

# Impact Analysis of Malware Based on Call Network API With Heuristic Detection Method

<sup>1</sup>One Tika Suryati, <sup>2</sup>Avon Budiono

<sup>1,2</sup>Department of Information System, School of Industrial and System Engineering, Telkom University

---

## Article Info

### Article history:

Received Feb 16, 2020

Revised Mar 11, 2020

Accepted Mar 25, 2020

---

### Keywords:

Malware

Malware analysis

Heuristic detection

Call network API

---

## ABSTRACT

Malware is a program that has a negative influence on computer systems that don't have user permissions. The purpose of making malware by hackers is to get profits in an illegal way. Therefore, we need a malware analysis. Malware analysis aims to determine the specifics of malware so that security can be built to protect computer devices. One method for analyzing malware is heuristic detection. Heuristic detection is an analytical method that allows finding new types of malware in a file or application. Many malwares are made to attack through the internet because of technological advancements. Based on these conditions, the malware analysis is carried out using the API call network with the heuristic detection method. This aims to identify the behavior of malware that attacks the network. The results of the analysis carried out are that most malware is spyware, which is lurking user activity and retrieving user data without the user's knowledge. In addition, there is also malware that is adware, which displays advertisements through pop-up windows on computer devices that interfaces with user activity. So that with these results, it can also be identified actions that can be taken by the user to protect his computer device, such as by installing antivirus or antimalware, not downloading unauthorized applications and not accessing unsafe websites.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



---

## Corresponding Author:

One Tika Suryati,  
Department of Information Systems,  
Telkom University,  
Bandung, West Java, Indonesia, 40257  
Email: [onetika@student.telkomuniversity.ac.id](mailto:onetika@student.telkomuniversity.ac.id)

---

## 1. INTRODUCTION

In the current era of globalization, technology and the internet are developing very rapidly. The internet has an important role in all fields in society both in terms of economics to government. But with the rapid development of the internet, making the security system on the internet and PC users must be further improved. One threat from the security system is the presence of cyber-crime. Cyber-crime is a variety of crimes that are illegal or prohibited by an individual or group of computer devices, network information technology, and actions targeting an individual in the internet world [1]. The US Department of Justice defines cyber-crime into three categories, namely, a crime where the main target is a computer device, a crime where a computer is used as a weapon (for example: denial-of-service (DoS) attacks) and crime where a computer is used as an accessory (example: used to store illegal data). The most common cybercrime attacks are attacks using malware. Malware or malicious software is software that is harmful to a computer system. Software that becomes malware generally can be in the form of worms, viruses, trojans, spyware, adware and rootkits.

At this time, malware generally spreads through various ways on the internet, such as through drive-by downloads, social engineering and exploitation of network services so

that users can be incited and deceived into using these services. The main purpose of an attacker is to make money from a computer that has been attacked by selling stolen data, sending spam emails and extortion [2]. According to anti-virus companies such as Symantec, there are reports that there are 4300 malware samples every day. While McAfee stated that there were 12300 malware samples every day [3]. Then according to a survey by FireEye in June 2013, the level of organizations that experienced incidents of malware security or network violations in the past year reached 47% [4].

The development of malware at this time, the need for malware analysis. Malware analysis techniques can help to understand the risk and intensity of the dangers of the malware. The results of the analysis obtained can be used to take preventative steps to overcome future threats from malware. Malware analysis is useful for seeing how malware works and seeing the nature of the malware. In this study, the malware analysis used is a static method with heuristic detection techniques. The advantage of using a static method is that it is faster and safer because it will collect the structure of the malware from the program code that it clicks on [5]. Malware analysis with heuristic detection uses information from an API call [13,14]. API call is a procedure, protocol and tool for building an application. Information from the API call will be used to determine the activity of malware, so that information will be used to classify malware using heuristic detection techniques. Heuristic detection is a technique that searches for or detects malware by searching for commands or instructions that do not exist in the application where it will be easier to detect types of malware that have not been discovered or known before [5]. The purpose of the malware analysis, which are also to know the characteristics of malware and the targets to be attacked by malware [6].

Based on these data, to classify types of malware the authors conducted research related to malware analysis and classification by conducting simulations on virtual machines using heuristic detection techniques. Therefore, the results of this study are in the form of analysis and classification of malware with heuristic detection techniques.

