International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 4 ǁ April 2023 ǁ PP. 267-277

Stepping-Stone Attacks: A Bibliometric Analysis

Ali Yusny Daud[1], Cik Fazilah Hibadullah [2]
*[*1,2]School of Information Technology, Universiti Utara Malaysia, UUM Sintok, Malaysia*
Corresponding Author: Ali Yusny Daud

Abstract
A stepping-stone is an intermediary host or node that is actively used as a hop point in the network to target the host of a victim. Determining the path taken to get from the intermediate location to the attack's starting point will assist in identifying the starting point rather than just the nearby host from which the connection originates. Accordingly the information from the Scopus database will be used in this paper to analyse and report on published documents that are related to it. We concentrate on analysis of publications by year, different types of documents and sources, subject areas, language used in publications, geographical distribution of publications, most active source title, significant keywords, and citation analysis. The data from 2000 to September 2022 indicate that research into "stepping-stone attacks" is still going on today, demonstrating the need for interest in this area.

Keywords: *Stepping-stone, Stepping-stone attacks, Intrusion detection, Bibliometric.*

Date of Submission: 01-04-2023 Date of acceptance: 12-04-2023

I. INTRODUCTION

Computer attacks can be carried out quickly by sending malicious code through the network and without the victim being aware of them. The attackers may be found anywhere in the world. Even worse, the attackers can channel their attacks through an intermediary host. Attacks of this kind will start by seizing control of the intermediate host. Because it appears that the attacker is not directly involved, it will maintain the attackers' anonymity. Attacks from nearby hosts can quickly reveal the attacker, but it will be more difficult to identify the initial attacker in a series of attacks.

In a stepping-stone attack, the attackers conceal their identity while attacking the victims by using a network of infected intermediate nodes [4]. An outsider could compromise a host in a network that is being managed by taking advantage of certain vulnerabilities, and then use the compromised host as a launching point to learn useful information about the network and every host that is a part of it. Staniford-Chen and Heberlein's study in 1995 on stepping-stone detection (SSD) was the first significant one [9]. Since then, extensive research has been done to identify stepping-stone attacks, which has increased the relevance of SSD to this day.

The Panama Papers leak is a recent example of a stepping-stone incident [10]. In April 2016, attackers gained access to the Panama-based firm via the email server. According to speculations, an external attacker exploited vulnerabilities in the email server to compromise it. The attacker used these compromised servers as stepping-stones to obtain more information from the internal network and stole highly confidential documents revealing information about the clients. The attacker moved around the network interactively and stole a large amount of data in the company's internal network undetected for a long time. The incident is similar to stepping-stone attacks in that the attack traffic containing stolen data passed through a chain of stepping-stones from the attacker to reach the victim. The attacker established a chain of connections via intermediate or stepping-stone hosts and then executed the attacking command [6].

Stepping-stone attacks target the victim by attacking a series of hosts (stepping-stones). Due to the attack's indirect connection to the victim's computer or host, the attacker will remain anonymous. The chaining path from the initiator to the victim through stepping-stone devices is known as the stepping-stone's connection. Stepping-stone attacks had since escalated in danger and threat. Despite the difficulty of detection, SSD research has continued to keep up with the evolving nature of attacks [12]. Figure1 shows target host only identified adjacent host as the attackers while the initial attackers escape the detection.

The variety of strategies or techniques shows how seriously SSD research is being taken. Evidently, as the majority of researchers concurred, content-based approach was the first detection [9]. Unfortunately, given that the majority of data is now encrypted [1], [7], & [8], this approach seems out of date. Only unencrypted or unmodified data can be used with the content-based approach. Additionally, it may jeopardise the privacy of data exposed during network traffic [2].

