

Name-Dinesh Pradhan

Topic- Detecting and Preventing Phishing Attack

Phishing assaults mislead people into providing personal information, downloading malware, or otherwise exposing themselves to criminals by sending false emails, texts, phone calls, or websites.

1.Attacking :

1. There might be an automated tool or attacker designed website URL that is sent by attacker to victim. Also the website interface or website URL looks similar as trusted URL or websites, which is to make victim to enter their personal or sensitive credential into the website and on the other side those information are accessed by attacker.

Below is the example :

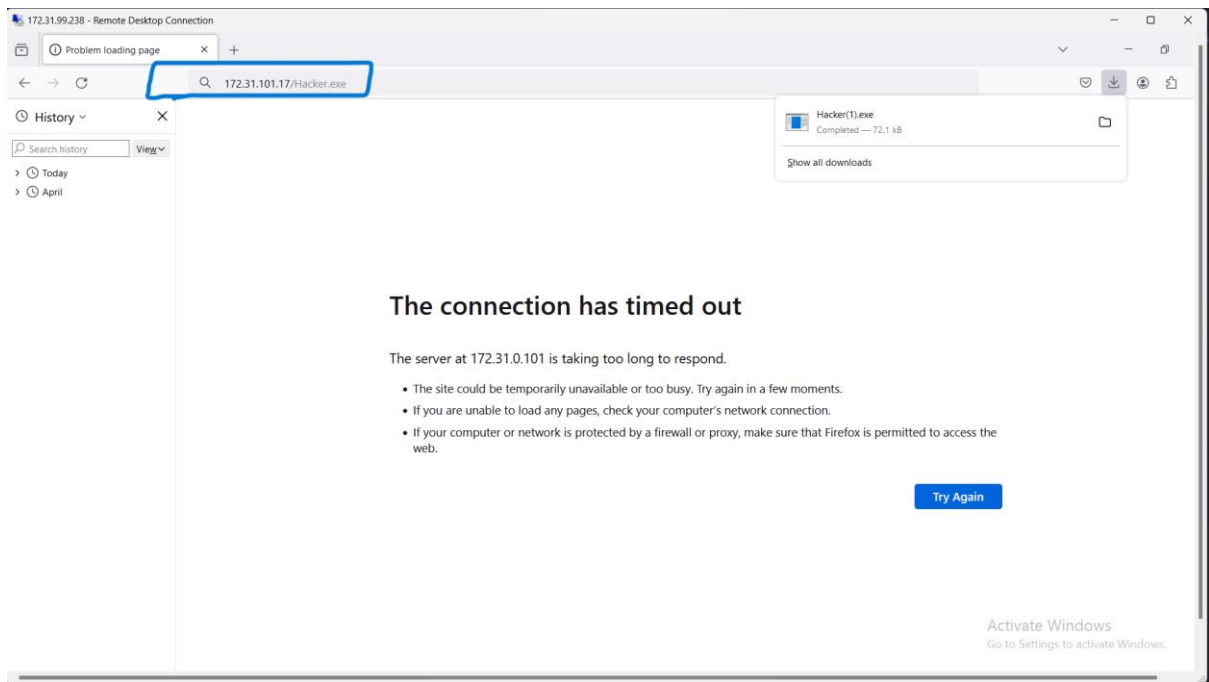
1.

[illegible]

The above is a automation tool which is designed to generate a url by itself . As you can see in the highlighted part of image .

2.

