Journal of Network and Computer Applications 75 (2016) 58–76

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

The rise of “malware”: Bibliometric analysis of malware study

Mohd Faizal Ab Razak [a,b,*], Nor Badrul Anuar [a,*], Rosli Salleh [a], Ahmad Firdaus [a,b]

[a] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia
[b] Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, Lebuhraya Tun Razak, 26300 Gambang, Kuantan, Pahang, Malaysia

ARTICLE INFO

Article history:
Received 10 June 2016
Received in revised form
3 August 2016
Accepted 24 August 2016
Available online 26 August 2016

Keywords:
Malware
Bibliometric analysis
Malware analysis
Intrusion detection system
Mobile malware

ABSTRACT

Malicious software (malware) is a computer program designed to create harmful and undesirable effects. It considered as one of the many dangerous threats for Internet users. Rootkit, botnet, worm, spyware and Trojan horse are the most common types of malware. Most malware studies aim to investigate novel approaches of preventing, detecting and responding to malware threats. However, despite the many articles published to support the research activities, there is still no trace of any bibliometric report that demonstrates the research trends. This paper aims to fill in that gap by presenting a comprehensive evaluation of malware research practices. It begins by looking at a pool of over 4000 articles that are published between 2005 and 2015 in the ISI Web of Science database. Using bibliometric analysis, this paper discusses the research activities done in both North America, Asia and other continents. This paper performed a detailed analysis by looking at the number of articles published, citations, research area, keywords, institutions, terms, and authors. A summary of the research activities continues by listing the terms into a classification of malware detection system which underlines the important area of malware research. From the analysis, it was concluded that there are several significant impacts of research activities in Asia, in comparison to other continents. In particular, this paper discusses the number of papers published by Asian countries such as China, Korea, India, Singapore and Malaysia in relation to the Middle East and North America.

Contents

* Corresponding authors at: Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia.

E-mail addresses: faizalabrazak@siswa.um.edu.my (M.F.A. Razak), badrul@um.edu.my (N.B. Anuar), rosli_salleh@um.edu.my (R. Salleh), ahmadfirdaus@um.edu.my (A. Firdaus).

http://dx.doi.org/10.1016/j.jnca.2016.08.022
1084-8045/© 2016 Elsevier Ltd. All rights reserved.

1. Introduction

Malware is a malicious software which threatens Internet users. Rootkit, botnet, worm, spyware and Trojan horse are the most common types of malware that capable of causing harm to the network and operating systems (Feizollah et al., 2015; Rieck et al., 2008). Unscrupulous authors design malware with specific goals and functions. When activated, malware spreads through the Internet and causes defects to operating systems. Malware uses vulnerabilities in computer applications and operating systems to exploit data through malicious code. It also uses social engineering to attract users into running the malicious code with useful tools and applications. The aforementioned activities cause computer, mobile device, network performance, and stability problems. To combat this problem, security researchers have designed anti-malware and antivirus applications which are used to detect malware. This is done by monitoring the computer activities via specific algorithms and pre-defined signatures or patterns. There are many types of malware that are currently available on the Internet. Verizon reported that around 170 million of malware events occur across organizations, with the frequency of five malware occurring every one (1) second (Verizon, 2015). PandaLabs was said to have managed to neutralize 75 million new malware in 2014, double the record in 2013 (Lopez, 2015) while Symantec identified more than 317 million new pieces of malware that are created in 2014, a figure suggesting that nearly one (1) million new threats are released every day (Symantec, 2015).

Although there are existing approaches such as firewall, antiviruses and Intrusion Detection Systems (IDSs) to overcome malware attacks, the noticeable spikes of the aforementioned malware statistic still require novel approaches to detect malware. With the availability of new technologies, malware authors are able to use novel approaches to hide detection. This has led to the many studies which are conducted to explore the malware domain. The study of malware is a domain of investigating and analyzing malware characteristics in order to propose a new approach to aid prevention, detection and response to malware. For example, studies such as (Tang et al., 2014) and (Sahs and Khan, 2012) applied machine learning approaches to detect malware but another (Nadeem and Howarth, 2014) applied adaptive response as an approach to halt attacks, mitigate damages and prevent attacks in a mobile ad hoc network (MANET). The aforementioned examples demonstrate that the research activities conducted in this domain are significant. Nonetheless, despite so many articles being published to support the research activities, there is still no trace of any bibliometric article that reports on the research impacts and trends of such investigations.

Bibliometric is the statistical analysis which analyzes bibliometric characteristics and data such as citations, publications, and research outputs. It allows researchers to understand the structure, characteristics, and patterns of research activities. The analysis process synthesizes the research activities into a realistic trend of a research domain as it involves literature studies of scientific activities in different contexts such as publications, authors, institutions, citations, and countries. It is a method that reports on the comprehensive evaluation of the expansion of research fields (Dehdarirad et al., 2015; Wu et al., 2015). Such a method, for example, was used by (Olijnyk, 2015) and (Zainab and Anuar, 2009) to measure the intellectual profile and evolution in computer science and information security. There are many benefits of bibliography studies. They are (a) authors are able to demonstrate the significance of their research and publication, (b) institutions are able to evaluate the publication performance and measure the impact quality, (c) researchers are able to predict future research and significant impact on any particular domains, and (d) researchers are able to evaluate the growing body of knowledge.

In order to demonstrate the growth of the malware domain, this paper aims to conduct an investigation of the domain by presenting a comprehensive evaluation of malware research practices published in the Web of Science from 2005 to 2015. The approach involves the appraisal of malware research, publication patterns, research topics, and assessment on malware. In order to address this study, we formulated the following research questions: (a) what is the trend of publications in malware study in the Asian context; and (b) how does this trend help to identify the future direction of malware study?

Using "malware" as the main keyword, we identified over 4000 articles and scrutinized before being classified into 2158 main related articles. All these are taken mainly from the Web of Science Core Collection. The exclusion was done on some journal databases such as KCI-Korean Journal Database, Derwent Innovations Index, and SciELO Citation Index. This is done for the following reasons: (a) to remove non-English articles (e.g. Korean and Portugal Language) and (b) to remove patents. With the selected 2158 articles, we performed an analysis by creating the relationship between the abstract, title, publication, citation, research area, geographical location and the keywords use. In addition, this paper also discusses the classification of malware detection system by focusing on the frequency of words used in the abstract and title. Finally, this paper discusses the trends by summarizing the substantial research efforts and highlighting possible future tracks for malware research. To justify the warrant of this paper, we performed an analysis by separating the research activities into seven (7) main continents including Asia, North America, South America, Europe, Middle East, Australia, and Africa. Table 1 tabulates the distribution of research publication where North America leads with 34.07% followed by Asia with 30.6%.

Table 1
Distribution of malware research based on 7 continents.

Geographical areas	Publications (%)
North America	34.7
Asia	30.6
Europe	26.5
Middle East	3.7
Australia	3.3
South America	1.0
Africa	1.0

The rest of this paper is organized as follows. Section 2 describes the research method. Section 3 presents findings and information of malware studies. Section 4 provides a classification of the malware detection system. Section 5 describes the challenges and future trend of malware study. Section 6 is the conclusion to the study.

2. Methodology

Bibliometrics is a method to evaluate, monitor and visualize the structure of scientific fields (Koskinen et al., 2008; McKerlich et al., 2013a). It describes the publication information and determine the impact of the effectiveness of researcher and organization such as universities. According to (Wilson, 2016), bibliometrics is the oldest research methods in library and information science. This paper applied bibliometrics method by referring to this study (Koskinen et al., 2008). The researcher described how to use bibliometric methods in research evaluation. The researcher divided bibliometric methods in two part: general instructions and publication analysis. For general instructions, researcher brief about how to search article using search engine to avoid possible sources of error in search process. While publication analysis describes about the evaluation of publication such as impact factor, citations, publisher and country. This method applied in several studies as well. For examples, (Wu et al., 2015) analysis of published landslide studies for the period 1991–2014 to explore landslide research trends, (Dehdarirad et al., 2015) study the expansion and growth of scientific literature on women in science and higher education, (Loomes and van Zanten, 2013) study top 100 clinical articles in digestive disease, (Mao et al., 2015) analysis the trends of the literature of biomass energy and (Fahimnia et al., 2015) analysis green supply chain by using 1000 publications.

In this paper, several strategies were used to retrieve publications and it begins by using “malware” as the main keyword. The keyword is very important because it offer the information of research trend and discover research direction and interest (Sun et al., 2012). We applied Computer automatic and manual search method to analyze the retrieved articles. Fig. 1 illustrates the flowchart of the data collection process. By using “malware” as a main keyword, a search for related publications indexed in the Web of Science Core Collection helps to limit the study to the past 10 years i.e. between 2005 and 2015. Consequently, we detected a total of 4546 publications from various journals, books, book sections and patterns. To remove unrelated publications such as patterns and non-English publications an exclusion was made on databases like KCI-Korean Journal Database, Derwent Innovations Index, and SciELO Citation Index. Due to this exclusion, 2158 articles were secured for analysis purpose. The analysis was conducted based on the following criteria, (a) impact journals, (b) highly cited articles, (c) research areas, (d) productivity, (e) keyword frequency, (f) institutions and (g) authors. Finally, to visualize the results, we adopted the VOSviewer tool as it is free and contains excellent features that support various types of bibliographic visuals for analysis. Fig. 1 is provided for illustration.

2.1. Web of science

There are many databases used to index journal articles such as Web of Science (Wos), Elsevier's Scopus, Google Scholar, IEEE

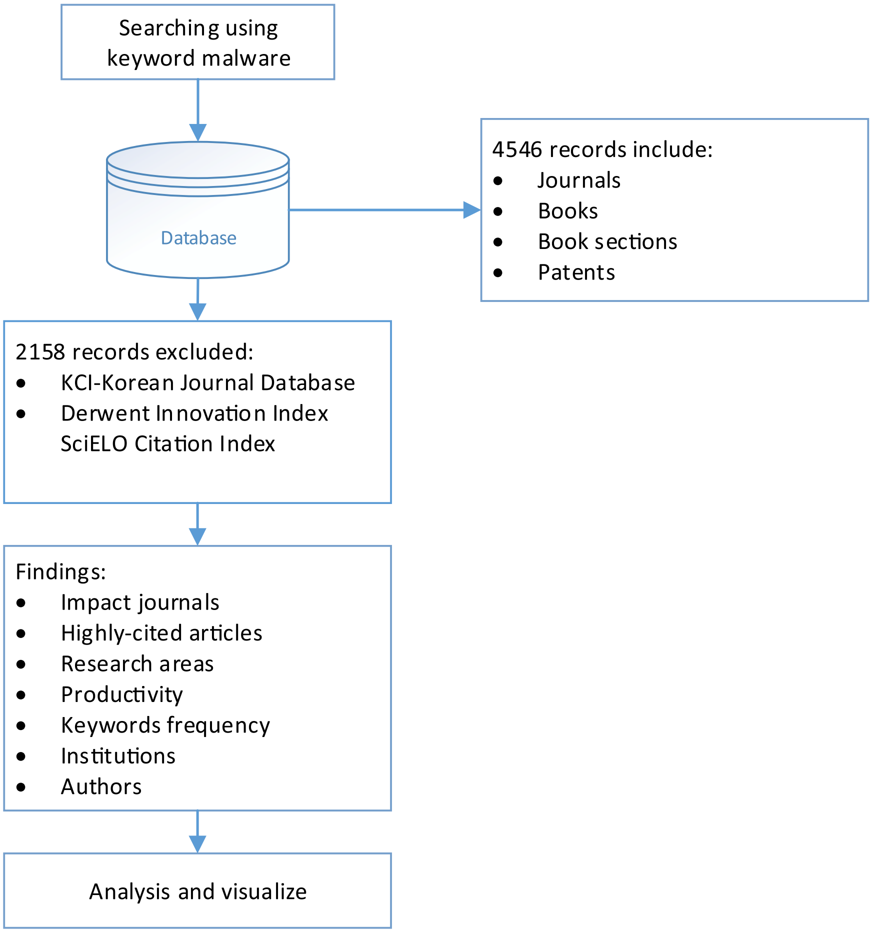


Fig. 1. The schematic of data collection process.

Explore, ScienceDirect, Association for Computing Machinery (ACM) and Springer. However, WoS, Elsevier's Scopus and Google Scholar are the three (3) main bibliometrics data source for searching literature (Abrizah et al., 2013; Mingers and Leydesdorff, 2015; Mongeon and Paul-Hus, 2016). These data sources are commonly used to rank journals in terms of their productivity and the total citations received to indicate the journals impact, prestige or influence (Abrizah et al., 2013; Chadegani et al., 2013). In this paper, we select WoS database based upon the following reasons. Firstly, it is an only tool for bibliometrics analysis until the creation of Scopus and Google Scholar in 2004 (Mongeon and Paul-Hus, 2016; McKerlich et al., 2013a) and secondly, 94% of Scopus highest impact factor journals were indexed in WoS (Lopez-Illescas et al., 2008). In addition, we exclude Scopus and Google Scholar in order to avoid overlap between the databases. We exclude Google Scholar as it has low data quality that raises questions about its suitability for research evaluation (Mongeon and Paul-Hus, 2016). Furthermore, IEEE Explore, ScienceDirect, ACM and Springer limit themselves by indexing their own publishers, and WoS combines the selected and high impact publication from the aforementioned databases.

