

# BACKORIFICE 2000 TUTORIAL

Mark E. Donaldson

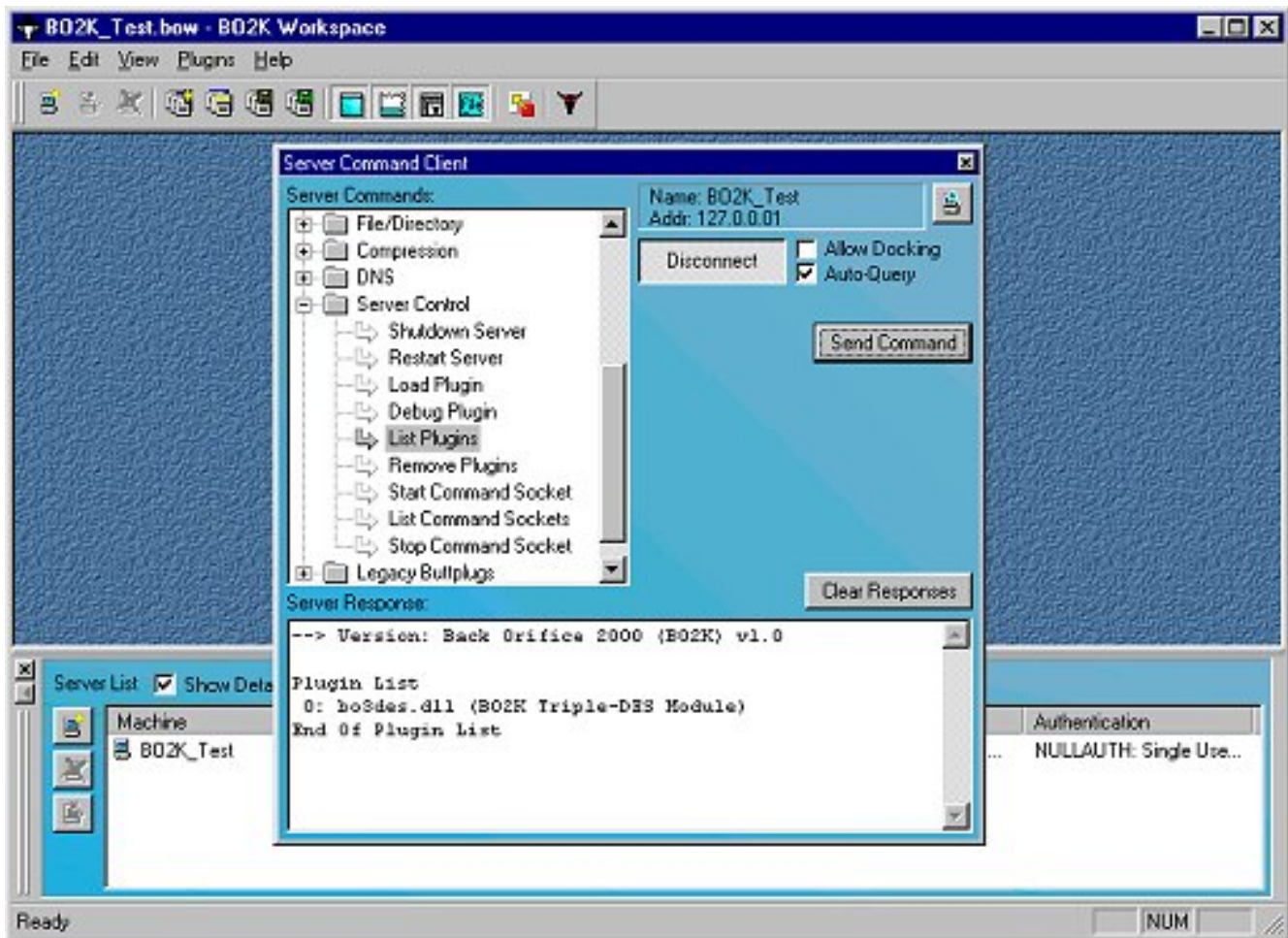


## BASIC INFORMATION

Back Orifice 2000 is a new version of the famous Back Orifice backdoor trojan (hacker's remote access tool). It was created by the Cult of Dead Cow hackers group in July 1999. Originally the BO2K was released as a source code and utilities package on a CD-ROM. There are reports that some files on that CD-ROM were infected with CIH virus, so the people who got that CD might get infected and spread not only the compiled backdoor, but also the CIH virus.

