OIC-CERT Computer Emergency Response Team

OIC-CERT Journal of Cyber Security
Volume 2, Issue 1 (February 2020)
69 – 76

Malware Discovery using Lebahnet Technology

Fathi Kamil Mohad Zainudin[1], Izzatul Hazirah Ishak[2], Sharifuddin Sulaman[3], Farah Ramlee[4], Nur Sarah Jamaludin[5], and Shuaib Chantando[6]
[1,2,4,5,6] Malaysia Computer Emergency Response Team, CyberSecurity Malaysia, Cyberjaya, Malaysia
[3] International Engagement, CyberSecurity Malaysia, Cyberjaya, Malaysia
fathi.kamil@cybersecurity.my, izzatul.hazirah@cybersecurity.my, sharifuddin@cybersecurity.my, farah.ramlee@cybersecurity.my, nursarah.jamaludin@cybersecurity.my, shuaib@cybersecurity.my

ARTICLE INFO

Article History
Received 4 Jul 2019
Received in revised form 15 Aug 2019
Accepted 25 Sep 2019

Keywords:
malware discovery, lebahnet, honeypot

ABSTRACT

Recent trends indicate that the cyber-crimes caused by the malware is increasing as these malicious tools are authored to spread through multiple platform and affecting the millions of users. In order to explore new attack and exploitation trends, virtual honeypot is used to simulate the virtual computer systems at the network level. This paper presents the Lebahnet technology, an improved version of virtual honeypots which consists of simulated the networking stack of different operating systems, data analytics and visualisation platform and also the sandboxing technology to examine the code samples behaviour. This paper also discusses the Lebahnet architecture and shows how the Lebahnet framework helps to explore new attack trends and provide insight for early warning mechanism.

I. INTRODUCTION

Cyber-crimes are crimes that occurs via the Internet that is increasing from previous years and shows no sign of decreasing in the near future. It has already been considered in alarming stage since the Internet of Things (IoT) nowadays are crucial in day-to-day activities to help human life easier. This eventually opens up an opportunity for adversaries to gain financially and keep on evolving the technique, tactics and procedures of cyber-attacks to potential targets every day.

In recent news, most of the cyber threats' goals are targeting for profitable gains. Based on a study conducted by Centre for Risk Studies, University of Cambridge, the WannaCry ransomware cryptoworm resulted in an estimated US$4 billion in losses globally where NotPetya's wiper cryptoworm caused an estimated US$10 billion in losses [1]. Surprisingly, the victims especially businesses would be willing to forked out the expenses and pay upwards of close to a million dollar to decrypt their data [2] without knowing whether they would receive the decryption keys from the attacker. This fact will only lead the attacker to gain more financially and is deemed intolerable for the victim's business returns.

NTT Communication in 2018 Global Threat Intelligence Report (GTIR) highlighted that ransomware attacks are growing more than 350 percent compared to attacks in 2016 [3]. Well known malware such as ransomware, crypto jacking and data breaches are foreseen as top common cybercrime listed nowadays. These attacks

ISSN 2636-9680
eISSN 2682-9266

are focusing on the adversary's intent, capability and opportunity to compromise an organization to achieve their desired objectives. Threat actors are then motivated to persistently attack their targets and would eventually formulate behavioural profiles based on the trends of intrusion used that is known as campaign. As a result, a harmless computer can turnaround into a powerful device for illegal activity based on the actor's preferences.

As an initiative to mitigate cyber-attacks, Malaysia Computer Emergency Response (MyCERT) developed a CyberSecurity Malaysia Honeynet Project, also known as Lebahnet. Lebahnet is developed based on honeypot technology. The purpose of this technology is to lure cyber attackers to invade into other valuable machine and obtain unauthorised access to information systems, allow in-depth analysis of techniques and approaches of adversaries during and after exploitation of the machine or provide early warning about new attack and exploitation trends[4]. MyCERT utilised Lebahnet to generate high value information that is focused on network trends and malicious activities to support advisory and incident handling activities. This paper will discuss on malware collected and analysis starting in 2017 until May 2019 using Lebahnet.

