SLIS Connecting

Volume 10 | Issue 2 Article 8

2021

Ransomware: A Bibliometric Research Study

Allyce Andrew Sears, MLIS

Recommended Citation

Allyce Andrew Sears, MLIS (2021) "Ransomware: A Bibliometric Research Study," *SLIS Connecting*: Vol. 10 : Iss. 2 , Article 8.
DOI: 10.18785/slis.1002.08
Available at: https://aquila.usm.edu/slisconnecting/vol10/iss2/8

Ransomware: A Bibliometric Research Study

By Allyce Andrew Sears

Master's Project, December 2021
Readers: Dr. Stacy Creel, Dr. Xinyu Mills

INTRODUCTION

Malware based information and identity-related attacks in the virtual realm are on the rise on an institutional and individual level in the United States and abroad (Alwan, 2019; Jeffery & Ramachandran, 2021; Slayton, 2018). Ransomware is one of the fastest growing malware threats to cyber security and should be studied and monitored in order to mitigate the threat (Alwan, 2019; Slayton, 2018; Veresha, 2018). This threat is especially relevant to Library and Information Science (LIS) professionals whose duties and patrons are permanently entangled in increasingly digitized spaces and platforms (Rubin & Rubin, 2020). This research employed a bibliometric, literature mapping method to investigate core authors, core journals and publishing data regarding ransomware located in technology and LIS-focused databases over the course of 2010 to 2020. The intent of this study was to gather and analyze data of published scholarly literature regarding ransomware in order to share this knowledge with LIS professionals for their own use and education.

Purpose Statement

The purpose of this research is to track publication data and the potential rise in ransomware literature located in scholarly journals over the last decade (2010-2020).

Research Questions

R1. Has scholarly literature around ransomware increased over the last 10 years (2010-2020)?

R2. Which journals have published the most literature on this topic between 2010 and 2020?

R3. Which authors have published the most literature on this topic between 2010 and 2020?

Definitions

Ransomware: "A type of malicious software designed to block access to applications or files on a computer system until a sum of money is paid" (OED, n.d.-a).

Malware: "Programs written with the intent of being disruptive or damaging to (the user of) a computer or other electronic device; viruses, worms, spyware, etc., collectively" (OED, n.d.-b).

Bibliometrics: "According to ODLIS, bibliometrics is: 'To analyze the historical development of a specific body of literature, especially its authorship, publication and use'" (Mangrum, 2021).

Bradford's Law: "'The bibliometric principle that a disproportionate share of the significant research results on a given subject are published in a relatively small number of scholarly journals in the field' (ODLIS)" (Mangrum, 2021).

Lotka's Law: "'The bibliometric principle that most authors will contribute only one article to the scholarly literature on a given subject or in a given field' (ODLIS)" (Mangrum, 2021).

Delimitations

The resources collected for this bibliometric study were limited by a few factors. The following databases were consulted due to their academic, technology and LIS-related content: Academic Search Premier; Computer Source; Computers & Applied Sciences Complete; Information Science & Technology Abstracts (ISTA); Library & Information Science Source; and Library, Information Science & Technology Abstracts. Only peer-reviewed, full-text and English-language articles published on the subject of ransomware between 2010 to 2020 were collected. Any duplicate articles were deleted. This bibliometric research sought information specific to "ransomware" instead of "malware" within these databases in order to take a closer look at this specific type of developing cyberthreat. Additionally, as ransomware first appeared in 1989, important information might be excluded from the study by focusing on the ten-year span of 2010 to 2020.

Assumptions

It was assumed that the consulted databases were properly indexed so that the appropriate articles were

collected for the research topic as the search was completed. Consequently, it was assumed that the advanced search options and the utilized keyword during the search process produced pertinent and accurate results within these databases.

Importance of Study

A plethora of published information exists regarding malware, but the prolific rise in ransomware attacks warranted a closer look at this specific type of cyberattack (Slayton, 2018). LIS professionals and the patrons they serve are vulnerable to ransomware attacks, as they are both the disseminators and consumers of information in an increasingly virtual capacity. Literature on this topic should be collected and shared to ensure that LIS employees have access to the information they need to educate themselves and the public regarding this threat (Rubin & Rubin, 2020). This collection and study of ransomware data found on academic, technology-focused and library and information-centered databases was intended to research if literature published on ransomware has increase over the last ten years. This study also intended to seek out core publications and authors who have published works on ransomware within these databases. The importance of the study is that it will add to the body of scholarly LIS literature, and it may be useful for providing insight into data regarding ransomware literature among scholarly publications.