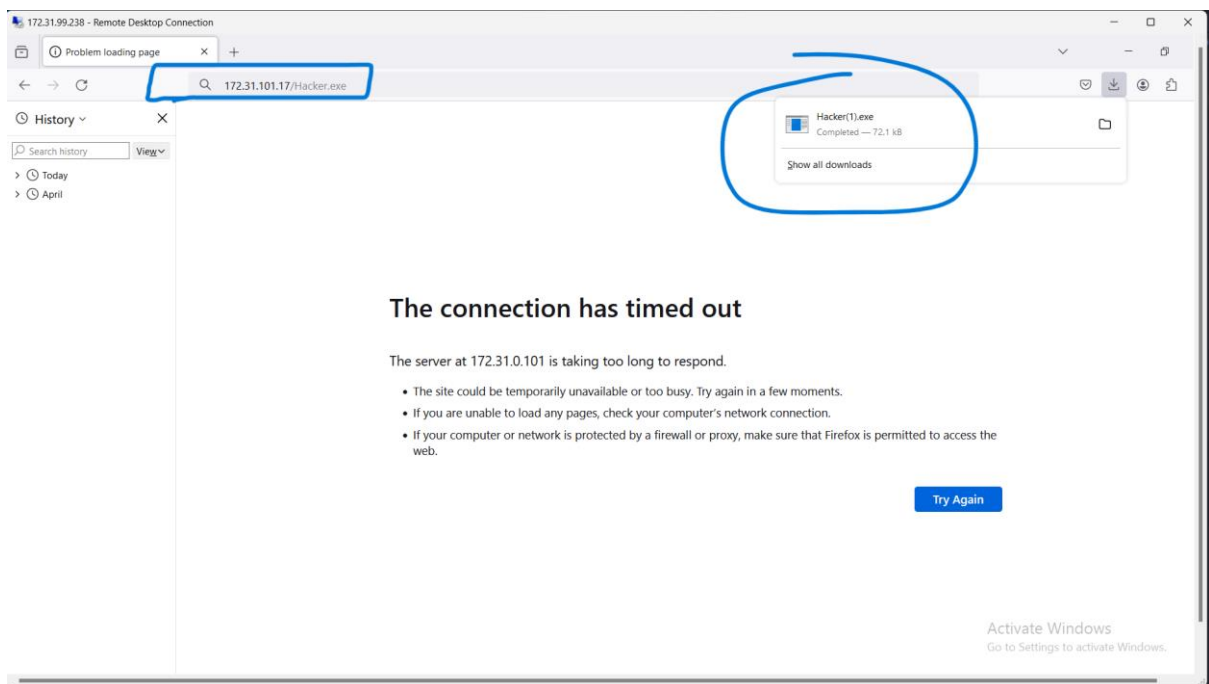
Then the website url sent over to victim or make the victim run the url in browser



In the above you can see the url run in the browser .