## **2. STUDY OF LITERATURE**

### **2.1 Definition of Malware**

Malware is a program that has a negative influence on a computer system that does not have user permission to refer to malware [7]. Malware is usually developed by people who are not responsible such as fraudsters, extortionists, vandals or other criminals who have the main goal to get money illegally [8]. Actions that are usually carried out by malware when it has been installed or entered into a system include [8]:

1. Flooding a computer system or web browser with advertisements.
2. Splitting themselves and attacking other files or systems.
3. Installing applications that trigger malware to work without the user's knowledge has an impact on computer performance.
4. Lock the file or operating system from the computer so that it cannot be used and force the user to make payments in order to access the file or operating system again.

Different types of malware, so different steps or actions that must be taken to remove the malware. Avoiding suspicious links, visiting unsafe websites, is one way to prevent a computer from being infected with malware.

### **2.2 Malware Classification**

According to [4,14-20], malware can be divided into several types, namely:

#### **1. Backdoor**

Is a malware that installs itself to attack computer devices. Backdoor works by entering the system and accessing files illegally. This malware will let users connect to the system and then will attack network traffic to get a password [21-24].

#### **2. Botnet**

Almost like a backdoor, but all computers accessed by attackers will receive the same commands that are managed remotely. Attacker will try to attack many computers that act as bots that can do a lot of spam attacks.

### 3. Rootkit

It is malware that hides dangerous program code. This malware is commonly used to hide worms, bots and malware. Rootkits can delete logs and hide processes from malware. The rootkit operating system is planted at the kernel level and core level so that it is difficult to detect.

### 4. Trojan-Horse

Malware disguised as legitimate software commonly used by hackers to get access to user systems.

### 5. Worm or virus

Malware that can reproduce itself and infect a user's computer. The virus spreads through programs that have been previously infected and are only active when the program is run. Whereas a worm is a stand-alone program and runs its program without relying on other programs.

### 6. Spyware

Malware is installed on a computer device without the knowledge of the user. Spyware causes a reduction in speed on the processor and network connection.

### 7. Adware

Adware is an application program that displays advertisements when the program is running, such as pop-up windows and banners.

## 2.3 Malware Analysis

Malware analysis is an investigation of malware that aims to find out specific malware that can build security to protect devices [9]. Heuristic Detection is a malware analysis technique that works by searching for commands or instructions that can enable the discovery of new types of malware [10]. Here are the advantages and disadvantages of heuristic detection [11]:

#### a. The advantages of heuristic detection are:

1. Can see the behavior of malware to be executed.
2. Potential to find unknown malware on the system.
3. Giving understanding to the unexpected in the future.
4. Can be used simultaneously with other analytical techniques.

#### b. The disadvantages of heuristic detection are:

1. Can give a false warning (false positive) to the system because of the detection of more detail.
2. Requires sufficient knowledge in analyzing
3. The analysis process is done manually so it requires more time.

## 2.4 Application Program Interface (API)

According to Vangie Beal, API is a procedure, protocol and tool for building an application that will determine how a software interacts. The advantage of using the Windows API is that it can save time in analysis but the drawback is the lack of tolerance for errors [12].

Generally, malware attacks the network functions in running its programs, because in Windows API the most common communication in an application is through the network [4]. Based on this statement, this research will focus on the network API for analysis.

Network API allows an application to communicate with other applications, but it can also be used as access to a sharing resource [12]. The way the API network works is by looping so that the network resources on an operating system become full and the computer's performance will be slower.

## 3. RESEARCH METHOD

In this study the method used is explained by using a conceptual model. Conceptual models can identify data in the research process so that they can formulate solutions to existing problems. With the explanation of the conceptual model, researchers can explain how a malware is analyzed with heuristic detection techniques so that it can find commands or instructions that have the potential to become malware.

The problem in this research is the development of types of malware in the internet world so that the operating system is more vulnerable on a computer. From these problems, obtained an opportunity to reduce vulnerabilities in the operating system of a computer is to do an analysis on a program or file that is suspected.