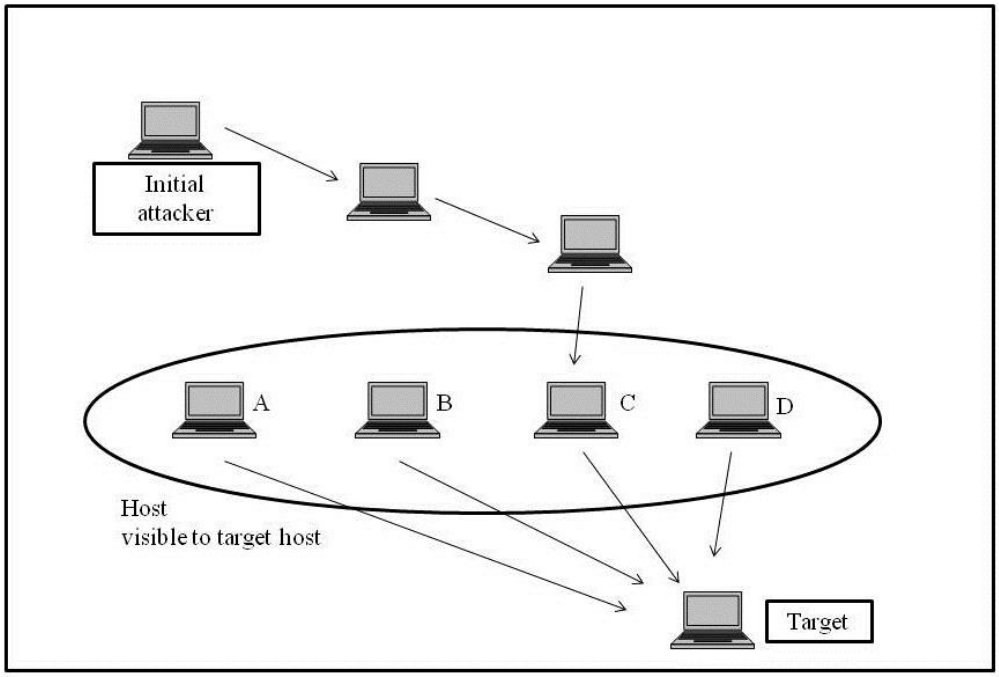

Figure1: Target Host Identified Only Adjacent Host

Similarly, deviation-based approaches are also unadaptable at stepping-stones [1]. Due to the need to measure every packet across all networks, it is also expensive [7]. Undoubtedly, deviation-based, and watermark-based methods are expensive. The use of a "watermark" requires additional hardware for detection, such as a water marker and detector [11]. The ability to detect and alter the watermark compromises the ability to detect stepping-stones. Additionally, [5] showed how the "watermark" could be copied and pasted onto other traffic flows that compromised SSD.

Many timing-based and RTT-based SSD approaches are currently being used, but RTT-based has come under fire for its tendency to inaccurately compute timing, particularly when dealing with data that uses programming script [7]. Furthermore, because it must consider timing for both "send" and "echo" packets, RTT-based approach took twice as long as timing-based approach. The timing characteristic in the timing-based approach is distinctive enough to be used in the detection of stepping-stones, even though the accuracy of time in RTT-based is questioned. The timing-based approach is acknowledged as a current strategy and potentially a promising one for SSD [12].

Despite growing interest in research on stepping-stone attacks, no bibliometric study has yet been conducted in this area, to our knowledge. Applying statistical methods to the objective and quantitative evaluation of scholarly publications within a given topic is what is meant by bibliometric analysis [3]. In order to comprehend the achievements in this field, including research productivity, important articles, and significant issues that the research community is concerned about, we used bibliometric methodologies in this paper. The remaining sections of this article are organized as follows. Section 2 of this analysis's methodology is described. Section 3 presents the study's findings. The conclusion of this paper is provided in Section 4.

II. METHODS

Method that has been used in this study is illustrated in figure2. The flow of this figure shows how the bibliometric analysis on ‘stepping-stone attacks’ being conducted. The analysis using Scopus database produced 254 articles. However, after doing the refining phases, only 220 articles that really match the stepping-stone attacks in network. There are 34 articles that using stepping-stone attacks but not meant in computer network area. Among the articles that being excluded were articles in aircraft, medication, socio-politics, chemical and energy.