.

II. METHODOLOGY

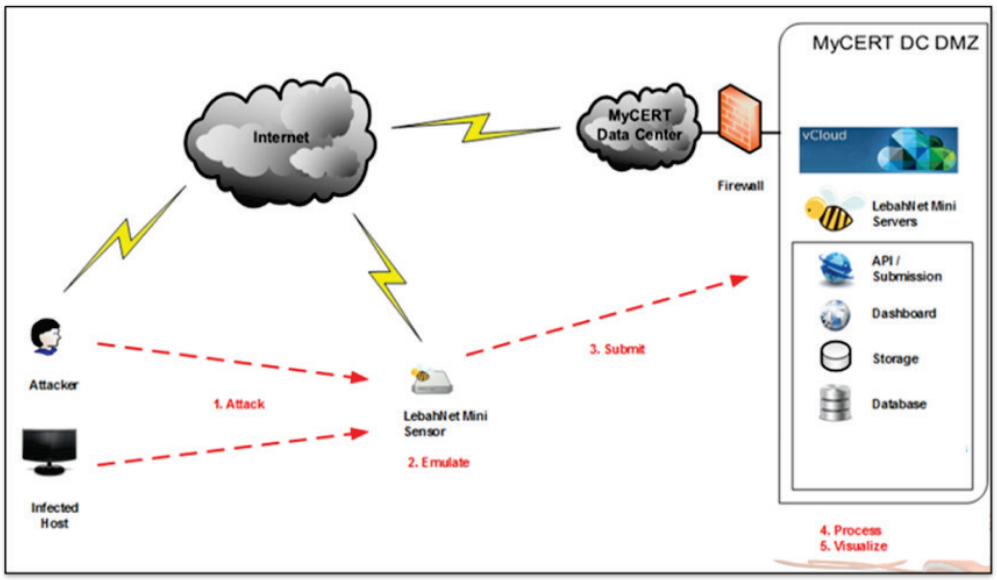

Fig. 1: Overview of Lebahnet

The current version of Lebahnet sensor consist of 2 main components for service emulations which known as Cowrie and Dionaea. These emulations work by luring attacker to think they have successfully compromised a real valuable machine when it is actually a disguise setup for them to run malicious activities. This is because the emulation services respond to each command and request from the attacker.

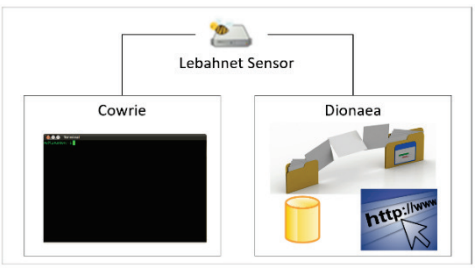

Fig. 2: Lebahnet component

ISSN 2636-9680
eISSN 2682-9266

A. Cowrie Honeypot

Cowrie is an open source project which is developed by Michel Oosterhof. It covers the medium interaction Secure Shell (SSH) and Telnet honeypot which can generate log brute force attacks and attacker's shell interaction. When accessing Lebahnet sensor using SSH, the attacker needs to guess all possible combination of username and password to have access into the server. This scenario gives the attacker to experience "real situation" before gaining access into the server. Upon success gaining access into the sensor, the attacker may proceed with the malicious activities which will be logged and used for further analysis in Lebahnet.