The first binary version of BO2K was compiled and spread in the US. A few days later there appeared an international version of this backdoor. With the time there may appear lots of versions of BO2K with different compilers and having different features.

As its previous versions, the Back Orifice 2000 backdoor has 2 major parts: client and server. The server part needs to be installed on a computer system to gain access to it with the client part. The client part connects to the server part via network and is used to perform a wide variety of actions to remote system. The client part has a dialog interface that eases the process of hacking of the remote computer. Here's the screenshot of the client part:



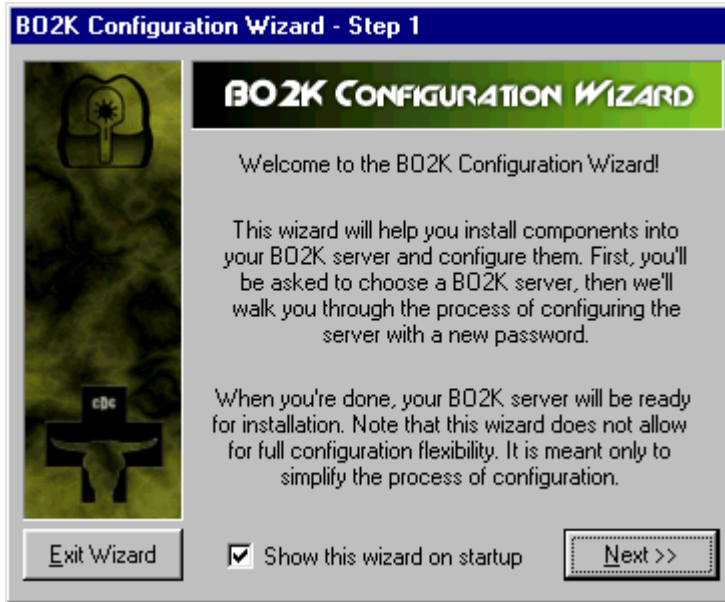
In the same package there comes also a configuration utility that is used to configure the server part of BO2K. By default the server part doesn't install itself to system being run. It should be properly configured to be used as a backdoor. The configuration utility has a wizard that helps to quickly

# BACKORIFICE 2000 TUTORIAL

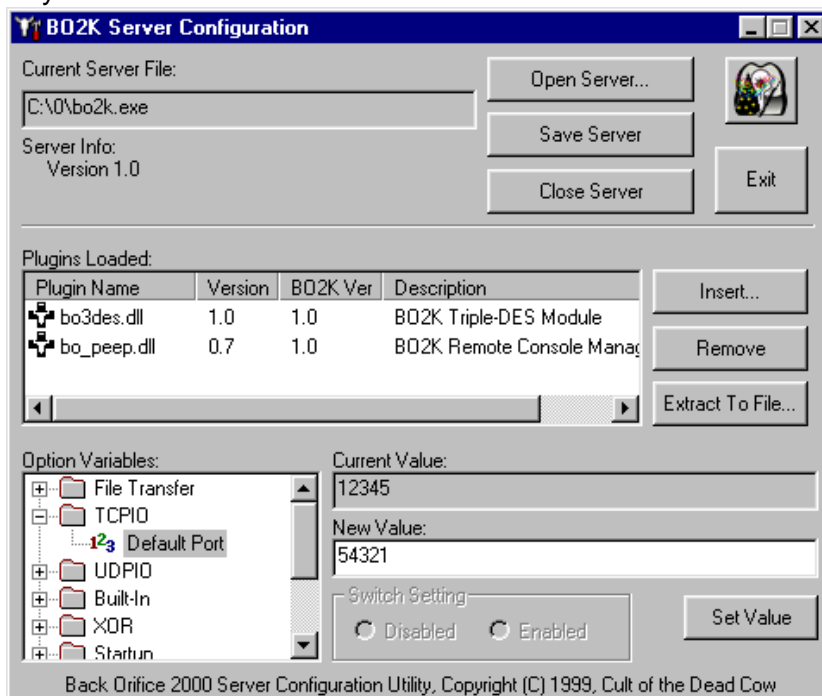
Mark E. Donaldson



configure the server part. It asks the user to specify networking type (TCP or UDP), port number (1-65535), connection encryption type - simple (XOR) or strong (3DES) and password for encryption that will be the password for the server access also. Here's the screenshot of the BO2K configuration wizard:



The configuration utility allows to flexibly configure the server part. It can add or remove plugins (DLLs) from the server application, configure file transfer properties, TCP and UDP settings, built-in plugins activation, encryption key, and startup properties. The startup properties setup allows to configure automatic installation to system, server file name, process name, process visibility and also NT-specific properties (NT service and host process names). Here's the screenshot of BO2K configuration utility:



# BACKORIFICE 2000 TUTORIAL

Mark E. Donaldson



When the server part is configured to act like a trojan i.e. to install itself hideously to someone's system it writes itself to \Windows\System\ or \WinNT\System32\ folders under a name specified during configuration (default is UMGR32.EXE). Then it modifies the Registry. Under Windows 95/98 server execution string is written to:

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices**

under Windows NT the execution string is written to:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**

Then the file from which the server part started can be deleted (if it was specified during configuring). After that the BO2K will be active in memory each time Windows starts and will provide access to the infected system for hackers who have the client part and the correct password.

Being active the server part can hide its process or prevent its task to be killed from Task Manager (on NT). The backdoor uses a smart trick on NT by constantly changing its PID (process ID) and by creating the additional process of itself that will keep the backdoor alive even if one of the processes is killed. Besides, the server part adds a random (but large) number of spaces and 'e' at the end of its name, so the server part file can't be deleted from Windows (invalid or long name error occurs) though disk checking utilities don't find any problems with filename. The server part file can be only deleted from DOS or DOS session (if the file is not locked of course).

Back Orifice 2000 like its ancestors has a lot of features. But unlike the older versions the BO2K has many improvements: connection encryption (including strong 3DES), ability to work under NT, to use UDP, to allow internal plugins in DLL format, a more advanced security, more remote system control features.

Here's the list of Back Orifice 2000 capabilities:

1. Ping and query server part version.
2. Rebooting, locking up system, listing of passwords (yes, it works - passwords are retrieved from memory), getting system info.
3. Logging keyboard activities, operations with log file: view, delete.
4. Opening a messagebox with specified text and title.
5. Mapping TCP ports to another IP, console application, HTTP fileserver, filename, listing of mapped ports and TCP file sending.
6. Adding and removing network shares, listing of shares (including LAN), mapping of shared devices, listing of active connections.
7. Process control (works under NT as well): list, kill, start.
8. Full access to Registry (though the way it is done is not convenient - all keys should be typed manually).

# BACKORIFICE 2000 TUTORIAL

Mark E. Donaldson



9. Playing WAV files (looped playback is possible), capturing screen, AVI and video still.
10. Full disk access: listing of directories and files, finding, viewing, deleting, moving, copying of files and folders, transfer list maintenance.
11. Remote compression and decompression of files (to receive big files from remote system).
12. Resolving full host name and IP address.
13. Flexible server control including each plugins control, command sockets manager.
14. Possibility to run any plugins ('buttplugs') and to activate any functions in them with specified parameters. For example one plugin can initiate a video stream and 'highjack' a remote system.

The US version has some serious bugs - sometimes installation of the backdoor fails under NT. On NT shutdown an error messagebox is displayed for some time.

When more version of Back Orifice 2000 appear this description will be updated with new facts.

Detection and removal of Back Orifice 2000 is available with the special update that can be downloaded from Data Fellows ftp site free of charge.

**<ftp://ftp.DataFellows.com/anti-virus/updates/avp/>**  
**<ftp://ftp.Europe.DataFellows.com/anti-virus/updates/avp/>**

How to remove the server application:

- Start the Registry Editor.
- Go to:  
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- Delete the UMGR32.EXE key.
- Close the Registry editor, and reboot the system.
- Delete the UMGR32~1.EXE file from the \Windows\System directory.

# BACKORIFICE 2000 TUTORIAL

Mark E. Donaldson



## BACK ORIFICE TUTORIAL



`bo2kcfg.exe`

This is a simple tutorial for those who want to get started using BO2K quickly.

### Step One: Configure the BO2K Server

Alright, once you've unpacked the BO2K distribution into a directory, start up the BO2K server configuration tool by running the tool. The configuration program pops up.