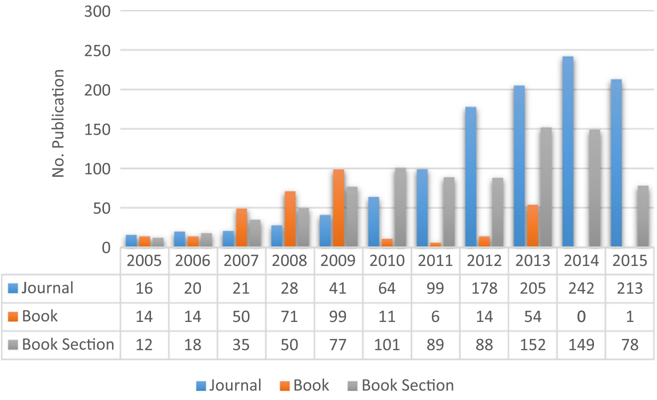
Besides that, we choose WoS database because it famous in the bibliometric analysis for visualizing the evaluation of literature in scientific fields (McKerlich et al., 2013b). It has a literature for all years since 1900 while literature from Scopus retrieves until 1996 (Mingers and Leydesdorff, 2015). WoS database claims it has the most depth and the most quality than Scopus and Google Scholar (Chadegani et al., 2013). The important of WoS database is that it includes all articles types and index institutions, authors, and bibliographic references for each article (Mongeon and Paul-Hus, 2016).

The WoS database acted as the search engine for this paper. It is a product derived from "Thomson Reuters Institute of Scientific Information" (ISI) and it contains over 12,000 titles of journals from multidisciplinary areas (Dehdarirad et al., 2015). The database provides powerful searching and browsing options by enabling different options to filter and narrow the search results (Fahimnia et al., 2015). In addition to the searching options, the WoS database is also able to sort the articles based on certain parameters such as publication dates, recently added publications, number of times cited, usage counts, relevance, and based on first author names. Moreover, refining the results in the ISI Web of Science database also enabled certain results to be excluded by document types, authors, years, institutions and countries. Added to that is its ability to provide necessary information such as citation counts, impact factors, and quartile ranks. This made the study more conducive.

3. Findings

This section discusses the finding of the topic that is related to malware. This section is divided into 7 sub-topics: productivity, research areas, institutions, authors, impact journals, highly-cited articles and keyword frequency. These findings are important because they show the publishing rates with bibliometric data. In addition, it is also able to unravel high-quality research that helps to generate new knowledge and to ensure that the pursuit into malware studies is more in-depth. Fig. 2 is provided to show the number of publications in 2005–2015.

Fig. 2 shows the various publications extracted from various studies and are related to malware. It shows three categories of publications including journals, books, and book sections. The journal category has the highest proportion of publications with a total of 48.78% publications. This proportion is followed by the book sections that comprise 36.75% publications while books carry the lowest percentage of 14.45% of publications.



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
■ Journal	16	20	21	28	41	64	99	178	205	242	213
■ Book	14	14	50	71	99	11	6	14	54	0	1
■ Book Section	12	18	35	50	77	101	89	88	152	149	78

Fig. 2. Number of publications.

Looking at Fig. 2, in 2015, publication of journals, books, and book sections have declined slightly. This is possibly because the time taken by journals in accepting articles for publications is too long, thereby, affecting the number of publications in the said year. Following this, it is likely that journal publications would be on the increasing trend in the following year of 2016. Furthermore, the increment of journal publications able to increase the citations.

As mentioned earlier, citation analysis is used to assess the frequency of the journals based on data extracted from the citation index. This used to evaluate researchers' performance based on citation patterns, especially for academics. It also provides the information about researchers to other researchers using shared references whilst also providing a holistic view of the topic researched. It has been realizing that there are three types of publications in the academic research study. These publications focusing on originality and developers of the contents to show the significant of research. Fig. 3 illustrates the citation distributions.

Fig. 3 illustrates the citations received by the publications over the last 10 years. It shows that the number of publications influences the number of citations. The number of citations obtained by a published article increases after the published articles stays in the database for a longer period of time. In other words, the earlier it is published the more it is cited.

The average number of citations collected by published articles is about 341 annually during the period of 2005–2015. In addition, the number of annual citations shows a positive proliferation pattern with three distinct peaks occurring in 2013, 2014, and 2015. The citations had increased by 52.35% in 2013 as compared to 2012. This is possibly because in 2013, there was a surge in researchers conducting studies to solve a wave of malware attacks. Researchers citing other researchers' works as references had also resulted in an increase in the citation. This trend illustrates a

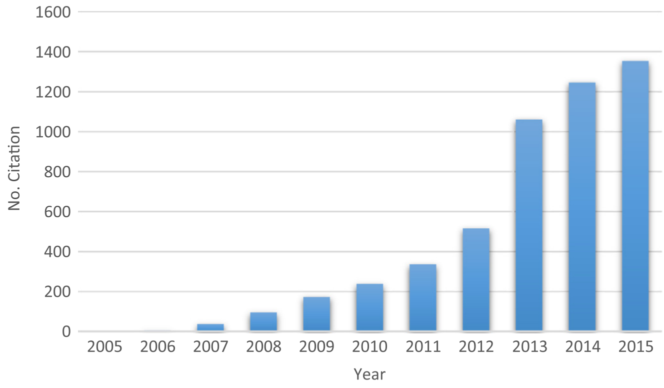


Fig. 3. Citation distributions.

positive result until 2015. From this pattern, it concluded that the number of citations for 10 years include co-citation. The citation is a way to show the evidence of material in the articles. This study examines the citation to illustrate the increasing number of citations and the research activities that contributed to the high impact of articles.

3.1. *Productivity*

This section discusses productivity among the continents. Productivity in publications refers to the frequency or number of publications incurred. It is used as a tool to measure the number of articles that were published among continents. A study of productivity growth of articles is important because it allows the researcher to stay focused and competitive on the publication of articles as well as strengthen the research components while conducting research involving analysis on malware. An important role for putting focus in the analysis of productivity is that it helps to increase and improve the productivity efficiency of the publications. In addition, it is also able to contribute to the research community in terms of new technology and in the identification of new or best methods in research. It also assists in the assessing of countries and continents which have produced much publications. Table 2 lists the number of publications with respect to the time trend analysis during 2005–2015 according to continents.

Table 2 above show that the continent of North America is the major contribution in publishing articles with the United States being most outstanding. This is followed by the continents of Asia, Europe and subsequently, the continents of the Middle East, Australia, Africa and South America which comparatively, conducted lesser research on malware. Data show that the United States contributed to 31.5% of the entire publication of articles in the continent of North America. In contrast, in the continent of Asia, China served as the country with the major contribution to research related to malware. This is followed by India, South Korea, Japan and Taiwan.

Based on the above, the continents of Asia and North America are the most productive in publishing articles. Asia seems to be slightly behind the continent of North America and this is probably due to the lesser amount of research funding provided by the respective countries in conducting research in similar research areas. In any research, the funding aspect is important because it enables researchers to perform new studies and to be able to publish research articles. As an example, it is observed that the American government spent the amount of $140 billion on research and development (Jahkne, 2016) while the government of China only provides funds amounting to $ 6.6 billion for basic research (Qiu, 2016). This difference suggests that adequate research funding is able to assist in the production of articles in a country thus, indirectly raising the number of articles identified in that continent. It is expected that there is intense competition between the two continents of Asia and North America in publishing articles in the next few years. Ability in good writing and able to publish high impact research related to malware allows North America become the top in the continent in publishing articles.

3.2. *Research areas*

This section discusses a number of publications involving certain research areas. Research areas consist of single disciplined and multidisciplinary as they aim at developing a scientific understanding of specific research areas and how these challenge other areas in different sectors of other industries. Research areas are very important element others use to measure the performance of a research based on publication and citation rates. The

Table 2
Productivity.

List of continents	No. of articles	No. of articles (%)
Asia	**670**	**30.6**
Bangladesh	1	0.0
China	268	12.4
India	98	4.5
Japan	78	3.6
Malaysia	33	1.5
Singapore	23	1.0
South Korea	92	4.2
Taiwan	63	2.9
Thailand	10	0.4
Uzbekistan	1	0.0
Vietnam	3	0.1
North America	**752**	**34.7**
Canada	62	2.8
Mexico	5	0.2
Russia	6	0.2
United States	679	31.5
South America	**24**	**1.0**
Argentina	3	0.1
Brazil	20	0.9
Colombia	1	0.0
Europe	**612**	**26.5**
Austria	31	1.4
Bulgaria	1	0.0
Belgium	4	0.1
Cyprus	1	0.0
Czech Republic	14	0.6
Denmark	2	0.0
England	69	3.1
Estonia	1	0.0
France	59	2.7
Finland	14	0.6
Germany	102	4.7
Greece	33	1.5
Hungary	5	0.2
Italy	83	3.8
Ireland	5	0.2
Iceland	1	0.0
Lithuania	3	0.1
Luxembourg	7	0.3
Netherland	19	0.8
Norway	7	0.3
North Ireland	10	0.4
Romania	23	1.0
Poland	14	0.6
Portugal	6	0.2
Rep of Georgia	1	0.0
Scotland	3	0.1
Serbia	2	0.0
Spain	60	2.7
Slovakia	1	0.0
Slovenia	2	0.0
Switzerland	16	0.7
Sweden	8	0.3
Ukraine	1	0.0
Wales	4	0.1
Australia	**74**	**3.3**
Australia	60	2.7
New Zealand	14	0.6
Middle East	**98**	**3.7**
Algeria	1	0.0
Egypt	1	0.0
Iraq	1	0.0
Iran	17	0.7
Israel	22	1.0
Jordan	3	0.1

Table 2 (*continued*)

List of continents	No. of articles	No. of articles (%)
Kuwait	2	0.0
Lebanon	3	0.1
Morocco	2	0.0
Oman	1	0.0
Pakistan	15	0.6
Qatar	4	0.1
Saudi Arabia	11	0.5
Turkey	12	0.5
United Arab Emirates	3	0.1
Africa	**27**	**1.0**
Ethiopia	1	0.0
Kenya	1	0.0
Nigeria	1	0.0
South Africa	22	1.0
Sudan	2	0.0

Table 3
Research areas.

Research areas	Publications	Publications (%)
Computer Science	1795	83.2
Engineering	711	32.9
Telecommunications	473	21.9
Automation Control Systems	50	2.3
Information Science Library Science	32	1.5
Science Technology Other Topics	28	1.3
Mathematics	26	1.2
Optics	25	1.2
Physics	24	1.1
Business Economics	21	1
Operation Research Management Science	19	0.9
Government Law	17	0.8
Robotics	16	0.7
Remote Sensing	13	0.6
Communication	13	0.6
Mathematical Computational Biology	10	0.5
Materials Science	10	0.5
Imaging Science Photographic Technology	9	0.4
Social Sciences Other Topics	6	0.3
Public Administration	6	0.3

performance of any research area is able to show the trend of the publication over time. The Web of Science database contains an index of various disciplines including 150 scientific research areas. Some of these research areas encompass Computer Science, Engineering, Telecommunications, Automation & Control Systems, Information Science Library of Science and Technology Science Topics. More about the publications are provided in Table 3.

Table 3 illustrates that majority of the published articles come under the area of Computer Science and Engineering. In this regard, Computer Science and Engineering is an integration that used to develop new methods and technologies that useful to academia and the public at large. Software engineering, computer architecture and algorithms, artificial intelligence, big data, machine learning, data processing, neural, and security are some of the sub-areas that come under the umbrella term of Computer Science and Engineering.

Of the articles published, the top article with the highest citation in Computer Science area was “Toward automated dynamic malware analysis using CWSandbox”. Since topics on malware analysis use algorithms, artificial intelligence, machine learning, and security analysis as an approach, an increase in publications produced under the area of Computer Science was noticeable. Table 4 illustrates the list of publications according to numbers.

Table 4 lists a number of publications noted in the area of Computer Science. It illustrates that most publications came mostly from the continent of North America. However, due to the fact that some of the articles published only show the email addresses minus a full address, the full results of indicating which part of the continent unable to realize. As a whole, this study shows that acceptances rate is high for the continent of North America because their researchers able to tailor the articles based on the journal focuses, formats, and fields.

3.3. Institutions

This section discusses the number of publications noted according to institutions. This section aims to identify which of the institutions are active and also to measure their quality by comparing institutions according to publications (Buela-Casal et al., 2007). Table 5 list the institutions which conducted research related to malware. These institutions consist of five continents encompassing North America, Asia, Europe, the Middle East and Australia.

It shows that institutions coming from North America have the highest number of publications. This is followed by Asia which carries the second highest number of publications. Subsequent to that is Europe. It appears that the Georgia Institute of Technology from North America has the highest number of publications totaling 75.8% of the entire publications including conference papers listed in ISI ranking proceedings.

The other five (5) institutions are from Asia including Korea University, National Institute of Information and Communications Technology, Chinese Academy of Sciences, National University of Defend Technology, and University of Electronic Science and Technology of China. The most prominent institutions in Asia are located in China. It seems that the speed of publication in China is much faster than the other countries in Asia. This evidence suggests that there is keen competition among institutions across Asia as well as other continents in term of publications. As conclude, researcher able to perform high impact research, having a good facility, and ability in writing allows university in the United States become most active in publishing articles.

3.4. Authors

This section discusses the number of publications noted according to authors under continents. This section aims to identify who is most active in terms of authorship in continents. Table 6 lists authors who are most productive according to countries/ continents.

As the table illustrates, the majority of the authors are from the United States. In addition, it shows that Asia is also active in publishing articles. Countries such as Japan, India and China are part of Asia. It appears that these three (3) countries are able to contribute many publications among countries in Asia. Further to that, it is noted that authors from the continent of Europe and the Middle East produced fewer publications. This emergence implies that authors from the continent of North America and Asia were more active comparatively. As is shown in Table 6, Krugel Christopler from the United States and Bringas Pablo Garcia (Bringas Pablo Garcia, 2016) from Spain are the top authors in producing publications while the rest of the authors contributed to less than 0.9% of publications.

