**Social Engineering**

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

* **Theoretical organization scenario for demonstrating the attack.**

Organization name: Imarticus Learning

Company: Education

We have the the organization name as Imarticus learning

We are going to perform a social engineering attack and techniques for demonstrating a social engineering ,social engineering techniques,methodology,campaign,attack.

At a first we got the information about target organization and employee .. etc.Which we are using in attack vector.

There are two scenario’s

1. We have the current employee’s of company.

2.we have the person, who is taking the admission in company.

This above information we find during footprinting and reconnaissance stage.

Now in any company we can try phising attack on any employee, depend on a employee behaviour in company and personal life

Let’s take a example the one employee is good in work at a company and he is doing his job fantastic and if we talk about the personal life then he is foody

So we can tempt the person with food offer like Zomato,swiggy etc..

But in this we are using the Rewards and Recognition .

Because all person have personal life and different different interest, but the Rewards and Recognition of company is the thing in which all employee are interested .

So ,we are going to craft and create phising mail which seems like its from company and Rewarding or recognizing employee.

**● Collect information about the target that will help him/her convert that information into the attack vector. Cyber Security – Project**

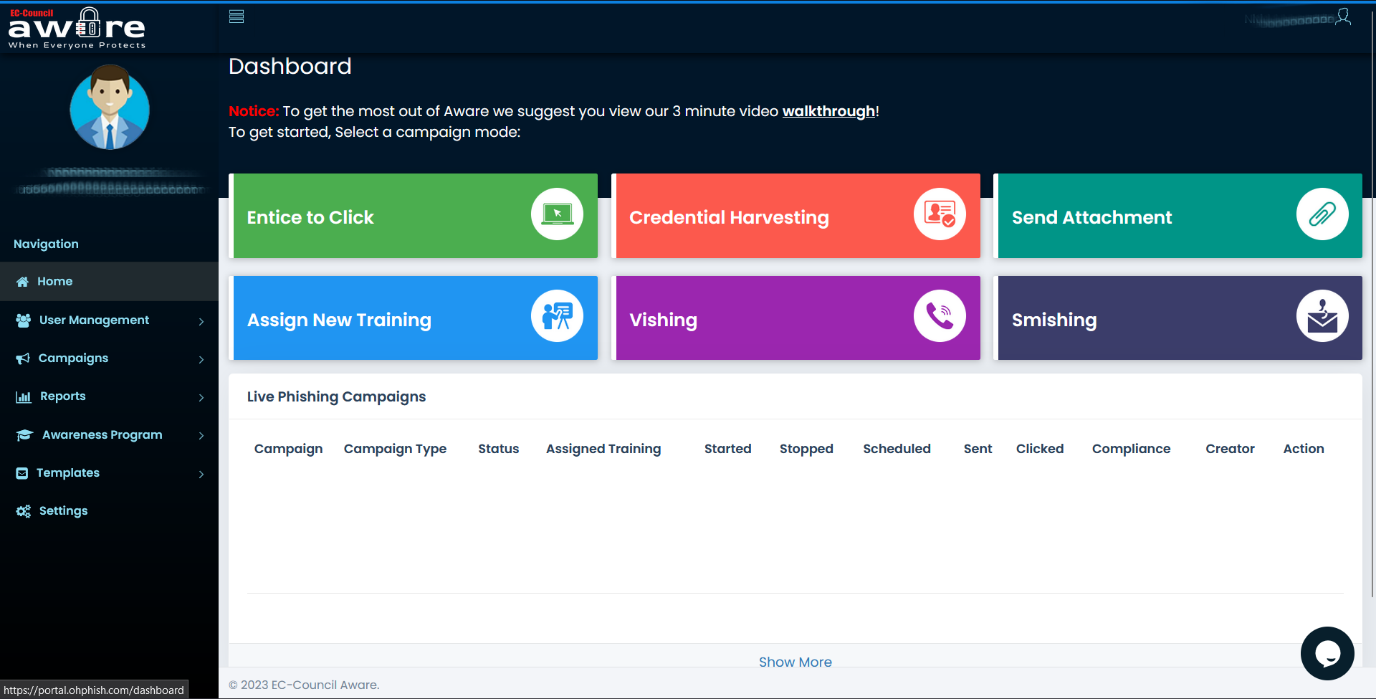
**● The attack will get deployed according to the information collected on the target, it can be a shopping offer, gym offer or a dating site, or anything according to the target's information.**

**● The well-crafted social engineered phishing e-mail that will convenience or gain the trust of the target.**

We are using a tool known as ohPhish provided by ec-councill

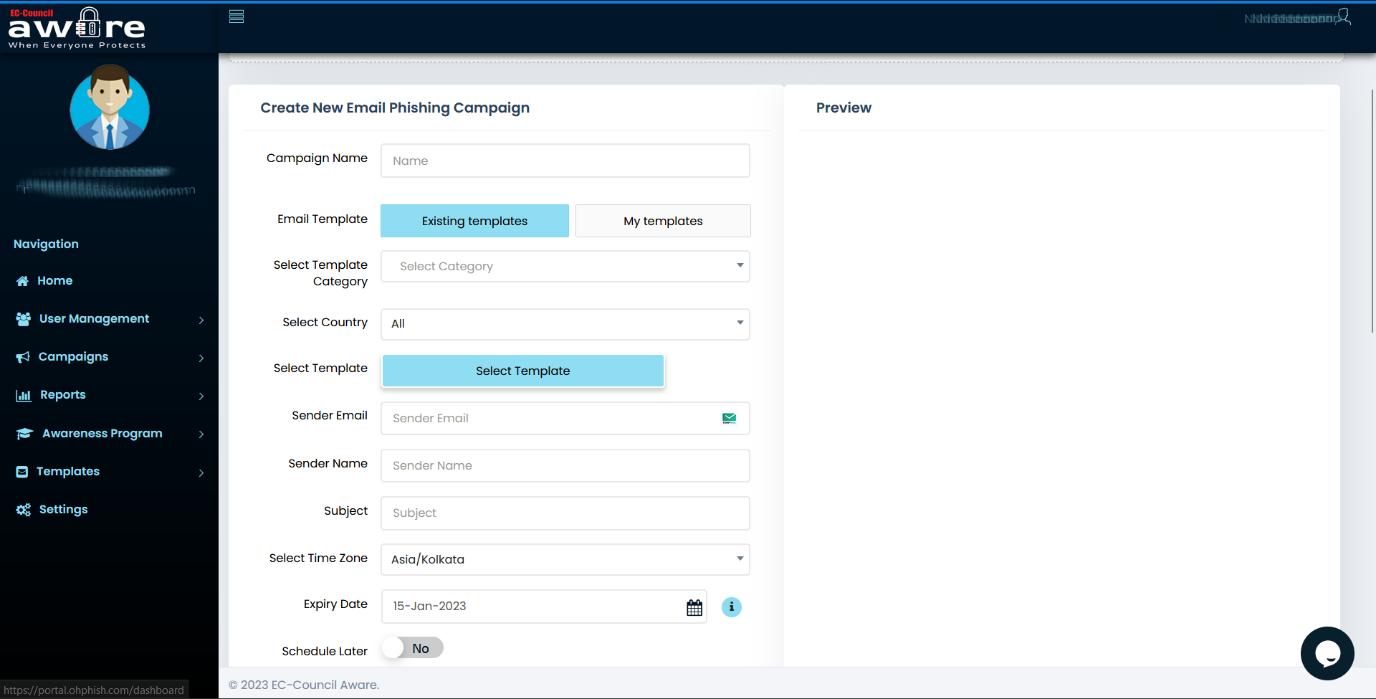
ohPhish tool is standard tool used for creating,crafting,and run social engineering attacks ,compaign and techniques.

**Dashboard:**

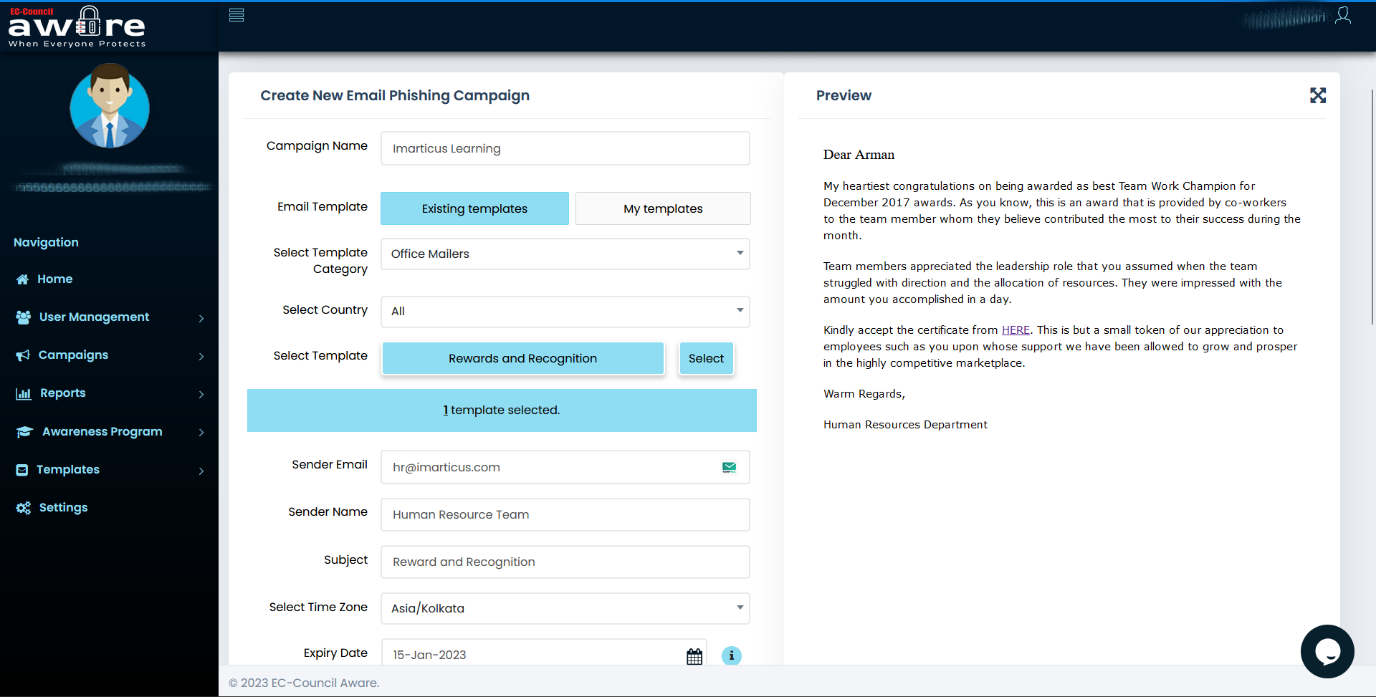


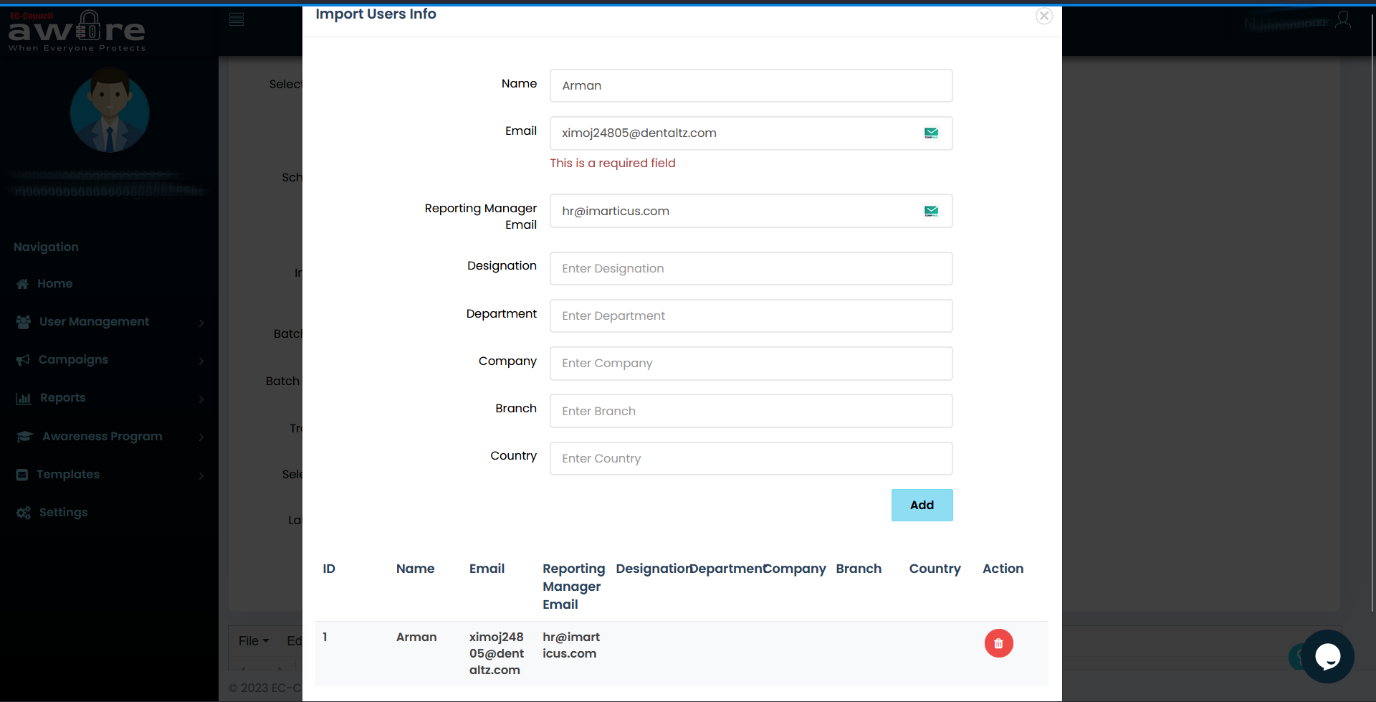
Click on Entice to click.

Fill the details accordingly .

