JOIV : Int. J. Inform. Visualization, 6(2-2): A New Frontier in Informatics - August 2022 489-497

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

The Relevance of Bibliometric Analysis to Discover the Area's Research Efforts: Root Exploit Evolution

Che Akmal Che Yahaya [a], Ahmad Firdaus [a,*], Ferda Ernawan [a], Wan Isni Sofiah Wan Din [a]

[a] *Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang, 26600 Pekan, Pahang, Malaysia*
Corresponding author: [*]firdausza@ump.edu.my

***Abstract*— Malware steals, encrypts, and damages data of the targeted machines for private, money, or fame purposes. The types of malwares are root exploit, cryptojacking, Trojan, worms, viruses, spyware, ransomware, and adware. Among these types, root exploit is one of the most destructive malware types since it disguises and obscures all types of malwares and provides a mechanism for other malware to carry out malicious acts invisibly. To review the progress of root exploitation efforts globally, there is a need to inspect all publications that involve root exploitation. Among all malware reviews previously, to date, there is still no trace of any bibliometric analysis that demonstrates the research impacts of root exploit and trends in bibliometric analysis. Hence, this paper adopts bibliometric analysis specifically on root exploit studies which evaluate: (1) Wordcloud; (2) WordTreeMap; (3) Three fields plot; (4) Thematic evolution; (5) Thematic maps; (6) Correspondence analysis (CA); (7) Dendrogram; and (8) Multiple correspondence analysis (MCA). To conclude, our bibliometric discovers that; 1) Linux and Android become the main interest in root exploit studies. 2) Types of root exploit in the virtualization layer and studies to detect this area are increasing. 3) USA and China have become the leaders in root exploitation research. 4) Research studies are more towards memory forensics to detect root exploit, which is more promising. 5) Instead of researching new methods of root exploit in compromising victims, root exploits researchers were more focused on detecting root exploits.**

***Keywords*— Root exploit; rootkit; bibliometric; security; detection; review.**

Manuscript received 11 Dec. 2021; revised 12 Jan. 2022; accepted 28 Apr. 2022. Date of publication 31 Aug. 2022.

I. INTRODUCTION

Malware is any malicious software designed or written to attack and harm a computer system. Among all the malware categories, root exploit is one of the most dangerous threats as it can conceal and hide all varieties of malware and provide a way for other malware to execute malicious actions stealthily [1]. Root exploit is a type of malware that modifies the operating system's kernel (OS) and subsequently steals sensitive and confidential data without the user's permission. Root exploit attackers have unrestricted administrator rights once the OS kernel has been broken. If these privileges are granted, all harmful executions will be flagged as approved by the antivirus or intrusion detection system. Because the root vulnerability may avoid antivirus and intrusion detection, the attacker can carry out any harmful activity invisibly [2]. Securelist from Kaspersky recently discovered a new rootkit or root exploit known as 'Moriya'. With the famous rootkit's capability to execute malicious actions stealthily, it installs passive backdoors on public-facing servers, establishing a covert command and control (C&C) for botnet communication channels without having been recognized by antivirus [3]. In another recent case, Microsoft officially verified that they authorized a malicious driver distributed in gaming environments. This "Netfilter" driver is a rootkit that has been observed communicating with the command and control (C&C) Internet protocol (IP), without raising any suspicion at all [4].

On the other hand, although the existing surveys provide a profound view of malware efforts, there are unavailable review publications that specifically focus on root exploit. Furthermore, no trace of any bibliometric analysis is seen that demonstrates the research impacts of root exploit and trends in bibliometric analysis. Hence, this paper fills in the gap and reviews the root exploit publications activities using bibliometric analysis.

A quantitative analysis of publications published on a certain topic is known as bibliometrics. The bibliometric method is used to assess published papers' impact and aid researchers in comprehending the research life cycle. It shows the study's focus, increasing the interest and attention of

scholars and funding organizations. The bibliometric method allows for comparing the countries that contributed to the publications based on their respective fields. Bibliometric research has benefited the COVID-19 pandemic [5], environmental, agricultural [6], sustainable development [7], accounting [8], economic [9], linguistic decision making [10], and fuzzy research [11]. The benefits of bibliometric analysis include: (a) the ability for academics to use the publication of relevant studies for future investigations; and (b) the ability for new researchers to increase their expertise. (b) disclose the development of research based on the institution and performance; (c) reveal the importance of research in a related field; (d) reveal the importance of research in a related field; (e) reveal the importance of research in a related field.

The contribution of this bibliometrics analysis are as follows:

- The bibliometric analysis involves root exploit studies that were retrieved from the Scopus database, which includes all categories of papers, including ISI-indexed.
- This study investigates root exploit research globally by evaluating the number of publications, citations, title, authors, affiliation, abstract, and keywords.
- Finally, this study addresses the enthusiasm of root exploit efforts by elucidating the bibliometrics analysis thus far and then utilizing these to forecast possible future reflections.

II. Material and Method

Bibliometrics is a statistical analysis technique to systematically measure the influential factors of research publications, such as their productivity and visibility in a particular scientific field [12]. A search engine is used to explore valid scientific publications, and various scientific pools exist to search and index articles. For examples, Web of Science (WoS), Scopus, Google Scholar, IEEE Explore, Association for Computing Machinery (ACM), and springer. However, three main sources of bibliometric analysis for exploring literature include WoS, Elsevier Scopus, and Google Scholar [13], [14], [15]. In this paper, we used only the Scopus database for the following reasons; a) Scopus provides a simple logical expression function to include or exclude rules into the search query b) WoS only has a few papers related to root exploits c) Scopus has more publications focused on root exploit than WoS d) impact factor articles in Scopus are also indexed WoS [16], [17]. e) Google Scholar has a low quality of data which raises questions about its suitability [18], transparency of the coverage [19], and inconsistencies of data [15] for research evaluation.