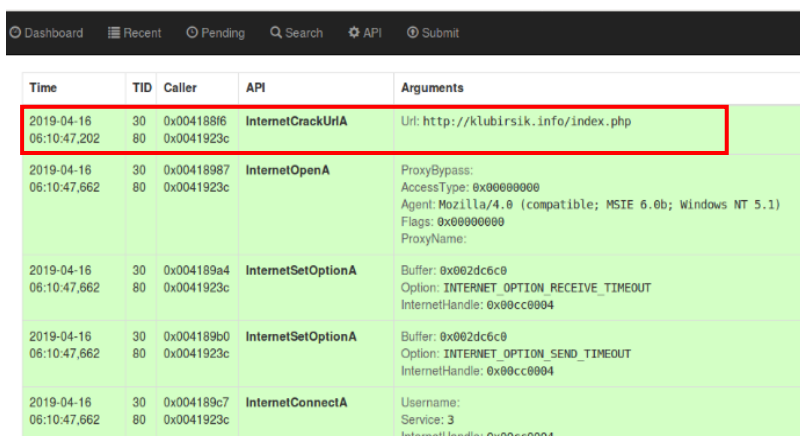
With the problems and opportunities contained in the research, an artifact can be generated, namely, in the form of malware analysis using heuristic detection techniques.

To perform malware analysis with heuristic detection techniques, concepts and methods are needed that can help the analysis. The concepts used include theories about static analysis, heuristic detection theory and API calls theory. While the method used is, literature study and malware analysis. The resulting analysis is a simulation of malware analysis based on the call network API using the heuristic detection method.

## 4. TEST RESULTS AND ANALYSIS

### 4.1. Testing Using Cuckoo Sandbox

Cuckoo Sandbox is a malware analysis tool that is installed on localhost. Data taken from the Cuckoo Sandbox is a network API.



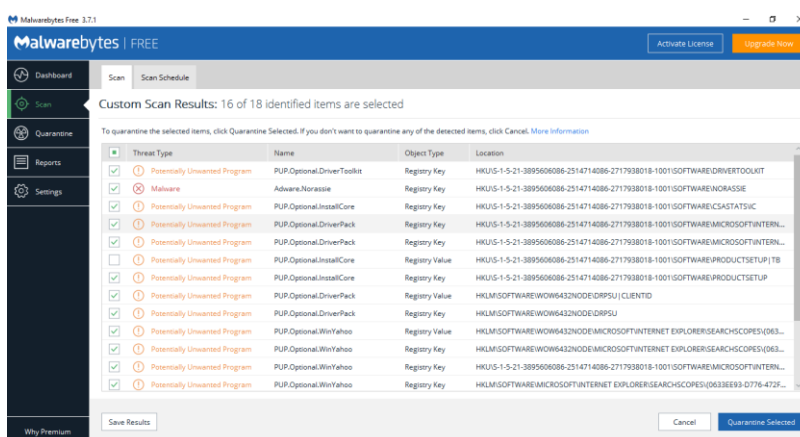
Time	TID	Caller	API	Arguments
2019-04-16 06:10:47,202	30 80	0x00418816 0x0041923c	InternetCrackUrlA	Url: http://klubirsik.info/index.php
2019-04-16 06:10:47,662	30 80	0x00418987 0x0041923c	InternetOpenA	ProxyBypass: AccessType: 0x00000000 Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1) Flags: 0x00000000 ProxyName:
2019-04-16 06:10:47,662	30 80	0x004189a4 0x0041923c	InternetSetOptionA	Buffer: 0x002dc6c0 Option: INTERNET_OPTION_RECEIVE_TIMEOUT InternetHandle: 0x00cc0004
2019-04-16 06:10:47,662	30 80	0x004189b0 0x0041923c	InternetSetOptionA	Buffer: 0x002dc6c0 Option: INTERNET_OPTION_SEND_TIMEOUT InternetHandle: 0x00cc0004
2019-04-16 06:10:47,662	30 80	0x004189c7 0x0041923c	InternetConnectA	Username: Service: 3 InternetHandle: 0x00cc0004

Figure 1. Results of the Cuckoo Sandbox

Figure 1 is the result of testing one of the malwares. It can be seen that there is some information regarding the network API used. One of them is the InternetCrackUrlA network API, which is a link targeted by malware. The link is a trap so that users access it so hackers can enter the user's computer system.

