Project Proposal

Introduction

Cyber security breaches are frequently brought on by human error (Chan, Woon and Kankanhalli, 2005) instead of technological error (Schneier, 2000). In order to force their targets to conform, offenders intentionally influence their targets' heuristics to make them commit systematic mistakes (Bullee, Montoya, Junger and Hartel, 2017). As these malevolent agents get more skilled and utilize social engineering techniques that combine psychological and technological deceptions to make hostile emails appear as trustworthy as possible, spear phishing assaults are on the rise and growing gradually more complex (Stembert et al., 2015a). These breaches might seriously challenge a company's reputation and financial standing. To prevent end-users from falling for email spear phishing attacks, it is crucial to detect spear phishing assaults. Such sophisticated spear phishing emails are difficult for standard email protection systems to detect (Cordero, 2022).

Therefore, this project will suggest a computer system that combines analysis, identification, and warning techniques to enable both inexperienced and knowledgeable users in a user-friendly setting to identify spear phishing assaults on emails (Stembert et al., 2015b).

Aims

This project will be about implementing a system to detect a spear phishing assault on an email system by fraudsters.

Objectives

This project intends to conduct experiments to see how a custom designed computer system can be effectively utilized to recognize and mitigate spear phishing emails.

Questions

To be able to reach the goal of this project the following research questions will be answered:

- What alternative methods can be used to reduce the impact of spear phishing emails?
- What different types of phishing emails exist based on the email content and to what extent do they share common identifiers?
- To what extent can a tool aid user in identifying spear phishing attack emails?

System to detect spear phishing emails

A problematic question in network security is identifying spear phishing emails. The structure and content of an email may be arbitrarily changed by a fraudster, from a simple Sender field spoof to well-planned sequences of fraudulent Received headers. Thus, it is difficult to distinguish between authentic and counterfeit emails in the absence of precise detection tools utilizing applicable algorithms, in practice, such as DKIM and DMARC (Gasco, Ullrich, Stritter and Rieck, 2018).

Consequently, various tools were discovered after doing in-depth research on open-source scripts related to spear phishing assaults on Github. Instead of identifying or blocking spear phishing assaults, most of them instead originate phishing attacks. The espoofer by chenjj was the ideal spear phishing assault tool discovered. This program attacks end-users by evading the SPF, DKIM, and DMARC authentication in email systems (GitHub - chenjj/espoofer: An email spoofing testing tool that aims to bypass SPF/DKIM/DMARC and forge DKIM signatures, n.d.).

Therefore, this project will use open-source solutions and make the necessary modifications to create a spear phishing assault detection tool for email systems.

The new mitigation tool shall be built using Python and use the DMARC (Domain-based Message Authentication, Reporting & Conformance) technology alongside other similar defences.

To authenticate senders, the new versioning tool must additionally include the Sender Policy Framework (SPF) and DomainKeys Identified Main (DKIM). We are better protected against phishing and spoofing emails when DMARC is combined with SPF and DKIM. Receiving mail systems use DMARC to decide what to do with messages from domains that fail SPF and DKIM checks.

Skeleton literature review

Phishing is a sort of criminal attack that uses social engineering to gain login credentials from a person or a business. Attackers employ spoof emails that appear to be from a reputable company. The message will then send the user to a fake website where they can steal personal information such as usernames and passwords or infect the user's computer with malware. Phishing assaults, on the other hand, are widely disseminated as spam emails, making them simpler to identify (Floderus and Rosenholm, 2019a).

Phishing is not a recent phenomenon; the first publicly acknowledged phishing attempt was launched against America Online (AOL), one of the major internet service providers at the time, around 1995. To deceive consumers into disclosing personal information like passwords or credit card details, hackers sent emails alleging to be from AOL staff. Due to the novelty of the practice, many people were duped despite red flags including a profusion of grammatical errors. Despite the fact that phishing assaults have been around for more than 25 years, they remain relevant today (Floderus and Rosenholm, 2019b).

Phishing comes in a variety of forms. The spear phishing technique and its closely related cousins, the clone phishing and website spoofing, are the most pertinent to this project.