In this paper, we have employed various strategies to collect publications that correspond to our analysis (Fig. 1). It describes a set of tools, materials, and methods used to conduct this study. The methodology applies three phases: 1) data collection, 2) data analysis, and 3) data visualization. The first phase is where a set of keywords is selected to explore valid scientific publications. In the interest of searching all root exploit publications, we used the term "root exploit" OR "rootkit" as the main keyword in the search engine. This is because several researchers utilize the rootkit term, while the others used root exploit.

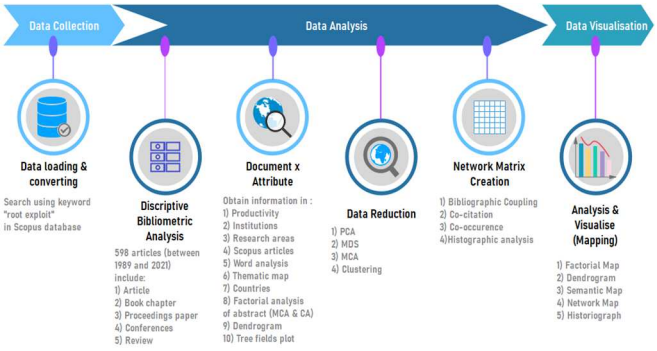

Fig. 1 Flowchart of the methodology

The second phase refines the retrieved publications from the previous phase by implying a more optimized query to trim the collected materials. We have excluded the unrelated databases from [16] by removing non-English languages and excluding databases like KCI-Korean Journal Database, Derwent Innovations Index, and SciELO Citation Index. Therefore, only WoS Core Collection was chosen to retrieve high-quality articles. Besides, some unwanted document types such as editorial material, retracted publications, corrections, and news items were removed from the results.

The findings in the third phase are analyzed based on the following criteria: a) impact journal, b) highly cited article, c) research area, d) productivity, e) keyword frequency, f) institutions, and g) authors. Finally, we have adopted an interactive data visualization software Tableau [20] and the bibliometric package [21] from the open-source statistical software known as R to visualize the result of our analysis.

III. Results and Discussion

A. Productivity

Fig. 1 visualizes a trend that root exploit researchers were most interested in publishing conference papers in the form of proceedings, rather than an accumulation of papers published on websites or in book form. The reason is that the conference papers were submitted before the conference event, so the papers became available to all the participants. This situation allows the readers to understand the idea behind the papers and where possible, to submit their feedback after the presentation of the papers when the conference ends. Based on this, the conference papers' authors can then improve and revise their research ideas based on significant feedback. Therefore, conference publications before the conference are much more useful as it allows the readers to read multiple times and understand the research in detail. Following this, the root exploit authors are able to retrieve the audience's feedback much better during the conference event.

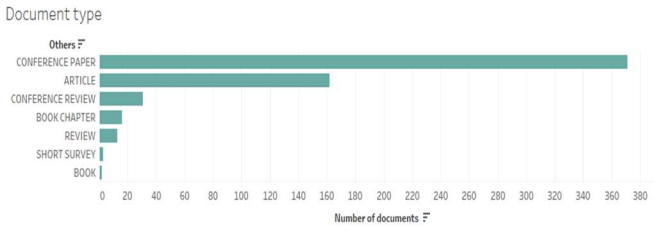

Fig. 1 Document type

B. Institutions

Here, it discusses the number of publications based on institutions or affiliations. It aims to identify which institutions are active in root exploit studies and measure their interest by comparing institutions according to the publications and collaborations.

A comparison of these institutions was made based on publications and collaborations. Table 1 below tabulates the number of articles based on institutions according to the top 10 rankings. The University of Illinois was placed at the top rank, with five articles, followed by the Cylab Carnegie Mellon University and Rutgers University. In this ranking, the universities involved were from the United States of America (USA), and Asia (China, South Korea, and India). The countries of the USA and China served as the two top nations with active universities that contributed the knowledge on root exploit to the world.

TABLE I
AFFILIATION OF ROOT EXPLOIT ARTICLES

Affiliations	Articles
University of Illinois at Urbana champaign united states	5
Cylab CMU Pittsburgh pa united states	4
department of computer science Rutgers university united states	4
Georgia Institute of Technology united states	4
North Carolina State University united states	4
school of computer science and engineering Beihang university Beijing 100191 China	4
university of Chinese academy of sciences Beijing China	4
Beijing Institute of SYSTEM engineering Beijing China	3
Catholic University of Daegu South KOREA	3
Department of Computer Science And Engineering Pondicherry Engineering College Puducherry 605 014 India	3

From the level of collaboration between affiliations, as noted in Fig. 2, it can be noticed that the universities were not well connected in terms of research. When it comes to root exploit research, several of these universities operate as independent organizations, suggesting that very few universities are interested in collaborating with others in root exploit studies. Most of these universities were apparently, more comfortable in conducting root exploit research within their circle. This shows that the possibility of expanding the root exploit research among universities is high if these universities make an effort to collaborate so as to detect more advanced types of root exploits.

