

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

## Dashboard:

**Dashboard**

**Notice:** To get the most out of Aware we suggest you view our 3 minute video [walkthrough!](#)  
To get started, Select a campaign mode:

**Entice to Click** **Credential Harvesting** **Send Attachment**

**Assign New Training** **Vishing** **Smishing**

**Live Phishing Campaigns**

Campaign	Campaign Type	Status	Assigned Training	Started	Stopped	Scheduled	Sent	Clicked	Compliance	Creator	Action
[Empty row]											
[Empty row]											
[Empty row]											

[Show More](#)

© 2023 EC-Council Aware.

Click on Entice to click.

Fill the details accordingly .

**EC-Council aware**  
When Everyone Protects

**Create New Email Phishing Campaign**

Campaign Name

Email Template Existing templates My templates

Select Template Category

Select Country

Select Template Select Template

Sender Email

Sender Name

Subject

Select Time Zone

Expiry Date

Schedule Later ☐ No

**Preview**

© 2023 EC-Council Aware.

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

**EC-Council aware**  
When Everyone Protects

**Create New Email Phishing Campaign**

Campaign Name

Email Template Existing templates My templates

Select Template Category

Select Country

Select Template Rewards and Recognition Select

**1 template selected.**

Sender Email

Sender Name

Subject

Select Time Zone

Expiry Date

Schedule Later ☐ No

**Preview**

Dear Arman

My heartiest congratulations on being awarded as best Team Work Champion for December 2017 awards. As you know, this is an award that is provided by co-workers to the team member whom they believe contributed the most to their success during the month.

Team members appreciated the leadership role that you assumed when the team struggled with direction and the allocation of resources. They were impressed with the amount you accomplished in a day.

Kindly accept the certificate from [HERE](#). This is but a small token of our appreciation to employees such as you upon whose support we have been allowed to grow and prosper in the highly competitive marketplace.

Warm Regards,  
Human Resources Department

© 2023 EC-Council Aware.

**Import Users Info**

Name:

Email:  This is a required field

Reporting Manager Email:

Designation:

Department:

Company:

Branch:

Country:

ID	Name	Email	Reporting Manager Email	Designation	Department	Company	Branch	Country	Action
1	Arman	ximoj24805@dentaltz.com	hr@imarticus.com						<input type="button" value="Add"/>

After filling the details of victim click on import

**Import Users Info**

Name:

Email:  This is a required field

Reporting Manager Email:

Designation:

Department:

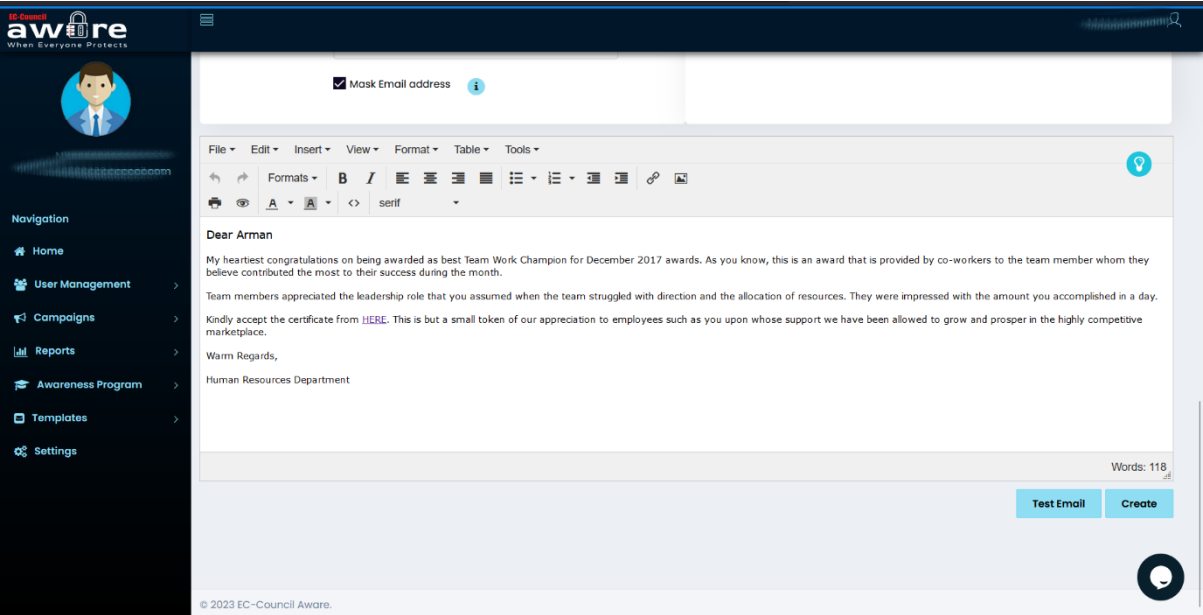
Company:

Branch:

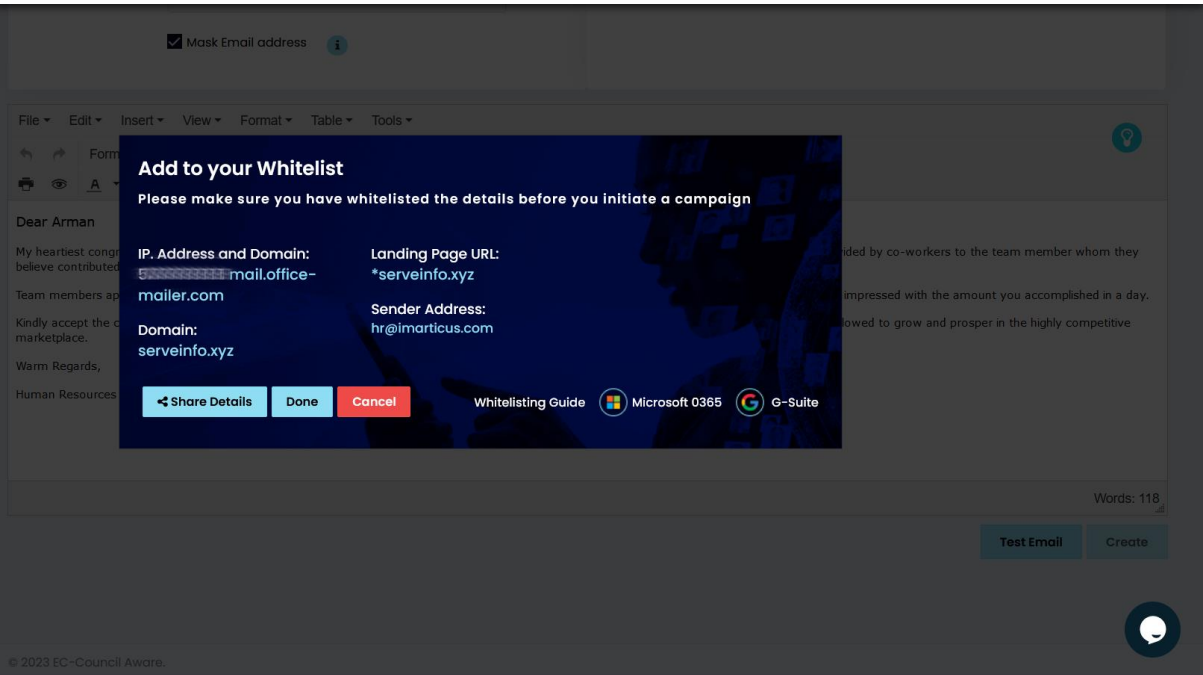
Country:

ID	Name	Email	Reporting Manager Email	Designation	Department	Company	Branch	Country	Action
1	Arman	ximoj24805@dentaltz.com	hr@imarticus.com						<input type="button" value="Add"/>

