

Blackshades NET 3.6 User Guide



SakiMCM

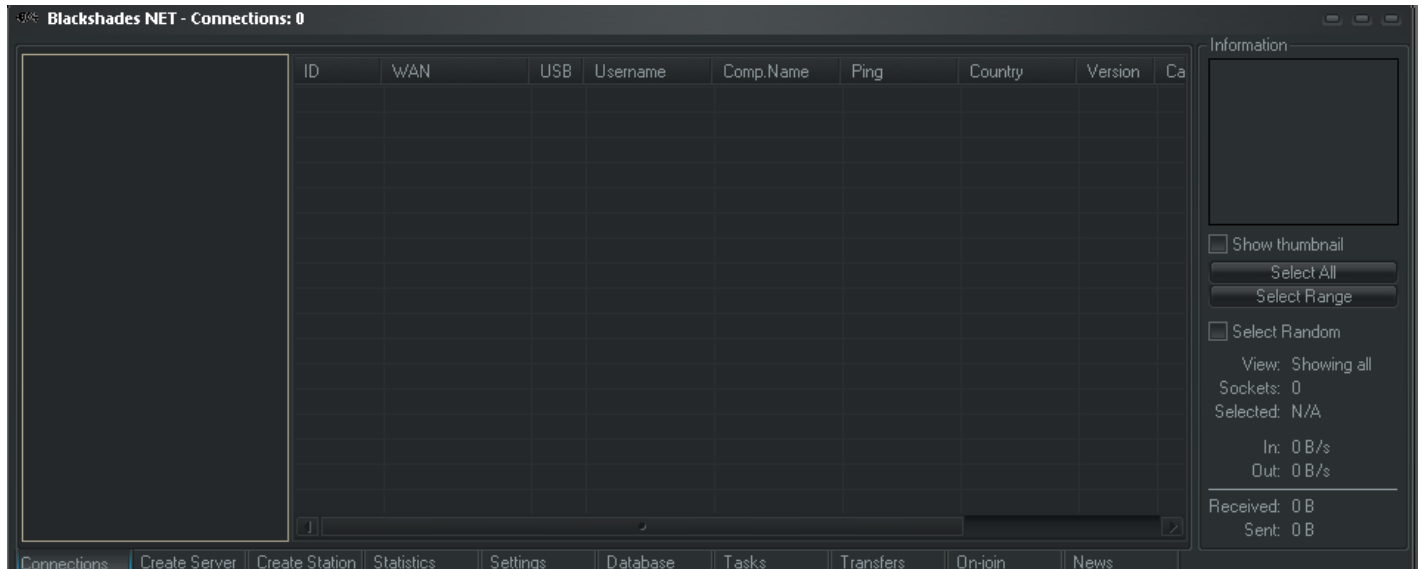
This Guide details how to use every feature that Blackshades NET has to offer. For the most part the host is my own computer, but some features are demonstrated on other bots.

SakiMCM@gmail.com

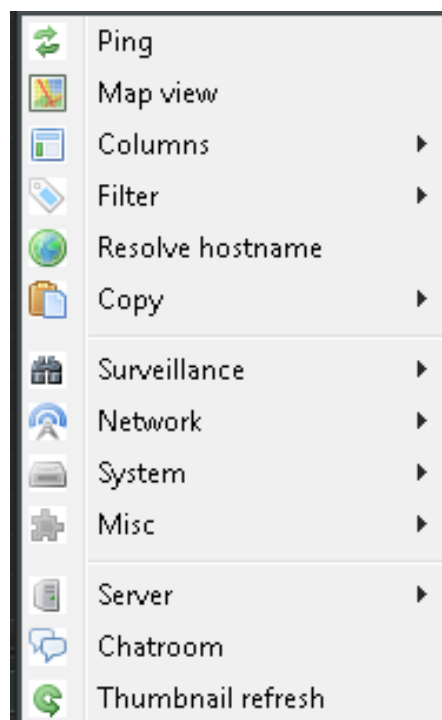
10/18/2010

Connections

When you launch Blackshades NET client and have activated your ports, you will see a screen not too dissimilar to this:



This is the Connections screen and lists all the bots that are online at the moment. To access the features menu, just select the bot and right click. A little menu will appear and you can then select which feature you want.



The Features Menu

Ping

The ping function gives you the average time (in milliseconds) that it takes for your computer to send out 4 32 byte packets to the bot and to receive them back. This gives you a good indication of how fast your transfer speeds with the computer will be as a shorter ping time means screen shots will take less time to come through.

Map View

The map view allows you to visualise where your victims are. It also allows you to select all bots in a certain area, e.g. all the bots on the west coast of America.



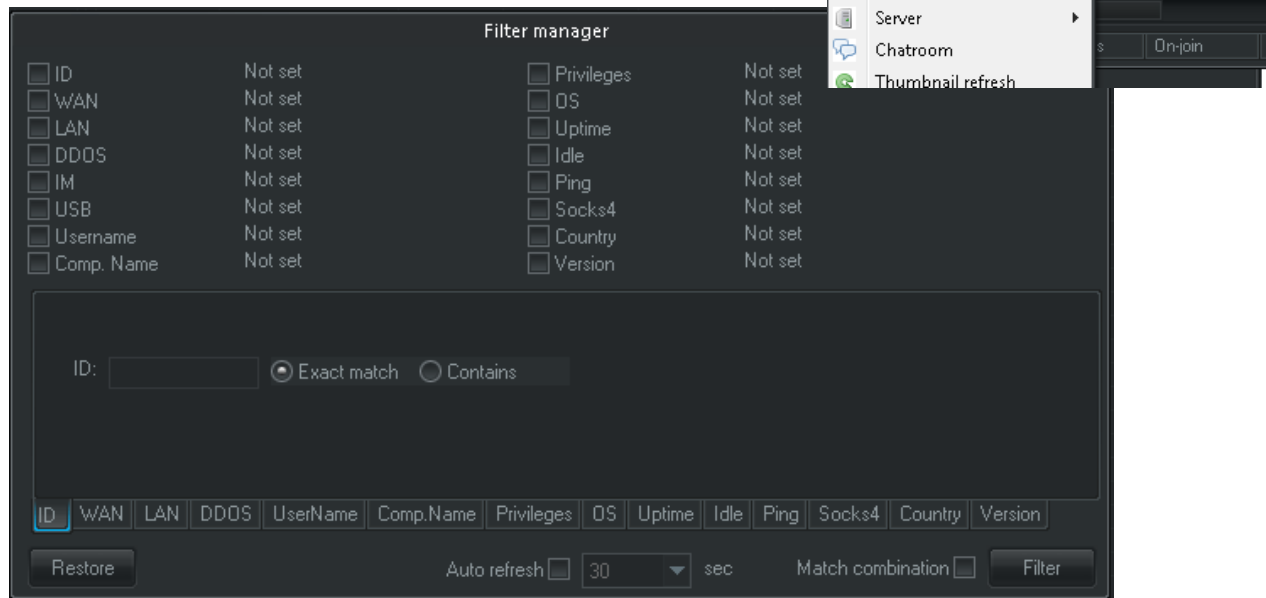
To use the map function, simply use the “Z” and “X” buttons to zoom in and out respectively and use the click and drag method to select multiple bots.

Columns

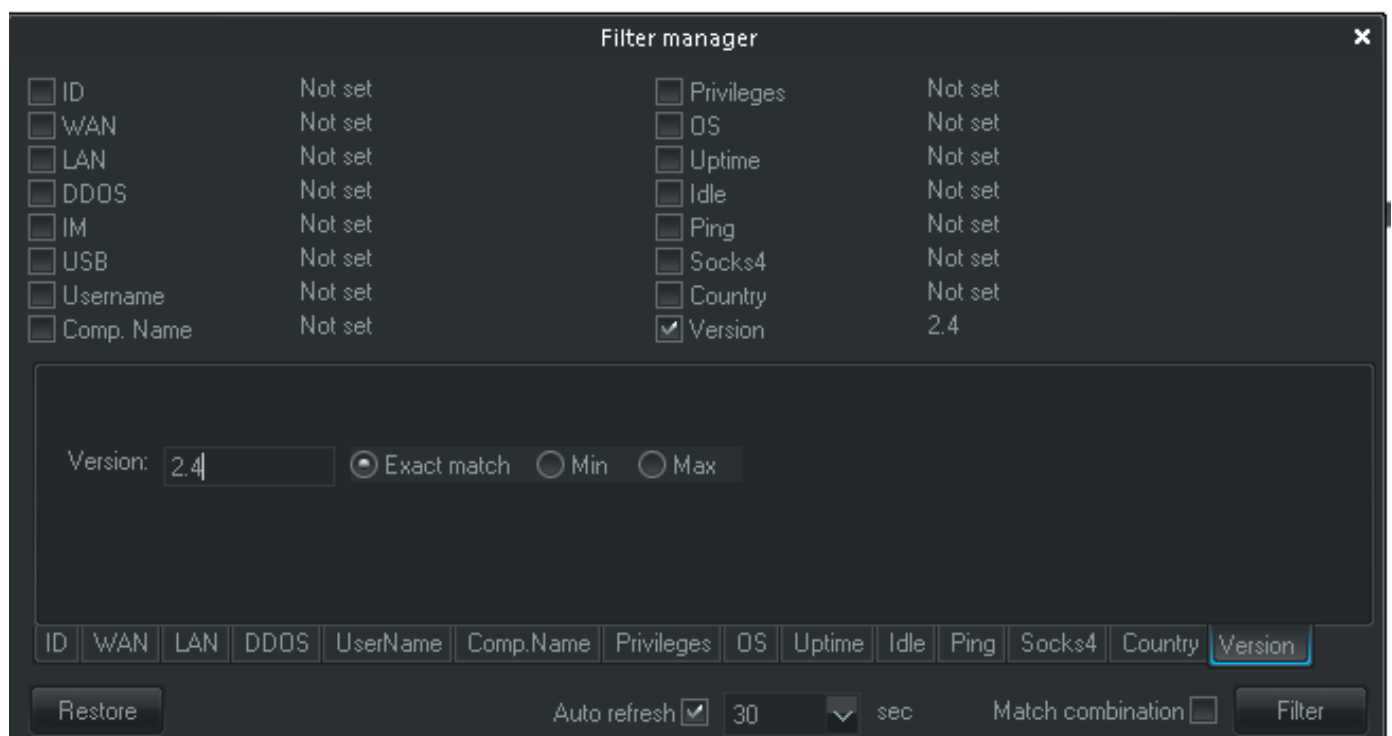
This allows you to select which bits of information you wish to see about your bots, simply uncheck the ones that you do not want to see. Simple.

Filter

The filter menu has two sub-menus; “Edit” and “Restore.” The filter menu allows you to select bots based on various settings.



To add a filter, simply check the box next to the feature you want to filter. For example, if I wanted to select only bots that run BS NET 2.4, I would select the Box next to “Version” (bottom right option) and then open the Version Tab and enter 2.4 in the box. The end result should then look something like this.



Now, you may be wondering what the difference is between “Exact Match”, “Min” and “Max”. Let’s say your version you entered was Blackshades NET 2.4

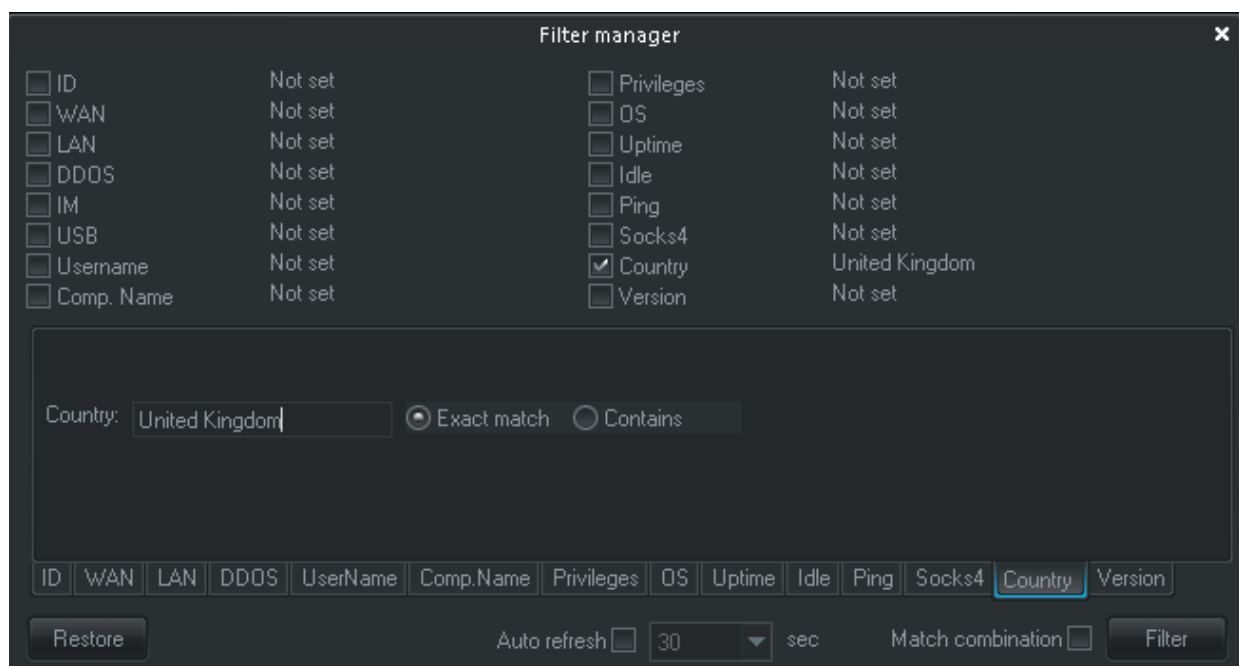
If you selected Exact Match, you would only see computers running, Blackshades NET 2.4.

If on the other hand, you select Minimum, it would show any computer with Blackshades NET 2.4 or above as they are a higher release.

If you select Maximum, you would see any computer running Blackshades Net 2.4 or below as they are lower releases.

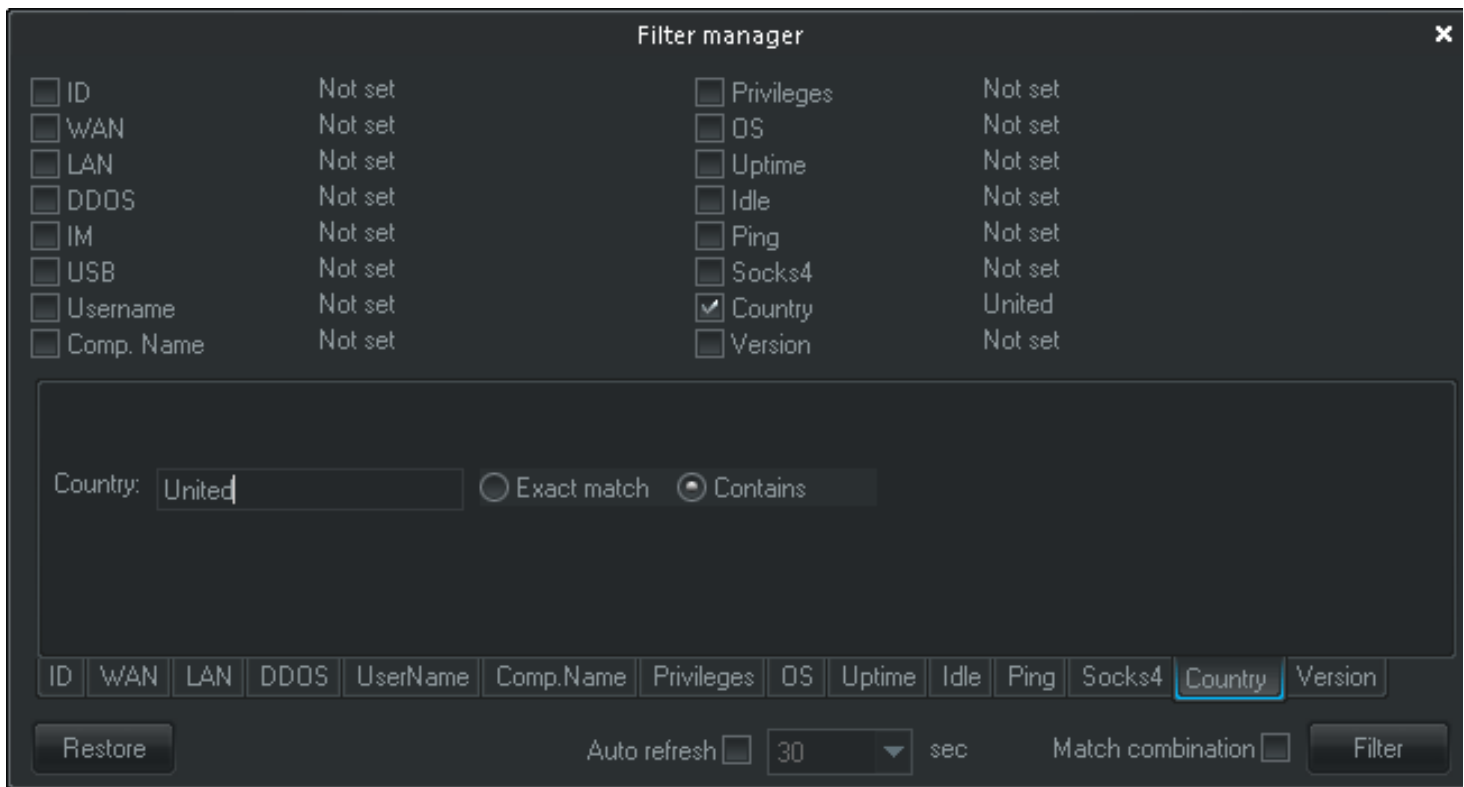
The Filter also allows you to edit things that have text values. Let’s take the country as an example.

If I wanted to see every server in the United Kingdom, I’d enter “United Kingdom” into the box and select “Exact Match”



If However, I wanted to see all servers from the United Kingdom and the United States, I would enter the word United into the box and select contains, that way I’d get both countries.

There are also options along the bottom of the manger, for those of you who didn't notice.



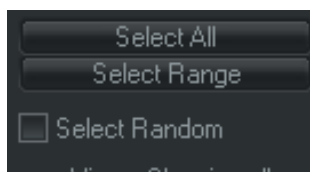
Restore – Remove all filters and text in the boxes.

Auto refresh – This checks all the bots every set period (1-60 seconds) to see if any bots which have recently connected fit the filter requirements. This means that your list will always include all possible bots.

Match combination – If you select several options, the filter will select bots which fit any of those requirements. E.g. if you filter bots from the USA and version 2.6, you will be shown every bot that is version 2.6 and every bot that is from the USA. If you only want to see bots that are version 2.6 and from the USA you must select match combination as well.

Select

When you have lots of bots, you may want to only execute commands on a certain number of bots. This is where the select option comes in.



With the select option you can either select:

1. All the bots you are connected to
2. A range of Bots e.g. 5 bots

3. Select random bots

To deselect the bots, just click somewhere else.

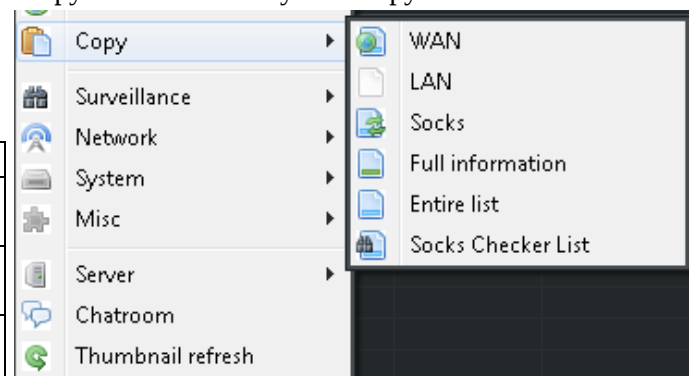
Resolve hostname

The resolve host name option gives you an insight into what internet company/wireless router your bot uses; this can be used for malicious purposes.

