BEAST 1.91

'Woe to you, oh Earth and Sea, for the Devil sends the Beast
with wrath, because he knows the time is short...
Let him who hath understanding reckon the number of the Beast
for it is a human number, its number is six hundred and sixty six.'

(Revelations ch. XII v. 12, ch. XIII v. 18)

- USER'S GUIDE -

CONTENTS:

1. INTRODUCTION

Beast 1.91 has been released on January, 19 2003.

Here is a short description of the program, the using instructions being on Chapter 2 (*Server Settings*) and Chapter 3 (*Client*). The using instructions are only for newbies and in case you are an advanced user just bypass them.

Beast is a powerful Remote Administration Tool (AKA trojan) built with Delphi 6. The client is 100% coded in Object Pascal, the server is coded 98% in Object Pascal (without objects!) and 2% in BASM.

One of the distinct features of the Beast is that is an all-in-one trojan (client, server and server editor are stored in the same application). The server can be extracted from the Beast and its size is only 55.5 k. Considering the multitude of tasks which can be performed by the server, this size is really surprising. The most size consuming function is the *Screen Manager* (with this you can view almost in real time the victim desktop) which represents more than 40% (~23 k) of the server size.

Other important features of the server are that the memory usage is very low (usually ~300 k) and the server stability is almost 100% (by example, the server can't be crashed by closing the client during a file transfer or any other operation).

The server is running in the *system* directory and writes few registry entries, so the victim must have the appropriate privileges on NT platform. If the victim is a restricted user then the server won't run on NT (2k, XP).

2. SERVER SETTINGS

Unlike other trojans, here is no server which can be edited. At least not a visible one. First of all you have to build the server from the Beast executable. When you run the Beast, on the main window you'll notice a *Build Server* button (see **here**). Just click this button and another window will appear. This is the window where you configure the server:
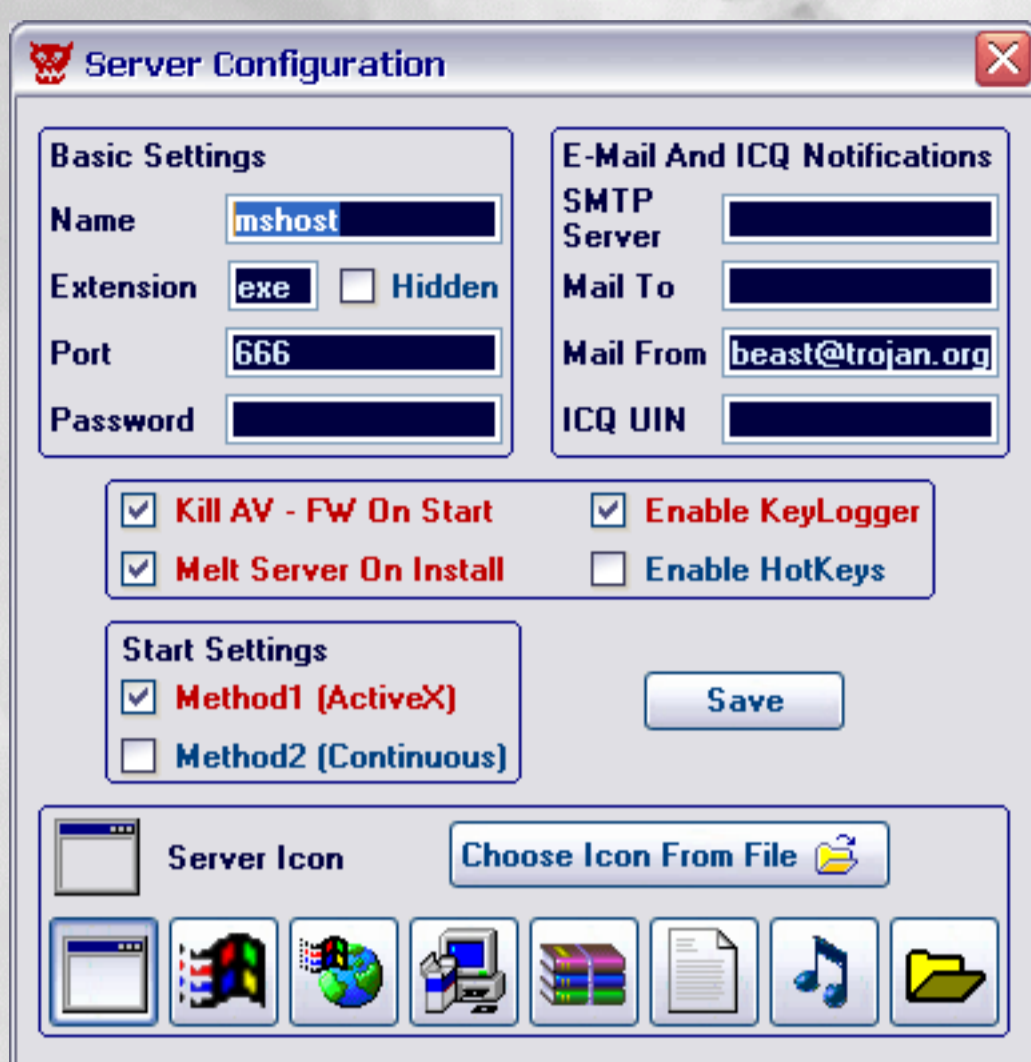
Let's discuss all the settings one by one.