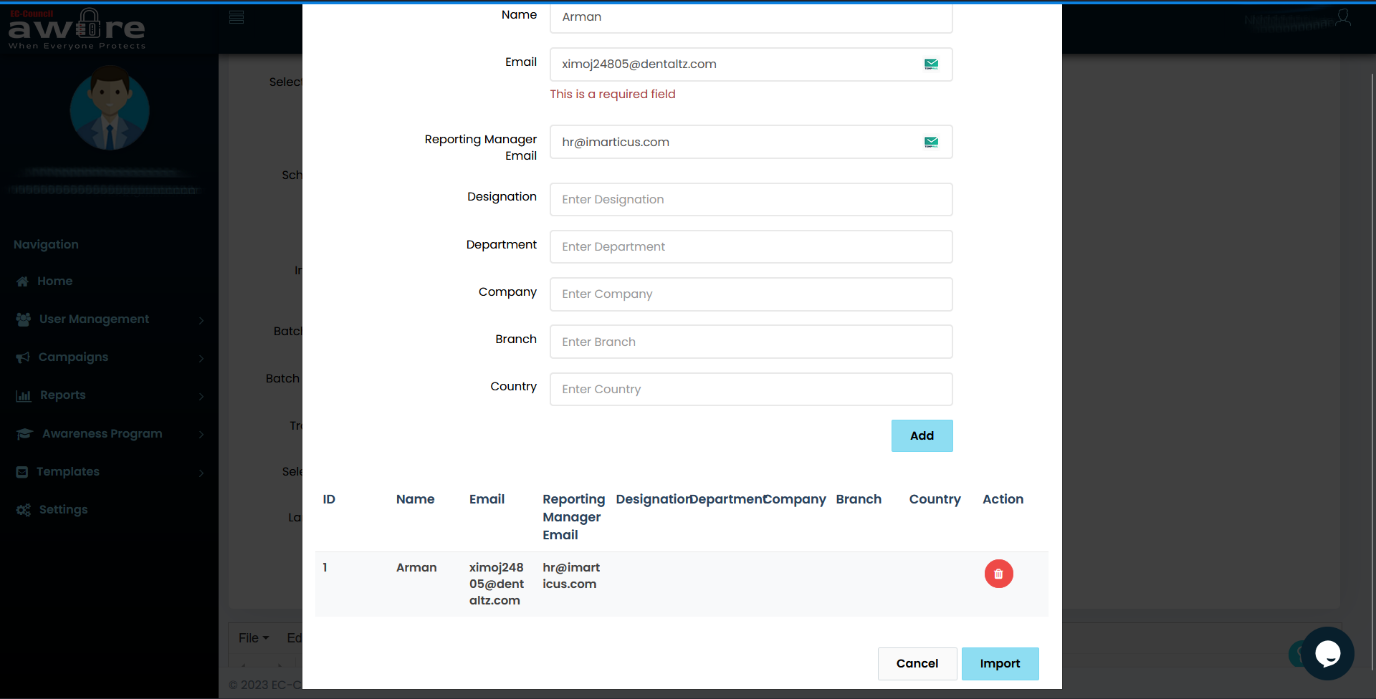


You can see preview in right side and edit mail in edit box.

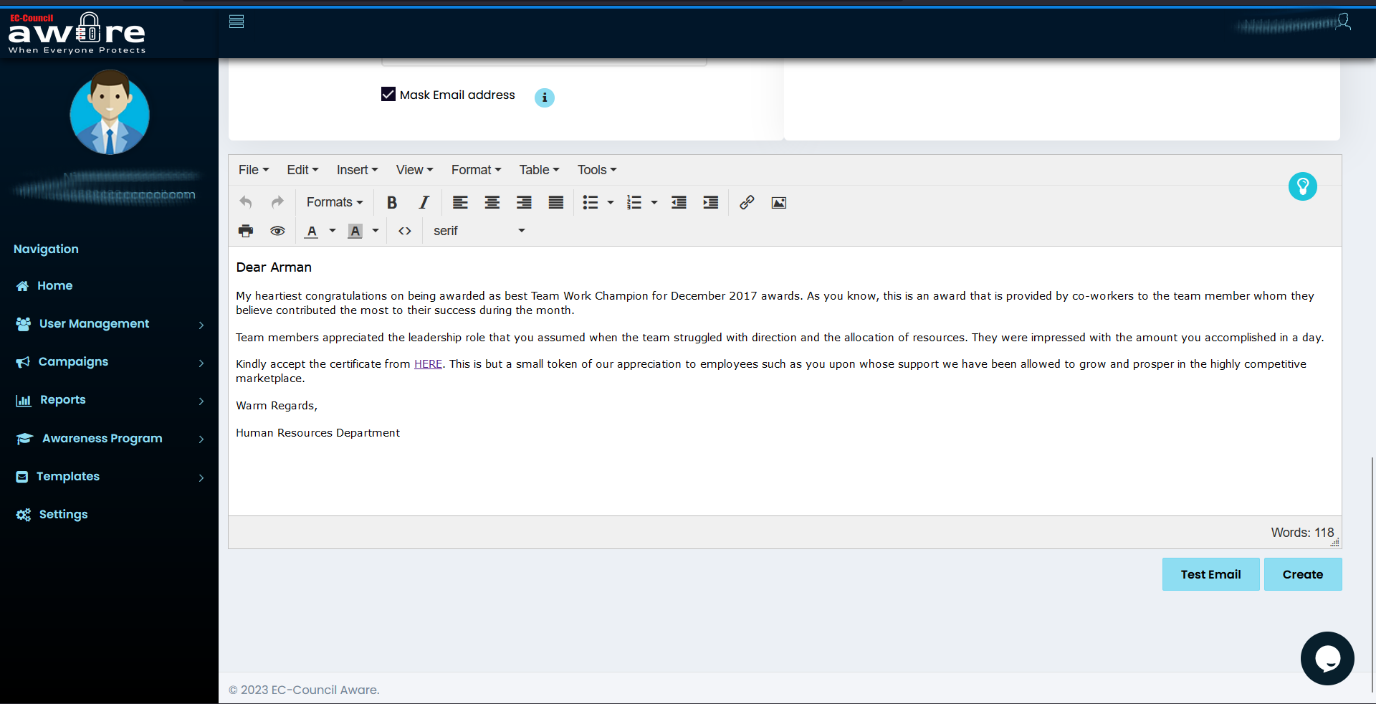




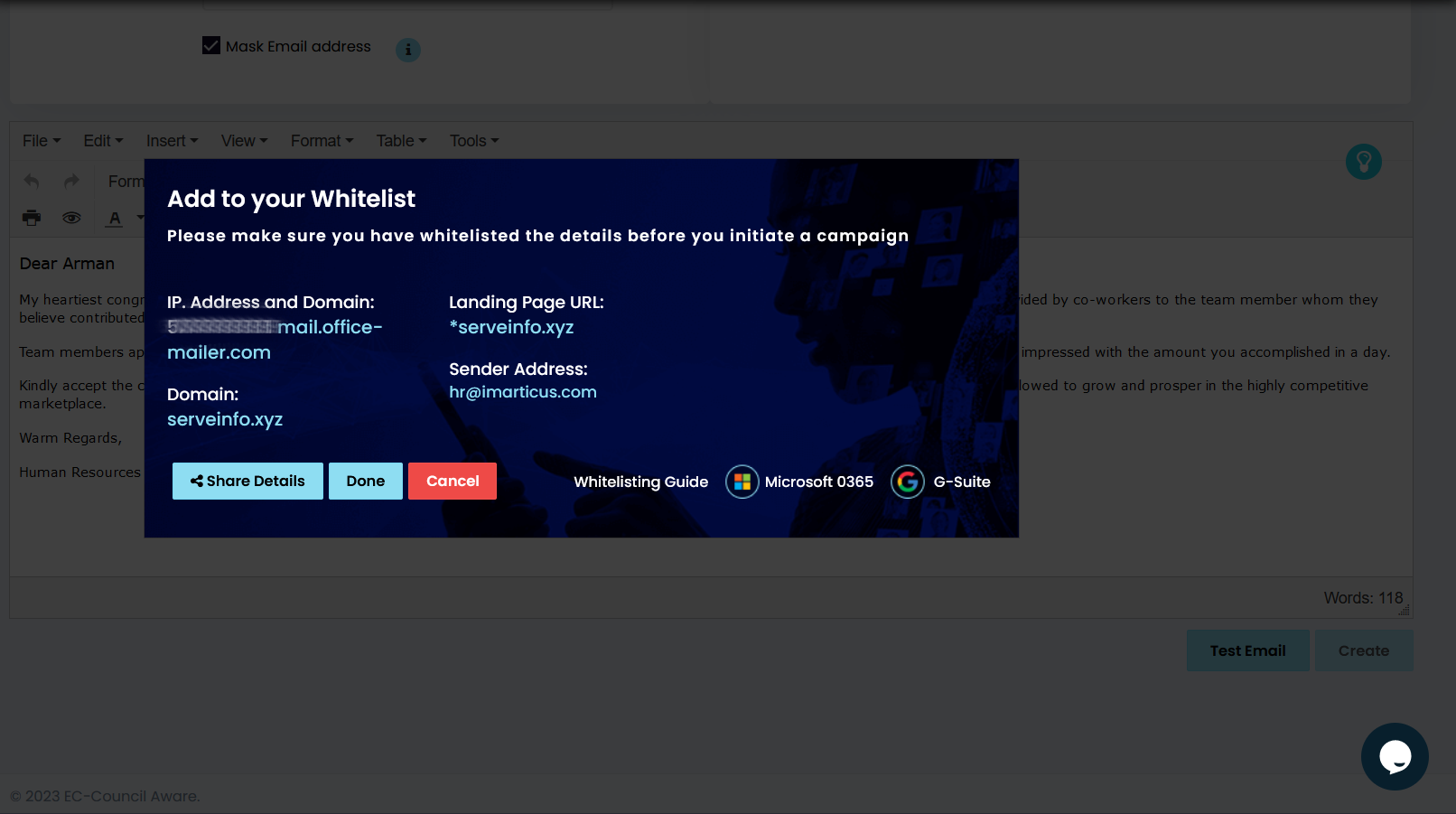
After filling the details of victim click on import