A closer view indicates that these two authors had produced many articles because they were directly involved in Research and Development (R & D), contributing to technology development, security research and knowledge transference to society. As an example, Krugel Christopler conducts research on security analysis such as malware, the web, network, and vulnerability (Kruegel, 2016). He is also the co-founder of Lastline, Inc. and founder of

Table 4
Number of publications.

List of continents	Year										
	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Asia	**0**	**0**	**0**	**1**	**5**	**3**	**3**	**9**	**20**	**15**	**20**
Bangladesh	0	0	0	0	0	0	0	0	0	0	0
China	0	0	0	1	0	0	1	4	4	5	6
India	0	0	0	0	0	0	0	0	6	2	4
Japan	0	0	0	0	3	1	1	1	1	0	1
Malaysia	0	0	0	0	1	0	0	0	1	0	2
Singapore	0	0	0	0	0	1	0	0	0	0	2
South Korea	0	0	0	0	1	0	1	4	4	5	2
Taiwan	0	0	0	0	0	1	0	0	4	3	3
North America	**6**	**3**	**4**	**10**	**8**	**4**	**7**	**15**	**10**	**14**	**18**
Canada	0	0	0	0	0	0	1	1	1	1	0
Russia	0	0	0	0	0	0	0	0	0	0	1
United States	6	3	4	10	8	4	6	14	9	13	17
South America	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**
Brazil	0	0	0	0	0	0	0	0	1	0	0
Colombia	0	0	0	0	0	0	0	1	0	0	0
Europe	**1**	**1**	**4**	**4**	**4**	**5**	**3**	**6**	**9**	**6**	**12**
Austria	0	0	0	0	0	0	0	0	1	0	0
Czech Republic	0	0	0	0	0	0	0	0	0	0	1
Denmark	0	0	0	0	0	0	0	0	0	0	1
England	1	0	0	1	0	3	0	1	0	0	2
France	0	0	0	1	1	0	1	0	0	2	1
Germany	0	0	1	0	1	0	0	1	0	2	2
Greece	0	0	0	1	0	0	0	0	0	0	2
Italy	0	0	2	0	2	0	0	1	5	1	1
Lithuania	0	0	0	1	0	0	0	0	0	0	0
Netherland	0	1	0	0	0	0	0	0	0	0	0
Norway	0	0	0	0	0	0	0	0	1	0	0
North Ireland	0	0	0	0	0	0	0	0	0	1	0
Romania	0	0	0	0	0	1	0	0	0	0	1
Poland	0	0	0	0	0	0	0	1	0	0	0
Portugal	0	0	0	0	0	0	0	0	0	0	1
Spain	0	0	0	0	0	0	1	2	2	0	0
Switzerland	0	0	1	0	0	0	1	0	0	0	0
Sweden	0	0	0	0	0	1	0	0	0	0	0
Australia	**0**	**0**	**0**	**0**	**0**	**1**	**3**	**3**	**3**	**1**	**1**
Australia	0	0	0	0	0	1	3	2	2	1	1
New Zealand	0	0	0	0	0	0	0	1	1	0	0
Middle East	**0**	**0**	**0**	**1**	**3**	**0**	**2**	**3**	**4**	**7**	**3**
Iran	0	0	0	0	0	0	1	1	0	2	1
Israel	0	0	0	0	1	0	0	2	1	3	0
Jordan	0	0	0	0	0	0	0	0	0	1	0
Lebanon	0	0	0	0	1	0	0	0	1	0	0
Pakistan	0	0	0	0	0	0	0	0	1	0	1
Saudi Arabia	0	0	0	0	0	0	0	0	0	1	0
Turkey	0	0	0	1	1	0	1	0	1	0	0
United Arab Emirates	0	0	0	0	0	0	0	0	2	2	1
Africa	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**1**	**0**
South Africa	0	0	0	0	0	0	0	0	2	1	0
Type	**2**	**5**	**10**	**14**	**23**	**18**	**14**	**19**	**21**	**15**	**75**
Book	2	3	4	8	11	3	1	8	0	0	0
Book Section	0	2	6	6	12	15	13	11	21	15	75

iSecLab (Christopler, 2016). In addition, Cloud-based malware analysis tool (Anubis) is currently, the most well-known development of iSecLab, used by over ten thousands of users. This evidence shows that the involvement of the researcher directly in R & D able to boost earnings in terms of article production. The authors who able to understand the journals requirement such as research topics, methods and able to follow the rapid changes in research become advantages to them in publishing articles.

3.5. *Impact journals*

This section discusses the list of impact journals under

Table 5
List of institutions.

Institutions	Publications	Publications (%)	Country
Georgia Institute of Technology	29	1.3	United States
University Michigan	26	1.2	United States
Carnegie Mellon University	24	1.1	United States
Purdue University	23	1.0	United States
Korea University	22	1.0	South Korea
Vienna University Technology	21	0.9	Austria
Deakin University	20	0.9	Australia
Chinese Academy of Sciences	19	0.8	China
National Institute of Information and Communications Technology	17	0.7	Japan
Concordia University	17	0.7	Canada
Pennsylvania State University	16	0.7	United States
National University of Defend Technology	16	0.7	China
George Mason University	16	0.7	United States
University of Deusto	15	0.6	Spain
North Carolina State University	15	0.6	United States
Ben-Gurion University of the Negev	15	0.6	Israel
University of Electronic Science and Technology of China	14	0.6	China
University of Pennsylvania	13	0.6	United States
Texas A&M University	13	0.6	United States
National Chiao Tung University	13	0.6	Taiwan
Indiana University	13	0.6	United States
University of Texas at Dallas	12	0.5	United States
Tsinghua University	12	0.5	China
Technical University of Berlin	12	0.5	Germany
Ruhr University Bochum	12	0.5	Germany

Table 6
List of authors.

Authors	Publications	Publications (%)	Country
Krugel Christopler	19	0.9	United States
Bringas Pablo Garcia A	19	0.9	Spain
Santos Igor	18	0.8	Spain
Inoue Daisuke	18	0.8	Japan
Kirda Engin	16	0.7	United States
Vinod Padmanabha Rao	15	0.7	India
Nakao Koji	15	0.7	Japan
Mukkamala Srinivas	15	0.7	United States
Jiang Xuxian	15	0.7	United States
Gu Guofei	14	0.6	United States
Elovici Yuval	14	0.6	Israel
Yoshioka Katsunari	13	0.6	Japan
Holz Thorsten	13	0.6	Germany
Eto Masashi	13	0.6	Japan
Mourad Debbabi	13	0.6	Canada
Sarkar Saswati	12	0.6	United States
Lee Wenke	12	0.6	United States
Zhang Xiangyu	11	0.5	China
Schultz Eugene	11	0.5	United States
Vijay Laxmi	11	0.5	India
Stefano Zanero	10	0.5	United States
Heng Yin	10	0.5	United States
Xu Dongyang	10	0.5	United States
Sakir Sezer	10	0.5	United Kingdom

Computer Science area. This section is important because it shows the most leading journal in publication and the highest citations received. From this information, researchers are able to strengthen their work by publishing in good quality journals.

Table 7 lists 20 journal titles with the greatest number of publications. It shows that the greatest number of publication belongs to the collection of book series under Lecture Notes In Computer Sciences followed by Bioinformatics and BMC Bioinformatics journals. The book series of Lecture Notes In Computer Sciences has the greatest number of publications. This is because it provides publishing services especially in new development areas such as education and computer science and information technology research.

The table demonstrates that the book series has a good relationship with academics, prestigious institutions and it collaborates with the research and development (R & D) community in computer science (Hutchison and Mitchell, 2016). It has also become a focal point for publishing articles because it provides the most valuable publishing services which are quick and informal, therefore cutting down time. In addition, proceedings and post-proceedings also serve as some of the core publications. Two types of subseries help book series in the publishing services: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics (Hutchison and Mitchell, 2016). "Automated classification and analysis of Internet malware" is an example of a conference paper published in Lecture Notes Computer Sciences which carry 63 citations (Bailey et al., 2007).

Table 7 shows that Bioinformatics received 250,487 citations over the years followed by BMC Bioinformatics and Information Sciences with 97,406 and 68,000 citations respectively. Bioinformatics is a premier journal in computational biology. It focuses on bioinformatics and computational biology genome fields (Oxford, 2015). This is because these fields boost the ranking of Bioinformatics by describing a way to analyze genetic sequence (Noorden et al., 2014). In addition to that, the majority of journals listed in Bioinformatics appear to carry more than 1000 citations. Articles with the title "Clustal w and Clustal x version 2.0" received a total citation of more than 10,000 (Larkin et al., 2007). The high citations obtained by each journal have helped to raise the journal Bioinformatics, as the journal with the highest received citations.

Therefore, based on Table 7, it shows that journals with dominant publications and citations are Bioinformatics and BMC Bioinformatics. Further to that, eight (8) journal titles were also listed in Table 7 to highlight that these journals are present in the database. They suggest that these eight (8) journals are the most active in publishing research on malware. As a whole, the quality of high impact journals able to attract researcher to publish their article because it widely read by another researcher also increase their citations.

3.6. Highly-cited articles

This section discusses the number of citations received by the journals. This section reflects on the quality of research done and the influence it has on similar fields. Table 8 lists 25 of the most cited articles. It covers information such as a number of times cited, published journals, years, and research areas. These articles considerably contribute about 1.16% to the overall publications. Moreover, the top 4 most highly-cited articles were published between seven (7) to nine (9) years ago, showing a compliance with the concept that the longer the articles have been in the database, the higher the number of citations accumulated. The research areas which contribute to the publications are Mathematics, Telecommunications, Engineering, Physics, Science & Technology - other Topics, and Automation & Control Systems with Computer Science being the most prominent.

Of the articles published, the most cited were "Toward automated dynamic malware analysis using CWSandbox". The article describes the dynamic analysis used to determine malware by using simulated environment which was known as CWSandbox (Willems et al., 2007). The CWSandbox application was able to monitor, analyze and report malware activities based on system calls. Researchers who worked in malware detection used the CWSandbox to analyze any malicious activities via the dynamic analysis methods. From this, it concluded that highly cited articles

Table 7
Top 20 journals with the greatest number of publications and citations.

Journals title with the greatest number of publications	IF	Q	P	P (%)	Most cited journals title	IF	Q	C	C (%)
Lecture Notes In Computer Science	0.402	Q4	36,144	31.3	Bioinformatics	5.766	Q1	250,487	27.4
Bioinformatics	5.766	Q1	7645	6.6	BMC Bioinformatics	2.435	Q3	97,406	10.7
BMC Bioinformatics	2.435	Q3	6347	5.5	Lecture Notes In Computer Science	0.402	Q4	68,000	7.1
IEEE Transactions on Wireless Communications	2.925	Q1	5486	4.8	Information Sciences	3.364	Q1	64,396	7.1
Neurocomputing	2.392	Q1	5353	4.6	IEEE Transactions on Wireless Communications	2.925	Q1	50,085	5.5
IEICE Transactions on Communications	0.300	Q4	5251	4.6	Information Sciences	3.364	Q1	47,479	5.2
IEEE Transactions Information Theory	1.737	Q2	5098	4.4	Computer Methods in Applied Mechanics and Engineering	3.467	Q1	42,684	4.7
Theoretical Computer Science	0.643	Q3	4672	4.0	IEEE Journal on Selected Areas in Communications	3.672	Q1	29,318	3.2
IEEE Communications Letters	1.291	Q2	4544	3.9	Neurocomputing	2.392	Q1	29,035	3.2
Information Sciences	3.364	Q1	4416	3.8	Environmental Modeling & Software	4.207	Q1	27,194	3.0
IEEE Transactions on Communications	2.298	Q1	3782	3.3	Computers & Operations Research	1.988	Q2	26,192	2.9
Wireless Personal Communications	0.701	Q4	3712	3.2	IEEE Transactions on Communications	2.298	Q1	24,475	2.7
IEICE Transactions on Information and Systems	0.226	Q4	3685	3.2	IEEE Communications Magazine	5.125	Q1	22,343	2.4
Computer Methods in Applied Mechanics and Engineering	3.467	Q1	3227	2.8	Computers & Education	2.881	Q1	21,716	2.4
ACM SIGPLAN Notices	0.488	Q4	3102	2.7	ACM Transactions on Graphics	4.218	Q1	20,215	2.2
Applied Soft Computing	2.857	Q1	2873	2.5	Applied Soft Computing	2.857	Q1	19,781	2.2
International Journal of Innovative Computing Information and Control	1.667	Q1	2568	2.2	Journal of Machine Learning Research	2.450	Q1	19,757	2.2
Computer Networks	1.446	Q2	2530	2.2	Computers & Structures	2.425	Q1	18,360	2.0
Computers & Operations Research	1.998	Q2	2522	2.2	IEEE Communications Letters	1.291	Q2	18,200	2.0
Computer Communications	2.099	Q1	2445	2.1	Computers & Geosciences	2.474	Q1	16,015	1.8

IF, Impact Factors; Q, Quartile; P, Publication; P (%), Publications (%); C, Citation; C (%); Citations (%).

are not ordinary articles but are quality research articles in which the researcher acknowledged other author's findings, methods, ideas and influence in certain fields. As a whole, the interesting topic in articles also able to increase journal citations especially when it becomes special issues.

3.7. *Keywords frequency*

This section discusses the type of keywords which are frequently used by researchers. This is important because it enables articles to be detected in current as well as past issues of research journals. In 1990, the Web of Science began to provide author keywords and a description of an article's theme (Sun et al., 2012; Wu et al., 2015). These keywords and titles could be used to analyze research trends and to identify research gaps. Table 9 provides the list of unique keywords and title occurrences. This list was derived from a total of 26,994 keywords and 3866 titles that had emerged from 2158 articles for the period between 2005 until 2015.