B. Dionaea Honeypot

Dionaea is intended to replace Nepenthes honeypot which is renowned as a malware capturing honeypot which was initially developed under the 2009 Google Summer of Code (GSoC) Honeynet Project's. By utilising Dionaea component in the sensor, the malicious payloads will be captured and used for deep analysis and investigation. Dionaea uses LibEmu to detect the shellcode in the malicious file which make it surpass the capability in Nepenthes honeypot. LibEmu is a library that can be used for x86 emulation and shellcode detection [5]. The small piece of executable binary code is called shellcode [6]. If there is existence of the shellcode in the payload, LibEmu has the capability to execute it in LibEmu VM for assessment or profiling. Each API calls and arguments are recorded and need to be allowed to act such as creating network connection at the first place. This will facilitate the evaluation of the shellcode. Shellcode execution is sufficient to profiling most shellcodes; but not for multi-stage shellcodes [7], [8].

C. Kibana

All data captured via Lebahnet sensors is then been analysed and visualised in Kibana, one of the open source analytics and visualisation tools available. Due to the large amount of Lebahnet data, using Kibana as a platform to analyse data is convenient and cost saving.

Fig. 3: Overview Lebahnet Data in Kibana

D. Cuckoo Sandbox

Once the malware details have been harvested and listed, the sample of the malware is being searched through open source repository or in the wild and will be analysed or re-analysed using MyCERT's very own Cuckoo Sandbox. The sandbox is chosen because it is the leading open source automated malware analysis system [9].

All data captured via Lebahnet sensors is then be analysed and visualised in Kibana. Due to the large amount of Lebahnet data, using Kibana as a platform to analyse data is convenient and cost saving.

ISSN 2636-9680
eISSN 2682-9266

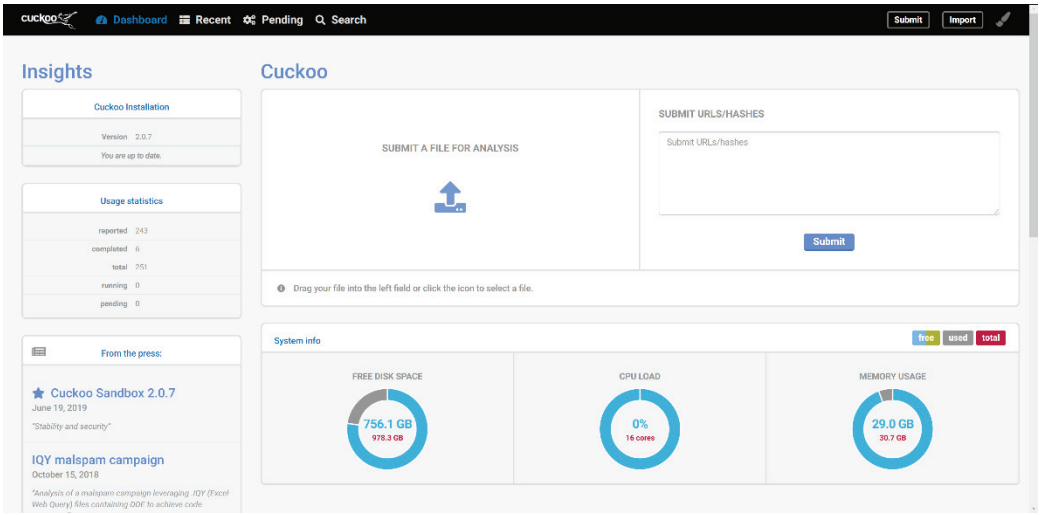

Fig. 4: MyCERT Cuckoo Sandbox

III. DISCUSSION

A typical IT Infrastructure that most small medium organisations used usually are vulnerable despite taking best practice measurement into consideration. The existing security element in a traditional infrastructure implemented may only be sufficient to block and filter any incoming attacks. However, attackers are often a step ahead and will always find ways to bypass the infrastructure and creating new attack patterns. It is important to understand how malware is operating in order to grasp the context, motivations, and the goals of an attack.

Hence, Lebahnet sensors are being placed in organisation's network. At the initial state of the attack, the sensor will respond by emulating according to the attack patterns and attackers' continuous attempts to drop the malware artefact. The payload is then captured and details of the malware such as binaries and hashes are being stored which later will be analyse and visualise in Kibana.