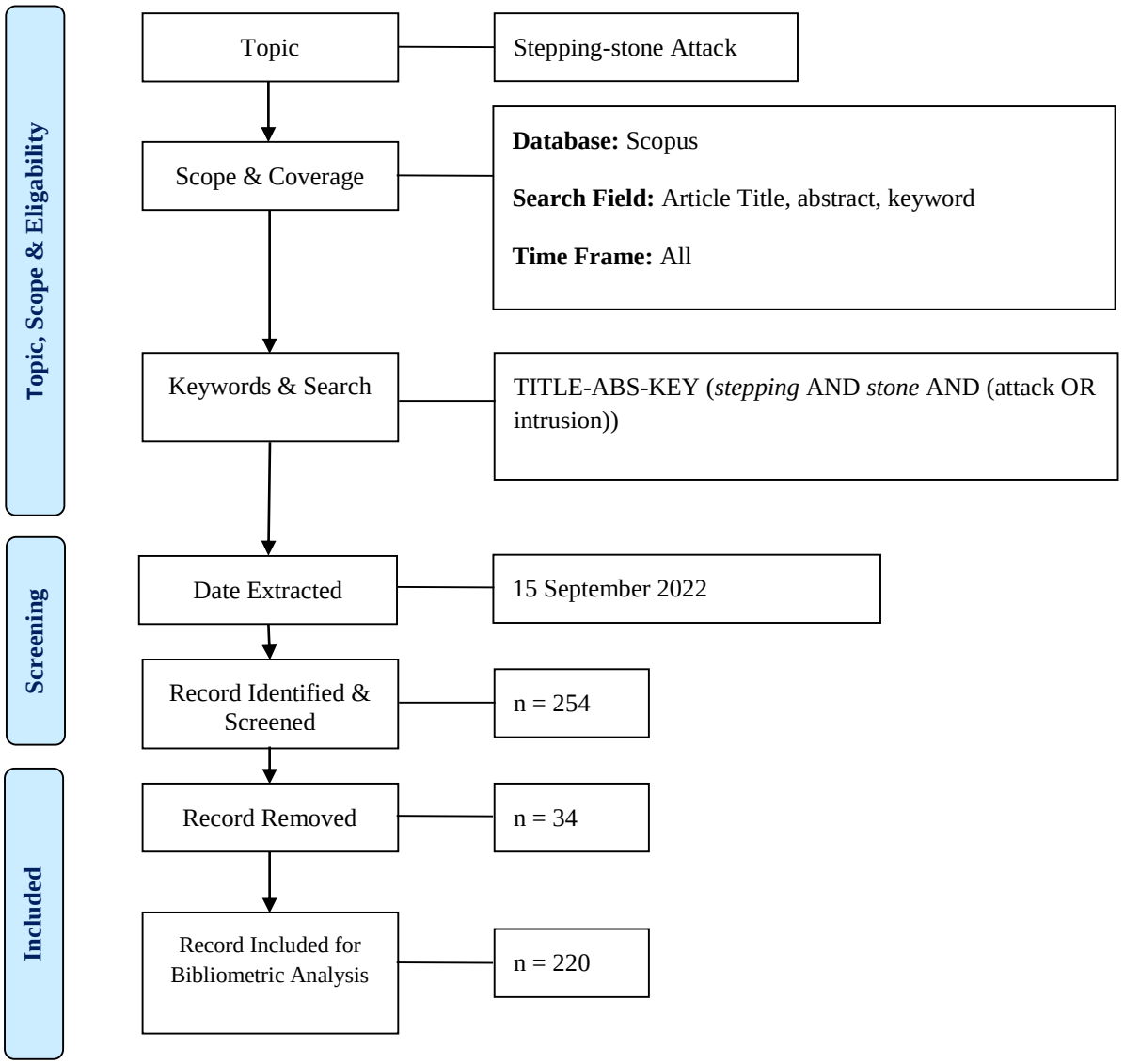

Figure2: Flow diagram of the search strategy [13].

Source: Zakaria, R., Ahmi, A., Ahmad, A. H., & Othman, Z. (2020) Worldwide Melatonin Research: A

Bibliometric Analysis of Published Literature between 2015 and 2019, Chronobiology International. https://doi.org/10.1080/07420528.2020.1838534

Modified from PRISMA (Moher D, Liberati A, Tetzlaff J, Altman DG, The PRISMA Group (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. PLoS Med 6(7): e1000097. doi:10.1371/journal.pmed1000097)

III. RESULT

3.1 Document and Source Type

First, the data was analysed using various types of scientific documents. The document types refer to the different types of documents based on their originality, such as conference papers, articles, book chapters, and so on. While source type refers to the source of documents, it could be a journal, conference proceedings, book series, or a book or trade publication. According to table 1, the vast majority of publications were conference papers, accounting for 65% of total publications, followed by articles (27.27%). The other types of documents accounted for less than 10% of all documents. It included less than 3% of each book chapter, conference review, review, and note document type.