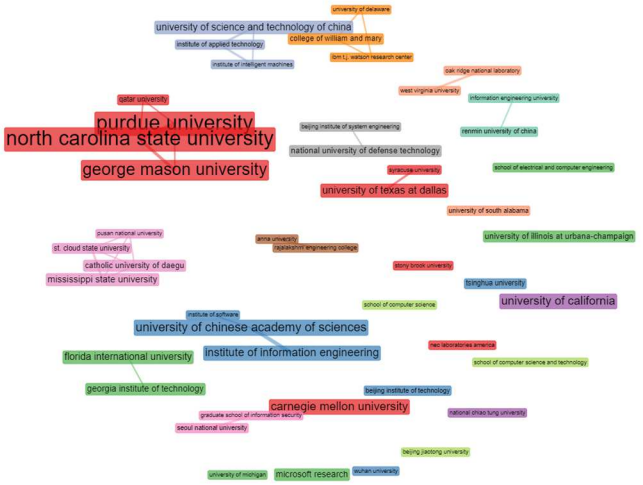

Fig. 2 Collaboration network between institutions

C. Authors

Here, it discusses the number of publications based on authors from continents. The aim is to identify the most active researchers in terms of authorship. The author's publications, dominance ranking factor, and total citations were analyzed to accomplish this. Fig. 3 shows the top 20 rankings. The blue circles indicate the number of publications, the bigger the circle, the more the publications. This figure reveals how many labeled publications were initiated and discontinued by the authors (time of year). As seen in the top five rankings, the highest authorship ranking was led by Jiang X, Xu D, Lin Z, and Wang X, who published from 2004 to 2020. It appears that Jiang X stopped publishing root exploit articles in 2014, while Lin Z (ranking three) and Wang X (ranking four) continuously published articles until 2018.

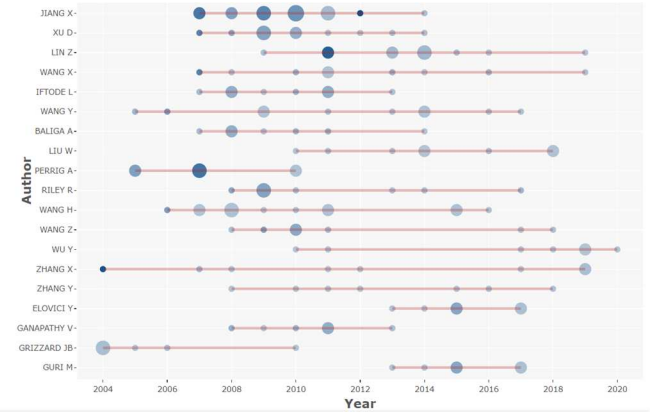

Fig. 3 Authors production over time in the top 20 ranking

A scatter plot demonstrates (Fig. 5) the h and g indexes, respectively. The figure depicts that Jiang X surpassed all other authors in both the h and g-index and outperformed all other authors with a significant margin, as noted in the upper right corner. The scatter plot thus indicates that Jiang X has a significant experience in root exploit studies, with outstanding publications. In contrast, Wang X was placed below the Riley R and Iftode L due to the fewer h-index. This demonstrates that both Riley R and Iftode L had more citations than Wang X even though Wang X had a higher number of publications.

Fig. 4 Scatter plot between h and g index

D. Words Analysis

Here, it discusses the keywords used by researchers in root exploit publications. Word analysis is important because it examines the terms often used, the relationship between keywords in root exploit research and the research trends. It also identifies the research gaps in the malware domain, the research field which interests researchers the most, by combining them within the root exploit research.

Fig. 5 displays a word cloud, with most occurrences being in the biggest font size. The center of the cloud showed that many researchers were attempting to detect root exploits from compromising machines rather than conducting experiments to uncover vulnerabilities by penetrating the OS.

The word analysis began with the 'detection' word, followed by the word 'monitored' (font with blue color in the bottom of the cloud). This suggests that researchers had also utilized 'monitoring' as part of their published titles. Hence the word served as one of the main choices when detecting root exploits.

Apart from detection, it shows that even with all the current OSes available (Windows, Linux, MacOS, IOS, and Android), only one OS, which is Android, has been mentioned in the word cloud. This indicates that many root exploits researchers were focusing on Android, whether in detection or attacks (font with green color under the detection word).

Fig. 5 Word cloud of titles

In the following word cloud, the author's keywords were also listed below the abstracts of each publication. Fig. 6 highlights three similar keywords: 1) root exploit (small font located on top of rootkit word), 2) rootkits, and 3) rootkit. This shows the various keywords related to root exploit studies.

Other words found to be related to detection include intrusion detection (left side of the word cloud), monitoring (bottom of the cloud), malware detection, anomaly detection, static analysis, dynamic analysis, and control flow integrity (most of them are located in the right side of the word cloud). This predominance has helped many researchers conduct experiments aiming to detect root exploits through various efforts.

It is interesting to note that root exploits researchers prefer to use several words related to virtualizations, such as those shown in Fig. 6, which include: virtual machines, virtual machines, virtual machine monitor, virtualization, and virtual machine introspection. This shows that the researchers actively scrutinized the virtual machine part in their root exploit research efforts.

From the perspective of memory, two words were found to be related to memory: memory forensics (left side), and memory acquisition (right side). This means that researchers were also keen to inspect the memory part in root exploit investigations besides looking at the virtual machine area.

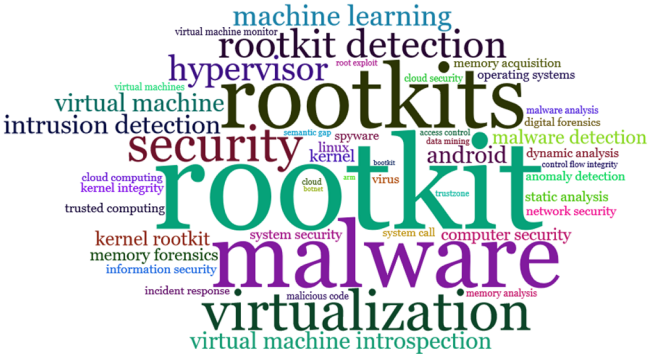

Fig. 6 Word cloud of author's keywords

E. Three Fields Plot

1) Sources, keywords and countries: Fig. 8 depicts the three-field plot which combines sources, keywords, and countries. It shows that most universities in many countries were interested in 'kernel' (the longest rectangle in gray color), and 'detection' (one of the longest rectangles in pink color), apart from other keywords. This occurrence suggests that root exploit researchers were spending their time in the detection and kernel area instead of attacking. Researchers also included keywords like 'monitoring', which served as one of the detection methods mentioned above. This shows that monitoring may be one of the solutions for improving computer security and preventing it from root exploit attacks. Other keywords that were relevant to monitoring include memory and virtual. This indicates that many researchers preferred to monitor the memory and virtual features when aiming to detect root exploits in their studies.

