Phishing Attack Domain Detection

10 Jan, 2022

Overview

This project focuses on solving the most common cyber attack called phishing. Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

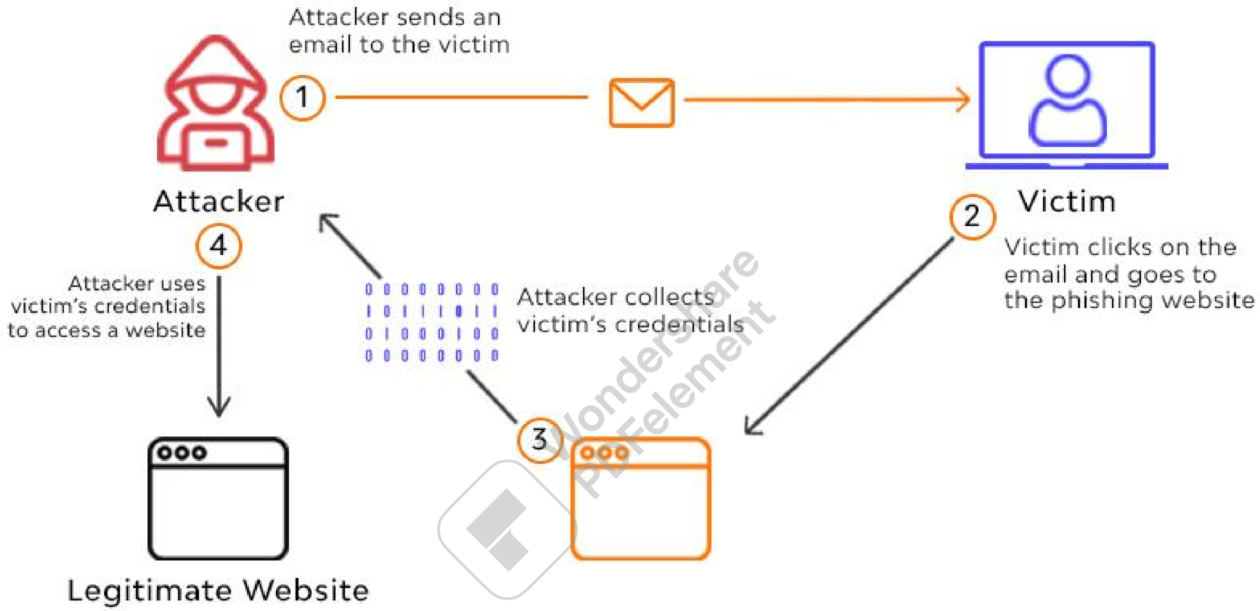
The purpose of this HLD document is to explain the high level details about the project. The HLD uses non-technical to mildly-technical terms which should be understandable to the administrators of the system.

Goals of HLD

1. **Explain the problem statement :** Explain the problem statement for the project and also explain how it affects the current situation.
2. **Technical Overview:** Give an of proposed solution and define all the requirements that will be used (including software & hardware) to build the system.

1. Problem Statement

We live in the digital era. This has steadily changed the way you buy things, pay your bills, rent an apartment, watch a movie, and everything else. This project focuses on solving a most common cyber fraud called “Phishing”.


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim’s credentials to access a website
Attacker collects victim’s credentials
3
Legitimate Website