Based on Table 9, it shows that the most relevant titles and keywords are malware detection and attack. Data provided also show that the malware detection and attack are consistently used in the literature. This implies that most researchers had used these titles and keyword in their research. For example, the article with the titles “Semantic-aware malware detection” and “Android botnets for multi-targeted attacks” have the term “detection” and “attack”. Fig. 4 is further provided to indicate an in-depth analysis. Data indicate that the word map was drawn from the content analysis of the articles. This shows that map words divided into 5 clusters. More is detected in Fig. 4 below.

The clusters in Fig. 4 demonstrate the increased development of research that is related to “malware”. It illustrates two (2) main topic clusters are the type of malicious (red, left) and algorithm (green, right). The types of malicious are highlighted by key terms which are related to security, specifically, “traffic,” “botnet”, “malicious website”, “social network”, “service”, “infrastructure”, “honeypot”, while malware analysis comprises terms such as “malware detection”, “algorithm”, “classification”, “malware family”, “static analysis”, “false positive”, “Naive Bayes”). In addition, “computer virus”, “behavior analysis”, and “compromise system” were noted as terms that act as links between the research topics within the types of malicious and algorithm clusters. The small cluster (purple, upper left) in Fig. 4 is mainly focused on mobile security research topics such as “android malware”, “mobile device”, “mobile malware”, “mobile application”, and “smartphone”. Table 8 illustrates the clusters according to colors.

Table 10 provides the list of unique clusters and their descriptions. This list was derived from in-depth analysis to establish the kinship between the clusters and topics. It shows five (5) categories of unique clusters, including red, green, yellow, purple and blue. These categories imply that most researchers had done their research on a certain topic such as malware classification, detection tools, type of algorithm and type of operating systems. As a whole, more analysis possible to be done in these five (5) categories. In order to show their relationship in malware detection system. In Section 4, we described details of malware detection systems since all these categories are part of it.

4. Malware detection system

This section discusses the classification of malware detection systems. This section aims to provide more information on malware detection system. Malware is a malicious software which is able to access mobile and computer devices in order to extract personal information and thereby, cause serious damage to the system. Table 11 describes the various types of malware.

Based on Table 11, it lists the various types of malware are very dangerous and able to harm the systems. Unscrupulous authors design various type of malware such as the botnet, Trojan, rootkit and worm for these intentions (Karim et al., 2014; Felt et al., 2011; Muthumanickam and Ilavarasan E, 2015). Each malware has its own goals and it usually causes undesirable results (Wu et al., 2014). Unscrupulous authors also design the botnet for phishing, malware distribution, spam emails, distributed denial of service (DDoS) attacks and also fraud (Karim et al., 2014).

To counter this, machine learning is used to detect botnet activity by looking at network traffic behavior (Zhao et al., 2013) and other malware categories such as Trojans, worms, and viruses (Sanz et al., 2013; Grecio et al., 2014). Of these malware, rootkits

Table 8
List top 25 of highly-cited articles.

Titles	Times cited	Published journal	Year	Research area
Toward automated dynamic malware analysis using CWSandbox	102	IEEE Security & Privacy	2007	Computer Science
Dissecting Android Malware: Characterization and Evolution	95	2012 IEEE Symposium on Security and Privacy	2012	Computer Science
Semantics-aware malware detection	93	2005 IEEE Symposium on Security and Privacy, Proceedings	2005	Computer Science
On Lightweight Mobile Phone Application Certification	70	Ccs'09: Proceedings of the 16th ACM Conference on Computer and Communications Security	2009	Computer Science
Automated classification and analysis of Internet malware	63	Recent Advances in Intrusion Detection, Proceedings	2007	Computer Science
Ether: Malware Analysis via Hardware Virtualization Extensions	59	Ccs'08: Proceedings of the 15th ACM Conference on Computer and Communications Security	2008	Computer Science
BitBlaze: A New Approach to Computer Security via Binary Analysis	56	Information Systems Security, Proceedings	2008	Computer Science
Learning and classification of malware behavior	53	Detection of Intrusions and Malware, and Vulnerability Assessment	2008	Computer Science
Lares: an architecture for secure active monitoring using virtualization	49	Proceedings of the 2008 IEEE Symposium on Security and Privacy	2008	Computer Science
Exploring multiple execution paths for malware analysis	48	2007 IEEE Symposium on Security and Privacy, Proceedings	2007	Computer Science
SubVirt: implementing malware with virtual machines	47	2006 IEEE Symposium on Security and Privacy, Proceedings	2006	Computer Science
Andromaly: a behavioral malware detection framework for android devices	44	Journal of Intelligent Information Systems	2012	Computer Science
Limits of static analysis for malware detection	43	Twenty-Third Annual Computer Security Applications Conference, Proceedings	2007	Computer Science
The nepenthes platform: an efficient approach to collect malware	43	Recent Advances in Intrusion Detection, Proceedings	2006	Computer Science
Stealthy Malware Detection Through VMM-Based "Out-of-the-Box" Semantic View Reconstruction	41	Ccs'07: Proceedings of the 14th ACM Conference on Computer and Communications Security	2007	Computer Science
TrustVisor: Efficient TCB Reduction and Attestation	40	2010 IEEE Symposium on Security and Privacy	2010	Computer Science
Your Botnet is My Botnet: Analysis of a Botnet Takeover	40	Ccs'09: Proceedings of the 16th ACM Conference on Computer and Communications Security	2009	Computer Science
Thresholds for virus spread on networks	40	Annals of Applied Probability	2008	Mathematics
Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis	38	Ccs'07: Proceedings of the 14th ACM Conference on Computer and Communications Security	2007	Computer Science
A Survey on Security for Mobile Devices	36	IEEE Communications Surveys and Tutorials	2013	Computer Science
Privilege Escalation Attacks on Android	36	Lecture Notes in Computer Science	2011	Computer Science
Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software	36	European Journal of Information Systems	2009	Computer Science
Behavioral Detection of Malware on Mobile Handsets	32	Mobisys'08: Proceedings of the Sixth International Conference on Mobile Systems, Applications, and Services	2008	Computer Science
Using entropy analysis to find encrypted and packed malware	30	IEEE Security & Privacy	2007	Computer Science
A Survey of Botnet and Botnet Detection	29	2009 Third International Conference on Emerging Security Information, Systems, and Technologies	2009	Computer Science

Table 9
Relation between titles and keywords in malware topic.

Titles	Frequency	Keywords	Frequency
Malware detection	128	Attack	522
Network	128	Network	407
Security	71	Detection	392
Attack	64	User	354
Study	42	Security	246
Machine	37	Feature	243
Malware analysis	37	Signature	228
Defense	30	Algorithm	225
Design	27	Code	220
Survey	26	Experiment	213
Malware propagation	25	Program	205
Malware attack	20	Service	189
Mobile device	20	Internet	184
Evaluation	18	Smartphone	179
Smartphone	18	File	169
Intrusion detection	16	Device	165
Implementation	15	Malware detection	158
Android malware	14	Worm	157
Internet	13	Control	147
Static Analysis	13	Experimental result	146

Table 10
Type of clusters.

Clusters	Descriptions
Red	Type of malicious
Green	Algorithm is used to solve the problem on malware analysis
Yellow	Simulation tools are used to modeling the prototype and observe the operation
Purple	Mobile malware analysis able to detect suspicious activity in mobile platform
Blue	Network-based monitor intrusion in network traffic

Table 11
Types of malware.

Types	Descriptions
Botnet	Botnet allows an attacker to take control over the infected computer. The infected computer is known as a zombie and always spread themselves through the network
Worm	The worm infects the operating systems by multiplying itself to affect the operating systems and sending copies of itself through networks
Rootkit	Rootkit is a malicious application which gained root privilege to modify operating system functionalities (M and G, 2012)
Trojan	Trojan able distinguishes as a normal application to attract user for run its. After successfully run, Trojan take over the resources and able to disrupt the availability of operating system with denial of service

are very difficult to detect because it able to start the malicious activities while the user is not using the devices. However, (Schmidt et al., 2011) there is a way to detect rootkit in cloud computing by performing live-scanning on all binary system calls. Fig. 5 shows the classification of malware detection system.

In this paper, malware detection systems are classified into categories. The classifications are based on 3 parts, (a) analysis technique, (b) detection approach and (c) deployment approach. These classifications are important in showing the relationship in the publications which are related to malware.

4.1. Analysis technique

This section discusses the type of malware analysis techniques which provides the purpose and functionality of malware analysis. Malware analysis is a process of examining the malware code and identifying the dynamic characteristics of the malware. Unscrupulous authors strive to avoid malware analysis with obfuscation (Sharif et al., 2008), packer and anti-debugging technique (Rad et al., 2012; Xie et al., 2013; Alazab et al., 2010). These techniques make malware analysis harder thus, enabling them to better hide their devious intentions. As a result of this, lead security analysts are unable to examine what is happening between malware and normal applications.

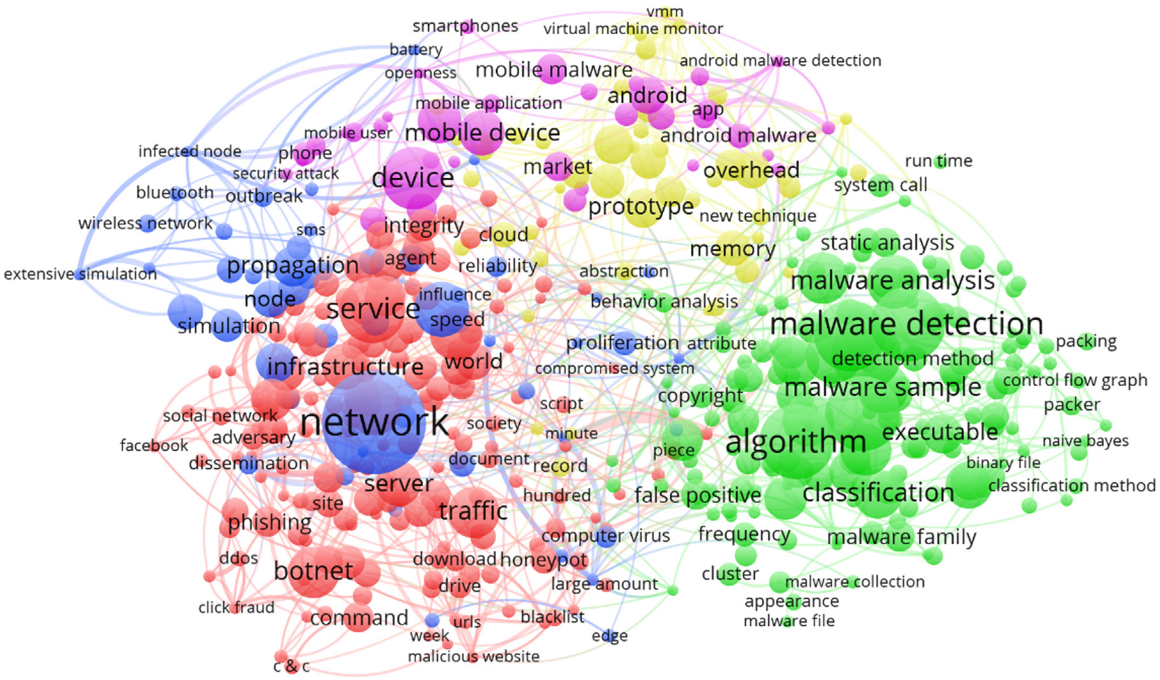


Fig. 4. Keyword clusters. (For interpretation of the references to color in this figure, the reader is referred to the web version of this article.)

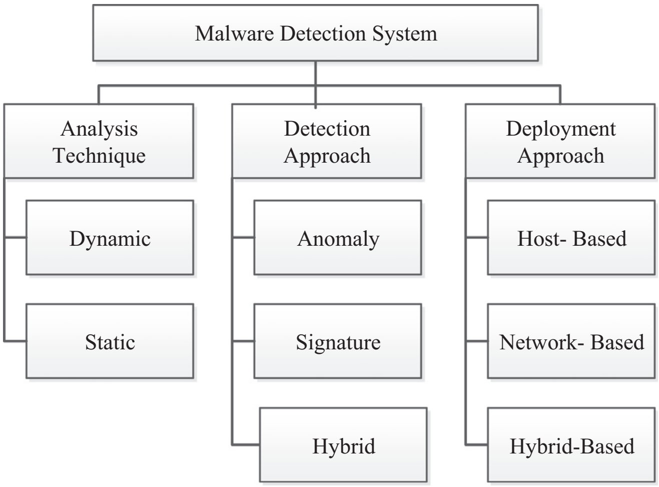


Fig. 5. Classification of malware detection system.

Table 12
Type of malware analysis.

Analysis technique	Advantages	Disadvantages
Dynamic	• Able to detect unknown malware	• Time intensive • Resource consuming
Static	• Fast detection	• Unable to detect malware with obfuscation technique

The aim of malware analysis is to study the component by dissecting the application code and its behavior (Zhou and Jiang, 2012; Platforms and Threats, 2013). In addition, the analyst conducting the test has to be careful during the malware analysis process in order to avoid further spread of contamination. Analyzing malware needs a proper environment setup so as to ensure security and to prevent systems from getting infected. The process of conducting a malware analysis begins with an isolated environment such as virtualization software (Damopoulos et al., 2012; Gonzalez et al., 2014). The two techniques known in malware analysis are static and dynamic analysis (Ravula et al., 2013; Gandotra et al., 2014). Table 12 lists the types of malware analysis.

