**REMOTE ADMINISTRATION TOOL – GUIDE**

posted on MAY 10, 2017

**REMOTE ADMINISTRATION TOOL (RAT) ZEUS BOTNET**

The best aspect of going digital lies ín the convenience of having a computer that replaces physical activity. Some say remote administration tool is counterproductive to the human function. However, remote administration tool has more pros than cons. Being connected is one such advantage. You can have access to any computer, and distance may not matter.

Remote Access Control or RAT is a software. It allows a certain user to control any system even without physical access to it. Thus, the remote “operator” gains full control over the device.

Although RAT and desktop sharing has legal uses, this type of software is often used in malicious activity. The operator can control RAT through a network connection. This is more so because it hides from detection by security software.

RATs can take on a number of activities when activated in a “client” computer. Apart from gathering login and account information, RATs can also format drives. Additionally, RATs can install applications silently. They can also run and operate without the victim’s knowledge.

**Guide to set up Remote Administration Tool (RAT) Zeus BotNet:**

This guide will help in setting up Remote Administration Tool (RAT) Zeus BotNet. However, the guide requires download of the software. We also need a database server and web server for this task.

Zeus or Zbot is the infamous Trojan horse that was spread through phishing schemes and drive-by downloads. It installs itself and uses form grabbing and keystroke logging to steal banking information. In 2009, Zeus compromised over 74,000 FTP accounts in company websites. Such companies included the Bank of America and NASA.

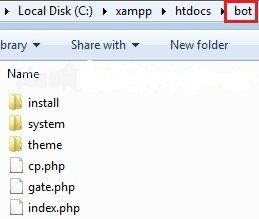
In 2010, Internet security providers claimed the creator of Zeus was retiring. As a result, he was to sell the code to his competitor, SpyEye Trojan creator. Experts later retracted this statement. They said that it was a ruse and that the developer might come back with new tricks. Binaries and source code are on GitHub since 2011.

**How to setup Zeus Botnet RAT:**

1. The first thing to do is have a database server and web server running. Download XAMPP [here](https://www.google.com.ph/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjelpT3i9DTAhWMyLwKHSr2C8YQFgglMAA&url=http%3A%2F%2Fdownload.cnet.com%2FXAMPP%2F3000-10248_4-10703782.html&usg=AFQjCNGB9RdfBpadzALLm5w6dW67vkqhyg&sig2=5N3XvggiuiUD_) to use for this task. Make sure that you have it up and running, as well as your MySQL service.
2. In your internet browser, type <http://localhost/phpmyadmin>. Next, enter the username and password. Afterward, key in the default username **root** and leave the password blank. Create a database after that. Use the database name earlier created to setup Remote Administration Tool later.



1. Download the RAT file and extract it. There are three main folders in the archive: builder, server (PHP) and other. On your XAMPP files, locate the **htdocs** folder (C:\xampp\htdocs) and create a new folder inside it (you can use <bot> as folder name). Finally, copy the contents of server[php] to C:\xampp\htdocs\bot.



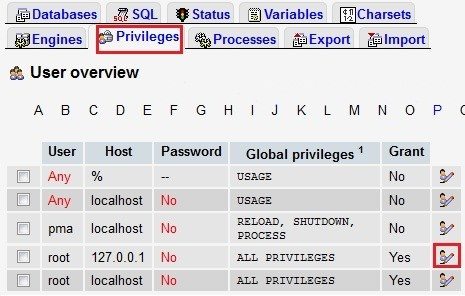
1. Next, go back to your web browser and search <http://localhost/install/bot>. Supply the correct details in each of the fields.



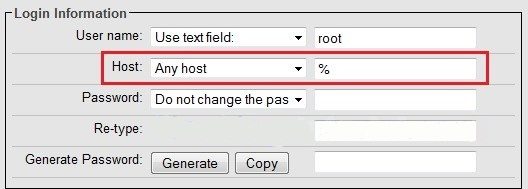
Your database server IP address will fill the host address in MySQL server. This is your IP address in XAMPP. Supply the database name in step 2, and fill the encryption key with any characters 1-255 in length. Afterward, proceed by clicking Install.

