Efficient Client-Side Cross-Platform Compatible Solution for Phishing Prevention

Ben Stewart S., Anna University, India
Dhanush N., Anna University, India
Santhosh G., Anna University, India
Angelin Gladston, Anna University, India*

ABSTRACT

Phishing is a crime where the victim is contacted by an attacker posing as a trustworthy source and lures them into providing sensitive information. This work makes sure that time delay is averted, and the attack can be thwarted with fewer computational resources. To solve the above-mentioned problem, a web browser add-on that works as a background script on the client side is implemented. All the background scripts are made cross-platform compatible to make the development easier and more efficient. The contribution in this paper is the new add-on, Off-the-Hook-Plus. The main objective of this Off-the-Hook-Plus is to find if the web page that the user visits is a phish or not. The page redirect logs along with the page details are used to find if the site is a phish or not. And then, if the site happens to be a phish, the similar looking site, which this web page tries to impersonate, is given. To make the repeated accesses faster, a whitelist is maintained, where all the safe sites are logged. The add-on is experimentally evaluated, and the results are discussed and found to be effective.

KEYWORDS

Attackers, Links, Log, Off-the-Hook-Plus, Phishing, Whitelist

1. INTRODUCTION

In this section, how the issue of phishing began and how it was tried to be curbed both in policy writing and that of its implementation are discussed in detail.

The Internet had its humble beginnings as a research project to share and access resources in other computers. And in fact these “other” computers were the main frames of the time that were located in the research facilities and college laboratories of the United States of America. This Internet is not the traditional Internet that we know as the World Wide Web. It was just a network of computers that could be operated from other nodes in the network. One main roadblock that was encountered was that the main frames were expensive and far exceeded the computational requirements of the then public. As a result of this there were only a handful of expensive mainframes

DOI: 10.4018/IJCWT.297855

*Corresponding Author

with a few government and private institutions in a single country. Never would they have imagined the used for the internet unless the next era of personal computers boomed. As this phase had computers be considered almost as national assets they were sometimes compromised by enemy nations performing acts of sabotage (Steven, 1984).

In the stage of the personal computers, people bought computers to perform basic operations like spreadsheets and graphics related tasks. Once the internet had been introduced to those machines, they were still restricted by the slow DSL connections that the telephone companies provided. But once this threshold was broken, we would think that the Internet as we know today would have started to thrive. But it did not. The way in which the information is accessed was not intuitive till the World Wide Web made its appearance in 1989 developed by Tim Berners-Lee at CERN (https://webfoundation.org/about/vision/history-of-the-web/, 2018). This era with the internet has its own set of unethical activities that were performed using computers or against the computers. Some elaborate sabotage attempts even involved using the internet connections of those computers.

The World Wide Web started the phase known as the "Internet of Content" were the websites of different organizations could be accessed by any person on the internet to get to know the organization and other details like the availability time, recruitment offers and so on. The impact of the World Wide Web was accelerated once the search engines were developed to index and display the billions of webpages that were loaded into servers connected to the Internet. This made it possible for people to access almost anything hosted on the Internet without knowing upfront the URL related to the resource. This opened a plethora of problems related to the act of performing unethical activities using or against the World Wide Web. The most common internet based crimes were phishing and site defamation. And this is where the roots of performing malicious activities for the gain of nations or individuals can be traced to.

For the next era to come upon, there were a few changes that were required on the internet. They were the ability to host dynamic content based on the users and the ability for the user to interact with such content. These abilities were provided by the advent of web based programming languages with Javascript leading the way. This made it possible that people could perform online cash based transactions for the services that the internet made possible in the first place. This kind of opened Pandora's box for the cyber related crimes of this day. The notoriety of phishing greatly increased because of the scope that you could have the banking credentials of several thousands of users.

And before deep diving into the domain of phishing let us have a short look into the other eras of the internet that have come along. We have had the "Internet of People" which was brought by the advent of social media platforms like FaceBook, Twitter and LinkedIn. People now share much more data online about themselves over the internet to the public. This has led to even more problems like social media addiction, anxiety and attention deficit among the users. But let us not just paint a dark picture of this era and move on to what the future has in store.

We are currently in this era of the "Internet of Machines" were more and more IOT devices with the capability to connect to the Internet and use it to communicate with other IOT devices and some centralized computers. This is probably exciting times as even the standards of the Internet of Machines has yet to be decided and wonder if we would be having another World Wide Web like platform available with the machines in mind. Even in this age, the unethical activities can be performed as was done in the previous eras of the Internet.

Now that we have an understanding of what the Internet is and why it is so important and how it is being used, let us dive into the topic of phishing. If a definition were needed, phishing is any social engineering made to trick the people to access the malicious resources that may get critical information such as passwords, bank account numbers etc. from the victims. Phishing is done not only for the monetary incentives it provides but also for the impersonation of people in social media or to compromise the networks of organizations or countries (George et. al., 2015). They are targeted upon the users who have access to such details like an e-commerce customer or a company manager.