Table 1. Document Type

Document Type	TP	%
Conference Paper	143	65.00%
Article	60	27.27%
Book Chapter	6	2.73%
Conference Review	6	2.73%
Review	4	1.82%
Note	1	0.45%
Total	220	100.00%

There are five types of sources visible in the search result under source type (see Table 2). Thus, conference proceedings were the most common type of source, accounting for 119 (54.09%), followed by journal 64 (29.09%). Book series 32 publications (14.55%), books 4 (1.82%), and trade journals are only one (0.45%) of the total publications on this topic.

Table 2. Source Type

Source Type	Total Publications (TP)	Percentage (%)
Conference Proceeding	119	54.09%
Journal	64	29.09%
Book Series	32	14.55%
Book	4	1.82%
Trade Journal	1	0.45%
Total	**220**	100.00%

3.3 Languages

According to Table 3, just two languages have been used in this study. With a total of 217 articles, the most of retrieved documents (98.64%) were published in English. Another language used for this study is Chinese, which accounts for approximately three or 1.36% of all publications.

Table 3. Languages

Language	Total Publications (TP)*	Percentage (%)
English	217	98.64%
Chinese	3	1.36%
Total	**220**	**100.00**

3.4 Subject Area

Table 4 summarises the total number of subjects as published in the article stepping-stone attacks. The majority of studies on 'stepping-stone attacks are published in the field of computer science, accounting for (185: 84.09%) of total articles, followed by engineering (99: 45%), mathematics (45: 20.45%), and social sciences (11:5%). Table 4 depicts the remaining subject areas.

Table 4. Subject Area

Subject Area	TP	%
Agricultural and Biological Sciences	1	0.45%
Arts and Humanities	1	0.45%
Biochemistry, Genetics and Molecular Biology	3	1.36%
Business, Management and Accounting	1	0.45%
Chemistry	2	0.91%
Computer Science	185	84.09%
Decision Sciences	16	7.27%
Energy	1	0.45%
Engineering	99	45.00%
Health Professions	1	0.45%
Immunology and Microbiology	1	0.45%
Materials Science	4	1.82%
Mathematics	45	20.45%

Medicine	4	1.82%
Multidisciplinary	2	0.91%
Physics and Astronomy	8	3.64%
Social Sciences	11	5.00%

3.5 Number of Publication by Years

The first study on 'stepping-stone attacks was released in 2000; however, this study was not widely circulated. A year later, only one (1) report published under this title. However, from 2002 to 2008, the number of 'stepping-stone attacks published increased gradually, from one in 2002 to 18 in 2008, and then gradually decreased until 2014. (Figure3). However, study on 'stepping-stone attacks revived from 2014 (7 publications) to 2018 (17 publications). The highest number of citations occurred in that year (1633 citations), as shown in table 2. Even though the number of publications in this field has decreased since then, research on 'stepping-stone attacks is still continuing.

Table 5. Year of Publication

Year	TP	%	NCP	TC	C/P	C/CP	h	g
2000	1	0.45%	1	281	281.00	281.00	1	1
2001	1	0.45%	1	4	4.00	4.00	1	1
2002	4	1.82%	3	227	56.75	75.67	3	4
2003	4	1.82%	3	188	47.00	62.67	1	4
2004	6	2.73%	6	133	22.17	22.17	4	6
2005	6	2.73%	5	97	16.17	19.40	3	6
2006	14	6.36%	13	257	18.36	19.77	8	14
2007	10	4.55%	10	129	12.90	12.90	6	10
2008	18	8.18%	15	191	10.61	12.73	7	13
2009	14	6.36%	11	112	8.00	10.18	7	10
2010	12	5.45%	11	91	7.58	8.27	5	9
2011	14	6.36%	12	122	8.71	10.17	7	11
2012	8	3.64%	8	91	11.38	11.38	6	8
2013	12	5.45%	10	365	30.42	36.50	6	12
2014	7	3.18%	6	34	4.86	5.67	3	5
2015	10	4.55%	7	40	4.00	5.71	4	6
2016	12	5.45%	10	124	10.33	12.40	6	11
2017	11	5.00%	8	82	7.45	10.25	4	9
2018	17	7.73%	15	1633	96.06	108.87	6	17
2019	16	7.27%	11	162	10.13	14.73	5	12
2020	8	3.64%	5	32	4.00	6.40	3	5
2021	8	3.64%	6	11	1.38	1.83	2	2
2022	7	3.18%	3	5	0.71	1.67	2	2
Total	**220**	**100.00%**						

Notes: TP=total number of publications; NCP=number of cited publications; TC=total citations; C/P=average citations per publication; C/CP=average citations per cited publication; h=h-index; and g=g-index.