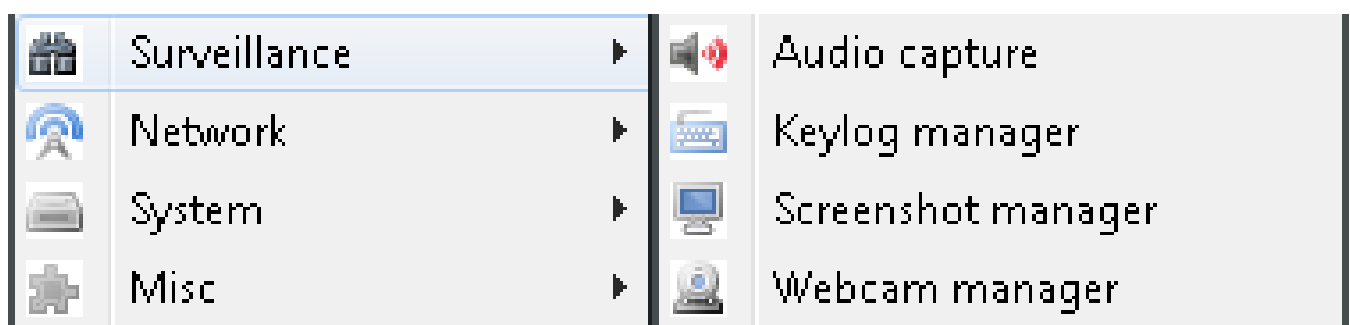
Copy

This is pretty straight forward and self-explanatory. The copy function allows you to copy some or all of the bot information onto the clipboard.

Select	Copies
WAN	The computers IP Address e.g. 92.139.43.234
LAN	The computers local Address e.g. 192.168.0.1
SOCKS	Marjinz added this, but what it does no one knows.
Full Information	All the information available for that bot
Entire List	All the Information available for every bot
SOCKS Checker List	This copies anything with a value in the SOCKS field and the IP, one per line e.g. 123.45.67.89:1080 so you can check online.

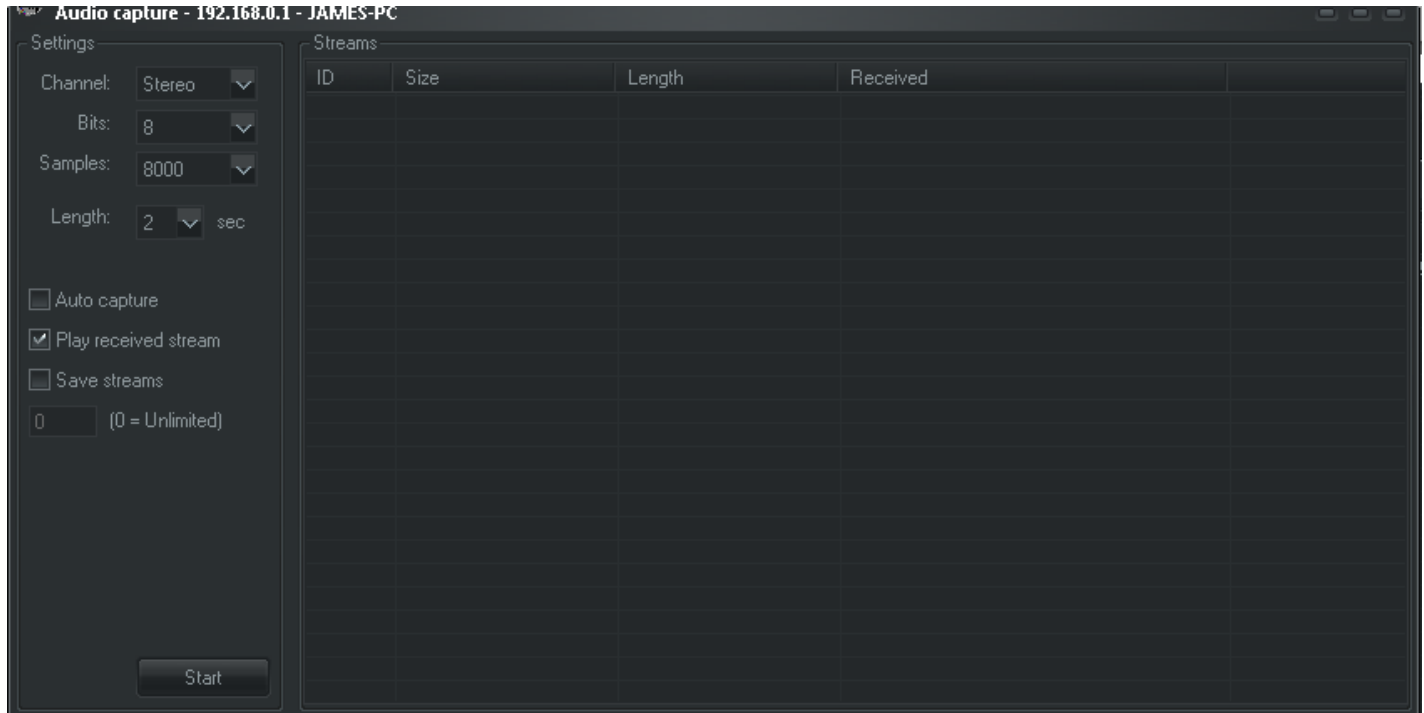


Surveillance



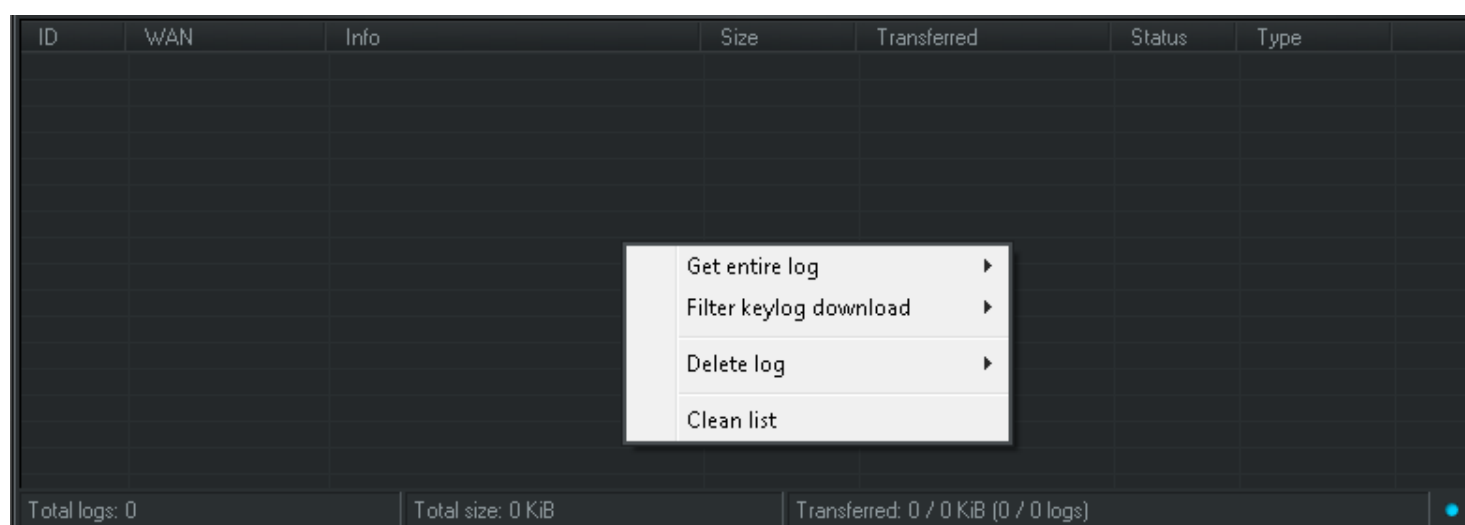
This is one of the most useful parts of Blackshades NET. It basically allows you to spy on the person whose computer you've ratted. There are four options in this menu, but before you use any of them, you **MUST** port forward and activate the transfer port, or you'll end up looking at a blank screen. To access the options, just select the bot you want to spy on, right click and select the option you want.

Audio Capture



The Audio Capture is pretty straight forward to use. Simply select the settings and press start. The sound is recorded for the set length of time, and then transferred to your computer so the audio isn't in real time.

Setting	What it does
Channel	Do you want stereo sound or mono?
Bits	How good do you want it to be? 16 bit is better but takes more space
Samples	How good do you want it to be? Higher is better but again takes up more space.
Length	How long should each recording be? (The longer it is the more out of sync it is.
Audio Capture	Do you want to hear the computer audio e.g. if the person is using headphones
Play Received Streams	Do you want to hear the audio when it's received?
Save Streams	Pretty obvious, do you want to save the audio you receive?

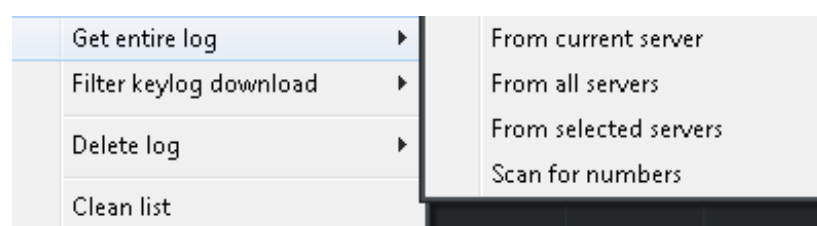


Keylogger

The Keylogger is one of Blackshades NET's defining features. It allows you to filter keylogs and search through them for any information you want.

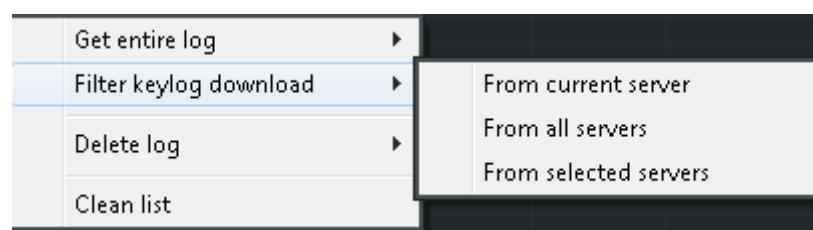
To access the keylog menu, simply right click anywhere in the Keylogger window and it should pop up. There are then a number of menus and sub menus to choose from.

Get entire log



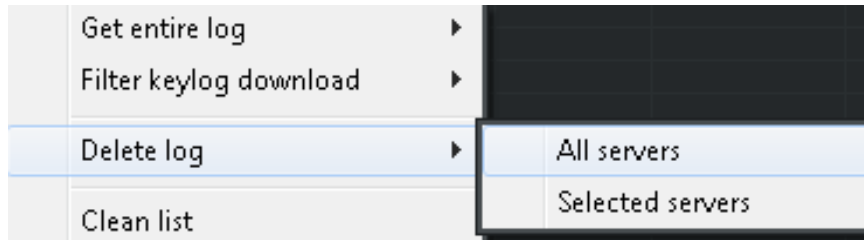
Sub-Menu	What it does
From current server	Downloads the log from the server you right clicked on
From all servers	Downloads the logs from every server online
From selected servers	Downloads the logs from any servers you may have selected e.g. random or all from the USA.
Scan for numbers	Looks through all the logs to see if there are any numbers, useful for credit cards and the like.

Filter keylog download



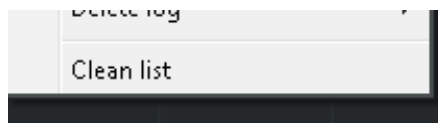
This menu allows you to filter the logs by searching for specific words and is pretty straight forward. All you do is select whether you want to filter the Keylogger from the options given; you then put in the filter keyword and how many characters before and after you want.

Delete Log



The delete function allows you to remove logs from the remote that contain nothing of interest or have been thoroughly read and all valuable data extracted. This means that you won't be continually getting data that's years old (If your bots stay online that long!) If you have some logs with interesting info, some with none, simply select the logs that have no data in and select the "Selected servers" button. If all the logs have been used or contain no information select the "All servers" button.

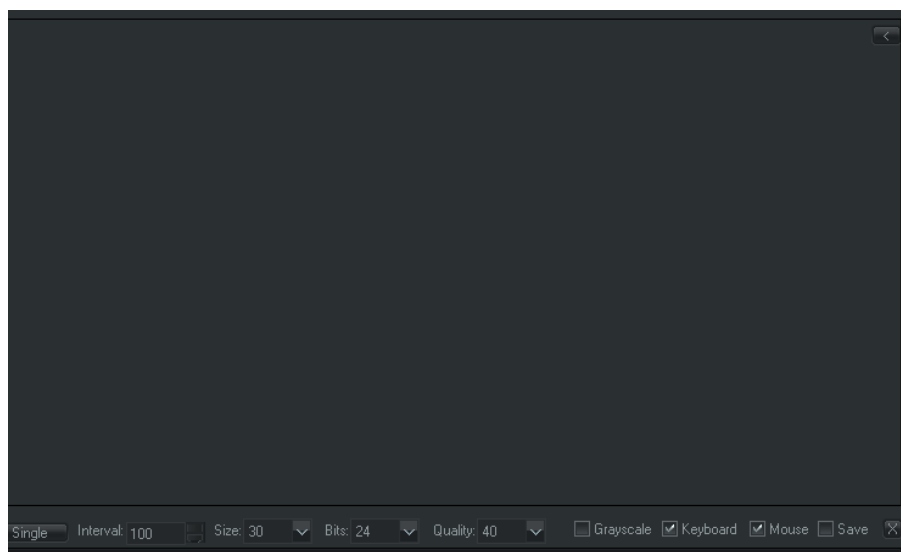
Clean list



The Clean list function just clears the keylog field so instead of displaying all the logs downloaded it appears blank.

Screenshot

The screenshot manager allows you to remotely view your victims screen, just as with team viewer, except that it can't be disconnected.



To Activate the screenshot feature simply enter your settings and press start. If you just want a single picture, press single.

Option	What it does/ Configuration
Interval	How often is a picture taken (in milliseconds)
Bits	Affects the picture quality, more bits, better quality larger file)
Size	How big will the picture be (larger size, more data, slower speed)
Quality	How good will the picture be (better quality, more data, slower speed)
Grayscale	Incoming images in black and white, helps keep file size down
Keyboard and mouse	Allows you to click anywhere and type info into fields
Save	Allows users to save the screenshots

Webcam

The Webcam feature is really easy to use, simply right click on the bot you want and select Webcam Manager. You can vary the quality of the webcam depending on how fast your connection is, lower quality = less data used = less jerky but also less clear. Select Save if you want to save the feed, it is however saved in pictures rather than as a video.

Quality at 100



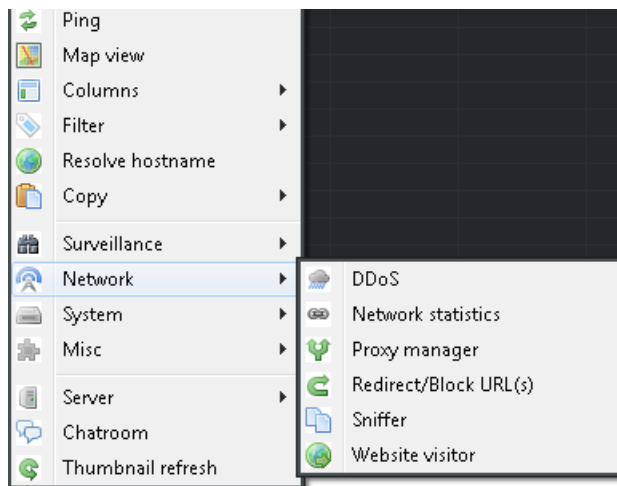
Quality at 50



Quality at 0

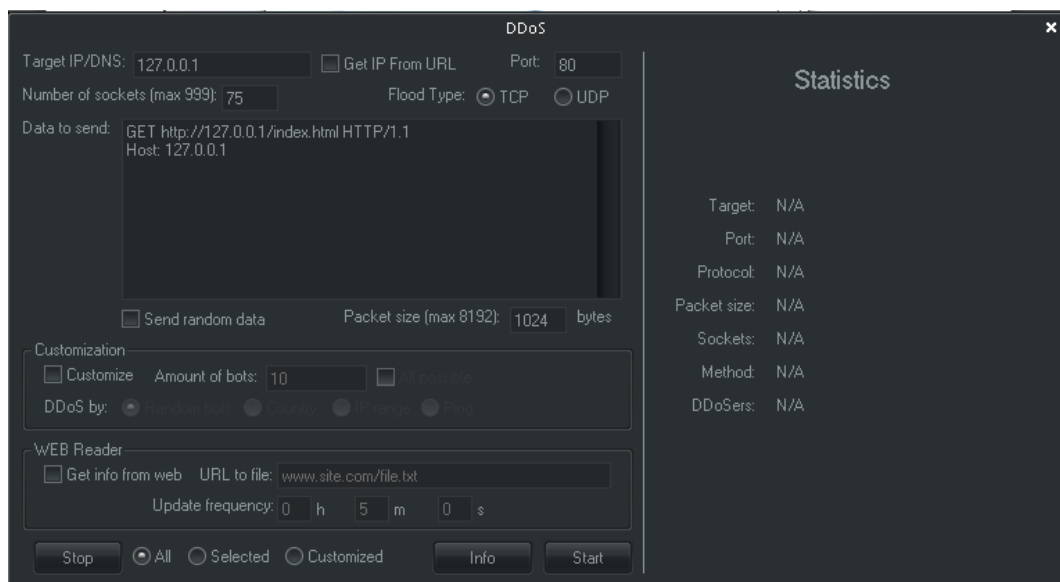


Network Manager



The Network tab allows you to interfere with the computers network settings and execute the internet related functions of Blackshades NET

DDoS

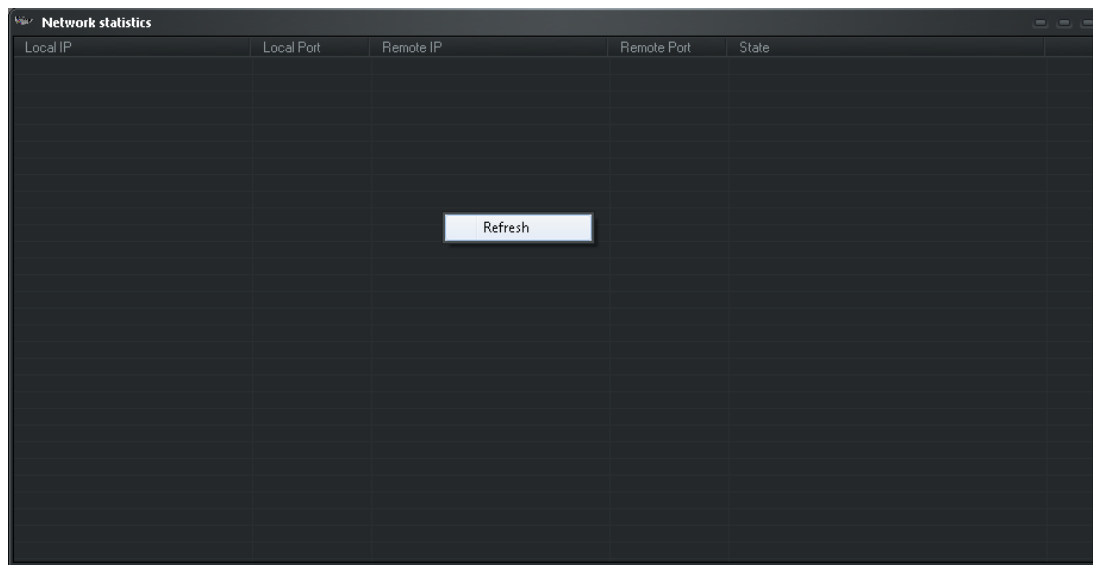


I'm not going to go into detail about how to DDoS here, there's plenty of information on that on HF and other such forums. I'm just going to explain what to put where.

Option	What to put in.
Target IP/DNS	The IP address or DNS you want to DDoS if you want to DDoS a website you can enter the URL and select Get IP from URL
Port	The port that service runs on e.g. websites:80, FTP:21
# of Sockets	How many connections do you want each bot to make
Flood Type	TCP for Websites , UDP for Networks
Data to send	What you want to send
Other Options	Random Data; Send anything (overrides "Data To Send"), Packet size; the larger the more effective the greater the bandwidth used.
Customize	Bots; How many bots to use (the more bots, the more efficient, DDoS By; use bots selected by certain criteria e.g. location.

WEB Reader	Get settings from a website allowing you to update it remotely.
------------	---

Network Statistics



To use this function simply right click and select refresh. This function tells you all the connections the server is making, what IP address they're going to and which port it's using.

Local IP	Local Port	Remote IP	Remote Port	State
192.168.1.68	6111		4488	
192.168.1.68	6111		57496	
192.168.1.68	6111		61867	
192.168.1.68	6111		4187	
192.168.1.68	6111		1531	
192.168.1.68	6111		40459	
192.168.1.68	61540		1863	
192.168.1.68	61862		8080	
192.168.1.68	64142		46229	
192.168.1.68	64303		26368	
192.168.1.68	64309		443	
192.168.1.68	64310		57824	
192.168.1.68	64338		60380	
192.168.1.68	64359		17459	
192.168.1.68	64370		37391	
192.168.1.68	64396		5112	
192.168.1.68	64399		50001	
192.168.1.68	64455		21300	
192.168.1.68	64456		443	
192.168.1.68	64459		443	
192.168.1.68	64465		64311	
192.168.1.68	64490		80	
192.168.1.68	64525		53612	
192.168.1.68	64534		17494	
192.168.1.68	64551		14936	
192.168.1.68	64555		60601	
192.168.1.68	64569		42652	
192.168.1.68	64571		63139	
192.168.1.68	64576		33885	
192.168.1.68	64579		17588	

So what's what?