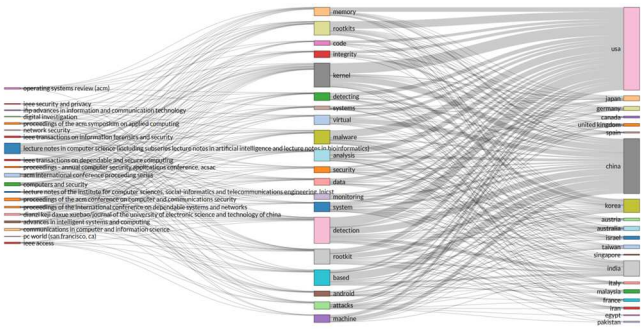

Fig. 7 Three fields plot of sources, keywords, and countries

Fig. 7 also illustrates that the word of kernel, memory and virtual existed in the middle plot. By combining those three terms, the countries were more interested in monitoring the kernel, memory, and virtual area when detecting root exploit.

2) Universities, keyword, and keyword plus: Fig. 9 shows the three-field plot which involved affiliations, keywords, and keyword plus. From the left side, the plot showed the affiliation, a keyword closely related to another. In the middle field is the keyword. A keyword is an idea or piece of content that defines what the article is about. In the right field is the keyword plus (extended by Scopus system). The keyword plus (ID) refers to the Scopus system's extended keywords and phrases, which are made up of keywords derived from the references utilized by the authors of a publication.

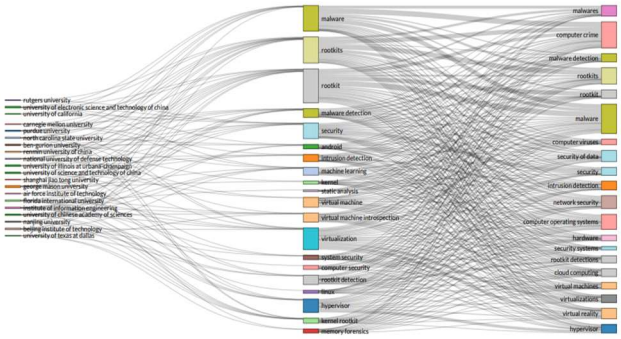

Fig. 8 Three fields plot of affiliation, keywords, and keyword plus

There were terms related to virtualization, such as virtual machine, virtual machine introspection, virtualization, and hypervisor, which were mentioned in the keywords (middle). The keyword plus (right side) lists keywords, such as virtual machines, virtualizations, virtual reality, and hypervisors. This observation suggests that root exploit researchers were beginning to focus on the virtual level and considering virtualization as one of the important areas when examining and detecting root exploit and its attacks. In the middle of the figure (third last row), and on the right side (last row), the focus was on the keyword of hypervisor, which is the essential part of virtualization. All these keywords revealed that root exploits researchers were conducting experiments widely in virtualization.

From another perspective, the figure also addresses forensic memory (the last row in the middle plot), and this shows that researchers were beginning to show interest in forensic memory. This is because a root exploit that remains in the memory can be a challenge since it is integrated with the memory. The only way to remove the root exploit is to modify the memory. Moreover, attackers can infiltrate confidential information through the memory without being recognized by the antivirus. This is because the antivirus only scans the hard disc and excludes the memory.

The graph (middle plot) only shows two operating systems, Linux and Android, excluding other OS such as Windows, iOS, and Ubuntu. The academic security community prefers these two types of operating systems because they are both open sources that are accessible to anyone with interest in the security area. Here, researchers were free to modify the configurations and settings so as to fulfill the requirements of specific situations based on their needs.

Fig. 8 also demonstrates the strong interest in research in root exploit detection. Several detection terms, such as malware detection, intrusion detection system (IDS), machine learning, static analysis [22], [23] rootkit detection, and virtual machine introspection (VMI) were mentioned in the middle plot. VMI is a technique that externally monitors the runtime state of a system-level virtual machine. This figure shows that root exploits are extremely harmful, and so they require more effective detection methods.

Another method of detection that has been utilized is machine learning. Fig. 8 highlights machine learning in the 8th row in the middle plot. Machine learning has become a top priority for researchers when deciding on the detection method for their research [24], [25]. This is due to the advancement of AI technology [26]–[30]. Many research studies have discovered that machine learning effectively and efficiently detects root exploits [35].

The left plot depicts the various universities actively conducting root exploit research. From the continental perspective, Asia has eight Chinese universities, the Middle East has one university from Israel, and the West has eleven universities from the USA. Computer crime is the most intriguing of the many terms included in the keyword plus (right plot, second row). This demonstrates that academics had explicitly used 'computer crime' to refer to the existing crime involving root exploit. This implies that attacking a victim through root exploit is a computer crime, hence, a serious matter.

F. Countries

Here, it 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 the continents. This productivity analysis helps researchers to focus on the research components and their strengths, thereby helping researchers to get an overview of the productivity performance of the publication in targeted research areas.

TABLE II
COUNTRIES WITH FREQUENCIES OF PUBLICATIONS

Region	Frequencies
USA	364
China	202
India	56
South Korea	43
Germany	27
France	22
Australia	20
Israel	16
Taiwan	16
Japan	15
UK	15
Malaysia	12
Austria	11
Iran	10
Italy	10
Canada	9
Pakistan	8
Singapore	7
Spain	6
Egypt	5

Researchers can also discover newer technologies or better methods from this productivity analysis. The productivity analysis may also assist researchers in evaluating the performance of various countries. As provided above, Table 2 tabulates the level of frequency among the countries.