LITERATURE REVIEW

As technology progresses rapidly, so do cybersecurity threats. Veresha (2018) states that, "Cybercrime is a combination of information, financial and personal security threats" (p.189). Cybercrime acts are often completed through malware, which are invasive computer viruses, worms, spyware and other nefarious programs (Guo, Cheng, & Kelley, 2016). One of the greatest, modern malware threats is ransomware, which the United States Department of Justice called the "fastest growing malware threat" in 2016 (Slayton, 2018, p.293).

Allen (2017) defines ransomware as, "the kidnapping of data or access to equipment by locking out those with legitimate access rights and then offering to sell them a key to accessing it for a fee, effectively kidnapping the access and holding it for ransom" (p.65). A synonym for this type of malware might be cyber extortion and the three main results of this malware are threatening emails, locked computer screens or encrypted files (Ali, 2017; Allen, 2017). Once the ransomware threat has been made known to the computer user, the cybercriminal will demand a ransom, or payment, for the release of their files. Cybercriminals seek cryptocurrency payments through digital currencies like Bitcoin, which protect the anonymity of their identities (Goldsborough, 2016).

This malware was first identified in 1989 (Slayton, 2018; Ali, 2017) and now, more than 400 types of ransomware threats exist (Goldsborough, 2017). Ransomware attacks affect millions of people a year and rose by 62 percent globally and by 158 percent in North America between 2019 and 2020 (Jeffery & Ramachandran, 2021). Ransomware does not just afflict everyday computer users, but cybercriminals target hospitals, metro systems, police departments and government entities (Allen, 2017). As a result of this growing threat, the Department of Defense requested nearly $4 billion in 2020 for fighting and preventing cybercrime (Musielewicz, 2020). Cybercriminals are at an advantage because modern technology users in the United States lack the skills and infrastructure needed on an individual and governmental level to protect themselves from ransomware attacks (Alwan, 2019; Musielewicz, 2020). Alwan (2019) cited a study that showed that, "95 pervect of cybersecurity breaches are due to human errors" (p.70).

Ransomware may be installed on a computer from software downloads or even unintentional advertisement clicks (Ali, 2017). Additionally, phishing, the use of fake emails containing links that collect login information and credentials, is a common type of ransomware threat (Alwan, 2019). Veresha (2018) states, "technology by itself cannot guarantee security in the sphere of information exchange within cyberspace" — it is ultimately up to the individual technology-user to prevent crime (p.196). Ways in which individuals and institutions might protect themselves from ransomware attacks are by malware identification training, utilizing antivirus software, frequently backing up files, implementing password protection measures and investing in new technology and computers that are less susceptible to these threats (Ali, 2017; Allen, 2017; Goldsborough, 2016).

Ransomware in Libraries

Everyday activities like emailing or using social media may lead to cybercrimes or privacy violations.

As libraries in the United States offer internet access to their patrons, LIS professionals must remain vigilant in educating themselves and the public about these threats while they provide and utilize public resources (Rubin & Rubin, 2020). The American Library Association (ALA) (2020) weighed in on this threat with the following statement: "Libraries should take appropriate steps to ensure that malware or other unauthorized software does not reside on the computer or device. These steps could include security protection (anti-malware, anti-spam, anti-virus programs) as well as restoration software to remove all software installed without authorization." Though the ALA's security recommendations are practical, cyberattack events have shown that anti-virus software is not always sufficient at preventing ransomware attacks (Pundsack, 2018).

