

BEAST- The Trojan

Or

"Free GOBO Project"



Questions? mutsonline.com

<http://mutsonline.com>

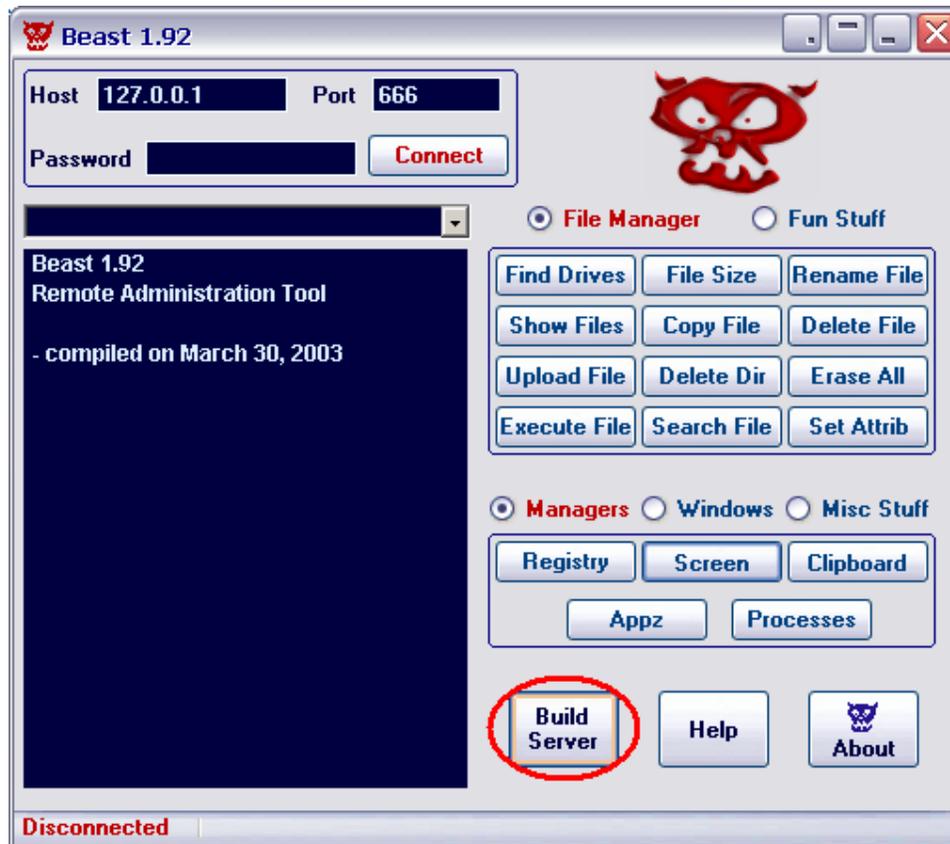
BEAST - A good Trojan

DESCRIPTION

Beast is a Trojan made in Delphi. The Trojan runs on Windows NT (XP) and also on 9x. The Beast has an easy to use interface and the server is very configurable.