On the *Basic Settings* group you can set the server name, port and password. The default settings mean that the server will run under the name *mshost*, will open the port *666* (at which will listen for connection requests) and for connection is not needed a password. All these default settings could be changed with your own. When you change the server name it is strongly recommended to not use a name which is in use (i.e. *svchost.exe*, *services.exe*, *lsass.exe* etc.) or could be a critical system process (*logonui.exe* etc.). Another option here is to set the server extension. The common extension for an executable is, of course, *.exe*, but for deceiving the victim you can set another extension. In case you want your server to have a different extension I'll suggest to set an unknown one, like abc, aaa etc. If you set a registered extension then could be an unpredictable or weird behavior of the system. By example, if you set the server extension to *.txt*, then the victim won't be able to open with doubleclick any *.txt* file (will receive an error message) and will become very suspicious. The extension of the server could also be hidden in *Explorer* by checking the *Hidden* checkbox.

On the E-Mail And ICQ Notifications group you can set the mode in which you prefer to be announced by the server about the victim IP. When you receive the victim IP you'll also receive the server listening port and the password for connection. If you want the E-Mail Notification you have to find a RELAY SMTP server, otherwise this doesn't work. In case you know a RELAY SMTP server, then you have to fill out the required data (SMTP Server and Mail To fields). The ICQ Notification works all the time and in case you don't have an ICQ UIN I suggest you to create an ICQ account.

Kill AV - FW On Start option is checked by default and this means that at every start the server will kill (close) over 300 FireWall and AntiVirus executables. The server terminates also the NT services, not only the normal applications.

Melt Server On Install option is checked by default. When building the server (after *the Save* button is clicked), its name will be *server.exe*. This name could be changed in whatever you want (but NOT the running name of the server) and if you doubleclick the server you'll notice that it'll disappear (will be *melted*). What's happened is that the server has copied itself in the *system* (usually *C:\Windows\System*) with the name you gave him and is running silently. After building, the server could also be bound with another executable and for this you have to use a binder (you have to find one which is undetected by AV). If you uncheck the *melting* option the server is only copying itself in the *system* (and also will run, of course).

Enable KeyLogger option is checked by default. All the pressed keys and opened windows are trapped and stored in an encrypted file (log). The keylogger is working all the time (offline & online) and from the client you can get the log and see all the victim activity at the computer.

Enable HotKeys option is unchecked by default. If you enable this option you can stop the server with CTRL-ALT-SHIFT-DOWN and kill (remove) it with CTRL-ALT-SHIFT-TAB (this could be useful when testing the server or your own computer).

On the *Start Settings* group you can set the server startup mode. If you choose the *continuous* method the server will be launched instantly when another executable is launched. If the victim closes (or even deletes) the server, after another application runs the server will be active again. This method has an side effect - the computer can't be restarted or shuted down from the start button. If you choose the *ActiveX* method, the server will be started at the windows boot. In this case, if the victim closes (and deletes) the server, at the next boot the server will be also active again.

