Brief description of the malware

The project is a malware that its duty is to run commands from the distance without the user understanding it and its purposes.

The user downloads the malware with a fake ChatGPT page that offers him to be a beta user of ChatGPT4.5, the chat tells him he cannot help him unless the user downloads the program that "is communicating with the OpenAI servers in order to deliver information about crashes and errors in ChatGPT4.5" he cannot use the service, the user also needs to register in order for us to get information about the person and not only the computer he is using.

The process of the simple victim

1. Gets an offer for testing ChatGPT4.5 and clicking on the link.
2. The website asks for simple registration information for communicating with him in order to get a full review of the product.
3. After the registration it allows the user to communicate with the bot- the bot may be using the ChatGPT API (not for sure) and will give him the answer he wanted or telling him that to use the chat he needs to download the file its suggesting.
4. After downloading and activating the program the victim's pc communicate with the server and registering with some basic information (username. ipv6, operating system)
5. After the pc successfully registered to the SQL server the administrator of the server(me) can control its command without the user knowing.
6. Spreading of the malware through the victim's pc in his local and public network.

The foundation of the project

The malware is being divided into 2 parts one in the server and on the victim's computer.

- **Server side**

  The server side includes an SQL database and amache2 server that contains all of the PHP and html files that the administrator uses in order to interact with the victim's commands and information and communicating with the SQL database.

- **Victim Side**

  The victim's side include few C# class (GeneralInfo|Operations|Presistence|Program) each of them control other part of the communications with the server.

The goal of the malware

Is to be able to send itself with a given text via email/other communication system in order to infect more computers. And offering the admin a lot of computing power with remote controlling. Remote controlling is the most powerful thing we can have on a victim's computer.

Milestones

1. Writing a html page that will help the administrator control everything.
2. Creating a server running on Ubuntu VM.
3. Creating a SQL Control Panel database contains users and victims tables.
4. Writing a PHP to all those html pages.
5. Creating the victim's side program with C#.
6. Setup the first communication with the victim's side program.
7. Setup the victim registration to the database and delivering the data to the admin.
8. Setup the admin’s manage page which he can control the victim's commands from.
9. Being able to see the result from the victim's pc.
10. Setup full working malware on the local network.
11. Creating an outside server running on Ubuntu with public IP available.
12. Check everything is running fine.
13. Developing new features to spread the malware between computers on the local network.
14. Developing new features to spread the malware with many communication systems to get to new computers.
15. Mimic the ChatGPT site with html.
16. Creating registration with PHP page on the same web page.
17. Generate many comments in order to get the user to download the malware.
18. Looking for security weaknesses and trying to fix them.
19. Looking for encryption method I need to use to keep my server and databases safe from hacking.
20. Finish with some cosmetic touchups.

Time schedule

Most of the work (1-12 except for 9) is already done to this date (31.01.2024).

Section 9 will be done in the next week (07.02.2024)

Sections 13-14 will be done in week after (14.02.2024)

Sections 15-16 will be done until the next month (31.02.2024)

Sections 17-20 will be dealt with until the submission of the work.

Challenges and difficulties

- Coming across coding languages I have never came across (C#, PHP).
- Dealing with creating a webpage that need to mimic a real website via HTML.
- Encrypting the passwords of the victims and mine.
- Working on a server only using commands (No VM).
- Dealing with the creation of database using SQL.
- Creating a catfish page is reliable enough to create a stream of victims.
- Working under a lot of pressure in work and school.
- Find sources on the Internet that will explain hacking and data transfer techniques.
- Find ways to transfer data "under the radar."
- to make a transition from a local environment to a public environment.
- Look for ways in which the information will be as secure as possible.
- Remote control is among the most powerful tools you can give a hacker, knowing how to use the power optimally.
- Produce a file download as reliable as possible which will work from the first moment and transfer information every 5 seconds.

Strengths

- Not too complicated code that can be changed when needed.
- Remote control - the power among the greatest that can be given to a hacker.
- Very reliable social engineering that can attract many populations.
- The flow of information is not huge and will be difficult to detect.
- All the operations run on the victims' computers and no great computing power is needed.
- All information is saved and can be used in the future.
- The "registration" step that the user completes when he tries to register for BETA can help us link people's names and details to their computers and thus gives an important piece of information.
- The server is external and can be turned off without direct contact with me.
- The ways of distribution come from within the victims themselves, which makes them more reliable.

Naor Cohav naorcoha@post.bgu.ac.il **0586126161**

318672490