An example of preventative cybersecurity that was not sufficient at blocking a ransomware attack occurred in 2018 at Spartanburg County Public Libraries (SCPL). SCPL had suffered a previous ransomware infection and reinforced its cybersecurity measures, which did not prevent a more "aggressive" form of ransomware from infecting its system through email. This infection "'went right through'" the library's antivirus protection defenses (Pundsack, 2018, p.23). The effects of this attack forced librarians to manually check out materials for days as they repaired the infected system. During the ransomware attack, patrons were not able to access the library's computers or certain digital services throughout all the library's eleven branches (Pundsack, 2018). St. Louis Public Libraries (SLPL) also suffered a ransomware attack in 2017, despite their preventative measures. SLPL identified the malware's entry point as, "a four-year-old voice mail server with an unpatched security vulnerability" (Enis, 2017, p.20). The effects of the SLPL attack were minimal due to the library's encrypted backup systems, so the library's catalog, website and virtual materials were safe from infection. This forethought allowed SLPL to restore their checkout system and public computer access days after the attack (Enis, 2017).

More than 400 types of ransomware exist (Goldsborough, 2017) and modern cybercriminals are offered a unique advantage when choosing to target a public institution, such as a public library, because their budgets are often made available as public knowledge. This provides the ransomware attacker the opportunity to tailor their chosen ransom-sum based on what they know the library will be able to pay. Regardless of whether a library is able to pay the ransom, the FBI urges libraries not to meet the attacker's demands because payment does not ensure that the criminals will unlock the encrypted files. The FBI also believes that refusing to pay the ransom might discourage future attacks. Both SCPL and SLPL did not pay the ransom, but reported the attack to the FBI and restored their systems via backups (Pundsack, 2018). Another example of a library that refused to pay the ransom is the Daviess County Public Library (DCPL). DCPL experienced a ransomware attack in 2019, where the attackers demanded $30,000 for file restoration. Rather than paying the ransom, DCPL utilized a similar sum of money to reinforce its cybersecurity measures, which included hiring outside assistance to evaluate the strength of its network protection. In the end, the DCPL library director described the attack as a "'blessing in disguise'" because it forced staff to increase their cybersecurity skills and malware prevention strategies (Mulliken, 2020, p.1).

If ceding to the attacker's demands and basic cybersecurity measures are not failproof ways to prevent ransomware attacks, then libraries must rely on collective experiences to prevent and mitigate ransomware cyberattacks. Ransomware extortion may result in weeks of disrupted library services and, as SCPL librarian Stephens states, '"the attacks are sophisticated and will continue to morph'" (Landgraf, 2018, p.21). Additionally, regarding ransomware attacks, Pundsack states, "It is not a matter of if, but when, your computers or library will see an attempt" (2018, p.23). As information professionals, a librarian's role includes providing free access to information (Pundsack, 2018) and, "In many cases public libraries are the only community provider of computer and internet services (ALA 2019c)" (Rubin & Rubin, 2020, p.440). With this in mind, librarians might view ransomware attacks as an attack on the core principles of their profession itself, which includes providing the ability for patrons to freely access and utilize information (Pundsack, 2018).

As mentioned above, libraries are vulnerable institutions to cyber extortion attacks due to the public nature of its yearly budget. Additional vulnerabilities of libraries stem from small budgets that do not allow for an institution to adequately defend its online resources, such as virtual catalogs or public computers. This lack of defense might lead to multiple

entry points for a cybercriminal (Caverly, 2021). Additionally, staff members untrained in cybersecurity best practices present an unopposed entryway for cybercriminals to enter a LIS-institution's system or network (Pundsack, 2018). As ransomware evolves, librarians and information professionals must educate themselves on this developing threat. Knowledge gleaned from LIS professionals who have experiences this type of malware extortion encourages librarians to complete nightly file backups on encrypted servers, train staff and volunteers to identify malware, update software often, and to develop a recovery plan in advance (Landgraf, 2018; Pundsack, 2018).

Similarities of Methodology

The scholarly articles mentioned in the literature review did not utilize bibliometric research methods. There was little information regarding bibliometric studies pertaining to ransomware, but there were studies that utilized bibliometric methods to monitor malware data. Garg, Sidhu and Rani (2019) utilized a bibliometric analysis to study cloud computing security. These researchers reviewed more than 15,000 works published between 2009 to 2018 and looked for publishing patterns, subject areas and countries in which the works were published. Similarly, Sardi et al. (2020) used bibliometric methods to track literature regarding cybersecurity threats to health care institutions. These researchers studied the publication data of 84 publications between the dates of 1995 to 2020 and found that the healthcare field lacks the research necessary to prevent and protect against cyberattacks in this industry.

