *source IP address* is the victim and the *destination IP address* is the attacker which are significant to the pattern that found in victim and attacker.

In this analysis, the researchers have identified the attributes from the victim, attacker and multi-step fingerprint. These findings are further use to construct the proposed general worm attack pattern.

V. PROPOSED GENERAL WORM ATTACK PATTERN

This research proposed the general worm attack pattern based on victim, attacker and multi-step point of view. The following section describes the details.

A. *General Attacker Pattern*

Attacker's worm attack pattern presents a systematic description of the attack goals and attack strategies for defending against the attack. This pattern is a useful guide for researcher in identifying the attacker of an attack. Based on the finding in TABLE I, the overall general attacker's attack pattern illustrated in Fig. 4 indicate that the worm pattern at the attacker's host used *port 135 TCP* to allow the local host scan and transmit RPC DCOM exploit codes to the remote host which execute the windows shell to initiate worm code to be downloaded using *port 4444 TCP*.

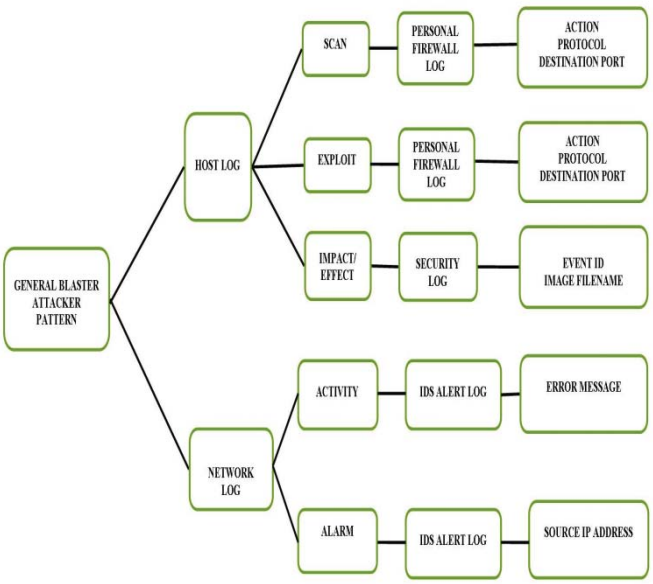

Fig.4 Proposed general Blaster's attacker attack pattern

Then TFTP client service is launched using *port 69* to allow the client (remote host) to download the worm code from the local host. The activity of *TCP Portsweep* also exists in the network log that supports all the fingerprint found on the host.

B. General Victim Pattern

Victim's attack pattern is useful for identifying on how the victim attacked by the potential attacker.

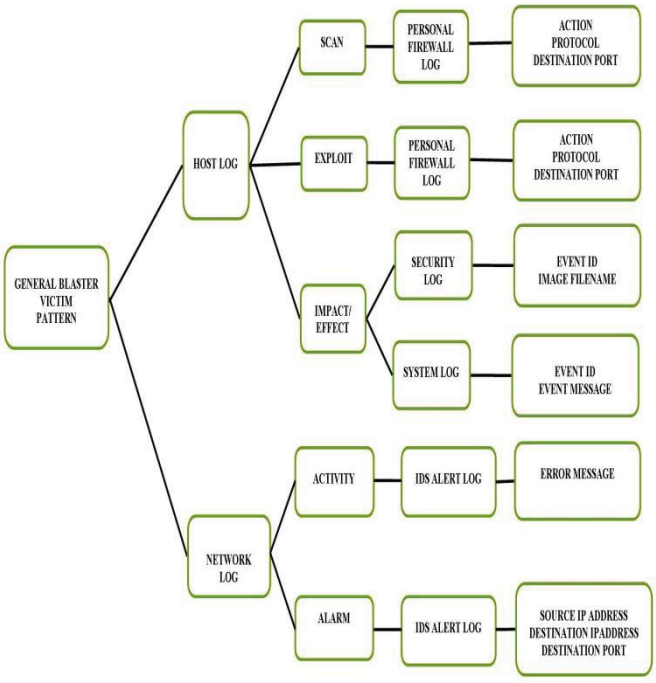

Fig.5 Proposed general Blaster's victim attack pattern

According to the analysis and findings from TABLE II, the overall general victim's attack pattern is summarized in Fig. 5. The fingerprint described that the blaster worm attack pattern at the victim's host used *port 135 TCP* to authorize the scanning and transmitting RPC DCOM exploit codes from remote host which execute the windows shell to begin downloading the worm code through *port 4444 TCP*. Next the *TFTP* client service is launched on *port 69* to download the worm code. The *TFTP Get* on *port 69 UDP* fingerprint is traced in the network log that supports the entire fingerprint found on the host log.

C. General Multi-step (Victim/Attacker/) Pattern

Multi-step's attack pattern is used as a guide for administrator to identify the true attacker or true victim. This attack pattern is a combination of victim's and attacker's attack pattern in which the data is extracted from a log of the same host.