As the table illustrates, there are two types of malware analysis: Dynamic and Static. The static analysis applies reverse engineering, similarity and command techniques (Veerwal and Menaria, 2013). Dynamic analysis analyzes the malicious behaviors and error programs through the observations conducted in the controlled environment (Ghiasi et al., 2015). Unlike static analysis, dynamic analysis is able to detect malware when it applies the obfuscation techniques. This analysis technique also reduces costs, provides accurate results and validation of code analysis findings as well as identifies the problem in the controlled environment.

Static analysis has the advantage of fast detection but its major problem is its use of the obfuscation techniques. It examines malware without executing it. These techniques are able to read the code program, determine the goals and also detect malware (Talha et al., 2015). This is a disadvantage because malware is capable of evading detection (Moser et al., 2007). Unscrupulous authors apply other techniques like polymorphism, metamorphism, and encryption to evade such detections (Rad et al., 2012). The other analysis technique is that of dynamic which is capable of detecting unknown malware. It executes the malware through monitors in a controlled environment (Egele et al., 2012; Seideman et al., 2015).

4.2. *Detection approach*

This section discusses the malware detection approach together with their characteristics. It also provides an overview of the existing approach including the advantages and disadvantages. The two common detection approach seen in IDS are anomaly and signature (Feizollah et al., 2013a; Elshoush and Osman, 2011; Yassin et al., 2012; Hubballi and Suryanarayanan, 2014). Anomaly approach detects malicious activities by monitoring the level of activities seen in network traffic and systems (Shabtai et al., 2014; Narudin et al., 2014). The anomaly detection approach is better able to detect new and unfamiliar attacks through the use of normal and abnormal patterns. In addition to signature and anomaly detection approach, a hybrid approach combines the signature database with anomaly pattern to detect known or new variants of malware attacks (Inayat et al., 2015; Wang et al., 2015). The hybrid approach able to perform dynamic analysis during the running application and then statistically analyze using signature database (Arshad et al., 2016). By using this type of approach, it able to overcome the weaknesses of both signature and anomaly detection approach. However, this approach needs more research and subjected to the malware detection designs.

Besides that, machine learning is also used to trace the normal and abnormal patterns (Inayat et al., 2015; Haq, 2015). In this regard, machine learning is thus, a type of artificial intelligence that provides computational learning theory that also predicts the data. Machine learning focuses on prediction making and acts without being explicitly programmed. In addition, machine learning is an approach that searches through data to look for patterns. Supervized and unsupervized classifier in machine learning is also used to trace the model and analyze the features (Narudin et al., 2014). This approach helps to determine the validity of normal and malicious activities. Decision trees, random forest, and SVM are the type of algorithm classifiers used on supervized learning for this purpose. Table 13 presents the anomaly approach.

Table 13
Anomaly approach.

Reference	Objective	Algorithm	Result
(Wang and Wang, 2014)	To develop an automatic malware detection system by based on behavior signatures	Support vector machines (SVM)	Accuracy=97.67%
(Kim et al., 2015)	To identify fake AV web pages in the Internet.	Random forest, SVM and Gradient-Boosted Tree	Accuracy=90.4%, FPR=0.2%.
(Cui et al., 2015)	To identify the malicious behaviors of the mobile applications using data mining packet	Naive Bayes and Decision tree	Accuracy=60%
(Lin et al., 2015)	To select and extract malware features	SVM	Accuracy=0.98, Precision=0.85, TPR=0.92, TNR = 0.98
(Ghiasi et al., 2015)	To find similarities of run-time behaviors based on the assumption that binary behaviors affect registers values	Random forest, Decision tree, Bayesian logistic regression	Accuracy=95.9%, FP=4.5%

Table 14
Signature approach.

Reference	Objective	Algorithm	Result
(Elish et al., 2015)	To advocate the approach of benign property enforcement	Trigger based API dependence	FP=2%, FN=2.1%
(Talha et al., 2015)	To characterize and classify Android applications as benign or malicious.	Statistical score	FPR=0.050, TPR=0.101, FNR=0.898
(Sheen et al., 2015)	To design malware detection using multi feature collaborative decision fusion (MCDF).	Naive Bayes, Decision tree, SVM, IBk (Instance based learning), JRip (Rule based learning)	Precision=83%, TPR=97%
(Choi et al., 2015)	To detect the act of leakage internal private information	Context Ontology Reasoning	Condition reasoning (high, low, active, available)
(Faruki et al., 2014)	To detect unknown malware	Clustering algorithm	Accuracy=76%, TPR=80.65%
(Cen et al., 2015)	To develop effective technique for malware detection	Naive Bayes	Accuracy=0.95, TPR=0.95, FPR=0.05
(Clemens, 2015)	To classify architecture of computer object code	SVM, Decision tree, Random Forest, Naive Bayes, Neural network	Accuracy=90%

Table 15
Advantage and disadvantage of detection approach.

Detection approach	Advantages	Disadvantages
Anomaly	• Dynamically adapt to new, unique, or original attacks. • Less dependent on identifying specific operating system vulnerabilities • Effective to detect new and unforeseen vulnerabilities	• Higher false alarm rates • Usage patterns that change often and not be static enough to implement an effective behavior-based IDS.
Signature	• Lower false alarm rates • Alarms are more standardized and more easily understood than behavior-based • Simplest and effective method to detect known attacks (Liao et al., 2012)	• Signature database must be continually updated and maintained • Ineffective to detect unknown attacks, evasion attacks, and variants of known attacks (Liao et al., 2012) • Time-consuming to maintain the knowledge

Besides the anomaly approach, another type of approach is called the signature approach. Table 14 presents the signature approach.

As is seen in the table above, signature detection approach detects malicious activities by matching the normal pattern with abnormal signatures. It also discovers malware pattern by using the signature which is stored in a database. However, this approach is unable to detect unknown malware if the signature is not yet available in the database. Moreover, this type of approach needs to frequently update the signature database so as to ensure that it able to detect new variants of malware and to define possible pattern variations (Feizollah et al., 2013a). Any mistake in defining the malicious pattern cause a false alarm and decrease the accuracy of the detection technique. Table 15 lists the advantage and disadvantage of the detection approach. From this table, it noted that each of these approaches has its strengths and weaknesses.

4.3. Deployment approach

This section discusses the type of deployment approach used in the IDS. This section looks at how the deployment approach (hybrid, network and host-based) monitors and detects malicious activities (Inayat et al., 2015; Shameli-Sendi et al., 2014; Lar, 2011). Hybrid-based Intrusion Detection System is a combination of both Network-based Intrusion Detection System (NIDS) and Host-based Intrusion Detection System (HIDS) approach (Butun et al., 2014). NIDS is used analyze data over the network traffic by using deep packet analyzer (Zhang et al., 2003). The packet analyzer is able to identify any malicious activities during interactions between the network and computer (Patel et al., 2012). HIDS monitors and analyzes any intrusive activities which assess the system resources. The HIDS focuses on memory, the device, CPU consumption, the user, system activities and also file systems (Weiss et al., 2012). Andromaly (Shabtai et al., 2012) is an example of host-based malware detection.

The HIDS collects resource from mobile devices, computers, and servers. Over the years, the boom of mobile devices has stimulated users into replacing personal computers in terms of the Internet usage particularly in the use of online banking, games, emails, social media, and news articles. The mobile device is more appealing to users since the applications are downloadable and are free from the official website.

4.4. Mobile malware

The emergence of mobile devices and their usage on sensitive application such as internet banking has risen the threat and makes them the target of malware authors. To understand the malware threat, this section discusses a review of mobile malware. We have selected papers contributed to the research of mobile malware from ISI Web of Science database published in 2005–2015. Fig. 6 demonstrates publication trends related to mobile research.

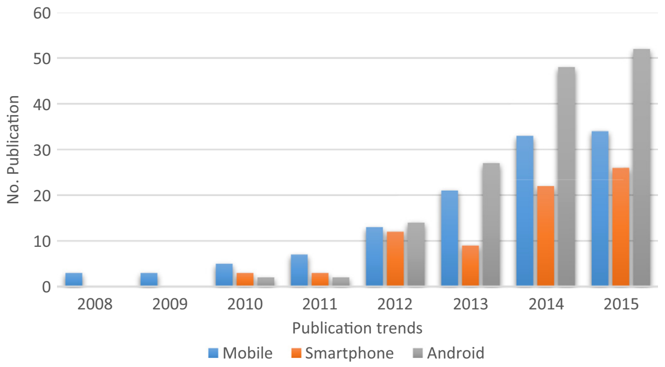


Fig. 6. Publication trends.

Table 16
List of malware features.

Type of features	Features	Reference
Dynamic	Systems calls	(Grégio et al., 2011; Feizollah et al., 2015)
	Network traffics	(Muniyandi et al., 2012; Feizollah et al., 2015)
	System components	(Feizollah et al., 2015)
	User interactions	(Feizollah et al., 2015)
Static	API	(Qiao et al., 2013; Aafer et al., 2013)
	Strings	(Sanz et al., 2013)
	Byte	(Santos et al., 2013)
	URL	(Thomas et al., 2011)
	Permissions	(Arp et al., 2014; Feizollah et al., 2015)
	Java code	(Feizollah et al., 2015)
	Network address	(Feizollah et al., 2015)
	Hardware components	(Feizollah et al., 2015)
	Intent filters	(Feizollah et al., 2015)
Hybrid	Combination static and dynamic features	(Feizollah et al., 2015)
Application's Metadata	Application description	(Feizollah et al., 2015)
	Creator ID	(Feizollah et al., 2015)
	Application categories	(Feizollah et al., 2015)

As part of the utilization, certain sensitive data such as passwords, contact lists, pictures, videos, and account numbers are stored on these mobile devices. Due to this prominent usage of the mobile devices, unscrupulous authors are able to turn their attention to mobile devices and cause mischief. These unscrupulous authors spread the mobile malware so as to obtain the sensitive data and in doing so, are able to damage the systems. Mobile malware cause financial loss for example, when sending a premium short message (SMS) without the user's consent. Mobile malware has become a security issue whereby detection and analysis are seriously needed so as to curb further problems. The Android is one type of mobile operating systems which has become the target of attackers (Symantec, 2014). Malgenome data set (Zhou and Jiang, 2012) release in 2012 contains 1260 in 49 different Android malware families. In particular, the first work is one of the most appreciated paper in mobile malware detection because it represents the first families' classification on Android malware. Table 16 lists a group of malware features.

Table 16 illustrates the list of malware features. Android consists of the various potential part to be a feature in malware detection (Feizollah et al., 2015). It shows that the effective detection system for Android depends on the features.

In order to protect the user from Android malware threats, the different solution has been proposed. For example, DroidAPIMiner (Aafer et al., 2013) analysis malware behavior at API level to mitigate Android malware installation by providing lightweight and robust classifier. As a result, it able to achieve 99% accuracy with a false positive rate 2.2%. (Canfora et al., 2015) proposed a static analysis mechanism using sequences of opcode for detecting malware in Android platform. It shows 96.88% accuracy for detecting Android malware. Fig. 6 illustrates publication trends related to mobile research.

Fig. 5 shows the publications trend extracted from word map which is related to malware. It shows three (3) categories of publication trends including mobiles, smartphone and Android. Android becomes popular in malware research with 42.8% of publications. It shows that the current issue is more on Android research and it continues to grow since 2012 until 2015. It is also expected to increase for the next few years. This Android malware is best described as the new direction for research in security.

Android is a mobile operating system made by Google (Schmeelk et al., 2015). It is installed on a variety of mobile devices and it offers Google's services like Google search, Gmail, YouTube, and Google maps. The android also delivers a free application for download and these easily installed on mobile devices. Such services fascinate user's attention and so, further encourage them to use mobile Android operating systems. The mobile Android is more popular than other operating systems (Apvrille and Strazzere, 2012). Gartner estimates that 60% of mobile devices installed with the Android operating systems (Gartner, 2015).

Android applications able to download from its official website Google Play and also from third party markets such as SlideMe, GetJar, and Amazon's Appstore (Narudin et al., 2014). Android applications are free but payment is required for full premium version. Applications are downloaded onto Android mobile devices manually without using a store. Android has become a trendy mobile operating system thus, it experiences more targets from malware. Table 17 displays the deployment approach. As is seen in the table below, HIDS and NIDS able to be implemented on Android malware detection. The IDS method is used to identify and analyze Android mobile malware (Corona et al., 2013).

4.5. Evaluation measure

This section discusses various evaluation measures used by researchers to assess accuracy in malware detection and the effectiveness of their methods. This section identifies common

Table 17
Deployment Approach.

Reference	Titles	Deployment approach	Detection approach	Year
(Shabtai and Elovici, 2010)	Applying behavioral detection on android-based devices	HIDS	Signature	2010
(Grace et al., 2012)	Unsafe exposure analysis of mobile in-app advertizements	HIDS	Signature	2012
(Dini et al., 2012)	MADAM: A multi-level anomaly detector for android malware	HIDS	Anomaly	2012
(Zhao et al., 2012)	RobotDroid: A Lightweight Malware Detection Framework on Smartphones	HIDS	Anomaly	2012
(Wu et al., 2012)	DroidMat: Android Malware Detection through Manifest and API Calls Tracing	HIDS	Signature	2012
(Feizollah et al., 2013b)	Anomaly Detection Using Cooperative Fuzzy Logic Controller	NIDS	Anomaly	2013
(Narudin et al., 2014)	Evaluation of machine learning classifiers for mobile malware detection	NIDS	Anomaly	2014
(Cen et al., 2015)	A Probabilistic Discriminative Model for Android Malware Detection with Decompiled Source Code	HIDS	Signature	2014
(Gonzalez et al., 2014)	DroidKin: Lightweight Detection of Android Apps Similarity	HIDS	Signature	2014
(Gheorghe et al., 2015)	Smart malware detection on Android	NIDS	Anomaly	2015
(Chen et al., 2015)	Simple and effective method for detecting abnormal internet behaviors of mobile devices	NIDS	Anomaly	2015
(Wang et al., 2015)	Novel Hybrid Mobile Malware Detection System Integrating Anomaly Detection With Misuse Detection	HIDS	Hybrid	2015
(Chuang and Wang, 2015)	Machine Learning Based Hybrid Behavior Models for Android Malware Analysis	HIDS	Hybrid	2015

evaluative measures noted in the research community. The effectiveness of malware detection assesses how accurate it is in detecting malware through the evaluation measures used (Feizollah et al., 2015; Wu et al., 2012). In this paper, the standard metrics is used to evaluate malware detection. A true positive (TP) refers to an instance where detection is correctly noted as malicious. The higher the true positive, the better the result. A false negative (FN) represents an instance where detection is incorrectly noted as benign. A true negative (TN) is a benign application detected correctly as benign. A false positive (FP) is a benign application detected incorrectly as malicious. The following metrics are used for evaluating malware detection systems (Gheorghe et al., 2015; Wu et al., 2012).

