Assignment 1

COURSE CODE (DV 2582): MALWARE ANALYSIS

Sep 2022

Title	Detection of phishing URLs.	
Student 1	Name	Sandaka Gowtham Kumar
	E-Mail	gosa20@student.bth.se
	Person nr	20001117-T071
	Program	Masters in computer science
Student 2	Name	Mohit Battu
	E-Mail	mobt20@student.bth.se
	Person nr	19991007-T175
	Program	Masters in computer science
Student 3	Name	Monica Gattupalli
	E-Mail	Moga20@student.bth.se
	Personal nr	1999-1130-T308
	Program	Masters in computer science

I. INTRODUCTION

We have explored some clean URLs and some phishing URLs in order to complete this task. This allows us to determine the legitimacy of a site by analyzing the attributes of the site in order to determine whether or not it is legitimate. This was accomplished by using a few tools that were available to us. We have been able to complete this task with the help of the following tools, which have been listed below.

- **Phish tank:** It is a free online group site that anyone can join for the purpose of reporting, verifying, tracking, exchanging, and collecting information regarding phishing attacks.

- **Who is**: To receive information about the public registrar of a domain name and other domain-related information. It was utilized for this study to collect information on the site's registrar, expiration date, creation date, and the country in which the site is situated.

- **Geo IP**: With the help of this tool, it is possible for individuals to see in which country a device with a particular IP address is located throughout the entire world. In this experiment, Geo IP was used as a means of identifying the location of the URLs.

II. RESULT

A total of 90 clean URLs were tested in this experiment, as well as 90 phishing URLs. According to the pie charts of frequency tables shown in Figures 1-6, it can be concluded that "US" has contributed the most to maintaining phishing URLs and clean URLs within the scope of the research. It is common for the majority of phishing URLs to have a lifetime of "1 year," which means that the URL works throughout the entire year. The domain names for the clean URLs are as follows: ".com", ".org", ".cn", ".co", ".xyz", ".uk" and for the phishing URLs, we can see that the domain names are as follows: ".com", ".org", ".net", and ".se". There is an average lifespan of 20 years for clean URLs. If you are familiar with the name of the registrar, we can also say that the URL is clean in most cases. Based on the findings of this experiment, we can conclude that phishing URLs have a relatively short lifespan and are active throughout that time period. According to the study's scope, the majority of URLs used in phishing are from countries such as "US", "KR", and "HK", plus some others that are not specifically mentioned.

II.I ALGORITHM

- **Inspect the website URLs:** First, determine whether the URL comprises HTTP or STTP; when it doesn't, then the data sent on the website will not be secured, indicating that the site is a phishing site. After that, double-check the spelling of the sites because fraudsters are capable of changing minor typos of clean URLs to fool the audience. If the URL has a lot of irrelevant symbols and directories, it can be altered to www.Paytm.com instead of www.Paytm.com. This clearly shows the presence of phishing.

- **The website owner should be checked:** A free domain name checker, such as whois.net, can be used to verify a domain name so use it. There is no doubt that a website that has a life span of around a year or less and belongs to an unknown organization is a phishing site.

- **Trusted payment methods**: A phished website is one that accepts financial transfers. Most services accept credit card payments and employ secure payment partners such as Paytm, PayPal, and UPI.

III. FREQUENCY DIAGRAMS

In this assignment, we used to draw some frequency diagrams for the URL data that we have collected the diagrams have been drawn according to the attributes of the URLs. The following attributes are:

- Register
- Lifetime
- Country

So, the diagrams are as below:

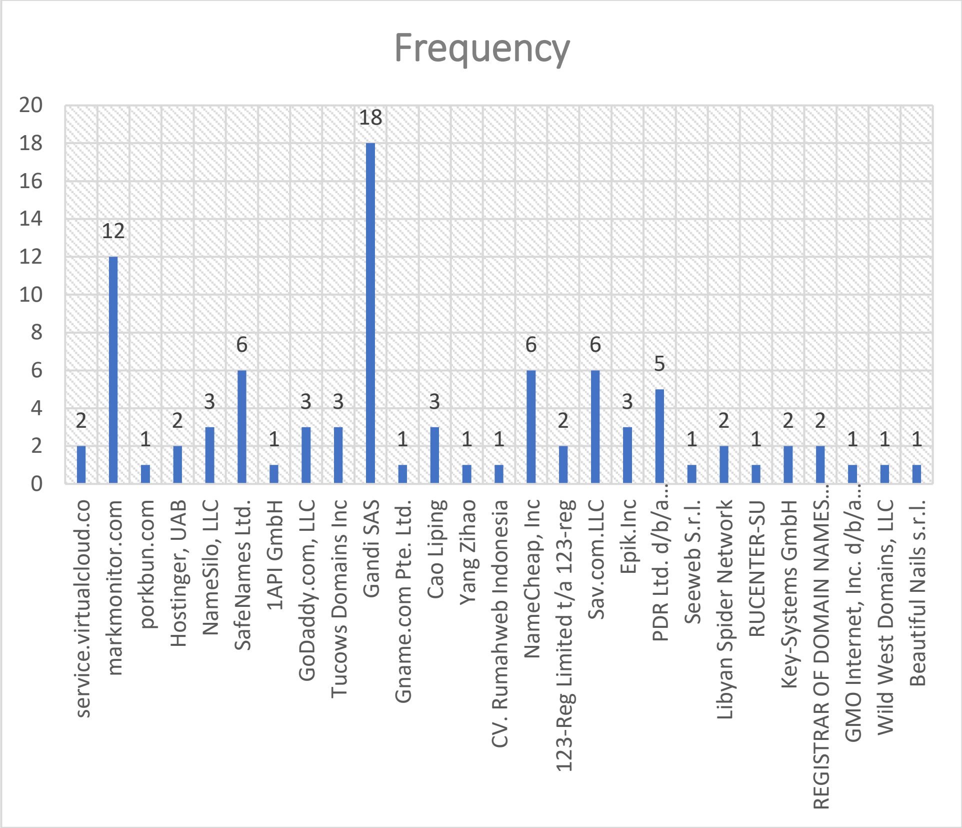

Fig1: Register for Phishing URLs

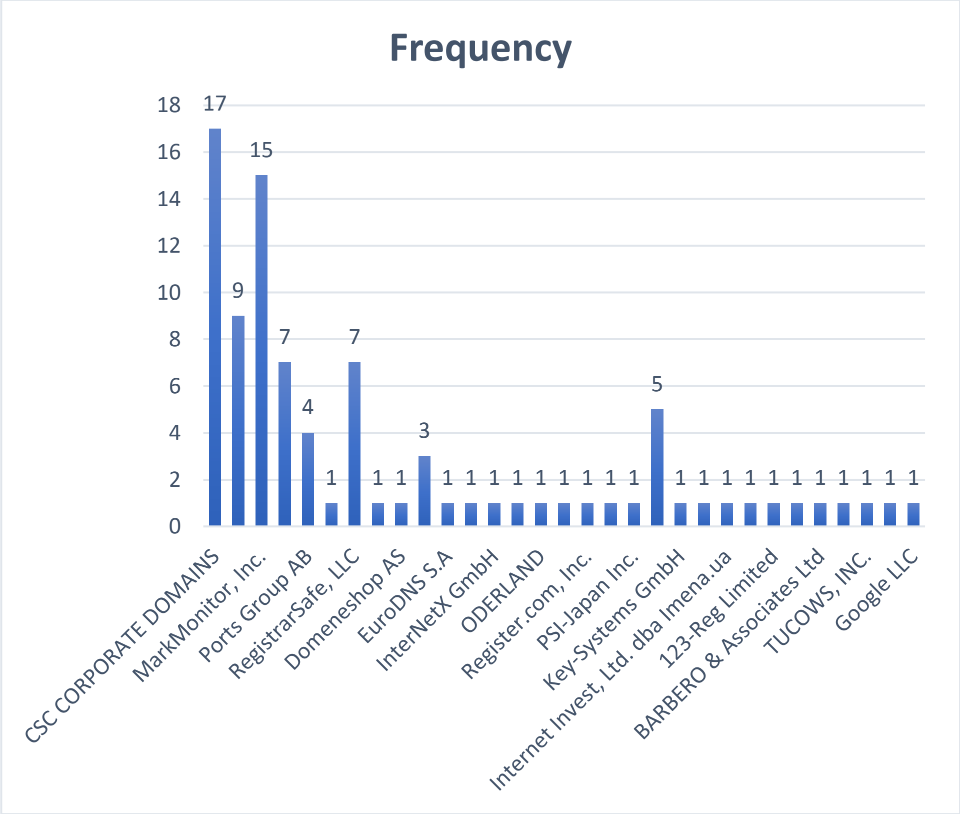

Fig2: Register for Clean URLs