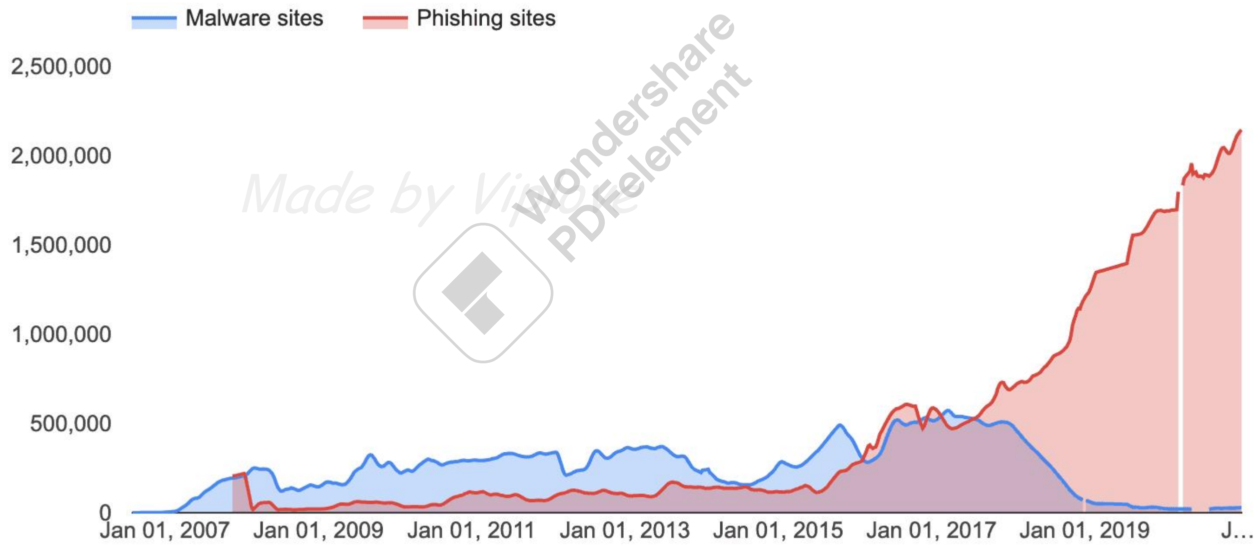
Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into **clicking a malicious link**, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

1.1 Frequency of phishing attacks

Phishing is a huge threat and growing more widespread every year. 2021 Tessian research found that **employees receive an average of 14 malicious emails per year**.

Almost 96% of phishing attacks arrive by email, 81% of organizations around the world have experienced an increase in email phishing attacks since March 2020. Despite the very real threat,only 1 in 5 organizations only deliver phishing awareness training to their employees once per year.



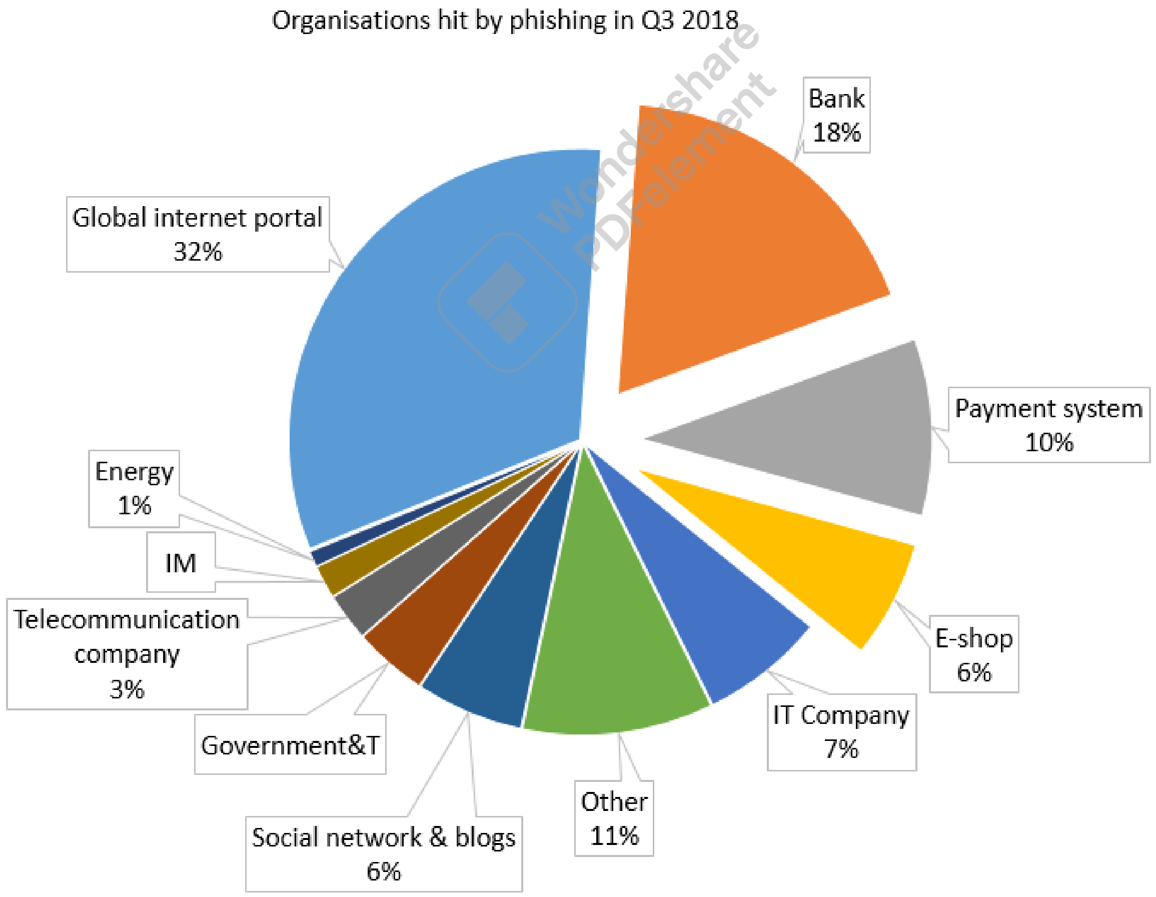
This chart - pulled from Google Safe Browsing - shows the steep increase in the number of websites deemed unsafe between January 2016 and January 2021.