The remaining thing that could be done is to change the server icon. There are few built-in icons or you can select another icon from specific files (exe, ico, dll). You can choose any icon, you are not restricted to a certain icon size or color depth, but the new icon will have 32x32 pixels and 16 colors.

Well, these are all the server settings which can be changed.

3. CLIENT

This is the client main window:

First of all you have to fill the *Host*, *Port* and *Password* fields and then click the *Connect* button (in the image above the button caption is *Disconnect* because was established a connection). The default values are *127.0.0.1* (*Host*) and *666* (*Port*). If the server is running on your own computer, then *127.0.0.1* is the address you need for connection. If you want to connect to a remote computer, then you have to put its IP in the *Host* field. The *Host*, *Port* and *Password* are received by ICQ or by E-mail. The *Port* and *Password* are those you set when you built the server (see Chapter 2, Server Settings). Now I assume that the connection with the server has been established and let me show you what can be done.

FILE MANAGER

File Manager option button is checked by default. You can do different things with the remote files and the buttons captions from this group are almost self-explanatory. First you have to click *Find Drives* and shortly after this you'll notice that the contents of the first fixed drive (usually C:) is listed in the left side of the main window (as seen in the image above). Now you can browse (doubleclick a folder or click *Show Files* button), delete files and directories, execute files (the file will be opened with the appropriate program), copy files (files are copied in the client current folder) etc. It is also possible to upload files on the remote machine. After you click on *Upload File* button a new window will appear. You can browse for a local file, set the remote file name and the remote folder for upload.

In case you want to search for files you have to click the *Search File* button. A new window shows up and now fill the file name for searching. The search is not case sensitive, can't be used wildcards and, an example, when you search *C=Mm* you'll find also the *command.com* file.
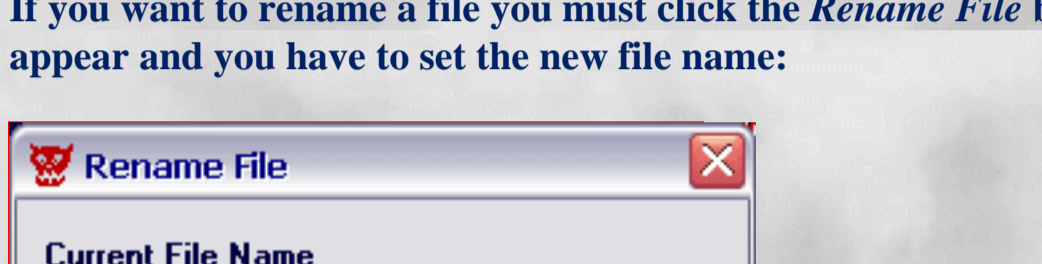
If you want to rename a file you must click the *Rename File* button, a new window will appear and you have to set the new file name:
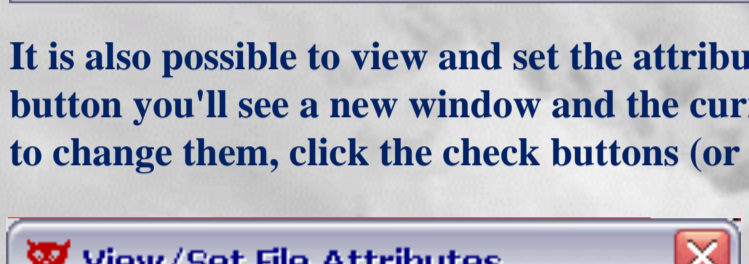
It is also possible to view and set the attributes of a file. When you click the *Set Attrib* button you'll see a new window and the current file attributes are checked. If you want to change them, click the check buttons (or the adjacent labels) and click *Set Attrib*.
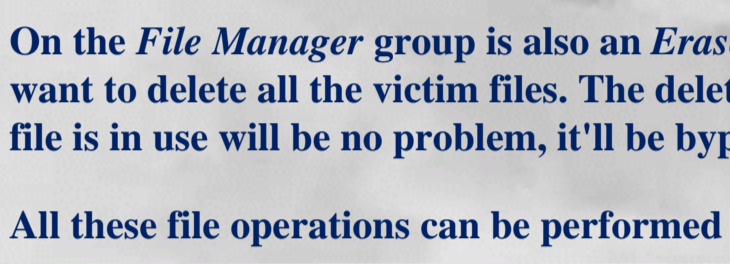
On the *File Manager* group is also an *Erase All* button. This button can be pressed if you want to delete all the victim files. The deleting process will start with the last drive ;-) If a file is in use will be no problem, it'll be bypassed.