In Kibana, for malware visualisation, selecting term *metadata.md5.keyword* and sorting the result in descending order, the malware hashes later will be displayed where the highest count is displayed at the top. It is recommended to rename metadata.md5.keyword for a better display in data table type of visualisation.

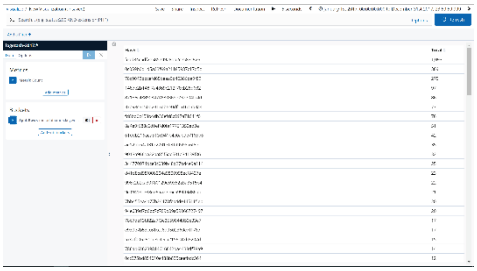

Fig. 5: Overview malware visualisation in Kibana

Illustrated in **Fig. 6** shows the general total malware captured within 2017 until May 2019. Starting from January 2017 until May 2019, a total of 15 858 of known malware binaries are been captured using Lebahnet technology. From 2703 in 2017, the total known malware captured is increased by 5582 in 2018. Even though the statistical data used on 2019 is until May, however, the total known malware captured is more than half of the statistic value in 2018.

ISSN 2636-9680
eISSN 2682-9266

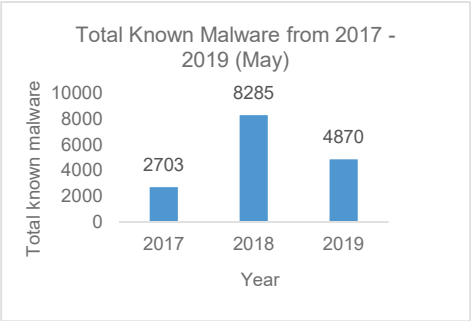

Fig. 6: Malware Trend From 2017 – 2019 (May) 1

Moving forward, **Fig. 7** shows the malware section classified by malware type. Ransomware attack in 2018 hit the highest total captured compare to the previous year, where Worm is the highest malware captured in 2017. Trojan Downloader and Trojan in 2018 also increased contrast with the previous year. Until May 2019, there is no sign for the Ransomware attack to be decline. In 2019, there is a new detection malware type which is known as Virus starts to peep in the Lebahnet technology. However, there is no sign that this malware type will be maintain in the future as the DDOS and Backdoor is not yet been found after 2017 and above. The pattern on the malware type is affected by the user utilisation which can be proved by the ransomware attack started to skyrocket from 2017 until today due to the big impact from all around the world.