According to the results of Terranova Security's *2020 Phishing Tournament*, almost 20% of all employees are likely to click on phishing email links and a staggering **67.5% go on to enter their credentials** on a phishing website.

1.2 Cost of phishing attacks

Phishing ranks as the second most expensive cause of data breaches—a breach caused by phishing costs businesses an average of $4.65 million, according to IBM.

According to Verizon, organizations also see a **5% drop in stock price** in the 6 months following a breach. The FBI's Internet Crime Report shows that in 2020, scammers made over $1.8 billion—far more than via any other type of cybercrime.



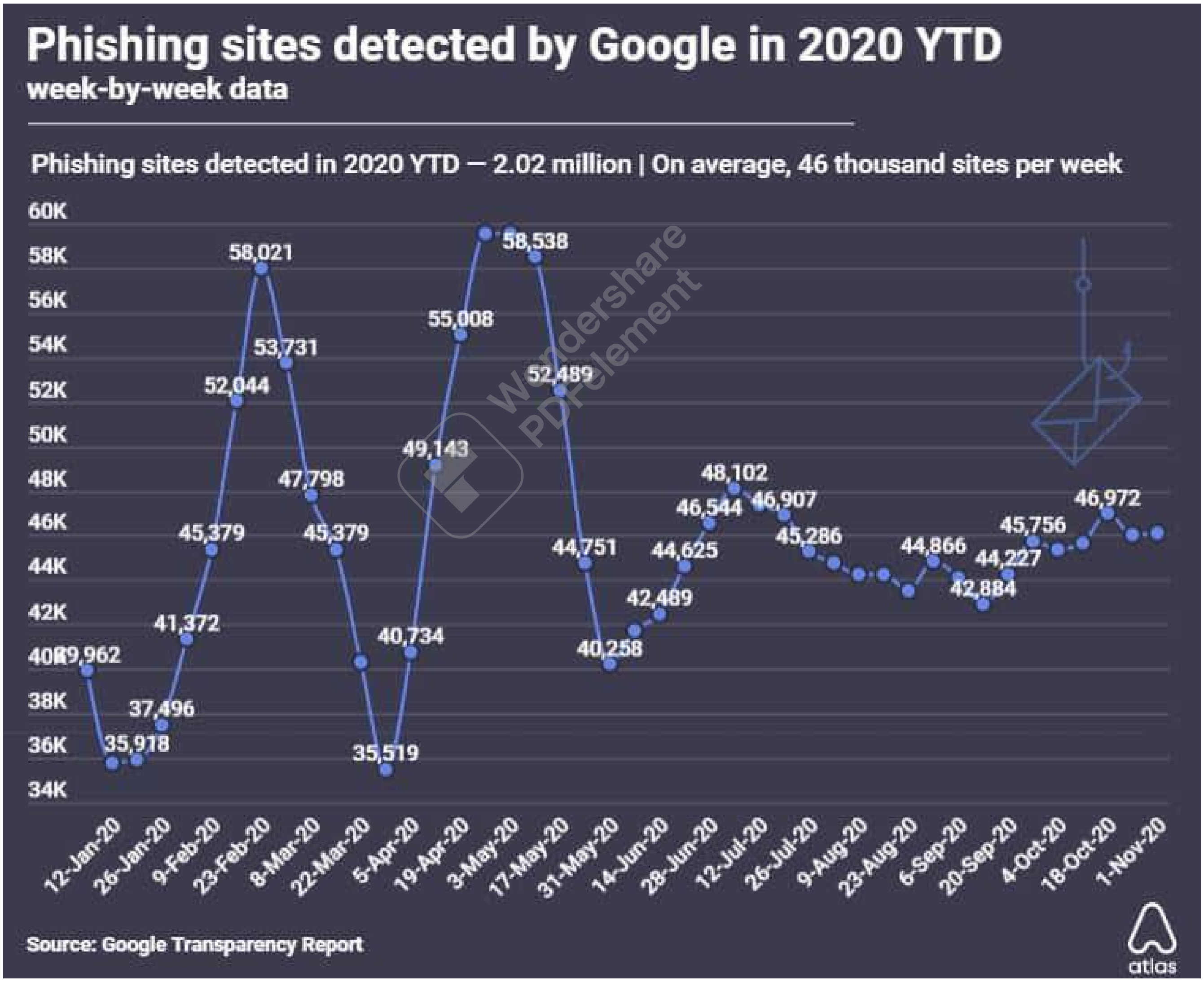
Phishing attacks can be devastating to organizations that fall victim to them, in more ways than one.