3.6 Geographical Distribution of Publications - Most Influential Countries

Table 6 shows the breakdown of the top 20 countries based on the amount of publishing in stepping-stone attacks. The United States of America ranked first with 123 documents, then followed by China (42), and Germany (11). Malaysia came in fourth place with nine publications.

3.7 Most Influential Institutions

Table 7 displayed the most influential institutions, each of which had at least five publications. With 29 publications, the University of Houston is the most active institution. Columbus State University comes in second with 21 publications. It was followed by NC State University and the University of Illinois Urbana-Champaign, each with 10 and 9 publications. Table 7 lists the remaining institutions.

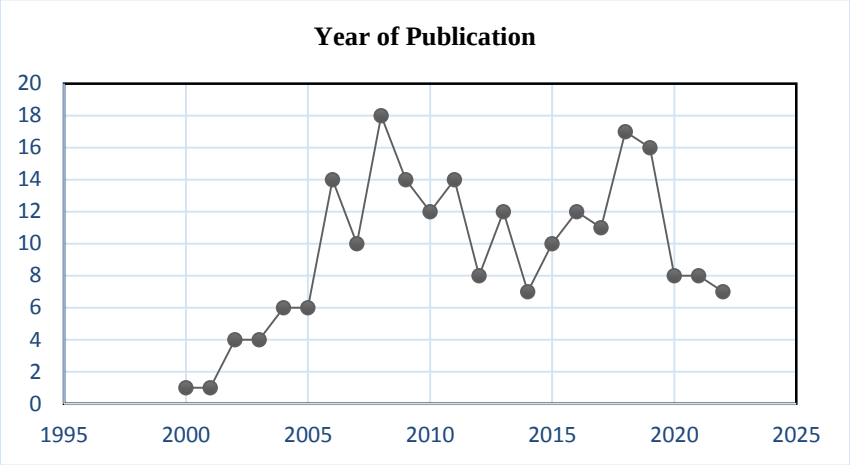

Figure3: Total Publications by Year

Table 6. Top 20 Countries contributed to the publications

Country	TP	%
United States	123	55.91%
China	42	19.09%
Germany	11	5.00%
Malaysia	9	4.09%
United Kingdom	8	3.64%
Australia	7	3.18%
Taiwan	7	3.18%
Canada	6	2.73%
India	5	2.27%
Italy	5	2.27%
Japan	4	1.82%
South Korea	4	1.82%
Austria	3	1.36%
Hong Kong	3	1.36%
Israel	3	1.36%
Netherlands	3	1.36%
Singapore	3	1.36%
Finland	2	0.91%
Greece	2	0.91%
Norway	2	0.91%

Notes: TP=total number of publications.

Table 7. Most influential institutions with minimum of five publications

Affiliation	Country	TP
University of Houston	United States	29
Columbus State University	United States	21
NC State University	United States	10
University of Illinois Urbana-Champaign	United States	9
Universiti Utara Malaysia	Malaysia	6
Iowa State University	United States	6
Southeast University	China	6
George Mason University	United States	6
Shanghai Open University	China	6
Cornell University	United States	5

Notes: TP=total number of publications.

3.8 Most Productive Authors

Table 8 lists the most productive authors who made a significant contribution to stepping-stone attacks' research. Yang, Jianhua, of Columbus State University in the United States of America, was the most active author in this field, with 32 publications. Huang, Shou Hsuan Stephen (25 publications) of the University of Houston in the United States of America was the second most productive author publishing on stepping-stone attacks.' He also collaborated on nine publications with the first productive authors (Yang, Jianhua). In third place, two authors, Wang, Lixin, affiliated with Columbus State University in the United States of America, and Zhang, Yongzhong, affiliated with Shanghai Open University in China, both had ten publications. Interestingly, they were also co-authors with the productive author Yang, Jianhua.The rest of the most productive authors are shown in table 8.