- True positive rate (TPR), also called recall rate, is defined as

$$TPR = \frac{TP}{TP + FN} \tag{1}$$

- True negative rate (TNR) is defined as

$$TNR = \frac{TN}{TN + FP} \tag{2}$$

- False positive rate (FPR) is defined as

$$FPR = \frac{FP}{FP + TN} \tag{3}$$

- False negative rate (FNR) is defined as

$$FNR = \frac{FN}{FN + TP} \tag{4}$$

- Accuracy is defined as

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{5}$$

- Precision is defined as

$$Precision = \frac{TP}{TP + FP} \tag{6}$$

- F-measure is defined as

$$F - measure = \frac{2xTPRx\ Precision}{TPR + Precision} \tag{7}$$

Table 18
Evaluation measures.

Evaluation measure	No. of tested apps	Type of analysis	Year	Reference
True positive rate	800	Dynamic	2015	(Gheorghe et al., 2015)
	1738	Static	2012	(Wu et al., 2012)
	2000	Static	2013	(Yerima et al., 2013)
	6863	Static	2015	(Suleiman Y. Yerima and Muttik, 2015)
True negative rate	1100	Static	2014	(Deshotels et al., 2014)
	2000	Static	2013	(Yerima et al., 2013)
False positive rate	1000	Dynamic	2014	(Narudin et al., 2014)
	1257	Dynamic	2013	(Feizollah et al., 2013a)
	120	Dynamic	2012	(Dini et al., 2012)
False negative rate	1100	Static	2014	(Deshotels et al., 2014)
	2000	Static	2013	(Yerima et al., 2013)
Accuracy	800	Dynamic	2015	(Gheorghe et al., 2015)
	1738	Static	2012	(Wu et al., 2012)
Precision	1000	Dynamic	2014	(Narudin et al., 2014)
	174,971	Static	2015	(Cen et al., 2015)
F-measure	1000	Dynamic	2014	(Narudin et al., 2014)
	1738	Static	2012	(Wu et al., 2012)
	800	Dynamic	2015	(Gheorghe et al., 2015)

With the formula provided in assessing accuracy, the section below discusses the evaluation measures. Table 18 is provided for illustration.

From the information given, it shows that evaluation measures and the number of datasets play an important part in calculating malware detection system.

5. Challenges and future trends

This section discusses the research challenges and future trends in research that is related to malware. In this section, the researcher proposes some idea to resolve the issue related to malware. Numerous studies have addressed the significant issues of malware and the challenges it poses. Nevertheless, in spite of the many reports and studies conducted, the amount of malware continues to increase (Alazab et al., 2012) and improvement to counter malware attack and the response appears to be getting less attention (Houmansadr et al., 2011). Several existing issues regarding malware detection and Intrusion Response System have not been fully discussed and the challenges of malware continue to emerge particularly those from manifested in mobile devices through free online applications.

5.1. Accuracy

The IDS operation represents one of the biggest challenges, especially on the part of false alarm where it is perceived to be a part of a large amount of false positive and false negative. This incidentally generates inaccuracies in reports. False alarm is described as triggering an alarm in false positive and false negative. The false positive describes a situation in which the IDS triggers an alarm when there is malicious activity or attack. In contrast, the false negative defines an IDS as being unable to detect correct instances under certain circumstances. Soft computing, Artificial Intelligent, and fuzzy logic techniques are applied to minimize false alarms while keeping the high detection of accuracy. The effectiveness of these detection techniques is measured by the detection rate and false alarm rate (Su, 2011). However, (Tchakounte, 2014) it was pointed out that artificial intelligent techniques such as machine learning-based detection have been known to present a high false alarm rate. Besides that, anomaly based detection and signature based detection able to generate many false alarms (Deshotels et al., 2014; Su, 2011). Eventually, false alarm serves as a big challenge in malware detection because it is almost impossible to remove false alarms to mention, reducing it.

5.2. Features

In order to detect and analyze malware, a significant feature plays an important role in the classification between normal and malicious activities. This feature alleviates false alarms (Seo et al., 2014). However, it is very difficult to achieve the ability to determine the features of what needs to be learned in the training phase in machine learning. Sometimes, it very difficult to decide on the number of features for the classification task (Shabtai et al., 2012). In order to select the best feature, the filter approach is applied to preserve high-level accuracy detection (Shabtai et al., 2012) and to see how specific these features are (Elish et al., 2015). Feature selection must be significant to the detection methods which encompass static, dynamic and application metadata. In addition, to ensure that most of the features are relevant, a rank used for classification purposes before the training phase so as to increase accuracy (McWilliams et al., 2014). In this manner, researchers able to achieve better results with low false alarms.

5.3. Dataset

Recently, there has been an increase in Android malware attacking users. The Android malware has been applied with metamorphism and modification in order to avoid detection by users (Lee et al., 2015). In 2013, it was found that more than 100 000 malware modifications belong to 777 families (Alzahrani et al., 2014). The limited dataset and the lack of understanding of malicious activities for a mobile device, however, restricts the detection mechanism from operating more efficiently. Although static and dynamic analysis offer better accuracy and low false positive, both of them generally focus on proving whether an application is normal or malicious. Besides that, both require a clear understanding of malware families, unique features, and the diversity of the sample and the existence of a modification in the malicious application. Because of the aforementioned change occurring in the malicious application, researchers need a new type of malware with unique activities. As an example, researchers able to discover a new variety of malicious applications and then reconcile to improve the detection mechanism.

5.4. Risk assessment

Risk assessment is a core process that defines the probability of certain risk levels occurring. Conducting risk assessment is quite challenging due to the lack of risk decision making and risk assessment processes. In addition, risk assessment process involves the likelihood of the threat, vulnerabilities and consequences that might result from the impact of the attack. Therefore, risk assessment is subjective and highly challenging in defining the likelihood and impact values, especially in qualitative methods (Lo and Chen, 2012). Although human interpretation is subjective, it still needs some standard evaluation to ensure the validity of results, particularly during data collection. The stage involved in identifying risk during data collection needs to address more caution in order to avoid missing any procedures and to apply correct sequences.

Besides that, the risk that was identified from threat and vulnerabilities must be prioritized based on the criticality of the issue at large (Anuar et al., 2013). In this regard, the role of qualitative assessment is needed so as to improve the quality of data for estimating the likelihood of risk impact (Lo and Chen, 2012). In this context, bias happens during weighting of the risk impact. Enabling the risk impact of assessment is extremely difficult for researchers who need to identify and evaluate based on their goals. It is also hard to evaluate the effectiveness of the approaches used (Shameli-Sendi et al., 2014).

6. Conclusion

Computer and mobile devices are vulnerable to various security threats such as malware. According to Verizon (Verizon, 2015), Symantec (Symantec, 2014), and PandaLabs (Lopez, 2015), it was reported that malware has grown exponentially in recent years and this includes rootkit, botnet, worm, spyware and Trojan horse (Rieck et al., 2008). Specifically, the user is infected by this malware during connection to the Internet. In order to overcome such malware problems and to apply security, it is proposed that a new approach to detect, prevent and response to malware is necessary.

In this paper, the bibliometric method was used to analyze malware research trends from 2005 until 2015. In this study, we presented seven (7) criteria including impact journals, highly-cited articles, research areas, productivity, keywords frequency, institutions across and authors. These criteria helped to uncover the global trends and frontiers related to malware publications. In the past 10 years, it was noted that the number of publications related to malware had increased with an average annual growth rate of 34.1%. The analysis also indicated that the trend of malware publications experienced a rapid growth with increased article publications and citations. From this, it was noted that to ensure the quality of research articles and to increase citations, it is essential to publish articles in high-ranking journals (Ale Ebrahim et al., 2013).

In this paper, we compiled and analyzed the articles published between 2005 and 2015. First, these were identified according to continents. Here, it was noted that North America is the major spatial cluster with the most production of publications in academic research. This is followed by the continent of Asia and Europe. Even though Asia was in the second place in terms of publication, after North America, competition is expected to increase from Asia. This is because more than two (2) countries of the Asian continent appear to be productive in publications and they include China and India. It appears that other countries like Taiwan, Japan, South Korea, Singapore and Malaysia are expected to participate. Data shown earlier had indicated that China, Japan, and South Korea also represent some of the countries where the top 20 institutions are located in the Asian continent.

This study also highlighted the active authors in terms of publications according to continents and of the top 20 most active authors, it was found that Bringas Pablo Garcia A from Spain contributed the most publications after Krugel Christopler from the United States.

A map analysis of keyword frequencies had also been used to describe the trends and research directions for future study in malware related research. In the past 10 years, several keywords and titles such as “malware detection”, “algorithm“, “attack”, “malware analysis”, “security” served as important words in research related to malware.

Acknowledgments

This work was supported by the Ministry of Science, Technology and Innovation, under Grant eScienceFund 01-01-03-SF0914.

References

Aafer, Y., Du, W., Yin, H., 2013. DroidAPIMiner: mining API-level features for robust malware detection in android. Secur. Priv. Commun. Netw. 127, 86–103. http://dx.doi.org/10.1007/978-3-319-04283-1_6.

Abrizah, A., Zainab, A.N., Kiran, K., Raj, R.G., 2013. LIS journals scientific impact and subject categorization: a comparison between web of science and scopus. Scientometrics 94, 721–740. http://dx.doi.org/10.1007/s11192-012-0813-7.

Alazab, M., Monsamy, V., Batten, L., Lantz, P., Tian, R., 2012. Analysis of malicious and benign android applications. In: Proceedings of 2012 32nd International Conference on Distributed Computing Systems Workshops. pp. 608–616. 〈http://dx.doi.org/10.1109/ICDCSW.2012.13〉.

Alazab, M., Venkataraman, S., Watters, P., 2010. Towards Understanding Malware Behaviour by the Extraction of API Calls. In: Proceedings 2010 Second Cybercrime and Trustworthy Computing Workshop. pp. 52–59. 〈http://dx.doi.org/10.1109/CTC.2010.8〉.

Ale Ebrahim, N., Salehi, H., Amin Embi, M., Habibi Tanha, F., Gholizadeh, H., Motahar, S.M., Ordi, A., 2013. Effective strategies for increasing citation frequency. Int. Educ. Stud. 6, 93–99. http://dx.doi.org/10.5539/ies.v6n11p93.

Alzahrani, A.J., Stakhanova, N., Gonzalez, H., Ali, A., 2014. Characterizing evaluation practices of intrusion detection methods for smartphones. J. Cyber Secur. 3, 89–132.

Anuar, N.B., Papadaki, M., Furnell, S., Clarke, N., 2013. Incident prioritisation using analytic hierarchy process (AHP): Risk Index Model (RIM). Security and Communication Networks 6 (9), 1087–1116.

Apvrille, A., Strazzere, T., 2012. Reducing the window of opportunity for Android malware Gotta catch'em all. J. Comput. Virol. 8, 61–71. http://dx.doi.org/10.1007/s11416-012-0162-3.

Arp, D., Spreitzenbarth, M., Malte, H., Gascon, H., Rieck, K., 2014. Drebin: effective and explainable detection of android malware in your pocket. In: Symposium on Network and Distributed System Security (NDSS). pp. 1–15.

Arshad, S., Ahmed, M., Shah, M.A., Khan, A., 2016. Android malware detection & protection: a survey. Int. J. Adv. Comput. Sci. Appl. 7, 463–475. http://dx.doi.org/10.14569/IJACSA.2016.070262.

Bailey, M., Oberheide, J., Andersen, J., Mao, Z.M., Jahanian, F., Nazario, J., 2007. Autom. Classif. Anal. Internet Malware, 178–197.

Bringas Pablo Garcia, 2016. Linkedin [WWW Document]. URL ⟨https://www.linkedin.com/in/pablogarciabringas⟩.

Buela-Casal, G., Gutiérrez-Martínez, O., Bermúdez-Sánchez, M.P., Vadillo-Muñoz, O., 2007. Comparative study of international academic rankings of universities. Scientometrics 71, 349–365. http://dx.doi.org/10.1007/s11192-007-1653-8.

Butun, I., Morgera, S.D., Sankar, R., 2014. A survey of intrusion detection systems in wireless sensor networks. IEEE Sens. J. 14, 1370–1379. http://dx.doi.org/10.1109/ITW.1998.706478.

Canfora, G., De Lorenzo, A., Medvet, E., Mercaldo, F., Visaggio, C.A., 2015. Effectiveness of opcode ngrams for detection of multi family android malware. In: Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015 333–340. ⟨http://dx.doi.org/10.1109/ARES.2015.57⟩.