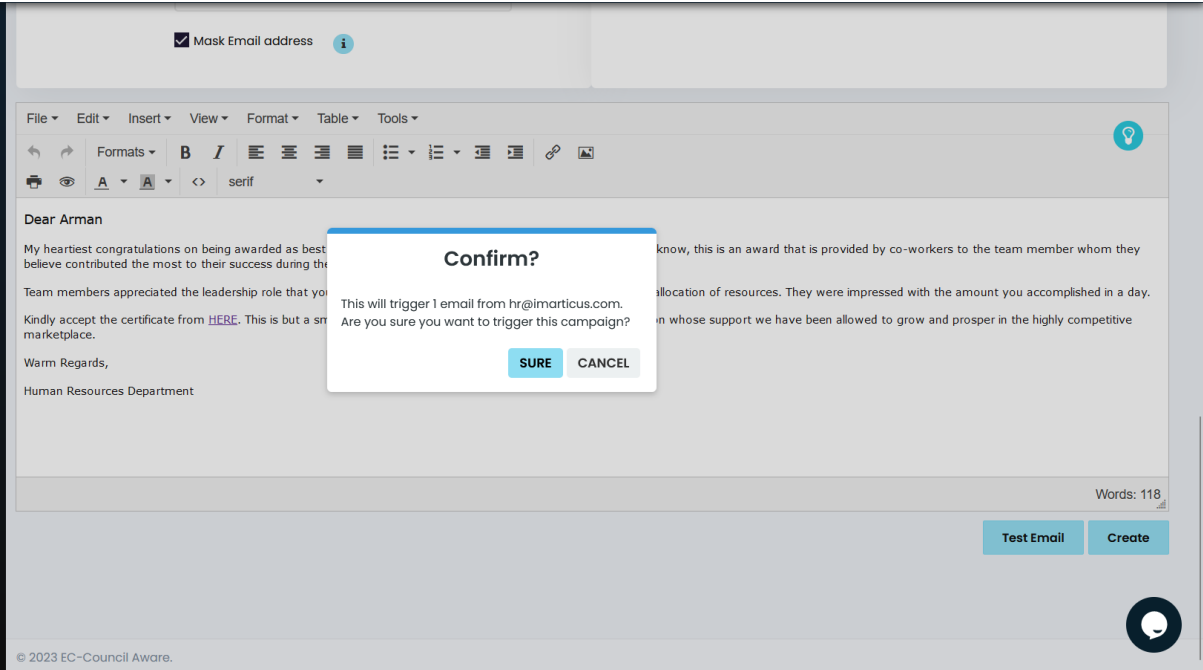
Click on create



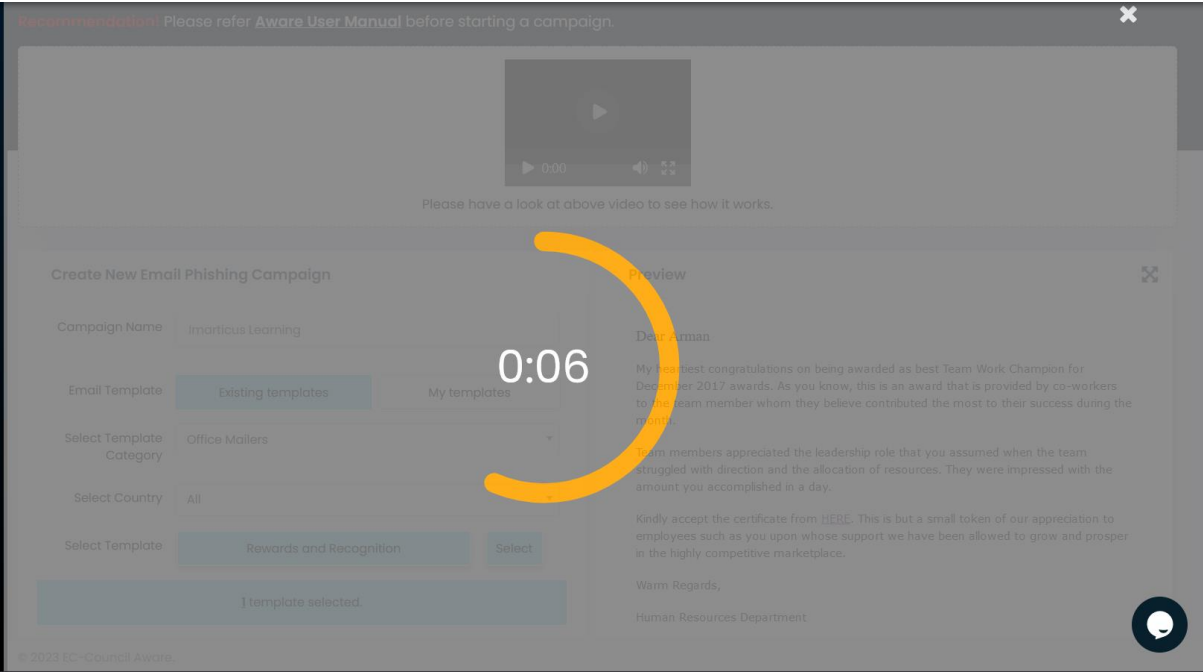
Click on done



It ask for confirmation, click sure



Creating ...



### Details :


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

© 2023 EC-Council Aware.



User mail inbox:

SENDER	SUBJECT	VIEW
<div><div></div><div>Human Resource Team</div><div>hr@imarticus.com</div></div>	Reward and Recognition	>



Human Resource Team  
hr@imarticus.com

Date:  
08-01-2023 10:45:33

Subject: Reward and Recognition

Dear Arman

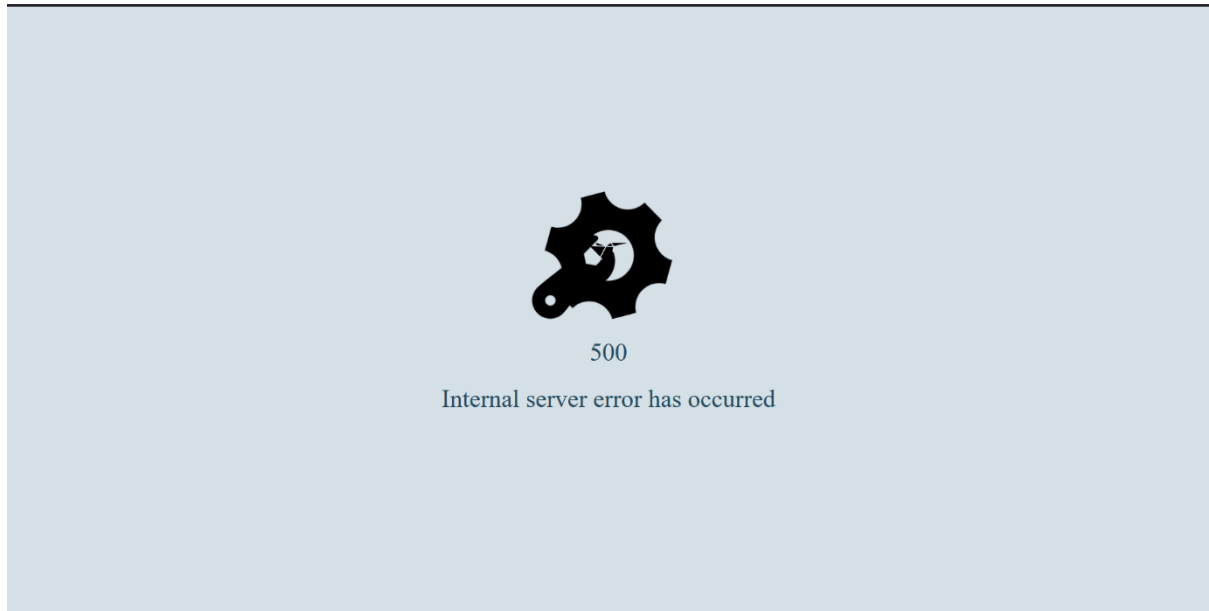
My heartiest congratulations on being awarded as best Team Work Champion for December 2017 awards. As you know, this is an award that is provided by co-workers to the team member whom they believe contributed the most to their success during the month.

Team members appreciated the leadership role that you assumed when the team struggled with direction and the allocation of resources. They were impressed with the amount you accomplished in a day.

Kindly accept the certificate from [HERE](#). This is but a small token of our appreciation to employees such as you upon whose support we have been allowed to grow and prosper in the highly competitive marketplace.

Warm Regards,  
Human Resources Department

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.