Table 8. Most Productive Authors with minimum five publications

Author's Name	Affiliation	Country	TP	NCP	TC	C/P	C/CP	*h*	*g*
Yang, J.	Columbus State University	United States	32	26	171	5.34	6.58	7	11
Huang, S.H.S.	University of Houston	United States	25	24	243	9.72	10.13	8	14
Wang, L.	Columbus State University	United States	10	8	24	2.40	3.00	3	4
Zhang, Y.	Shanghai Open University	China	10	7	34	3.40	4.86	4	5
Wang, X.	George Mason University	United States	9	8	412	45.78	51.50	8	9
Kuo, Y.W.	University of Houston	United States	6	6	30	5.00	5.00	3	5
Wu, H.C.	University of Houston	United States	6	5	44	7.33	8.80	3	6
Guan, Y.	Iowa State University	United States	5	3	40	8.00	13.33	2	5
Luo, J.	Southeast University	China	5	5	59	11.80	11.80	5	5
Wang, X.	Changzhou College of Information Technology	China	5	5	59	11.80	11.80	5	5
Yang, M.	Southeast University	China	5	5	59	11.80	11.80	5	5

Notes: TP=total number of publications; NCP=number of cited publications; TC=total citations; C/P=average citations per publication; C/CP=average citations per cited publication; h=h-index; and g=g-index.

3.9 Most Active Source Title

Table 9 summarised the top ten most active source titles in the stepping-stone attacks' research. According to Table 9, the top journals that contribute to publications in this study the Lecture Notes in Computer Science Including Subseries Lecture Notes in Artificial Intelligence And Lecture Notes In Bioinformatics.

Table 9. Most Active Source Title

Source Title	TP	Publisher	Cite Score 2021	SJR 2021	SNIP 2021
Lecture Notes In Computer Science Including Subseries Lecture Notes In Artificial Intelligence And Lecture Notes In Bioinformatics	23	Springer Nature	2.1	0.407	0.534
Proceedings International Conference On Advanced Information Networking And Applications AINA	13	Springer Nature	N/A	N/A	N/A

Computers And Security	4	Elsevier	10.1	1.726	2.302
Proceedings IEEE Symposium On Security And Privacy	4	IEEE	N/A	N/A	N/A
Proceedings Of The ACM Conference On Computer And Communications Security	4	ACM	9.7	2.512	3.005
Proceedings Of The International Conference On Parallel And Distributed Systems ICPADS	4	IEEE	2.3	0.375	0.578
Security And Communication Networks	4	Hindawi	3.3	0.734	1.075
International Journal Of Innovative Technology And Exploring Engineering	3	Blue Eyes Intelligence Engineering and Sciences Publication	0.6	0.102	0.346
Lecture Notes In Computer Science	3	Springer Nature	2.1	0.407	0.534
Proceedings IEEE Military Communications Conference MILCOM	3	IEEE	N/A	N/A	N/A

Notes: TP=total number of publications.

3.10 Citation Analysis

Table 10 sums up the citation metrics for the documents retrieved as of September 15, 2022. The citation metric for the extracted data from the SCOPUS database was determined using Harzing's Publish or Perish software. The summary comprises the overall number of citations, as well as the number of citations per year, paper, and author.

Table 10. Citations Metrics

Metrics	**Data**
Papers	220
Number of Citations	4411
Years	22
Citations per Year	200.5
Citations per Paper	20.05
Cites_Author	1350.46
Papers_Author	80.29
Authors_Paper	3.17
h_index	25
g_index	62

3.11 Highly Cited Articles

Table 11 shows that the most cited article by A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu (2018) received 1449 citations (362.25 citations per year) in the SCOPUS database. Table 8 lists the most productive authors in the field of 'Stepping-stone Attacks.' However, the article with the highest citations was not even written by the authors listed in table 8. The number of citations does not correspond to the number of publications. As a result, a researcher should have strategies in place to increase the visibility and impact of their research before and after publication.