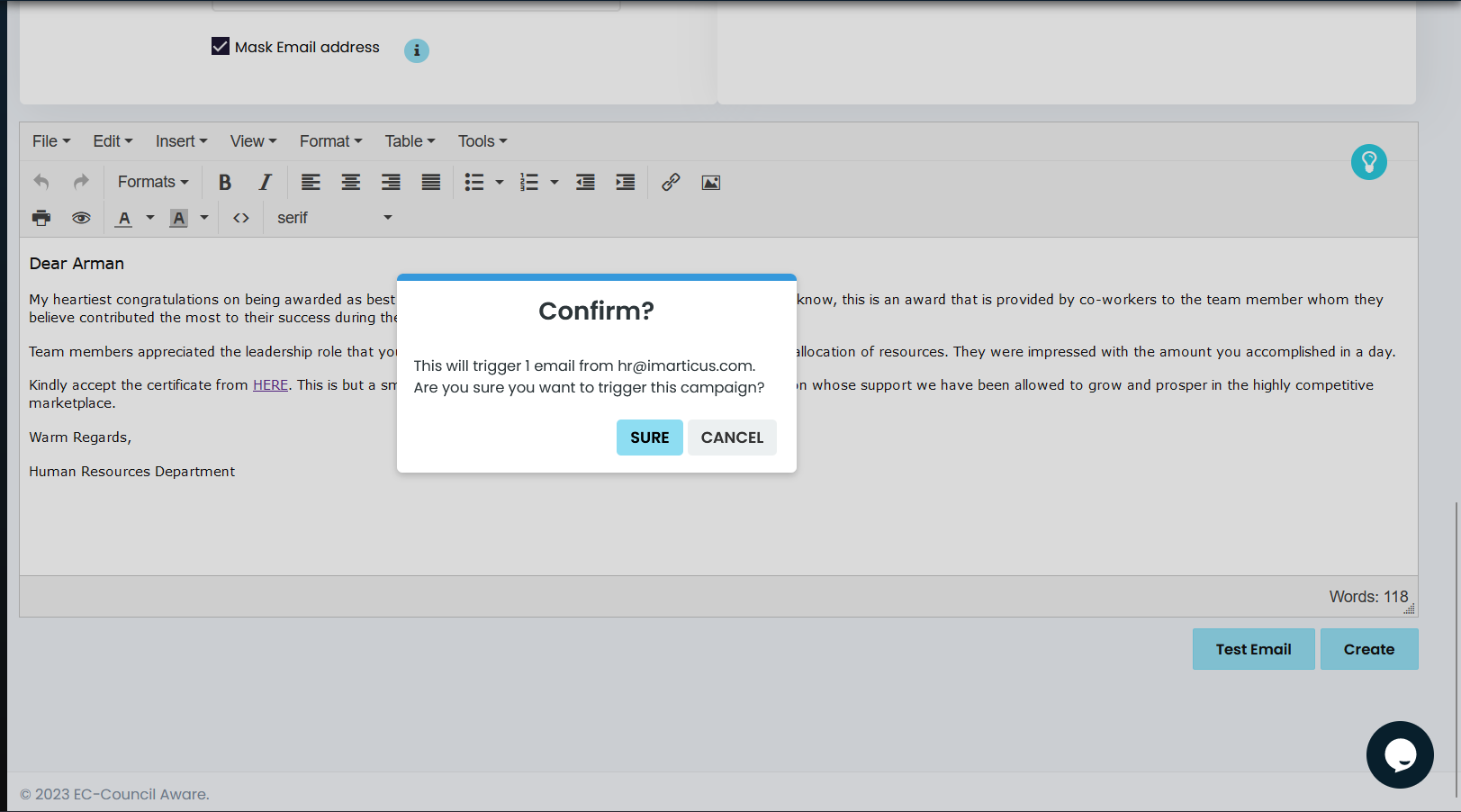
Click on create



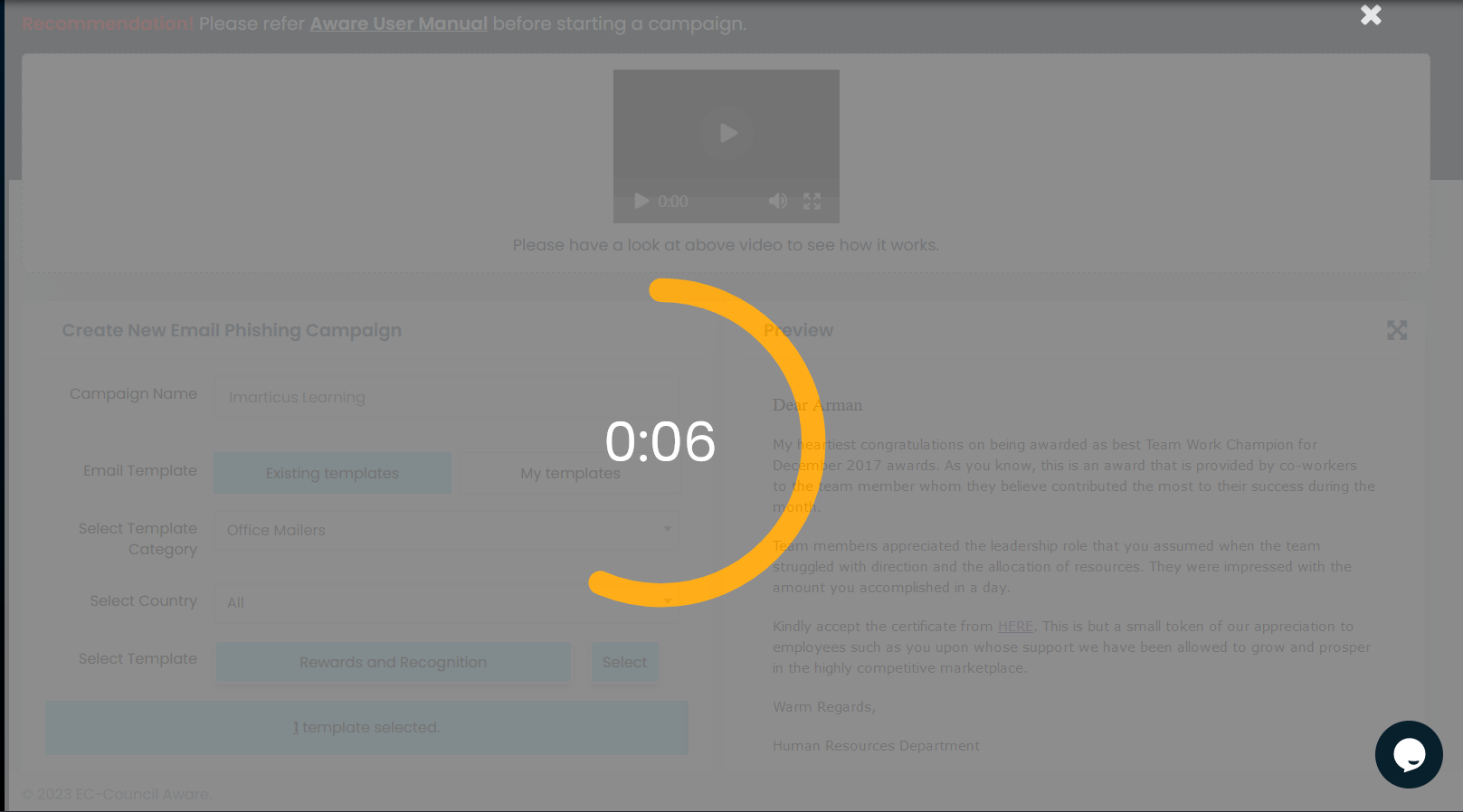
Click on done



It ask for confirmation, click sure



Creating …

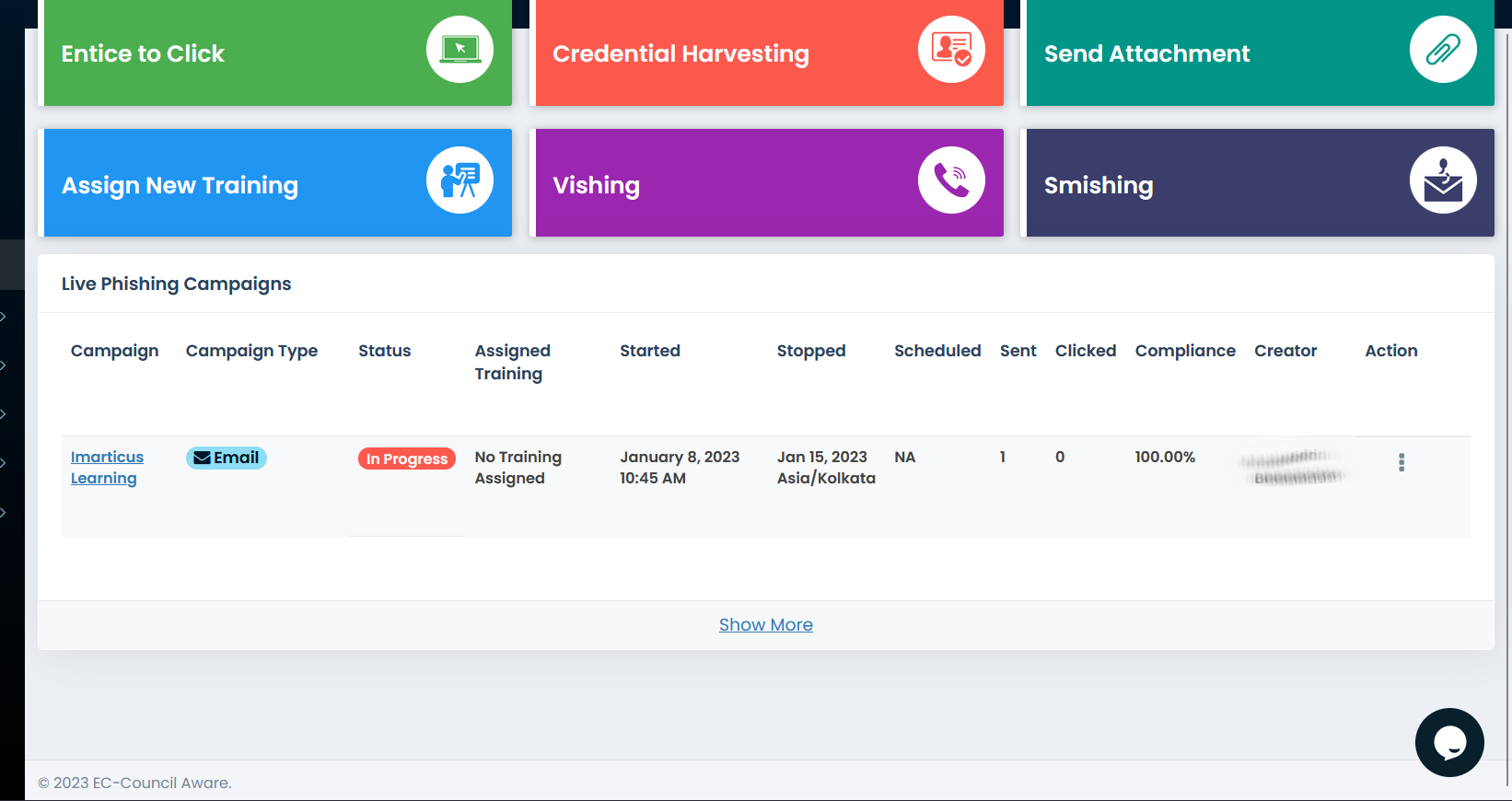


You can see live compaigns in dashboard

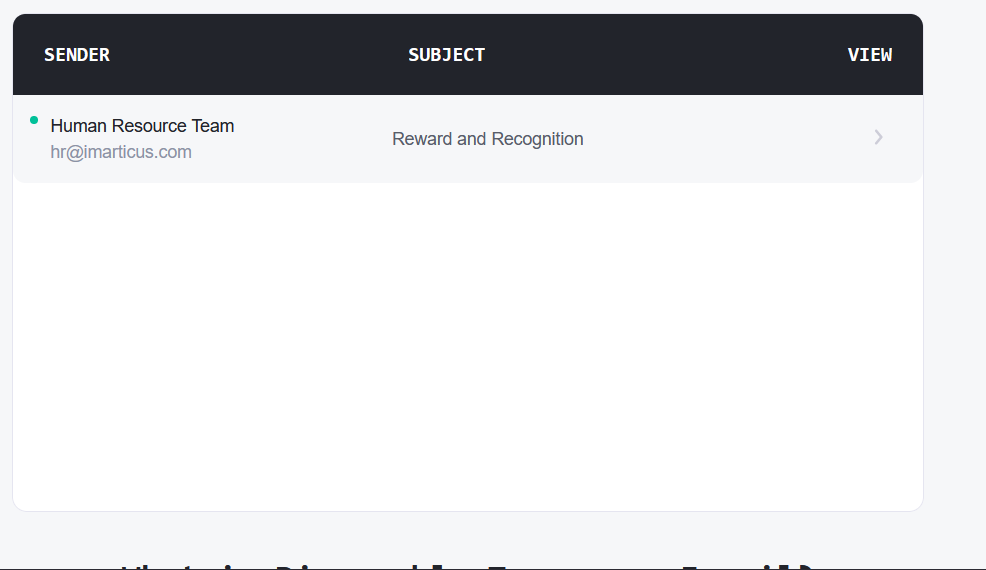
Details :

| **Campaign** | **Campaign Type** | **Status** | **Assigned Training** | **Started** | **Stopped** | **Scheduled** | **Sent** | **Clicked** | **Compliance** | **Creator** | **Action** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |

At a first the clicked tab is 0 because user didn’t clicked link on mail or opened mail.

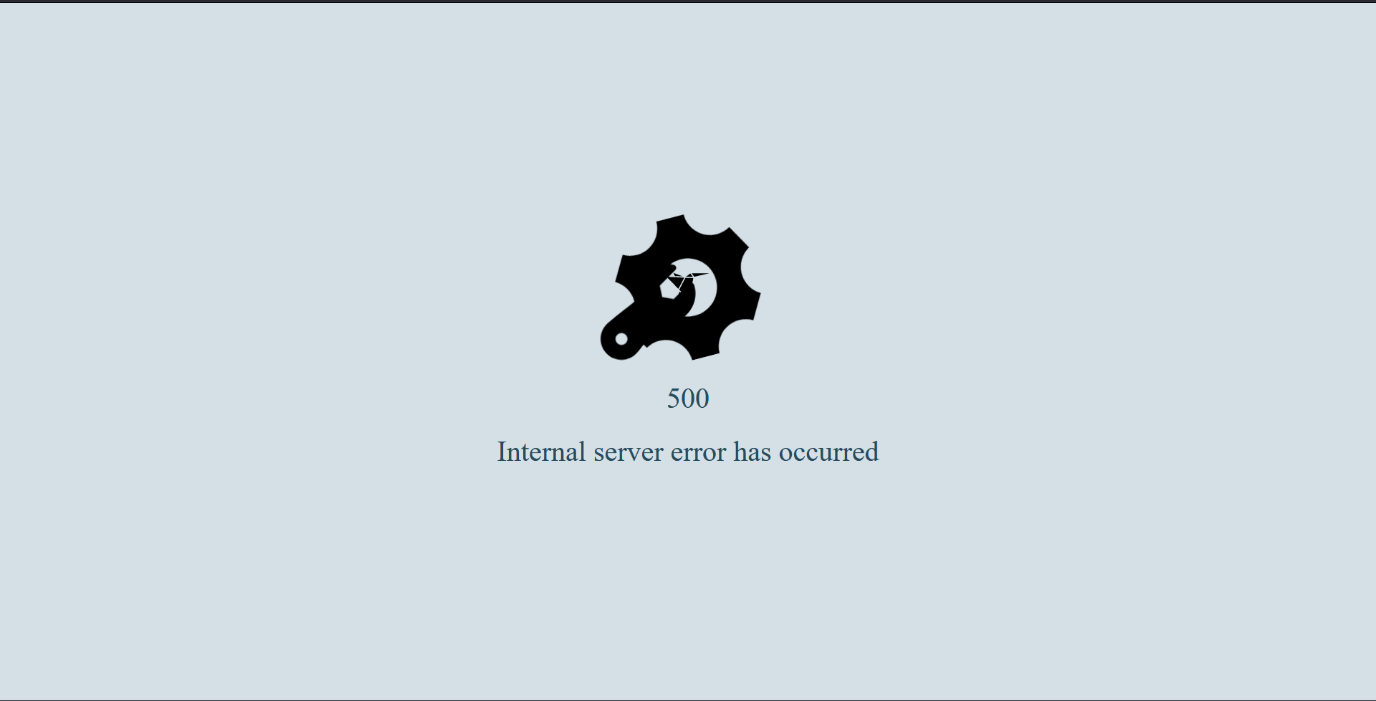


User mail inbox:

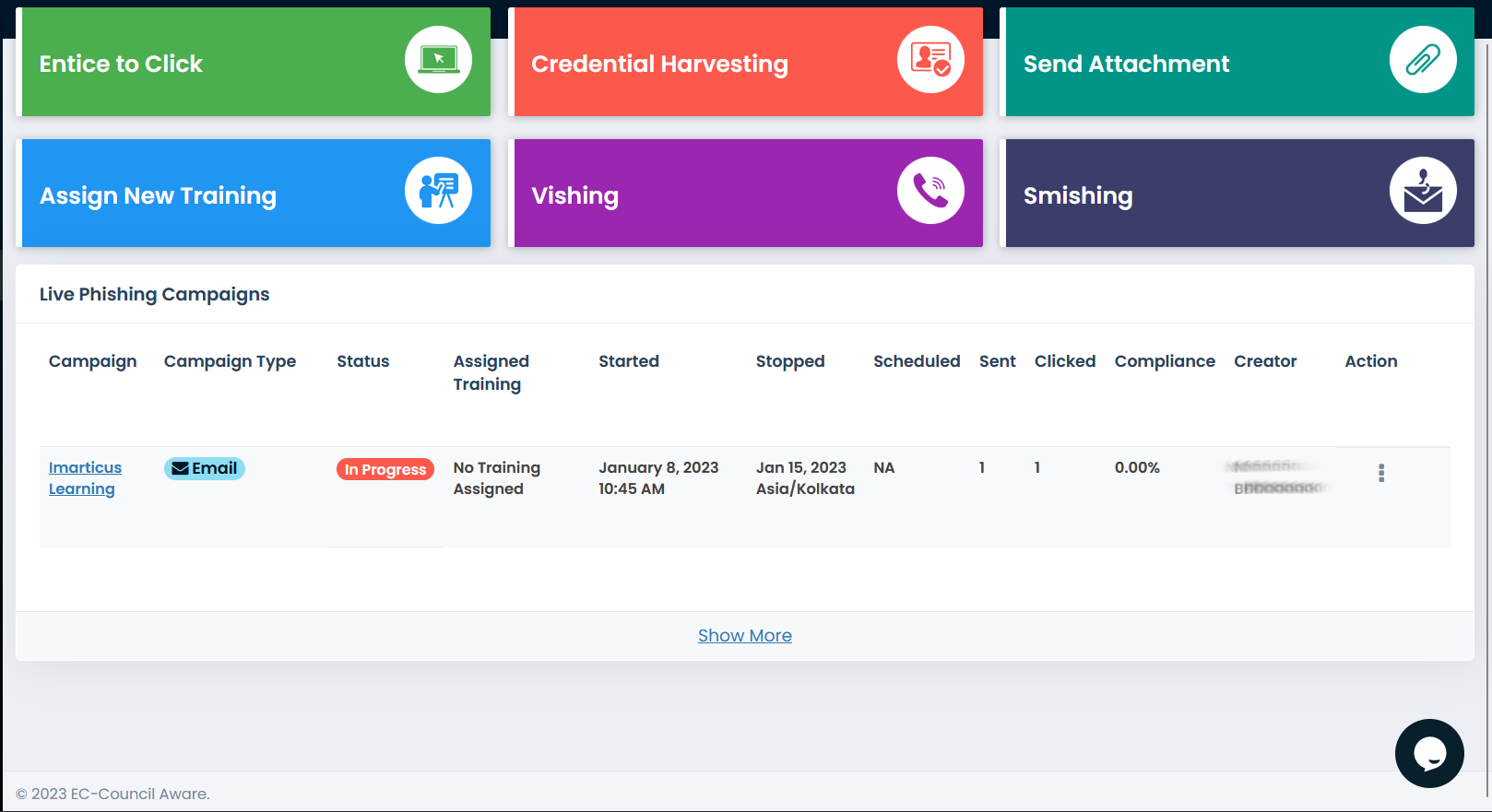




After user clicked link it’s redirect to the page and it’s hows internal server error because we puted like this so user will think its server error and server is not working or down .