Entice to Click	Credential Harvesting	Send Attachment
Assign New Training	Vishing	Smishing

Live Phishing Campaigns

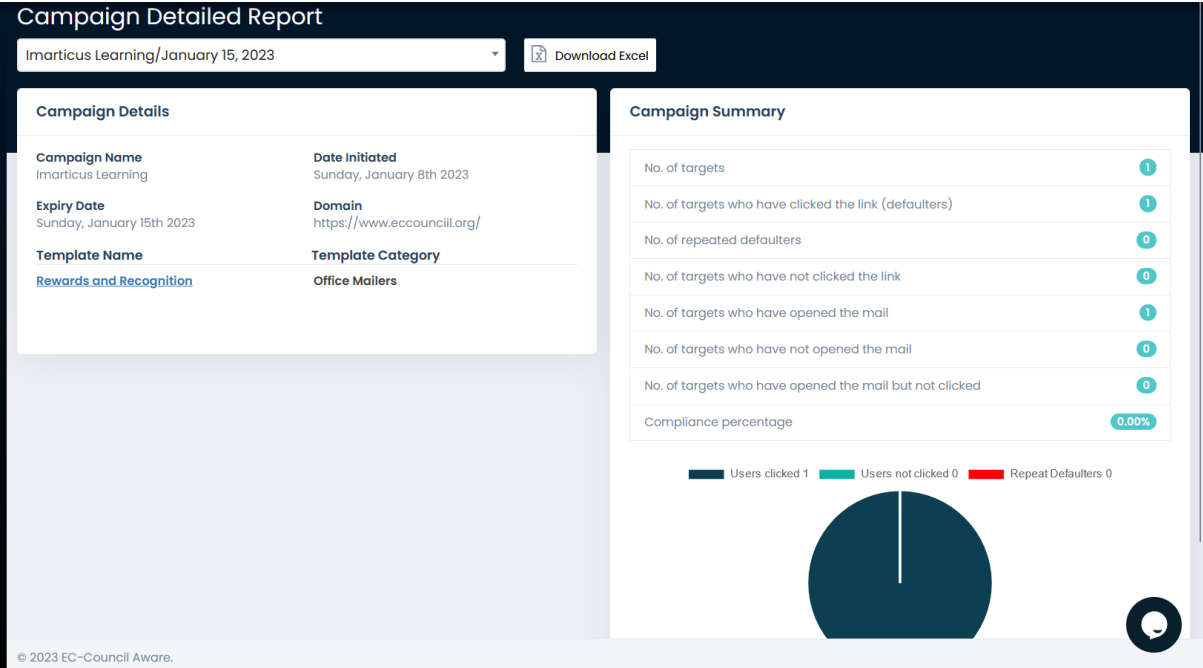
Campaign	Campaign Type	Status	Assigned Training	Started	Stopped	Scheduled	Sent	Clicked	Compliance	Creator	Action
Imarticus Learning	Email	In Progress	No Training Assigned	January 8, 2023 10:45 AM	Jan 15, 2023 Asia/Kolkata	NA	1	1	0.00%		

Show More

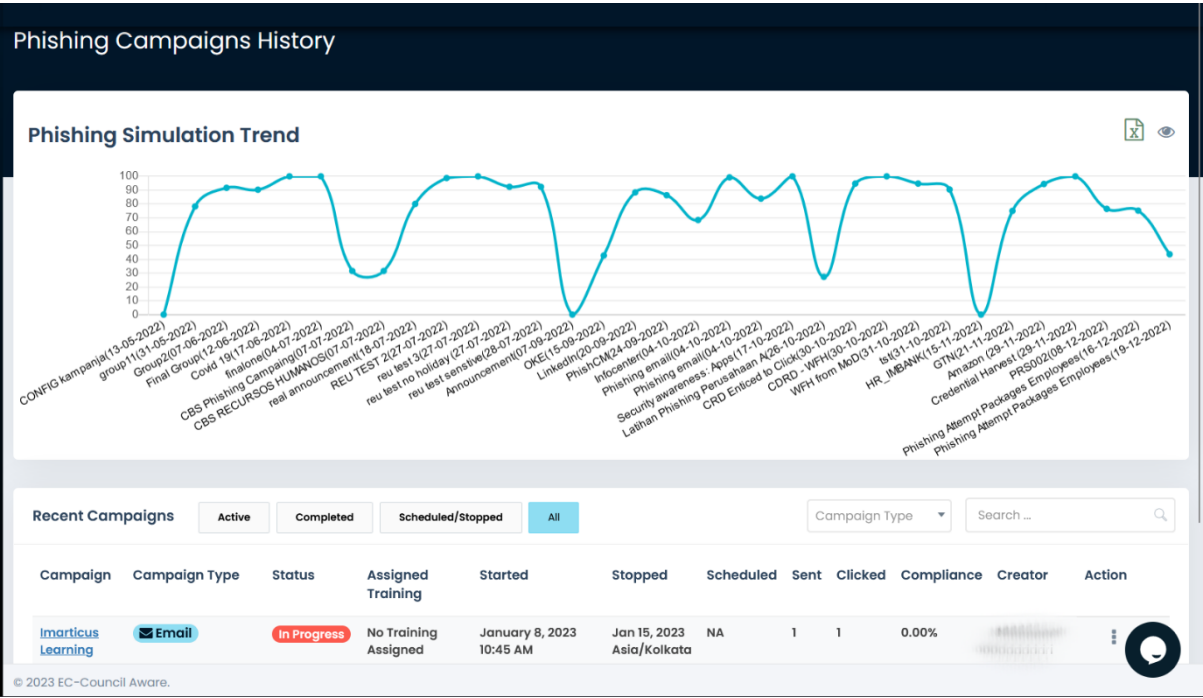
© 2023 EC-Council Aware.

Reports :

Campaign detailed report:



Phishing campaign history:



# Campaigns users:

Campaigns Users

Users Details

Search...

Employee ID	Employee Name	Email	Sent At	Opened At	Clicked At	Click Count	Risk Score	Template Used	IP Address	Location	Device	Status
1	Arman	xixxxxxxxxx@xxxxxxxx.com	Sun, Jan 8, 2023 10:45 AM	Sun, Jan 8, 2023 10:46 AM	Sun, Jan 8, 2023 10:46 AM	1	30	<a href="#">Office Mailers</a>	10.22.22.22.22.22	India India	Desktop	<span>Delivered</span>

© 2023 EC-Council Aware.

# Employee risk report:

Employee Risk Report

Arman 's Risk Report

here is how many campaigns held for Arman in last one year.

	Imarticus Learning
Risk Score	30/50
Held On	January 8, 2023

Avg. Score: 30.00

Imarticus Learning(30)

Close

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

**We are performing second scenario .**

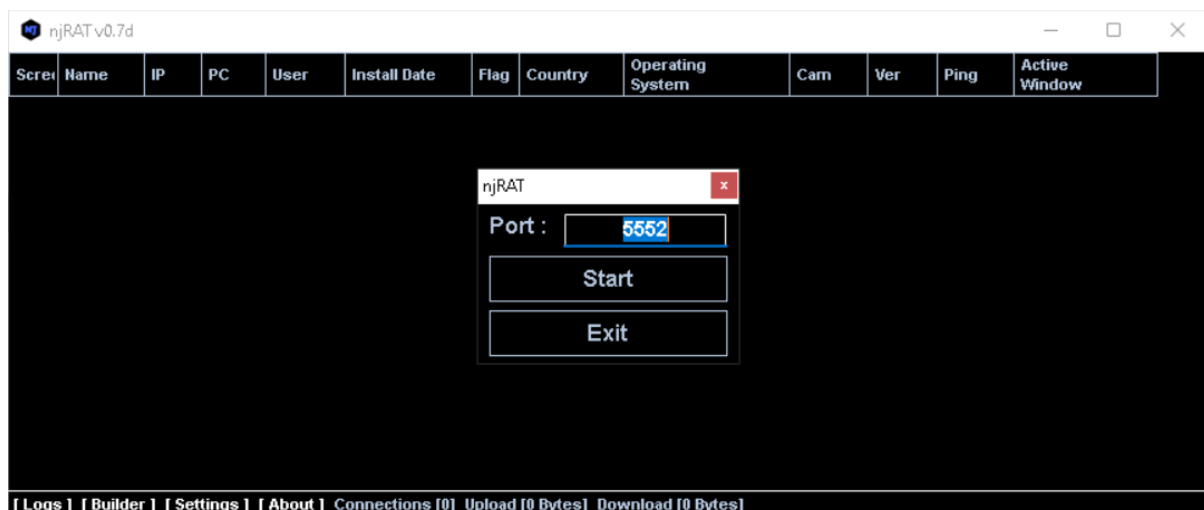
We are targeting person who had taken admission.