### 4.2. Testing Using Malwarebytes

Malwarebytes is an antimalware tool for scanning a program. This program will remove all malicious programs before the malicious program interferes with user activity.



Threat Type	Name	Object Type	Location
Potentially Unwanted Program	PUP.Optional.DriverToolkit	Registry Key	HKU\S-1-5-21-3895606086-2314714086-2717938018-1001\SOFTWARE\DRIVERTOOLKIT
Malware	Adware.Norassie	Registry Key	HKU\S-1-5-21-3895606086-2314714086-2717938018-1001\SOFTWARE\NORASSIE
Potentially Unwanted Program	PUP.Optional.InstallCore	Registry Key	HKU\S-1-5-21-3895606086-2314714086-2717938018-1001\SOFTWARE\CSASTATVIC
Potentially Unwanted Program	PUP.Optional.DriverPack	Registry Key	HKU\S-1-5-21-3895606086-2314714086-2717938018-1001\SOFTWARE\MICROSOFT\INTERNET...
Potentially Unwanted Program	PUP.Optional.DriverPack	Registry Key	HKU\S-1-5-21-3895606086-2314714086-2717938018-1001\SOFTWARE\MICROSOFT\INTERN...
Potentially Unwanted Program	PUP.Optional.InstallCore	Registry Value	HKU\S-1-5-21-3895606086-2314714086-2717938018-1001\SOFTWARE\PRODUCTSETUP\TB
Potentially Unwanted Program	PUP.Optional.InstallCore	Registry Key	HKU\S-1-5-21-3895606086-2314714086-2717938018-1001\SOFTWARE\PRODUCTSETUP
Potentially Unwanted Program	PUP.Optional.DriverPack	Registry Value	HKLM\SOFTWARE\WOW6432NODE\DRPSU\CLIENTID
Potentially Unwanted Program	PUP.Optional.DriverPack	Registry Key	HKLM\SOFTWARE\WOW6432NODE\DRPSU
Potentially Unwanted Program	PUP.Optional.WinYahoo	Registry Value	HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\INTERNET EXPLORER\SEARCHSCOPES\063...
Potentially Unwanted Program	PUP.Optional.WinYahoo	Registry Key	HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\INTERNET EXPLORER\SEARCHSCOPES\063...
Potentially Unwanted Program	PUP.Optional.WinYahoo	Registry Key	HKU\S-1-5-21-3895606086-2314714086-2717938018-1001\SOFTWARE\MICROSOFT\INTERN...
Potentially Unwanted Program	PUP.Optional.WinYahoo	Registry Key	HKLM\SOFTWARE\MICROSOFT\INTERNET EXPLORER\SEARCHSCOPES\0633EE93-0778-472F...

Figure 2. Malwarebytes Scanning Results

From the results of scanning in Figure 2, there are several PUPs detected, where the PUP can cause malware such as adware or spyware.

### 4.3. Testing Using ShowString

ShowString is a tool that functions to see the strings contained in a file. The string can describe how a file performs its job.

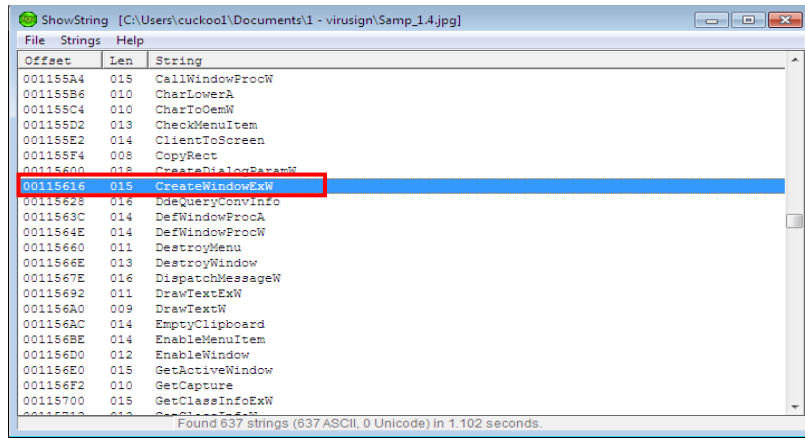


Figure 3. Malware String Detection Results

Figure 3 shows some functions contained in the two files. One function is CreateWindowExW which is where the file can create new windows that overlap each other like a pop-up window.