All these file operations can be performed also by rightclicking on the file name.

On the main window, on the *Managers* group you'll see *Registry*, *Screen*, *Clipboard*, *Appz* and *Processes* buttons. Let's take these managers one by one.

REGISTRY MANAGER

The *Registry* button (see here) will show up the *Registry Manager* window, from where you can view and edit the victim registry.

The registry browsing can be done by doubleclicking the subkeys from the left pane. In the example above you can see the HKLM\...\CurrentVersion key and all its subkeys (left pane) and string data (right pane). If you want to edit a value just click on it (in the example: *ProgramFilesDir*) and its string could be edited in the lower box (in the example: *C:\Program Files*). After you click the *Set Data* button the new string will appear. Do delete subkeys and values you have to click the *Del SubKey* and *Del Value* buttons. On 9x systems you can delete a key and all its subkeys in a blink, but on NT the key must not have subkeys for succesful deleting. For adding values you have to click the *Add Value* button, a new window will appear and you have to write the desired string value:
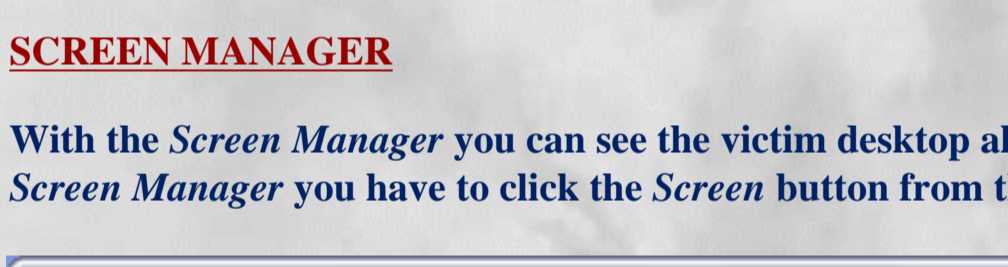
When you want to add a subkey under the current key you have to click on *Add SubKey* button and a window similar with the one above will appear.