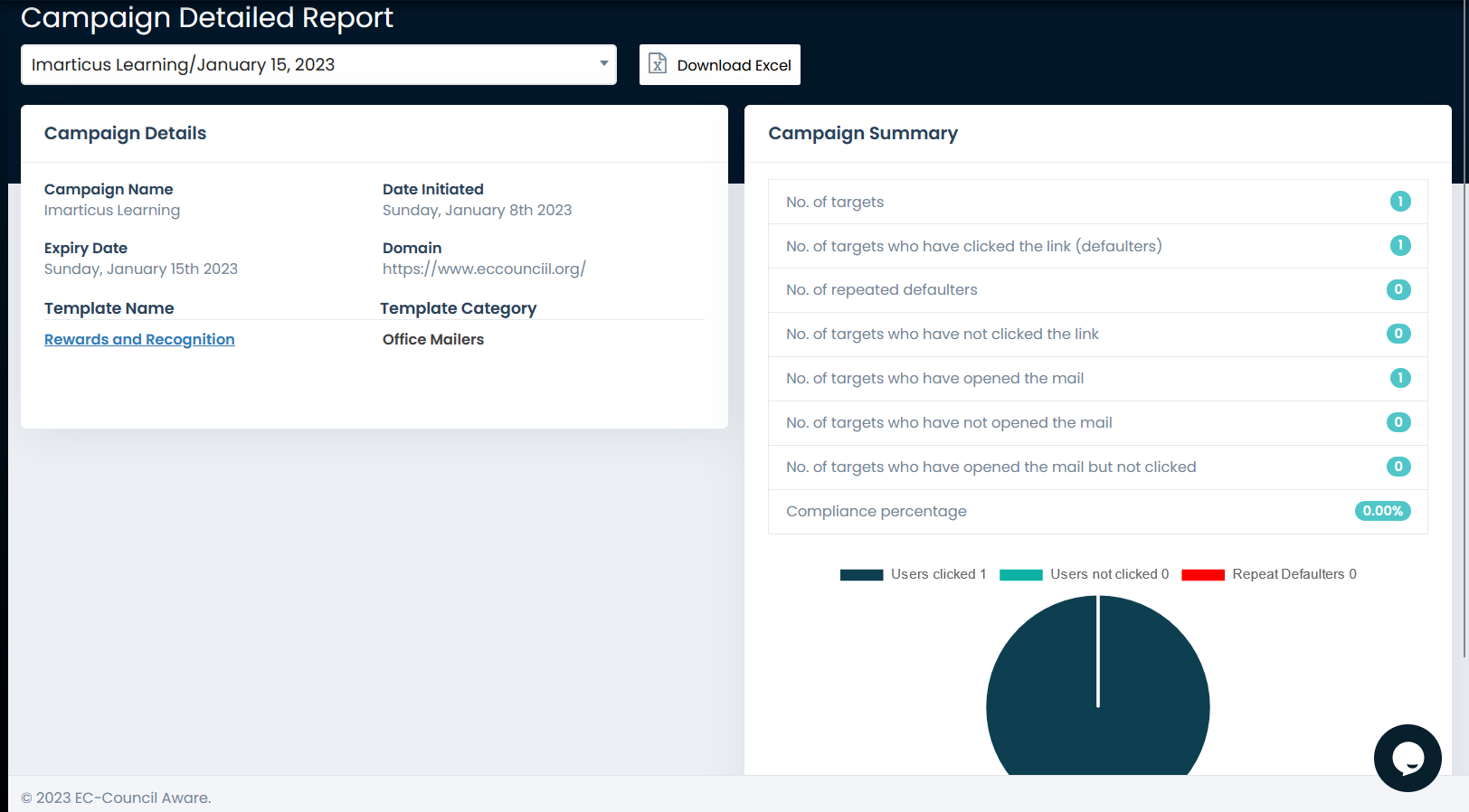


You can see in clicked tab number is 1 which means user opened a mail and clicked link.



**Reports :**

**Campaign detailed report:**



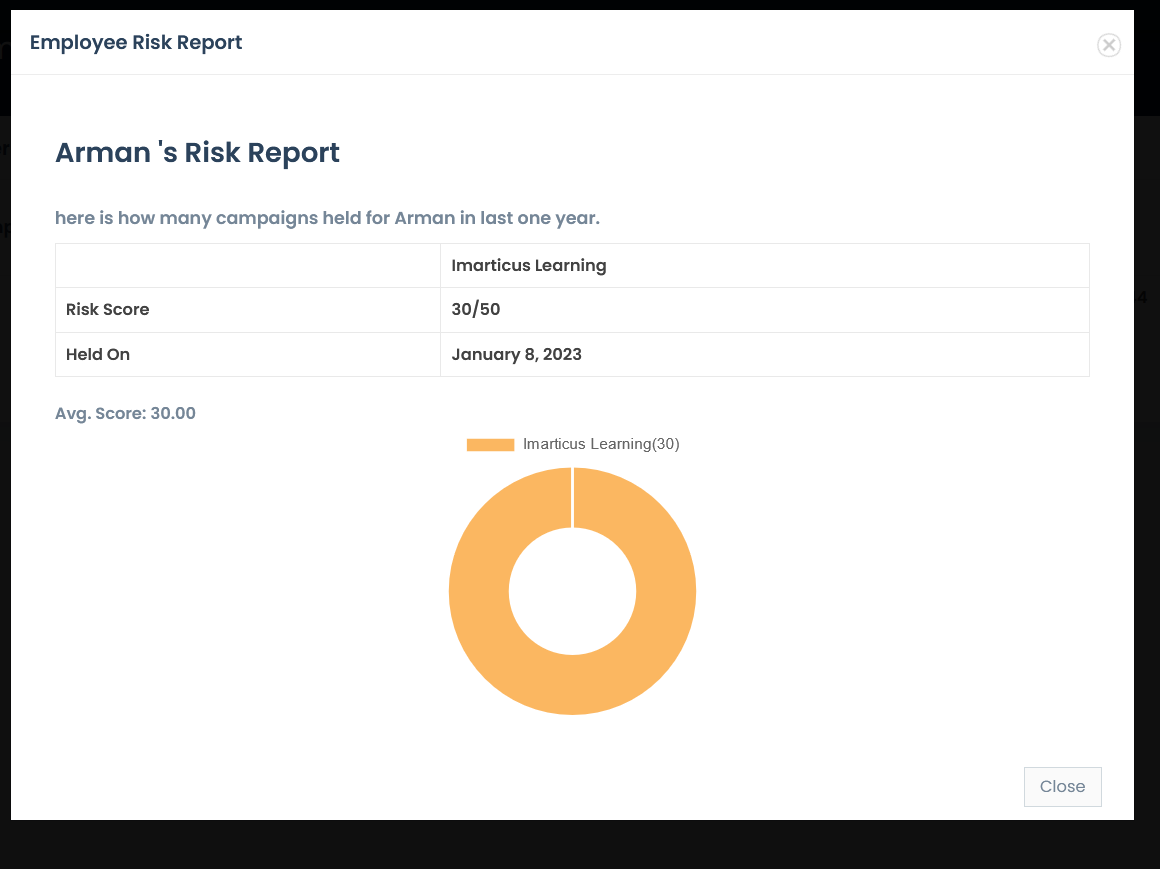
**Phishing campaign history:**



**Campaigns users:**



**Employee risk report:**



● **The information provided by the target on the phishing e-mail and also dropping malware to collect more information cloud be a good choice but stay undetected**

**We are performing second scenario .**

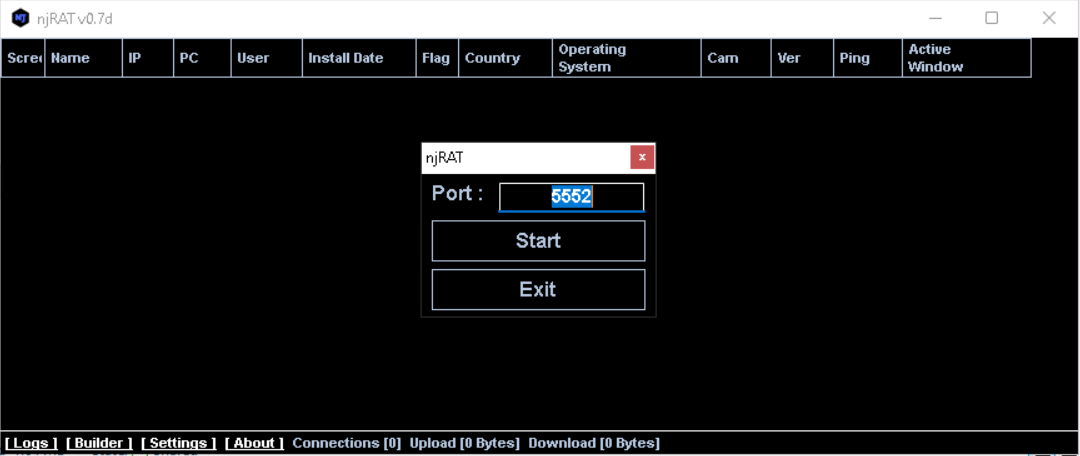
We are targeting person who had taken admission.

**Malware :**

Tool:njrat

We are creating a malware using njrat tool

Once we open njrat its show the promp to set the port, here our port is 5552.

