Malware Attacks Intelligence in Higher Education Networks

Charles Lim, Louis Lukito
The Indonesia Honeynet Project

Keywords:

Malware
Malware Analysis
Honeypot

ABSTRACT

Malware attacks have been the highest cyber security threats in many organizations for the last decade. The objective of this research is to analyze malware attacks discovered from implementation of honeypot dionaea at XYZ University. We described malware captured and malware analysis of each malware samples. Our analysis showed that there have been a surge of malware in terms of numbers as well as types and these threats need to be investigated to learn how these attacks affecting higher education network. We presented some recommendation to higher education on how to start their own effort to detect these growing malware attacks and learn how to anticipate malware behavior trends in higher education network.

Corresponding Author:

Charles Lim,
The Indonesia Honeynet Project
Email: Charles.lims@gmail.com

1. INTRODUCTION

With more and more people are using Internet for their daily activities, which include personal email, web browsing and personal financial transaction. Besides the benefits delivered by internet, there are cyber criminals whose exploiting tools and tries to cause harm to systems for their own advantage. Hacker may use malware as a way to breach security. According to Packel, E.A. (2012) [1], a malware named as Stuxnet was used to infect industrial equipment in Iran and cause destruction of centrifuges used to enrich uranium by modifying spin out of control. Uranium is made to construct nuclear weapon.

Unique malware samples are growing significantly over years starting from year 2005 until 2010 [2]. In addition, Ellen Messmer [3] has quoted that based on McAfee fourth quarter threat reports, the unique malware samples reached 75 million in 2011. The damage performed by malware attack may cause financial losses. Computer Economics Inc. [4] reported the worldwide damage caused by malware in total $13.3 billion. Even though antivirus software is good for protection against malware, however, antivirus software cannot 100 percent able to detect incoming malware attack. According to Mary Landesman [5], antivirus software relying on recorded malware signature to detect incoming malware attack. Therefore, antivirus cannot detect unknown malware and there is possibility of zero day exploit. Signature-based detection performed by antivirus depends on identification of unique strings in binary code [6]. First, antivirus vendor has to collect new malware, analyze it then create new signature. During the period of appearance of new malware and signature update, computers are vulnerable for malware attack.

Our goal in this research is to understand how malware threats affected university infrastructure and how we can provide some “intelligence” to the University by providing actual and live statistics, analysis of the malware attacks and recommendation to the University to counter these threats.

2. RESEARCH METHODOLOGY

Our research methodology follow closely malware analysis framework proposed by Roberto [8]. Sample of malware were collected from implementation of honeypot dionaea, and each of the malware sample, captured, is named using MD5 hash value of the sample. Then, each malware samples is analyzed using static analysis to understand the structure of the malware code and dynamic analysis to understand the behavior of malware when being executed in a isolated environment. In last step, malware samples are then uploaded to virustotal, a free and online virus scanner, to be scanned by several antivirus software.

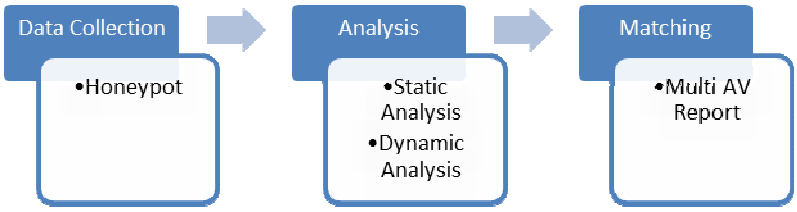

Figure 1. Malware Analysis Framework [8]

A Honeypot is "an information system resource whose value lies in unauthorized or illicit use of that resource" [7]. We have chosen to implement honeypot dionaea since most of the malware attacks occurred in Windows shared folder these days. Our honeypot dionaea was implemented in XYZ University and attached to public IP connection. Honeypot was located in a VM inside a physical computer and uses VMware workstation as virtualization software. Dionaea was configured earlier to open on specific ports and log certain information. Opened ports are http, https, tftp, ftp, smb, sip, MSSQL and MySQL. Opening many ports to ensure larger quantity of captured malware targeted to those ports. In addition, debug activities log should be removed to avoid unwanted logs recorded by dionaea.

Malware analysis is commonly performed using static and dynamic analysis. Static analysis is analysis of malware samples without executing it and the output of static analysis provide information such as data sections, imports, library used, strings, and anti-virus signature detection result. Tools used in our research are combination of Malwr, a free and online malware analysis tool, and Virustotal.

On the other hand, dynamic analysis is performed after malware sample is being executed in a sandbox environment. Dynamic analysis modules include file activities, registry activities, network activities and process activities. Dynamic Analysis tool we used in this research is Anubis [14]. Below is the table 1 that shows the comparison of output produced from these tools.

