KnE Social Sciences

FGIC2019
FGIC 2nd Conference on Governance and Integrity 2019
Volume 2019

Knowledge E
enriching | engaging | empowering

Conference Paper

Malware Mobile Devices in Indonesia

Drajad Wiryawan[1], Joni Suhartono[1], Surjandy[1], Yudi Fernando[2], Idris Gautama So[3], and Anderes Gui[1]

[1]Information Systems Department, School of Information Systems, Bina Nusantara University, Jakarta, 11480, Indonesia
[2]Faculty of Industrial Management, Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300 Gambang, Pahang, Malaysia
[3]Management Department, Binus Business School, Undergrdaute Program, Bina Nusantara University, Indonesia, Jakarta, 11480, Indonesia

Abstract

The number of mobile devices and information technology supporting applications is currently very diverse. Ranging from expensive to cheap, even new and used. On the other hand, the increase in connections needed every year always increases along with its development. Both of these are always accompanied by increasing crime in cyberspace so that the level of risk and threats that arise will also always spread threats from time to time. Many people do not understand what cyber risk is, its impact and how minimal handling is needed to overcome the above. This research was conducted to provide an overview of cybersecurity information to anyone about the amount of malware on existing and scattered devices and the user behavior itself. It starts with scanning network traffic, type of malware, then the patterns and its characteristics. On the other hand, this also provides input on how to make minimal handling as a way to control cybersecurity. The aim of the work is to focus on establishing the basic behavior of a user on mobile malware for user profiling analysis.

Keywords: malware, cybersecurity, user behavior, control.

Corresponding Author:
Anderes Gui
anderesgui@binus.edu.my

Received: 5 August 2019
Accepted: 14 August 2019
Published: 18 August 2019

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FGIC2019 Conference Committee.

1. Introduction

The role of information technology in the digital age is something that cannot be rejected or considered one by the eyes of anyone. Information technology explains some of the main concerns in it, ranging from data collection, processing it to become a piece of information than how to use the infrastructure owned such as computer resources, software, data and network by the use (Fox, 2013). With the existing information technology, these users can receive or provide information quickly and accurately to anyone directly or indirectly whether in secret or not. Starting from students, office workers to entrepreneurs and even children up to old age, all always take advantage of various information technology it has to support its daily activities. Until now, many sites on the

internet, official or unofficial, paid and unpaid, which provide services and support for various updates and maintenance of information technology, both systems, applications, and network information technology. According to IDC survey data in Jan 2017 – Dec 2018, the number of operating systems used was Android (86.78%). It is the most widely mobile operating system used than others, like iOS (3.72%), Nokia (1.628%), Blackberry (091%), Symbian (0.37%), and Windows Phone (0.26%). (GStatcounter, 2018). A world map with circles corresponding in size to the total number of reports received from specific countries (Kaspersky Cybersecurity Map, 2019).

Table 1: Malware Package Detected on Mobile Apps.

Period	Risk Tool	Trojan Dropper	Adware	Trojan	Trojan SMS	Trojan Banker	Trojan Ransom	Backdoor	Hacktool
(Q1) 2019	29.80 %	24.93 %	16.57 %	9.61 %	7 %	3.24 %	3.09 %	1.68 %	0.33 %
(Q4) 2018	48.59 %	11.04 %	8.32 %	16.6 %	5.74 %	1.85 %	2.4 %	1.89 %	0.31 %

Based on Table 1 above, there are 905,174 application packages detected by malware in the first quarter of 2019, which are mostly in the form of trojans and risk tools. A large number of mobile device usage followed by the availability of various applications and support through the links provided on each device. Starting from the Play Store by Google (2.8M), Apps store by Apple (2.2M) and Windows Phone by Microsoft (670K), as well as developers such as Apple Corp., Samsung Corp., Xiaomi and many other devices, always provide the need through online and offline connections.