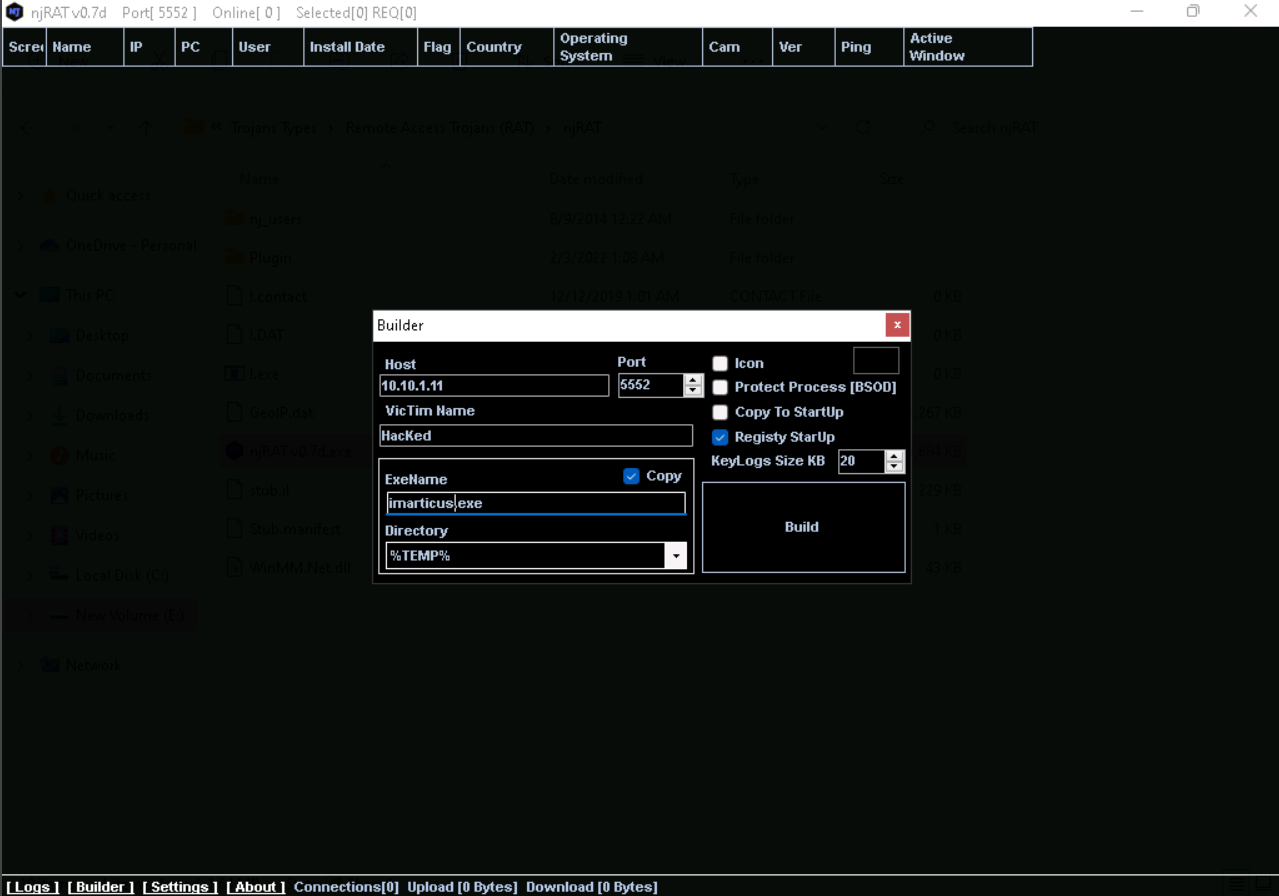


After clicking start we get the dashboard of njrat

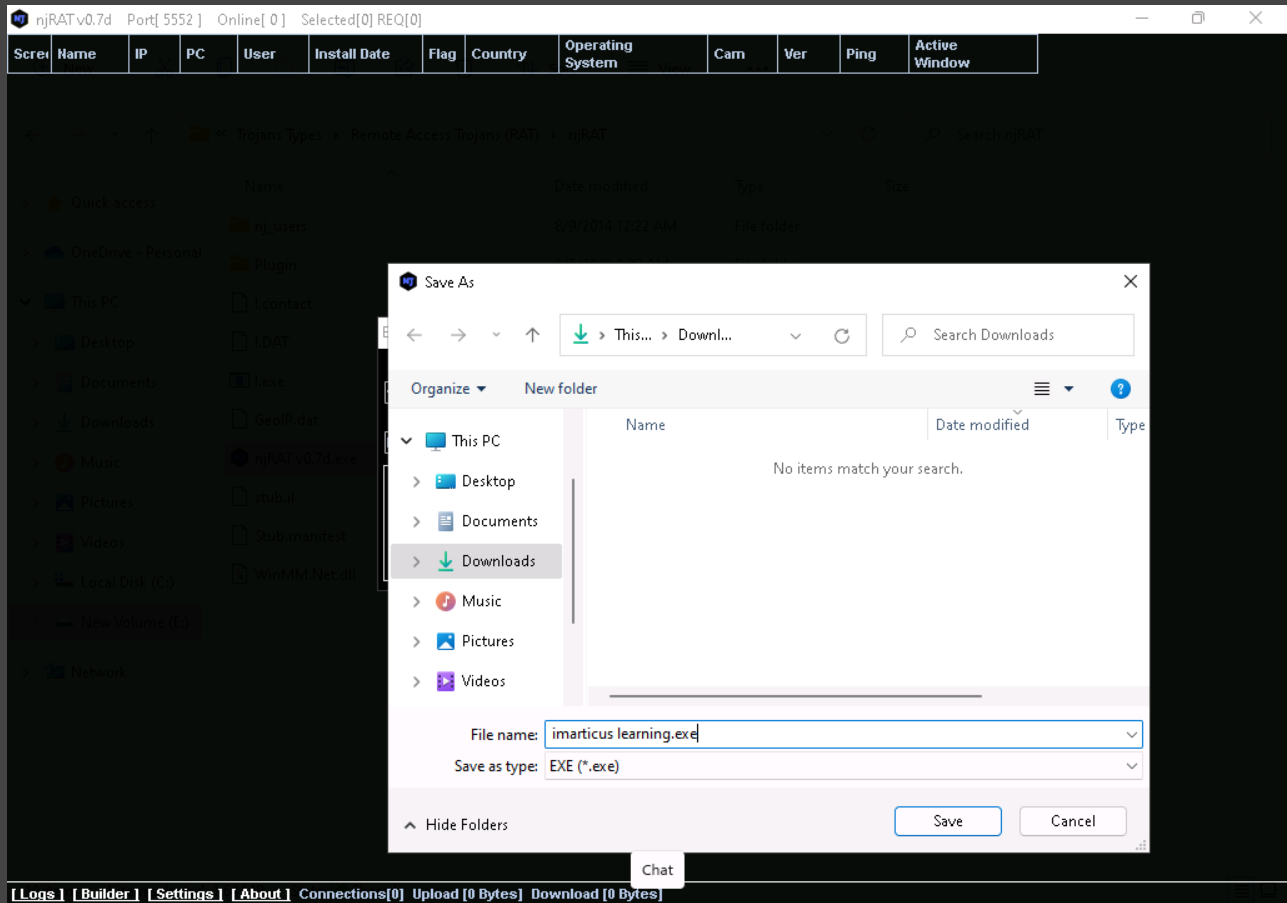


We can find a “Builder” option at the down bar of njrat for build a malware

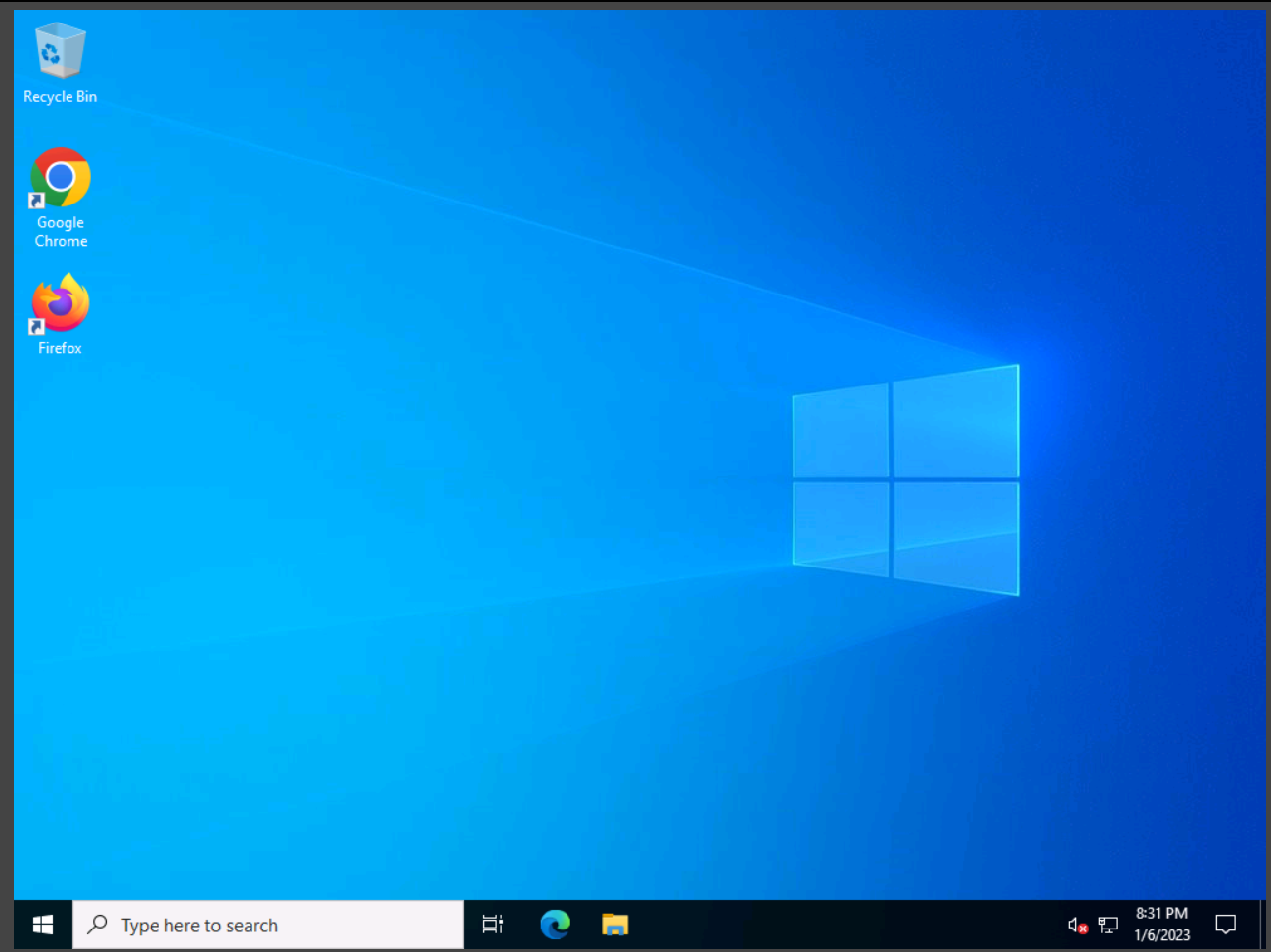
Builder prompt a window in which we can specify host,port,icon,directory ..etc



We save the malware with the organization name so it’s look like legitimate for end user

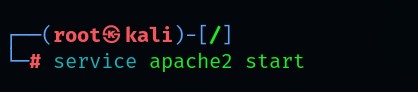


**Victim system**

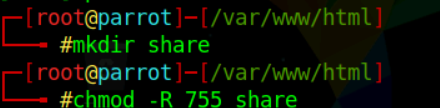


In parrot we are starting apache server in that we can upload our malware on server so the user can browser it





We make a directory in html named share, put the malware in share directory

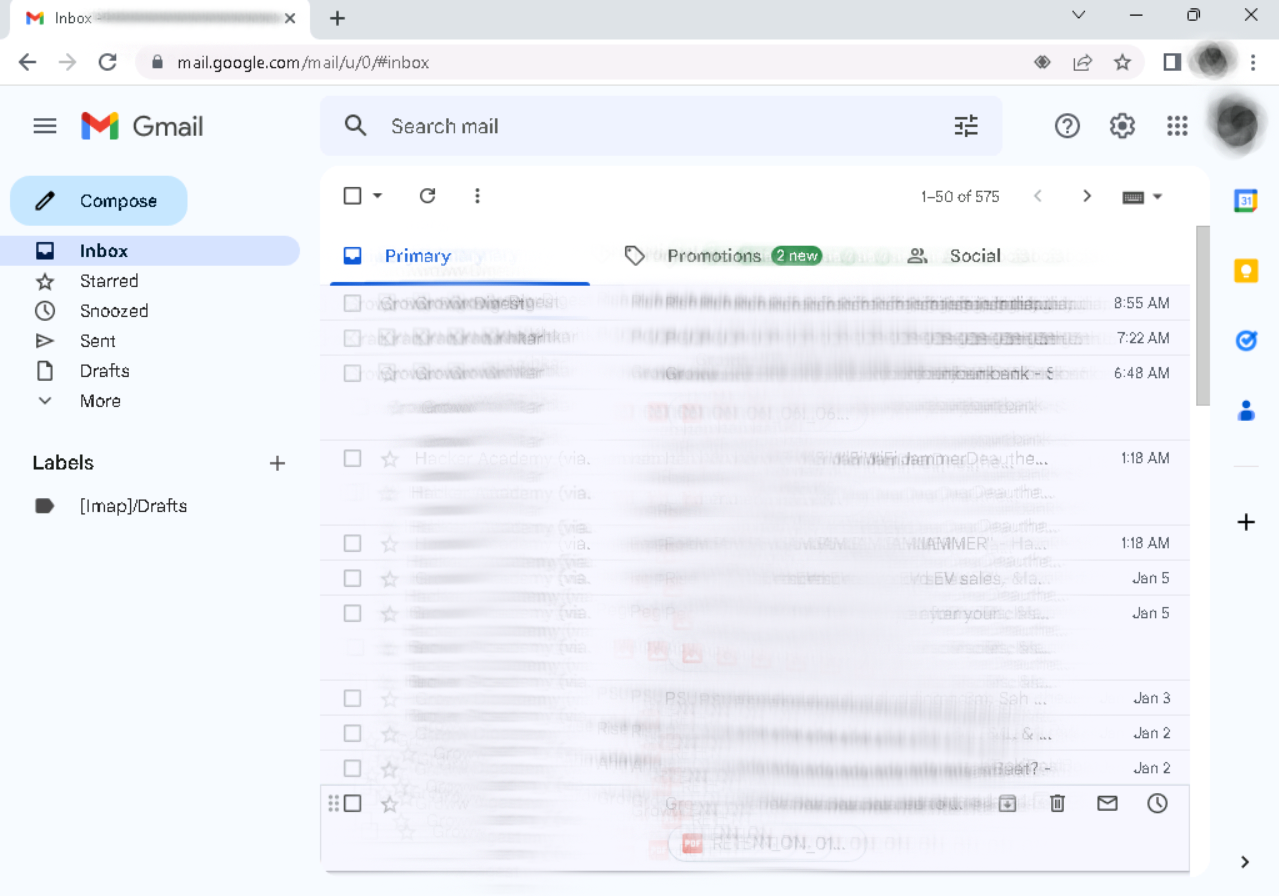


Now we are going to perform the main stage known as social engineering.

As a professional hacker or pentester you have to be able for making a phising mail which look legitimate that user think this is normal or genuine.so user click link or any attachment with out any hesitation.

