Lecture Notes on Data Engineering and Communications Technologies
Volume 135, 2022, Pages 583–594

Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation

Marusenko, R.[a], Sokolov, V.[b], Bogachuk, I.[b]

[a]Shevchenko National University of Kyiv, Kyiv, Ukraine
[b]Borys Grinchenko Kyiv University, Kiev, Ukraine

Abstract

Anti-spam software is constantly being improved. User behavior algorithms—the ability to recognize and correctly respond to phishing messages are widely known. The task of our research is to elaborate a way of effective dataset preparation from open scientific sources and test the efficacy of phishing attacks on a sample of respondents who represent the scientific community, as well as cybersecurity specialists. We developed and tested a method of mining data necessary for effective phishing attacks from open scientific sources. Authors suggest automated scripts to check the legitimacy of gathered data before use and to automate mailing bypassing spam detection algorithms. Elaborated scripts can be used not only for simulated attacks but for legitimate datasets cleaning and mass mailing. The experiment results confirm that successful phishing mailing is possible. Both scholars and cybersecurity specialists are vulnerable to this type of phishing attack based solely on open data. The study shows the way of effective testing and bypassing existing spam filters in the "black box" mode without knowledge of their algorithms. Even though these attacks are well-known and studied from the psychological perspective, we show that the scientific community and, in particular, the study demonstrates no difference in the vulnerability level to this type of attack between cybersecurity specialists and other scholars. We conclude that existing spam filters do not prevent phishing messages' mass delivery and require further improvement. The degree of users who still trust emails from an unknown source masquerading as legitimate ones and sending their data in return without caution remains relatively high in the scientific community and, particularly in a community of academic cybersecurity scholars.

Author keywords

Deduplication; Email validation; ORCID; Phishing; Social engineering; Spam filter

About this paper

https://link.springer.com/chapter/10.1007/978-3-031-04809-8_53

ISSN: 2367-4512
DOI: 10.1007/978-3-031-04809-8_53
EID: 2-s2.0-85129657396

Source Type: Book Series
Document Type: Book Chapter
Publisher: Springer, Cham