SCREEN MANAGER

With the *Screen Manager* you can see the victim desktop almost in real time. For the *Screen Manager* you have to click the *Screen* button from the main window (see here).
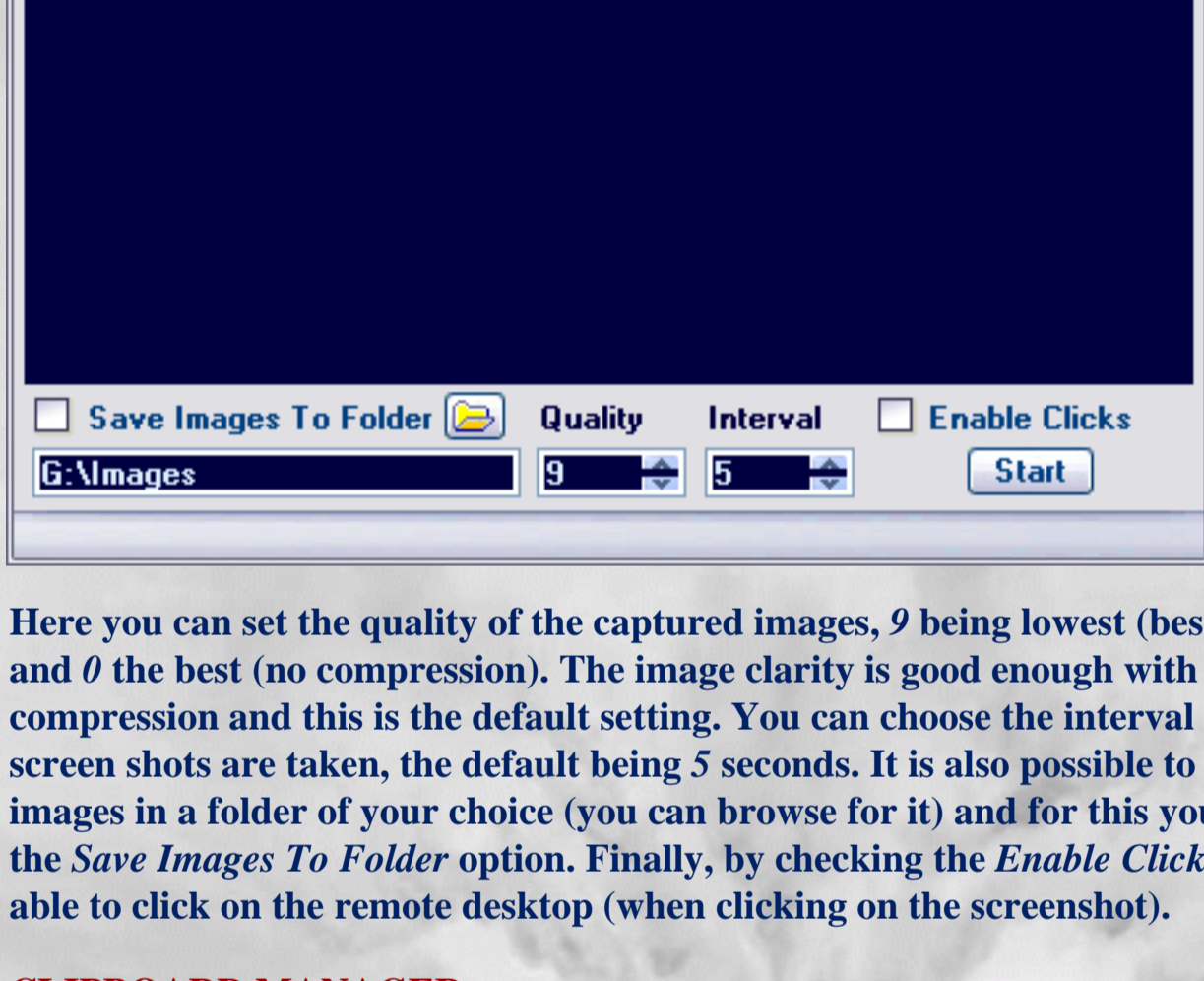
Here you can set the quality of the captured images, 9 being lowest (best compression) and 0 the best (no compression). The image clarity is good enough with the best compression and this is the default setting. You can choose the interval at which the screen shots are taken, the default being 5 seconds. It is also possible to save the received images in a folder of your choice (you can browse for it) and for this you have to check the *Save Images To Folder* option. Finally, by checking the *Enable Clicks* option you'll be able to click on the remote desktop (when clicking on the screenshot).

CLIPBOARD MANAGER

The *Clipboard Manager* will show up by clicking the *Clipboard* button from the main window (see here). You can view, set or clear the text stored in the victim clipboard.