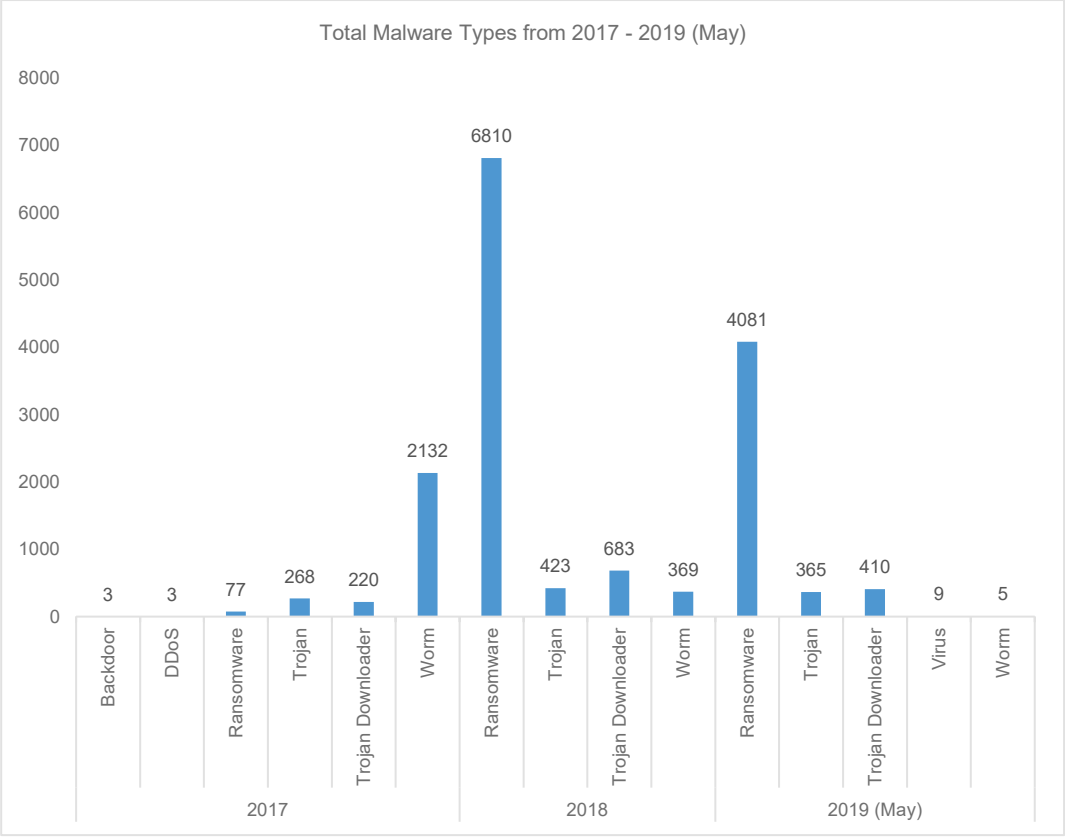

Fig. 7: Malware Trend From 2017 – 2019 (May) 2

From the results of the search, below are the highest malware hashes that have targeted our sensors.

ISSN 2636-9680
eISSN 2682-9266

TABLE 1: Data Extractions results from Kibana

Year	Total hits	Hash (MD5)	Malware
2017	1093	fead84c5df2e585749a8da2ce583c926	Conficker
2018	2266	ae12bb54af31227017feffd9598a6f5e	Wannacry Ransomware
2019 (January - May)	1186	ae12bb54af31227017feffd9598a6f5e	WannaCry Ransomware

In 2017, the highest hit to our sensors was a Conficker malware that was named after a vmware file. Details of the malware are as below:

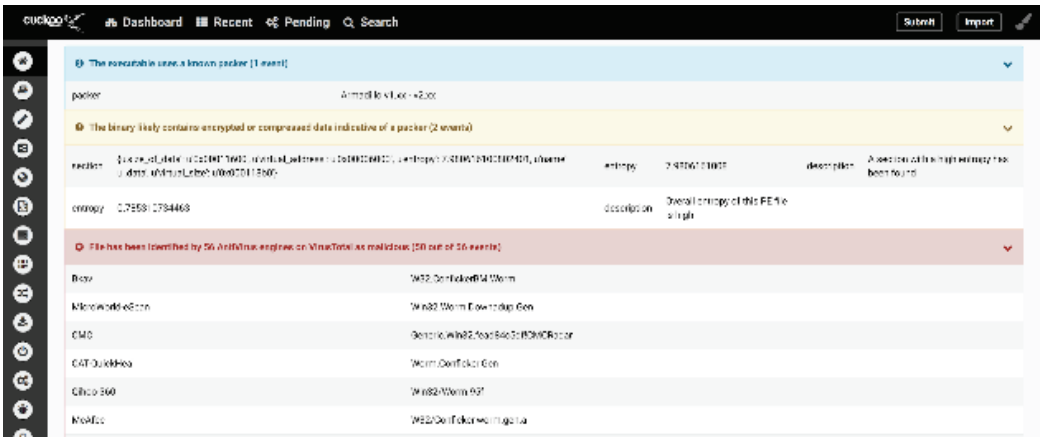

Fig. 8: Conficker result in MyCERT's Cuckoo Sandbox

Filename: jwgkvsq.vmx or jwgkvsq.dll
Md5:
fead84c5df2e585749a8da2ce583c926
File type: Win32 DLL
PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
File Size: 166.51 KB (170505 bytes)

This malware also known as Downadup, Downadup and Kido, that was first detected in November 2008 and is a fast-spreading worm that targets a vulnerability (MS08-067) in Windows operating systems.