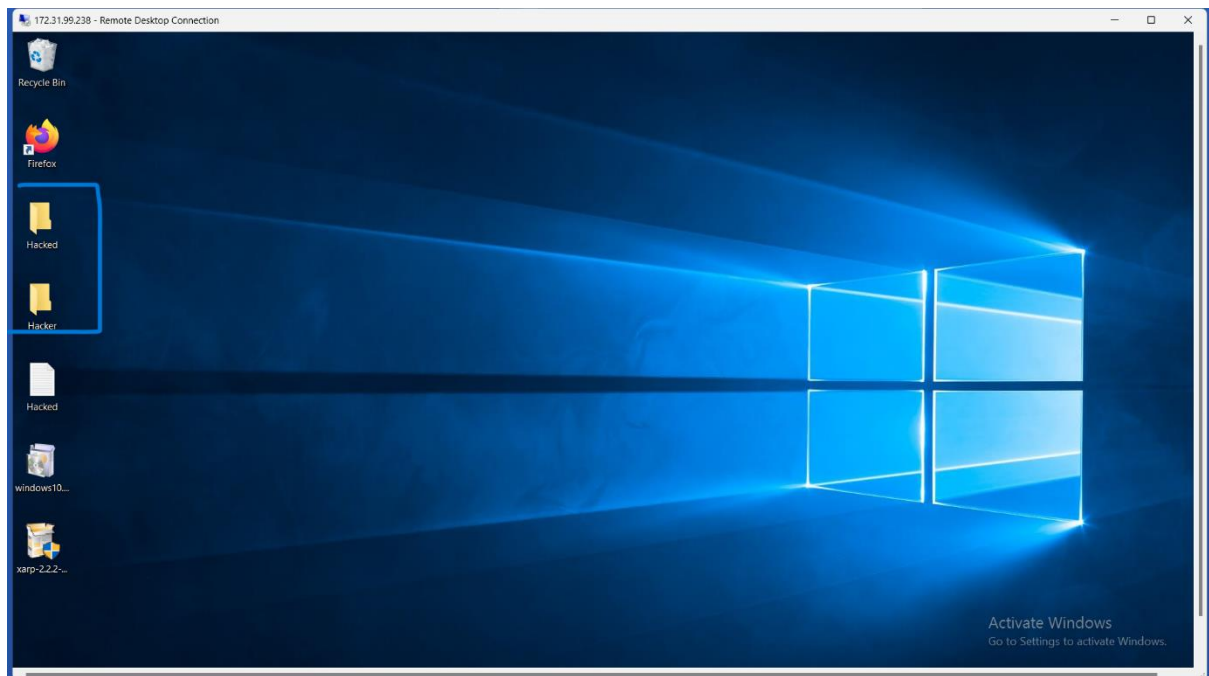
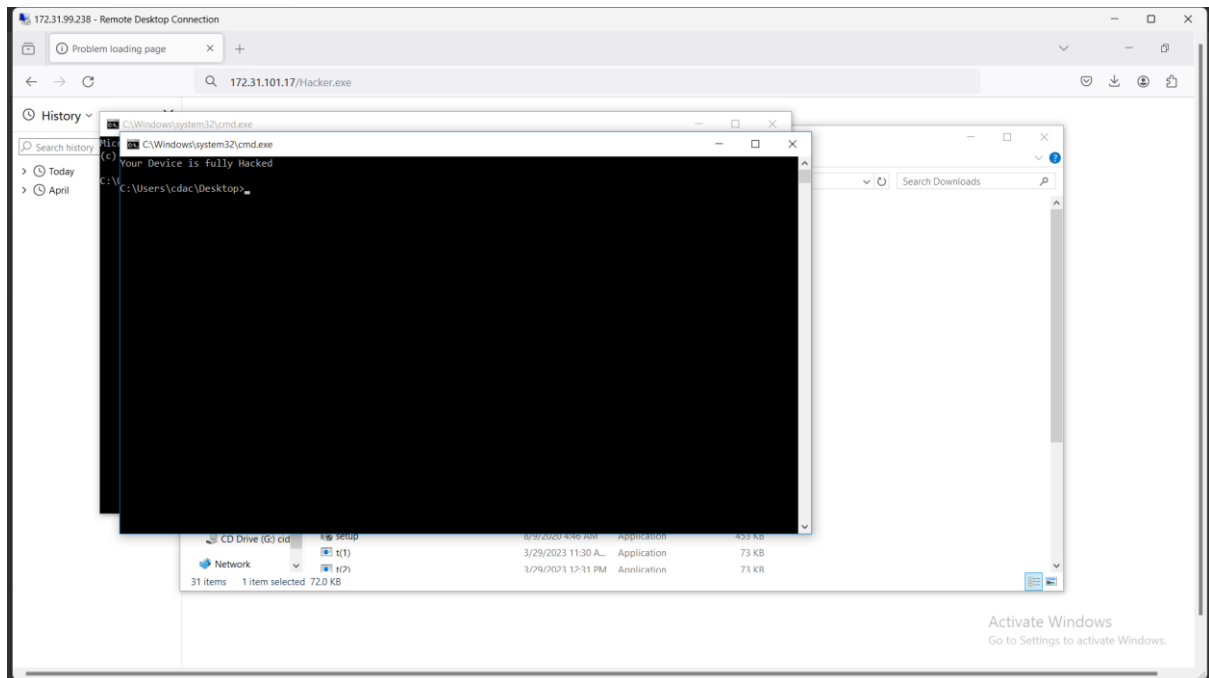
3. as a result of running the url a file is being downloaded on its own .

See in the right side highlighted part .



4. Out of curiosity when the victim runs the file then the automated script runs on the victim machine and steals the sensitive information from the victim machine.

As you can see in the below images.



Prevention of phishing attack :

1. Never provide your personal information in response to an unsolicited request .
2. If you believe the contact may be legitimate, contact the financial institution yourself.
3. Never provide your password over the phone or in response to an unsolicited Internet request
4. Review account statements regularly to ensure all charges are correct.
5. Always stay updated with software on computers with firewalls as well as software .
6. Don't install app from unknown sources .
7. Always take Backup of your data.