Local IP: your Network IP

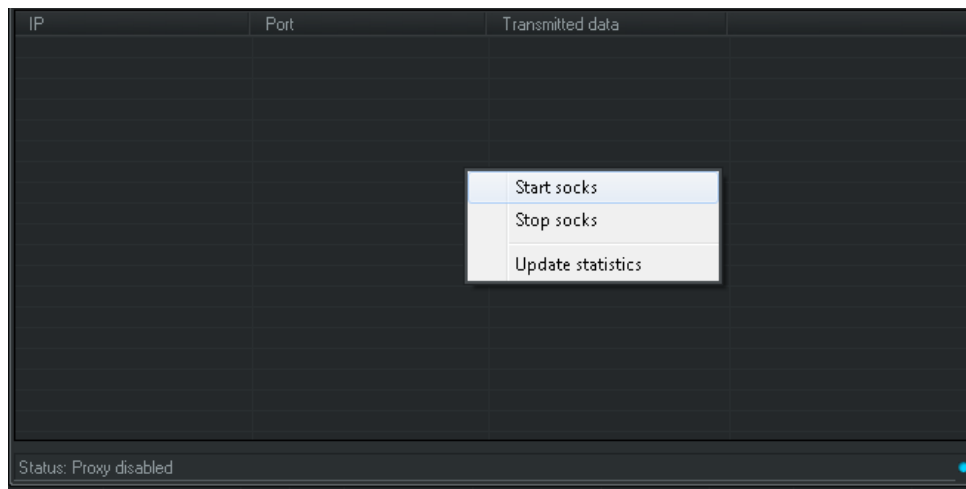
Local Port: the port you were connecting out of.

Remote IP: the server side IP of the computer you were connecting to (I blacked this out to protect the IPs of all my bots)

Remote Port: the port you used to connect to the machine.

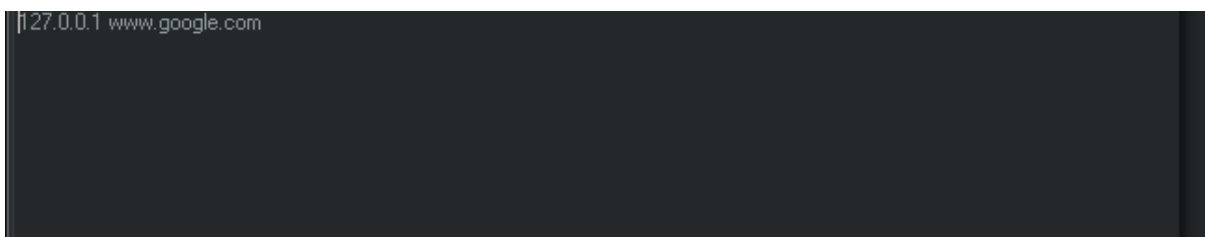
Proxy Manager

The proxy manager allows you to connect to the internet via the bots computer, making you anonymous.

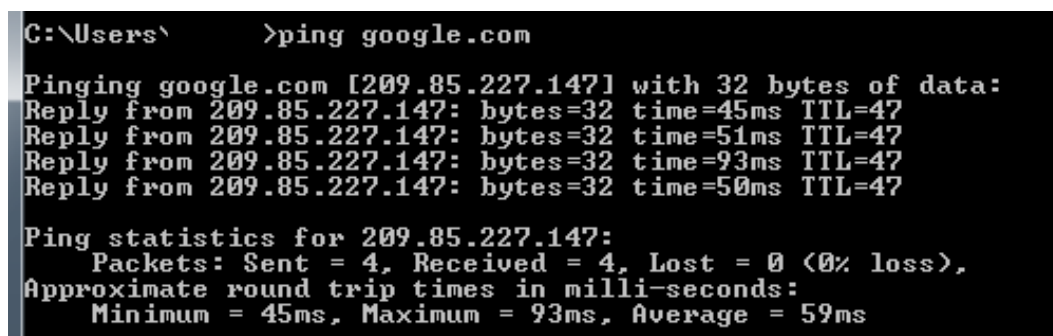


To start the Proxy, simply right click anywhere in the box and select “Start Socks” Then enter the SOCKS4 port for that bot and click ok, to update the transmitted data select “Update Statistics”

Redirect/Block URLs



To redirect the user away from a webpage, you must first get the web pages IP address. To find that go to cmd and type “ping www.website.com”changing the address to the website you want them to be redirected from. I’m going to use Google as an example.

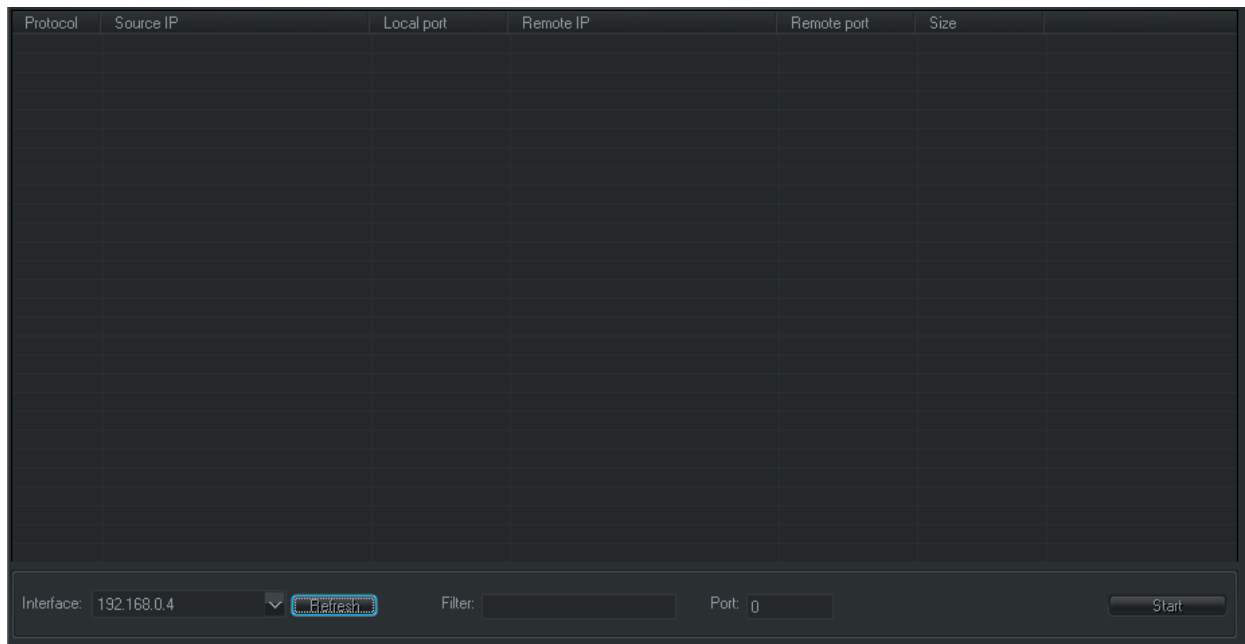


So the IP address for Google is 209.85.227.147. Now if I wanted to redirect to yahoo.co.uk I’d type:

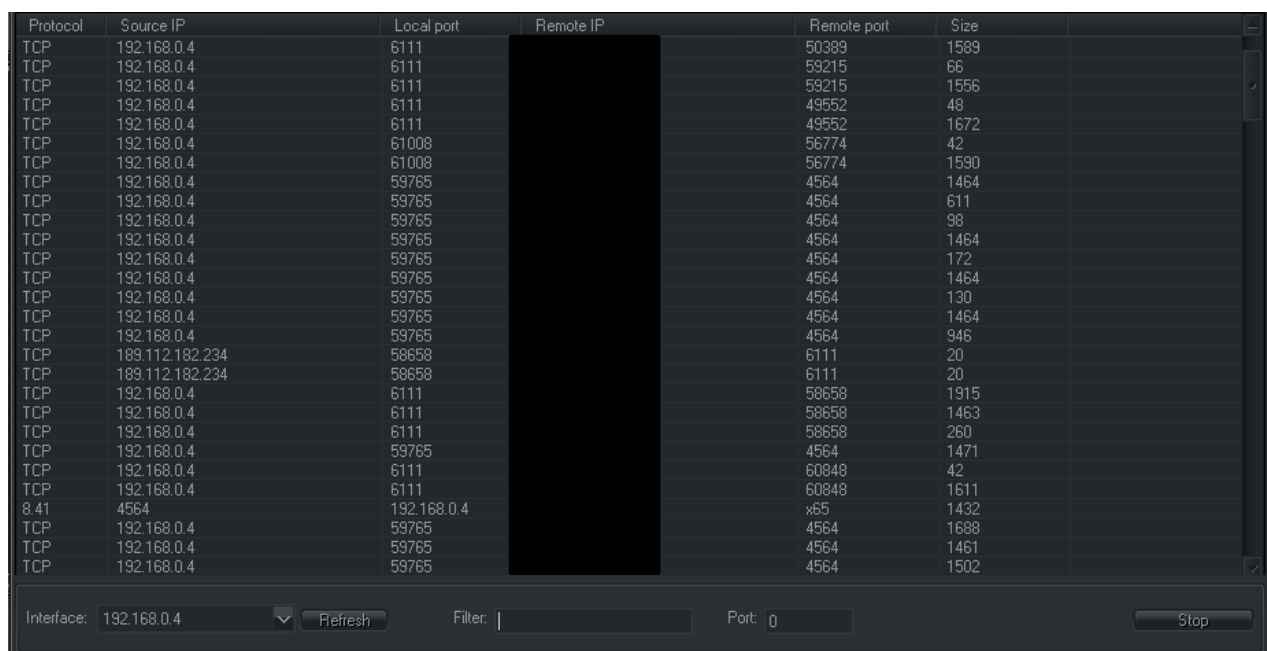
209.85.227.147 [IP Address of Yahoo] Then select update (single, selected or all) so when any bots tried to visit Google, they’d be redirected to yahoo.co.uk. To stop the redirection, simply remove it from the list and select update (single, selected or all) and it will stop redirecting.

Sniffer

The first thing to do with the sniffer is to click the refresh button, to load the local IP addresses for the server. Then just choose the one which comes up on the Blackshades NET Connections list as WAN.



Then Click the start button and it should load up which ports are open and what Protocol they're using, where they're connecting to.



You can then see which one is your computer by which one connects to your port. Mine is anything with the remote port 4564. If you want to see all the connections too one IP, just enter the Remote IP into the filter box and the port into the port box.

If you right click on the list you are presented with more options.

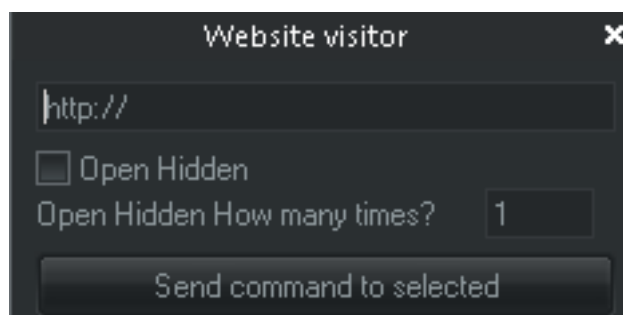
Display data will show all the Data that has been transmitted from the source to the destination on Hex format.



The save function has two settings, “All” or “Selected.” This allows you to save the entries for later inspection. To select ones not next to each other, just press the shift button and click on the ones you want to save.

Clear just empties the list so it can be refreshed.

Website Visitor

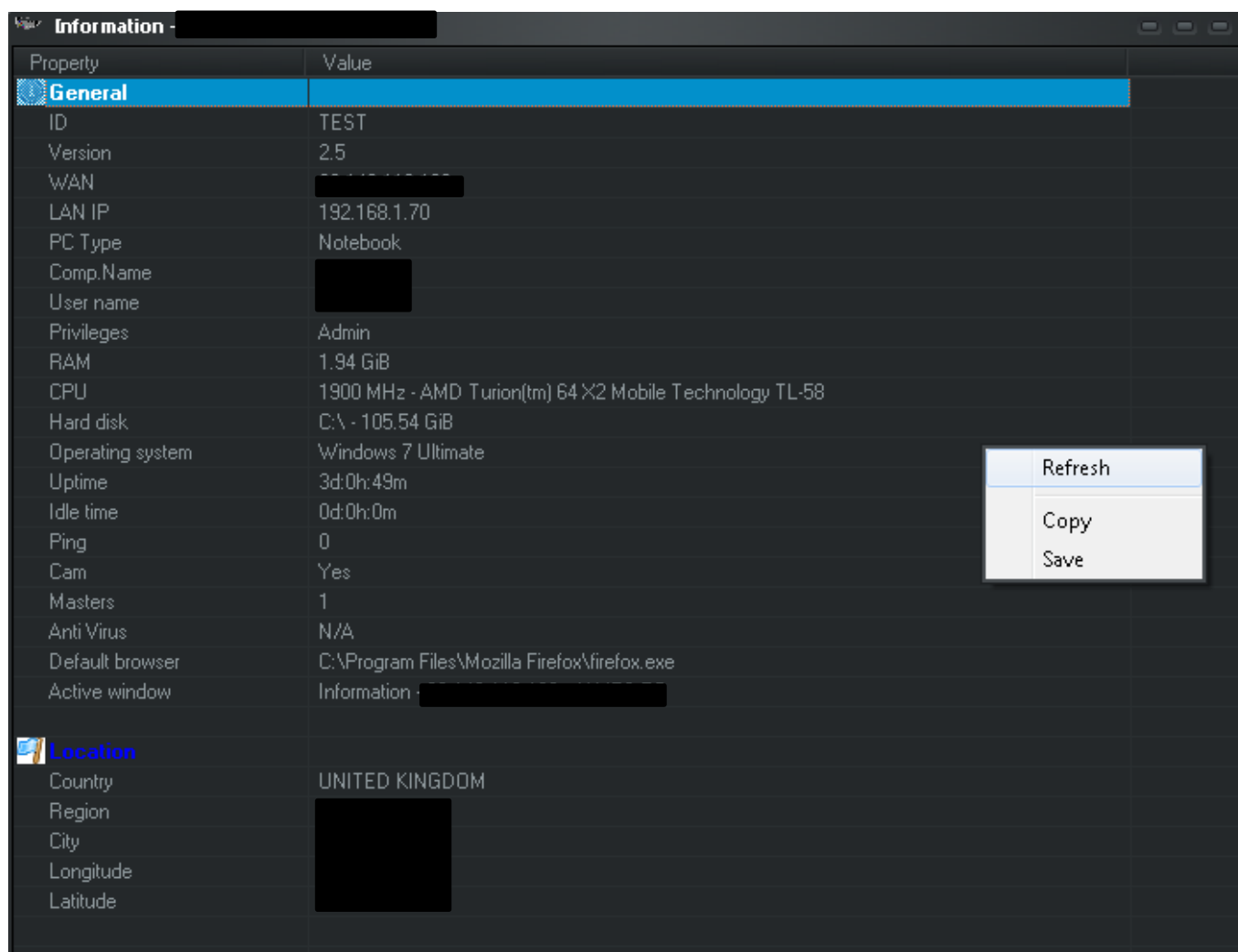
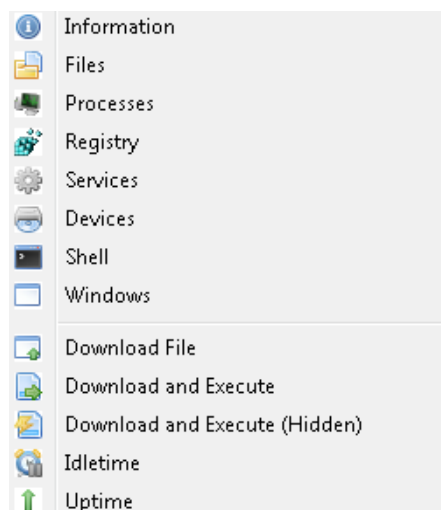


If you want to force your victim to view a website, for your own amusement, the easiest way is with the website visitor. Enter the website URL into the box and then decide whether you want the site to open on top or minimised (Hidden) and if you want it minimised, how many do you want to open? Then just click “send command to selected” and the website will open on all the victims hidden or otherwise.

System

Information

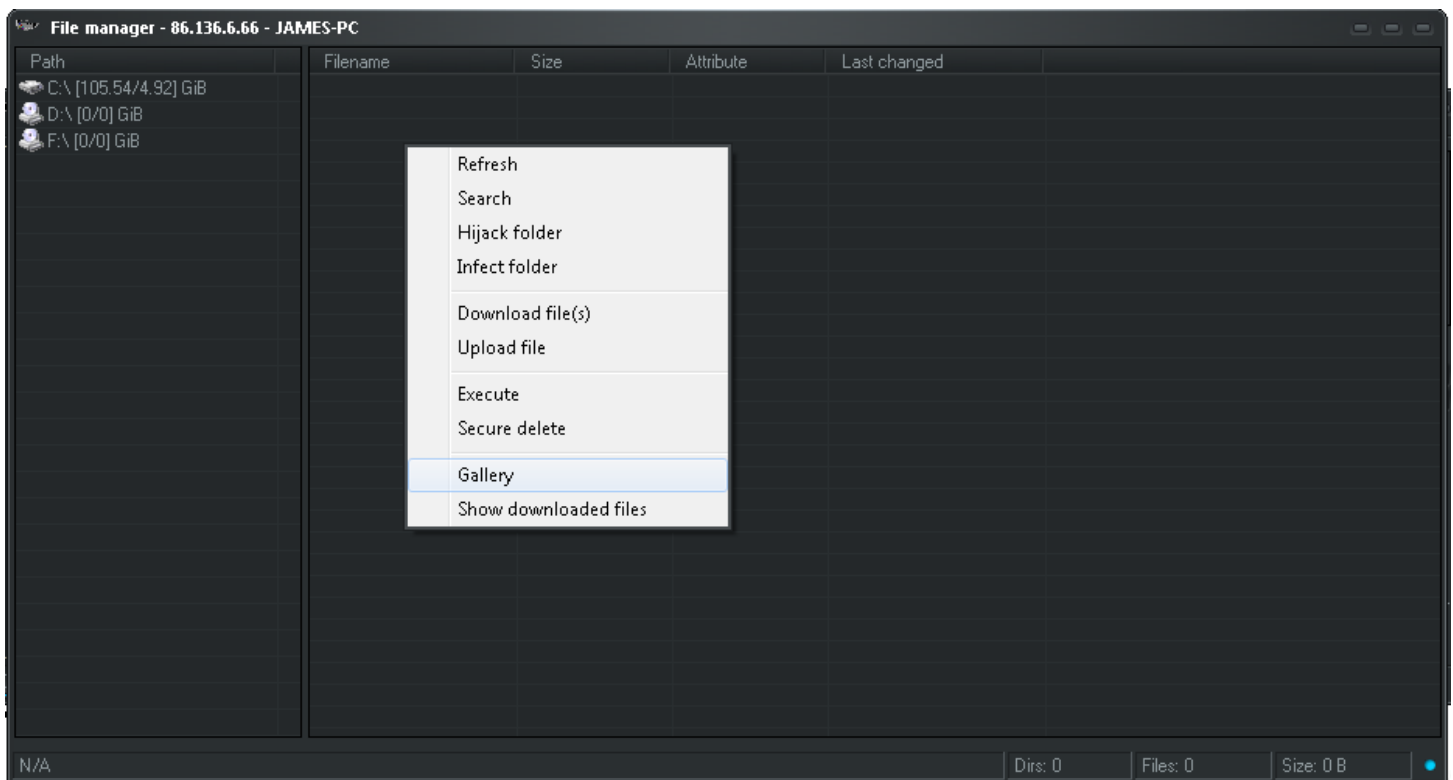
The information option allows you to see general information about the computer you've RAT'ed. It's also accessible by double clicking on the bot of your choice.



If you are presented with a black screen, just right click and select refresh. Should you want to copy various bits of information, just select the ones you want, using ctrl+click to select ones not next to each other and shift+click/arrows to select ones next to each other.