2. Literature Review

2.1. An overview of the literature review

In order to understand what cybercrime, cybersecurity, and malware, it is necessary for us to understand them first. Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets whereas (Kshetri, 2013). Cybercrime is defined as a criminal activity in which the computer or computer is the principal means of committing an offense or violating laws, rules or regulations (Kshetri, 2013). In another side, Malware is a general term for all the malicious code that is a program designed to harm or secretly access a computer system without the owners' informed consent, such as computer virus, backdoor, Trojan, and worm. (Tan, 2016). Mobile device

features are continually changing, so it is difficult to define the term “mobile device”. Mobile devices are also known as handheld computers. A mobile device is a handheld tablet or other device that is made for portability and is therefore both compact and lightweight. New data storage, processing, and display technologies have allowed these small devices to do nearly anything that had previously been traditionally done with larger personal computers (Souppaya and Scarfone, 2013). The following hardware and software characteristics collectively define the baseline for this publication: (1) At least one wireless network interface for network access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the Internet or other data networks. (2) Local built-in (non-removable) data storage (3) An operating system that is not a full-fledged desktop or laptop operating system (4) Applications available through multiple methods (provided with the mobile device, accessed through the web browser, acquired and installed from third parties).

2.2. Historical review

Cybersecurity in the digital age is very important and an integral part of information technology. Proper learning of online behavior and system protection will reduce the vulnerability of safer online environments. Rapid technology expansion also creates and makes cybersecurity more challenging, so it is necessary, a framework or technology useful for protecting networks and information not only for the short-term but also long-term. A better understanding of security and the right strategy can help to protect assets and reduce both financial and reputation losses (Wiryawan and Noerlina, 2016). Related to various things above, until now, there are so many risks that arise in cyber activities that are caused, including malware. According to Monnappa K A., the various motives of malware such as (1) Disrupting computer operations (2) Stealing sensitive information, including personal, business, and financial data (3) Unauthorized access to the victim’s system (4) Spying on the victims (5) Sending spam emails (6) Engaging in distributed-denial-of-service attacks (DDOS) (7) Locking up files on computers and holding them for ransoms (Monnappa, 2018)

2.3. Malware Characteristic

Based on Prayudi and Yusirwan (2015), some of the malware that has so far been found in Indonesia through previous research is: (a). The Trojan / Backdoor is a malicious

program that can install itself on a victim's computer to open a gate for hackers to enter it. Backdoor usually make a hacker able to connect to the victim's computer without certain permissions and immediately execute commands on the target computer. (b). The Botnet is a malware that has the ability like a backdoor, but when the computer has been infected (botnet), the infected computer will obey the command as if the instruction was given by the server control. (c). Downloader is a program that is usually installed by hackers when they already have access to the victim's computer system. This type of malware will download and install other malware to the system that is victimized. (d). Information-stealing malware is malware that collects information from the victim's computer, then send information that has been obtained to certain people. Examples of this type of malware are sniffers, password hash grabbers, and keyloggers. (e). Rootkits are programs that are made to hide other malware so that it cannot be detected by Anti-Virus. (f). Scareware is malware that aims to scare the victim with a specific message, where the victim is asked to buy a certain program to remove the malware (g). Viruses are malicious programs designed for destroying a computer system, like causing interference with the operating system, excessive memory usage on a computer, or data destruction.

3. Methodology

Based on Feys and Saeger (20150, the method of the approach taken in this study is a qualitative approach with the fishbone graph (Figure 1), where the main instrument research is data in the form of observation of the results article research both in the form of library books, and interviews with users of information technology devices. Source of research data are students, lecturers, and the general public. To collect data above, then the researcher conducts several stages, namely: (a) determining the literacy that is the subject of writing, (b) observing during the process of making the article takes place, (c) collecting various articles from previous studies, (d) conducting interviews with the writing object. Whereas in analyzing the authors conduct evaluations and reductions on data that are relevant to the research objectives. Then, the researcher presents the data in narrative form for later verification based on the predetermined study theories and conclude them.

