European Journal of Internal Medicine xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

European Journal of Internal Medicine

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

Review Article

Current and potential cyber attacks on medical journals; guidelines for improving security

Mehdi Dadkhah [a,*], Seyed Amin Hosseini Seno [b,**], Glenn Borchardt [c]

[a] Department of Management, Faculty of Economics and Administrative Sciences, Ferdowsi University of Mashhad, Mashhad, Iran
[b] Department of Computer Engineering, Ferdowsi University of Mashhad, Mashhad, Iran
[c] Progressive Science Institute, Box 5335, Berkeley, CA 94705, USA

ARTICLE INFO

Article history:
Received 22 November 2016
Received in revised form 25 November 2016
Accepted 28 November 2016
Available online xxxx

Keywords:
Academic journals
Predatory journals
Hijacked journals
Journals' websites
Information security

ABSTRACT

At the moment, scholarly publishing is faced with much academic misconduct and threats such as predatory journals, hijacked journals, phishing, and other scams. In response, we have been discussing this misconduct and trying to increase the awareness of researchers, but it seems that there is a lack of research that presents guidelines for editors to help them protect themselves against these threats. It seems that information security is missing in some parts of scholarly publishing that particularly involves medical journals. In this paper, we explain different types of cyber-attacks that especially threaten editors and academic journals. We then explain the details involved in each type of attack. Finally, we present general guidelines for detection and prevention of the attacks. In some cases, we use small experiments to show that our claim is true. Finally, we conclude the paper with a prioritization of these attacks.

1. Introduction

In the past, journals were only available in the print version and only certain regions could access them. Today, we are faced with a new type of scholarly publishing. The use of web technologies and the internet along with open access policies has removed boundaries to scientific publishing. People all over the world can access academic journals [1]. When we use web technologies, we must consider information security and possible web attacks. As recent post published in the Retraction Watch blog concerns the hacking of a medical publisher and the resulting publication of about 65 papers by cybercriminals [2]. After a while, the publisher detected the attack and retracted these papers. With the growth of open access since 2002, scholarly publishing entered a new age [3–4]. Open access, especially gold open access, has created concerns, along with advantages. In gold open access, authors pay open access charges for their papers to be freely accessible for all readers [5]. But this creates an issue; a journal that doesn't respect academic publishing ethics can earn more money by publishing more papers. In early 2009, low quality journals started to call for papers (CFP) by sending emails to authors. They introduced themselves as fast peer review journals that use open access policies. These journals had flaws in the procedures used for reviewing and publishing papers. Most seemed only interested in making a profit. Jeffrey Beall, a librarian at the University of Colorado, started to collect these CFP emails and coined the term "predatory journals" in 2010 [6]. He also presented criteria for detecting predatory journals [6]. After Beall, various researchers all over the world started to inspect these journals in their related domains and published articles to increase awareness about this issue. They concluded that predatory journals would lead to plagiarism, increase pseudoscience, and spawn all sorts of academic misconduct [7–9]. Today, predatory journals are still multiplying and spreading. Academicians receive numerous CFP emails offering quick and easy publishing [10]; it seems that the issue of predatory journals continues to plague legitimate academic publishing.

In early 2011, a new type of academic misconduct came into existence. Cybercriminals registered an expired domain "http://sciencerecord.com" and began mimicking three reputable journals, creating a fake website for each of them. They used "Science and Nature", "Innova Ciencia", and "Science Series", presenting their fraudulent websites as the authentic websites of these journals [11]. Abusing the gold open access model, cybercriminals defrauded authors of money for publishing papers in their fake journals. Mehrdad Jalalian, an e-Physician editor, is the first academician to describe the systematic process used to "hijack" journals. Mehrdad coined the term "hijacked journals" in his study of academic societies. In journal hijacking, cybercriminals search for indexed journals that have only a print version or published papers in a non-English language. They then create a website and mimic that non-English journal. In other words, they

* Correspondence to: M. Dadkhah, Department of management, Faculty of Economics and Administrative Sciences, Ferdowsi University of Mashhad, Mashhad 9177948951, Iran.
** Correspondence to: S.A.H. Seno, Department of Computer Engineering, Ferdowsi University of Mashhad, Mashhad 9177948951, Iran.
E-mail addresses: Mehdidadkhah@mail.um.ac.ir (M. Dadkhah), hosseini@um.ac.ir (S.A.H. Seno).

http://dx.doi.org/10.1016/j.ejim.2016.11.014
0953-6205/

present their fake website as the authentic website of a reputable journal, receiving money from authors for publishing their papers [11]. It seems that scholarly publishing is faced with yet another new issue related to information security that needs a solution. These issues threaten medical and medicine journals more than others, because any fake or non-peer reviewed papers will be used by others and may threaten the well-being of patients.

2. Literature review

As mention in the previous section, researchers in different domains started to do research about the problem of predatory journals. They began a discussion about the negative effects of these fake journals on science, also recommending some guidelines for detecting such journals [7–9,12]. There is other research on hijacked journals. Some of this research focuses on the evaluation of journal quality and points out the questionable quality of most hijacked journals [13]. Academicians such as Fisher discuss non-peer reviewed papers and blame hijacked journals as the source for invalid papers [14]. Some papers present techniques or guidelines for authors to detect hijacked journals or present a list of detected hijacked journals. The researchers try to increase awareness of authors by showing the differences between journals' authentic websites and hijacked ones [11,15–16]. There are editorials and papers that focus on hijacked journals in specific disciplines such as medicine and point out the relevant issues [17–18]. Most papers about hijacked journals use non-technical language to appeal to a general audience. But there are also some papers that use a more technical view to examine hijacked journals. Those researchers try to detect hijacked journals by analyzing their domain information and servers [19–20]. In 2015, a new type of hijacked journal emerged. In this type of journal hijacking, cybercriminals try to gain control of a journal's authentic website. A published paper in Science by Bohannon stated that cybercriminals had gained control of about 20 authentic websites of reputable journals [21]. The names of these hijacked journals were available in Thomson Reuters master list along with their hijacked URLs.