Table.1. Comparison Malware Analysis Tools

Virustotal	**Malwr**	**Anubis**
MD5	MD5	MD5
SHA-1	SHA-1	SHA-1
Imported DLL	Imported DLL	
PE Section	PE Section	
Machine Type		
Packer Identifier		
File Size	File Size	File Size
Malware Names		
File Type	File Type	
	Process Activity	Process Activity
	File Activity	File Activity
	Registry Activity	Registry Activity
	Network Analysis	
		Command line

3. MONITORING RESULTS

Dionaea monitoring was started from 10 April 2012 until 30 June 2012 and has caught various different malwares.

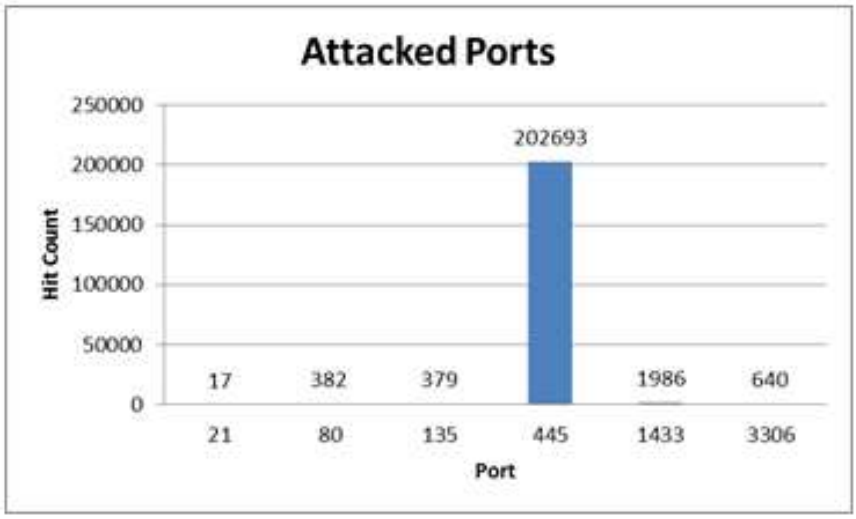

Figure 2. Number of Attacked ports

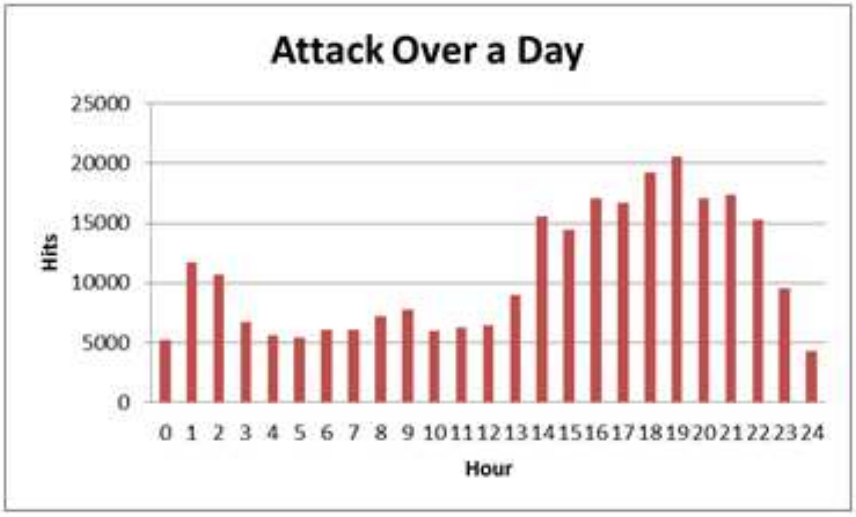

Figure 3. Attack Per Day

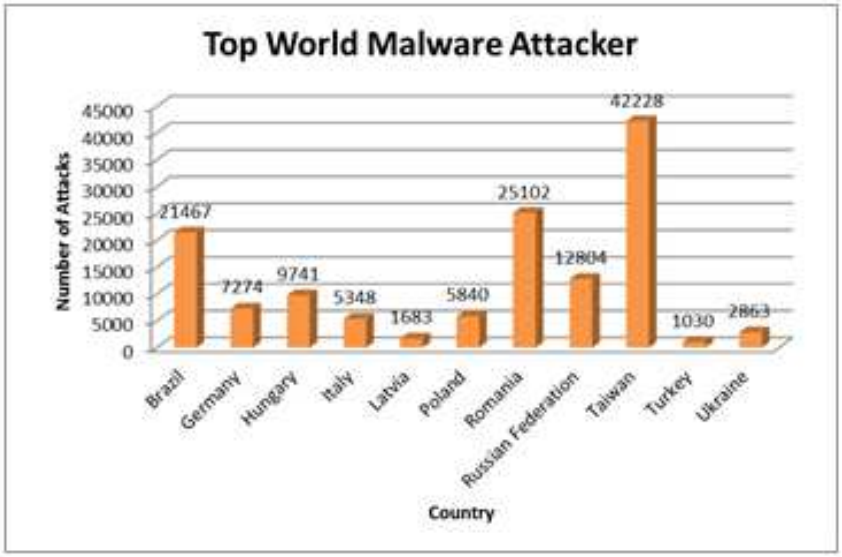

Figure 4. Top World Malware Attacker

For the period mentioned above, SMB service (port 445) seems to be the most frequent attacked service/port, as shown in figure 2. As observed in figure 3, the frequency of malware attack was highly active from noon until midnight. And during the monitoring period, Taiwan seems to be the country that generates most of the attacks as monitored by our honeypot system, as shown in figure 4.

Our collection of malware during the monitoring period consists of combination of Virus, Trojan, Worm and Spyware. Interestingly, during this period, most of the malware captured are conficker worms. Furthermore, all variant of conficker worms share same characteristics in terms of spreading method and execution command.

Below are the malware samples obtained through the honeypot installed (malware sample names uses MD5 hash function values of malware binaries captured)

3.1. 4d4c2729b8aa56e70eaf9ef84e9d5d3d

A Trojan horse that spawns many remote threads containing execution of particular malware file. In addition, the malware did DNS request to 74.125.224.53 and the IP host belongs to gmail.com. This malware is packed using Armadillo v1.71.

3.2. 6d0e0f6616d1aca972c84ad4a463827e

This Worm Allaple distributed malicious file to 5219 IP address under a subnet 81.88.0.0 and it made function call CreateRemoteThread 5363 times then execute malware file.

3.3. 14a09a48ad23fe0ea5a180bee8cb750a

The spyware collects some confidential information by changing registry value into cookies, history and cache. In addition, it creates a batch file in C:/ directory, executable ssms.exe file and merging registry file specified in 1.reg into registry. Moreover, it made network connection with botz.noretards.com on port 65146 as IRC server.

3.4. 036ee49ada38f73f2f5c51c9aced4ea4

This Trojan had network activity with 117.21.224.29 and creates explorer.exe and wuauclt.exe. Wuauclt.exe is windows update auto update client that checks updates to Microsoft website for host operating system.