TABLE III
COUNTRIES WITH TOTAL CITATIONS

Country	Total Citations	Average Article Citations Per Year
USA	4908	31.87
China	322	4.29
Australia	170	21.25
Canada	156	39.00
Korea	140	6.67
Japan	127	9.77
Austria	121	20.17
Germany	116	7.73
Israel	115	16.43
India	108	3.72
Netherlands	68	68.00
France	62	8.86
Iran	38	12.67
Italy	37	12.33
Greece	35	11.67
Qatar	29	14.50
Turkey	21	7.00
United Kingdom	20	3.33
Saudi Arabia	18	18.00
Taiwan	18	4.50

The USA was noted to be the country with the highest frequency of root exploit publications, followed by China, and then India. Three countries from Asia that were included in the top 5 rankings encompassed China, India, and South Korea. This indicates that many researchers chose to conduct root exploit studies in Asia. It also shows that these countries were well-supported by the government in terms of technological advancement as well as security, and these factors had driven them to become more knowledgeable about cyber security. This occurrence thus leads to more novel ideas of security which can be implemented in their respective countries.

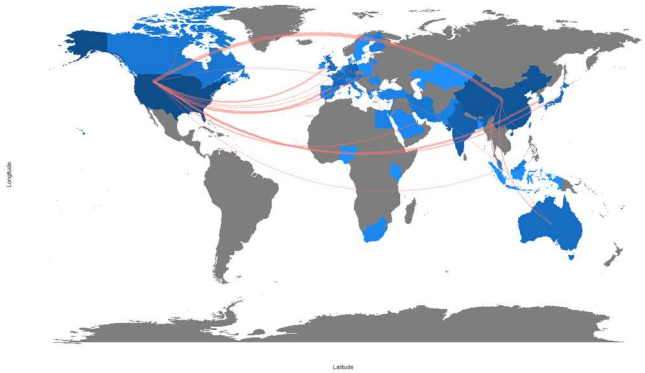

Fig. 9 Country collaboration engagement in root exploit research

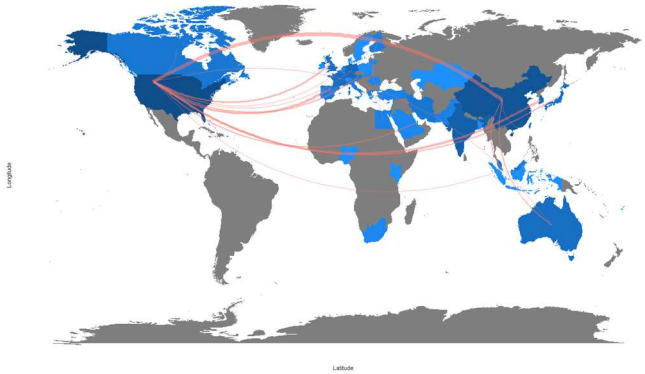

Fig. 9 depicts the individual country's collaboration worldwide, as hinted by the blue color. The dark blue shade indicates a higher frequency of collaboration with other countries. In this regard, China, the United Kingdom, Germany, India, France, the USA, and Australia were among the countries that actively interacted with others. According to the maps, the USA is the country that collaborated the most by practically being involved, with all the active countries publishing research in root exploit. The next country in line was China, and a few European countries. As the USA projected the highest frequency of publications, it also indicates that international partnerships can be an advantage, and it helps to boost the USA's publications.

In contrast, countries that were less interested in having collaborations in root exploit publications were indicated through the gray color, highlighting countries like New Zealand, Papua New Guinea, Russia, Algeria, Zimbabwe, Brazil, Argentina, and Mexico. This indicates that these countries were concentrating their efforts on other sorts of malware (botnets, ransomware, and Trojans), rather than root exploits. Alternatively, they also focused on topics other than cyber security (medical, plantation, or climate).

Table 3 tabulates the ranking of countries with citations in root exploit publications. In the top 5 rankings, it was observed that the USA has the highest total citations, followed by China, Australia, Canada, and Korea. The analysis shows three of these countries were from Asia (China, Australia, and Korea). This information reveals that researchers from Asia were also prominent in examining root exploits, besides those from the West (the USA and Canada).

As usual, the USA leads the ranking in citations. This may be due to the fact that events like world forums, such as Blackhat, were organized in the USA, resulting in increased citations for the USA. It also served as one of the most preferred references from all over the world. Additionally, the preference may also be affected by the convergence of international corporations such as Microsoft, Red Hat, Intel, and others, which tend to congregate in the USA, making the research atmosphere more intriguing [16].

From the general perspective, it can be seen that the Netherlands held the highest number of average article citations, totaling 68, followed by Canada, and then the USA. Nevertheless, even with the highest overall citations, the average number of papers derived from the USA was actually the lowest compared to the Netherlands and Canada. This phenomenon implies that even though papers from the Netherlands were fewer comparatively, it received more citations which means that the Netherlands had attracted the

majority of root exploit researchers who examined security improvements.

G. New Discoveries from Bibliometric of Root Exploit

1) Open-source OS (Android and Linux) has become the main interest in root exploit studies: Open source refers to software that is intended to be freely available to the public. Users have the capability to edit, change, and share the code based on their objectives. The open source was created decentralized and collaborative, with peer review and community output stated as key components. Since it was built by communities, the open source is frequently less expensive, more adaptable, and has a longer lifespan than proprietary alternatives. One of the open-source examples is Android.