However, financial loss isn’t the only impact that a phishing attack can have on your organization. A successful attack can also lead to :

- User downtime
- Damage to reputation
- Loss of intellectual property
- Loss of revenue and customers
- Compromised accounts or credentials
- Malware infections, including ransomware

1.3 Phishing and Remote Work

The move to remote work has presented many challenges to business and the increased range, frequency, and probability of security incidents are among the most serious.


Phishing sites detected by Google in 2020 YTD

week-by-week data

Phishing sites detected in 2020 YTD — 2.02 million | On average, 46 thousand sites per week

Source: Google Transparency Report

Since a remote working protocol includes the sharing of sensitive company data and communicating important information via virtual platforms, it is easier for hackers to access them.

A security research survey has disclosed that 37% of employees working remotely from home, have faced an increased risk of phishing attacks in the past 5 months post-outbreak.

Employees in an organization are usually unaware of cyber attacks and related consequences. They are unaware of the latest trends and techniques used by cybercriminals, and easily fall prey to such threats. Without spreading awareness among employees adequately, an organization can’t protect their assets and finances from hackers.

1.4 Conclusion

While we can't stop hackers from sending phishing or spear phishing emails, we can make sure we are prepared if and when one is received. Educate employees about the key characteristics of a phishing email and remind them to be scrupulous and inspect emails, attachments, and links before taking any further action.

But, humans shouldn't be the last line of defense. That's why organizations need to invest in technology and other solutions to prevent successful phishing attacks. But, given the frequency of attacks year-on-year, it's clear that spam filters, antivirus software, and other legacy security solutions aren't enough.

That's why in this project our aim is to build a Machine Learning solution for this problem. Our goal is to build a ML system which can analyze malicious URLs and indicate the user about it,before clicking them.

2. Technical Overview

In this section we'll discuss the technical solution for the above mentioned problem statement and also define some of the technologies we'll be using to create the system.

2.1 Proposed Solution

As we discussed above, most people either lack proper knowledge to identify a phishing attack or fail to take appropriate precautions, and any sort of cybersecurity training for company employees will only interrupt their daily workings.