Table 11. Top 20 Highly cited articles

No.	**Authors**	**Title**	**Year**	**Cites**	**Cites per Year**
1	A. Madry, A. Makelov, L. Schmidt, D. Tsipras, A. Vladu	Towards deep learning models resistant to adversarial attacks	2018	1449	362.25
2	Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-	Experimental measurement-device-independent quantum key distribution	2013	294	32.67

	L. Liu, L. Li, X. Ma, J.S. Pelc, M.M. Fejer, C.-Z. Peng, Q. Zhang, J.-W. Pan				
3	Y. Zhang, V. Paxson	Detecting stepping-stones	2000	281	12.77
4	X. Wang, D.S. Reeves	Robust correlation of encrypted attack traffic through stepping-stones by manipulation of interpacket delays	2003	186	9.79
5	P. Peng, P. Ning, D.S. Reeves	On the secrecy of timing-based active watermarking trace-back techniques	2006	113	7.06
6	K.L. Chiew, K.S.C. Yong, C.L. Tan	A survey of phishing attacks: Their types, vectors and technical approaches	2018	112	28
7	D.L. Donoho, A.G. Flesia, U. Shankar, V. Paxson, J. Coit, S. Staniford	Multiscale stepping-stone detection: Detecting pairs of jittered interactive streams by exploiting maximum tolerable delay	2002	99	4.95
8	X. Wang, D.S. Reeves, S. Felix Wu	Inter-packet delay based correlation for tracing encrypted connections through stepping-stones	2002	85	4.25
9	D. Rupprecht, K. Kohls, T. Holz, C. Popper	Breaking LTE on Layer Two	2019	77	25.67
10	A. Blum, D. Song, S. Venkataraman	Detection of interactive stepping-stones: Algorithms and confidence bounds	2004	75	4.17
11	N. Kiyavash, A. Houmansadr, N. Borisov	Multi-flow attacks against network flow watermarking schemes	2008	67	4.79
12	T. He, L. Tong	Detecting encrypted stepping-stone connections	2007	57	3.8
13	K.H. Yung	Detecting long connection chains of interactive terminal sessions	2002	43	2.15
14	J. Yang, S.-H.S. Huang	Matching TCP packets and its application to the detection of long connection chains on the Internet	2005	40	2.35
15	D. Ramsbrock, X. Wang, X. Jiang	A first step towards live botmaster traceback	2008	37	2.64
16	P. Peng, P. Ning, D.S. Reeves, X. Wang	Active timing-based correlation of perturbed traffic flows with chaff packets	2005	36	2.12
17	J. Yang, S.-H.S. Huang	A real-time algorithm to detect long connection chains of interactive terminal sessions	2004	36	2
18	W. Diao, X. Liu, Z. Li, K. Zhang	No Pardon for the Interruption: New Inference Attacks on Android Through Interrupt Timing Analysis	2016	34	5.67
19	L. Zhang, A.G. Persaud, A. Johnson, Y. Guan	Detection of stepping-stone attack under delay and chaff perturbations	2006	32	2
20	M. Chatterjee, A.S. Namin	Detecting phishing websites through deep reinforcement learning	2019	30	10

3.12 Top Keywords

Table 12 displays the top keywords that emerged from the bibliometric search. Based on the number of occurrences, keywords such as Stepping-stone, Network Security, and Intrusion Detection are found to be the most used keywords in the analysis of stepping-stone attacks.' Table 12 shows the top keywords used in the stepping-stone attacks' study's analysis.

Table 12. Top Keywords

Author Keywords	Total Publications (TP)	Percentage (%)
Stepping-stone	98	44.55%
Network Security	70	31.82%
Intrusion Detection	66	30.00%
Computer Crime	37	16.82%
Connection Chain	29	13.18%
Algorithms	27	12.27%
Security Of Data	24	10.91%
Packet Networks	23	10.45%
Watermarking	23	10.45%
Internet	19	8.64%
Stepping-stones	19	8.64%
Stepping-stone	19	8.64%
Internet Protocols	18	8.18%
Cryptography	16	7.27%
Traceback	16	7.27%
Round-trip Time	14	6.36%
False Positive Rates	13	5.91%
Computer Networks	12	5.45%

IV. DISCUSSION AND CONCLUSION

The trend of investigation on 'stepping-stone attacks' is studied in this research by employing a bibliometric analysis method. The productivity of research and publications in a specific area can be assessed using bibliometric analysis. Information obtained through bibliometric methods is becoming increasingly important in search evaluation. The bibliometric analysis provides an overview and adds to knowledge about the literature in a specific field [3]. Furthermore, the results of the bibliometric analysis can assist academicians in producing relevant and up-to-date research by highlighting the important area that needs to be addressed [3]. Based on the significance of stepping-stone attacks as a type of cybercrime in networks, this study focused on stepping-stone attack publication data gathered from the Scopus database.