3.5. 049b70ce8dd109ddb6a1129e59e52f35

The Trojan register itself to run in Windows startup program and changing registry by modifying ProxyEnable.

3.6. 9645f61e0913a58a29ecfcce940136fe

The rootkit downloads file.exe and file2.exe from a website that targeting to IP address 8.5.1.46. In addition, index.dat file is created in content, cookies and history.

3.7. b1efc25137fbe8d6d011e9be769ba551

This Trojan modifies the registry value by inserting new value intoHKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\" for running ecleaner.exe on Windows startup. The analysis report generated by Anubis shows there is IRC communication between sandbox and remote host.

3.8. db9e4e86f133975e2114898f8adac417

Trojan is known to create backdoor in computer and the remote attacker has an unauthorized access to computer via backdoor. IP address of 117.21.224.29 hosted by d.homler.net is suspected to be attacker's origin IP. This Trojan creates explorer.exe that manage to create a subdirectory "C:\RECYCLER\R-1-5-21-1482476501-1644491937-682003330-1013" and Desktop.ini and ecleaner.exe inside the subdirectory. In addition, then ecleaner.exe is configured to run on every windows reboot.

3.9. 393e2e61ff08a8f7439e3d2cfcb8056f

This malware is categorized as conficker worm. The total collected conficker worms are 548 malwares in honeypot dionaea. During the interaction of malware inside Anubis, it registers a dll file by executing command "regsvr32.exe /c /s .\d1.tmp.dll" stealthy. D1.tmp.dll is the result of modifying malware file name.

3.10. 6e9924223fb797722cf654f80640ec43

This malware was categorized as IRC bot that did registry activities and file activities then interact with outbound network. Firstly, it configures gwind.exe to run in windows startup, disabling proxy setting in internet explorer configuration. Then, it creates a directory containing both Desktop.ini and gwind.exe.

3.11. 7867de13bf22a7f3e3559044053e33e7

This malware replicates itself into 257 remote threads then spread it to numerous number of IP such as 67 IPs on port 139, 334 IPs on port 445 and 15 IPs on port 137. The outbound traffic caused by this malware for scanning other IPs for security vulnerability.

3.12. d05276441b548403dfe814cd84e0af86

It configures windows startup to run (C:\Documents and Settings\Administrator\Application Data\spooler.exe) and changed registry to include "Print Spooler" and "ctfmon.exe" in firewall authorized application list with registry key (HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List).

