After many people asking tutorial about Remote Administration Tool (RAT), today we will learn how to set up Remote Administration Tool Zeus BotNet (RAT). We choose Zeus because Zeus was one of the famous trojan horse in history that infected many servers around 2007-2010.

If you don't know about Zeus, here is some definition from [Wikipedia](http://en.wikipedia.org/wiki/Zeus_%28Trojan_horse%29):

Zeus is a Trojan horse that steals banking information by Man-in-the-browser keystroke logging and Form Grabbing. Zeus is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States Department of Transportation, it became more widespread in March 2009. In June 2009, security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and BusinessWeek.

In late 2010, a number of Internet security vendors including McAfee and Internet Identity claimed that the creator of Zeus had said that he was retiring and had given the source code and rights to sell Zeus to his biggest competitor, the creator of the SpyEye trojan. However, those same experts warned the retirement was a ruse and expect the cracker to return with new tricks. As of 13 May 2011, the source code and compiled binaries are found to be hosted on [GitHub](https://github.com/Visgean/Zeus).

**Requirements:**

1. Remote Administration Tool(RAT) Zeus BotNet ([**Download**](http://www.hacking-tutorial.com/tools/subscribers/index.php?id=zeus2101))

2. Web Server + Database Server (in this example we use [XAMPP](http://www.apachefriends.org/en/xampp.html))

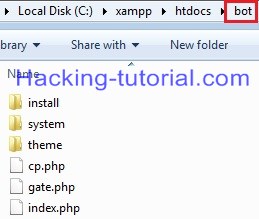
Remote Administration Tool(RAT) Zeus BotNet:

1. Firstly, we need to install the web server and database server. Since we're using XAMPP for this tutorial, you can refer to previous step by step [How to Install XAMPP in 7 Simple Steps](http://www.hacking-tutorial.com/tips-and-trick/how-to-install-xampp-in-7-simple-steps/) to install XAMPP on Windows machine and make sure your XAMPP apache and MySQL service was started and running.

2. Open the internet browser and type http://localhost/phpmyadmin. Input the username and password, by default the username is root and password leave it empty. After that create a new database, I named it bot, but you can change it into whatever you want. This database name will be used for the installation of remote administration tool.



3. The next step we need to download the remote administration tool file and extract it, you will find 3 main folder builder, other, and server[php]. Create a new folder inside C:\xampp\htdocs. I give the folder name as bot, then copy the server[php] contents into C:\xampp\htdocs\bot.



4. Now back again into our web browser and type http://localhost/bot/install into the address bar. Input all required field with the correct information.



**Information:**

– The host address for MySQL filled with your database server IP address. If you run XAMPP it should be your IP address.



– Database is filled with information about our database name that already created in step 2.

– Encryption key you can filed with any characters with length from 1 – 255

click Install to start installing.

**Notes**: If you get this error

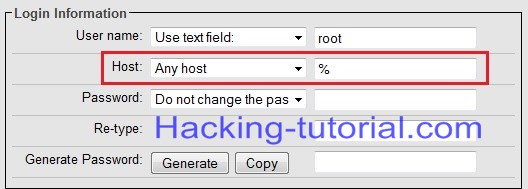
ERROR:Failed connect to MySQL server: Host 'myusername' is not allowed to connect to this MySQL server

You need to do the following step by step

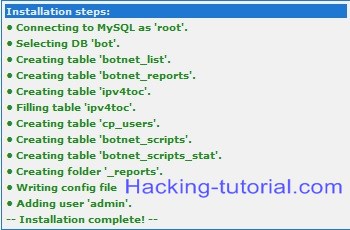
a. Open your PHPMyAdmin http://localhost/phpmyadmin and click the Privileges tab. Click edit button to edit the root user privileges.



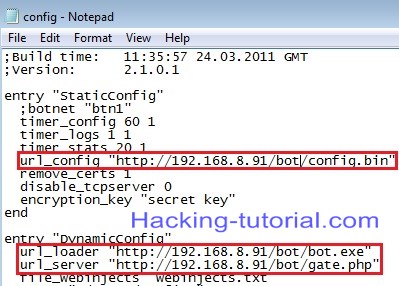
b. In the edit user page, scroll down and find the login information section. Change the Host from localhost to Any host and press Go button.



5. This is the information preview if zeus remote administration tool web server was successfully installed.

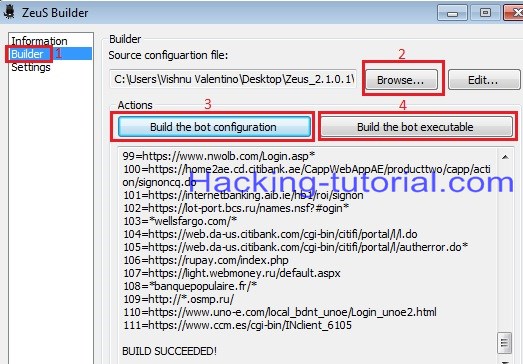


6. The next step is configuring and create the zeus bot client. Open the builder folder and open config.txt configuration file. Change the url\_config, url\_loader and url\_server configuration according to your setting, you can see my setting in the picture below.

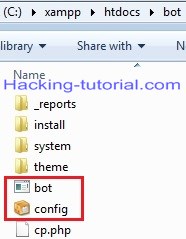


**Note**: don't forget to edit the path of webinjects.txt.

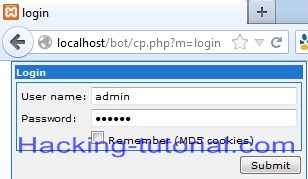
7. Now for the next step, open the zsb.exe file. In the picture below I've already create the step by step to build the bot executable. Just follow the step.



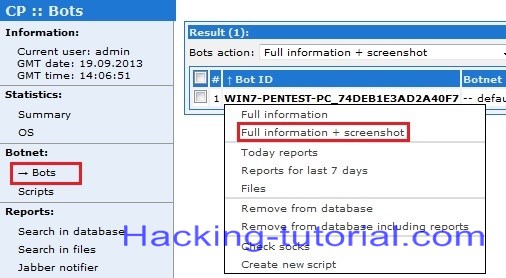
8. After all the build bot config and bot executable on step 7, now we have the new file config.bin and bot.exe. Copy those two file into the htdocs folder. Mine was inside C:\xampp\htdocs\bot.



9. Now let's says we will send the generated bot.exe to the victim. After victim execute the file we can check our attacker server. Open the browser and type http://localhost/bot/cp.php and insert your username and password.



10. We can see the new infected victim in the web interface and even view the desktop screenshot of the victim.



Here is the video tutorial in case you don't get the explanation above. Sorry if the video was cutted in the end, I accidentally stopped the recording, but anyway it's still working 🙂

**Conclusion:**

1. When victim already infected, attacker can gather many information from the victim including all internet activities and even gather all the website username and password since this tool can act as a keylogger and capturing the log in information.

2. To prevent the attack of this trojan, always update your operating system and anti virus and do not click any link that looks suspicious in your mail or chat messenger.

Hope you found it useful 🙂