ABSTRACT

Phishing attacks target system vulnerabilities caused by the human factor. Many cyber-attacks spread through mechanisms that exploit end-user vulnerabilities, making users the weakest link in the security chain. Since the phishing problem is broad and no single solution exists to effectively mitigate all vulnerabilities, multiple techniques are frequently implemented to mitigate specific attacks. The purpose of this paper is to survey many of the recently proposed phishing mitigation techniques.

INTRODUCTION

Phishing is a social engineering attack that seeks to exploit flaws in system processes caused by system users. For example, a system may be technically secure enough against password theft; however, if an attacker asks them to update their passwords via a specific Hypertext Transfer Protocol (HTTP) link, unaware end users may leak their passwords, threatening the overall security of the system. Furthermore, technical flaws (for example, DNS cache poisoning) can be exploited by attackers to create far more persuasive socially-engineered messages (for example, using legitimate but spoofed domain names can be far more persuasive than using different domain names). As a result, phishing attacks are a multi-layered problem, and effective mitigation would necessitate addressing issues at both the technical and human layers. It is difficult to mitigate phishing attacks because they aim to exploit human weaknesses (i.e. system end-users). Software phishing detection techniques are evaluated against bulk phishing attacks, so their performance against targeted phishing attacks is virtually unknown. Due to limitations in phishing mitigation techniques, several organizations, including leading information security providers, have experienced security breaches.

PROBLEM STATEMENT

The aim of the project is:

* Defining the phishing issue. It is important to note that the definition of phishing in the literature is not consistent, and thus a comparison of several definitions would be required.
* To understand the harm/effects of phishing attacks in the modern world, as well as how users are the weakest link in the cybersecurity chain. Investigate how the Social Engineering Engagement Framework (SEEF) is used to achieve the malicious goals.
* Detect potentially malicious websites and attachments using machine learning techniques.
* The ultimate goal is to demonstrate the steps for mitigating phishing attacks.

ESTIMATED APPROACH

I will follow a step-by-step approach to achieve the aim of this project.

* The first phase of research would focus on discovering what phishing is, how it is performed, what types of phishing attacks exist, how social engineering is used to achieve phishing, and how users are responsible for the same.
* The second phase will be to create a simple phishing attack from scratch to demonstrate how phishing works. In addition, for research purposes, I will employ a phishing framework to demonstrate how phishing works on a corporate level.
* The third phase will involve the use of machine learning to detect phishing attacks. The initial action will be to extract features and keywords to determine which URLs and documents are used for phishing and which are legitimate. The following step will be the analysis of the chosen datasets, which will include data cleaning, data filtering, and so on. The final step will be to choose the best classification algorithm by comparing different algorithms and selecting the one with the lowest error.
* The project's final phase will be to identify mitigation strategies for this cybersecurity threat.