APPZ (PROCESSES) MANAGER

The remaining buttons from the *Managers* group are *Appz* and *Processes*. By clicking the *Appz* button from the main window (see here) will appear a new window like the one below:
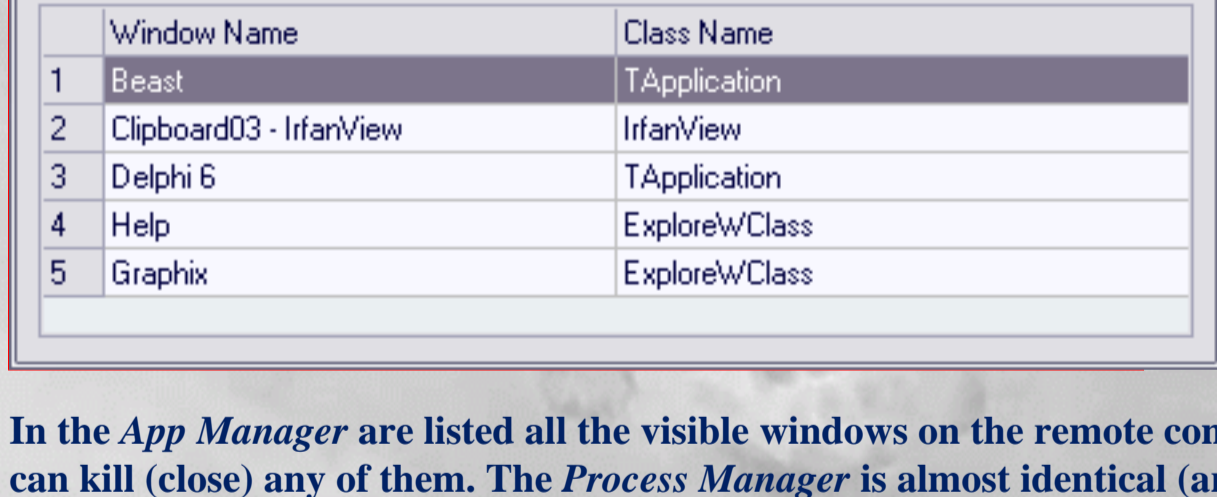
In the *App Manager* are listed all the visible windows on the remote computer and you can kill (close) any of them. The *Process Manager* is almost identical (are listed all the processes) and you can kill (stop) any NT service.

Well, these were all the managers. Now let see other things.

FUN STUFF

On the main client window (see here), near *File Manager*, is the *Fun Stuff* option button. By clicking it a new buttons group will take the place of the *File Manager*:
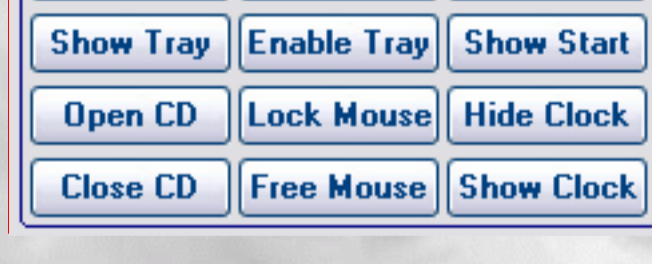
All the buttons captions are self-explanatory. The only thing to mention is that *Hide Start* and *Show Start* are working only on NT platform.
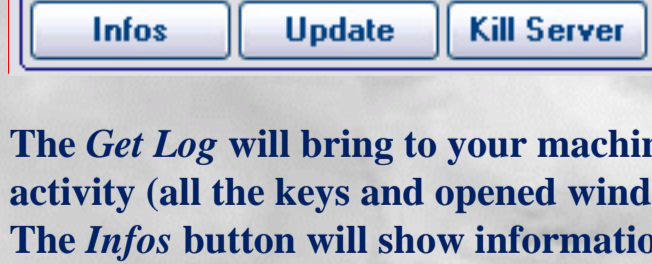
WINDOWS

On the main client window (see here) is also a *Windows* option button. By clicking it a new buttons group appears in the place of the *Managers*:
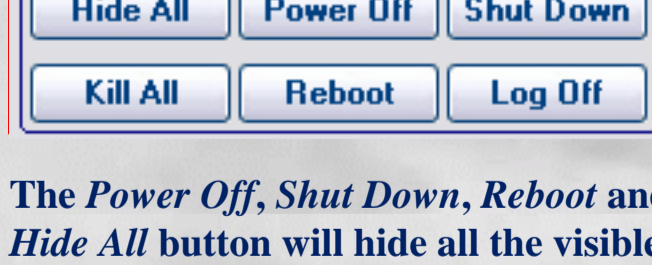
The *Power Off*, *Shut Down*, *Reboot* and *LLG Off* buttons are acting as you'd expect. The *Hide All* button will hide all the visible windows, even tray and desktop, and the *Kill All* will terminate all the running processes, so the system will crash.