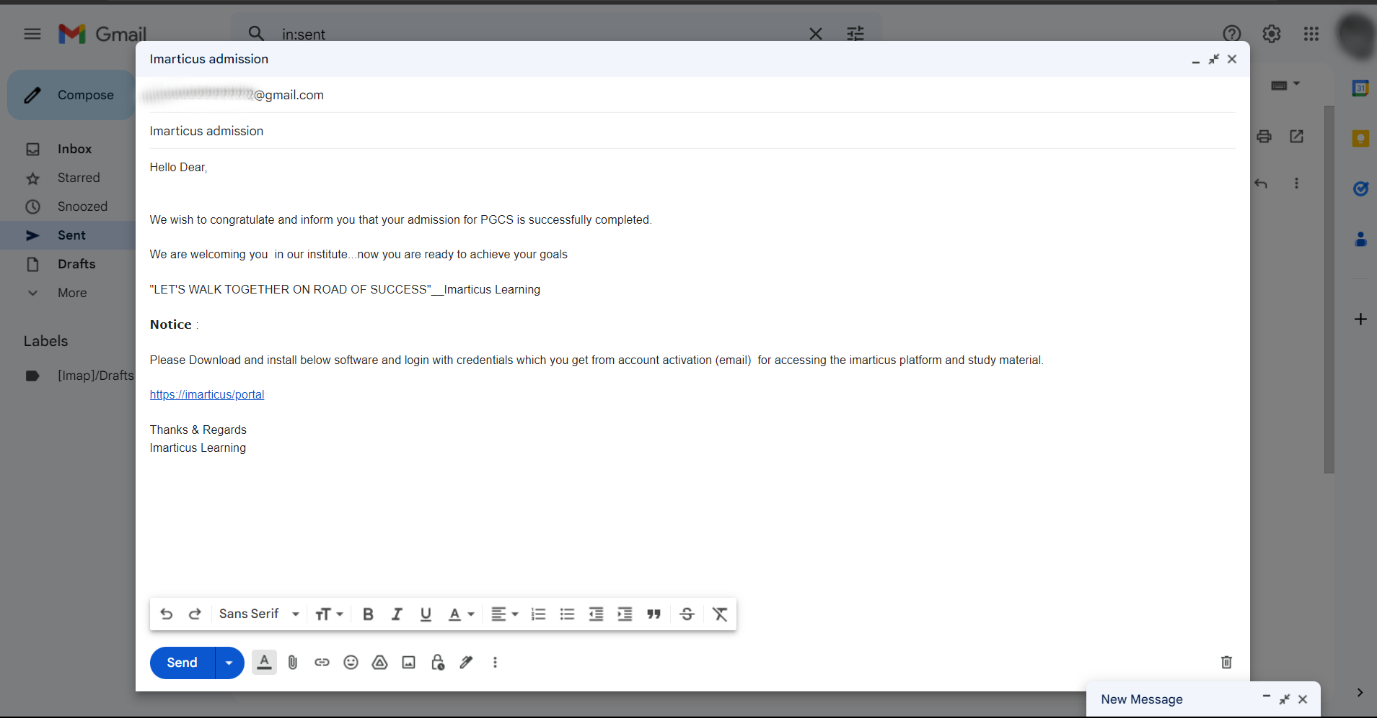
1.Open gmail

2.click on compose



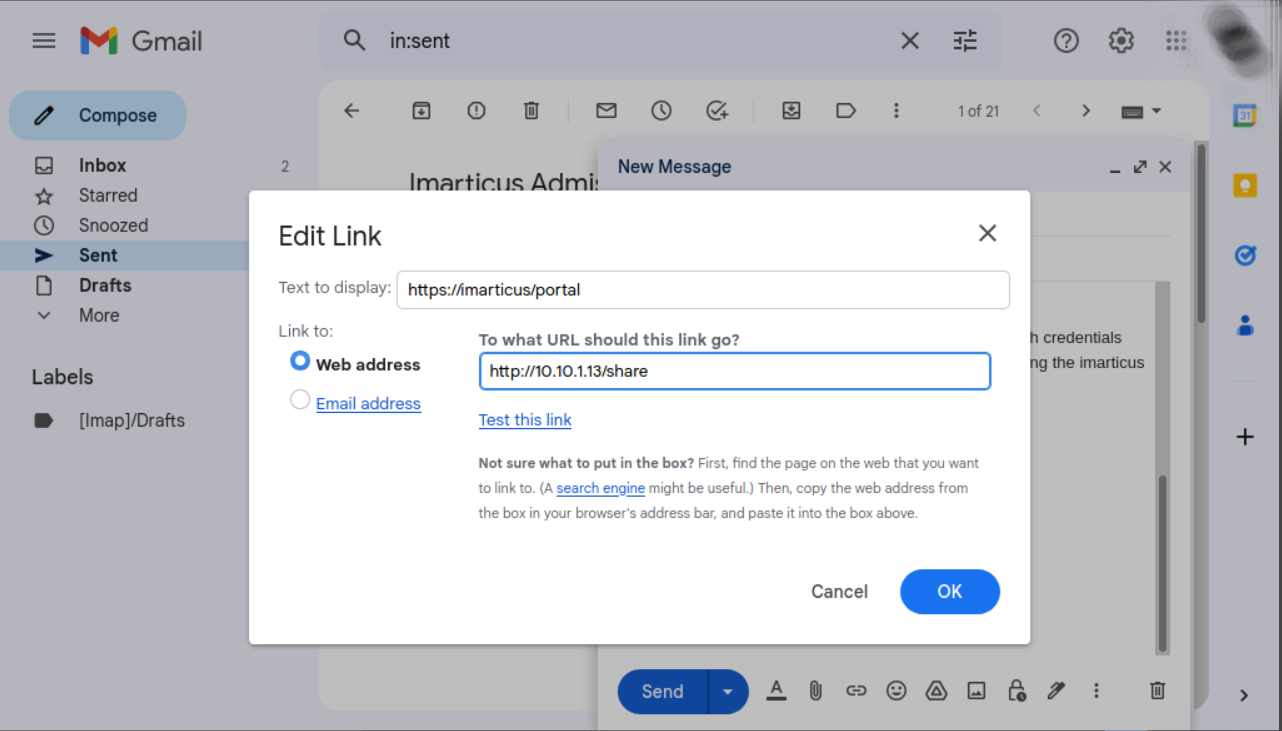
3.Once you click it open a window for writind and sending new mail

4.write a mail which is professional or tempted.



5. hide the original url .

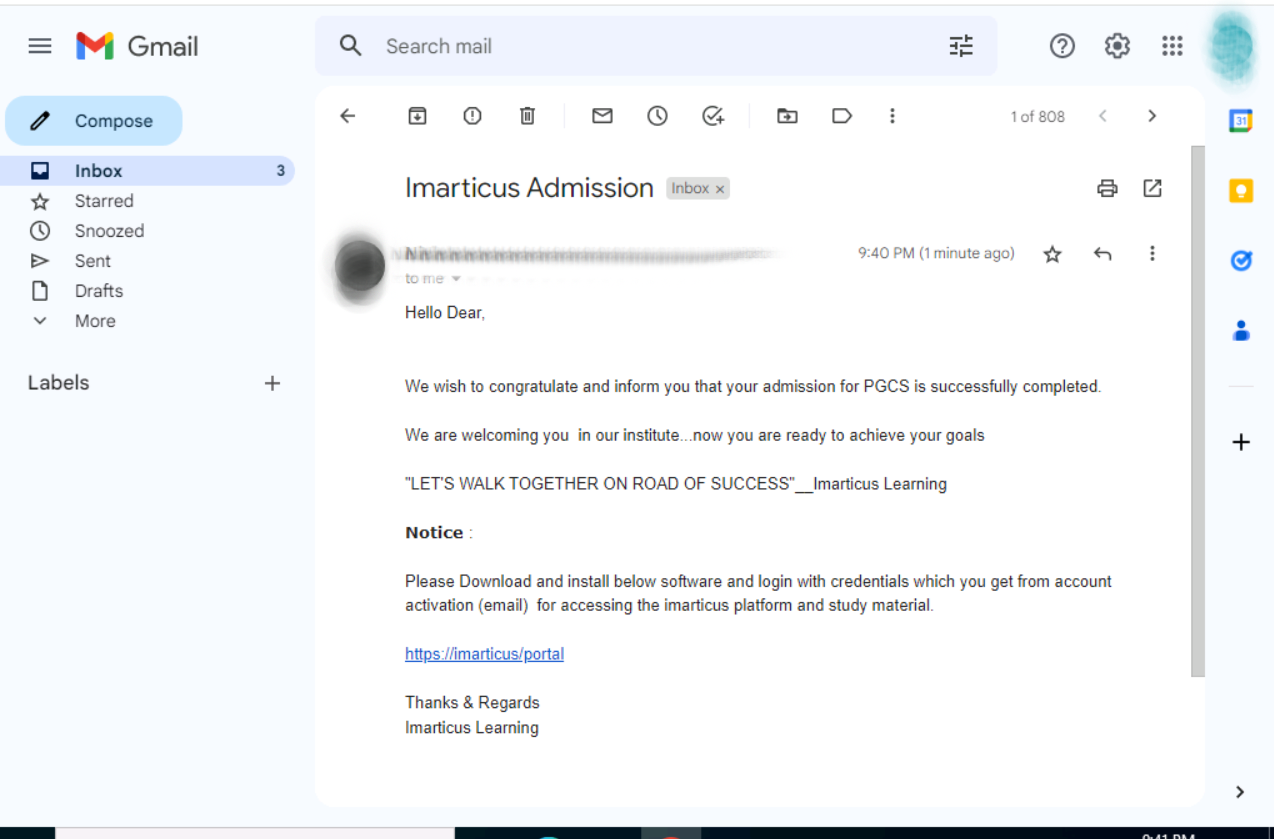
You can see in below image our malicious url is <http://10.10.1.13/share> and we are hiding or masking that url with <https://imarticus/portal>



The user got the mail it’s like this:

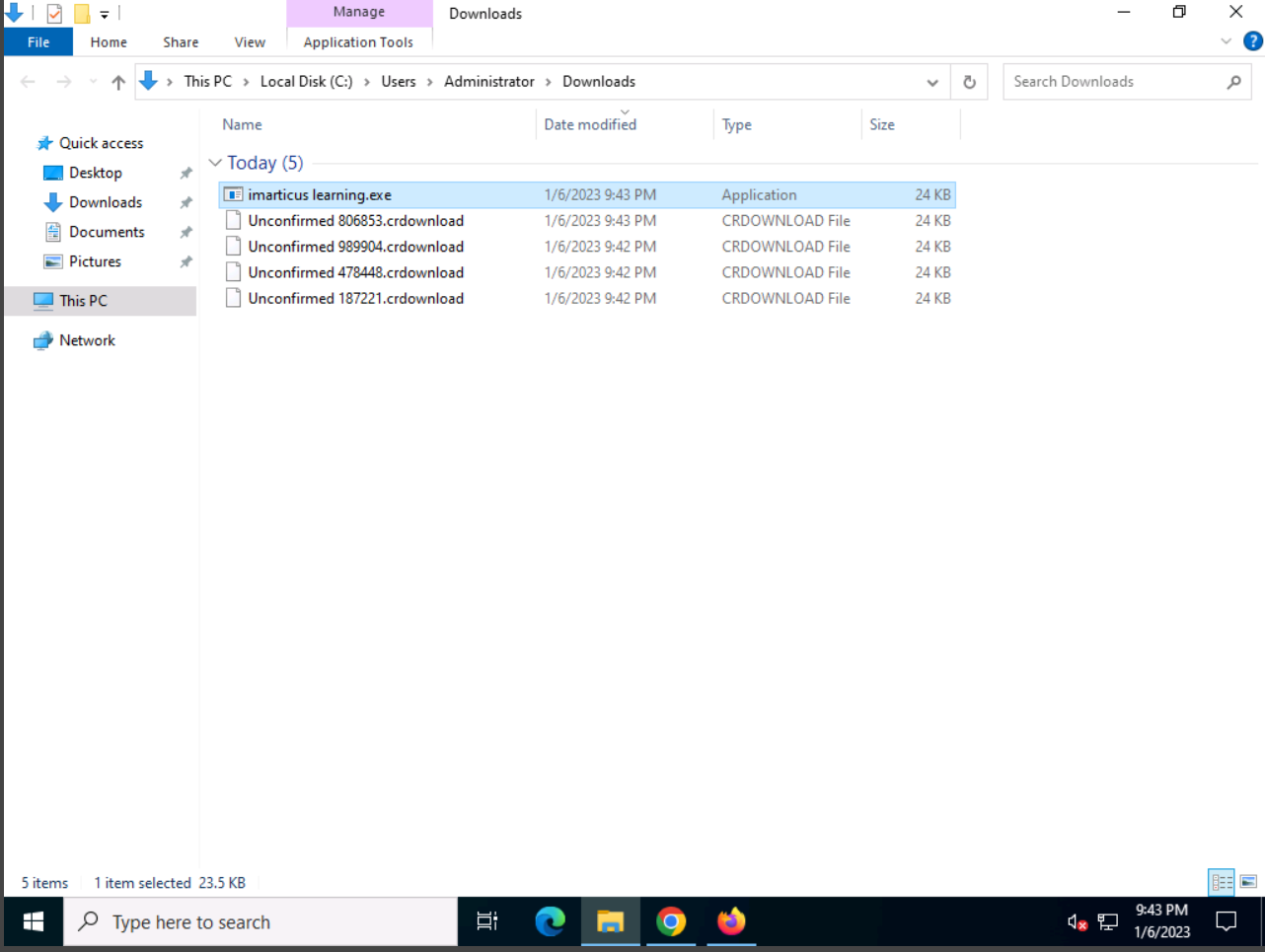
You can see the link in mail which we masked as <https://imarticus/portal>

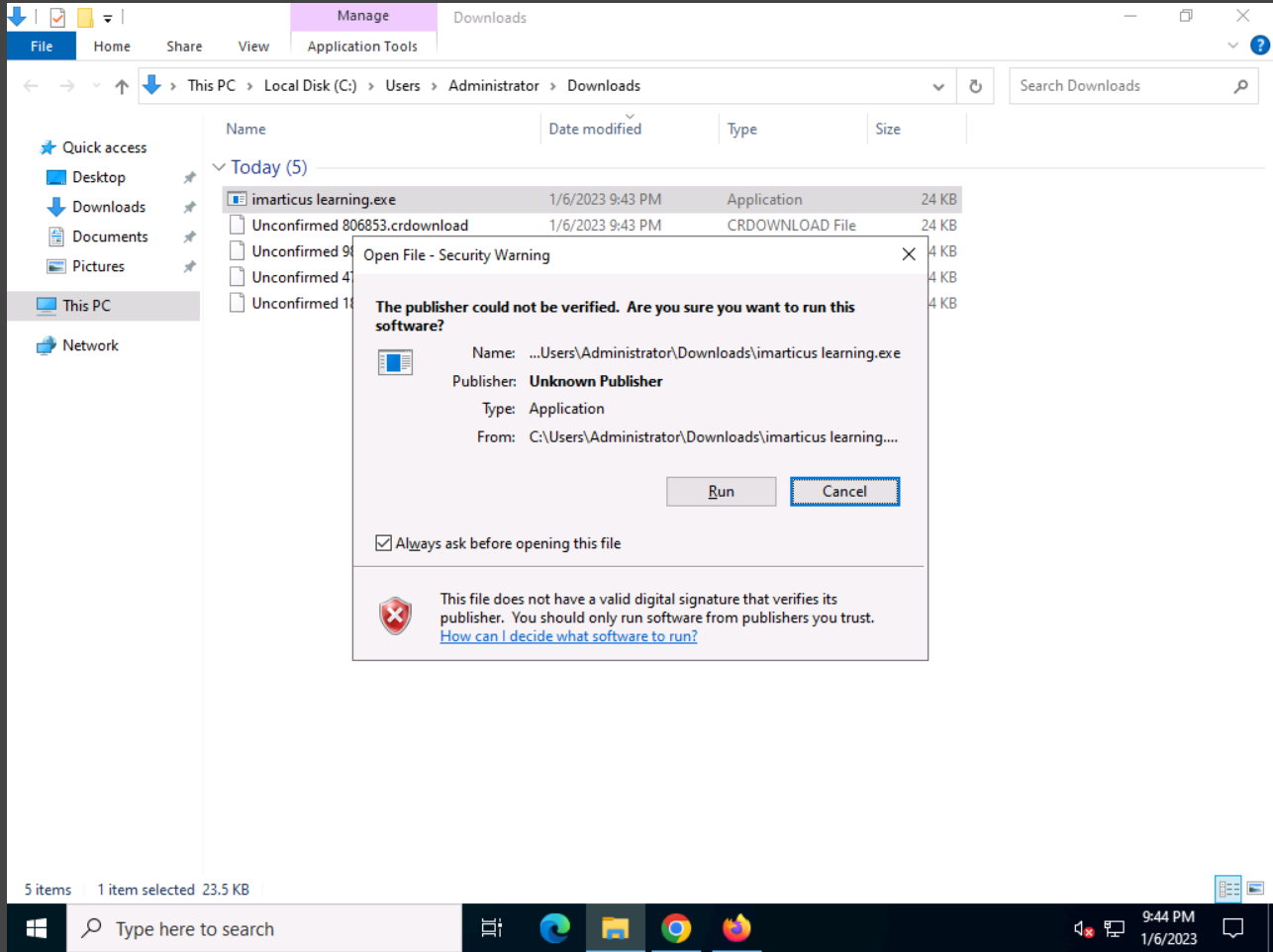
Once user click on it, the link redirect to the malicious link



Because of we craft mail as it’s seems like it’s from organization so user download our malware and think like he or she downloading the original software provided by organization.