Cen, L., Gates, C., Si, L., Li, N., 2015. A probabilistic discriminative model for android malware detection with decompiled source code. IEEE Trans. Dependable Secur. Comput. 12, 1–13. http://dx.doi.org/10.1109/TDSC.2014.2355839.

Chadegani, A.A., Salehi, H., Yunus, M.M., Farhadi, H., Fooladi, M., Farhadi, M., Ebrahim, N.A., 2013. A comparison between two main academic literature collections: web of science and scopus databases. Asian Soc. Sci. 9, 18–26. http://dx.doi.org/10.5539/ass.v9n5p18.

Chen, P.S., Lin, S.-C., Sun, C.-H., 2015. Simple and effective method for detecting abnormal internet behaviors of mobile devices. Inf. Sci. 321, 193–204. http://dx.doi.org/10.1016/j.ins.2015.04.035.

Choi, J., Sung, W., Choi, C., Kim, P., 2015. Personal information leakage detection method using the inference-based access control model on the Android platform. Pervasive Mob. Comput. http://dx.doi.org/10.1016/j.pmcj.2015.06.005.

Christopler, K., 2016. Lastline Advance Malware Protection [WWW Document]. URL ⟨https://www.lastline.com/company⟩.

Chuang, H.-Y., Wang, S.-D., 2015. Machine learning based hybrid behavior models for android malware analysis. In: Proceedings of 2015 IEEE International Conference on Software Quality, Reliability and Security. pp. 201–206. ⟨http://dx.doi.org/10.1109/QRS.2015.37⟩.

Clemens, J., 2015. Automatic classification of object code using machine learning. Digit. Investig. 14, S156–S162. http://dx.doi.org/10.1016/j.diin.2015.05.007.

Corona, I., Giacinto, G., Roli, F., 2013. Adversarial attacks against intrusion detection systems: taxonomy, solutions and open issues. Inf. Sci. 239, 201–225. http://dx.doi.org/10.1016/j.ins.2013.03.022.

Cui, B., Jin, H., Carullo, G., Liu, Z., 2015. Service-oriented mobile malware detection system based on mining strategies. Pervasive Mob. Comput. 24, 101–116. http://dx.doi.org/10.1016/j.pmcj.2015.06.006.

Damopoulos, D., Kambourakis, G., Gritzalis, S., Park, S.O., 2012. Exposing mobile malware from the inside (or what is your mobile app really doing?). Peer-to-Peer Netw. Appl. 7, 687–697. http://dx.doi.org/10.1007/s12083-012-0179-x.

Dehdarirad, T., Villarroya, A., Barrios, M., 2015. Research on women in science and higher education: a bibliometric analysis. Scientometrics 103, 795–812. http://dx.doi.org/10.1007/s11192-015-1574-x.

Deshotels, L., Notani, V., Lakhotia, A., 2014. DroidLegacy: automated familial classification of android malware. In: Proceedings of ACM SIGPLAN on Program Protection and Reverse Engineering Workshop 2014. 3.

Dini, G., Martinelli, F., Saracino, A., Sgandurra, D., 2012. MADAM: a multi-level anomaly detector for android malware. Comput. Netw. Secur., 240–253. http://dx.doi.org/10.1007/978-3-642-33704-8-21.

Egele, M., Scholte, T., Kirda, E., Kruegel, C., 2012. A survey on automated dynamic malware-analysis. ACM Comput. Surv. (CSUR) 44, 1–42. http://dx.doi.org/10.1145/2089125.2089126.

Elish, K.O., Shu, X., Yao, D., (Daphne), Ryder, B.G., Jiang, X., 2015. Profiling user-trigger dependence for android malware detection. Comput. Secur. 49, 255–273. http://dx.doi.org/10.1016/j.cose.2014.11.001.

Elshoush, H.T., Osman, I.M., 2011. Alert correlation in collaborative intelligent intrusion detection systems - a survey. Appl. Soft Comput. J. 11, 4349–4365. http://dx.doi.org/10.1016/j.asoc.2010.12.004.

Fahimnia, B., Sarkis, J., Davarzani, H., 2015. Green supply chain management: a review and bibliometric analysis. Int. J. Prod. Econ. 162, 101–114. http://dx.doi.org/10.1016/j.ijpe.2015.01.003.

Faruki, P., Laxmi, V., Bharmal, A., Gaur, M.S., Ganmoor, V., 2014. AndroSimilar: robust signature for detecting variants of Android malware. J. Inf. Secur. Appl. 22, 66–80. http://dx.doi.org/10.1016/j.jisa.2014.10.011.

Feizollah, A., Anuar, N.B., Salleh, R., Amalina, F., Ma'arof, R.R., Shamshirband, S., 2013a. A study of machine learning classifiers for anomaly-based mobile botnet detection. Malays. J. Comput. Sci. 26, 251–265.

Feizollah, A., Anuar, N.B., Salleh, R., Wahid, A., Wahab, A., 2015. A review on feature selection in mobile malware detection. Digit. Investig. 3, 22–37.

Feizollah, A., Shamshirband, S., Anuar, N.B., Salleh, R., Kiah, M.L.M., 2013b. Anomaly detection using cooperative fuzzy logic controller. Intell. Robot. Syst.: Inspiring, 220–231.

Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D., 2011. A survey of mobile malware in the wild. In: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM'11. 3. ⟨http://dx.doi.org/10.1145/2046614.2046618⟩.

Gandotra, E., Bansal, D., Sofat, S., 2014. Malware analysis and classification: a survey. J. Inf. Secur. 5, 56–64. http://dx.doi.org/10.1007/978-94-007-5860-5.

Gartner, 2015. Gartner Says Tablet Sales Continue to Be Slow in 2015 [WWW Document]. URL ⟨http://www.gartner.com/newsroom/id/2954317⟩, (accessed 6.15.15).

Gheorghe, L., Marin, B., Gibson, G., Mogosanu, L., Deaconescu, R., Voiculescu, V.-G., Carabas, M., 2015. Smart malware detection on android. Secur. Commun. Netw. 8, 4254–4272. http://dx.doi.org/10.1002/sec.

Ghiasi, M., Sami, A., Salehi, Z., 2015. Dynamic VSA: a framework for malware detection based on register contents. Eng. Appl. Artif. Intell. 44, 111–122. http://dx.doi.org/10.1016/j.engappai.2015.05.008.

Gonzalez, H., Stakhanova, N., Ghorbani, A.A., 2014. DroidKin: lightweight detection of android apps similarity. In: Proceedings of the 10th SECURECOMM.

Grace, M.C., Zhou, W., Jiang, X., Sadeghi, A.-R., 2012. Unsafe exposure analysis of mobile in-app advertisements. In: Proceedings of the 5th ACM conference on Security and Privacy in Wireless and Mobile Networks. 67. pp. 101–112. ⟨http://dx.doi.org/10.1145/2185448.2185464⟩.

Grecio, A., Bonacin, R., Nabuco, O., Afonso, V.M., Geus, P.L. De, Jino, M., 2014. Ontology for malware behavior: a core model proposal. In: Proceedings of 2014 IEEE 23rd International WETICE Conference. pp. 453–458. ⟨http://dx.doi.org/10.1109/WETICE.2014.72⟩.

Grégio, A.R. a, Fernandes Filho, D.S., Afonso, V.M., Santos, R.D.C., Jino, M., de Geus, P. L., 2011. Behavioral analysis of malicious code through network traffic and system call monitoring. In SPIE Defense, Security, and Sensing. Int. Soc. Opt. Photonics, 1–10. http://dx.doi.org/10.1117/12.883457.

Haq, N.F., 2015. Application of machine learning approaches in intrusion detection system: a survey. Int. J. Adv. Res. Artif. Intell. 4, 9–18.

Houmansadr, A., Zonouz, S.A., Berthier, R., 2011. A cloud-based intrusion detection and response system for mobile phones. In: Proceedings of 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W). pp. 31–32. ⟨http://dx.doi.org/10.1109/DSNW.2011.5958860⟩.

Hubballi, N., Suryanarayanan, V., 2014. False alarm minimization techniques in signature-based intrusion detection systems: a survey. Comput. Commun. 49, 1–17. http://dx.doi.org/10.1016/j.comcom.2014.04.012.

Hutchison, D., Mitchell, J.C., 2016. Lecture Notes in Computer Science [WWW Document]. Springer. URL ⟨http://www.springer.com/series/558⟩, (accessed 12.30.15).

Inayat, Z., Gani, A., Anuar, N.B., Khan, M.K., Anwar, S., 2015. Intrusion response systems: foundations, design, and challenges. J. Netw. Comput. Appl. http://dx.doi.org/10.1016/j.jnca.2015.12.006.

Jahkne, A., 2016. Who picks up the tab for science? For half a century, the government funded research. Times are changing. [WWW Document]. URL ⟨http://www.bu.edu/research/articles/funding-for-scientific-research/⟩, (accessed 1.1.16).

Karim, A., Salleh, R. Bin, Shiraz, M., Shah, S.A.A., Awan, I., Anuar, N.B., 2014. Botnet detection techniques: review, future trends, and issues. J. Zhejiang Univ. Sci. C 15, 943–983. http://dx.doi.org/10.1631/jzus.C1300242.

Kim, D.W., Yan, P., Zhang, J., 2015. Detecting fake anti-virus software distribution webpages. Comput. Secur. 49, 95–106. http://dx.doi.org/10.1016/j.cose.2014.11.008.

Koskinen, J., Isohanni, M., Paajala, H., Jääskeläinen, E., Nieminen, P., Koponen, H., Tienari, P., Miettunen, J., 2008. How to use bibliometric methods in evaluation of scientific research? An example from Finnish schizophrenia research. Nord. J. Psychiatry 62, 136–143. http://dx.doi.org/10.1080/08039480801961667.

Kruegel, C., 2016. Christopher Kruegel [WWW Document]. Bibliography. URL ⟨http://www.cs.ucsb.edu/~chris/⟩, (accessed 1.1.16).

Lar, S.-U., 2011. Proactive security mechanism and design for firewall. J. Inf. Secur. 2, 122–131. http://dx.doi.org/10.4236/jis.2011.23012.

Larkin, M.A., Blackshields, G., Brown, N.P., Chenna, R., Mcgettigan, P.A., McWilliam, H., Valentin, F., Wallace, I.M., Wilm, A., Lopez, R., Thompson, J.D., Gibson, T.J., Higgins, D.G., 2007. Clustal W and clustal X version 2.0. Bioinformatics 23, 2947–2948. http://dx.doi.org/10.1093/bioinformatics/btm404.

Lee, S., Lee, J., Lee, H., 2015. Screening smartphone applications using malware family signature. Comput. Secur., 1–31. http://dx.doi.org/10.1016/j.cose.2015.02.003.

Liao, H.-J., Richard Lin, C.-H., Lin, Y.-C., Tung, K.-Y., 2012. Intrusion detection system: a comprehensive review. J. Netw. Comput. Appl. 36, 16–24. http://dx.doi.org/10.1016/j.jnca.2012.09.004.

Lin, C.-T., Wang, N.-J., Xiao, H., Eckert, C., 2015. Feature selection and extraction for malware classification. J. Inf. Sci. Eng. 31, 965–992.

Lo, C.C., Chen, W.J., 2012. A hybrid information security risk assessment procedure considering interdependences between controls. Expert Syst. Appl. 39, 247–257. http://dx.doi.org/10.1016/j.eswa.2011.07.015.

Loomes, D.E., van Zanten, S.V., 2013. Bibliometrics of the top 100 clinical articles in digestive disease. Gastroenterology 144, 673–676. http://dx.doi.org/10.1053/j.gastro.2013.02.013.

Lopez, M., 2015. PandaLabs [WWW Document]. URL ⟨http://www.pandasecurity.com/mediacenter/press-releases/pandalabs-neutralized-75-million-new-malware-samples-2014-twice-many-2013/⟩, (accessed 11.25.15).

Lopez-Illescas, C., Moya-Anegon, F. de, Moed, H.F., 2008. Coverage and citation impact of oncological journals in the Web of Science and Scopus. J. Informetr. 2, 304–316. http://dx.doi.org/10.1016/j.joi.2008.08.001.

M, S., G, P., 2012. Mobile device security: a survey on mobile device threats, vulnerabilities and their defensive mechanism. Int. J. Comput. Appl. 56, 24–29. http://dx.doi.org/10.5120/8960-3163.

Mao, G., Zou, H., Chen, G., Du, H., Zuo, J., 2015. Past, current and future of biomass energy research: a bibliometric analysis. Renew. Sustain. Energy Rev. 52, 1823–1833. http://dx.doi.org/10.1016/j.rser.2015.07.141.

McKerlich, R., Ives, C., McGreal, R., 2013a. Comparing bibliometric statistics obtained from the web of sciences and scopus. Int. Rev. Res. Open Distance Learn. 14, 90–103. http://dx.doi.org/10.1002/asi.

McKerlich, R., Ives, C., McGreal, R., 2013b. Comparing keywords plus of WOS and author keywords: a case study of patient adherence research. Int. Rev. Res. Open Distance Learn. 14, 90–103. http://dx.doi.org/10.1002/asi.

McWilliams, G., Sezer, S., Yerima, S.Y., 2014. Analysis of Bayesian classification-based approaches for Android malware detection. IET Inf. Secur. 8, 25–36. http://dx.doi.org/10.1049/iet-ifs.2013.0095.

Mingers, J., Leydesdorff, L., 2015. A review of theory and practice in scientometrics. Eur. J. Oper. Res. 246, 1–19. http://dx.doi.org/10.1016/j.ejor.2015.04.002.

Mongeon, P., Paul-Hus, A., 2016. The journal coverage of web of science and scopus: a comparative analysis. Scientometrics 106, 213–228. http://dx.doi.org/10.1007/s11192-015-1765-5.