Spear phishing

In spear phishing, a specific person inside an organization is targeted to get their login information. Before attacking, the assailant first learns about the victim, including their name, title, and contact information.

Close Phishing

A hacker creates an exact replica of a message that the recipient has already received in a clone phishing attempt. They could include a malicious link and say something like, "resend this."

Website spoofing

By using website spoofing, a hacker makes a false website that appears to be the real thing. Your information is gathered by the attacker when you use the site to check in to an account.

However, the following are potential outcomes of spear phishing assaults, according to the spear phishing facts sheet (2019) released by the IT Security Unit of the Ministry of Technology, Communication, and Innovation of Mauritius:

- The theft of confidential data, including passwords and credit card numbers, which might result in damages.
- Making fraudulent use of the victim's personal information, including name, address, and identification number.
- Make user's own reputation suffer.
- Can install malware and viruses on your computer.

Fraudsters may obtain access to critical corporate information, banking or credit card information, and wire transactions once they have persuaded their victim that they are reliable. Widespread fraud and system security intrusion may result from this. Experienced spear phishers are extremely good at establishing bases of operations from which to launch advanced persistent threat (APT) campaigns that cause lasting harm. As a result, it's crucial to recognize and stop spear phishing assaults on email.

Research methods

The findings and conclusions from literature reviews will be used as the research methodology for this project. The results shall provide us with the necessary knowledge to properly design the computer software to recognize spear phishing emails.

Breakdown of projects and timeline

To ensure timely completion, this project will be divided up into smaller components and will follow the timeline shown below.

Chapters/months	August	September	October	November	December	January
1. Perform background research						
2. Write initial project documentation						
3. Initiate tool implementation						
4. Perform and analyse testing						
5. Final analysis of generated data						
6. Refine project documentation and tool						

Figure 1 - Project Timeline

Indication of CyBOK category

CyBOK Category: Human, Organisational and Regulatory Aspects

Knowledge Area: Privacy and Online Rights

Topic: Privacy Engineering

References

Bullee, J., Montoya, L., Junger, M. and Hartel, P., 2017. Spear phishing in organisations explained. Information & Computer Security, 25(5), pp.593-613.

Chan, M., Woon, I. and Kankanhalli, A., 2005. Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. Journal of Information Privacy and Security, 1(3), pp.18-41.

Cordero, F., 2022. Spear Phishing Prevention | N-able. [online] N-able. Available at: <https://www.n-able.com/features/spear-phishing-prevention?fbclid=IwAR0Oo0kwRvkTE2hv3tC6JaRfHXcykO9fc39pfjwDlSIB-EpkA5N-NH9nMhs>.

Floderus, S. and Rosenholm, L., 2019. An educational experiment in discovering spear phishing attacks. Blekinge Institute of Technology, p.1.

Fortinet. 2022. 19 Types of Phishing Attacks with Examples | Fortinet. [online] Available at: <https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks> [Accessed 30 July 2022].

Gasco, H., Ullrich, S., Stritter, B. and Rieck, K., 2018. Reading Between The Lines: Content-Agnostic Detection of Spear-Phishing Emails. First Online,.

GitHub. n.d. GitHub - chenjj/espoofer: An email spoofing testing tool that aims to bypass SPF/DKIM/DMARC and forge DKIM signatures. [online] Available at: <https://github.com/chenjj/espoofer> [Accessed 30 July 2022].

Schneier, B., 2000. Secrets & Lies: Digital Security in a Networked World. John Wiley & Sons, Inc.605 Third Ave. New York, NYUnited States.

Spear phishing facts sheet, 2019. Spear Phishing - Know the impacts behind. p.1.

Stembert, N., Padmos, A., Bargh, M., Choenni, S. and Jansen, F., 2015. A Study of Preventing Email (Spear) Phishing by Enabling Human Intelligence. 2015 European Intelligence and Security Informatics Conference,.

Valimail, 2021. Spear Phishing vs Phishing: What's the Difference?. Available at: <https://www.valimail.com/blog/phishing-vs-spear-phishing/> [Accessed 30 July 2022].