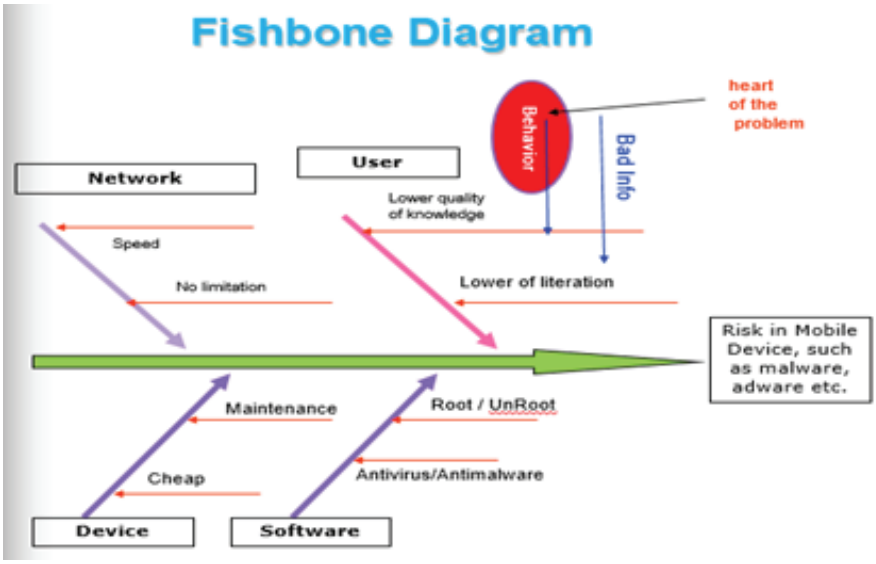

Figure 1: Fishbone Diagram.

4. Results

Based on survey results by analysis in 2018, internet usage rate in Indonesia is 75.5% dominated by 13-17-year-old age, 74.23% by 18-33 year, 44.06% by 34-54 years, and 15.72% for more than 54 years old. In another side, the education level of internet using were 88.24% for S2 / S3, 79.23% for S1/Diploma, 70.54% for the High School, 48.53% for Middle School, 25.10% for Elementary School, and only 5.43% unstudied. In relation to the survey of the device, most of 50.08% users have mobile devices such as smartphones or mobile phones, and only 44.16% of the devices are used to access various information over the internet. Compare with immobile ownership such as computer or laptop which is only 25.72%, of which only 4.49% is used for internet access. Based on the two images, it can be deduced that users prefer mobile devices compared to immobile devices, such as a PC or laptop. Indonesia has experienced tremendous growth in information technology. Shown with increased year-on-year internet access shows that the total number of internet users was up to 143.26 million, and its trend will be a rise in 2019. Although the majority is still dominated by Java (58.8%) and located only in big city cities (72.41%), but with the ongoing development time and infrastructure it does not rule out the potential of other regions will also increase significantly.

Related to the picture above, some things that become the most important part in it are about how people use the device they have, such as access to the site or installation of prohibited applications or not. It was shown that the usage points (operational) accounted for 60% of the spread of malware every day. Then on the point of maintenance, both on the side of the update/patch, the installation of antivirus or VPN