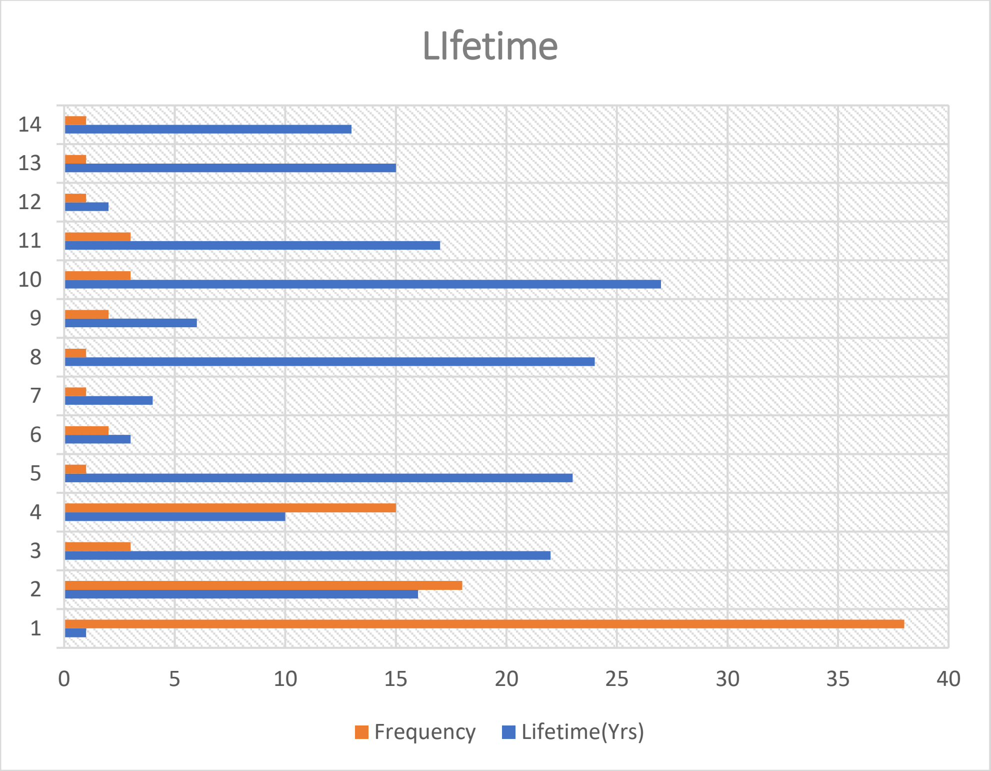

Fig3: Lifetime for Phishing URLs

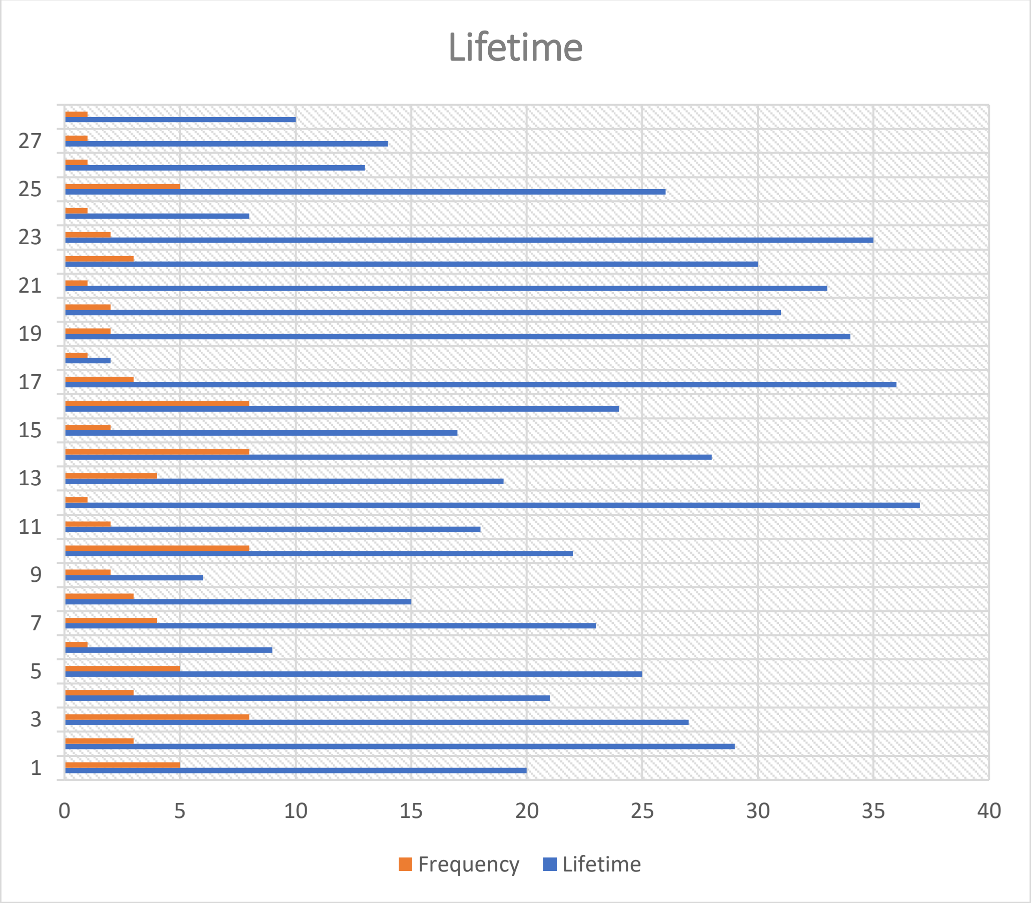

Fig4: Lifetime for Clean URLs