Finally, Razak's study (2016) is the most similar to this completed research study as it tracks the data of malware in general using bibliometric methods. Razak's work offered insight into core authors and core journals from 4,000 collected articles that were published between 2005 to 2015. This research utilized a similar time frame and also studied publishing data, but worked with a significantly smaller amount of data than most of the abovementioned articles. Additionally, all of the previously mentioned bibliometric studies sought to identify research regarding publishing data around the broader topic of malware. Meanwhile, this study focused explicitly on ransomware and how this growing malware threat corresponds with potential increases in scholarly literature on this topic. Though research regarding malware in general is useful, focusing on ransomware specifically is important as other cyberthreats like credit card fraud and identity theft are being phased out in favor of this new form of crime (Allen, 2017). Literature that is specifically published on the topic of ransomware is valuable to gather and share in order to support LIS professionals with their awareness and education on this type of cybercrime, as it is their duty to ensure patron privacy and protection.

METHODOLOGY

Information Sources and Procedures

The methodology was a quantitative, bibliometric study using literature mapping methods. The following databases were accessed through the University of Southern Mississippi's library: Academic Search Premier; Computer Source; Computers & Applied Sciences Complete; Information Science & Technology Abstracts (ISTA); Library & Information Science Source; and Library, Information Science & Technology Abstracts. These databases were selected in order to collect academic, technology and LIS-specific publication information regarding ransomware. Ransomware uses similar cyber-attacking methods to target individuals, governments and corporations. Consequently, information garnered from a ransomware attack or study related to an institution or entity outside of the LIS field would still be useful to consider while studying this threat (Alwan, 2019).

During the data collection, the Boolean/Phrase advanced search option was used to search for "ransomware." The results were refined and limited to only show "Peer Reviewed," "Full Text," English-language articles that were published between the dates of 2010-2020. Once the search was completed, the obtained articles were organized chronologically by selecting the "Date Newest" organization-option to allow for a linear collection of data from the databases. Each database was searched individually, and the resulting data were collected into a Microsoft Excel spreadsheet. The collected data were stored in the spreadsheet and were used to search for core publications, core authors and to identify whether there is an increase in literature on this topic over the course of the ten-year research span. The results were copied and pasted in the spreadsheet as newest to oldest articles from the individual database results and were organized in various ways to study the data. The information inputted in the Excel spreadsheet included

the article titles, author names, years of publication and journal names. Duplicate article information was identified and deleted after the data collection was completed. A Microsoft Word document was utilized to track applicable research data. A copy of the Excel spreadsheet that contained the unedited, initial results was created.

Limitations

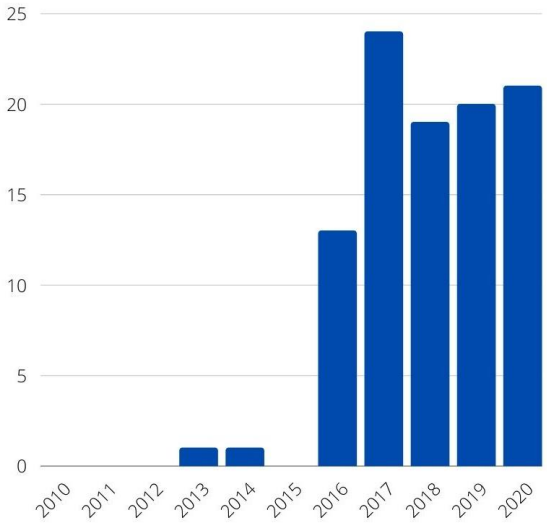
It was understood that searching across multiple databases individually was a risk due to an increased potential for inputting error, location of duplicate results or the retrieval of irrelevant results pertaining to ransomware. It was also understood that ransomware falls under the umbrella of malware, so some relevant texts that reference ransomware but primarily focus on malware might have been left out of the results due to database indexing. The results of this bibliometric research cannot be generalized.

RESULTS

R1. Has scholarly literature around ransomware increased over the last 10 years (2010-2020)?