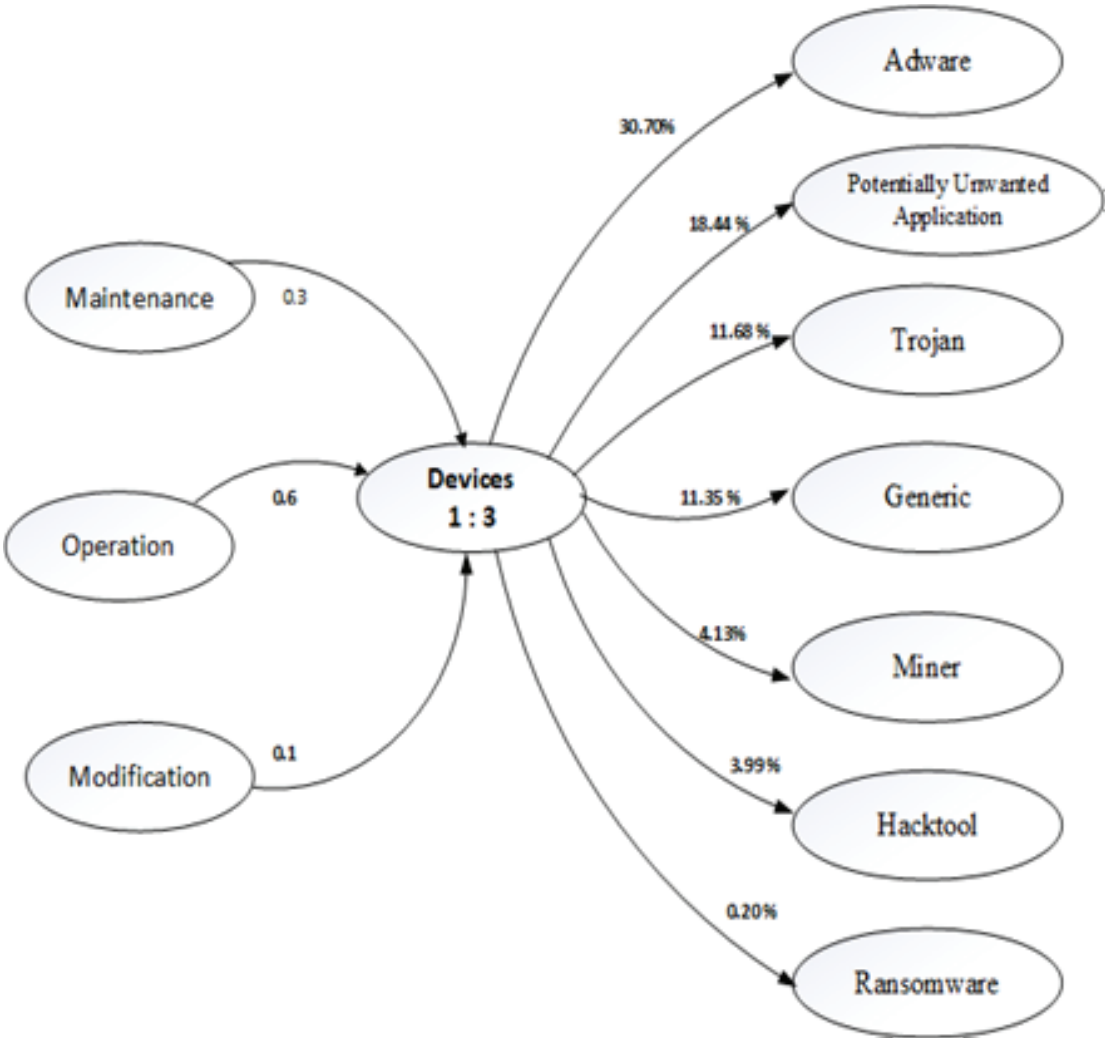

Figure 2: Malware Relation.

accounts for 30% in the spread of existing malware. Whereas on the side of changes in the operating system or internal devices, it only accounts for 10%. Although only small, but modifications to the technology devices used, also a factor in the spread of the intended malware.

Related to Figure 2 and Table 2 above, it can be explained (Table 3) that the results of the analysis carried out on user behavior for maintenance, operation, and modification in the device are as shown in (1) On the Maintenance side, only a few users pay attention to devices that are used daily. This is indicated by a value of 37, 9%. (2) On the Operations side, there are quite a number of users who can use or operate their information technology devices, indicated by a value of 86.2%. (3). On the side of Modification, only a few understand how to make changes to the technological devices used. This is indicated by the value of 8.3%.

Table 2: Malware Analysis.