**Malware :**

Tool:njrat

We are creating a malware using njrat tool

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

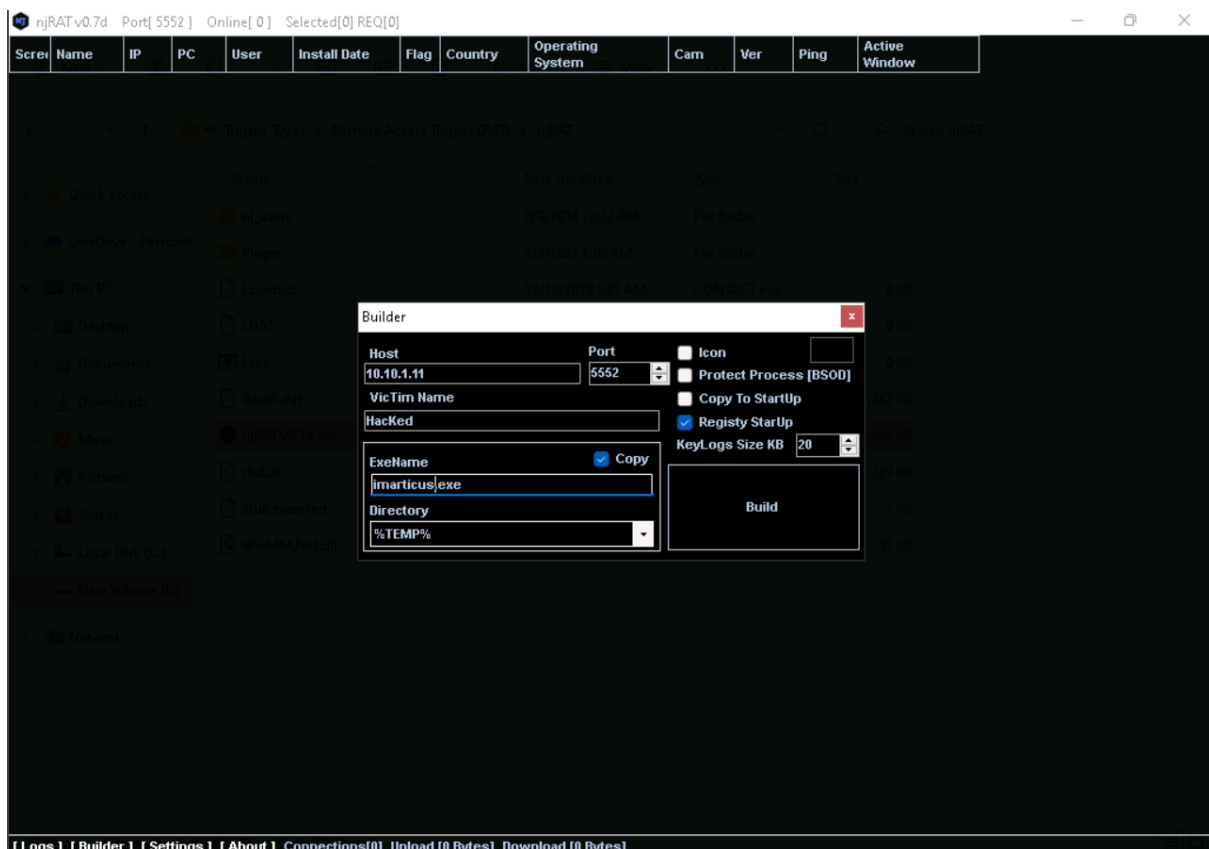


After clicking start we get the dashboard of njrat

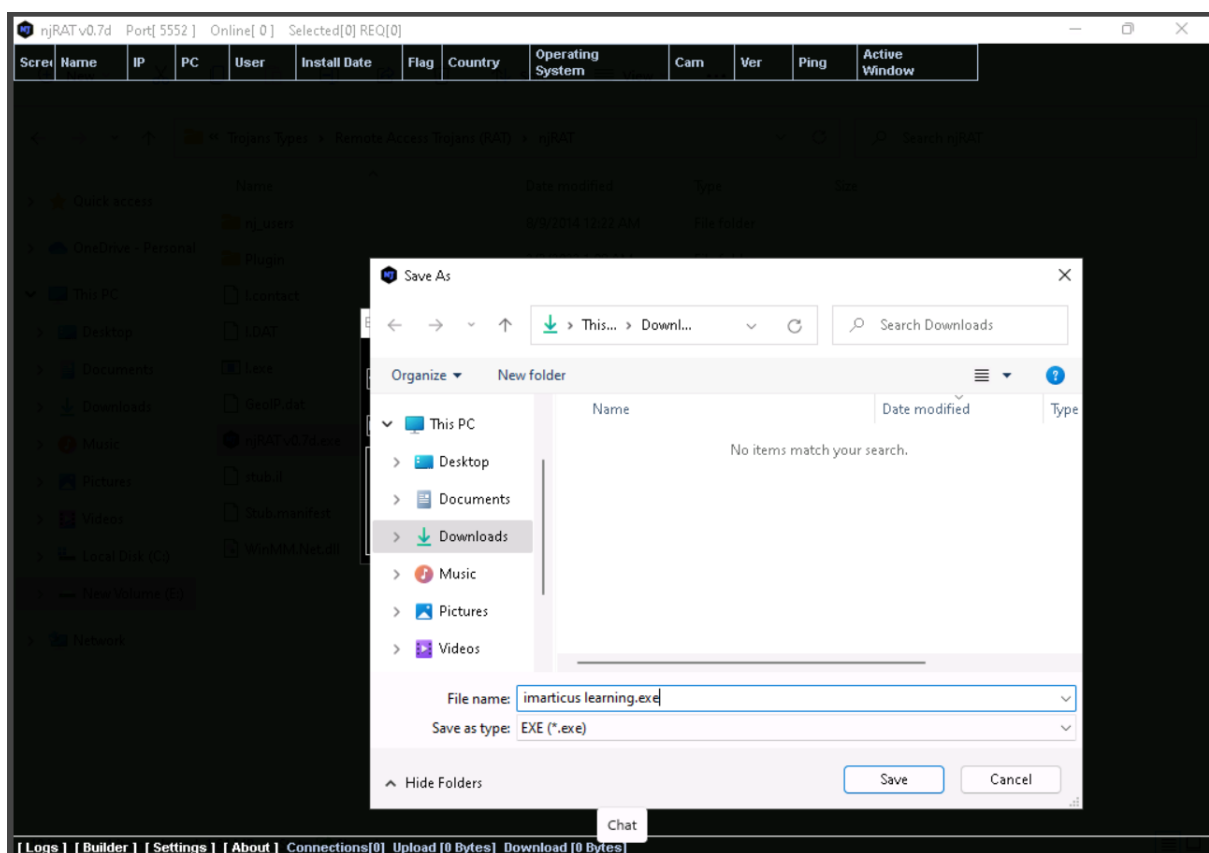


We can find a “Builder” option at the down bar of njrat for build a malware

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

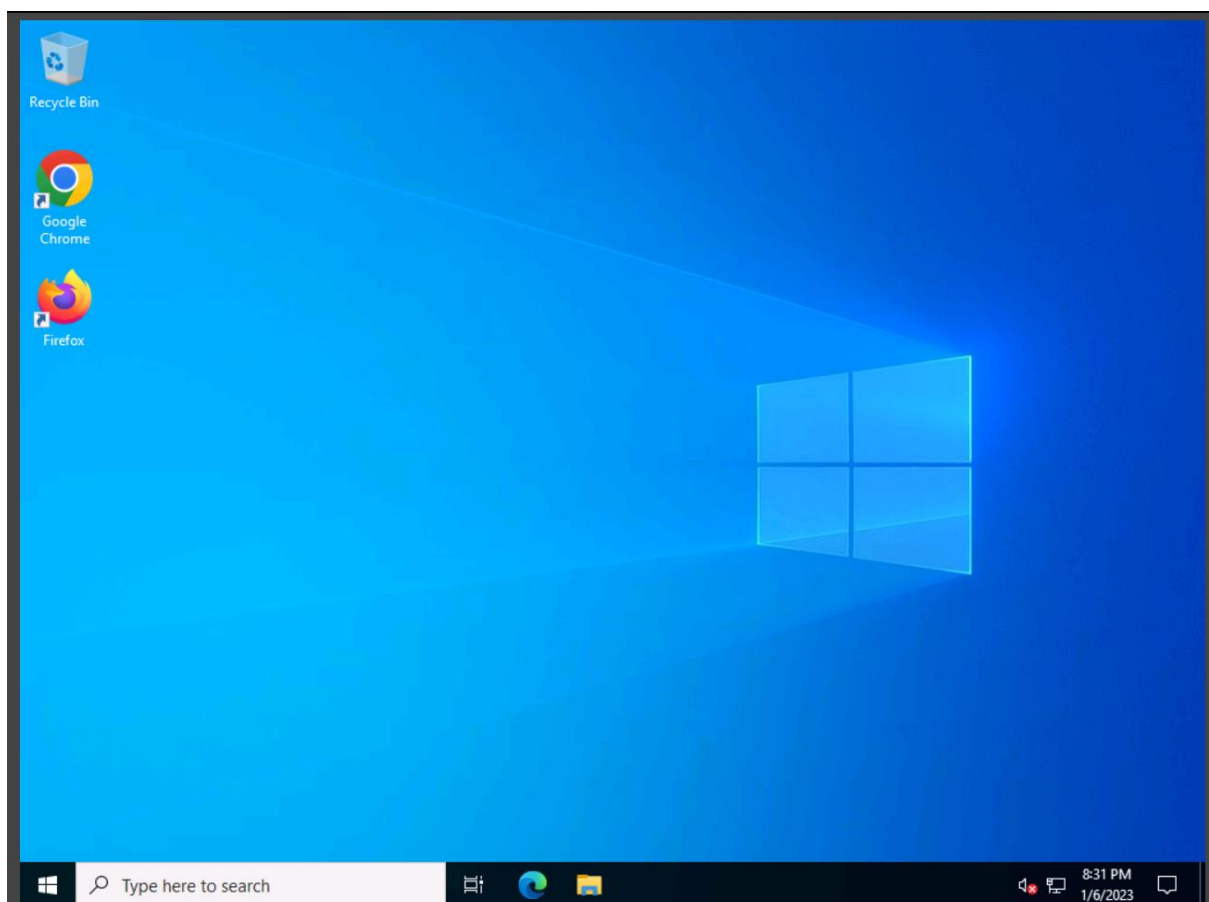


We save the malware with the organization name so it's look like legitimate for end user