Should you use the save function, make sure you save it as "filename.txt" not just "filename"

Files

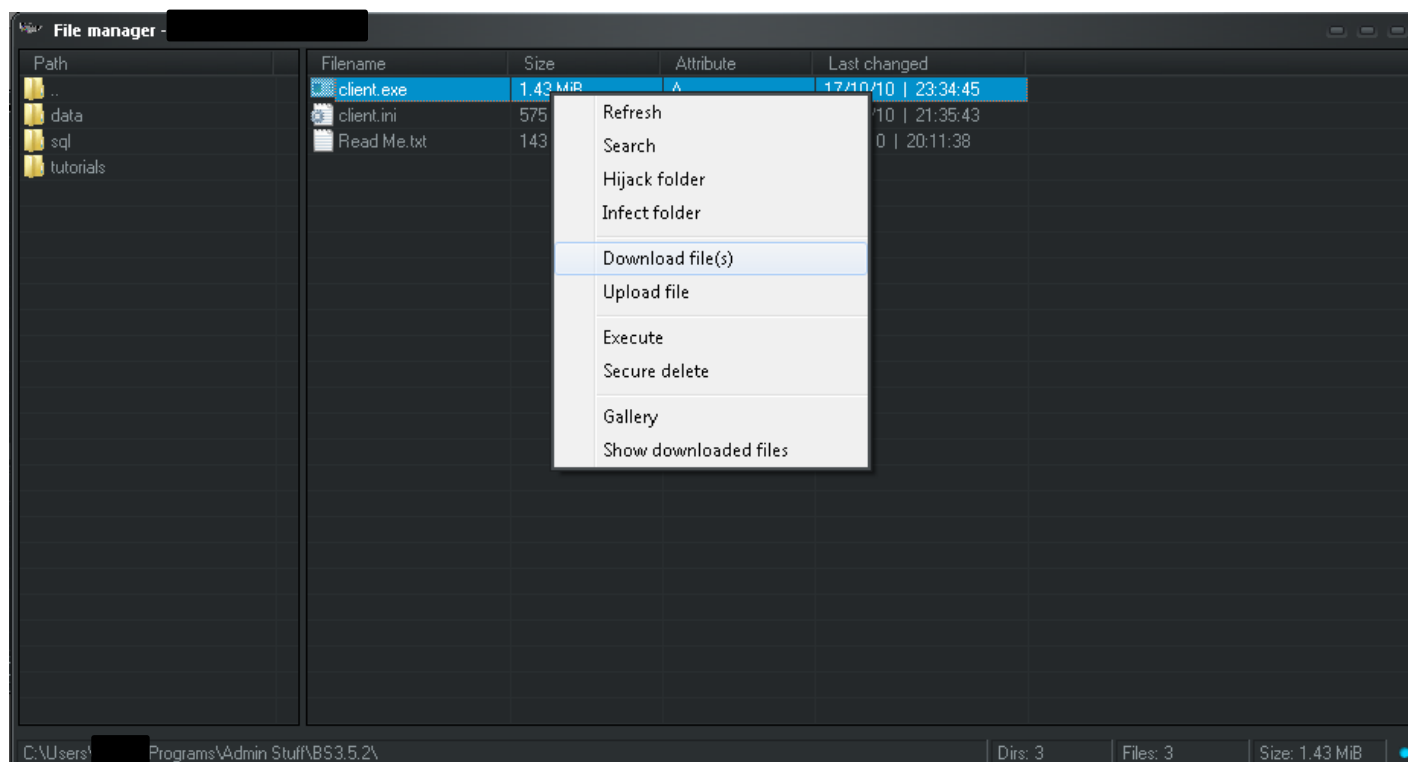


To browse the files on the user's computer, select files and then right click in the path column and select "update"

You can then browse through the user's files until you find something of interest. As you can see on the screenshot above, there are various functions in the file manager explained below.

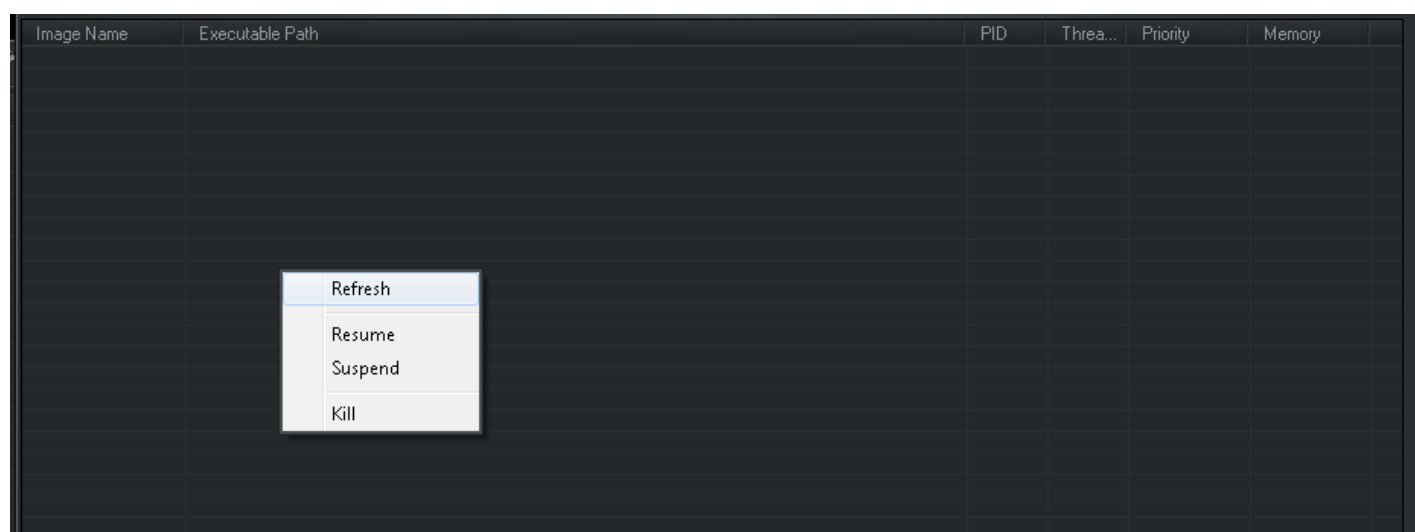
Option	What it Does
Refresh	Refreshes the folder , exactly like in windows
Search	Search the folder for specific files/file types
Hijack Folder	Use the Hijack function on the selected folder
Infect Folder	Use the Infect function on the selected folder
Download File	Download a file from their computer to yours
Upload File	Upload a file from your computer to theirs
Execute	Run/open the file on their computer
Secure Delete	Delete a file from their computer permanently.
Gallery	See a preview of the files
Show Downloaded Files	Will open the download directory for that machine on your computer so you can see which files you have downloaded.

In the following example I have navigated to my Blackshades 3.6.2 folder and am downloading the client.exe.



Processes

This is basically remote task manager, allowing you to start and stop their processes. As with all functions, right click in the window and select refresh.



This is the screen that you should see, the one in blue text is your RAT, Don't delete it.

Image Name	Executable Path	PID	Threads	Priority	Memory
AERTSr64.exe	C:\Program Files\Realtek\Audio\HDA\AERTSr64.exe	1456	4	Normal	2.7 MB
btwdins.exe	c:\Program Files\WIDCOMM\Bluetooth Software\btwdins.exe	1488	6	Normal	5.93 MB
svchost.exe	C:\Windows\system32\svchost.exe	1532	29	Normal	14.7 MB
McProxy.exe	C:\PROGRAM~2\COMMON~1\McAfee\McProxy\McProxy.exe	1644	18	Normal	6.47 MB
Mcshield.exe	C:\PROGRAM~1\McAfee\WIRUSS~1\mcshield.exe	1716	49	High	67 MB
MpfSrv.exe	C:\Program Files (x86)\McAfee\MPF\MPFSrv.exe	1912	16	Normal	5.27 MB
mksrver.exe	C:\Program Files (x86)\McAfee\MSK\MskServer.exe	2000	10	Normal	4.91 MB
SeaPort.exe	C:\Program Files (x86)\Microsoft\Search Enhancement Pack\SeaPort\SeaPort.exe	1672	9	Normal	8.22 MB
mcmcsvc.exe	C:\PROGRAM~2\McAfee\MSC\mcmcsvc.exe	2304	18	Normal	4.71 MB
svchost.exe	C:\Windows\system32\svchost.exe	2460	8	Normal	4.83 MB
svchost.exe	C:\Windows\system32\svchost.exe	2492	5	Normal	5.67 MB
dwm.exe	C:\Windows\system32\Dwm.exe	2600	5	High	25.9 MB
taskhost.exe	C:\Windows\system32\taskhost.exe	2300	9	Normal	7.18 MB
mcagent.exe	c:\PROGRAM~2\mcafee.com\agent\mcagent.exe	3060	6	Normal	1.77 MB
explorer.exe	C:\Windows\Explorer.EXE	2284	23	Normal	38.1 MB
iqs.exe	C:\Users\Sarah\AppData\Roaming\iqs.exe	3208	9	Normal	12 MB
rat.exe	C:\Users\Sarah\AppData\Roaming\rat.exe	3220	4	Normal	10.9 MB
Apoint.exe	C:\Program Files\DellITPad\Apoint.exe	3228	4	Normal	8.43 MB
RAVCpl64.exe	C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe	3236	11	Normal	10.5 MB
hkcmd.exe	C:\Windows\System32\hkcmd.exe	3252	3	Normal	9.81 MB
igfxpers.exe	C:\Windows\System32\igfxpers.exe	3320	3	Normal	8.47 MB
ApMsgFwd.exe	C:\Program Files\DellITPad\ApMsgFwd.exe	3328	2	Normal	5.41 MB
igfxsvc.exe	C:\Windows\system32\igfxsvc.exe	3384	4	Normal	6.18 MB
quickset.exe	C:\Program Files\Dell\QuickSet\quickset.exe	3408	5	Normal	9.31 MB
WLTRAY.EXE	C:\Program Files\Dell\Wireless WLAN Card\WLTRAY.EXE	3448	15	Normal	30.6 MB
WmiPrvSE.exe	C:\Windows\system32\wbem\wmiPrvse.exe	3456	6	Normal	6.9 MB
msnmsgr.exe	C:\Program Files (x86)\Windows Live\Messenger\msnmsgr.exe	3752	46	Normal	79.9 MB
ApntEx.exe	C:\Program Files\DellITPad\Apntex.exe	3936	4	Normal	5.25 MB
conhost.exe	C:\Windows\system32\conhost.exe	3952	2	Normal	4.62 MB
hidfind.exe	C:\Program Files\DellITPad\HidFind.exe	3980	1	Normal	4.42 MB

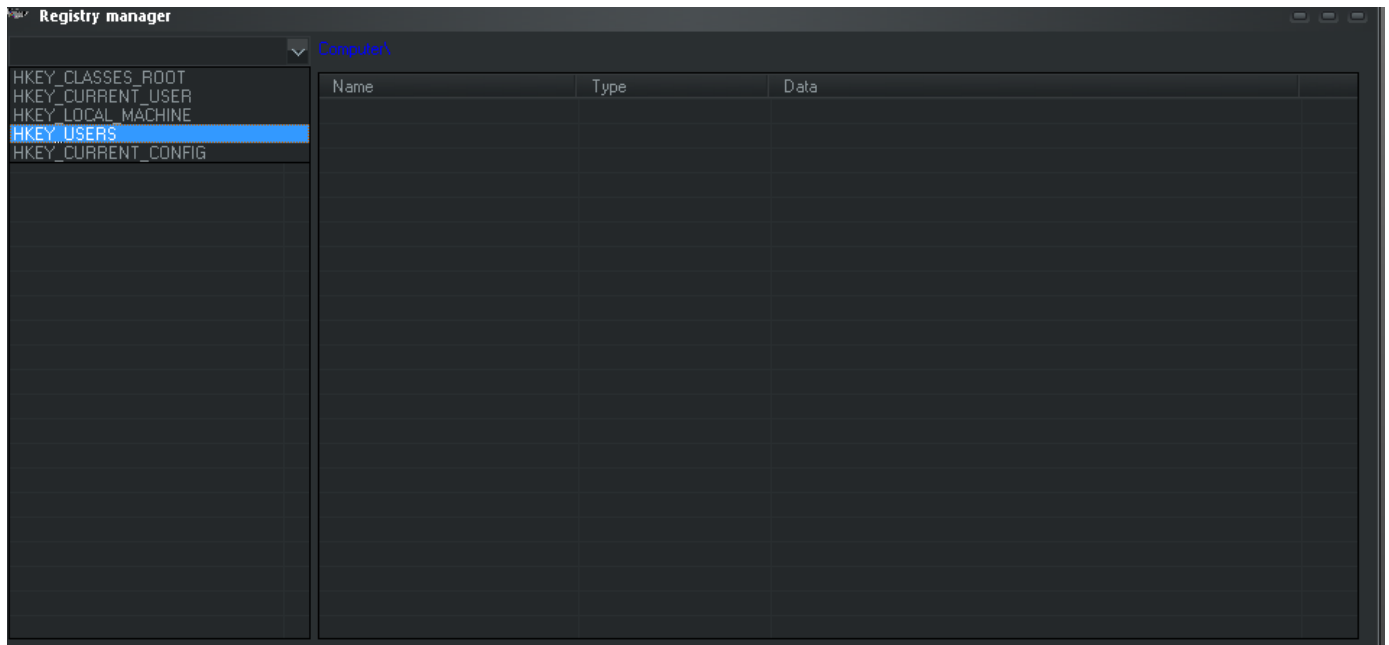
If you want to end a process say McAfee, which is the AV my bot is running. Simply select all the processes involved with McAfee then right click and select kill. To select processes that aren't next to each other use the shift key and click the processes.

Image Name	Executable Path	PID	Threads	Priority	Memory
btwdins.exe	c:\Program Files\WIDCOMM\Bluetooth Software\btwdins.exe	1488	6	Normal	5.93 MB
svchost.exe	C:\Windows\system32\svchost.exe	1532	27	Normal	14.8 MB
McProxy.exe	C:\PROGRAM~2\COMMON~1\McAfee\McProxy\McProxy.exe	1644	18	Normal	6.47 MB
Mcshield.exe	C:\PROGRAM~1\McAfee\WIRUSS~1\mcshield.exe	1716	49	High	66.9 MB
MpfSrv.exe	C:\Program Files (x86)\McAfee\MPF\MPFSrv.exe	1912	16	Normal	5.3 MB
mksrver.exe	C:\Program Files (x86)\McAfee\MSK\MskServer.exe	2000	10	Normal	4.91 MB
SeaPort.exe	C:\Program Files (x86)\Microsoft\Search Enhanc	1672	9	Normal	8.22 MB
mcmcsvc.exe	C:\PROGRAM~2\McAfee\MSC\mcmcsvc.exe	2304	20	Normal	5.14 MB
svchost.exe	C:\Windows\system32\svchost.exe	2460	8	Normal	4.83 MB
svchost.exe	C:\Windows\system32\svchost.exe	2492	5	Normal	5.67 MB
dwm.exe	C:\Windows\system32\Dwm.exe	2600	5	High	25.8 MB
taskhost.exe	C:\Windows\system32\taskhost.exe	2300	9	Normal	7.18 MB
mcagent.exe	c:\PROGRAM~2\mcafee.com\agent\mcagent.exe	3060	6	Normal	1.95 MB
explorer.exe	C:\Windows\Explorer.EXE	2284	23	Normal	38.3 MB
iqs.exe	C:\Users\Sarah\AppData\Roaming\iqs.exe	3208	7	Normal	11.9 MB
Apoint.exe	C:\Program Files\DellITPad\Apoint.exe	3228	4	Normal	8.43 MB
RAVCpl64.exe	C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe	3236	11	Normal	10.5 MB
hkcmd.exe	C:\Windows\System32\hkcmd.exe	3252	3	Normal	9.81 MB
igfxpers.exe	C:\Windows\System32\igfxpers.exe	3320	3	Normal	8.47 MB
ApMsgFwd.exe	C:\Program Files\DellITPad\ApMsgFwd.exe	3328	2	Normal	5.41 MB
igfxsvc.exe	C:\Windows\system32\igfxsvc.exe	3384	4	Normal	6.18 MB
quickset.exe	C:\Program Files\Dell\QuickSet\quickset.exe	3408	5	Normal	9.31 MB
WLTRAY.EXE	C:\Program Files\Dell\Wireless WLAN Card\WLTRAY.EXE	3448	15	Normal	30.6 MB
WmiPrvSE.exe	C:\Windows\system32\wbem\wmiPrvse.exe	3456	7	Normal	6.91 MB
msnmsgr.exe	C:\Program Files (x86)\Windows Live\Messenger\msnmsgr.exe	3752	46	Normal	79.9 MB
ApntEx.exe	C:\Program Files\DellITPad\Apntex.exe	3936	4	Normal	5.25 MB
conhost.exe	C:\Windows\system32\conhost.exe	3952	2	Normal	4.62 MB
hidfind.exe	C:\Program Files\DellITPad\HidFind.exe	3980	1	Normal	4.42 MB
BTTTray.exe	C:\Program Files\WIDCOMM\Bluetooth Software\BTTTray.exe	3028	10	Normal	14.1 MB
DellDock.exe	C:\Program Files\Dell\DellDock\DellDock.exe	3716	11	Normal	14.4 MB

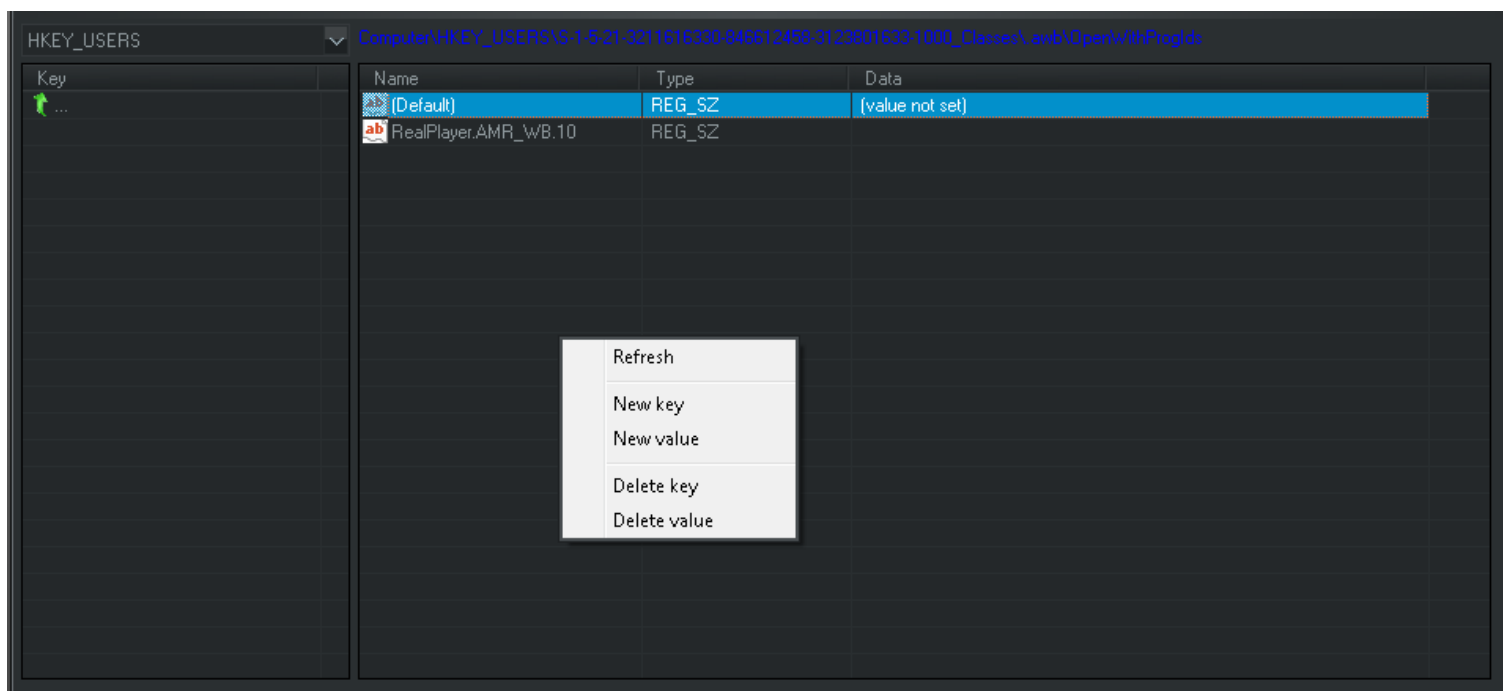
Then just select refresh to see the new list of programs, the ones you killed should have gone.