No	Name and Type		Percent (%)
1	Malware		44
	a	Backdoor	
	b	Generic	
	c	Heuristic	
	d	Mogoogwi	
	e	Worm	
	f	Ramnit	
	g	WannaCry	
	h	Others	
2	Adware		38
	a	Install Core	
	b	PUA	
	c	Generic	
	d	Others	
3	Trojan		18
	a	Dropper	
	b	Hacktool	
	c	Generic	
	d	Others	

Table 3: Behavior of User.

No	Behavior		Score (%)
1	Maintenance		
	a	Content Revision	15
	b	Update / Patching	17.2
	c	Cleaning	5.7
2	Operation		
	a	Content Control	40.8
	b	New Apps. Installation	25
	c	Capabilities	20.4
3	Modification		
	a	Unnecessary Apps.	2.3
	b	User Privilege	3
	c	Others	3

5. Discussion

The programs like malware, are created by people with a degree of technical skill, they are network security professionals or only amateurs. Tools such as port and vulnerability scanners that are ostensibly designed to be used by 'white-hat' or ethical

individuals and professionals may also be open to abuse by 'black-hat' attackers. The term 'script kiddies' also exists to describe amateur self-termed 'hackers' who lack the technical skills of their own to develop exploits and perform attacks but instead use tools developed by others, often with little understanding of how they work. Script kiddies such as these, therefore, are likely to make use of programs that are covered by the Hacktool detection. Based on various things related to the causes and impacts, malware is one of the activities that cause various losses that exist, especially not only in the user but in the other arrangements that exist in information technology systems, such as maintenance. Regarding current users, pay more attention to existing device users. Very few users pay attention to the maintenance of all the devices they have. Good for content revisions, updates are available for each application installed. This is very important. However, many do not want to know. Without maintenance, then all devices used will experience various things that are inappropriate in the future. Starting from losing data and information to financial losses in online transactions (such as mobile banking transactions, etc.)

6. Conclusion and Implications

If you think you have malware on your phone, the most important thing to maintain (more than 60 % did not maintain) is to stop the malware from causing any further damage. Do not wait until your device gets infected. Make protecting your device a priority. Having good anti-malware software that protects your PCs, tablets, and other mobile devices may help prevent malware from spreading from device to device. Some steps that need to be used as a reference in the first minimal handling malware that has been found in research are (1) Turn off the phone and restart in safe mode. (2) Uninstall the suspicious app. (3) Look for other apps you think may be infected. (4) Install a robust mobile security app on your phone. Based on research with static and dynamic analysis and increasing prevalence above, it has often been done. It is hoped that in the next study, this research will be able to help in the next step regarding the kind of maintenance for the user. Especially in how the user cannot maintain their devices? so that the technology used will not be something daunting the users. In other words, it is expected that the user will concern with malware being a something which very critical.

References

[1] Fox, R. (2013). Information Technology: An Introduction for Todays Digital World. *First Edition, CRC Press, FL, USA*, 1.

[2] K, S. M. (2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise. *NIST, US Department of Commerce*.

[3] Kshetri, N. (2013). Cybercrime and Cybersecurity in the Global South. *First Edition, Palgrave Macmillan, NY USA*, 6.

[4] Monnappa, K. (2018). Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware. *First Edition, Packt Publishing, Birmingham, UK*, 6.

[5] S, P. Y. (2015). The Recognize of malware characteristics through static and dynamic analysis approach as an effort to prevent cybercrime activities. *Journal of Theoritical and Applied Information Technology*, Vol. 77, No. 3, p. 438-445.

[6] Saeger, F. B. (2015). The Ishikawa Diagram for Risk Management: Anticipate and Solve the Problem for Future Business. *Lemaire Publishing, Namur, Belgium*, 8.

[7] Tan, Y. (2016). Artificial Immune System: Applications in Computer Security. *First Editiionn, John Wiley & Son Inc, NJ, USA*, 150.

[8] Wiryawan, D. a. (2016). Implementation of the acunetix for testing the banking website (owned by the government and non-government in Indonesia. *An International Interdisciplinary Journal, Vol. 19 Number 6(A)*, 1785-1792.