The methodology resulted in 129 returns for peer-reviewed, full-text, English-language articles that were published between the dates of 2010-2020 on the topic of ransomware. Once duplicate articles and an early edition of a duplicate published work were deleted, 99 results were identified. Among the 99 results, the following data were found (Figure 1): 0 articles were published in 2010, 2011, 2012, and 2015; 1 article was published in 2013; 1 article was published in 2014; 13 articles were published in 2016; 24 articles were published in 2017; 19 articles were published in 2018; 20 articles were published in 2019; and 21 articles were published in 2020. Sixty percent of the articles (60%) were published in the last three years of the study.

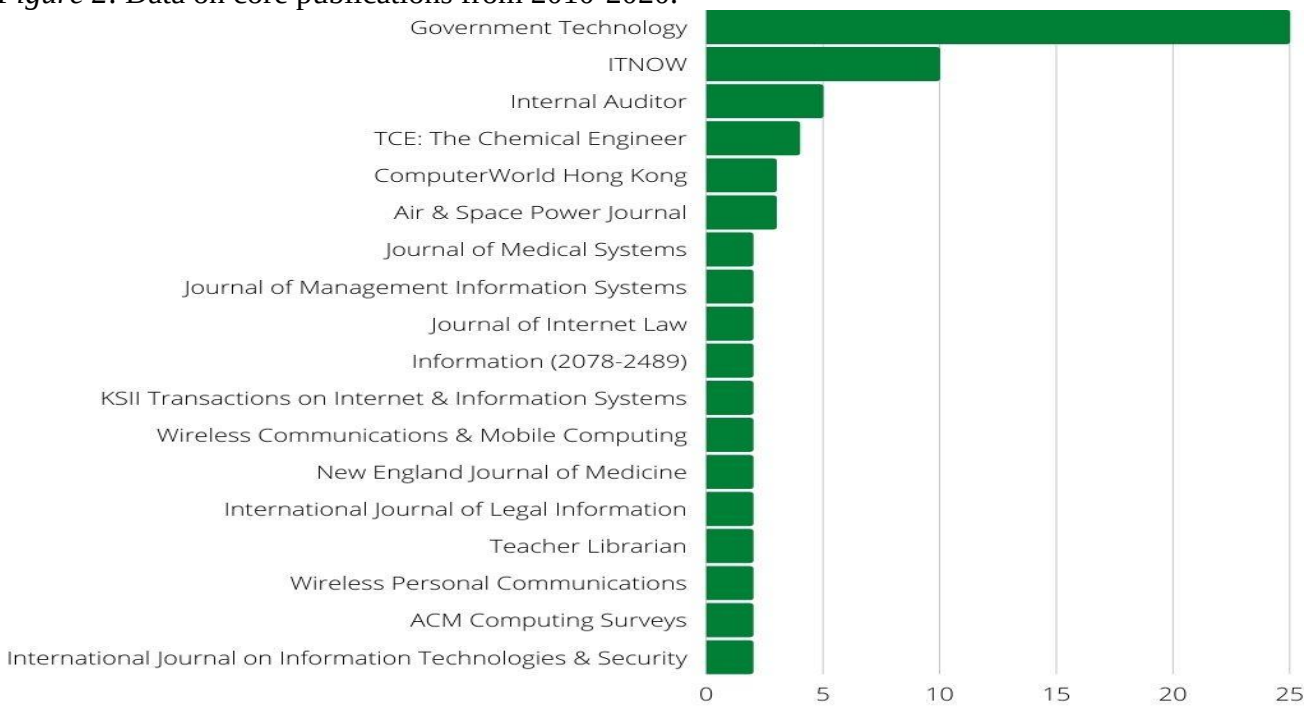
Figure 1: Data on the 99 peer-reviewed, full-text, English-language published works on ransomware from 2010-2020.



R2. Which journals have published the most literature on this topic between 2010 and 2020?