Fig. 5 and Fig. 6 were mentioned Android, highlight, that researchers mentioned Android more than any other operating system, suggest that researchers use several terms that were associated with Android. This outcome suggests that Android is becoming one of the trends in root exploit studies. Furthermore, the number of Android users has grown since its release, with wide prices ranging from cheap to expensive. There is also more addition of smart devices (smartphone, smart glasses, smart television, smart vacuum, smart refrigerator, and smart shoes) today, which also adopted Android as their OS. The number of Android users is more than desktop computers. Hence Android is more prone and vulnerable to root exploit attacks.

From the analysis, it was noted that many studies involving root exploit also looked at Linux OS. Fig. 6 displays the use of author keywords, including Linux, in many publications, as noted in the third branch of the dendrogram. This keyword was further combined with other keywords like execution, and overhead. The figure shows that Linux was listed with Android in the middle plot. Since Linux is the OS that was distributed prior to Android, which was developed based on the Linux kernel, it is thus, crucial to investigate the Linux OS in the initial study.

2) The rapid increase of root exploit in the virtualization area: Virtualization uses software to build an abstraction layer over the hardware components, for instance, processors, memory, or storage. Since 2006, Joanna Rutkowska had been presenting the 'BluePill' virtual root attack, which compromises the virtual layer in AMD processors. Prior to that, root exploit researchers had also made virtualization a top priority when researching the virtual characteristics and risks connected with root exploits.

The current bibliometric analysis was able to uncover several insights in terms of virtualization in root exploit publications. For instance, we uncovered the use of virtual machine (without s), virtual machines, virtual machine monitor, virtualization, and virtual machine introspection. Additionally, Fig. 8 depicts the use of main words, such as virtualization, and machines in the publications. This occurrence demonstrates that virtualization has a high risk of being attacked by root exploit, thereby exposing users to potential precarious activities. As a result, more novel research on root exploit relating to virtual machines is required.

3) Country involvement: Overall, it can be seen that the USA is leading in root exploit investigations. Previous figures and tables imply that the USA has the highest-ranking, hence more researchers who were involved in this area of research. In brief, it had more experts in root exploit studies. From the perspective of Asia, some statistics also indicate that Asia possesses active researchers involved in root exploit efforts. Previous figures and tables display the fact that the top countries in root exploit research include China, India, and South Korea, thereby suggesting that Asian countries have also contributed to root exploit studies over the years. These countries would probably outgrow other countries in the near future.

4) Significant authors in root exploit: In this regard, several authors or researcher practitioners were found to have a high impact in the root exploit research. The significant authors who were most active in root exploit studies and publications include Jiang X, Xu D, Lin Z, and Wang X, all of whom had published similar studies between 2004 to 2020. They were also among the researchers with the highest h and g indexes. It appears that they were constantly stepping up their efforts in this area and adding to the body of knowledge on root exploit research. Even though some authors seemed to have departed from root exploit research, their contributions to root exploit studies were still relevant for the future.

5) Enhancement of the potential of memory forensics: Memory is a critical component in computer hardware; it is required for running the system or for executing the system. Memory can be used to control contents as the program runs, whether on a normal or virtual basis. One component that is familiar to memory is the memory dump. It is the process of transferring all information contained in the RAM to a storage drive. This was also included as part of the computer forensic examination process.

Here, the word, 'analysis' and 'table' were presented together. Fig. 6 shows the terms used in the research title which was noted in the hardware frequency called memory. This demonstrates that memory can also be at risk of a root exploit attack, which can be performed at the privileged level rather than the operating system level. The root exploit is able to execute codes (hypervisor level) on a privileged level (user level), with the assistance of hardware virtualization technology. This allows attackers to gain access through the hypervisor, leaving the users vulnerable to 'Man-In-The-Middle' attacks. As a result, root exploits were able to spy and execute without being noticed, hence the reason why security practitioners need to consider the importance of the hypervisor level in preventing root exploit attacks [29], [30].

The three-field plot, the terms, memory, memory forensics, and memory acquisition appeared in the author's keywords, indicating that security practitioners were focusing their attention on memory as a component at high potential risk of root exploit. This demonstrates that the root exploit area necessitates the use of memory forensics, which can be traced and used to determine memory activities. It also suggests that memory forensics is an important part of root exploit research and may become a high priority in the near future.

6) *Detection is the main activity in root exploit investigation:* In root exploit publications, it seems that many researchers had conducted experiments in developing new methods to detect root exploit as well as new methods of root exploits in compromising the victim. However, detection was the main interest when compared to attacks. Fig. 7 depicts *detection* (one of longest rectangles in pink color) when compared to other keywords, and exhibits several detection terms - malware *detection*, intrusion *detection* system (IDS), machine learning, static analysis, rootkit *detection*. This outcome showed that it is challenging to detect root exploit, despite the many efforts made to detect it. As the nature of root exploit is to gain administrative privileges, the result of the detection is vague because the administrator actions were executed either by the real administrator or by the root exploit itself.

7) *Monitoring method in root exploit detection:* Fig. 5, Fig. 6, Fig. 7 and Fig. 8 exhibit the term, 'monitoring' among the countries. According to these figures and tables, security practitioners were placing a high value on the term, 'monitoring'. This shows that security researchers preferred the monitoring methods when exploring various detection methods of root exploit. The majority of the research was conducted to develop a better method of preventing root exploit attacks, identifying root exploits, and dealing with root exploit attacks, specifically its impact on hardware. The outcome derived would assist academia in gaining a better understanding of the interactions between hardware performance and root exploit.

IV. Conclusion

The advance of root exploit has drastically propelled security practitioners to conduct experiments in both root exploit attacks, and root exploits detection. As many devices were being invented (smart glasses, smart shoes, and smart vacuum), more OSes were created to cater to the operations and functions of these devices, based on the smart devices' objectives. Due to this prevalence, many malware attackers were also developing more root exploits which can be used to compromise the OS kernel of the smart devices, by stealing personal data which are then used for selfish and private purposes.

