1. **Tool Description and Purpose**:

   The project is designed to function as follows: upon user registration on the website, the user inputs details that are stored on my server in a SQL database. Additionally, users receive an executable file which, upon execution, initiates communication with my server. This allows me to remotely execute commands and adds the user's computer to a list of computers that I can control remotely.

   The project is meeting the definition of a virus that allows remote control.

2. **Challenges Encountered**:

   - Building a reliable enough website that can generate more traffic for me and new victims.
   - Working with external Linux servers using Kamatera.
   - A code that will allow me to use it smoothly and will run every time the computer is activated without opening any window that could indicate the use of malware.
   - Maintenance of SQL servers and Apache servers which includes an understanding of the folders and files.

3. **Strengths and Weaknesses of the Tool**:

   - **Strengths**:

     High level social engineering that manages to produce a very reliable scam that can draw in large audiences.

     Few commands pass between the server and the victim's computer, so it is difficult to detect suspicious activity.

     Remote control is a very powerful tool, and some say that it is the most powerful we have on external computers.

   - **Weaknesses**.

     Vulnerable to security risks if proper authentication and encryption measures are not implemented.

     An internet crash can damage the activity of the virus.

4. **Description of Tool Operation**:

   The process starts like this:

   The user is trying to find a free magic solution where he can use a very advanced technology that has not yet been published and be the first to use the GPT5 chat beta version.

   The user tries to talk to the chat but receives a random message (from a store of messages) telling him that he has not yet registered for the beta version and that he needs to install and run the software which "communicates with the OpenAI servers and updates on recurring errors" even though in practice he is running malicious code which calls with my servers and allows me to control his computer commands.

5. **Code Documentation and Key Components**:

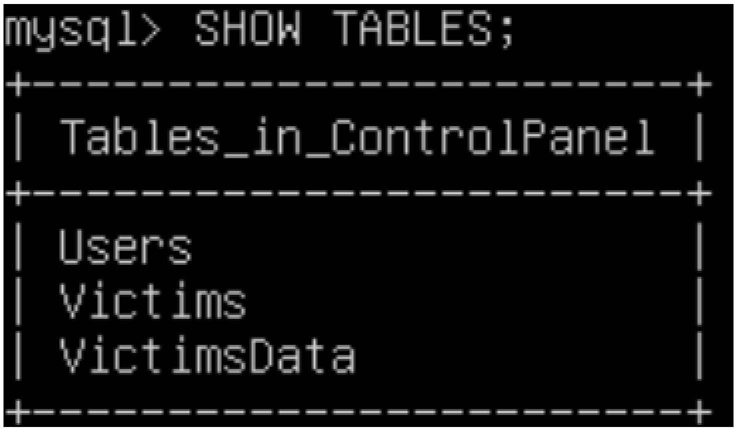
   The code is divided into two parts:

   One part is the victim part, an EXE file written in C# that communicates with the server and allows commands to be run "under the radar".

   The second part is the part of the server which also runs the site that imitates ChatGPT, also the registration and distribution phase to the SQL server and finally also the registration of the computers using an HTTP command and registration to another SQL server. The server also contains the admin's login files (which allows access to the controlled computers view) and a computer screen that confirms sending commands and receiving results.

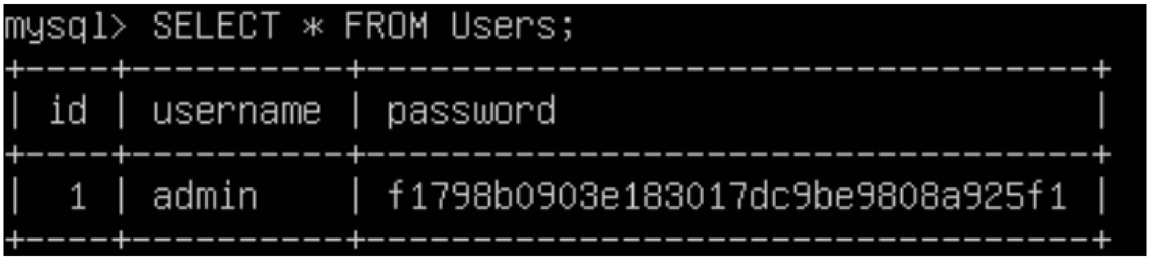
   Documentation will be in each code page and html.