All mentioned research on hijacked journals focuses on describing such journals or trying to present general guidelines for authors to detect and prevent submitting papers to them. It seems that editors have been forgotten in the discussion of this issue. How can editors of legitimate journals protect their work? Are detection techniques sufficient to solve the growing problem of hijacked journals? Are hijacked journals, predatory publishers, and other cybercrimes only problems for authors? There is a popular expression in medicine, “an ounce of prevention is worth a pound of cure”. We must follow that sentiment and try to find a solution to prevent such issues instead trying to cure them after fraud occurs. In other words, most related issues arise from an information security gap in the web based scholarly world.

A recently published correspondence tells the story of a hacked email account belonging to a reputable editor. Attackers used the e-mail account to send malicious content to researchers acquainted with the editor [22]. This case is clear type of identity theft which occurs in most web based attacks. Our observations and previous studies illustrate that academic journals and editors are constantly threatened by potential cyber-attacks. Since much previous research overlooks this important matter, in this paper we will describe such attacks and present general guidelines for editors. This paper's target audience is editors and researchers. Editors need to know how to protect their journals and protect themselves against cyber-attacks. Researchers need to increase their awareness about such attacks and adopt measures to protect themselves. We gathered most attacks by considering medicine and medical journals.

3. Our research; current and potential cyber attacks on academic journals with guidelines for improving security

In this section, we describe current and potential attacks from known fraudulent websites and their “editors”. We have gathered lists of these attackers by using previous studies and current literature. We then explain that many of these cybercriminals are still at large and then present guidelines to prevent or detect their attacks.

3.1. Method used for hijacking traditional journals

As Dr. Jalalian explained, cybercriminals look for reputable journals that don't have websites or are available only in print version. Then they create websites by using their names and ISSNs and proceed to cheat researchers [11]. We did a small experiment to see how easy or difficult this would be for a cybercriminal to do. First, we used Ulrich Web (a database that contains journal data; http://ulrichsweb.serialssolutions.com) and looked for suspended journals. Second, we selected 10 journals and created simple html webpages by using their titles and uploaded them to our own website (http://scires.ir/fpapers). Third, we then created a second website for each of our selected journals. Fourth, we then used SEO (search engine optimization) techniques to improve our website visibility in search engines. Thanks to SEO techniques, every person who searches for the suspended journal will see our faux website in the first eight returned results. Fig. 1 shows our simple html webpage.

Also, we searched for available titles of hijacked journals in Beall's list (http://scholarlyoa.com/other-pages/hijacked-journals/). We observed that in most cases, the hijacked websites are listed in the first or second page of search results. According to this evidence, we conclude that journals that have weak SEO are likely to be especially good candidates for hijacking. Cybercriminals can search for journals that have weak SEO, create second websites, improve the SEO, and preferentially direct traffic to those fake websites. If editors want to protect their journals against possible hijackings, they need to improve SEO at their journal's website. There are good academic resources for improving SEO such as “The Art of SEO” by Enge and his colleagues [23] or “Ultimate Guide to Search Engine Optimization: Drive Traffic, Boost Conversion Rates and Make Lots of Money” by Rognerud [24].

3.2. Method used for hijacking advanced journals

In this method, cybercriminals try to take full control of a journal's authentic domain. They have two options to get full control of a domain. First, they enter the journal's website by deciphering the password. You may think that this is not possible, but unfortunately it is a real and ubiquitous problem. We often check Zone-h (http://zone-h.org) and can see newly hacked websites related to academic journals. Zone-h is an archive that contains mirrors of most hacked websites. So far we did not observe a fake journal listed on the site. These hacks appear to be relatively benign—the invasions simply show website vulnerabilities. On the other hand, we must consider that fake journals eventually will be created through malicious hacking of authentic websites. Second, there is nothing stopping cybercriminals from registering the expired domains of academic journals. As Bohannon stated in his published paper in Science [21], cybercriminals easily could create 20 hijacked journals by using expired domains of authentic journals. They would have complete control of 20 authentic journal websites. This is a warning for scholarly publishers to give more consideration to information security policies. There are guidelines for website security available in print and online. Some of these are very general, such as “Web Application Security, A Beginner's Guide” by Sullivan & Liu [25], and some of them are technical, such as “The Web Application Hacker's Handbook Discovering and Exploiting Security Flaws” by Stuttard & Pinto [26]. Editors can also consult with information security engineers, for suggestions and advice on best practices.

3.3. Scam and spear phishing emails

Scam and phishing attacks via email are familiar to most internet users. In a phishing attack, cybercriminals create fake websites similar

Please cite this article as: Dadkhah M, et al, Current and potential cyber attacks on medical journals; guidelines for improving security, Eur J Intern Med (2016), http://dx.doi.org/10.1016/j.ejim.2016.11.014