Among the 99 articles, the following data were found (Figure 2): The most prolific publication was *Government Technology* with 25 published articles, or 25 percent of the total publication results. This prolific publication was followed by *ITNOW* with 10 published articles (10%), *Internal Auditor* with 5 published articles (5%), *TCE: The Chemical Engineer* with 4 published articles (4%), *ComputerWorld Hong Kong* with 3 published articles (3%) and *Air & Space Power Journal* with 3 published articles (3%). The following publications were the last of the core journals and each published 2 articles located in the data, which each accounted for 2 percent of the publications: *Journal of Medical Systems*; *Journal of Management Information Systems*; *Journal of Internet Law*; *Information (2078-2489)*; *KSII Transactions on Internet & Information Systems; Wireless Communications & Mobile Computing*; *New England Journal of Medicine*; *International Journal of Legal Information*; *Teacher Librarian*; *Wireless Personal Communications*; *ACM Computing Surveys*; and *International Journal on Information Technologies & Security*.

Figure 2: Data on core publications from 2010-2020.



R3. Which authors have published the most literature on this topic between 2010 and 2020?

The following data results were found (Figure 3): *Government Technology* was the most prolific author with 7 citations, which accounted for 7 percent of the collected, publication data. This prolific author was followed by Newcombe, Tod and *TCE: The Chemical Engineer* with 4 citations each (4% each). Next, Castro, Daniel and Onag, Gigi accounted for 3 citations each (3% each). The last of the core authors who accounted for 2 citations each, and each represented 2 percent of the collected, publication data, were: Mitchell, John; Piper, Arthur; Goldsborough, Reid; Alwan, Hala Bou; Zimba, Aaron; Knell, Noelle; and Mulenga, Mwenge (Appendix A).

Figure 3: Data on core authors from 2010-2020.

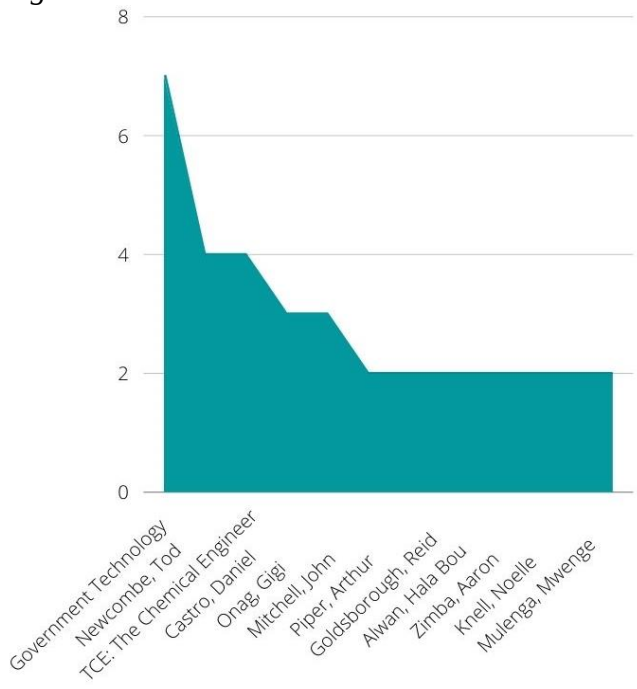


Figure 4: Data on publication results from 2010-2020.

DISCUSSION

The data collected in this bibliometric research offered interesting insight into ransomware literature published on academic, LIS and technology-related databases. The results collected from the databases, depicted in Figure 4, were as follows: 78 retrieved publication results from Computers & Applied Sciences Complete; 32 publications retrieved from Academic Search Premier; 8 from Library & Information Science Source; 6 from Computer Source; 4 from Library, Information Science & Technology Abstracts; and 1 from Information Science & Technology Abstracts (ISTA). A total of 129 results were collected and 30 duplicate articles were identified and deleted. One duplicate article that was removed was a 2019 early-edition draft of a scholarly article, which was also collected as a formally published piece in 2020. Once the duplicate articles were deleted, the data were studied in relation to the research questions. Libraries have been warned and educated on the dangers of ransomware attacks through resources like Public Libraries Online in 2017 and 2021 (Caverly, 2021; Lambert, 2017). From South Carolina to Indiana to Tennessee to Missouri to Pennsylvania, libraries have been the victims of ransomware (Landgraf, 2018). Yet these results, indicate that scholars in the Library and Information Science field are not researching and publishing as frequently on this topic.