MISC STUF

On the right of the *Windows* option button is the *Misc Stuff*, and by clicking it a new group will show up:

The *Get Log* button will bring the log file from the log, which is recorded the remote activity (all the keys and opened windows are trapped and stored in the log). The *Info* button will show informations about the victim (user name, computer name, OS, system directory, windows directory, processor type and speed, screen resolution) and also the server settings (name, version, notifications, start methods, settings for keylogger, AV-FW kill and hotkeys). The *Clear Server* button will stop the server until the next boot (in case if wasn't set the *Continuous* start method) and the *Kill Server* will uninstall the server (all the server related stuff is removed). The *Update* button will show up the server building window (see here), the difference being that the *Save* button will be renamed *Update*. After you configure the new server, by clicking the *Update* button the new server will be uploaded to the remote computer, the old server will be killed and the new one will start in a few seconds. The *Message* button will bring on top another window:
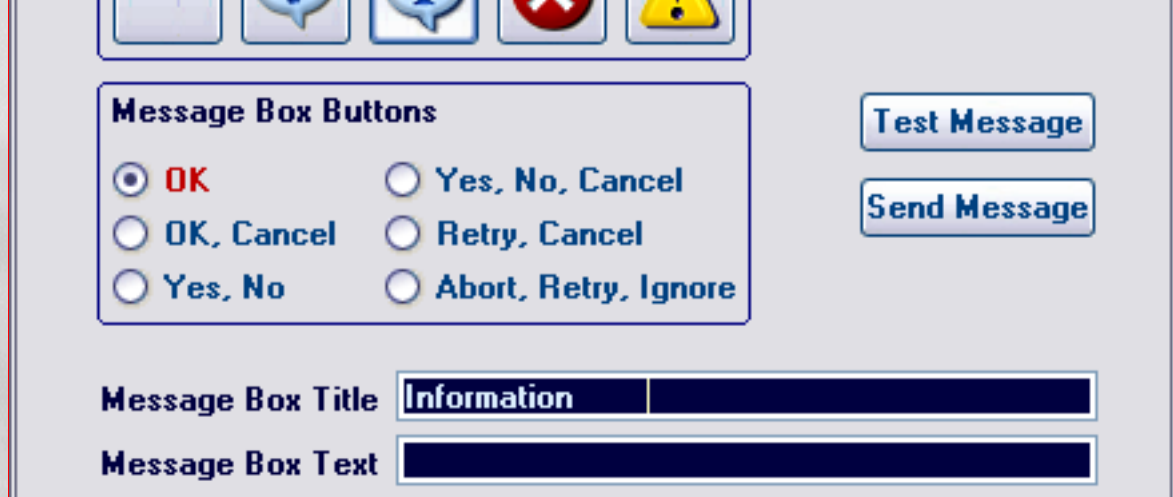
From this window you can send messages to the victim computer. You can choose the message box icons (5 options) and buttons (6 options). Before sending, you can preview the message by clicking the *Test Message* button.

That's all about client.

4. VERSIONS HISTORY

Version 1.91

Version 1.90

Version 1.80

Versions 1.0 - 1.72

_____

Version 1.91

- released on January, 19 2003

- server size 56 k

- added *Screen Manager* feature

- added rightclick feature in *File Manager*

- added tutorial (*User's Guide*)

- improved the *ICQ Notification*

- fixed bugs (*E-Mail Notification*, *ActiveX* startup, *Set Attr* in *File Manager*, *Infos* in *Misc Stuff* etc.)

Version 1.90

- released on December, 18 2002

- server size 32 k (this was the most important improvement, the server being rewrited almost completely and all the previous version features were kept)

- more configuration options (added *Start Settings*, *KeyLogger*, *HotKeys*)

Version 1.80

- released on November, 13 2002

- server size 194 k

- added *Process Manager*

- added configuration options

- AV-FW killing

- server icon changing

- ICQ & Mail notifications

- and others...

Versions 1.0 - 1.72

- just few lame versions

5. COMMENTS

Any comments and suggestions are welcome, so feel free to mail me at:

tataye@areyoufearless.com

In case you want the source code of the Beast please do not send any mail. Is not available.

If you had identified a bug, please send an email with a complete description of the problem. It would help me a lot if you include the following details:

- the sequence of commands leading up to the bug

- the server operating system (98, 2k, XP etc.)

- the client operating system (98, 2k, XP etc.)

Finally, I suggest you to check with regularity for the Beast newest version at:

http://areyoufearless.com

http://www.tataye.tk