Karlsruher Institut für Technologie

Institute of Applied Informatics
and Formal Description Methods
Prof. Dr. Melanie Volkamer

Your website has been hijacked: Raising awareness for an invisible problem

Anne Hennig (Karlsruhe Institute of Technology)

Motivation

Most website owners use CMSs to manage their websites. Yet, those can pose security risks and provide vulnerabilities for manipulations. With a SEO Spam attack, for example, an attacker deploys malicious code on a website. The manipulation is not visible on the genuine website, but in the search engine results the sites appear as, for example, shops selling illegal or banned drugs and medicines.

Since current literature does not draw a comprehensive picture on how to create convincing vulnerability notifications [i.a. 1-8] our motivation is to investigate the topic of vulnerability notifications in more detail. Furthermore, we will develop awareness and education materials for website owners, hosting provider, industry branches, and other intermediaries like internal (web) administrators or CISOs.

Research Plan

Interview Study

Description
- Interviews with 25 German website owners who had previously been informed about the vulnerability

Research Question
- What do the website owners consider necessary in future vulnerability notifications?

Notification Experiment

Description
- We designed notifications for three senders with three different framings – each framing is send out by each sender.

Research Question
- Can we increase remediation rates by choosing senders that match the framing?

Content Analysis + Online Survey

Description
- We plan a content analysis of websites, YouTube videos, news media and scientific paper, as well as an online survey to collect content for awareness and education materials related to SEO Spam infections.

Research Question:
- How should awareness materials be designed to meet the needs of the website owners?

User Studies

Description
- We plan to implement expert and/or focus group interviews, (online) surveys and/or observational studies on our awareness and education materials

Research Question:
- How effective are the awareness materials we developed?

Current Findings

- Providing verification possibilities and creating plausible notifications are the most important factors for the recipients to establish trust in vulnerability notifications
- Establishing a connection to the sender helps the recipient to verify the message
- Providing incentives for remediation helps the recipients to recognize the severity of the problem
- Raising awareness for the problem also among external service providers is important

Industry Partners

BDO

mindUp Web + Intelligence GmbH

Acknowledgements

Bundesministerium für Bildung und Forschung

References

[1] Z. Durumeric, et al. 2014. The Matter of Heartbleed. https://doi.org/10.1145/2663716.2663755[2] F. Li, et al. 2016. You've Got Vulnerability: Exploring Effective Vulnerability Notifications. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/li[3] M. Maass, et al. 2021. Effective notification campaigns on the web: A matter of Trust, Framing, and Support. https://www.usenix.org/conference/usenixsecurity21/presentation/maass
[4] B. Stock, et al. 2018. Didn't You Hear Me? – Towards More Successful Web Vulnerability Notifications. https://publications.cispa.saarland/1190/
[5] M. Vasek and T. Moore. 2012. Do Malware Reports Expedite Cleanup? An Experimental Study. https://www.usenix.org/conference/cset12/workshop-program/presentation/vasek
[6] E. Zeng, et al. 2019. Fixing HTTPS Misconfigurations at Scale: An Experiment with Security Notifications.
[7] F. O. Çetin, et al. 2017. Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning[8] O. Çetin, et al. 2016. Understanding the role of sender reputation in abuse reporting and cleanup. https://doi.org/10.1093/cybsec/tyw005