Registry

As with the process manager, registry manager works in much the same way as regedit.exe. To start off just select which HKEY you want to browse and select it. It should then automatically load up all the folders in that class



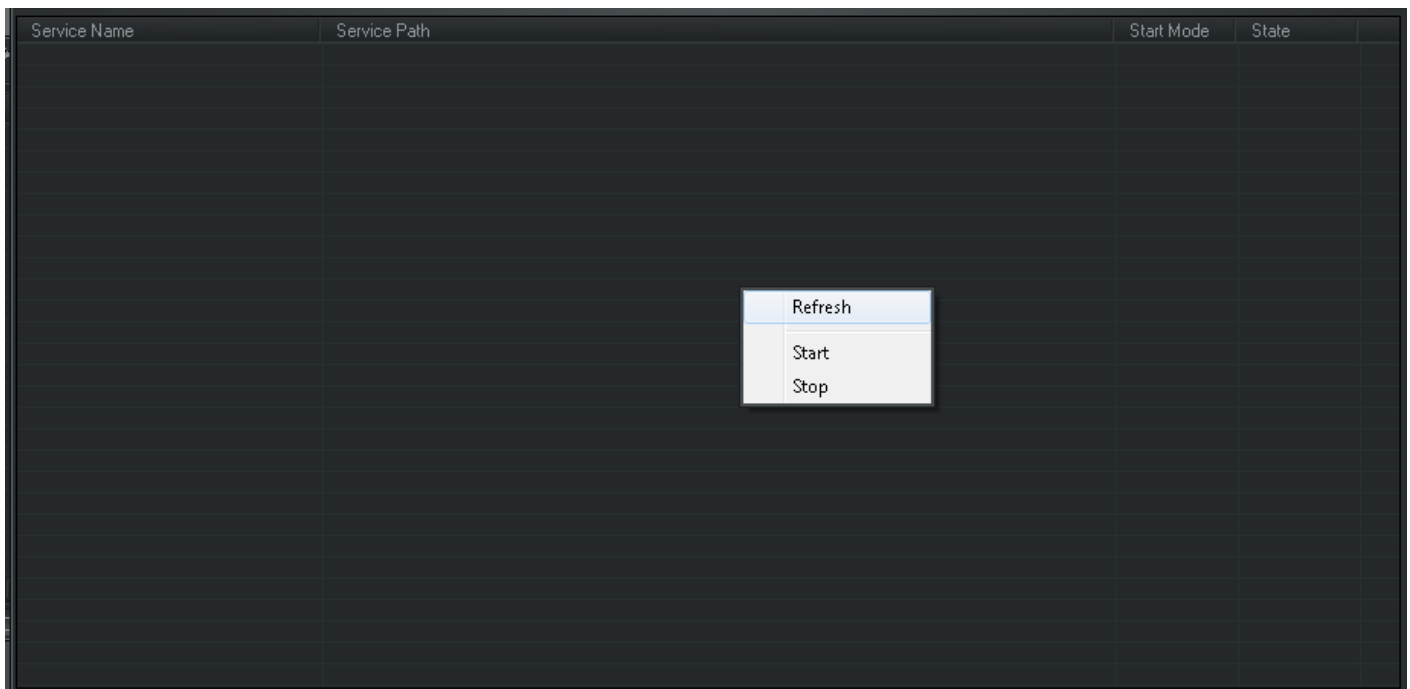
Then just browse to the folder that you want to edit the registry entries for and right click in the main box.



As with the DDoSer, I'm not going to explain what it the registry does, that would take too long. Google it. When you've made any changes, just right click again and select refresh to see them.

Services

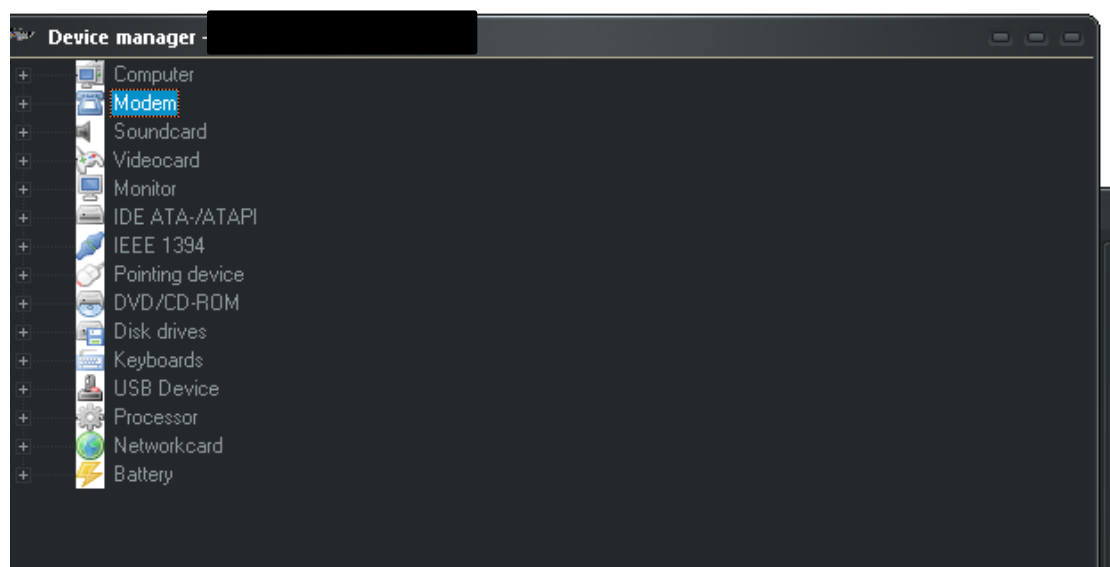
The services feature allows you to start and stop windows services e.g. Windows firewall. To access the list of services on the computer just right click and select refresh.



Then just select the processes you want to start or stop (using the shift key if they're not next to each other) and right click and select start or stop.

Devices

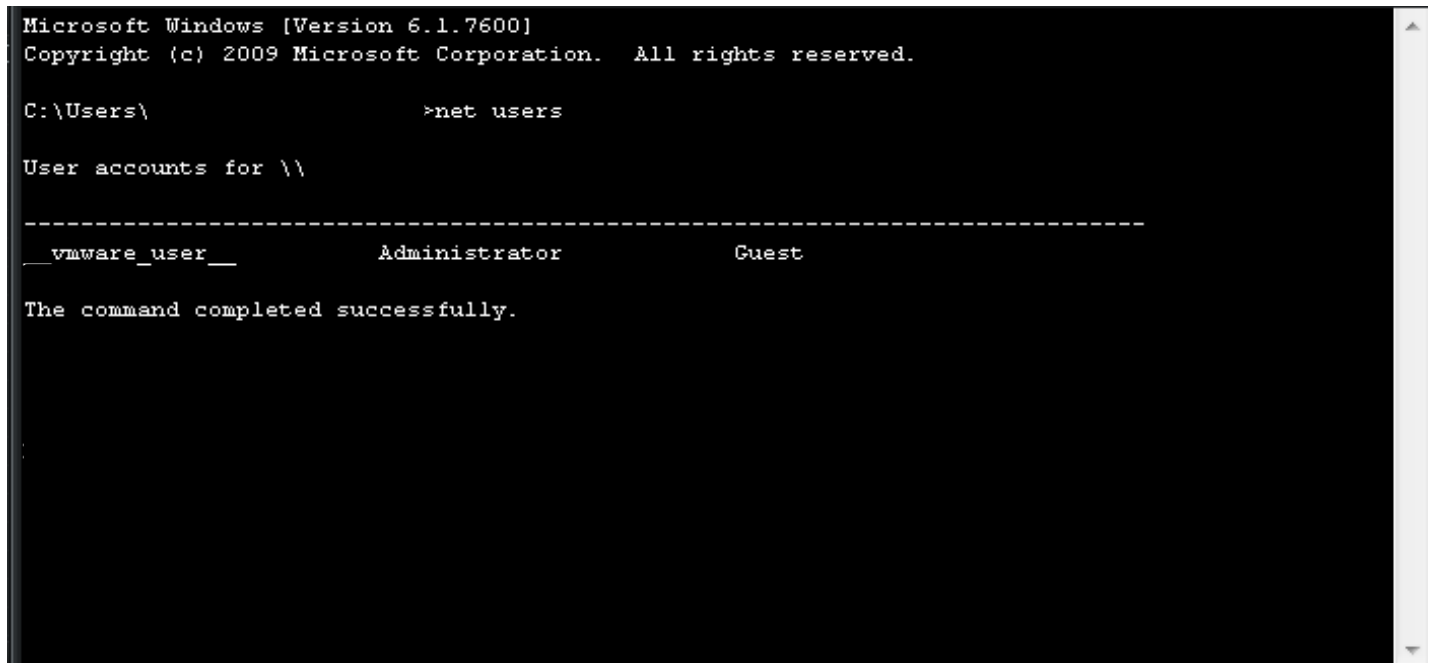
You may at some point, want to know more information about your bot's computer. For this you use the device manager. At the moment, there's not a lot that you can use this for apart from seeing what



software they use and exploiting it.

Shell

The shell works in exactly the same way as a windows command prompt and allows you to execute commands such as “net” without having to use screenshots, which would be blindingly obvious. Just open the screenshot and you’re ready to go.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