Many reviews examined malware in many aspects, but very few focused on root exploits. Addressing this gap, the current paper thus focused on showcasing the depth and breadth of this research area by conducting a bibliometric analysis of 32 years of publication involving root exploit. A total of 598 articles published between 1989 and 2021 were retrieved for analysis. Through this review, we were able to understand that many aspects of the research area encompass productivity performance. Our findings showed that throughout the year, the number of publications on this topic had increased exponentially, suggesting the research area's popularity.

Our bibliometric analysis also revealed that: 1) Linux and Android served as the main interest in root exploit studies. Linux is the OS invented earlier while Android was developed based on the Linux kernel. Due to this, it is crucial to investigate the Linux OS for initial studies. 2) The types of root exploit in the virtualization layer and studies have also increased. Many researchers focused on root exploit attacks and root exploit detection within the virtual parts, especially in CPUs embedded with virtual features. 3) The USA and China have become leaders in root exploit research. 4) Root exploit studies were more inclined towards memory forensics to examine root exploit detection, which is more promising. Nevertheless, there were still many research gaps that can be addressed in memory forensics, especially in smart devices. 5) Root exploit researchers were more focused on detecting root exploit, rather than finding ways to attack root exploits. This is because once a novel method has been compromised by root exploit, it becomes more challenging to detect since root exploits can surpass the existing security parameters.

Acknowledgment

The authors than the Ministry of Higher Education (MOHE) for Fundamental Research Grant Scheme (FRGS) with grant number RDU192607, RACER/1/2019/ICT02/UMP//5, and the Universiti Malaysia Pahang for additional financial support under Internal Research Grant UMP Postgraduate Research Grants Scheme (PGRS2003100).

References

[1] W. Kong, "Research on Technology of Process Hiding based on VMM," *2015 International Conference on Computer Science and Applications (CSA)*, pp. 339–344, 2015, doi: 10.1109/CSA.2015.26.

[2] P. Nimbalkar and D. Kshirsagar, "Feature selection for intrusion detection system in Internet-of-Things (IoT)," *ICT Express*, vol. 7, no. 2, pp. 177–181, 2021, doi: 10.1016/j.icte.2021.04.012.

[3] M. Lechtik and G. Dedola, "Operation TunnelSnake," 2021. https://securelist.com/operation-tunnelsnake-and-moriya-rootkit/101831/ (accessed May 06, 2021).

[4] A. Sharma, "Microsoft admits to signing rootkit malware in supply-chain fiasco," 2021. https://www.bleepingcomputer.com/news/security/microsoft-admits-to-signing-rootkit-malware-in-supply-chain-fiasco/ (accessed Sep. 09, 2021).

[5] S. R. T. Mat, M. F. Ab Razak, M. N. M. Kahar, J. M. Arif, S. Mohamad, and A. Firdaus, "Towards a systematic description of the field using bibliometric analysis: malware evolution," *Scientometrics*, vol. 126, no. 3, pp. 2013–2055, 2021, doi: 10.1007/s11192-020-03834-6.

[6] S. K. Jalal, "Co-authorship and co-occurrences analysis using bibliometrix r-package: A case study of india and bangladesh," *Annals of Library and Information Studies*, vol. 66, no. 2, pp. 57–64, 2019.

[7] D. Agapito, "The senses in tourism design: A bibliometric review," *Annals of Tourism Research*, vol. 83, no. December 2019, 2020, doi: 10.1016/j.annals.2020.102934.

[8] I. Firmansyah and A. S. Rusydiana, "Bibliometric Analysis of Articles on Accounting and Covid-19 during the Pandemic," *Library Philosophy and Practice*, vol. 2021, pp. 1–15, 2021.

[9] R. Orastean, S. C. Marginean, and R. Sava, "Bitcoin in the scientific literature - A bibliometric study," *Studies in Business and Economics*, vol. 14, no. 3, pp. 160–174, 2019, doi: 10.2478/sbe-2019-0051.

[10] D. Yu, D. F. Li, J. M. Merigó, and L. Fang, "Mapping development of linguistic decision making studies," *Journal of Intelligent and Fuzzy Systems*, vol. 30, no. 5, pp. 2727–2736, 2016, doi: 10.3233/IFS-152026.

[11] F. Afifi, N. B. Anuar, S. Shamshirband, and K.-K. R. Choo, "DyHAP: Dynamic Hybrid ANFIS-PSO Approach for Predicting Mobile Malware," *Plos One*, vol. 11, no. 9, pp. 1–21, 2016, doi: 10.1371/journal.pone.0162627.

[12] J. Koskinen *et al.*, "How to use bibliometric methods in evaluation of scientific research? An example from Finnish schizophrenia research," *Nordic Journal of Psychiatry*, vol. 62, no. 2, pp. 136–143, 2008, doi: 10.1080/08039480801961667.

[13] A. Abrizah, A. N. Zainab, K. Kiran, and R. G. Raj, "LIS journals scientific impact and subject categorization: A comparison between Web of Science and Scopus," *Scientometrics*, vol. 94, no. 2, pp. 721–740, 2013, doi: 10.1007/s11192-012-0813-7.