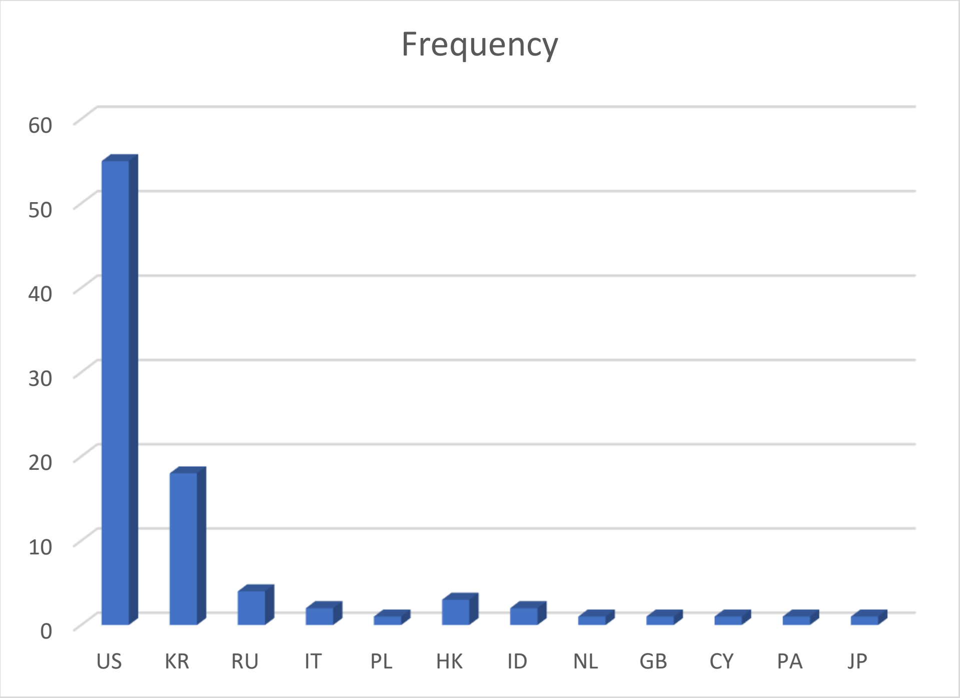

Fig5: Country for Phishing URLs

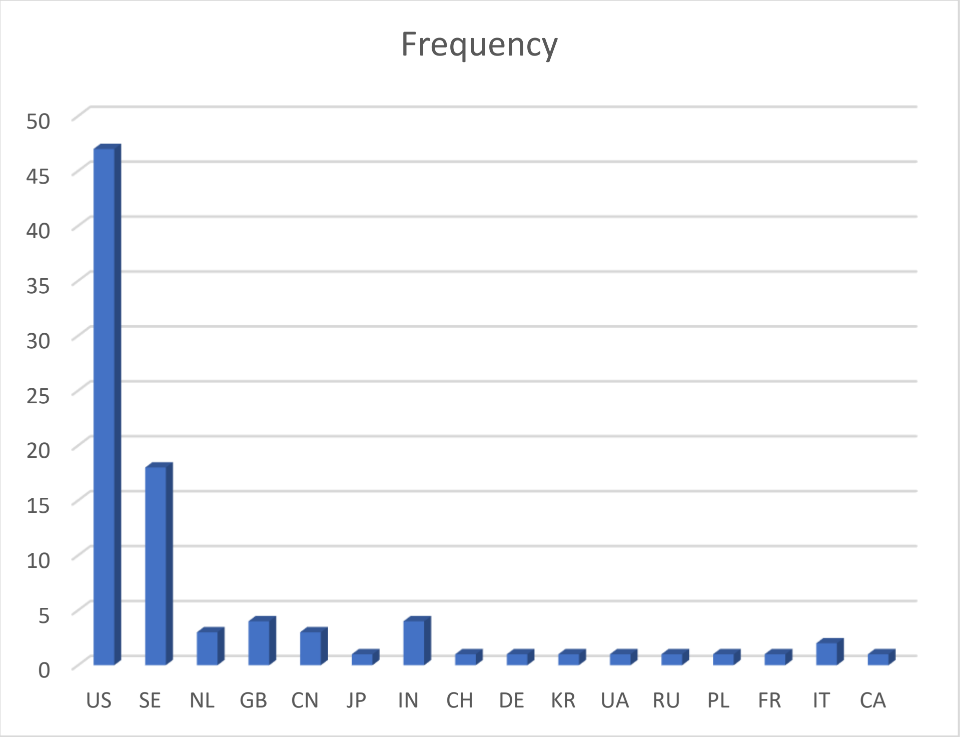

Fig6: Country for Clean URLs