Since 2002, there has been a significant increase in the number of publications in this field. This study also reveals that more authors from different countries collaborate each year, indicating that the importance of social media is spreading across different regions. According to the findings, English is the primary language used in 98.64% of research papers, and more than half of them (54.09%) are published in conference proceedings. The remaining papers (29.09%) were published in academic journals, book series (14.55%), books (1.82%), and trade journals (0.45%). The citation metric, as shown in Table 10, can be used to assess the impact of a publication. Based on nearly 22 years of publications (from 2000 to September 2022), 220 papers were produced by researchers worldwide, with a total of 4411 citations. The topic generated 200.5 citations on average, with each paper being cited 20.05 times.

While the Scopus database is one of the largest databases that index academic literature across many disciplines, other databases such as Web of Science and Google Scholar can be included in the search query. If the search query is run on all available academic databases, the results will be more comprehensive and provide more insights. Despite the limitations of the search database, this study presents an intriguing trend on 'stepping-stone attacks' research up to September 2022. By utilising the bibliometric approach, this study also contributes to the expansion of the body of knowledge in stepping-stone attacks' literature.

REFERENCES

[1]. Almulhem, A. and I. Traore, I (2007) "A survey of connection-chains detection techniques" IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, 2007 (PacRim 2007), Pp. 219–222.

[2]. Crescenzo, G. D., Ghosh, A., Kampasi, A., Talpade, R.and Zhang, Y. (2011) "Detecting anomalies in active insider stepping stone attacks" Journal of Wireless Mobile Networks, Ubiquitous Computing Dependable Applications, Vol. 2, No. 1 Pp. 103–120.

[3]. Ellegaard, O., and Wallin, J. A. (2015) "The bibliometric analysis of scholarly production: How great is the impact?" Scientometrics, 105(3), 1809-1831. DOI 10.1007/s11192-015-1645-z

[4]. Huang, S. H. S., Zhang, H. and Phay, M. (2016) "Detecting stepping-stone intruders by identifying crossover packets in SSH connections" Proceedings of the International Conference on Advanced Information Networking and Applications (AINA) Pp. 1043–1050.

[5]. Lin, Z. and Hopper, N. (2012) "New Attacks on Timing-based Network Flow Watermarks" Proceedings of the 21st USENIX Conference on Security Symposium.

[6]. Kumar, R.and Gupta, B. B. (2016) "Stepping stone detection techniques: Classification and state-of-the-art" Proceedings of the international conference on recent cognizance in wireless communication & image processing Pp. 523–533.

[7]. Kuo, Y. (2011) "Algorithms to detect stepping-stone intrusions in the presence of evasion techniques," (Doctoral dissertation), Availabe from ProQuest Dissertations and Theses database (UMI No. 3492359).
[8]. Omar, M. N., Amphawan, A. and Din, R. (2012) "Evolution of Stepping Stone Detection and Emerging Applications," Advances in Remote Sensing, Finite Differences and Information Security Pp. 199–205.
[9]. Staniford-Chen, S. and Heberlein, L. T. (1995) "Holding intruders accountable on the internet," Security and Privacy, 1995, Pp. 39–49.
[10]. Temperton, M. B. J. (2016) "The security flaws at the heart of the Panama Papers" wired.co.uk.
[11]. Wang, X., Luo, J. and Yang, M. (2012) "An efficient sequential watermark detection model for tracing network attack flows," in Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design Pp. 236–243.
[12]. Yang, J., Zhang, Y. and Zhao, G. (2017) "Integrate stepping-stone intrusion detection technique into cybersecurity curriculum" Proceedings of 31st IEEE Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA Pp. 1–6.
[13]. Zakaria, R., Ahmi, A., Ahmad, A. H., & Othman, Z. (2020) Worldwide melatonin research: A bibliometric analysis of the published literature between 2015 and 2019, *Chronobiology International*. https://doi.org/10.1080/07420528.2020.1838534