Regarding whether published, scholarly material has increased from 2010-2020, the data indicate growth. This growth is apparent as 0 results were retrieved from the years 2010, 2011, 2012 and 2015. Besides the years with no results, the years with the smallest number of retrieved results were 2013 and 2014 with 1 retrieved result each among the six databases. The retrieved data increased to 13 articles published during 2016 and 24 in 2017. It is noteworthy that the data collected across the databases decreased in 2018 to 19, but began to increase again in 2019 with 20 retrieved results and in 2020 with 21 publications' data retrieved. The growth shown is not completely linear, but does reflect an overall increase, as 60 percent of the retrieved articles were published in the last three years of the study.

Core publication data were retrieved as expected, but potential inconsistencies were noted as the data were analyzed. The prolific core-publication with the most published data collected was *Government Technology*, which was followed by a majority of medical, technology and industry journals. The data show that multiple information-related journals were present among the core publications, but the only library-specific focused journal that might be considered a core publication based on the data was *Teacher Librarian*, with 2 collected published works. This disproportionate representation of other industries and institutions, including the information sector of the LIS field, compared to the data retrieved that were specific to libraries is represented in the database collection information. For example, the databases Library & Information Science Source and Library, Information Science & Technology Abstracts produced few results compared to technology or academic-focused databases like Computers & Applied Sciences Complete and Academic Search Premier. Additionally, the potential inconsistency noted in the results was related to the retrieval of the separate results ACM Computing Surveys, ACM Transactions on Embedded Computing Systems and ACM Transactions on Privacy & Security. ACM stands for the Association of Computer Machinery and these retrieved publications are separate journals published under the ACM umbrella (ACM, 2021). As

the journals are separate publications, they were not counted as the same publication when core publications data were considered. The data appeared consistent with the bibliometric principle of Bradford's Law. The data show that Bradford's Law appeared accurate within the results of the ten-year research span, as only 18 core publications were identified in the data. These core publications reflected 18 percent of the publication data. Among these 18 core journals, 6 publications were noteworthy as their published works on ransomware included more than 2 article publications.

Core author data produced noteworthy results. The prolific author was *Government Technology* with 7 publishing citations. *TCE: The Chemical Engineer* represented another core author that was also published under the moniker of a journal. The retrieved results that attributed a journal title in lieu of an author's name were manually checked for accuracy during data collection. The databases appeared to be accurate in nearly all instances, though two authors were identified in this process that were not properly indexed. These authors were Darryl Booth, who was only indexed as the *Journal of Environmental Health*, and Karl Henderson, who was only indexed as *Chemistry & Industry*. These errors were fixed during the data input process, but these authors were not core authors. Additionally, the author Gigi Onag was not properly indexed for their *ComputerWorld* Hong Kong published works. As the data were analyzed, it was noticed that this author's name was improperly indexed as "Gigi Onag" on one occasion. Gigi Onag is a core author and their identified published works increased from 2 to 3 after this inconsistency was mitigated. Lotka's Law also appeared to be consistent with the data results, as only 12 core authors were identified within the 99 publication results, which represented 12 percent of the publication data. Additionally, two of these prolific authors were indexed as journals, so the true nature of the core author data might only include 10 authors who contributed two or more pieces of literature among the 99 scholarly article results. Regardless of whether the abovementioned modifications to the results are made to determine additional core publication and author information, Bradford's Law and Lotka's Law were supported within these results. This was shown in the data, which revealed that less than one third of the data's journals and authors represented the core publishing results.

CONCLUSION

If Pundsack (2018) is correct in their statement that ransomware attacks on libraries are not a matter if, but when, then the lack of published data regarding ransomware from library-focused journals is noteworthy. The data indicate that other industries and institutions steeped in technology and information usage, i.e. computer, technology, government and medical fields, are publishing peer-reviewed journals on the topic of ransomware. Overall, the data also show that this published information is increasing, though with some publishing setbacks. Information-related journals are publishing works on ransomware, but the lack of published information from a library-specific perspective might present concerns in the future, especially if the risks of experiencing a ransomware attack are as dire as the United States Department of Justice believes it to be (Slayton, 2018). As ransomware attacks rise, a librarian's ability to effectively serve patrons and keep their institution running might be hindered by this form of malware, so an increased, scholarly focus on this threat might be necessary (Alwan, 2019; Enis, 2017; Pundsack, 2018).