### 4.4. Results of Analysis with the Heuristic Detection Method

The analysis using the heuristic detection method is based on the test results detected on Malwarebytes. Here is a graph of the results of testing.

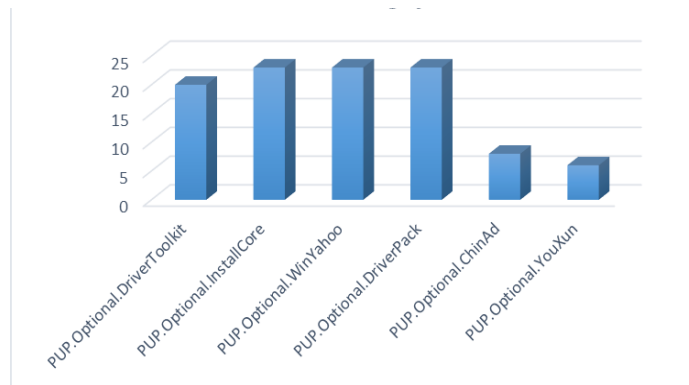


Figure 4. Graph of PUP Test Results

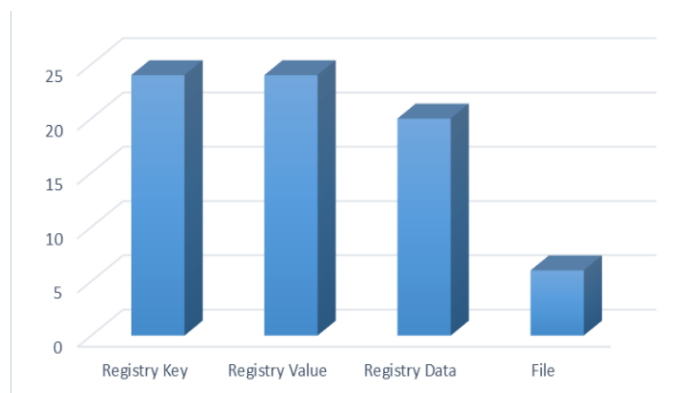


Figure 5. Object Type Testing Graph

Figure 4 shows that the most detected PUPs as threats to malware using the network API are:

1. PUP.Optional.InstallCore, this PUP is a bundler that will install adware. The impact that can be caused is by displaying pop-up advertisements that interfere with the user.
2. PUP.Optional.WinYahoo will make changes to the browser default page. This results in an extension that is automatically installed in the browser and can direct the browser to open a site that is not desired by the user.
3. Optional.DriverPack PUP is a PUP that will automatically install drivers on a computer system. This can trigger the entry of spyware.

Based on this data, malware that uses the network API has a pattern of behavior, such as making changes to the browser, installing unauthorized drivers, and displaying pop-ups of unwanted advertisements. Of the three behaviors, spyware activity is the most numerous activities, so malware that uses the network API has a tendency towards the entry of spyware. Whereas PUP that is not dominantly detected is:

1. PUP.Optional.DriverToolkit downloads the Driver Toolkit application automatically when a user accesses an insecure website. Users will be directed to do an installation that aims to improve the user's computer operating system.
2. PUP.Optional.ChinAd is an adware that displays marketplace sites originating from China. The impact of this malware is browser hijacking and can make users misclick while using browser.
3. Optional.YouXun PUP, PUP that downloads a file infected with malware that impacts the entry of malware on the user's computer device and affects the performance of the computer device.

PUP.Optional.DriverToolkit and PUP.Optional.YouXun have the same pattern of behavior, which is downloading a file. Both of these PUPs do the download automatically without the user's knowledge, but the installation is still done manually so that the user can still prevent the installation of malware programs on the computer. While PUP.Optional.ChinAd is a little PUP that is detected because adware which usually attacks computer devices is broad, that is, it can display advertisements in the form of pop-ups or new tabs on browsers that can come from anywhere. Adware that attacks computer devices can also be a gaming site that is not desired by the user.