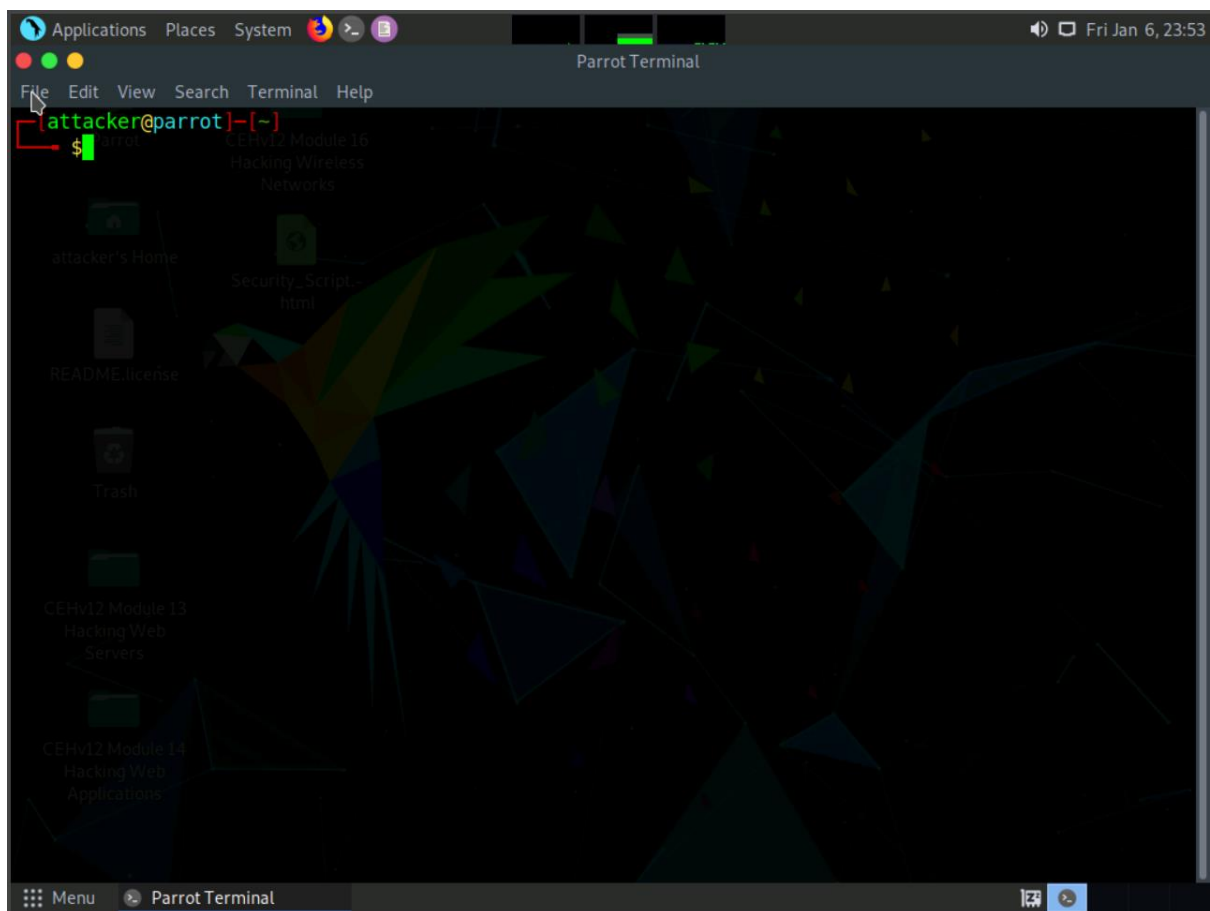




## Victim system



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



```
(root@kali)-[/  
# service apache2 start
```

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

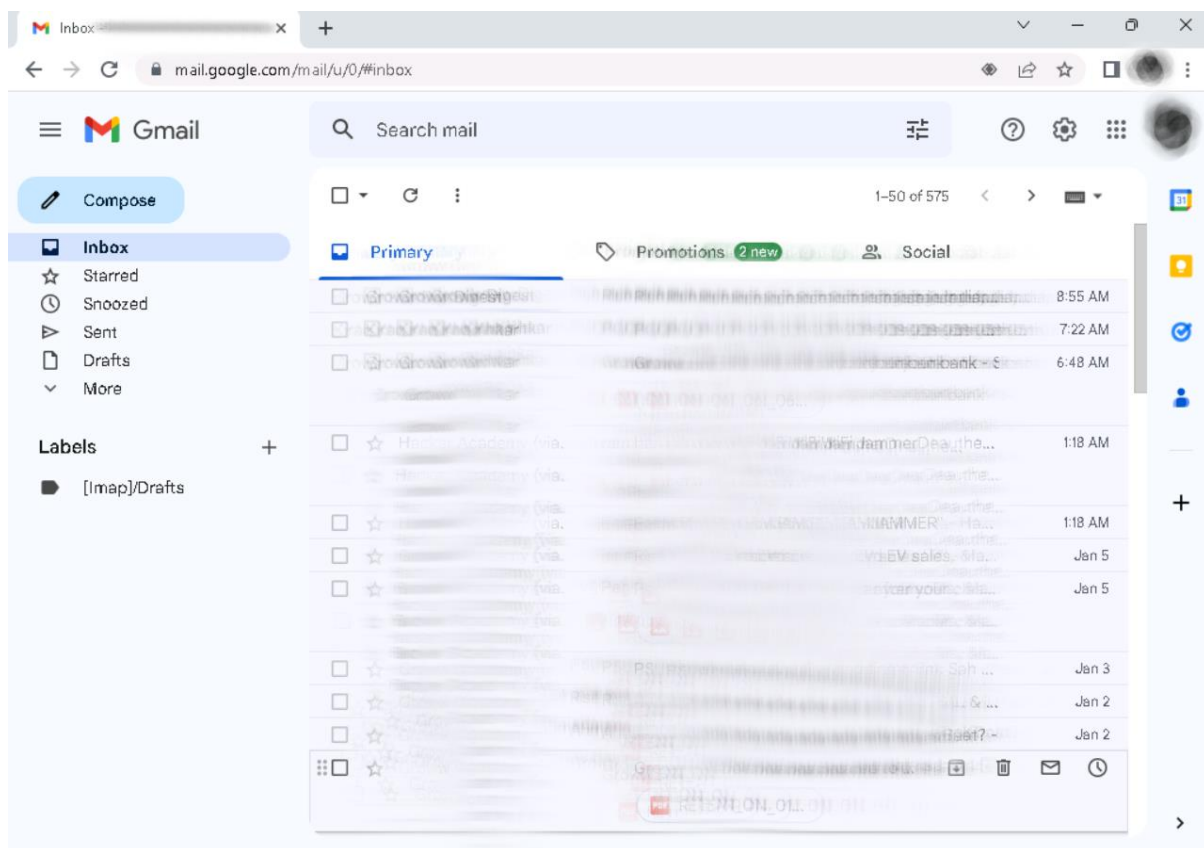
```
[root@parrot]-[/var/www/html]  
#mkdir share  
[root@parrot]-[/var/www/html]  
#chmod -R 755 share
```

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 phishing mail which look legitimate that user think this is normal or genuine.so user click link or any attachment without any hesitation.