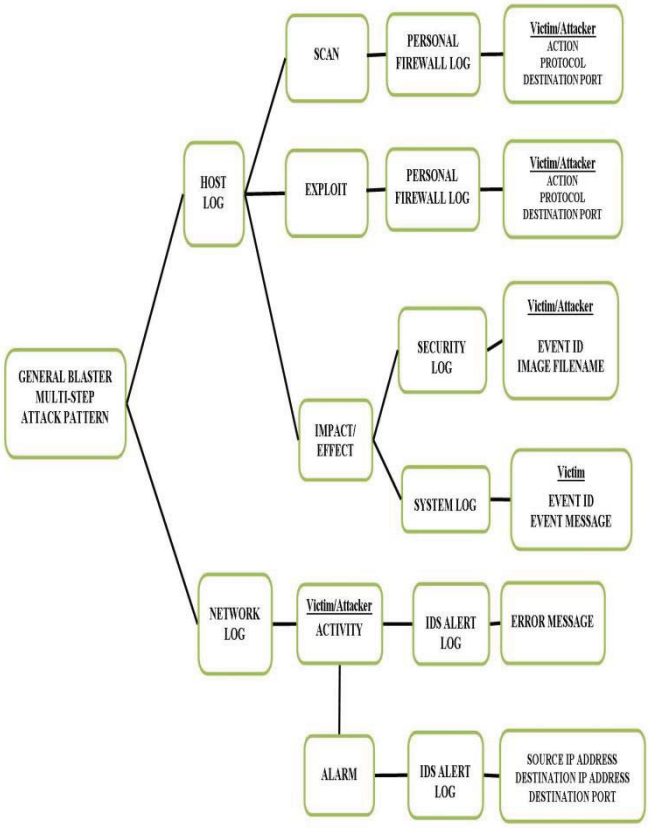

Fig. 6 Proposed General Blaster's Multi-step Attack Pattern

Referring to the analysis done in TABLE III, the summary of the fingerprint on multi-step at the host's logs from victim/attacker perspective depicted in

Fig. 6 illustrated the blaster worm scanning and exploiting activity by using *port 135 TCP* and *port 69 UDP* respectively. This is based on the fingerprint captured in network logs, showing *(Portscan) TCP Portsweep* and *TFTP Get* activities. The worm then transfers RPC DCOM exploit codes from remote host which perform the windows shell to download the worm code through port *4444 TCP*.

Immediately after the host is infected (act as victim), it's (act as attacker) then generate traffic; attempt to infect other vulnerable hosts. Based on the *TFTP Get*, the *source IP address* from the host log described the remote host is the victim and the *destination IP address* which is the local host is the attacker. Hence, the proposed general multi-step

(victim/attacker) attack pattern could identify the true victim or true attacker.

VI. Conclusions and Future Works

In this paper, the researchers have analyzed diverse logs in order to identify attack pattern from attacker and victim perspective in three different Blaster attack scenario: scenario A, scenario B and scenario C. The output of the analysis are the proposed general worm attacker attack pattern, general worm victim attack pattern and general worm multi-step attack pattern for Blaster. This general worm attack pattern is then extended to be further used in designing worm attack model. The finding is essential for further research in alert correlation and computer forensic investigation.

Acknowledgement

We thank to Universiti Teknikal Malaysia Melaka for the Short Grant funding (PJP/2009/FTMK (8D)S557) for this research project.

References

[1] Bailey, M., Cooke, E., Jahanian, F., Watson, D., & Nazario, J. (2005). The Blaster Worm: Then and Now. *IEEE Computer Society*.

[2] Foster, A. L. (2004). Colleges Brace for the Next Worm. *The Chronicle of Higher Education, 50* (28), A29.

[3] McAfee. (2003). Virus Profile: W32/Lovsan.worm.a [Electronic Version]. Retrieved 23 July 2009 from http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=100547.

[4] Hoglund, G., & McGraw, G. (2004). *Exploiting Software: How to Break Code*. Boston, Massachussetts: Addison-Wesley/Pearson.

[5] P. Moore, A., J. Ellison, R., & C. Linger, R. (2001). *Attack Modeling for Information Security and Survivability.* (No. CMU/SEI-2001-TN-001.): Pittsburgh, Pennsylvania: Software Engineering Institute, Carnegie Mellon University.

[6] Barnum, S., & Sethi, A. (2006). Introduction to Attack Patterns. [Electronic Version]. Retrieved 18 April 2010.

[7] Fernandez, E., Pelaez, J., & Larrondo-Petrie, M. (2007). *Attack Patterns: A New Forensic and Design Tool.* Paper presented at the IFIP International Federation for Information Processing.

[8] Kent, K., Chevalier, S., Grance, T., & Dang., H. (2006). Guide to Integrating Forensic Techniques into Incident Response: NIST Special Publication 800-86.

[9] Robiah, Y., Siti Rahayu, S., Shahrin, S., Mohd Faizal, A., Mohd Zaki, M., & Marliza, R. (2010). New Multi-step Worm Attack Model. *Journal of Computing, 2*(1), 1-7.

[10] Microsoft. (2003). Virus alert about the Blaster worm and its variants [Electronic Version]. Retrieved 23 July 2009 from http://support.microsoft.com/kb/826955

[11] Symantec. (2003, 9 December 2003). W32.Blaster.Worm. Retrieved 27 January, 2010, from http://www.symantec.com/security_response/writeup.jsp?docid=2003-081113-0229-99&tabid=2

[12] Cliff, C. Z., Don, T., & Weibo, G. (2006). On the Performance of Internet Worm Scanning Strategies. *ACM Performance and Evaluation Journal., 63* (7), 700-723.

[13] Dübendorfer, T., Arno, W., Theus, H., & B, P. (2005, 7-8 July). *Flow-Level Traffic Analysis of the Blaster and SobigWorm Outbreaks in an Internet Backbone* Paper presented at the Detection of Intrusions and Malware & Vulnerability Assessment, IEEE. , Vienna, Austria.

[14] Braverman, M. (2005, October). *Win32/Blaster: A Case Study from Microsoft's Perspective.* Paper presented at the Virus Bulletin Conference.