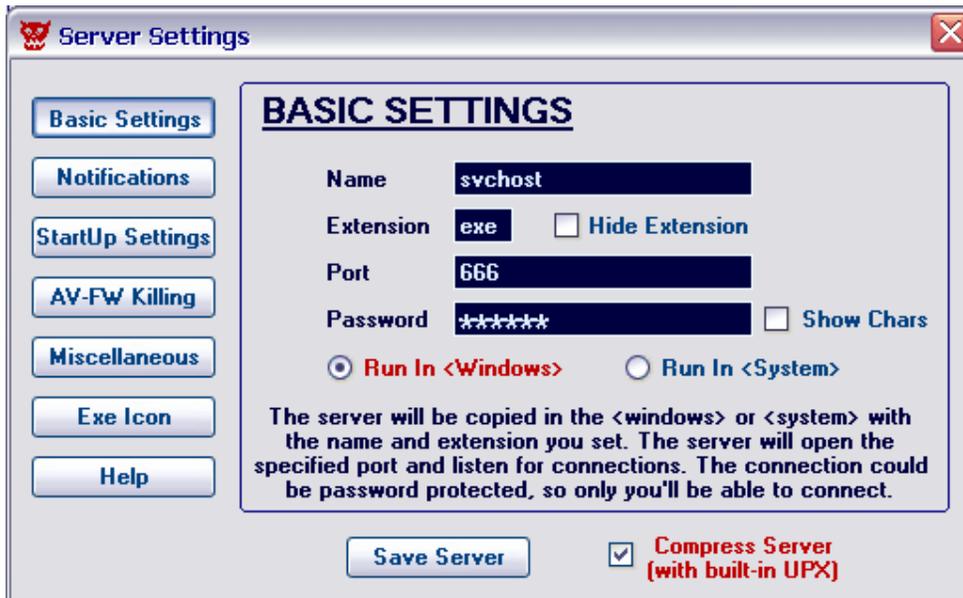
Environment

1. Run Beast. You will first need to build the server. Click on "Build Server".



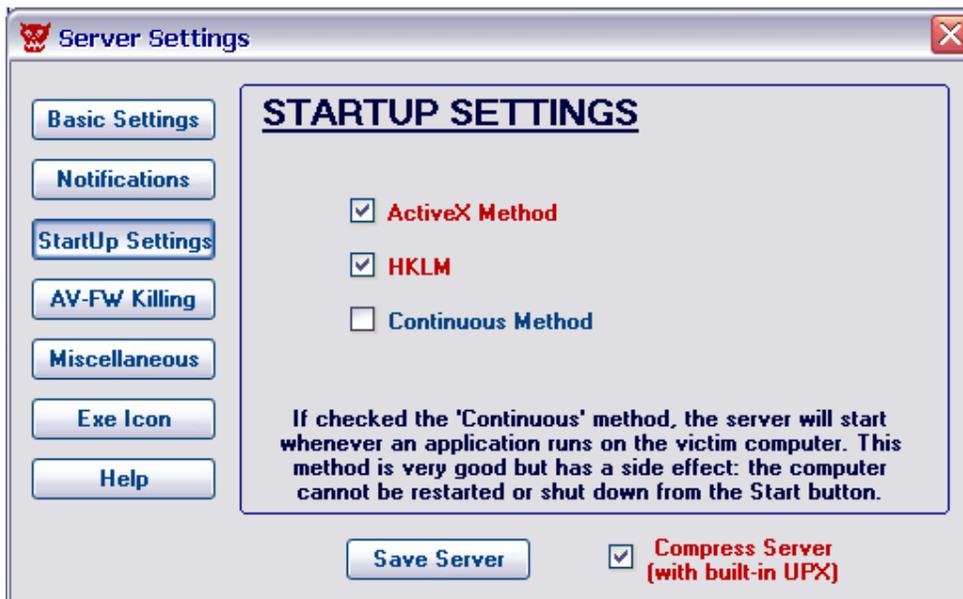
2. You will get a configurable "Server Settings" window, with lots of options. Notice all the cool options you have for building the server, such as AV disable, Startup settings, etc.