From the sandbox analysis result, the malware is seen using the .vmx file extension in naming the malicious file to lure victims to think they are opening a harmless virtual machine file. This file is a disguise and it is actually a DLL that could allow remote code execution if an affected system received a specially crafted RPC request and later run arbitrary codes without authentication.

This shows that malware is still at large even after many years of existing. This could be the reason that the operating system that is vulnerable to this exploit is still being used in the network where our sensors were being deployed. It proves that malwares can be reused and evolved as years gone by.

As for 2018 and mid-year of 2019, the top hit malware found in our sensors is known as WannaCry ransomware. Ransomware is one of malware types that infects computing platform and limits

ISSN 2636-9680
eISSN 2682-9266

user's access until the stated ransom amount is paid in order to access the encrypted file. WannaCry ransomware infects the victim computers via EternalBlue vulnerability that exist in the Windows Server Message Block (SMB) service which later patched by Microsoft in March (MS17-010) [10]. Details of the malware are as per below:

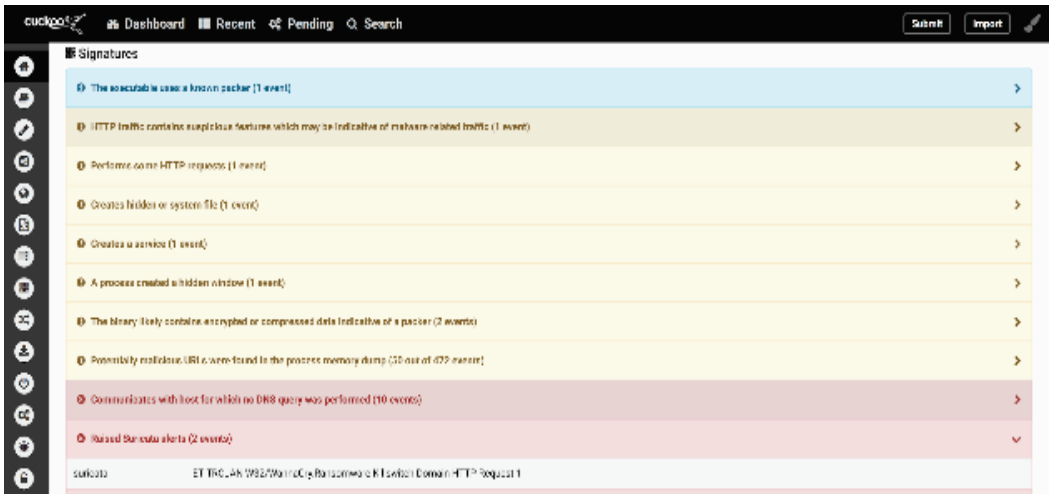

Fig. 9: Wannacry result in MyCERT's Cuckoo Sandbox

Filename: 1561866018332_hbtbr_dionaeajpn1_ae12bb54af31227017feffd9598a6f5e
Md5: ae12bb54af31227017feffd9598a6f5e
File type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
File Size: 5.0 MB (5145000 bytes)

From the sandbox analysis, the malware is a DLL file. It is a dropper that is being used to download process that can impersonate a legitimate process. Through an export function called "PlayGame" in the DLL file, the process is then being spawned as "mssecsvc.exe" which is exploiting the "CVE-2017-0147" to compromise the neighbouring PCs in the same network.