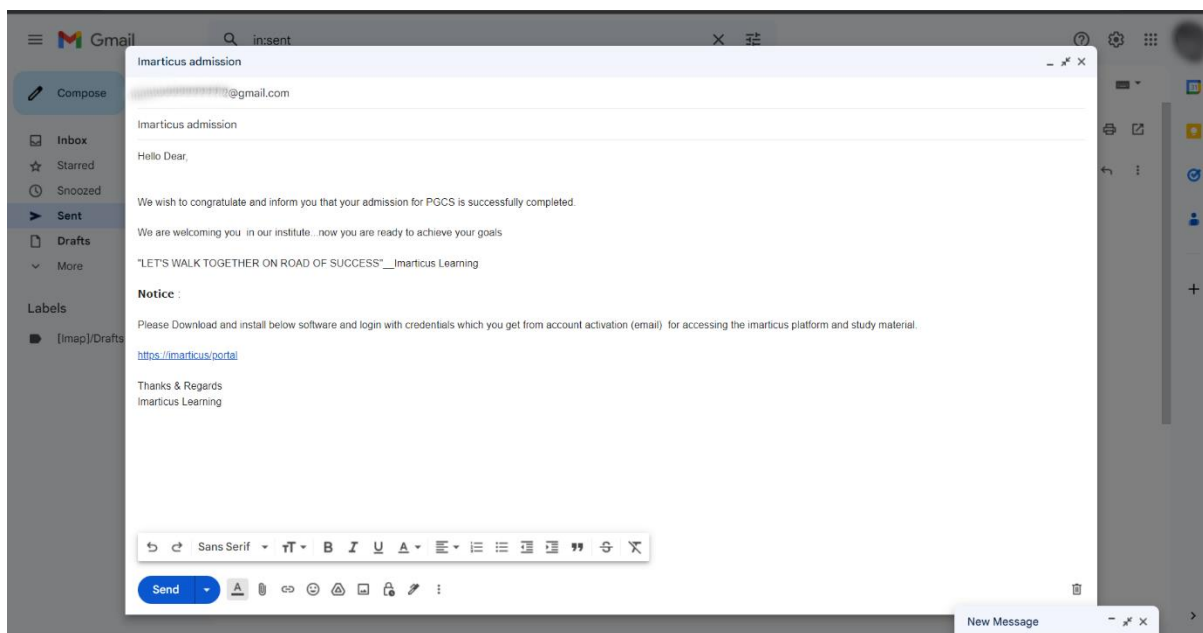
1.Open gmail

2.click on compose



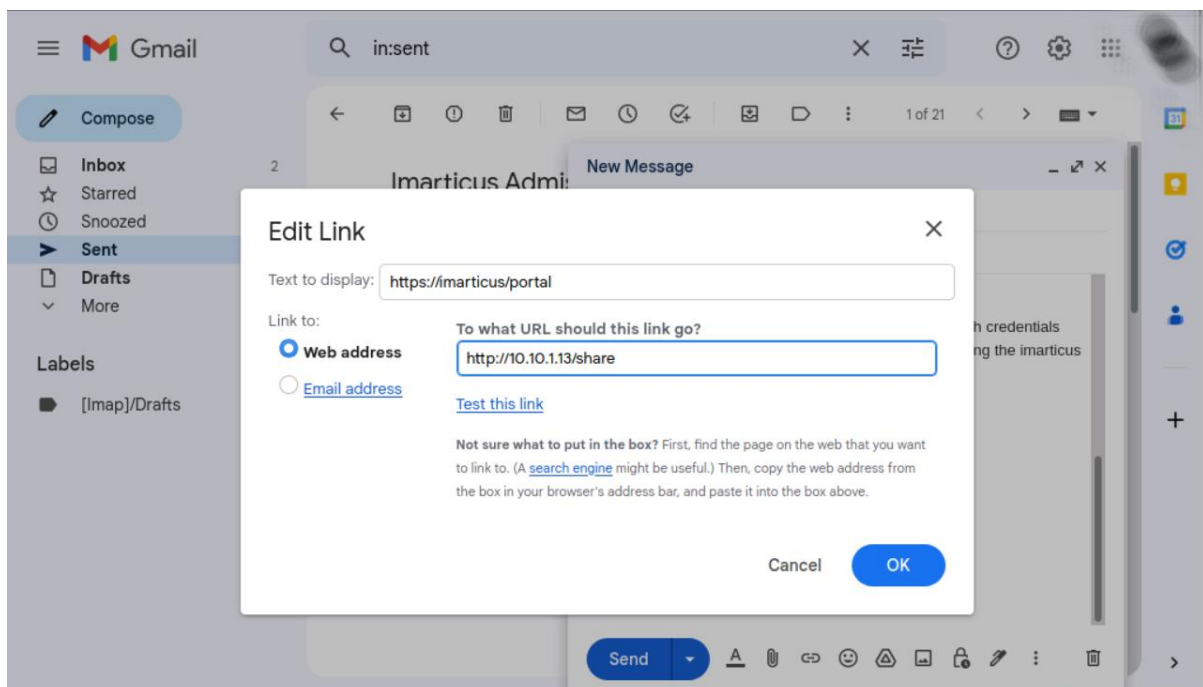
3. Once you click it open a window for writing and sending new mail

4. write a mail which is professional or tempting.



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>

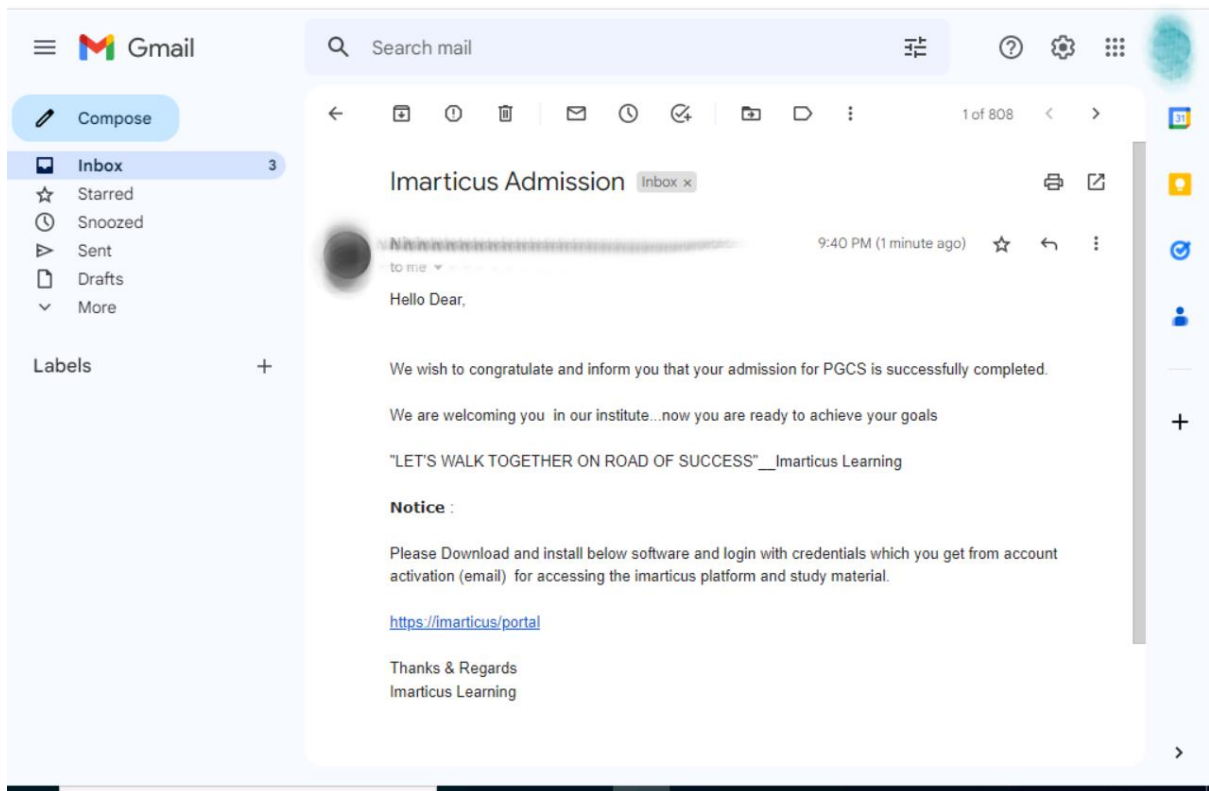


The user got the mail it's like this:

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



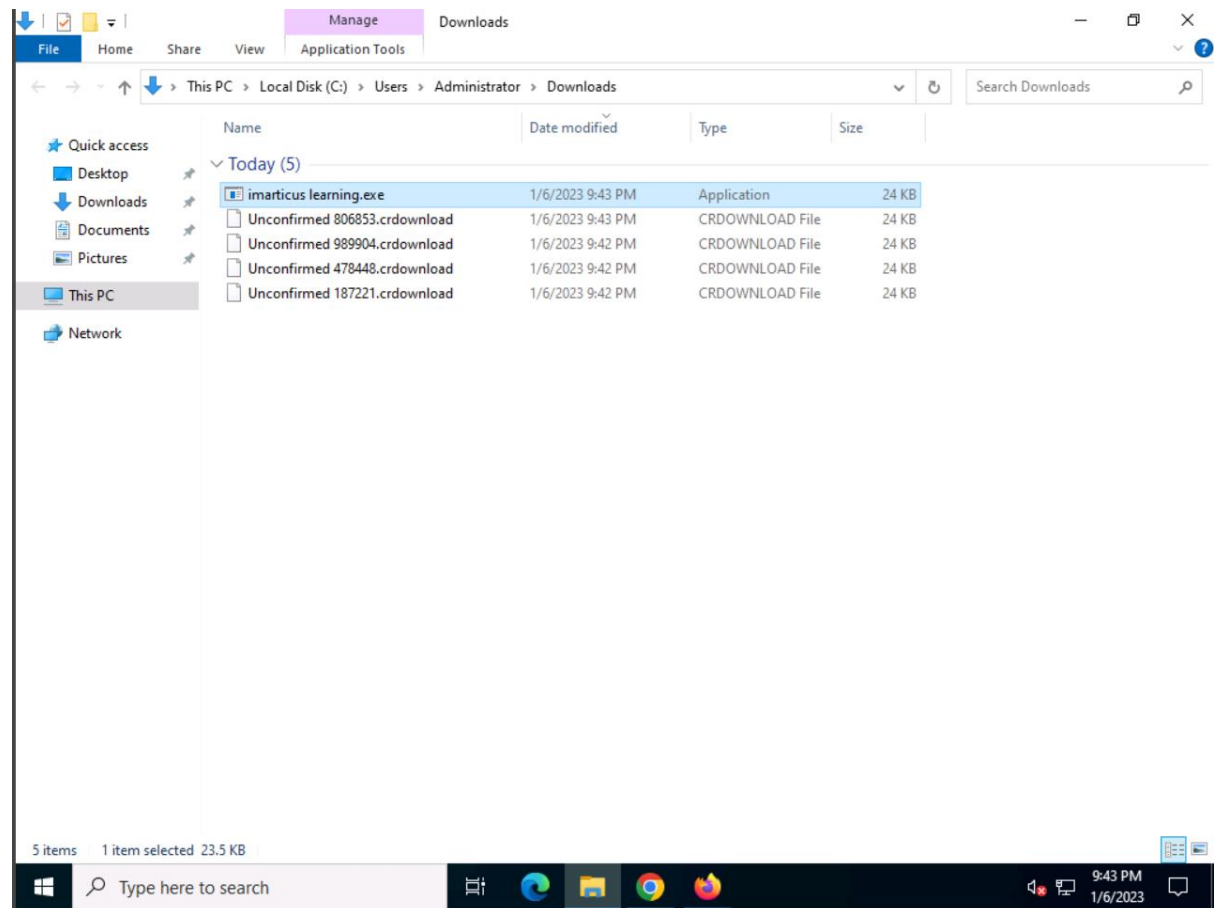
Because of we craft mail as it's seems like it's from organization so user download our malware and think like he or she downloading the original software provided by organization.

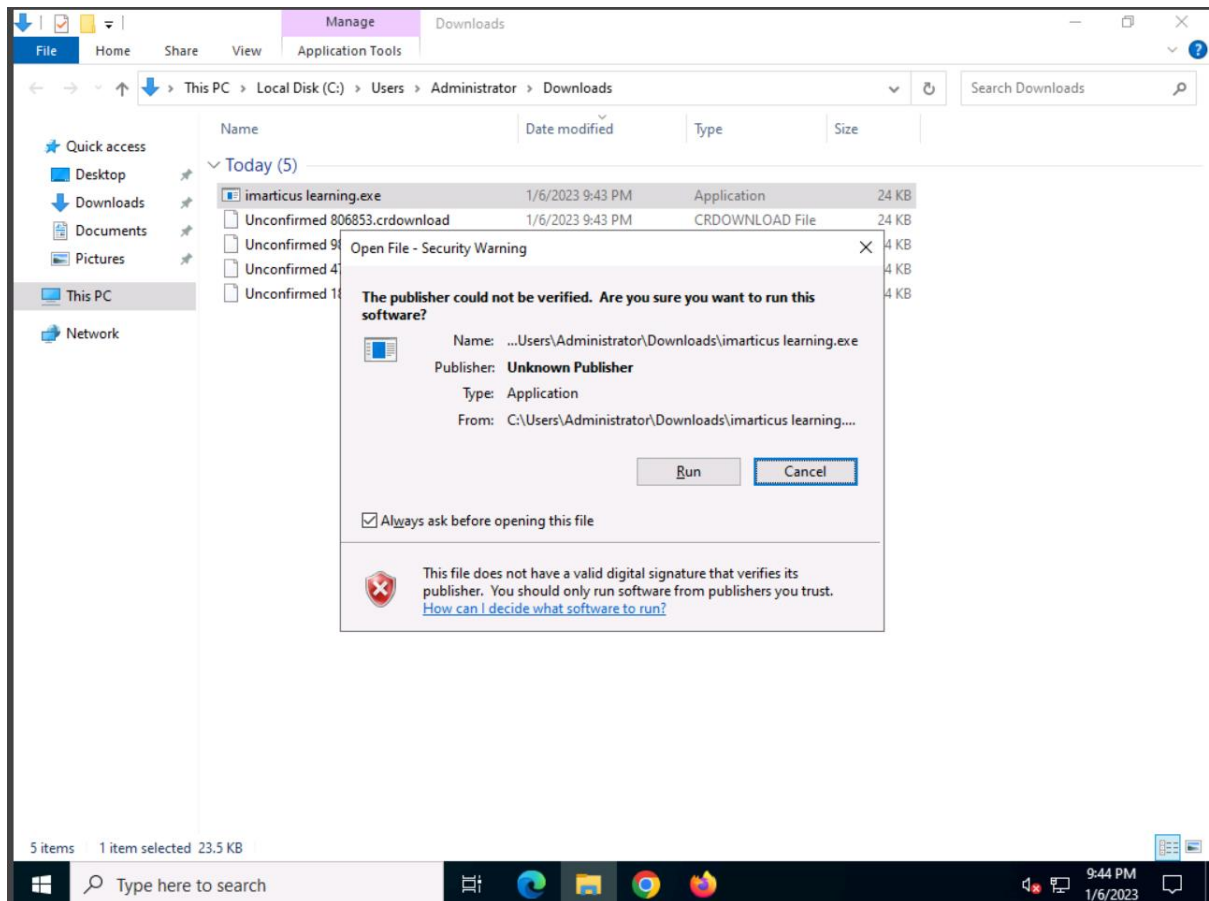


## Index of /share

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>			
 <a href="#">imarticus.exe</a>	2023-01-06 23:36	24K	
 <a href="#">imarticus learning.exe</a>	2023-01-07 00:30	24K	

Apache/2.4.51 (Debian) Server at 10.10.1.13 Port 80





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


njRAT v0.7d   Port[ 5552 ]   Online[ 1 ]   Selected[1] REQ[0]

Screen	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	HackEd_64F01AF7	10.10.1.22	SERVER2022	Administrator	23-01-06		N/A	Win Server 2022 StandardSP0 x64	No	0.7d	014ms	Downloads

[ Logs ]   [ Builder ]   [ Settings ]   [ About ]   Connections[1]   Upload [ 0 Bytes ]   Download [ 0 Bytes ]



9:44 PM  
1/6/2023



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

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

Manager

Run file

Remote cam

Microphone

Get passwords

Keylogger

Openchat

Server

Openfolder

njRATv0.7dPort[ 5552 ]Online[ 1 ]Selected[1]REQ[0]

Screen	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	Hacked_64f81AF7	10.10.1.22	SER		06	?	N/A	Win Server 2022 StandardSP0 x64	No	0.7d	004ms	