3. Most settings are intuitive, but just a quick overview of the options:

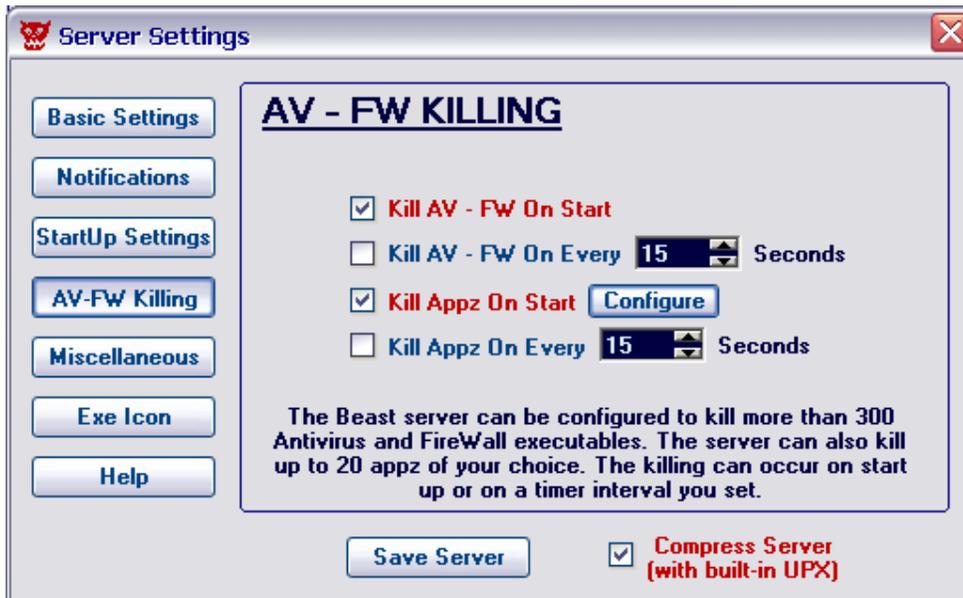


Here you can specify the name of the service, port and optional password you want the Trojan to run with.

