Intro:

Here is an idea of how to investigate and prevent Fraud and Brand Abuse using Yara.

How to create the enviorment

Choose 35 names of singers and add them to a document. Each phishing kit will have a different name. For example:

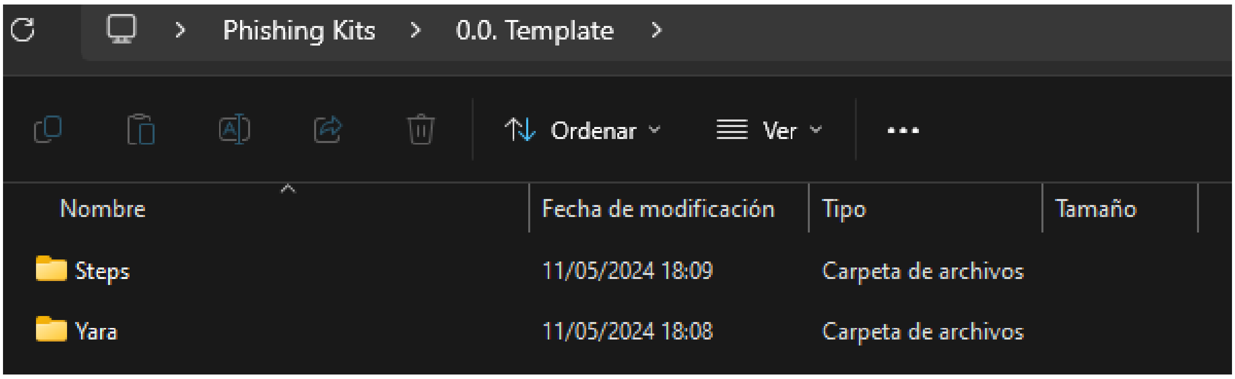
1. Adele
2. Alicia Keys
3. Ariana Grande
4. Beyoncé
5. Billie Eilish
6. Bruno Mars
7. Camila Cabello
8. Chris Martin (Coldplay)
9. Demi Lovato
10. Drake
11. Dua Lipa
12. Ed Sheeran
13. Eminem
14. Enrique Iglesias
15. Harry Styles
16. J Balvin
17. John Legend
18. Justin Bieber
19. Justin Timberlake
20. Katy Perry
21. Khalid
22. Lady Gaga
23. Lizzo
24. Maluma
25. Ozuna
26. Post Malone
27. Rihanna
28. Sam Smith
29. Selena Gomez
30. Shakira
31. Shawn Mendes
32. Sia
33. Taylor Swift
34. The Weeknd
35. Usher

Now create another document named Campaigns. And add a table like the following one. Here's where you are going to track a record of all the analized phishings.

Date	Kit Name	Url	IP
YYYY-MM-DD	Adele	www.example.com	0.0.0.0
YYYY-MM-DD	Alicia Keys	www.example.com	0.0.0.0
YYYY-MM-DD	Ariana Grande	www.example.com	0.0.0.0

Once you have the list of names, you are ready to do the template enviorment:

1. Create a folder named Template.
2. Create 2 subfolders with the name of Steps and Yara.



Nombre	Fecha de modificación	Tipo	Tamaño
Steps	11/05/2024 18:09	Carpeta de archivos	
Yara	11/05/2024 18:08	Carpeta de archivos	

a. Inside the Steps subfolder you're going to create a table like so (you can use Excel or Word):

Steps	Compressed File	Capture
Step 1	.zip	Capture 1
Step 2	.zip	Capture 2
Step 3	.zip	Capture 3

b. Inside the Yara subfolder you are going to create a file called template.yml . The content of this file has to be a Yara template.

```
yara template
{
        meta:
                description = ""
                author = ""
                date = ""

        strings:
                step1input = ""
                step2input = ""
                step3input = ""

        condition:
                all of them
}
```

Now you have created all the templates. You are going to duplicate the mother folder and rename it per each phishing kit analized.