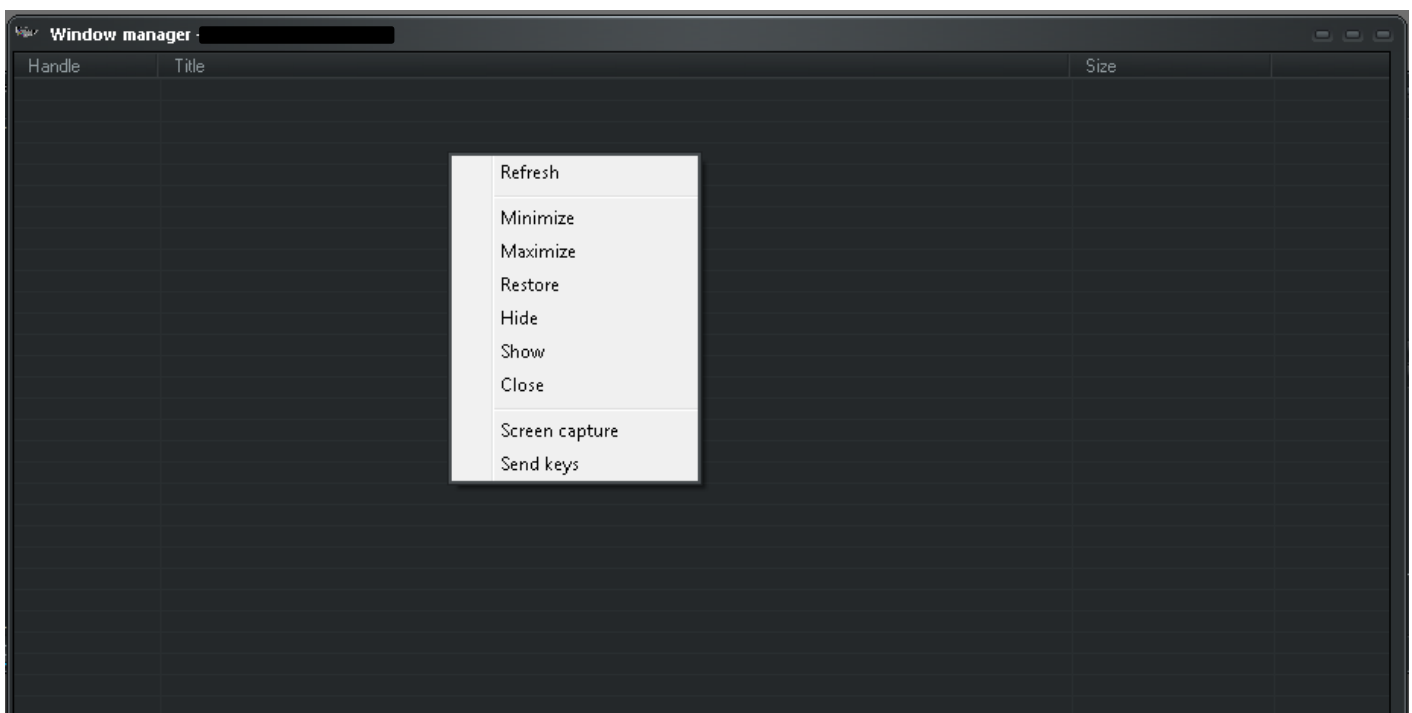
C:\Users\          >net users

User accounts for \\

-----
_ VMware_user_      Administrator      Guest
The command completed successfully.
```

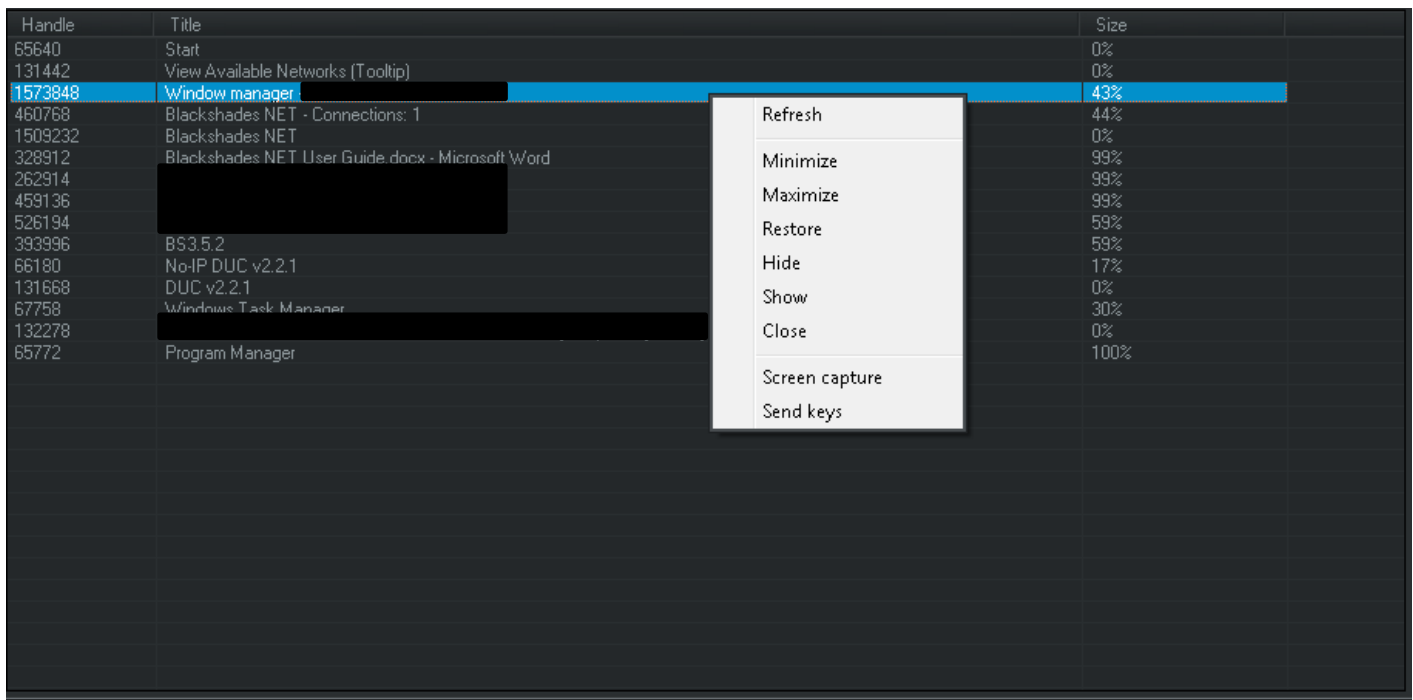
Window Manager

The Window Manager allows you to change the current window on a bot, maximise and minimise windows and to close programs without having to use the screen capture which can be slow/take up a lot of bandwidth. I’m not going to explain the commands because they’re so self explanatory. Have a play around if you’re not too sure. The Window manager can, however, only be used on V3.6 Bots.



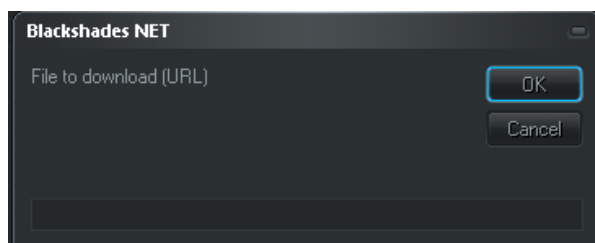
Windows

The Windows function allows you to control a bot's open windows as if you were at their computer without having to use the screen capture.



Option	What it does
Minimise/maximise	Same as in windows, make the window larger/smaller
Restore	Make the window size smaller/bigger
Hide	Hide a window from the taskbar
Show	Show a hidden window on the taskbar
Close	Close a window
Screen Capture	Start the Screenshot Manager (See Surveillance)
Send Keys	Allows you to send messages to your chosen window

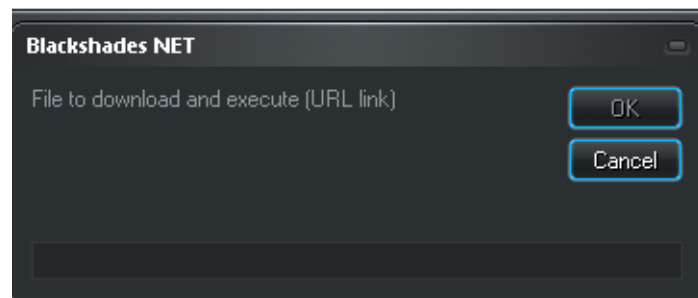
Download



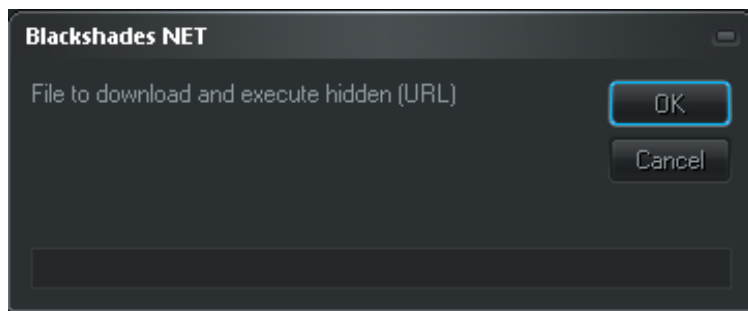
Use the download function when you wish to download a file to one of your bots, but not execute it. Just upload your file to a site where you can get a direct download link e.g. fileave.com NOT mediafire, megaupload etc. Then just enter it into the box and select Ok.

Download and Execute

Use the download and execute to install a virus/other hacking tool on your victims computer. Use the same method as with download, the only difference being the file will execute at the end.



Download and Execute Hidden



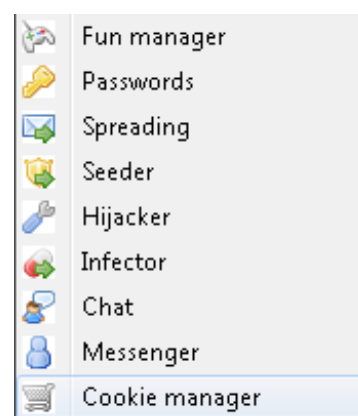
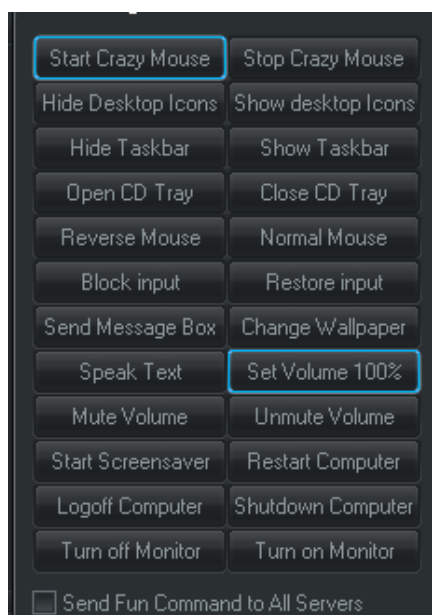
The download and Execute Hidden does just what it says on the tin, It will download a file to a bot, and execute it hidden i.e. there won't be a screen pop up etc.

Idle time and Uptime

These two commands don't open any windows, clicking them just updates the idle time and uptime values for your servers in the columns.

Misc.

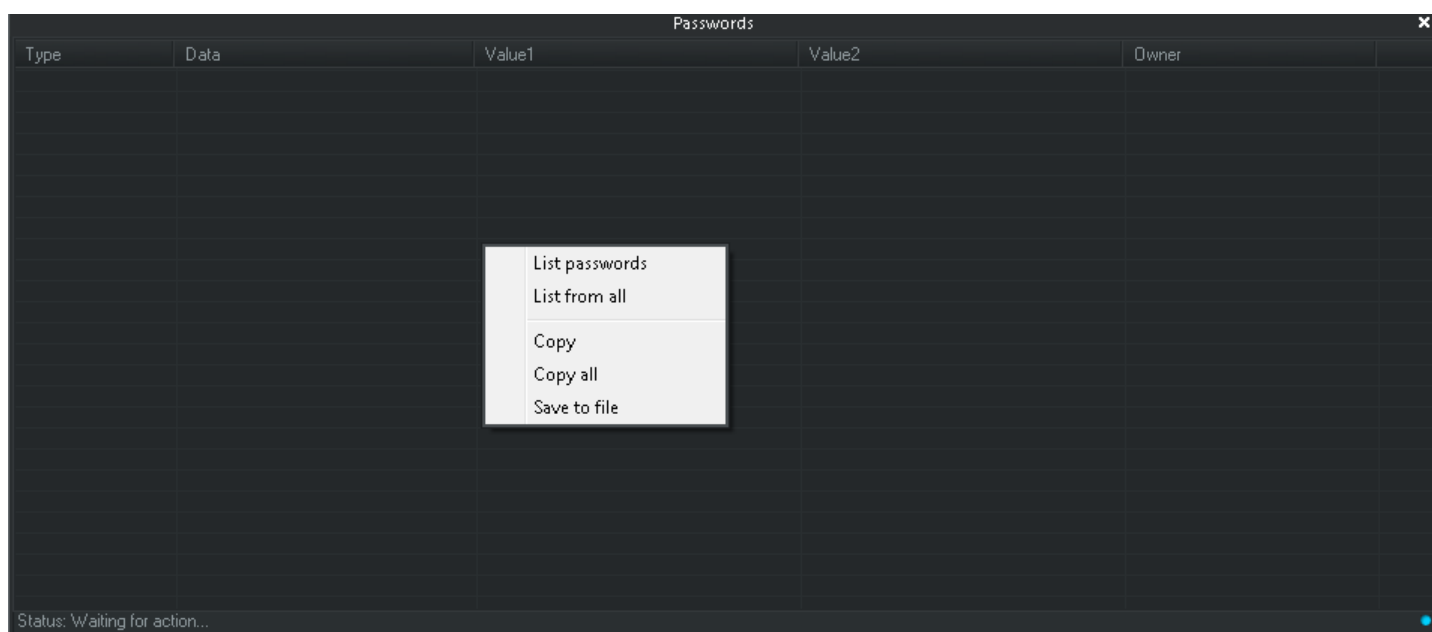
Fun Manager



Option	What it does
Start Crazy Mouse	Makes the mouse move around the screen so fast it's un useable
Hide Desktop Icons	Hides the desktop icons
Hide Taskbar	Hides the taskbar
Open CD Tray	Opens CD Tray (only opens on laptops can't close)
Reverse Mouse	Left click becomes right click.
Block Input	Stop them from controlling their computer
Send Message Box	Send your victim a message.
Change Wallpaper	Does what it says on the tin.
Speak Text	Type text and their computer will play it.
Set Volume 100%	Maximum Volume, useful if you want to use speak text so they hear it.
Mute Volume	Turn Volume to 0
Start Screensaver	...
Shutdown/restart/logoff	Same as windows functions
Turn off monitor	...

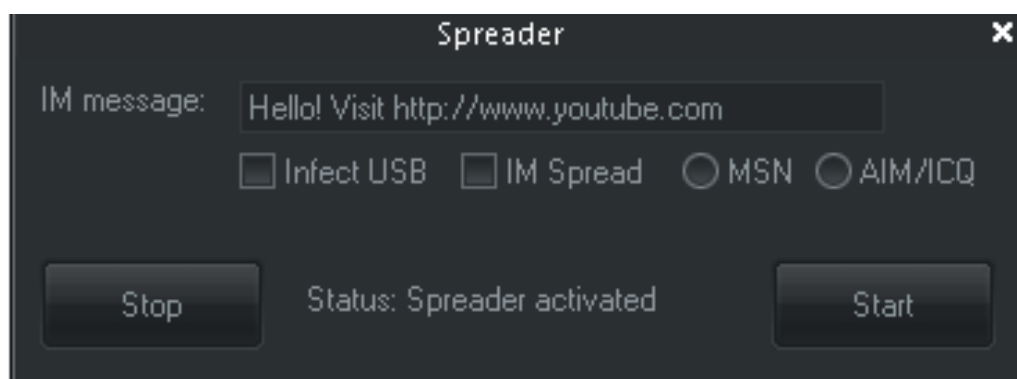
To revert these changes, just click the button to the right e.g. if you clicked "Start Crazy Mouse" click "Stop Crazy Mouse" to stop it. "..." means it's so simple it can't be explained in simpler terms.

I know this is self-explanatory, but I thought I'd include it just in case someone didn't understand.

Passwords

To get passwords and CD Keys from the server just open up the right click button and select the option you require.

Option	What it does
List Passwords	Lists all passwords from the server you right clicked on
List from All	Lists all passwords from all servers
Copy	Copies the one password/key you've selected
Copy All	Copies all passwords/keys
Save to File	Saves all the passwords and keys to a file (windows save window)

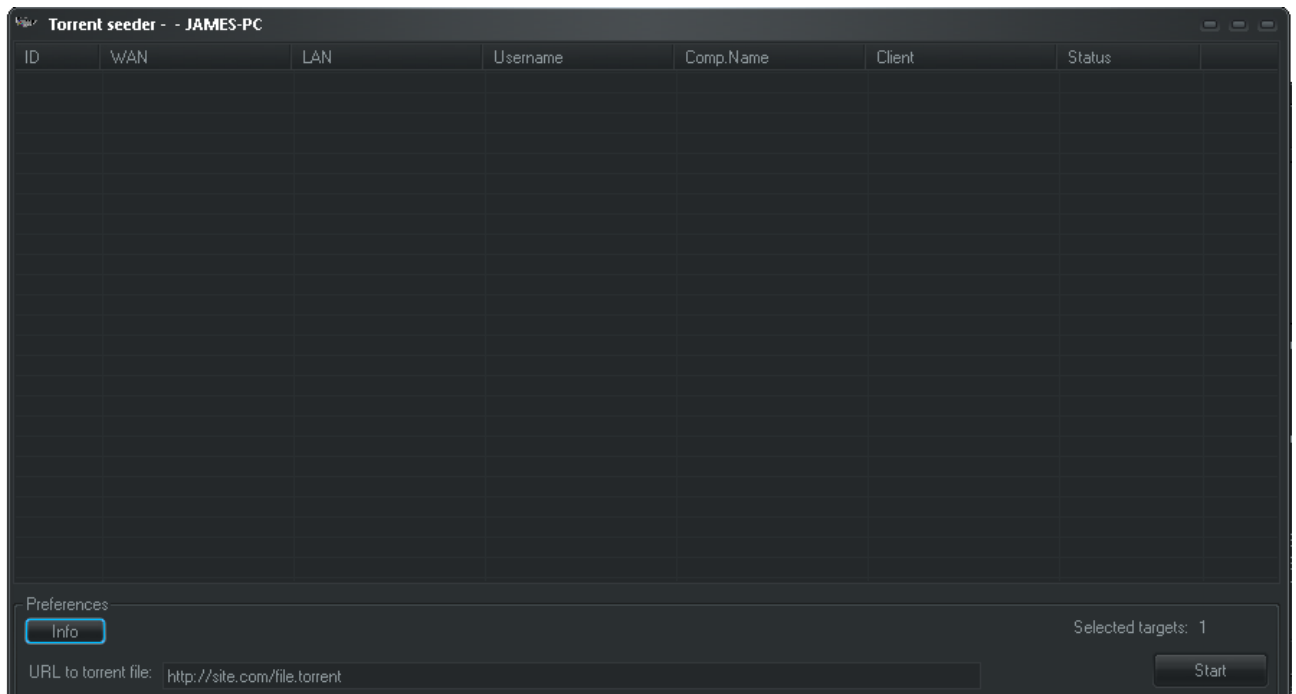
Spreading

Option	What to enter
IM Message	Link to download your server
Infect USB	Check if you want to spread using their USB
IM Spread	Check If you want to spread using IM then select Either MSN or AIM/ICQ

Enter whichever settings you want then click start.

Seeder

The seeder function forces all your bots to download a torrent from a given web address and then eventually seed it. This is good if you want to make you torrents look legit to prospective bots.



Make sure that you select all the bots you want to download your torrent first, and then select the seeder function or it will only operate on one machine. The seeder function only operates on: uTorrent, BitTorrent, Azerus/Vuze and LimeWire.

Hijacker

The hijacker can be used to encrypt the contents of someone's computer or certain file types so that they are inaccessible.

PLEASE NOTE, THIS IS FOR EDUCATION ONLY! DO NOT HOLD PEOPLES' COMPUTERS TO RANSOM AS THIS IS ILLEGAL AND YOU WILL PROBABLY GO TO JAIL. NEITHER MYSELF (SAKIMCM) NOR ANYONE ON THE BLACKSHADES TEAM (XVISCERAL, MARJINZ ETC.) ENDORSE ANY ILLEGAL ACTIVITY WHILST USING BLACKSHADES NET, IT IS ONLY TO BE USED ON COMPUTERS YOU HAVE PERMISSION TO USE IT ON.

File hijacker - 86.148.113.160 - JAMES-PC

Layout

Header: ☐ Blink Color: Red

Info: Warning! Please take your time to read the following text for your own best. Your computer has basically been hijacked, and your private files stored on your computer has now been encrypted, which means that they are impossible to access, and can only be decryped/restored by us. Color: Black

Instructions: Please settle X USD
IBAN: XX27 0040 0168 0000 0178 2101 XXXX
SWIFT: XX XX XXXXX XXXXXX
Account: IBAN505010100000225-1000
Name: Somename Somelastname
City: Somecity
Reference: Blackshades_key (WARNING: This must be included as a message or reference, otherwise your files will not be restored) Color: Black

Help Note: Read the help section if this is the first time! Background color: White Example

Settings

Encryption key: Blackshades_key Generate File extension(s): txt.doc.jpg (* = Any) Max file size: 3 KiB (0 = Any)

Display duration: 3600 sec Target path: Homepath Custom path: N/A

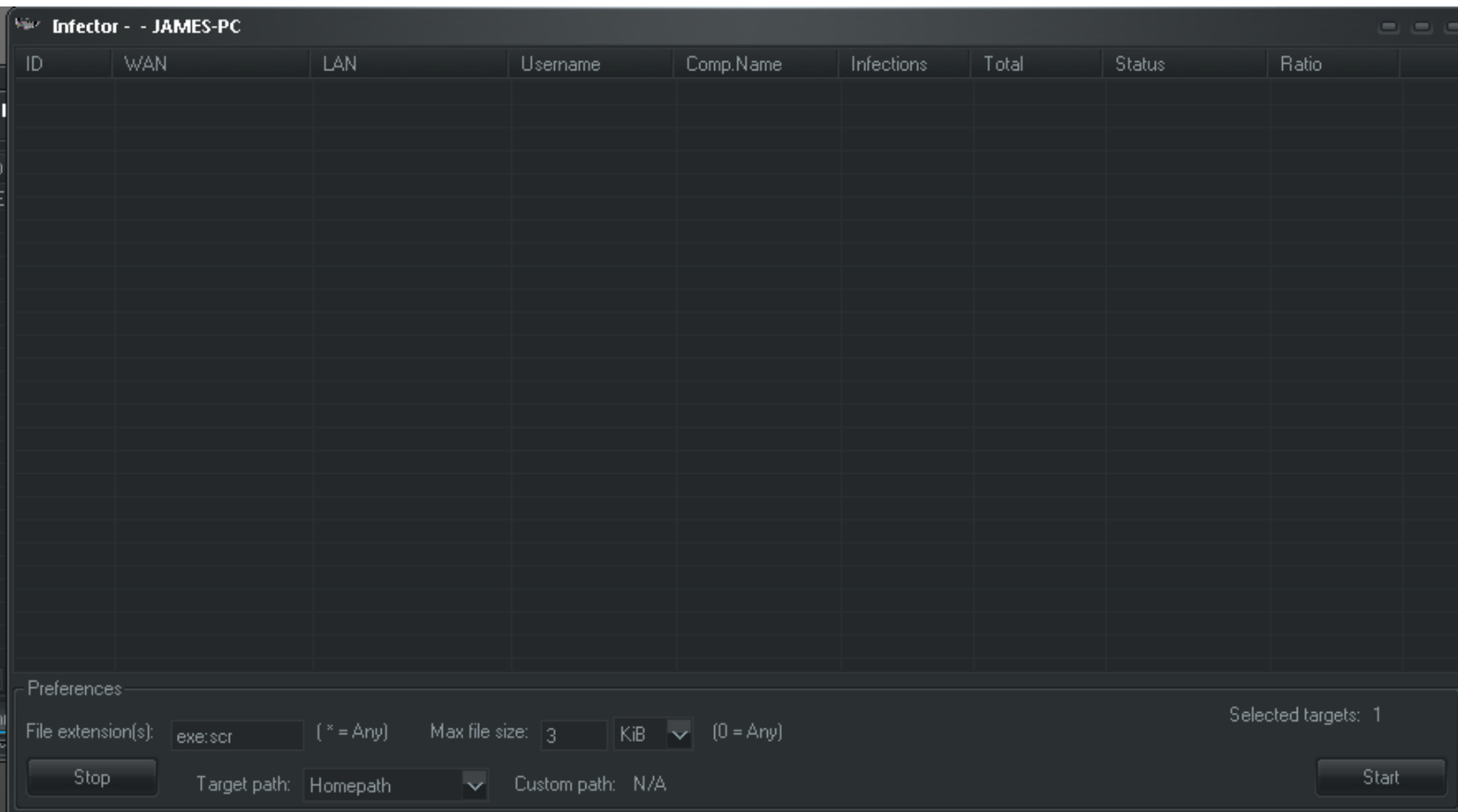
Test Selected targets: 1 ☐ I'm responsible for whatever this action results in Execute