WannaCry ransomware started to spread in May 2017 but Microsoft have announced the patch in March 2017. Meanwhile, Lebahnet sensors detected this malware binary on October 2017. Over the past two years, two hundred sixty (260) of different binaries and hashes has been detected which is related to WannaCry ransomware.

IV. CHALLENGES

From the past few years of Lebahnet technology consumption, the data captured only covered certain region and area based on the participation from organisation and institution. Thus, the statistic data limited to the covered region or area. Apart from that, Lebahnet technology need to be enhanced and keep maintaining the same pace with the current IoT device as IoT evolves for the past few years and even for the future. In order to detect new malware, the detection of malware technology needs to be enhanced. However, the deficiency of LibEmu library which is been used in Dionaea component is only capable to analyse and profile for single-stage shellcode. As a result, the profiling is insufficient for the multi-stage shellcode as the data from the second shellcode and upward cannot be recorded for further analysis. This might affect Lebahnet technology to miss certain valuable binary to be analysed.

ISSN 2636-9680
eISSN 2682-9266

V. CONCLUSION

Lebahnet technology is developed based on honeypot technology. The deployment of Lebahnet technology successfully serve it purpose. Not to mention that the data captured can be used for further analysis such as malware binaries and hashes. According to the malware binaries and hashes collected, this paper concludes the findings from 2017 until May 2019, the malware trend changes from Conficker malware in 2017 to Wannacry ransomware in early 2018. However, there is a possibility to have a change in the malware trend in the future based on the vulnerable exploits which will be discovered in the future. Apart from the evolving of malware, the number of operating system using the vulnerability to the exploit contributes to the growth of the malware within the network. This is because the attacker or attackers believes that the potential victims exist all around the world, thanks to the Internet.

VI. REFERENCES

[1] S.K.A. Manoj and D.L. Bhaskari, "Cloud forensics-A framework for investigating cyber attacks in cloud environment," *Procedia Computer Science*, 85 (Cms), pp.149–154, 2016.

[1] A. Coburn et al., "Cyber risk outlook", Risk Management Solutions, Inc., California, 2019.

[2] IBM Security, "IBM study: Businesses more likely to pay ransomware than consumers", 2016. [Online]. Available: https://www03.ibm.com/press/us/en/pressrelease/51230.wss. [Accessed: 14-Jun-2019].

[3] NTT Communications, "2018 global threat intelligence report", 2018.

[4] N. Provos, "A virtual honeypot framework", in *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA, USA, 2004, pp. 1–14.

[5] D. Lukan, "Shellcode detection and emulation with libemu", 2014. [Online]. Available: https://resources.infosecinstitute.com/shellcode-detection-emulation-libemu/. [Accessed: 15-Jun-2019].

[6] T. Lu, L. Zhang, and Y. Fu, "A novel immune-inspired shellcode detection algorithm based on hyperellipsoid detectors", *Secur. Commun. Networks*, vol. 2018, p. 10, 2018.

[7] E. Tan, "Dionaea – A malware capturing honeypot", 2014. [Online]. Available: https://www.div0.sg/single-post/dionaea-malware-honeypot. [Accessed: 15-Jun-2019].

[8] S. Shahrivartehrani and Shadil Akimi Bin Zainal Abidin, "Dionaea honeypot implementation and malware analysis in cloud environment", *Journal of Computing Technologies and Creative Content,* vol. 1, pp. 1-5, 2016.

[9] S. Jamalpur, Y. S. Navya, P. Raja, G. Tagore, and G. R. K. Rao, "Dynamic malware analysis using cuckoo sandbox", in *2018 Second International Conference on Inventive Communication and Computational Technologies, Coimbatore, India, April 20-21 2018,* 2018, pp. 1058–1060.

[10] MyCERT, "MA-663.052017: MyCERT Advisory – Technical Detail: WannaCry Ransomware," 2017. [Online]. Available: https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1265/index.html. [Accessed: 10-Dec-2017].

ISSN 2636-9680
eISSN 2682-9266