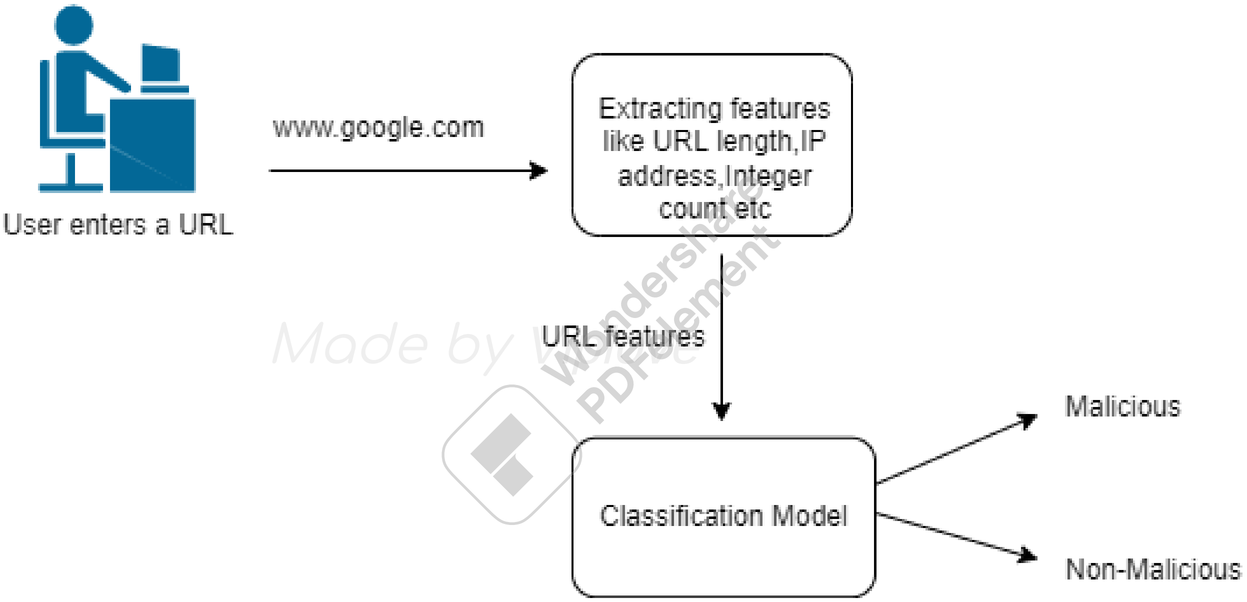
Most phishing attacks happen when a user clicks a malicious URL, so our primary goal should be to **prevent the user from clicking any malicious links**.

So in order to prevent such phishing attacks we propose a Machine Learning solution that can automatically analyze incoming malicious URLs and classify the links on its own rather than putting the Human as the last line of defense.

The end-goal machine learning system can be then used in web browsers,search engines,social media platforms etc or can be used directly by the user to detect phishing website domains.

2.2 Classifier Architecture

The below Image shows a high level architecture of our trained classification model. Basically it takes a single URL from the user, Extracts the url's features and then makes a prediction based on them whether the given URL is malicious or not.



The prediction of the classifier model is high based upon the features of the given URL like its length,Integer count,IP address presence in domain etc.

This model will be designed to function as standalone so that it can be used in various applications like web browsers.search engines,social media sites etc.

NOTE : More details on the classification model in the LLD document.

2.3 Data Requirements

In order to create a binary classification model which can optimally predict malicious phishing URLs,first we need to train the model on similar datasets.

This kind of data can be obtained from either public dataset or through scrapping suitable websites. Some of the properties that make a good dataset for our problem are the following :

- The dataset must contain an equal amount of positive and negative samples.
- The data must contain diverse features and characteristics with less sparsity among features.
- The data must contain both numerical and categorical features in balance.
- The dataset must be verified, if possible contain real-life scenarios for optimal results and less artificially generated samples.

Some example datasets are listed below :

- https://www.unb.ca/cic/datasets/url-2016.html
- https://www.sciencedirect.com/science/article/pii/S2352340920313202

2.4 Technology Requirements

Python programming language and frameworks such as NumPy, Pandas, Scikit-learn, TensorFlow, Keras will be used to build the whole model.

- PyCharm is used as an IDE.
- For visualization of the plots, Matplotlib,Seaborn and Plotly are used.
- Heroku is used for deployment of the model.
- Front end development is done using React & Css
- Python FastAPI is used for backend development.
- GitHub is used as a version control system.

Conclusion

In this HLD document we skimmed over the problem statement of phishing attacks and also discussed our proposed solution. But this was just a high level summary for project managers, we'll discuss the project in much more detail in the LLD document.