Manager

Run File

Remote Desktop

Remote Cam

Microphone

Get Passwords

Keylogger

Open Chat

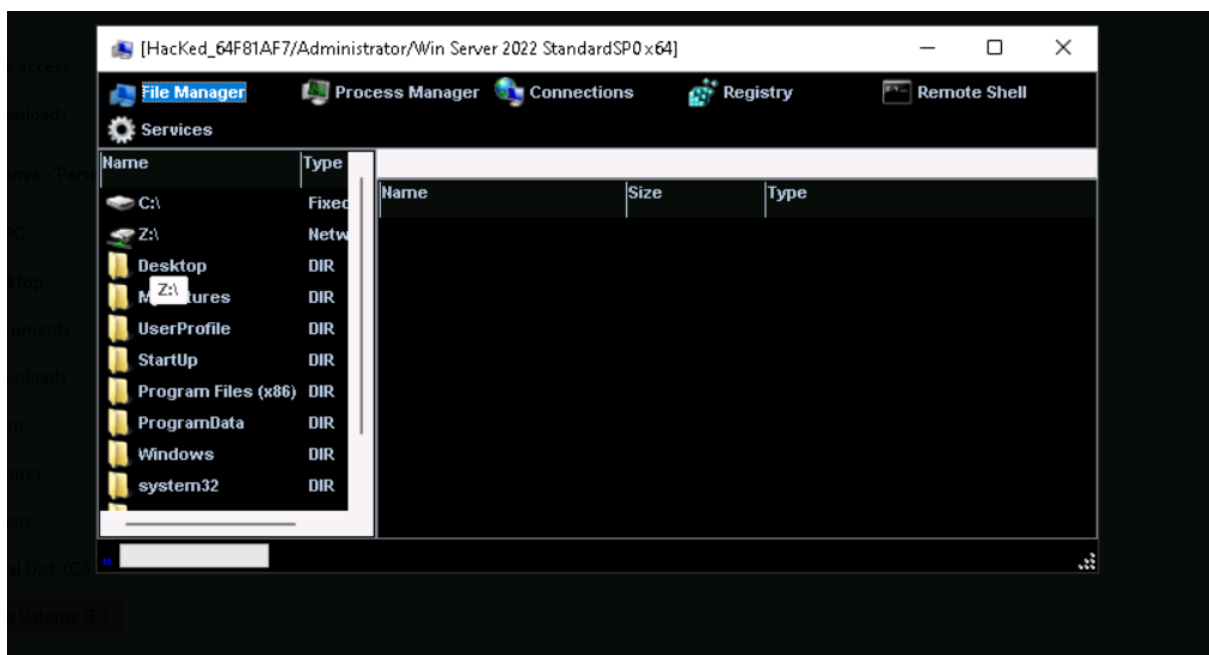
Server

Open Folder

LogsBuilderSettingsAboutConnections[41]Upload[0 Bytes]Download[0 Bytes]

Victim system...

File manager :



Services:

njRATv0.7d | Port[ 5552 ] | Online[ 1 ] | Selected[1] REQ[0]

Screens	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	HacKed_64F81AF7	10.10.1.22	SERVER2022	Administrator	23-01-06	?	N/A	Win Server 2022 StandardSP0 x64	No	0.7d	004ms	

Quick search

Downloads

OneDrive

This PC

Desktop

Documents

Downloads

Music

Pictures

Videos

Local Disk (C:)

New Volume (E:)

CD4-Tools

Network

[HackEd\_64F81AF7/Administrator/Win Server 2022 StandardSP0 x64]

File Manager

Process Manager

Connections

Registry

Remote Shell

Services

Name	PID	Directory
AggregatorHost.exe	4240	System32
armsvc.exe	1728	1.0
csrss.exe	504	
csrss.exe	576	
ctfmon.exe	2644	system32
dfsrs.exe	3116	system32
dfsrv.exe	3472	system32
dns.exe	3140	system32
dwm.exe	1060	system32
explorer.exe	2728	Windows
firefox.exe	5820	Mozilla Firefox
firefox.exe	6800	Mozilla Firefox

Logs

Builder

Settings

About

Connections[1]

Upload [0 Bytes]

Download [0 Bytes]



# Registry:

njRATv0.7d | Port[ 5552 ] | Online[ 1 ] | Selected[1] REQ[0]

Screen	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	HacKed_64F81AF7	10.10.1.22	SERVER2022	Administrator	23-01-06		N/A	Win Server 2022 StandardSP0 x64	No	0.7d	004ms	

Quick access

Downloads

OneDrive - Person

This PC

Desktop

Documents

Downloads

Music

Pictures

Videos

Local Disk (C:)

New Volume (E:)

CDN-Tools

Network

[HacKed\_64F81AF7/Administrator/Win Server 2022 StandardSP0 x64]

File Manager | Process Manager | Connections | Registry | Remote Shell

Services

	Name	Type	Value
	HKEY_CLASSES_ROOT		
	HKEY_CURRENT_USER		
	HKEY_LOCAL_MACHINE		
	HKEY_USERS		

Logs | Builder | Settings | About | Connections[1] | Upload [0 Bytes] | Download [0 Bytes]

Command prompt :

njRAT v0.7d | Port[ 5552 ] | Online[ 1 ] | Selected[1] REQ[0]

Screen	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	HacKed_64F81AF7	10.10.1.22	SERVER2022	Administrator	23-01-06		N/A	Win Server 2022 StandardSP0 x64	No	0.7d	952ms	

Quick access

Downloads

OneDrive

This PC

Desktop

Documents

Downloads

Music

Pictures

Videos

Local Disk (C:)

New Volumes (E:)

CEH-Tools

Network

[HacKed\_64F81AF7/Administrator/Win Server 2022 StandardSP0 x64]

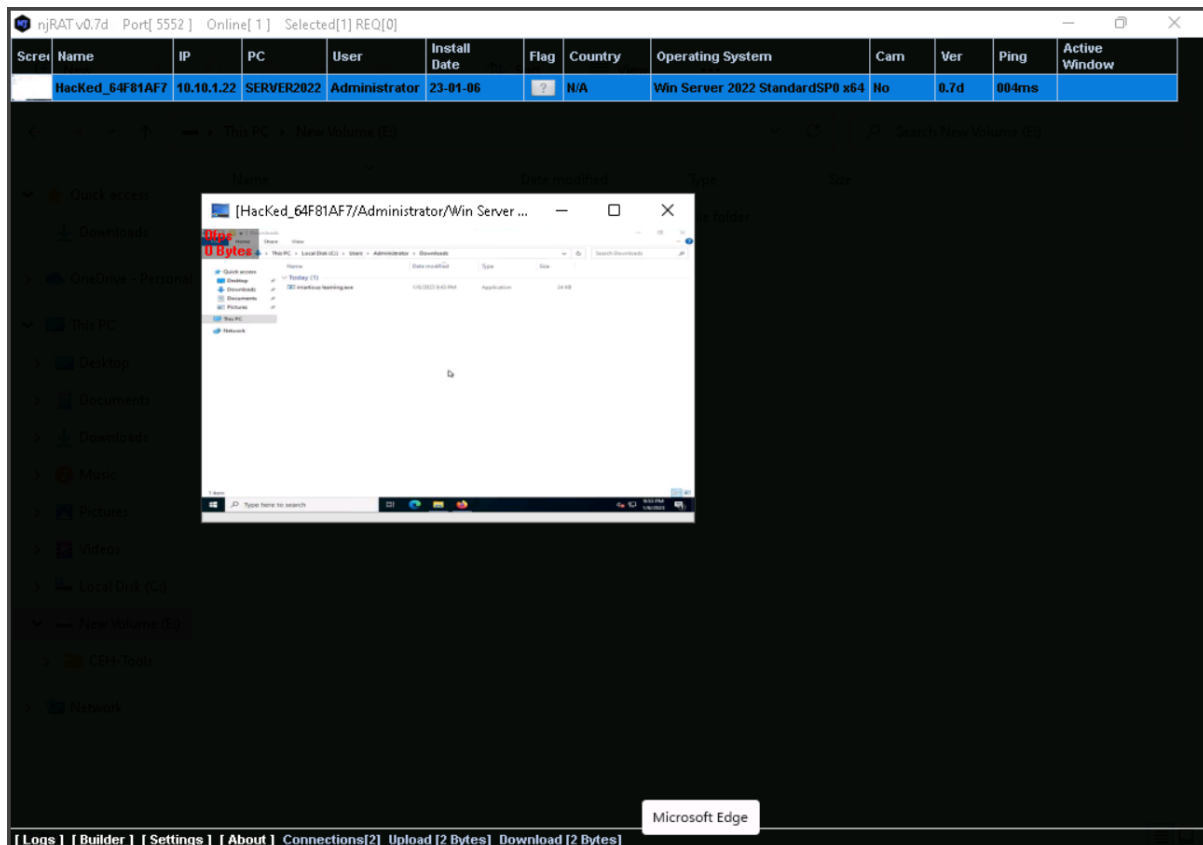
File Manager | Process Manager | Connections | Registry | Remote Shell

Services

02/01/2022 01:48 AM <DIR> ..  
02/01/2022 01:13 AM <DIR> 3D Objects  
02/01/2022 01:13 AM <DIR> Contacts  
02/01/2022 01:13 AM <DIR> Desktop  
02/01/2022 01:13 AM <DIR> Documents  
01/06/2023 09:45 PM <DIR> Downloads  
02/01/2022 01:13 AM <DIR> Favorites  
02/01/2022 01:13 AM <DIR> Links  
02/01/2022 01:13 AM <DIR> Music  
02/01/2022 01:13 AM <DIR> Pictures  
02/01/2022 01:13 AM <DIR> Saved Games  
02/01/2022 01:13 AM <DIR> Searches  
02/01/2022 01:13 AM <DIR> Videos  
0 File(s) 0 bytes  
14 Dir(s) 84,138,037,248 bytes free

Logs | Builder | Settings | About | Connections[1] | Upload [0 Bytes] | Download [0 Bytes]

## Remote Desktop:





# Keylogger :