Figure 5 shows that places or locations that are widely used as malware targets are:

1. Registry key and registry value, if the malware directly attacks the two registry, there will be a change in the operating system, because malware can change the configuration contained in the two registry, such as the computer cannot shutdown, cannot open files that have been hidden, and cannot access some of the applications contained in the user's computer.
2. Registry data, the impact caused when the registry data is infected with malware is almost the same as the impact of the registry key and registry value, because the registry data is the actual configuration file that is inside the registry value.
3. Files, when a file is infected by malware, then the file may not be opened or the file can be turned into another virus, lost or hidden by malware that infects it.

Based on the analysis results, PUP that has been detected as a whole can cause malware, but there are PUPs that require user action first to run the malware. PUP.Optional.DriverToolkit and PUP.Optional.YouXun are PUPs that require user action first. Both of these PUPs will only download files automatically without the user's knowledge, but installation requires user approval. Whereas the other four PUPs enter the operating system directly and infect the operating system with malware. The biggest impact of malware that uses the network API is the emergence of spyware.

#### 4.5. Recommended Analysis Results

Based on the results of the analysis in point 4, the following recommendations for each PUP are obtained.

**Table 1.** Recommended Analysis Results

No	Name	Recommendation
1	PUP.Optional.DriverPack	Action that can be done is to not easily believe the warnings that appear on the system and do not install applications that do not come from the official website.
2	PUP.Optional.WinYahoo	Precautions that can be taken are using antivirus or antimalware to protect the user's computer operating system and should not access unsafe websites.

3	PUP.Optional.InstallCore	Precautions to protect the system from adware are not to install unknown applications and not to install additional applications that are not needed when installing an application.
4	PUP.Optional.DriverToolkit	Precautions that should be taken are using antivirus or antimalware to protect the user's computer operating system.
5	PUP.Optional.ChinAd	The thing that can be done to prevent the entry of adware is not to carelessly install freeware software.
6	PUP.Optional.YouXun	Precautions that can be taken are by not accessing insecure websites, using antivirus and antimalware and not installing additional applications from the application to be installed.

## 5. CONCLUSION

Based on research on the Impact Analysis of Malware Based on API call Network with Heuristic Detection Method, it can be concluded that:

1. Testing malware can use several environments that function as sandboxes. In this study the Windows operating system is run on VMware which functions as a sandbox so that the main operating system is not infected. The Windows operating system is used as a target in the analysis using Cuckoo Sandbox.
2. The research results are based on test results from Malwarebytes that can detect programs that cause malware with the heuristic detection method and see the malware string on ShowString.
3. Malware with a network API will attack the operating system registry key and have a program that can cause spyware or adware that can interfere with user activity when using a computer device.
4. Recommendations for protecting computer systems such as using antivirus or antimalware, not installing unauthorized applications, not accessing insecure websites and not needing to install additional applications that are not needed when installing an application.

## REFERENCES

- [1] C. Donalds and K. Osei-Bryson, "Toward a cybercrime classification ontology: A knowledge-based approach", *Computers in Human Behavior*, vol. 92, pp. 403-418, 2018. Available: 10.1016/j.chb.2018.11.039.
- [2] Z. Bazrafshan, H. Hashemi, S. M. H. Fard, and A. Hamzeh, "A survey on heuristic malware detection techniques," *The 5th Conference on Information and Knowledge Technology*, 2013.
- [3] Teknik Penyebaran Malware | Jul Ismail, Jul Ismail, 2016. [Online]. Available: <https://julismail.staff.telkomuniversity.ac.id/teknik-penyebaran-malware/>. [Accessed: 23- Sep- 2018].
- [4] E. Gandotra, D. Bansal and S. Sofat, "Malware Analysis and Classification: A Survey", *Journal of Information Security*, vol. 05, no. 02, pp. 56-64, 2014. Available: 10.4236/jis.2014.52006.
- [5] D. Uppal, V. Mehra and V. Verma, "Basic survey on Malware Analysis, Tools and Techniques", *International Journal on Computational Science & Applications*, vol. 4, no. 1, pp. 103-112, 2014. Available: 10.5121/ijcsa.2014.4110.
- [6] D. Deka, N. Sarma and N. Panicker, "Malware detection vectors and analysis techniques: A brief survey", 2016 *International Conference on Accessibility to Digital World (ICADW)*, 2016. Available: 10.1109/icadw.2016.7942517 [Accessed 26 May 2019].
- [7] P. Shijo and A. Salim, "Integrated Static and Dynamic Analysis for Malware Detection", *Procedia Computer Science*, vol. 46, pp. 804-811, 2015. Available: 10.1016/j.procs.2015.02.149.
- [8] J. Raymond, "What is Malware and How Can We Prevent It?", *Comodo Antivirus Blogs | Anti-Virus Software Updates*, 2018. [Online]. Available: <https://antivirus.comodo.com/blog/how-to/what-is-malware/>. [Accessed: 09- Dec- 2018].
- [9] S. More and P. Gaikwad, "Trust-based Voting Method for Efficient Malware Detection", *Procedia Computer Science*, vol. 79, pp. 657-667, 2016. Available: 10.1016/j.procs.2016.03.084.
- [10] N. Zalavadiya and P. Sharman, "A Methodology of Malware Analysis, Tools and Technique for windows platform – RAT Analysis", *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no. 3, 2017.