SQL Tables:



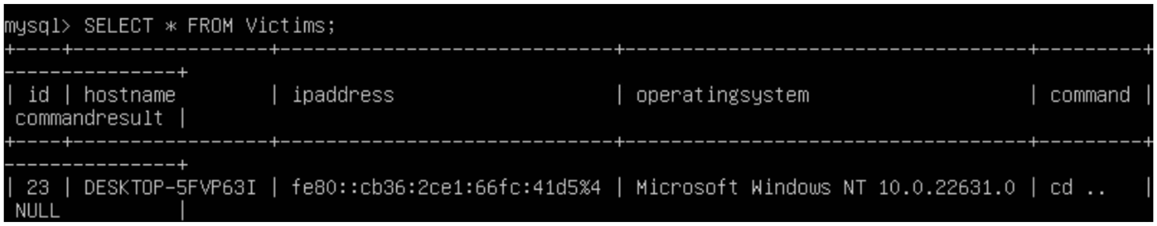
```
mysql> SHOW TABLES;
+-------------------------+
| Tables_in_ControlPanel |
+-------------------------+
| Users                   |
| Victims                 |
| VictimsData             |
+-------------------------+
```

Users (admin) table



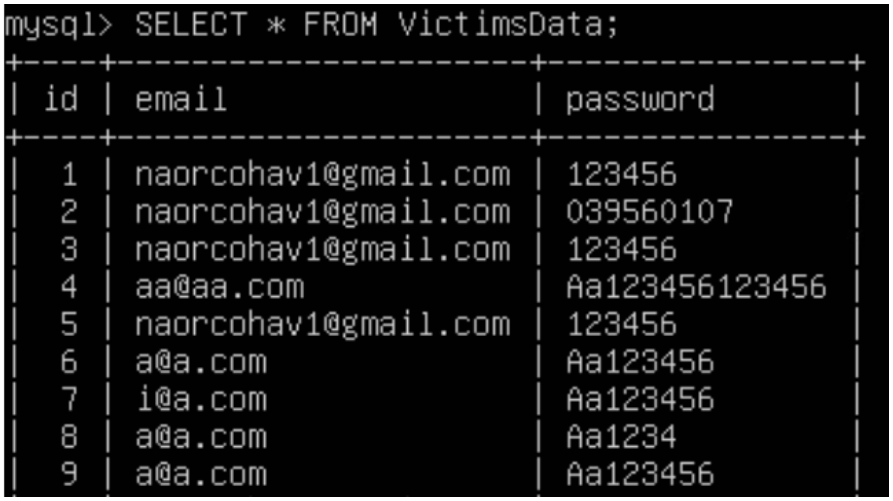
```
mysql> SELECT * FROM Users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | admin    | f1798b0903e183017dc9be9808a925f1 |
+----+----------+----------------------------------+
```

Victims PC table



```
mysql> SELECT * FROM Victims;
+----+-----------------+-----------------------------+-----------------------------------+---------
--------------+
| id | hostname        | ipaddress                   | operatingsystem                   | command |
 commandresult |
+----+-----------------+-----------------------------+-----------------------------------+---------
--------------+
| 23 | DESKTOP-5FVP63I | fe80::cb36:2ce1:66fc:41d5%4 | Microsoft Windows NT 10.0.22631.0 | cd ..   |
 NULL          |
```

Victims personal info(registration phase)



```
mysql> SELECT * FROM VictimsData;
+----+----------------------+----------------+
| id | email                | password       |
+----+----------------------+----------------+
|  1 | naorcohav1@gmail.com | 123456         |
|  2 | naorcohav1@gmail.com | 039560107      |
|  3 | naorcohav1@gmail.com | 123456         |
|  4 | aa@aa.com            | Aa123456123456 |
|  5 | naorcohav1@gmail.com | 123456         |
|  6 | a@a.com              | Aa123456       |
|  7 | i@a.com              | Aa123456       |
|  8 | a@a.com              | Aa1234         |
|  9 | a@a.com              | Aa123456       |
```

You can check out the FakeGPT (as I call it) page by clicking this link:

http://45.83.40.161/

You can also try and see the html (without the download of the exe) in this domain I bought:

https://openoi.online/

תודה רבה על הסיוע בתהליך!

נאור כוכב 318672490

מדעי המחשב שנה ג' אוניברסיטת בן גוריון

למידע נוסף

0586126161 / naorcoha@post.bgu.ac.il