Once the user download the malware and install it at a time we successfully exploited and get the access of target or victim system

Which we can see in below image

We successfully get the access of target system

The details we are able to see:

Name:HacKed\_64f81Af7

Ip:10.10.1.22

Pc:SERVER2012

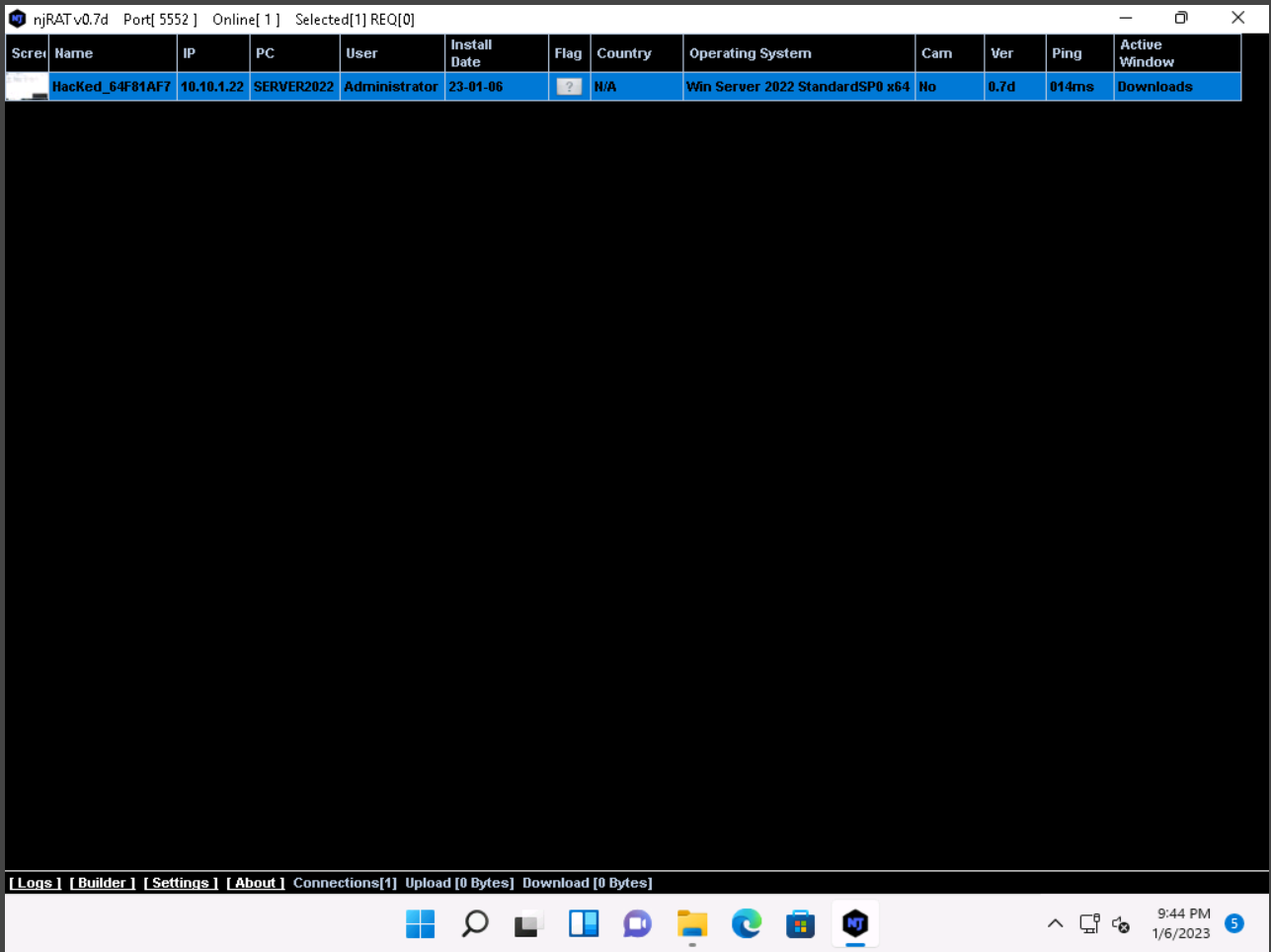
User :Administrator

Install date:23-01-06

Country:N/A

Os: Win server 2022 standard dsp0 x64

Active window:Downloads



Through right clicking on the tab we can see dop down list.

