ABSTRACT

Phishing attacks target vulnerabilities that exist in systems due to the human factor. Many cyber attacks are spread via mechanisms that exploit weaknesses found in end-users, which makes users the weakest element in the security chain. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks. This paper aims at surveying many of the recently proposed phishing mitigation techniques.

INTRODUCTION

Phishing is a social engineering attack that aims at exploiting the weakness found in system processes as caused by system users. For example, a system can be technically secure enough against password theft, however unaware end users may leak their passwords if an attacker asks them to update their passwords via a given Hypertext Transfer Protocol (HTTP) link, which ultimately threatens the overall security of the system. Moreover, technical vulnerabilities (e.g. Domain Name System (DNS) cache poisoning) can be used by attackers to construct far more persuading socially-engineered messages (i.e. use of legitimate, but spoofed, domain names can be far more persuasive than using different domain names). This makes phishing attacks a layered problem, and an effective mitigation would require addressing issues at the technical and human layers.

Since phishing attacks aim at exploiting weaknesses found in humans (i.e. system end-users), it is difﬁcult to mitigate them. Software phishing detection techniques are evaluated against bulk phishing attacks, which makes their performance practically unknown with regards to targeted forms of phishing attacks. These limitations in phishing mitigation techniques have practically resulted in security breaches against several organizations including leading information security providers

PROBLEM STATEMENT

The aim of the project is:

* Deﬁning the phishing problem. It is important to note that the phishing deﬁnition in the literature is not consistent, and thus a comparison of a number of deﬁnitions would be required
* Studying the types of phishing attacks and how they are achieved
* To see the damage/effects of phishing attacks in the modern world and how users are the weakest link in the cybersecurity cycle. In the process, also explore how social engineering engagement framework(SEEF) is used to achieve the malicious objectives.
* Use machine learning techniques to detect the potential malicious websites and attachments
* Final aim is to showcase the steps of mitigation to phishing attacks

ESTIMATED APPROACH

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

* In the first phase, the research would be concentrated on discovering what is phishing, how it is performed, what are the different types of phishing attacks, how social engineering is used to achieve phishing and how users are responsible for the same.
* Second phase will be to develop a simple phishing attack to show how phishing works which will be done from scratch. And for research purposes, I will use a phishing framework to showcase how phishing works on a corporate scale.
* Third phase will be using machine learning to detect phishing attacks. First step will be feature and keyword extraction to identify which URLs and which documents are used for phishing and which are legitimate. Next step will be the analysis of datasets chosen such as data cleaning, data filtering and so on. Final step will be to select the appropriate classification algorithm by comparing different algorithms and selecting the one which gives the least error.
* The final phase of the project will be to find the mitigation steps to this cybersecurity threat.