Moser, A., Kruegel, C., Kirda, E., 2007. Limits of static analysis for malware detection. In: Proceedings of Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007). pp. 421-430. 〈http://dx.doi.org/10.1109/ACSAC.2007.21〉.

Muniyandi, A.P., Rajeswari, R., Rajaram, R., 2012. Network anomaly detection by cascading K-means clustering and C4.5 decision tree algorithm. Procedia Eng. 30, 174–182. http://dx.doi.org/10.1016/j.proeng.2012.01.849.

Muthumanickam, M., Ilavarasan E, E., 2015. CoPDA: concealed process and service discovery algorithm to reveal rootkit footprints. Malays. J. Comput. Sci. 28, 1–15.

Nadeem, A., Howarth, M.P., 2014. An intrusion detection & adaptive response mechanism for MANETs. Ad Hoc Netw. 13, 368–380. http://dx.doi.org/10.1016/j.adhoc.2013.08.017.

Narudin, F.A., Feizollah, A., Anuar, N.B., Gani, A., 2014. Evaluation of machine learning classifiers for mobile malware detection. Soft Comput., 1–15. http://dx.doi.org/10.1007/s00500-014-1511-6.

Noorden, R. Van, Maher, B., Nuzzo, R., 2014. The top 100 papers [WWW Document]. URL 〈http://www.nature.com/news/the-top-100-papers-1.16224〉, (accessed 1.1.16).

Olijnyk, N.V., 2015. A quantitative examination of the intellectual profile and evolution of information security from 1965 to 2015. Scientometrics . http://dx.doi.org/10.1007/s11192-015-1708-1.

Oxford, 2015. Bioinformatics [WWW Document]. URL 〈http://bioinformatics.oxfordjournals.org/〉, (accessed 12.30.15).

Patel, R., Thakkar, A., Ganatra, A., 2012. A survey and comparative analysis of data mining techniques for network intrusion detection systems. Int. J. Soft Comput. 2, 265–271.

Platforms, N., Threats, C., 2013. Security Threat Report 2013, SOPHOS.

Qiao, Y., Yang, Y., Ji, L., He, J., 2013. Analyzing malware by abstracting the frequent itemsets in API call sequences. In: Proceedings of 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. pp. 265–270. 〈http://dx.doi.org/10.1109/TrustCom.2013.36〉.

Qiu, J., 2016. China Goes Back to Basics on Research Funding [WWW Document]. URL 〈http://www.nature.com/news/china-goes-back-to-basics-on-research-funding-1.14853〉, (accessed 1.1.16).

Rad, B.B., Masrom, M., Ibrahim, S., 2012. Camouflage in malware: from encryption to metamorphism. Int. J. Comput. Sci. Netw. Secur. 12, 74–83.

Ravula, R.R., Liszka, K.J., Chan, C., 2013. Learning attack features from static and dynamic analysis of malware. Knowl. Discov. Knowl. Eng. Knowl. Manag., 109–125.

Rieck, K., Holz, T., Willems, C., Patrick, D., Laskov, P., 2008. Learning and classification of malware behavior. Detection of Intrusions and Malware, and Vulnerability Assessment. pp. 108–125.

Sahs, J., Khan, L., 2012. A machine learning approach to android malware detection. In: Proceedings of 2012 European Intelligence and Security Informatics Conference 141–147. 〈http://dx.doi.org/:10.1109/EISIC.2012.34〉.

Santos, I., Brezo, F., Ugarte-Pedrero, X., Bringas, P.G., 2013. Opcode sequences as representation of executables for data-mining-based unknown malware detection. Inf. Sci. 231, 64–82. http://dx.doi.org/10.1016/j.ins.2011.08.020.

Sanz, B., Santos, I., Nieves, J., Laorden, C., 2013. MADS: malicious android applications detection through string analysis. Netw. Syst. Secur., 178–191.

Schmeelk, S., Yang, J., Aho, A., 2015. Android malware static analysis techniques. In: Proceedings of the 10th Annual Cyber and Information Security Research Conference.

Schmidt, M., Baumg, L., Graubner, P., David, B., Freisleben, B., 2011. Malware detection and kernel rootkit prevention in cloud computing environments. In: Parallel, Distributed and Network-Based Processing (PDP), 2011 19th Euromicro International Conference on IEEE. pp. 603–610. 〈http://dx.doi.org/10.1109/PDP.2011.45〉.

Seideman, J.D., Khan, B., Vargas, C., 2015. Quantifying malware evolution through archaeology. J. Inf. Secur. 6, 101–110.

Seo, S.-H., Gupta, A., Mohamed Sallam, A., Bertino, E., Yim, K., 2014. Detecting mobile malware threats to homeland security through static analysis. J. Netw. Comput. Appl. 38, 43–53. http://dx.doi.org/10.1016/j.jnca.2013.05.008.

Shabtai, A., Elovici, Y., 2010. Applying behavioral detection on android-based devices. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering 48 LNICST. pp. 235–249. 〈http://dx.doi.org/10.1007/978-3-642-17758-3_17〉.

Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C., Weiss, Y., 2012. "Andromaly": a behavioral malware detection framework for android devices. J. Intell. Inf. Syst. 38, 161–190. http://dx.doi.org/10.1007/s10844-010-0148-x.

Shabtai, A., Mimran, D., Rokach, L., Shapira, B., Elovici, Y., 2014. Mobile malware detection through analysis of deviations in application network behavior. Comput. Secur. 43, 1–18. http://dx.doi.org/10.1016/j.cose.2014.02.009.

Shameli-Sendi, A., Cheriet, M., Hamou-Lhadj, A., 2014. Taxonomy of intrusion risk assessment and response system. Comput. Secur. 45, 1–16. http://dx.doi.org/10.1016/j.cose.2014.04.009.

Sharif, M., Lanzi, A., Giffin, J., Lee, W., 2008. Impeding Malware Analysis Using Conditional Code Obfuscation. Informatica, United States.

Sheen, S., Anitha, R., Natarajan, V., 2015. Android based malware detection using a multifeature collaborative decision fusion approach. Neurocomputing 151, 905–912. http://dx.doi.org/10.1016/j.neucom.2014.10.004.

Su, M.Y., 2011. Using clustering to improve the KNN-based classifiers for online anomaly network traffic identification. J. Netw. Comput. Appl. 34, 722–730. http://dx.doi.org/10.1016/j.jnca.2010.10.009.

Suleiman Y. Yerima, S.S., Muttik, I., 2015. High accuracy android malware detection using ensemble learning. IET Inf. Secur., 1–10. http://dx.doi.org/10.1049/iet-ifs.2014.0099.

Sun, J., Wang, M.-H., Ho, Y.-S., 2012. A historical review and bibliometric analysis of research on estuary pollution. Mar. Pollut. Bull. 64, 13–21. http://dx.doi.org/10.1016/j.marpolbul.2011.10.034.

Symantec, 2015. 2015 Internet Security Threat Report, Internet Security Threat Report.

Symantec, 2014. Symantec Internet Security Threat Report.

Talha, K.A., Alper, D.I., Aydin, C., 2015. APK auditor: permission-based Android malware detection system. Digit. Investig. 13, 1–14. http://dx.doi.org/10.1016/j.diin.2015.01.001.

Tang, A., Sethumadhavan, S., Stolfo, S., 2014. Unsupervised anomaly-based malware detection using hardware features. Res. Attacks Intrusions Def., 109–129.

Tchakounte, F., 2014. Permission-based malware detection mechanisms on android: analysis and perspectives. J. Comput. Sci. Softw. Appl. 1, 63–77.

Thomas, K., Grier, C., Ma, J., Paxson, V., Song, D., 2011. Design and evaluation of a real-time URL spam filtering service. In: Proceedings of 2011 IEEE Symposium on Security and Privacy. pp. 447–462. 〈http://dx.doi.org/doi:10.1109/SP.2011.25〉.

Veerwal, D., Menaria, P., 2013. Ensemble of soft computing techniques for malware detection. Int. J. Emerg. Technol. Comput. Appl. Sci. 6, 159–167.

Verizon, 2015. 2015 Data Breach Investigations Report. Information Security. pp. 1–70.

Wang, P., Wang, Y.-S., 2014. Malware behavioural detection and vaccine development by using a support vector model classifier. J. Comput. Syst. Sci. 1, 1–15. http://dx.doi.org/10.1016/j.jcss.2014.12.014.

Wang, X., Yang, Y., Zeng, Y., Tang, C., Shi, J., Xu, K., 2015. A novel hybrid mobile malware detection system integrating anomaly detection with misuse detection. In: Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services. pp. 15–22. 〈http://dx.doi.org/10.1145/2802130.2802132〉.

Weiss, Y., Fledel, Y., Elovici, Y., Rokach, L., 2012. Cost-sensitive detection of malicious applications in mobile devices. Mob. Comput. Appl. Serv., 382–395.

Willems, C., Holz, T., Freiling, F., 2007. Toward automated dynamic malware analysis using CWSandbox. IEEE Secur. Priv. 2, 32–39.

Wilson, V., 2016. Evidence based library and information practice. Evid. Based Libr. Inf. Pract. 11, 50–52.

Wu, D.-J., Mao, C.-H., Wei, T.-E., Lee, H.-M., Wu, K.-P., 2012. DroidMat: android malware detection through manifest and API calls tracing. In: Proceedings of 2012 Seventh Asia Joint Conference on Information Security. pp. 62–69. 〈http://dx.doi.org/doi:10.1109/AsiaJCIS.2012.18〉.

Wu, F., Narang, H., Clarke, D., 2014. An overview of mobile malware and solutions. J. Comput. Commun. 2, 8–17. http://dx.doi.org/10.4236/jcc.2014.212002.

Wu, X., Chen, X., Zhan, F.B., Hong, S., 2015. Global research trends in landslides during 1991 – 2014: a bibliometric analysis. Landslides 12, 1215–1226. http://dx.doi.org/10.1007/s10346-015-0624-z.

Xie, P., Lu, X., Wang, Y., Su, J., Li, M., 2013. An automatic approach to detect anti-debugging in Malware analysis. Trust. Comput. Serv., 436–442.

Yassin, W., Udzir, N.I., Muda, Z., Abdullah, A., Abdullah, M.T., 2012. A cloud-based intrusion detection service framework. In: Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). pp. 213–218. 〈http://dx.doi.org/10.1109/CyberSec.2012.6246098〉.

Yerima, S.Y., Sezer, S., McWilliams, G., Muttik, I., 2013. A new android malware detection approach using bayesian classification. In: Proceedings of 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA) 121–128. 〈http://dx.doi.org/10.1109/AINA.2013.88〉.

Zainab, A.N., Anuar, N.B., 2009. A single journal study: Malaysian journal of computer sciences. Malays. J. Comput. Sci. 22, 1–18.

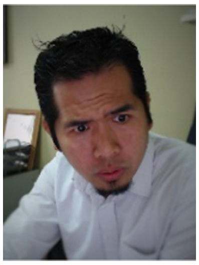
Zhang, Y., Lee, W., Huang, Y.-A., 2003. Intrusion detection techniques for mobile wireless networks. Wirel. Netw., 545–556. http://dx.doi.org/10.1023/A:1024600519144.

Zhao, D., Traore, I., Sayed, B., Lu, W., Saad, S., Ghorbani, A., Garant, D., 2013. Botnet detection based on traffic behavior analysis and flow intervals. Comput. Secur. 39, 2–16. http://dx.doi.org/10.1016/j.cose.2013.04.007.

Zhao, M., Zhang, T., Ge, F., Yuan, Z., 2012. RobotDroid: a lightweight malware detection framework on smartphones. J. Netw. 7, 715–722. http://dx.doi.org/10.4304/jnw.7.4.715-722.

Zhou, Y., Jiang, X., 2012. Dissecting android malware: characterization and evolution. In: Proceedings of 2012 IEEE Symposium on Security and Privacy. pp. 95–109. 〈http://dx.doi.org/10.1109/SP.2012.16〉.

Mohd Faizal Ab Razak has distinctively received his Masters of Computer Science (Networking) from University Malaysia Pahang, Malaysia. He is currently pursuing his Ph.D. from University of Malaya, Malaysia. His area of research includes Mobile Computing, and Mobile Security.



Nor Badrul Anuar obtained his Master of Computer Science from University of Malaya in 2003 and a Ph.D. at the Center for Information Security & Network Research, University of Plymouth, UK. He is a senior lecturer at the Faculty of Computer Science and Information Technology at University of Malaya, Kuala Lumpur. He has published a number of journal papers related to security areas locally and internationally. He has a good profile of publications in renowned Journals. His research interests include Intrusion Detection System (Intrusion Detection Systems, Intrusion Response Systems, Security Event and Management, Digital Forensic and Network Security), High Speed Network (Switching, Routing, IPV6, and Multicast) and Management Information System (E-thesis, Library Systems and Online Systems). He is also a member of IEEE Communications Society, IEEE Young Professionals and IEEE Computer Society.

Rosli Bin Salleh is an Associate Professor and Deputy Dean of Research in Faculty of Computer Science and Information Technology, University of Malaya, Malaysia. He has obtained his bachelor degree from University of Malaya, Malaysia and later Masters and Ph.D. degree from Salford University, UK. He has a good profile of publications in renowned Journals and Proceedings. He is actively supervizing students at Master and Ph.D. level. His interests of research include Mobile IPv6, Wireless Handoff and Mobile Security. He is also an associate member of Cisco Systems, Inc. 2008–2016. He has been serving for different administrative duties since 2002 in University of Malaya.

Ahmad Firdaus has distinctively received his Masters of Computer Science (Networking) from University Teknologi Mara, Malaysia. He is currently pursuing his Ph.D. from University of Malaya, Malaysia. His area of research includes Mobile Computing, and Mobile Security.