Enter whatever you want in the first three boxes. The Blink function makes it flash.

Option	What to enter
Encryption Key	Either create an encryption key or press generate to create one
File Extension(s)	Select what files you want to encrypt *=all files
Max File Size	What is the biggest file it should encrypt, make sure to change it from 3 KB or you will look like an idiot.
Display Duration	How long should the screen stay up for (3600 Secs=1 hour)
Target Path	Where do you want to look for files (Root will encrypt all files)

Infector

The infector allows you to infect all the users' files with your bot, so that whenever they are run, they run your bot even on another computer.

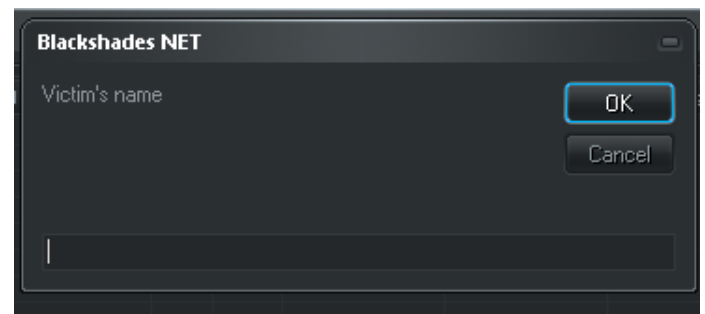
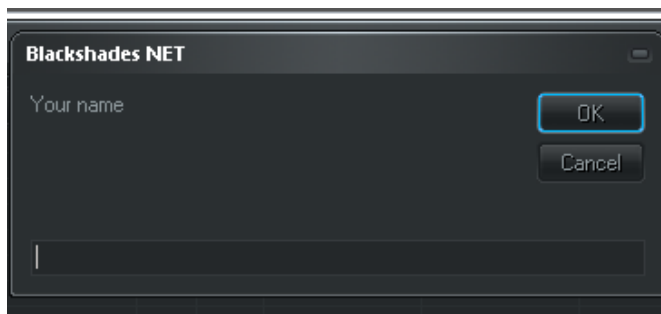


Option	What to enter
File extensions	Either just use program extensions, select a specific one or select all (*)
Max File Size	The largest file you want to infect (0 for all files)
Target Path	Where are the files going to be that you infect – select root to infect all programs.

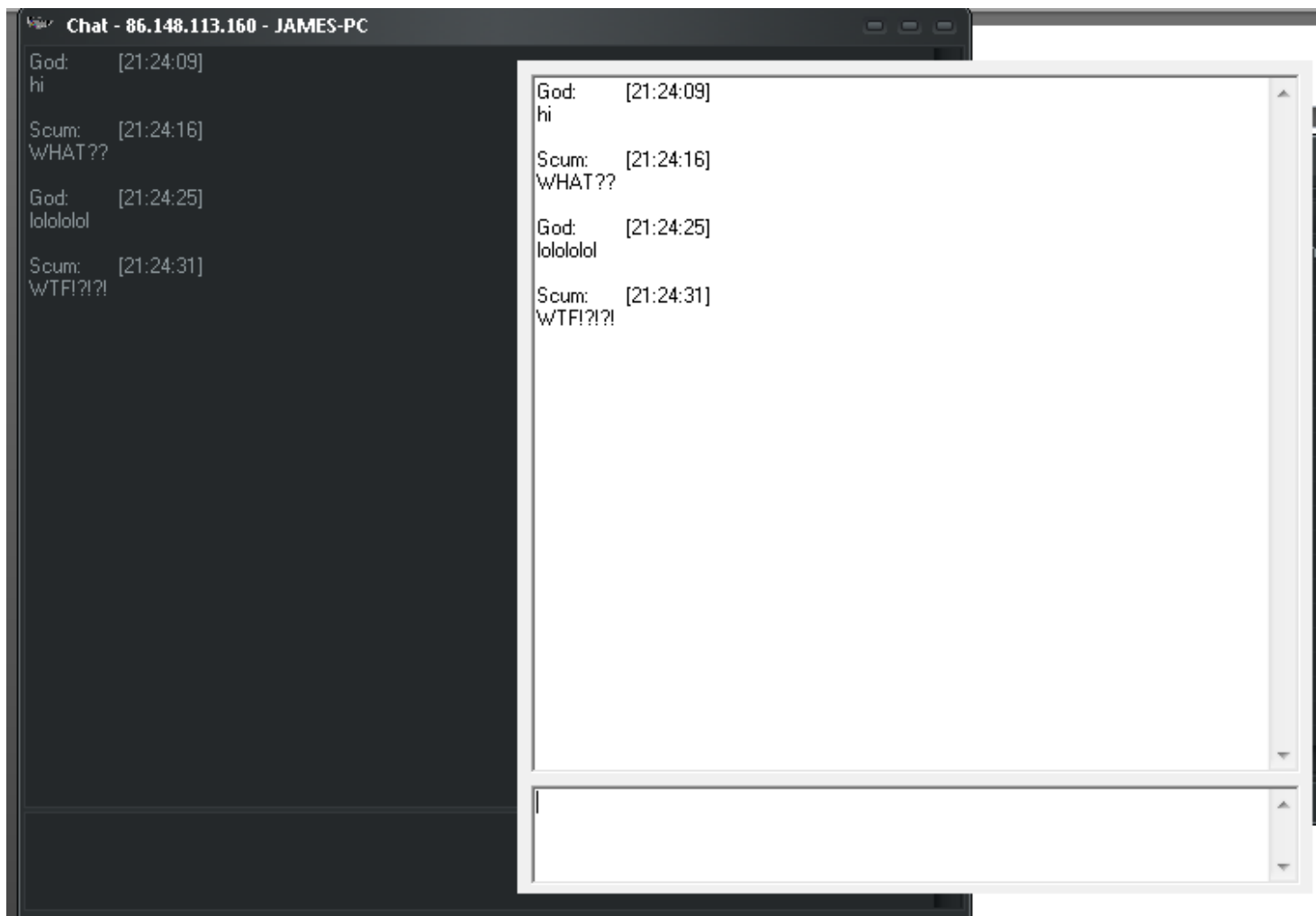
The infector basically allows you to infect some/all of a user's files with your server, that way, if they do manage to delete your server, as soon as they run a file; it will execute your server again. The options are exactly the same as with the hijacker.

Chat

The Chat feature allows you to communicate with your victims.

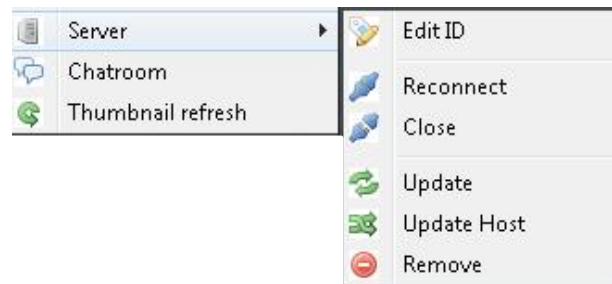


The first thing to do is to decide on what to call yourself and your victim. If you use your own name, you're an idiot.



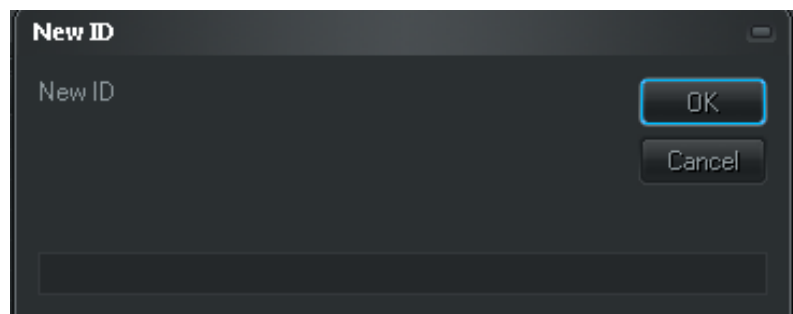
This is an example convo between me and... me. You type in the box at the bottom of the black convo box, your victim types at the bottom of the white convo box. The conversation only ends when you close the box or the victim shuts his/her computer down.

Server



Edit ID

The edit ID feature can be used to identify bots through spreading e.g. USB spreading to trace it to the host bot. Just enter the new name in the popup box.

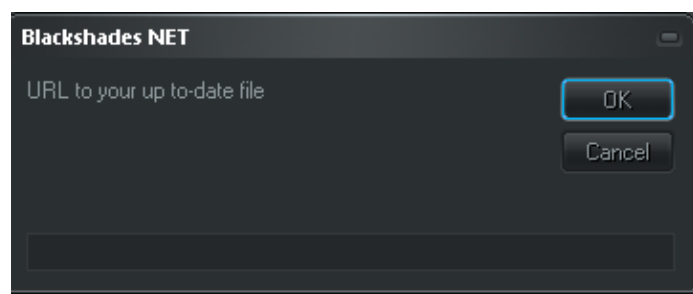


Reconnect and Close

The Reconnect function simulates the computer restarting; it stops the server and then starts it again, so it reconnects to you. The close function stops the server and doesn't restart it, so you will only reconnect to that bot when the computer restarts

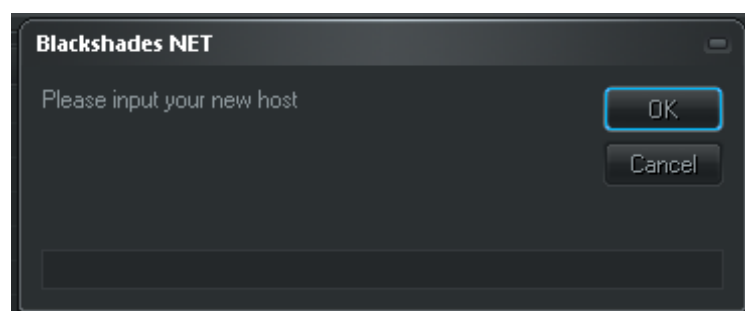
Update Server

When a new release of Blackshades NET comes out or your server is no longer FUD, and you want to update all your servers to the new version without losing all your bots, just make and crypt your server, upload it to a website that offers direct link downloading e.g. fileave.com and then enter the address for your new server into the update box.



Update Host

If you wish to change your DNS name or provider, simply sign up to a new one, enter your new Dynamic DNS in the box and it will update all bots that connect to the new DNS.



Remove Server

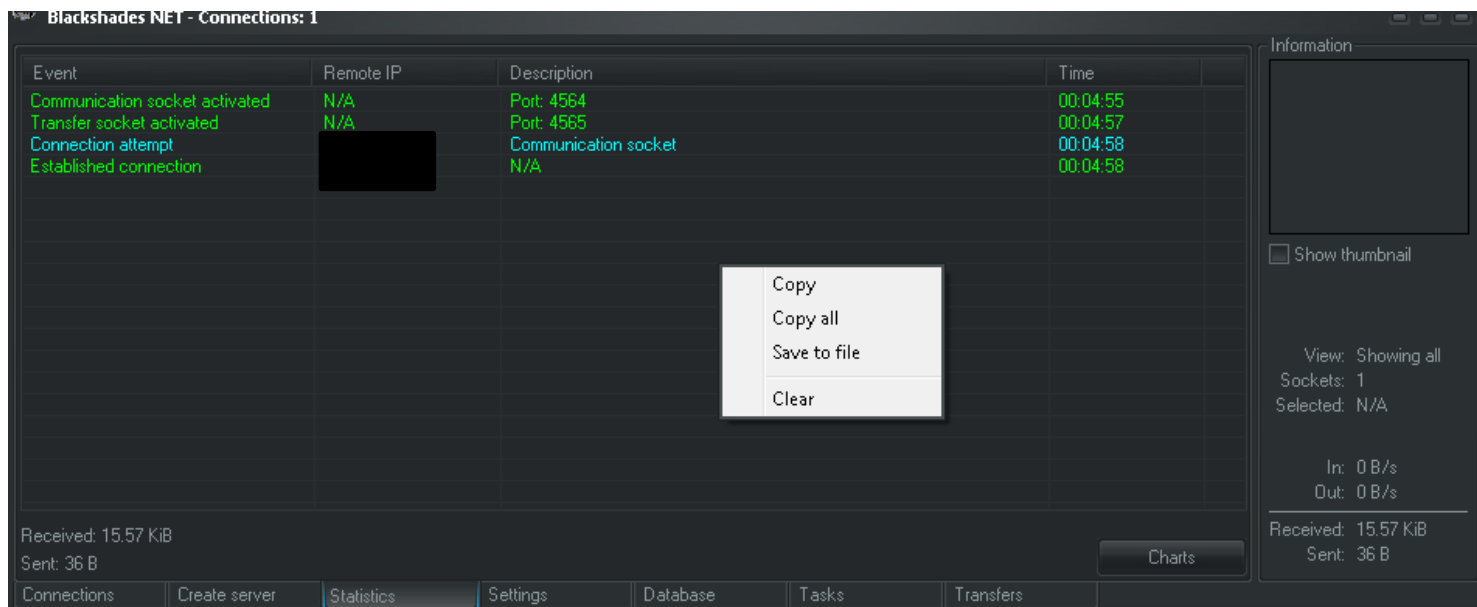
The terms of service for Blackshades NET say:

You agree that if you do by some sort of means connect to another computer, by means of accident or other ways, that you will use the uninstall feature to completely remove the connection between the two of you forever.

If you accidentally connect to a computer you don't have permission to connect to, then select that server and use the uninstall function, otherwise you could face jail time.

Statistics

The statistics window provides useful information on what connections your computer is making. You can also see charts showing the figures for various options.



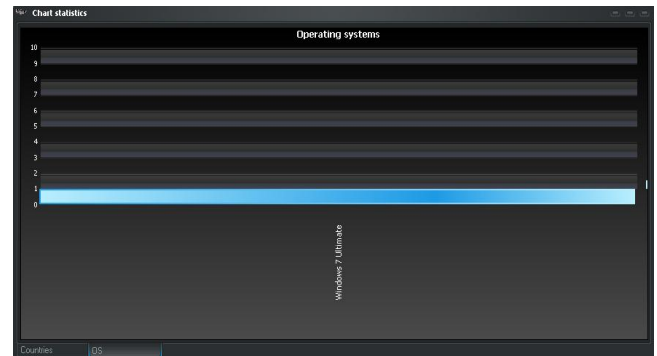
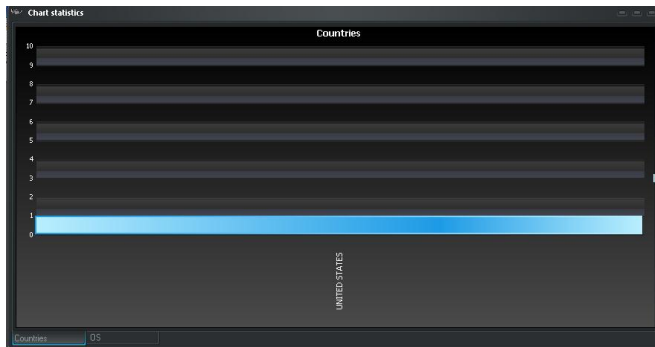
If you want to save the information about the connections you can do one of three things.

Option	What it does
Copy	Copy selected event
Copy all	Copy all events
Save to file	Save all events to file

If the list gets too crowded, just select clear and it will remove all entries.

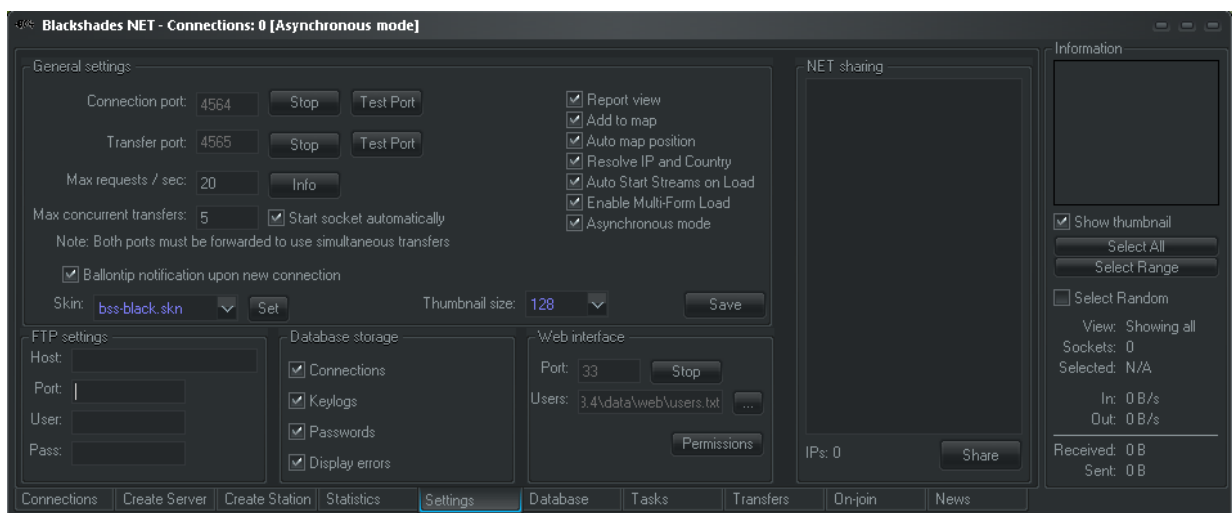
Charts

To access the charts, click the charts button in the bottom right of the statistics screen. You can then either view charts showing the number of bots from each country or running each OS. If no bars appear, right click and select refresh.



To toggle between charts, just use the tabs on the bottom left.

Settings



Option	What it Does
Connection Port	The port for incoming server connections (the one you used to build the server)
Transfer Port	The one used for webcams and to download Files. Make sure it's port forwarded
Max Reqs/Sec	How many requests can your computer make/sec e.g. how may keylog requests. Click the info button and use those specs to get the right number.
Max Concurrent Transfers	How many Transfers can your computer manage per second?
Report View	Check if you want to see the columns on the connections tab.
Add To Map	Adds bots immediately to the map
Auto Map Position	Automatically locate the bots position.
Resolve IP/Country	Identifies the bot's IP and country it is located in.
Asynchronous Mode	Allows you to connect to more bots as the bots don't fully connect, they just register that they are online and can be connected to.
Save	Saves your settings for future use
Skin	Changes what Blackshades NET looks like, make sure you press set
Database Settings	What do you want to upload to your database?
Net sharing	Share your bots with other BS NET users (just right click, add IP, enter their IP, click share), use remove to stop sharing bots.
Web Interface	Allows you to view and control your bots away from your computer

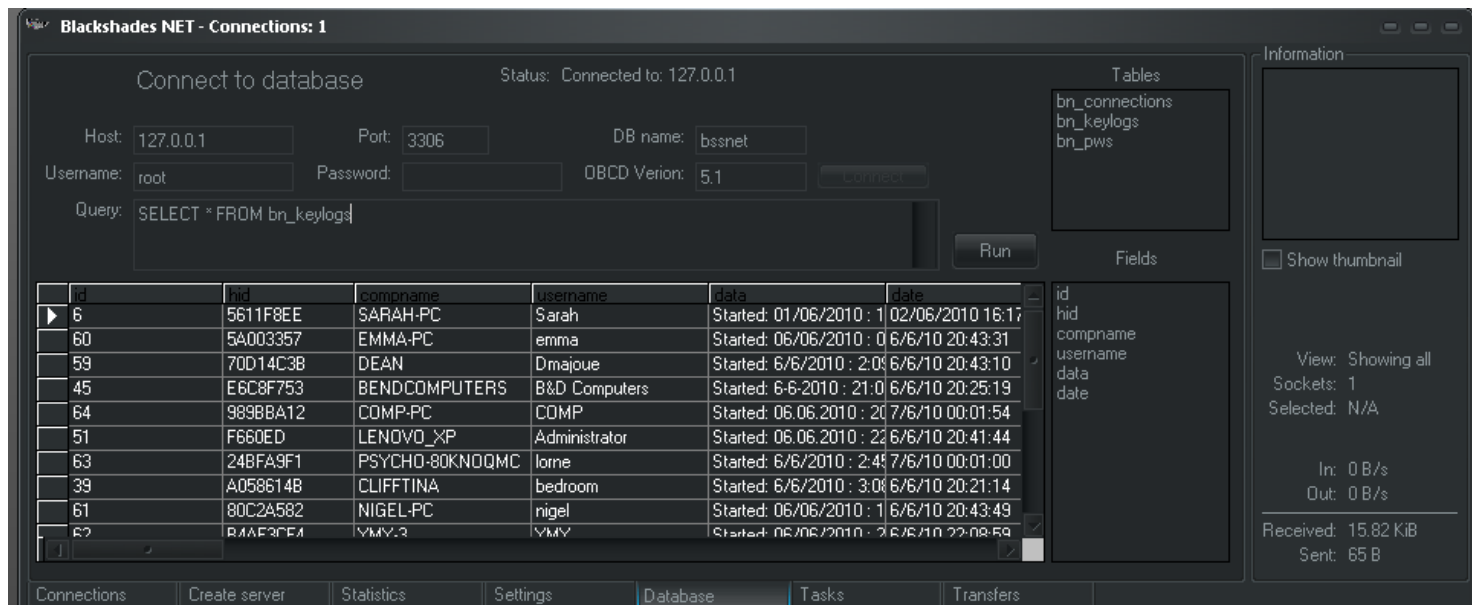
Database

Query

To use the query function simply decide which database you want to see then enter it in the form:

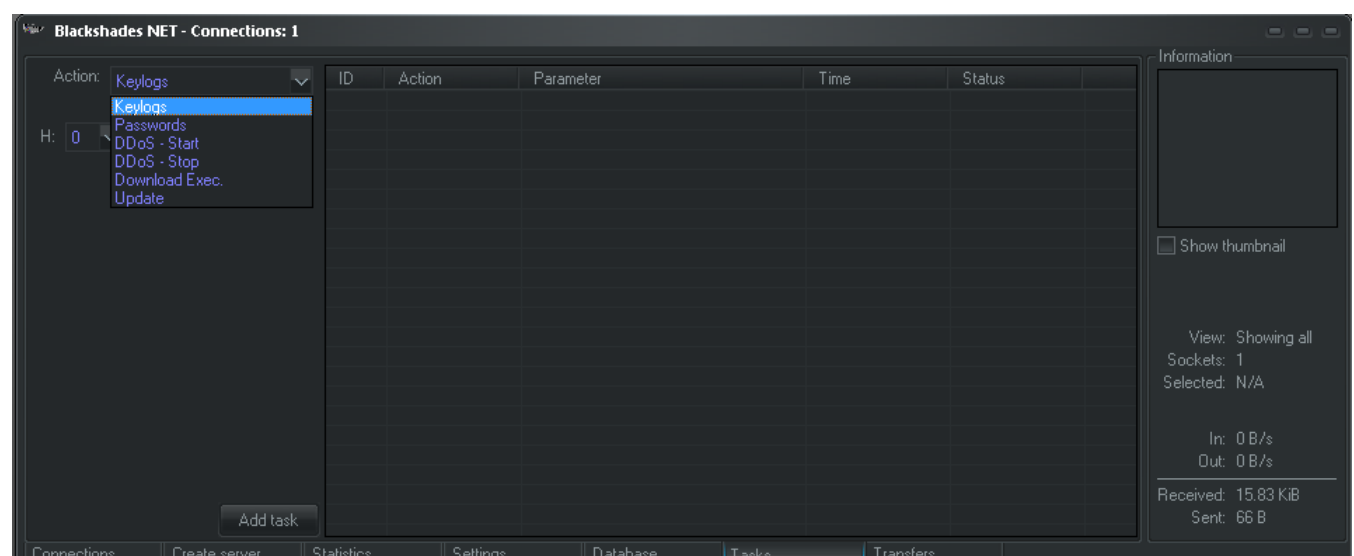
```
SELECT * FROM DB_NAME
```

Replacing DB_NAME with the database name e.g. bn_keylogs



This feature can be used to see if the database is updating correctly

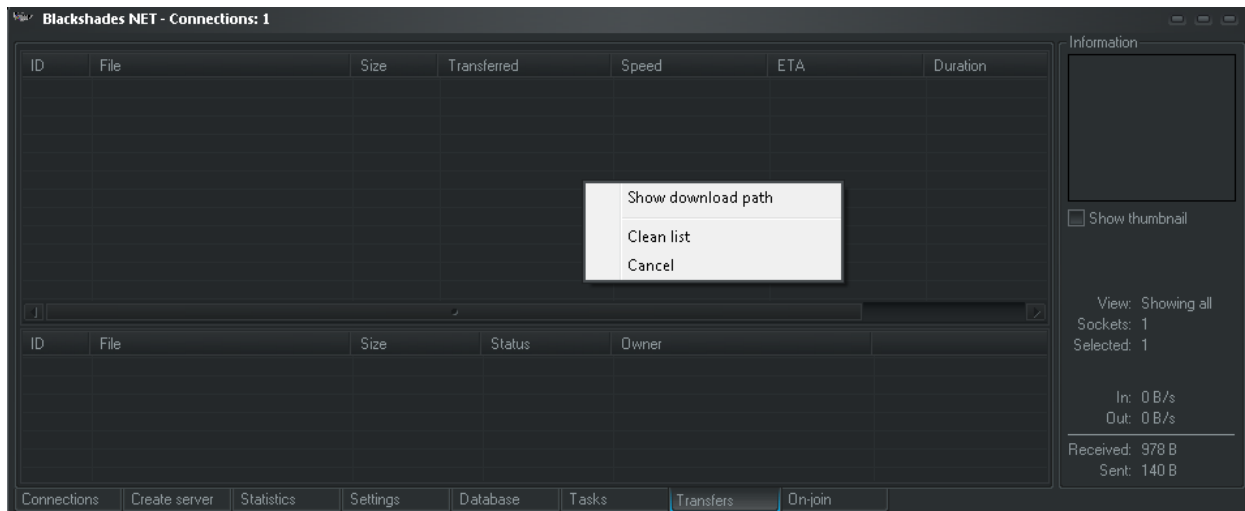
Tasks