We can perform all the things which under the drop down list

Manager

Run file

Remote cam

Microphone

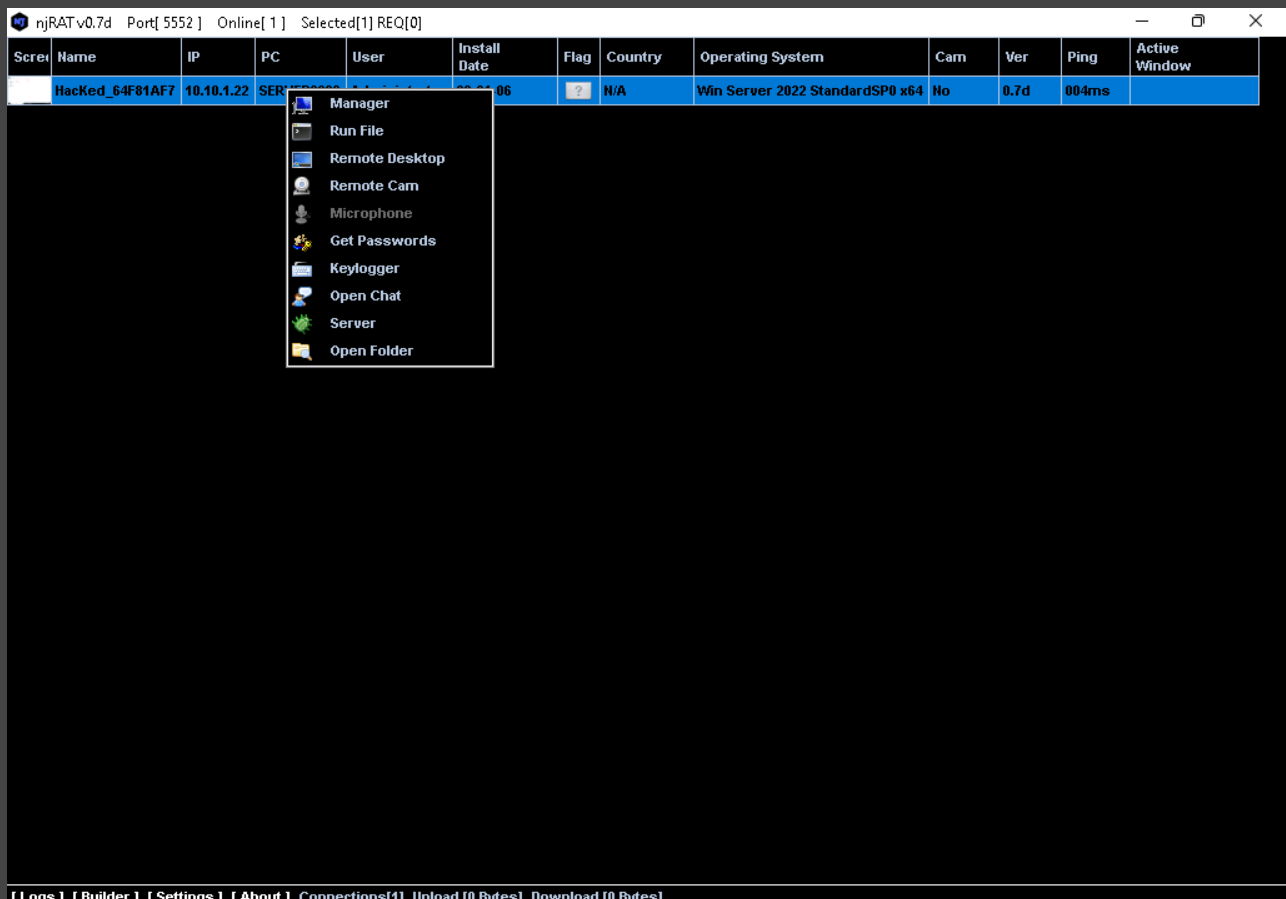
Get passwrods

Keylogger

Openchat

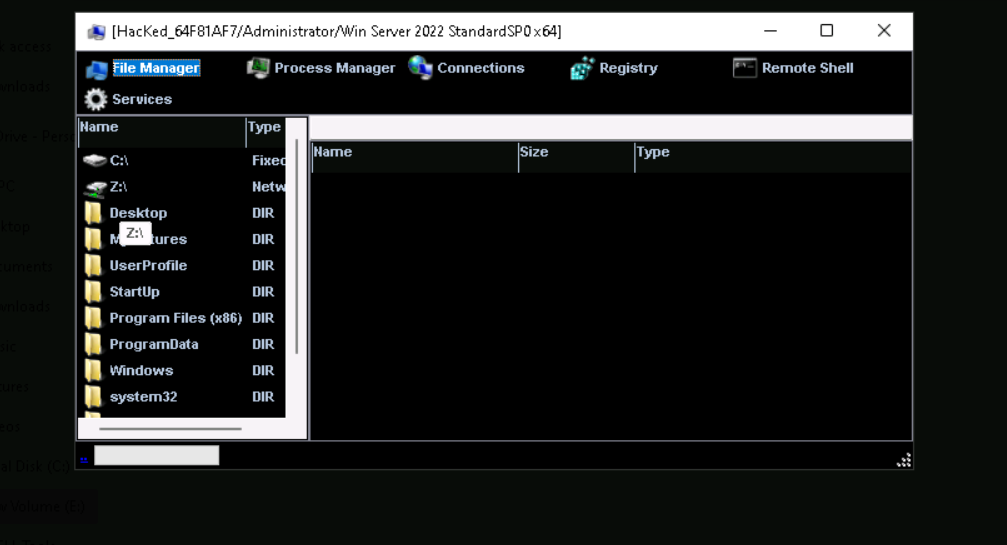
Server

Openfolder

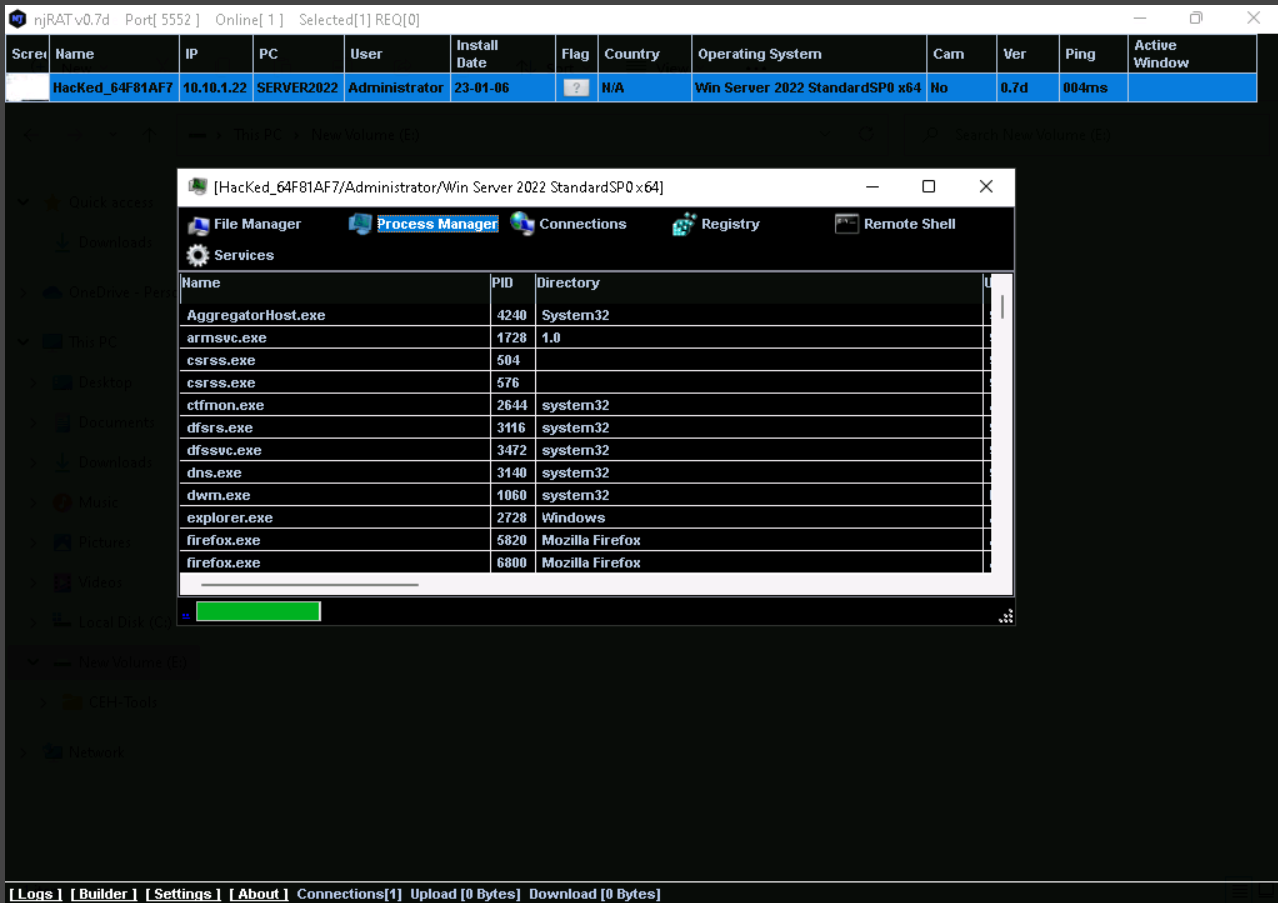


**Victim system…**

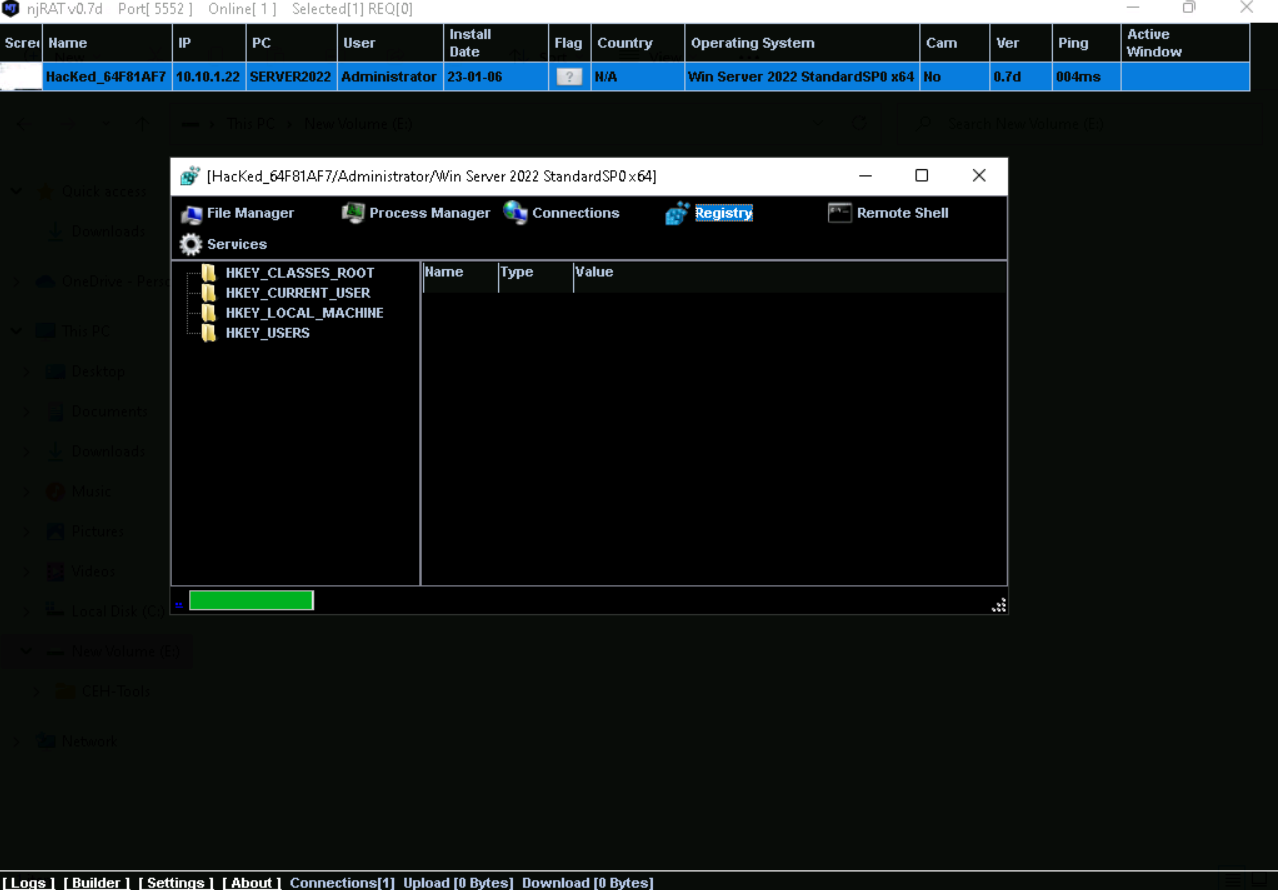
**File manager :**



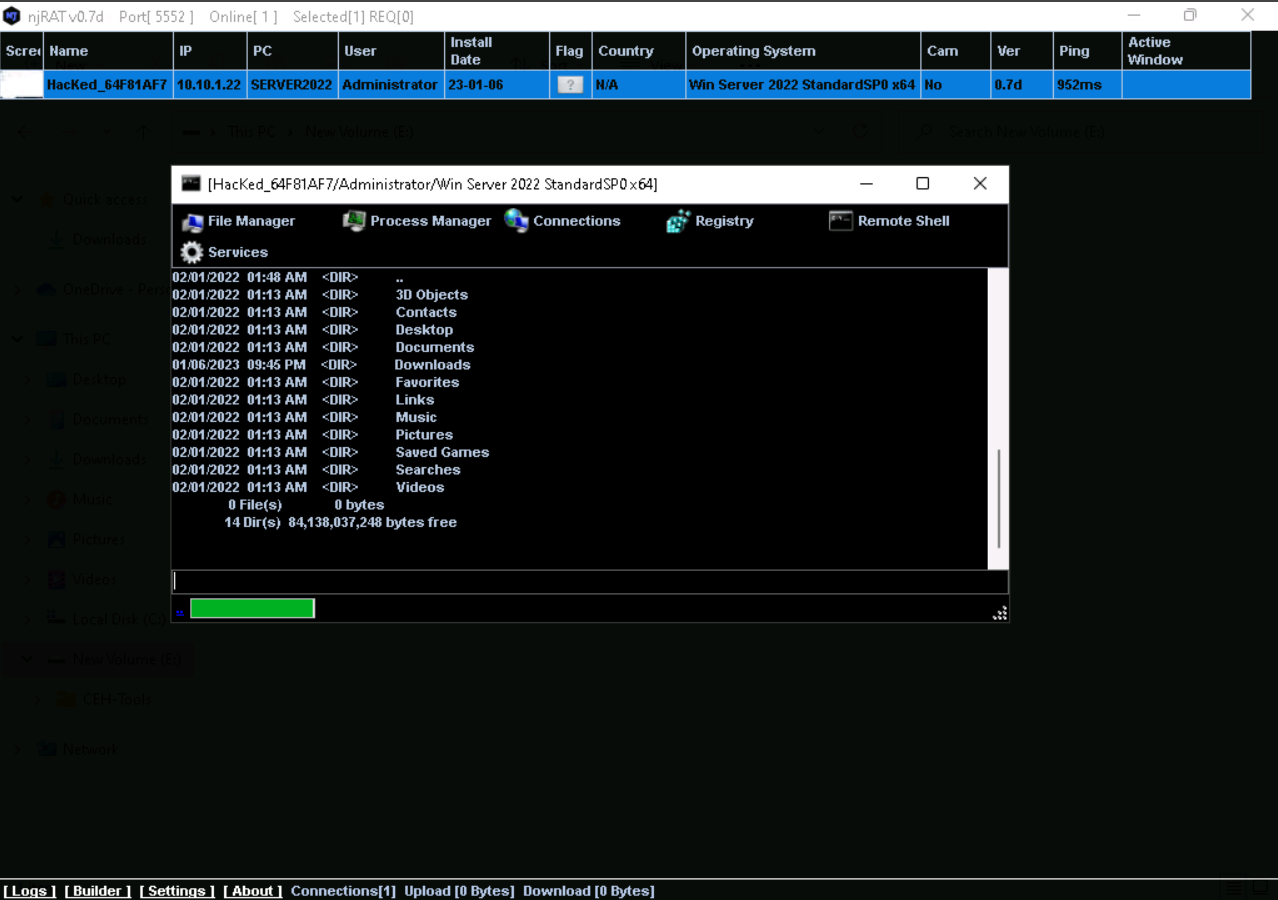
**Services:**



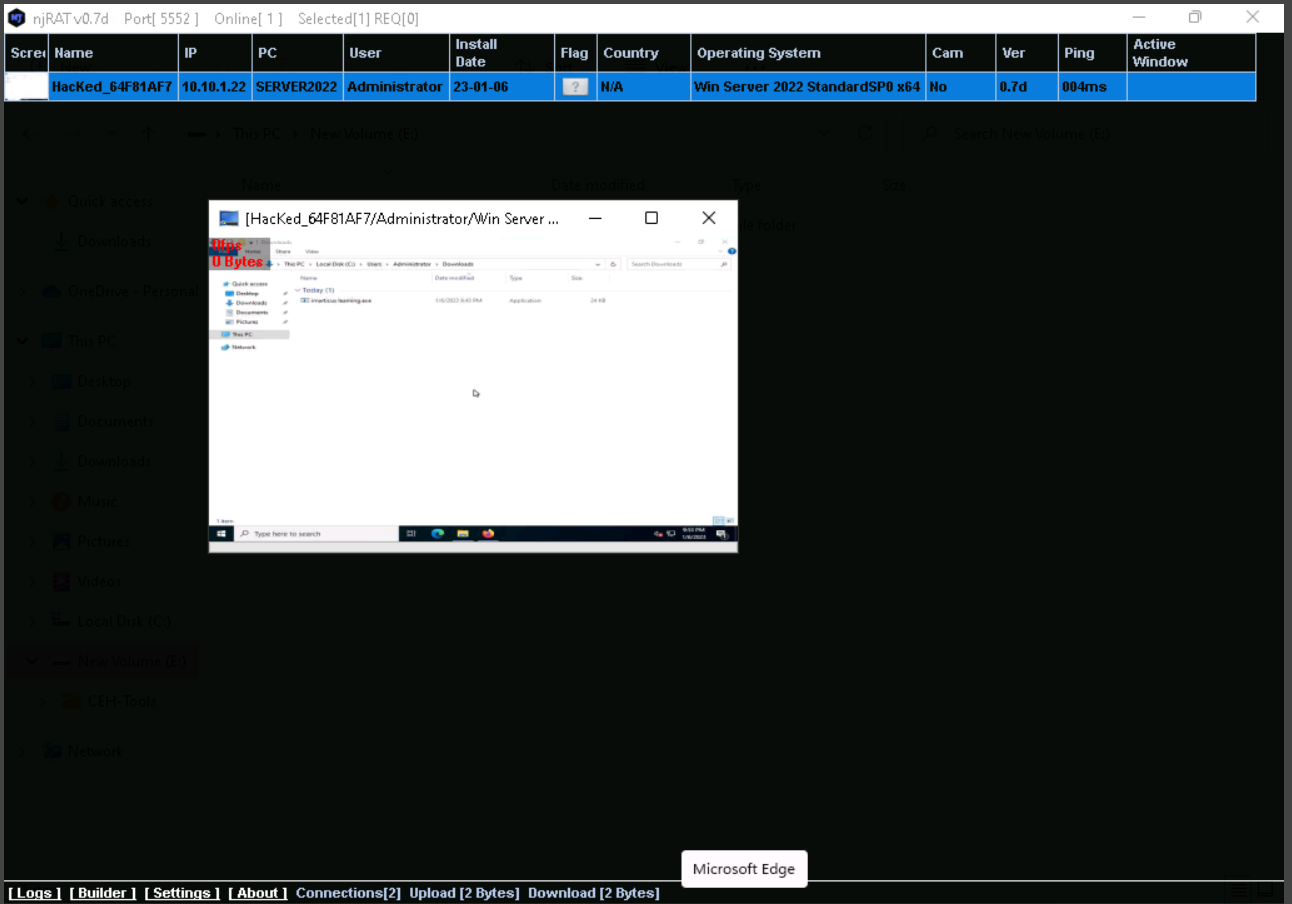
**Registry:**

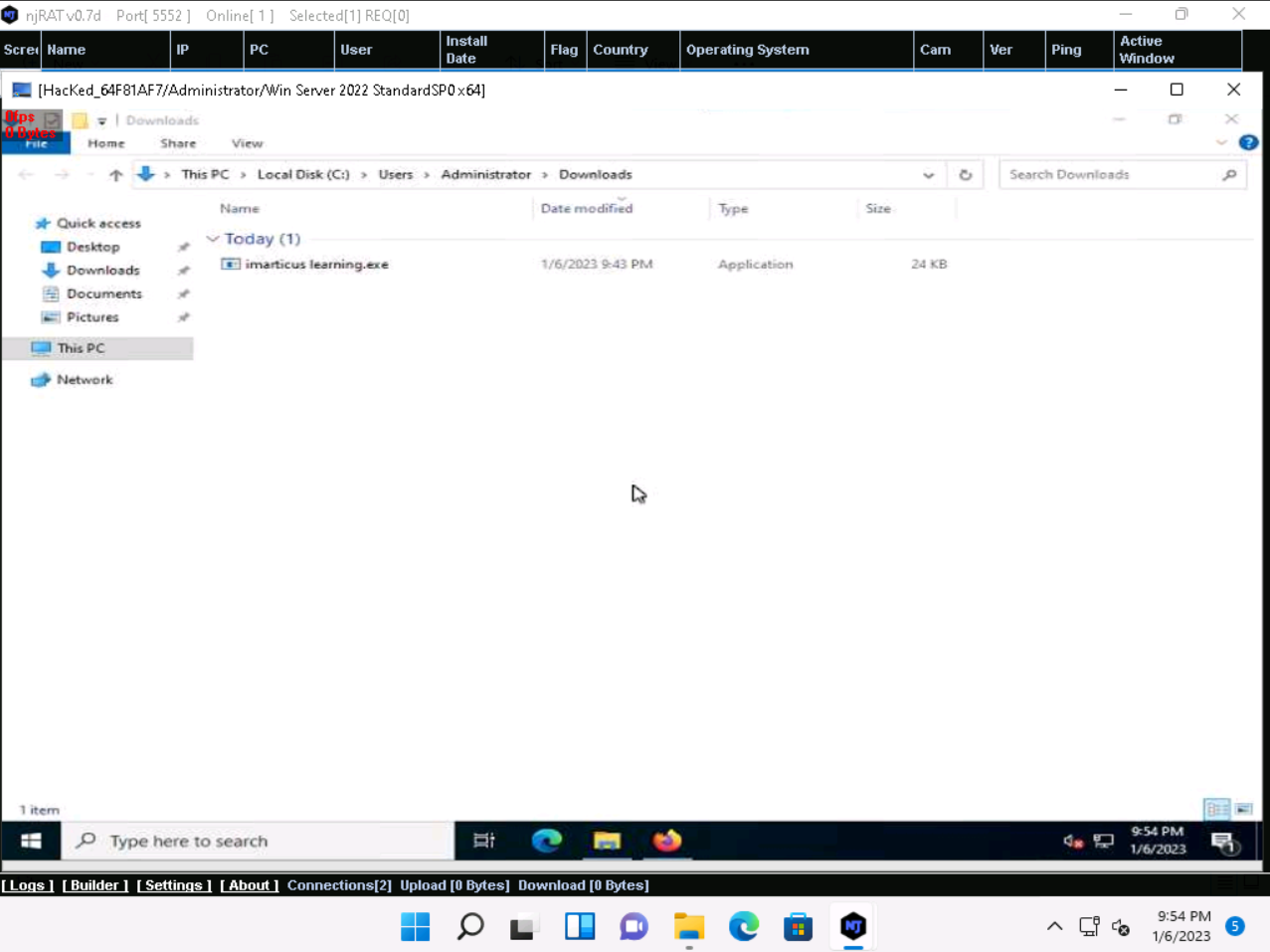


**Command prompt :**



**Remote Desktop:**





**Keylogger :**