- 
- [11] R. Sihwail, K. Omar and K. Zainol Ariffin, "A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis", *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 4-2, p. 1662, 2018. Available: 10.18517/ijaseit.8.4-2.6827.
- [12] Walkthrough: Calling Windows APIs (Visual Basic), Docs.microsoft.com, 2015. [Online]. Available: <https://docs.microsoft.com/en-us/dotnet/visual-basic/programming-guide/com-interop/walkthrough-calling-windows-apis>. [Accessed: 09- Dec- 2018].
- [13] Windows API Index - Windows applications, Docs.microsoft.com, 2018. [Online]. Available: <https://docs.microsoft.com/en-us/windows/desktop/apiindex/windows-api-list>. [Accessed: 09- Dec- 2018].
- [14] Ki, Y., Kim, E. and Kim, H., 2015. A Novel Approach to Detect Malware Based on API Call Sequence Analysis. *International Journal of Distributed Sensor Networks*, 11(6), p.659101.
- [15] PUP.Optional.DriverPack - Malwarebytes Labs, Malwarebytes Labs, 2019. [Online]. Available: <https://blog.malwarebytes.com/detections/pup-optional-driverpack/>. [Accessed: 26- Apr- 2019].
- [16] PUP.Optional.DriverToolkit - Malwarebytes Labs, Malwarebytes Labs, 2019. [Online]. Available: <https://blog.malwarebytes.com/detections/pup-optional-drivertoolkit/>. [Accessed: 26- Apr- 2019].
- [17] PUP.Optional.InstallCore - Malwarebytes Labs, Malwarebytes Labs. [Online]. Available: <https://blog.malwarebytes.com/detections/pup-optional-installcore/>. [Accessed: 26- Apr- 2019].
- [18] PUP.Optional.WinYahoo - Malwarebytes Labs, Malwarebytes Labs. [Online]. Available: <https://blog.malwarebytes.com/detections/pup-optional-winyahoo>. [Accessed: 26- Apr- 2019].
- [19] What is spyware? - Definition from WhatIs.com, SearchSecurity, 2019. [Online]. Available: <https://searchsecurity.techtarget.com/definition/spyware>. [Accessed: 28- Apr- 2019].
- [20] Malwarebytes for Windows - Antivirus Replacement for PCs, Malwarebytes. [Online]. Available: <https://www.malwarebytes.com/premium/>. [Accessed: 29- Apr- 2019].
- [21] What are Registry Keys? - Remove Spyware & Malware with SpyHunter - EnigmaSoft Ltd, Remove Spyware & Malware with SpyHunter - EnigmaSoft Ltd. [Online]. Available: <https://www.enigmaoftware.com/what-are-windows-registry-keys/>. [Accessed: 29- Apr- 2019].
- [22] T. Adi Cahyanto, V. Wahanggara and D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis", *Justindo*, vol. 2, no. 1, 2017. [Accessed 26 May 2019].
- [23] A. F. Muhtadi and A. Almaarif, "Analysis of Malware Impact on Network Traffic using Behavior-based Detection Technique", *International Journal of Advances in Data and Information Systems*, vol. 1, no. 1, pp. 17-25, Mar. 2020.
- [24] M. K. Shankarapani, S. Ramamoorthy, R. S. Movva, and S. Mukkamala, "Malware detection using assembly and API call sequences," *Journal in Computer Virology*, vol. 7, no. 2, pp. 107–119, Mar. 2010.