[14] J. Mingers and L. Leydesdorff, "A review of theory and practice in scientometrics," *European Journal of Operational Research*, vol. 246, no. 1, pp. 1–19, 2015, doi: 10.1016/j.ejor.2015.04.002.
[15] P. Mongeon and A. Paul-Hus, "The journal coverage of Web of Science and Scopus: a comparative analysis," *Scientometrics*, vol. 106, no. 1, pp. 213–228, 2016, doi: 10.1007/s11192-015-1765-5.
[16] M. F. A. Razak, N. B. Anuar, R. Salleh, and A. Firdaus, "The rise of "malware": Bibliometric analysis of malware study," *Journal of Network and Computer Applications*, vol. 75, pp. 58–76, 2016, doi: 10.1016/j.jnca.2016.08.022.
[17] C. López-Illescas, F. de Moya-Anegón, and H. F. Moed, "Coverage and citation impact of oncological journals in the Web of Science and Scopus," *Journal of Informetrics*, vol. 2, no. 4, pp. 304–316, 2008, doi: 10.1016/j.joi.2008.08.001.
[18] J. Grimm, "Users, narcissism and control – tracking the impact of scholarly publications in the 21st century," *World Statistics on Mining and Utilities 2018*, p. 50, 2012, doi: 10.4337/9781788974585.00003.
[19] M. Clermont and H. Dyckhoff, "Coverage of Business Administration Literature in Google Scholar: Analysis and Comparison with Econbiz, Scopus and Web of Science," *SSRN Electronic Journal*, pp. 1–54, 2012, doi: 10.2139/ssrn.2016850.
[20] P. H. C. Chabot, "What is Tableau?," 2021. .
[21] M. Aria and C. Cuccurullo, "bibliometrix: An R-tool for comprehensive science mapping analysis," *Journal of Informetrics*, vol. 11, no. 4, pp. 959–975, 2017, doi: 10.1016/j.joi.2017.08.007.
[22] H. A. Parhusip, B. Susanto, L. Linawati, S. Trihandaru, Y. Sardjono, and A. S. Mugirahayu, "Classification Breast Cancer Revisited with Machine Learning," *International Journal on Data Science (IJODS)*, vol. 1, no. 1, pp. 42–50, 2020, doi: 10.18517/ijods.1.1.42-50.2020.
[23] N. Mohd Hatta, Z. Ali Shah, and S. Kasim, "Evaluate the Performance of SVM Kernel Functions for Multiclass Cancer Classification," *International Journal on Data Science (IJODS)*, vol. 1, no. 1, pp. 37–41, 2020, doi: 10.18517/ijods.1.1.37-41.2020.
[24] M. Sajjad, M. Pasha, and U. Pasha, "Parametric Evaluation of E-Health Systems," *International Journal of Information Systems and Computer Technologies (IJISCT)*, vol. 1, no. January, pp. 31–37, 2022.
[25] H. Ghous, M. H. Malik, M. Abbas, and M. Ismail, "Early Detection of Breast Cancer Tumors using Linear Discriminant Analysis Feature Selection with Different Machine Learning Classification Methods," *International Journal of Information Systems and Computer Technologies (IJISCT)*, vol. 1, no. 1, pp. 1–12, 2022, doi: 10.5121/cseij.2022.12117.
[26] M. Sulistiyono, L. A. Wirasakti, and Y. Pristyanto, "The Effect of Adaptive Synthetic and Information Gain on C4. 5 and Naive Bayes in Imbalance Class Dataset," *International Journal of Advanced Science Computing and Engineering (IJASCE)*, vol. 4, no. 1, pp. 1–11, 2022.
[27] S. K. Mohamed, N. A. Sakr, and N. A. Hikal, "A Review of Breast Cancer Classification and Detection Techniques," *International Journal of Advanced Science Computing and Engineering (IJASCE)*, vol. 3, no. 3, pp. 128–139, 2021.
[28] E. Juma Adwan and B. Ali Alsaeed, "Cloud Computing adoption in the financial banking sector-A systematic litreture review (2011-2021)," *International Journal of Advanced Science Computing and Engineering (IJASCE)*, vol. 4, no. 1, pp. 48–55, 2022.
[29] N. Qadir and R. Ahmad, "Secrs Template To Aid Novice Developers in Security Requirements Identification and Documentation," *International Journal of Software Engineering and Computer Systems (IJSECS)*, vol. 8, no. 1, pp. 45–52, 2022, doi: 10.15282/ijsecs.8.1.2022.5.0095.
[30] H. Chaudhary, H. Chaudhary, and A. Kumar Sharma, "Optimized Genetic Algorithm and Extended Diffie Hellman as an Effectual Approach for DOS-Attack Detection in Cloud," *International Journal of Software Engineering and Computer Systems (IJSECS)*, vol. 8, no. 1, pp. 69–78, 2022, doi: 10.15282/ijsecs.8.1.2022.7.0097.
[31] M. F. A. Razak, N. B. Anuar, F. Othman, A. Firdaus, F. Afifi, and R. Salleh, "Bio-inspired for Features Optimization and Malware Detection," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 6963–6979, 2017, doi: 10.1007/s13369-017-2951-y.
[32] S. Y. Yerima, S. Sezer, G. McWilliams, and I. Muttik, "A New Android Malware Detection Approach Using Bayesian Classification," in *IEEE 27th International Conference on Advanced Information Networking and Applications (AINA), Barcelona, Spain*, Mar. 2013, pp. 121–128, doi: 10.1109/AINA.2013.88.
[33] S. Y. Yerima, S. Sezer, and I. Muttik, "Android malware detection: An eigenspace analysis approach," *2015 Science and Information Conference (SAI)*, pp. 1236–1242, 2015, doi: 10.1109/SAI.2015.7237302.
[34] R. Jusoh, A. Firdaus, S. Anwar, M. Z. Osman, M. F. Darmawan, and M. F. Ab Razak, "Malware detection using static analysis in Android: a review of FeCO (features, classification, and obfuscation)," *PeerJ Computer Science*, vol. 7, no. e522, pp. 1–54, 2021, doi: 10.7717/peerj-cs.522.
[35] C. A. Che Yahaya, A. Firdaus, S. Mohamad, F. Ernawan, and M. F. A. Razak, "Automated Feature Selection using Boruta Algorithm to Detect Mobile Malware," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 5, pp. 9029–9036, 2020, doi: 10.30534/ijatcse/2020/307952020.