If you want a task to occur frequently, e.g. getting keylogs, select it from the drop down list, then select at what time you want it to happen Hours: Minutes: Seconds and click add. So if you wanted to download all keylogs at 1:35 PM, you'd select keylogs, then enter: H: 13 M: 35 S: 00.

Transfers

The transfer window is split into two parts. The top part shows all the files you've downloaded or are downloading.



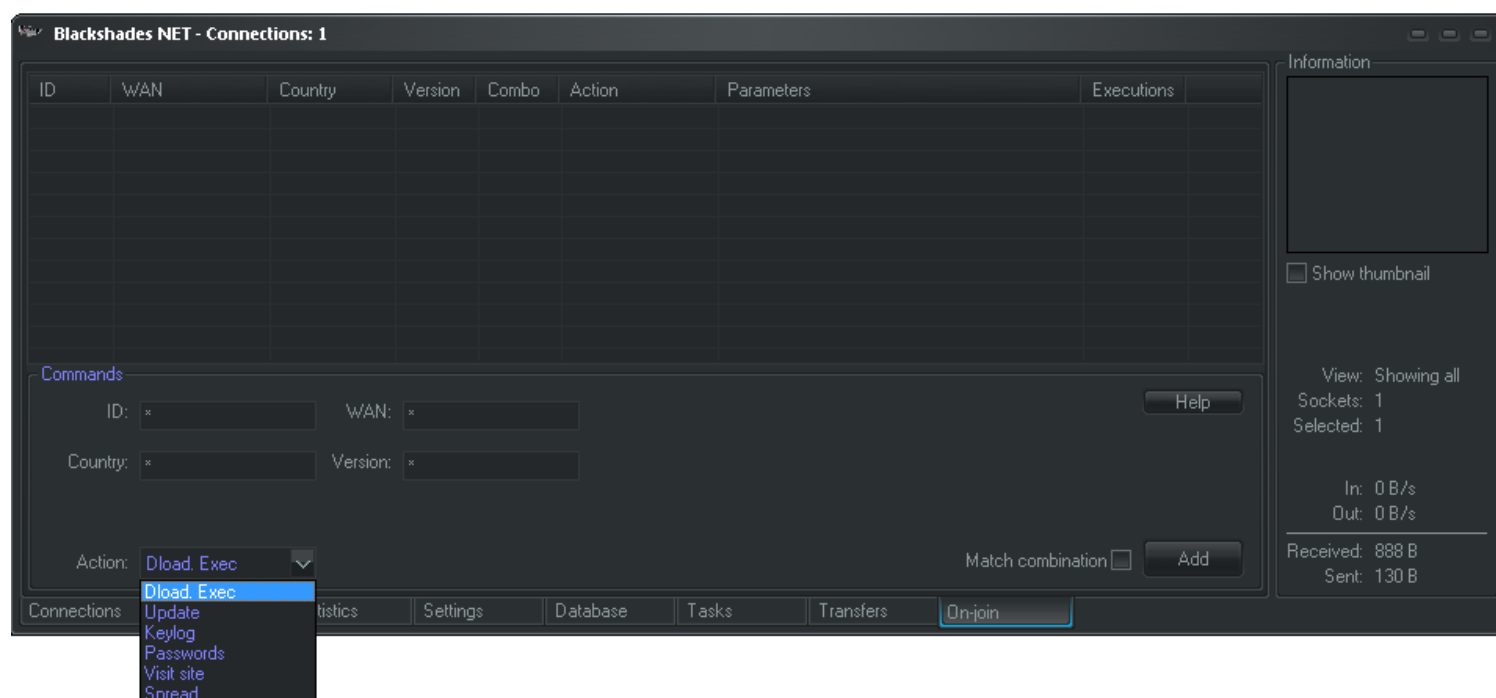
If you right click on the top, it gives you the option to cancel downloads, or clean the list, which will remove all entries, but the files will continue to download. To view the file's location just click "Show Downliad Path."

If you are downloading more files than you have open ports, files will queue in the bottom section and then move to the top when they are downloading. You can at this time remove them from the download list by right clicking on the file and selecting remove.

On-Join

Sometimes, you may not notice that some of your bots haven't been upgraded, or you haven't seen the keylogs in a while. The On-Join screen allows you to execute certain commands on bots when they are connected, without you having to lift a finger.

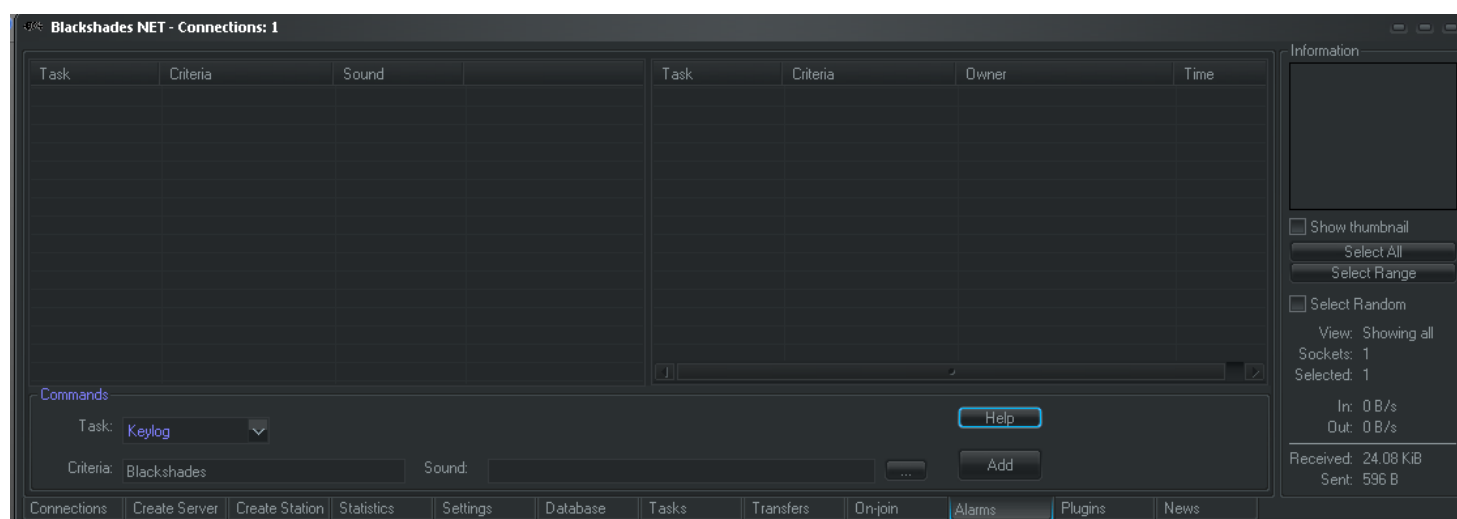
Option	What to enter
ID	The ID of the bots, e.g. all the bots you got from using omegle that have the ID "Omegle"
WAN	The first digits of the WAN e.g. 100 will target all bots with a WAN starting with 100
Country	The Country whose bots you wish to target
Version	The Version of Bot you wish to target, useful for upgrading
Action	What do you want it to do?



As with the Filter, Match combinations means that instead of being either Version 2.6 and with ID Omegle, it must have bot before the command is executed. Then just click Add. If you get stuck see if clicking help works.

Alarms

The alarms function is a clever add-on by xvisceral which means that if a window with a certain term in the title e.g. “PayPal” or “Facebook” is open, it will play a sound and log it. It can also monitor keylogs so if someone types a term in, it will again sound an alarm and log it.

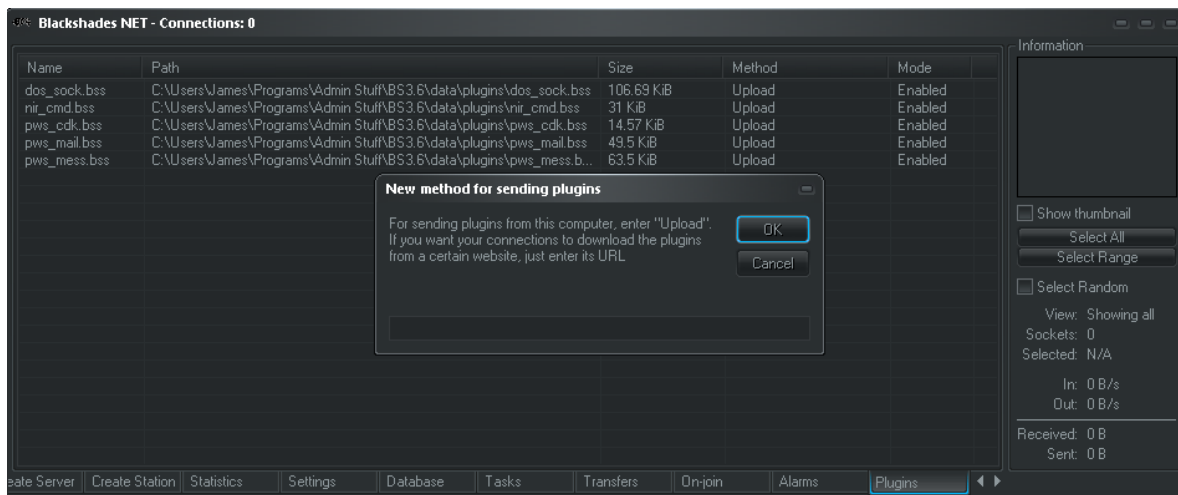


The Task can either be Keylog, where it will search the logs, or Windows Title, where it looks at open windows. Simply select which option you wish to monitor, enter your search criteria and select a sound file (must be in WMV format) and click add. Simple really. To remove the alarm, just right

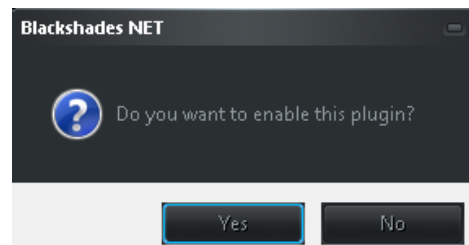
click on it and select remove. In the box on the left hand side, you will be able to see all incidences of the alarm.

Plugins

The Plugins feature allows you to choose what features are active in blackshades. The purpose of this is to make the size of the server smaller as it doesn't contain all the information in it. This does however mean that your bots all have to download the plugins from you later.



This can take up quite a lot of your bandwidth, especially if you have lots of bots. If this is the case, you can simply upload all your plugins to a direct download site, such as fileave, and then right click on each of the plugins in turn, select new method and then enter the download link. If you don't want to use a plugin, right click, select "New Mode" then No. If you later wish to use a plugin, select New Mode, then yes.

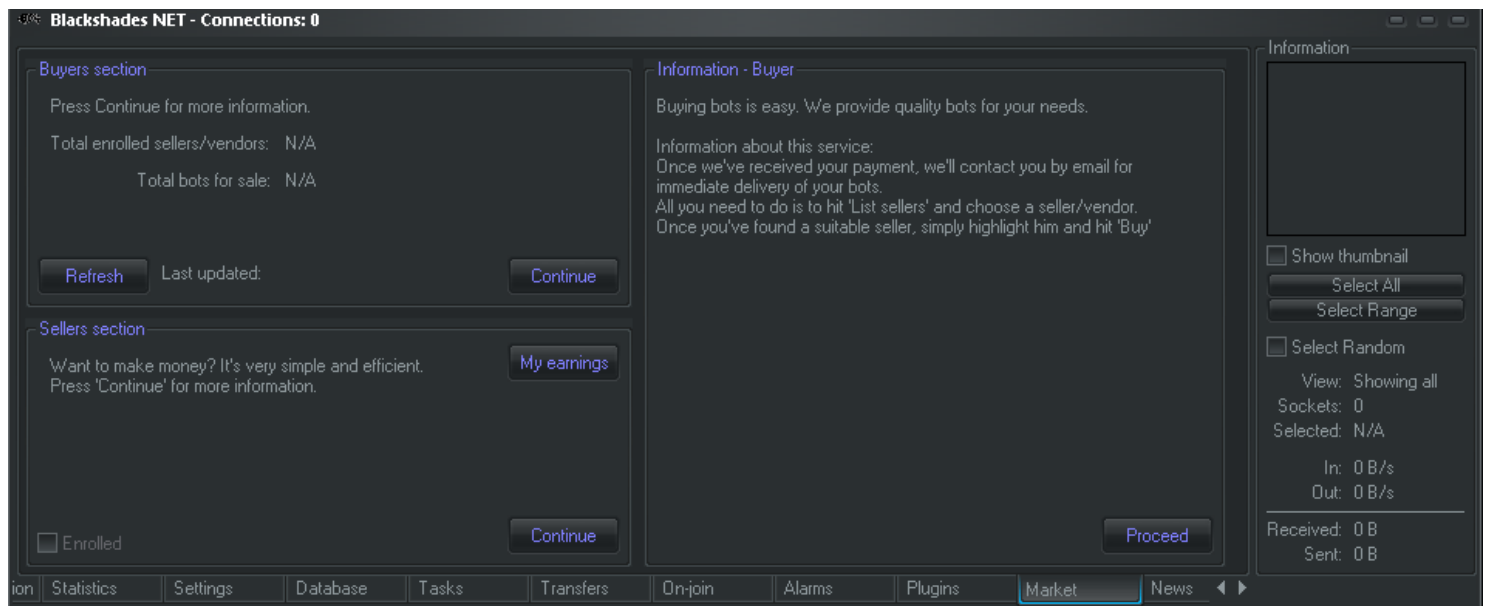


The Plugins have different functions so it's probably best you know what they are.

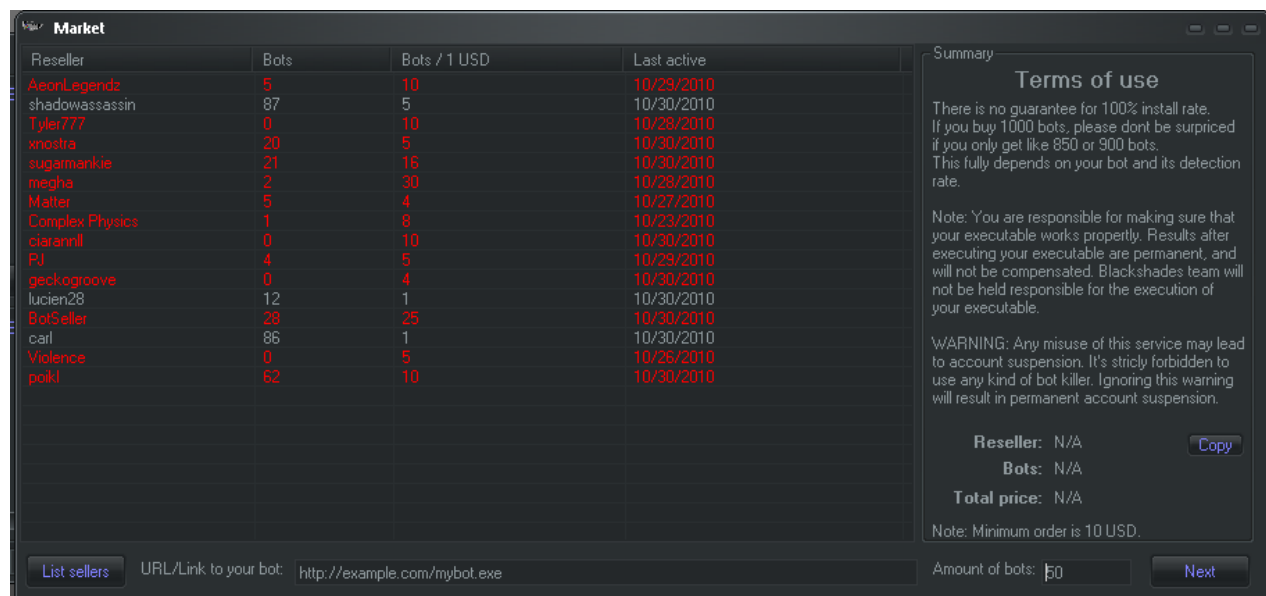
Plugin	What it does?
Nir_cmd.bss	Required to use fun commands
Dos_sock.bss	Used for DDOS
Pws_*.bss	Used in gathering passwords

Marketplace

The market place is a tab added to BSNET3.6, which allows users to buy and sell bots over the Blackshades NET system, whereby users list the number of bots they have for sale and the number of bots available for 1 USD. To purchase Bots, Simply select "Continue" in the buyers section and then click proceed.

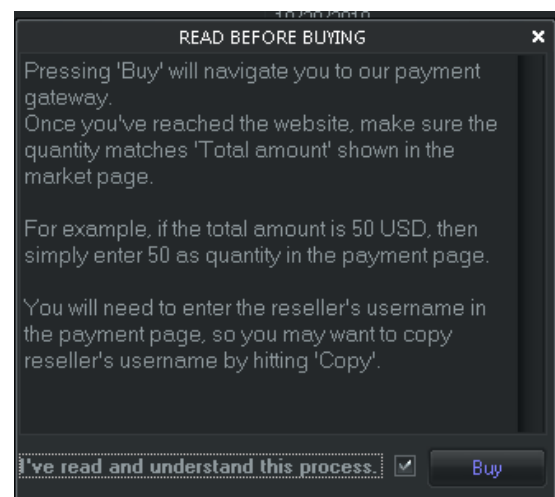


You will then see the Purchasing page. If you don't see any sellers, just click "list sellers."

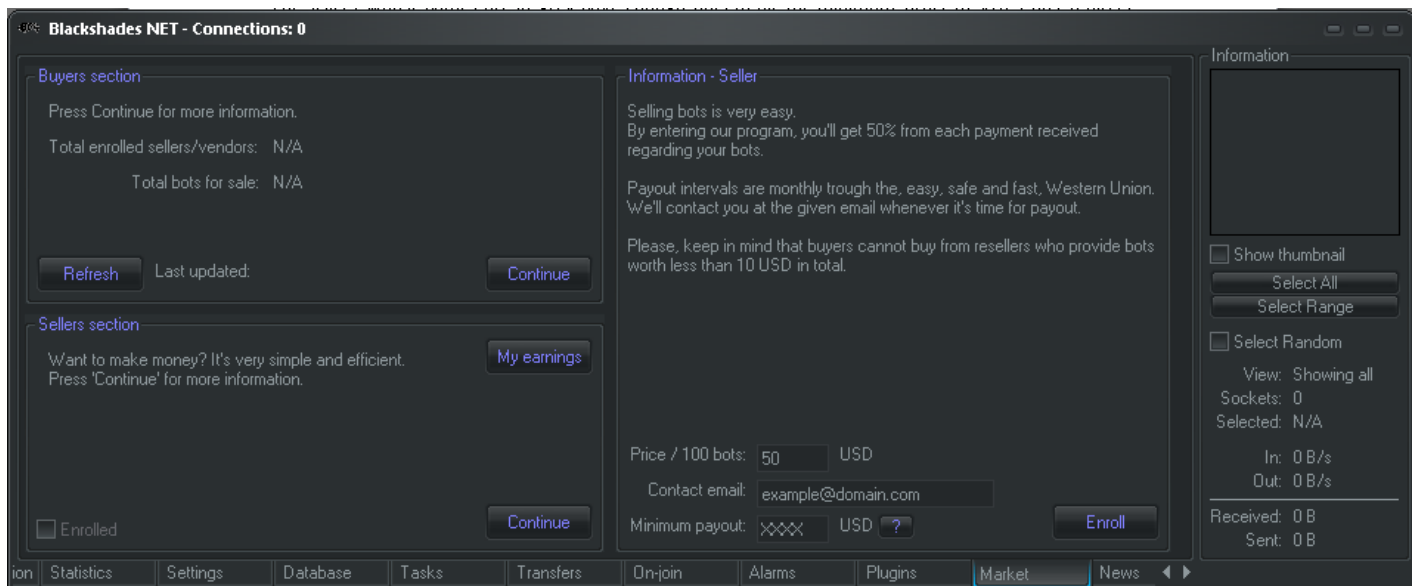


The sellers whose names are in grey have enough bots to fill the minimum order of \$10. Enter a direct download link in the "URL/Link to your bot" box e.g. fileave.com and the number of bots you wish to purchase in the "Amount of bots" box. Then click next.

You will then see this box. PAY ATTENTION TO IT!
The amount that you enter on the Plimus Payment site IS NOT the number of bots you have ordered, it's the total price e.g. I purchase 100 bots at 4 bots/dollar, the total price is 100/4=\$25. I enter 25 on the plimus site, NOT 100. It's not that hard. Make sure you enter your username (Blackshades Login) and your resellers username correctly or your order may not be processed.



To sell on blackshades is just as simple. Just click continue in the sellers section box and enter the details asked of you.



The Price/100 bots should be the number of bots per 1 USD so divide 1 by the price of one bot e.g. 0.5USD the number you enter is 2. The contact e-mail can be any e-mail address and the minimum payout is how much money you wish to have earned before you get paid. **DON'T FORGET, BLACKSHADES NET TAKES A 50% COMMISSION ON ALL ORDERS.** If you are selling 1000 bots at 0.04USD/bot, the maximum you will earn if all bots are sold is \$40 subtract the 50% Commission, you can only get \$20. This means that if you set your minimum payout at \$30, you won't be contacted regarding payment. Then click enroll. To see your earnings, click the "My Earnings" button and then select refresh. Simple!

I have not included a section on the station function here I may make one if I have the time to do so. Some of the larger sections have been brushed over in enough detail to get by on. More advanced and in depth tutorials have been written and are available on the Blackshades NET forum.

Hope this makes everything a lot clearer. If there is something I could have done better, tell me, or my tutorials won't get any better.

SakiMCM