You might encounter an error while doing this step. The error says “Failed to connect to MySQL server: Host ‘myusername’ is not allowed to connect to this MySQL server.” Do the following to remedy this:

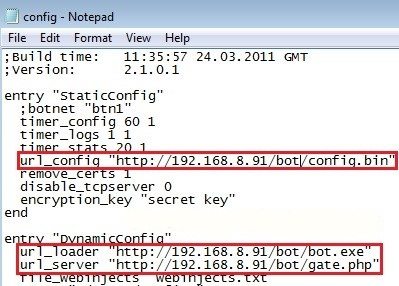
1. First, open <http://localhost/phpmyadmin>. Click the Privileges tab where you will find an edit button. Next, click the button to modify the user **root**privileges.



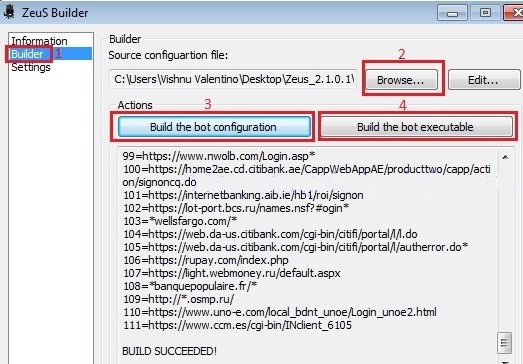
1. Clicking the button will, as a result, lead you to the edit user page. Scroll down to see the login information. Click the Host to **any host** from **localhost**and then press the “Go” button. A dialogue box opens when it successfully installs.



1. You need to create and configure the Zeus bot client. On the **builder** folder, open the configuration file named **config.txt.** Change the **url\_server**, **url\_loader,**and **url\_config** to match your settings. Also, remember to edit the path of **webinjects.txt**.



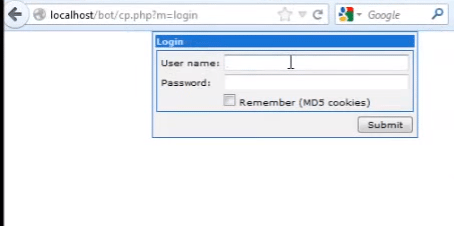
1. At this point, open the **zsb.exe**file. This opens a dialogue box. Follow the steps as numbered in the image. This will build your bot executable.



1. Bot executable and Bot config enables adding new files after step 6. These are the **bot.exe** and **config.bin.** Copy these files to the htdocs folder that we configured earlier (C:\xampp\htdocs\bot).



1. The way to test this is to send the bot.exe to the target victim. Say the victim executes the file, we can see and check through the attack server. Open your browser and key in <http://localhost/bot/cp.php>. Afterward, type your username and password.



1. Finally, you gain entry to the newly infected victim as seen from your browser. It has all the information. You can view right from your web interface. You can even see a screenshot of the desktop view of the victim.



**IMPORTANT REMINDERS:**

* Zbot is very forward when it comes to attacks. The attacker can collect data and information of the infected victim. It can also obtain some very private and sensitive information of the victim. It can also monitor internet activities of the victim.
* Zbot acts as a keylogger. Thus, it can capture login information. This means that it can save usernames and passwords entered in websites.
* Since Zbot is a persistent Trojan, having an up-to-date internet security is key. Even then, this malware uses stealth technique and therefore it is tough to detect. Antivirus software might only manage to prevent some infection attempts.
* The best form of protection against Zbot is vigilance about suspicious links from email and websites. Security experts advise users to avoid clicking anything that looks hostile. Staying on top of your pop-up settings can also help prevent Zbot infection.