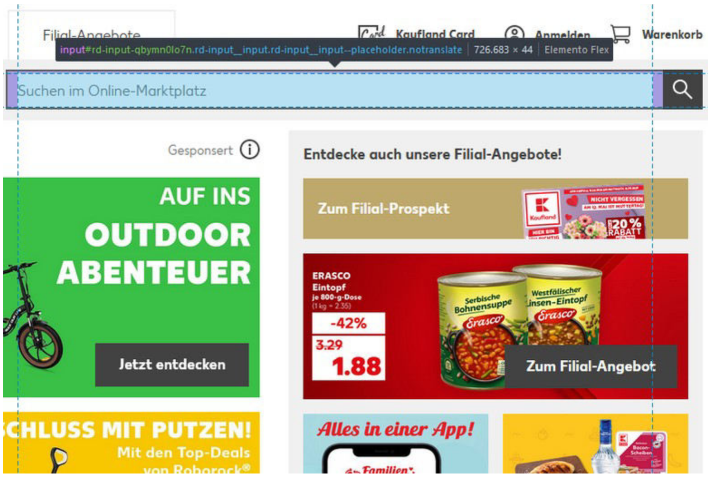
How to analyze the phishing kit.

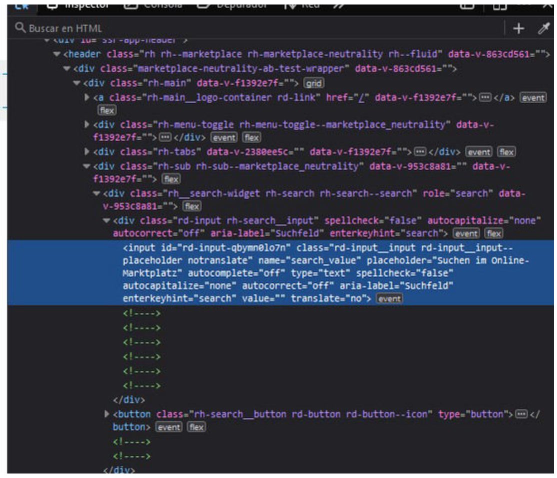
First of all you have to take a screenshot of every step of the phishing kit, for example:

1. Step 1: Home page
2. Step 2: Product page
3. Step 3: Payment page

Then, download the code of each step. And add the screenshots and the compressed code in the Steps file.

Now let's see which is the best part of the code to add to our yara rules. I would recomend to go to the *<input>* parts. They are usually written different in each phishing kit and in every step of the kit.





```
<header class="rh rh--marketplace rh-marketplace-neutrality rh--fluid" data-v-863cd561="">
  <div class="marketplace-neutrality-ab-test-wrapper" data-v-863cd561="">
    <div class="rh-main" data-v-f1392e7f=""> grid
      <a class="rh-main__logo-container rd-link" href="/" data-v-f1392e7f="">…</a> event
      flex
      <div class="rh-menu-toggle rh-menu-toggle--marketplace_neutrality" data-v-
      f1392e7f="">…</div> event flex
      <div class="rh-tabs" data-v-2380ee5c="" data-v-f1392e7f="">…</div> event flex
      <div class="rh-sub rh-sub--marketplace_neutrality" data-v-953c8a81="" data-v-
      f1392e7f=""> flex
        <div class="rh__search-widget rh-search rh-search--search" role="search" data-
        v-953c8a81=""> flex
          <div class="rd-input rh-search__input" spellcheck="false" autocapitalize="none"
          autocorrect="off" aria-label="Suchfeld" enterkeyhint="search"> event flex
            <input id="rd-input-qbymn0lo7n" class="rd-input__input rd-input__input--
            placeholder notranslate" name="search_value" placeholder="Suchen im Online-
            Marktplatz" autocomplete="off" type="text" spellcheck="false"
            autocapitalize="none" autocorrect="off" aria-label="Suchfeld"
            enterkeyhint="search" value="" translate="no"> event
            <!---->
            <!---->
            <!---->
            <!---->
            <!---->
            <!---->
          </div>
          <button class="rh-search__button rd-button rd-button--icon" type="button">…</
          button> event flex
          <!---->
          <!---->
        </div>
```

Then place every *<input>* part in the correct step in the yara rule. Once you have this info set, modify the yara rule as you want to detect the kit everytime that is executed.

Finally, remember to feed all the parts of the process like adding the URL, IP and Phishing Kit name in the document named Campaigns.