4. The "Startup Settings" specify the startup method of the Trojan Server:

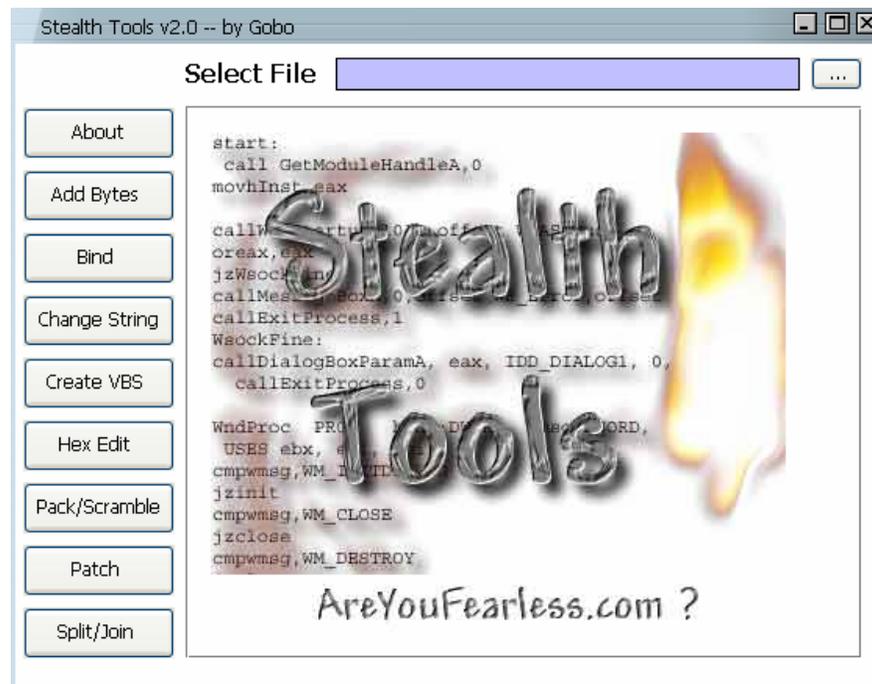


5. The Antivirus / Firewall killing feature:

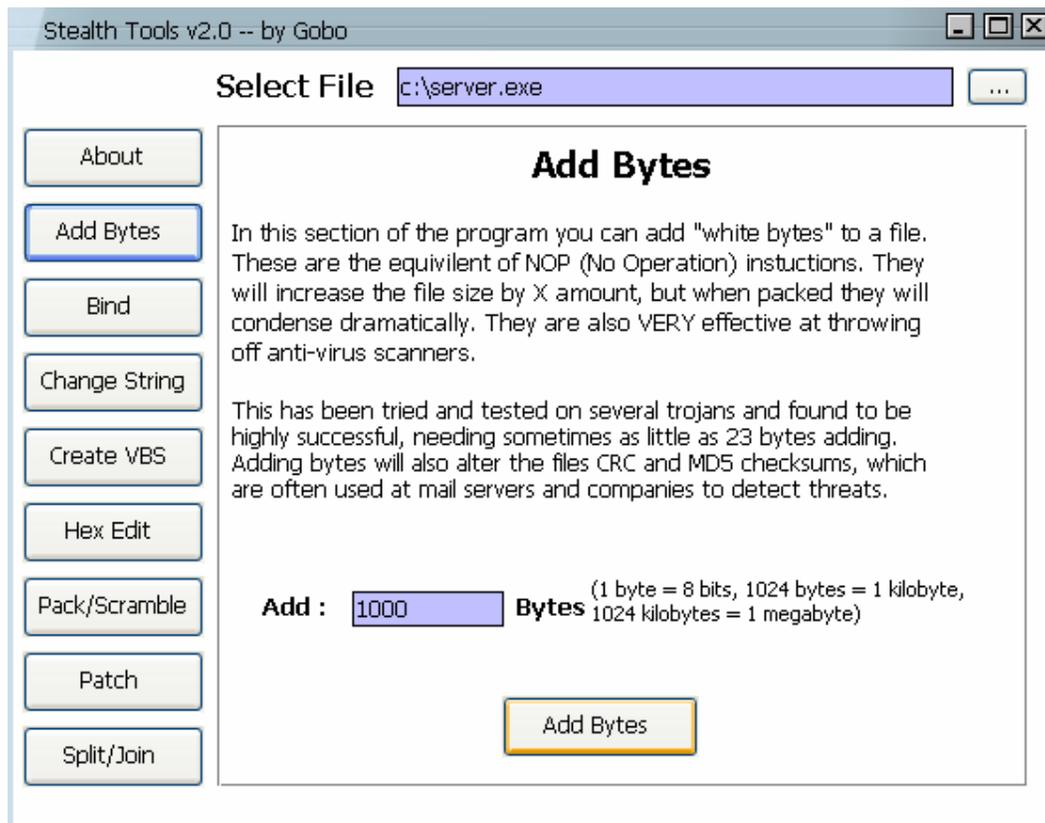


I'll leave the rest of the options for you to explore.

6. Once we have the server settings configured, we can "Save Server".
7. **Unfortunately**, the Trojan server is immediately identified as a virus by most updated antivirus software. **Fortunately**, there's something we can do about this.
8. What we need is a tool called Stealth Tools v2.0. This tool knows how to scramble / pad / modify files so that their virus signature is modified, thus undetectable.
9. So now we run Stealth Tools, and let's add 1000 bytes to server.exe we've just created.



10. We click on the "Add Bytes" button, and add 1000 bytes:



Once we are finished, server.exe should be undetectable by AV software. If for some reason this does not work, and server.exe *is* detected as a Trojan, we can try to use other masking methods.

11. Once the server is complete and undetectable, we can upload it to the victim computer (via one method or another – I'll leave that up to you) and execute it.
12. Once executed, you can connect to the victim machine with the Trojan Client (as shown on the next screen). From here onwards, its all fun and games. You have almost endless possibilities with this Trojan.

I would like to dedicate this tutorial to Simon Vallor, aka Gobo who was sentenced to 2 years in jail on January 21st, 2003. His crime was releasing a harmless virus onto the Internet. People who have committed by far more serious crimes such as rape, hit and run, drunk driving, assault, etc are sentenced to less time.