4. FURTHER ANALYSIS

During the monitoring period, we faced some challenges, which include common electricity issues in the server room – it is due to the nature of our experimental research where our server did not use any backup power such as UPS. This issue caused several outages during the course of our experiment and effect the overall number of malware samples captured. Nevertheless, longer period of time frame compensate these outages.

We are quite surprise to learn that most of the malware captured by our honeypot system is conficker worm. Conficker was an old malware and since 2011 the worm has infected more than 1.7 million hosts [9]. Some possibilities as to why these malware still active until today, include weak password and obsolete security updates [10]. In addition, other malware include IRC bot. These IRC bots are used to open backdoors in the infected computers to connect to IRC server [11]. The Trojan maintains IRC connection from IRC infected hosts to IRC master that waiting for commands from attackers.

As mentioned earlier that the highest volume of attacks has the origin from Taiwan. However, Taiwan may not be the real malware attack origin because malware attacker may use proxy or spoofing IP that pretending malware attacks come from Taiwan [12]. According to Barry Greene [13], the origin attacker's IP can be faked or spoofable.

5. CONCLUSION

We have successfully implemented Dionaea honeypot and analyzed the malware captured using combination of static and behavior analysis. Based on our research, the highest percentage malware infection was performed by conficker worm. Security updates and strong password could prevent host from conficker worm and Trojan infection. Trojan commonly setup IRC channel to communicate with the attacker to receive further instruction. Our analysis showed that attack from the origin of a certain country does not reflect the true source of attacks since the attacker may use proxy to masquerade the source of attack. Our future works include setting up more honeypots that monitor other services, not covered by Dionaea honeypot and automatically conducting analysis process that generate comprehensive reports as captured malware samples may grow exponentially during monitoring period.

REFERENCES

[1] E. Packel, [internet] 2012 [cited 2013 July 10]. Available from: http://www.databreachlegalwatch.com/2012/05/cyber-warfare-and-collateral-damage-flame-malware-heats-up-data-security-threat/

[2] ESET. 2012 [cited 2013 July 10]. Available from: http://go.eset.com/us/threat-center/

[3] E. Messmer, Unique malware samples broke the 75 million mark in 2011 [internet]. 2012 [cited 2013 July 10]. Available from: http://www.networkworld.com/news/2012/022112-mcafee-malware-report-256316.html

[4] Computer Economics [internet]. 2007 [cited 2013 July 10]. Available from: http://www.computereconomics.com/article.cfm?id=1225

[5] M. Landesman, [internet]. [cited 2013 July 10]. Available from: http://antivirus.about.com/od/antivirusglossary/a/What-Is-Antivirus-Software.htm

[6] Shabtai A. Moskovitch R. Elovici Y. Glezer C. Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey. Information Security Tech Report; 2009

[7] L. Spitzner, "History and Definition of Honeypots," in Honeypots: Tracking hackers. Addison Wesley; 2002.

[8] R. Roberto, Run-Time Malware Analysis System. [internet]. [cited 2013 July 10]. Available from: http://www.kaspersky.com/images/sponchioni,_roberto_-_rmas_a_framework_for_malware_analysis_and_malware_detection-10-98486.pdf
[9] Microsoft Security Intelligence Report [internet]. [cited 2013 July 10]. http://www.microsoft.com/security/sir/story/default.aspx#!conficker
[10] Microsoft Safety & Security Center [internet]. [cited 2013 July 10]. Available from: http://www.microsoft.com/security/pc-security/conficker.aspx
[11] Malware Protection Center [internet]. [cited 2013 July 10]. Available from: http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx
[12] CAIDA. [internet]. [cited 2013 July 10]. Available from: http://www.caida.org/projects/network_telescope/
[13] B. Greene, SENKI. [internet]. [cited 2013 July 10]. Available from: http://www.senki.org/everyone-should-be-deploying-bcp-38-wait-they-are/http://www.senki.org/everyone-should-be-deploying-bcp-38-wait-they-are/
[14] International Secure Systems Lab. Anubis: Analyzing unknown binaries. [cited 2013 July 10] http://anubis.iseclab.org

BIBLIOGRAPHY OF AUTHORS

	Charles Lim is currently leading Indonesia Chapter of Honeynet Project. He completed his Master Degree in Electrical Engineering from University of Hawaii-Manoa, HI, USA in 1991 and Bachelor Degree in Electrical Engineering from University of Wisconsin-Madison, WI, USA in 1989. He is currently an active lecturer and researcher of Swiss German University. He has extensive IT consulting experiences before joining Swiss German University in 2007. His current research interests are Malware, Web Security, Vulnerability Analysis, Digital Forensics, Intrusion Detection and Cloud Security
	Louis Lukito is a currently working as a System Specialist at PT. Prisma Global Solusi. He completed his bachelor of science from Binus International University in 2012. He is a member of Indonesia Honeynet Project.