The results of this study only offer a brief glimpse into the data of ransomware publishing information. Future researchers might consider replicating this study with a few key modifications. One modification might involve including 2021 in the research parameters. An additional modification might include consulting more databases during research. Finally, a future researcher might benefit from eschewing the boundary of this study, which only researched publication data regarding ransomware. Studying malware in general, especially from LIS-focused database, would offer an additional perspective regarding LIS institutions' overall response to malware.

REFERENCES

ACM. (2021). *ACM Journals*. ACM: https://dl.acm.org/journals.

ALA. (2020). *Library privacy guidelines for public access computers and networks*. ALA: https://www.ala.org/advocacy/privacy/guidelines/public-access-computer.

Ali, A. (2017). Ransomware: A research and a personal case study of dealing with this nasty

malware. *Issues in Informing Science & Information Technology*, 14, 87–99.

Allen, J. (2017). Surviving ransomware. *American Journal of Family Law*, 31(2), 65–68.

Alwan, H. B. (2019). National cyber governance awareness policy and framework. *International Journal of Legal Information*, 47(2), 70–89.

Caverly, W. (2021). *Ransomware attacks at libraries: How they happen, what to do*. Public Libraries Online: http://publiclibrariesonline.org/2021/05/ransomware-attacks-at-libraries-how-they-happen-what-to-do/.

Enis, M. (2017) Ransomware hits govt., libraries. *Library Journal*, 142(8), 19-20.

Garg, D., Sidhu, J., & Rani, S. (2019). Emerging trends in cloud computing security: A bibliometric analyses. *IET Software*, 13(3), 223–231. https://doi.org/10.1049/iet-sen.2018.5222.

Goldsborough, R. (2016). Protecting yourself from ransomware. *Teacher Librarian*, 43(4), 70–71.

Goldsborough, R. (2017). The increasing threat of ransomware. *Teacher Librarian*, 45(1), 61.

Guo, H., Cheng, H. K., & Kelley, K. (2016). Impact of network structure on malware propagation: A growth curve perspective. *Journal of Management Information Systems*, 33(1), 296–325.

Jeffery, L. & Ramachandran, V. (2021). *Why ransomware attacks are on the rise — and what can be done to stop them*. PBS: https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them.

Lambert, T. (2017). *Protecting your Library from ransomware.* Public Libraries Online: http://publiclibrariesonline.org/2017/03/protecting-your-library-from-ransomware/.

Landgraf, G. (2018). When ransomware attacks: How three libraries handled cyberextortion. *American Libraries*, 49(6), 20–23.

Mangrum, S. (2021). *Bibliometric Methods* [PowerPoint slides]. School of Library and Information Science, University of Southern Mississippi. https://usm.instructure.com/courses/61465/files/5700696?module_item_id=2121865.

Mulliken, J. (2020). Library officials confident post ransomware attack. *TCA Regional News*.

Musielewicz, D. (2020). The spectrum of cyber attack. *Air & Space Power Journal*, 34(4), 91–100.

OED. (n.d.-a). *ransomware.* OED.

OED. (n.d.-b). *malware*. OED.

Pundsack, K. (2018). Ransomware at the library: Time to boost your cybersecurity. *Public Libraries*, 57(4), 23–25.

Razak, M.F.A. (2016). The rise of "malware": Bibliometric analysis of malware study. *Journal of Network and Computer Applications*, 58–76.

Rubin, R., & Rubin, R. (2020). *Foundations of library and information science, fifth edition* (5th ed.). ALA Neal-Schuman.

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. *Sustainability* (Basel, Switzerland), 12(17), 7002–. https://doi.org/10.3390/su12177002.

Slayton, T. B. (2018). Ransomware: The virus attacking the healthcare industry. *Journal of Legal Medicine*, 38(2), 287–311.

Veresha, R. V. (2018). Preventive measures against computer related crimes: Approaching an individual. *Informatologia*, 51(3/4), 189–199.