Now we want to open the BO2K server, the one that we're going to be installing on the server machine, and configure it. First, make a copy of the BO2K executable, and open that one by clicking the open server button and choosing the proper BO2K.EXE executable from the list of files. You can configure the built-in system settings, such as encryption keys and default ports by using the tree control at the bottom of the window, and changing the setting on the right. For example, to change to port that BO2K listens on (aka, what BO2K 'binds to'), Do the following:

- Expand the 'Startup' option folder.
- Click on the 'Init Cmd Bind Str' and you'll see the current 'binding string' appear in the 'Current Value' box. A 'binding string' is a protocol-independent way to specify where the protocol will be

# BACKORIFICE 2000 TUTORIAL

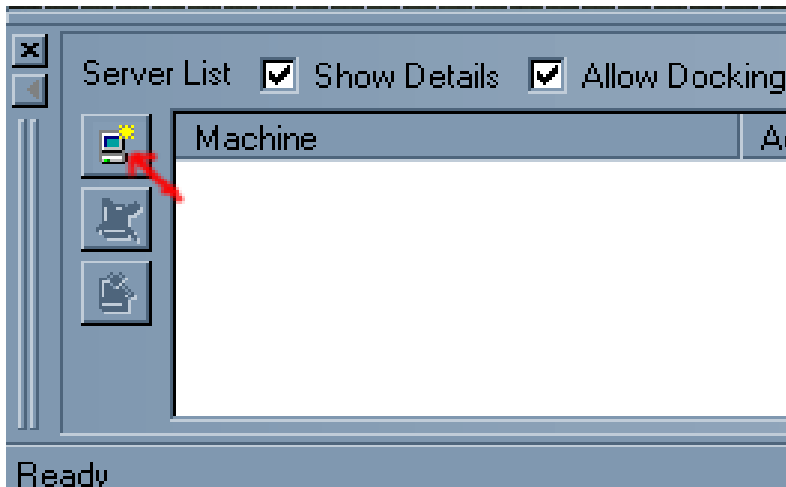
Mark E. Donaldson



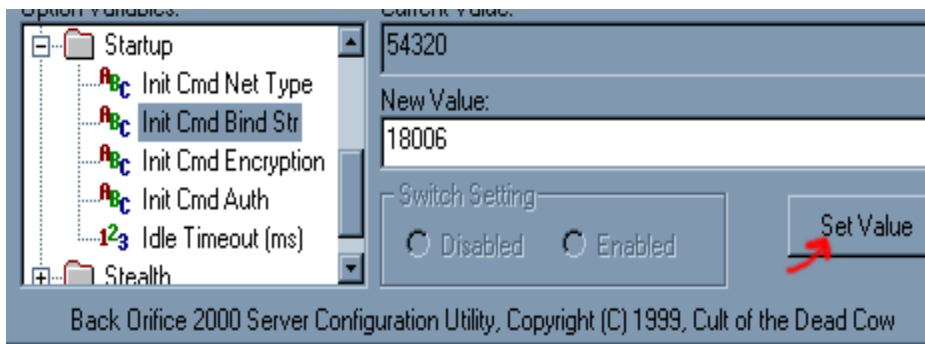
listening. For UDPIO and TCPIO protocols, this is simply a port number. If you were running a Netware/IPX plugin or some other protocol, the binding string would have a different syntax.

- Since the default value of the 'Init Cmd Net Type' option is still 'TCPIO', we'll go ahead and set the port to something like 18006. To do this, type 18006 into the 'New Value' box and hit 'Set Value'. Now, the server is configured to use TCPIO port 18006. Tada.

Now let's do one more thing. Add the BO\_PEEP plugin.



- To the right of the 'Plugins Loaded:' box, there is an 'Insert...' button. Click it.



- When the 'Insert BO2K plugin' box comes up, choose bo\_peep.dll and hit Open.

You'll notice that the BO\_PEEP plugin now shows up in the Plugins Loaded: box. Also, the list of options in the "Option Variables" box has been updated to include BO\_PEEP options. You can modify these later if you wish. Now on with the tour. Save the server by clicking the 'Save server' button, and close the program.

## **Step Two: Install The BO2K Server**

This is a relatively simple task. Just copy the server to the target machine, and run it. If you're installing on a Win95/98 machine, the server executable will move itself into the c:\windows\system directory and name itself 'UMGR32.EXE'. The name is configurable with the BO2KCFG tool that we just used. There are other things you can do to customize how BO2K behaves upon installation. A fuller description of these options are available in the Command Reference section of this website. If

# BACKORIFICE 2000 TUTORIAL

Mark E. Donaldson



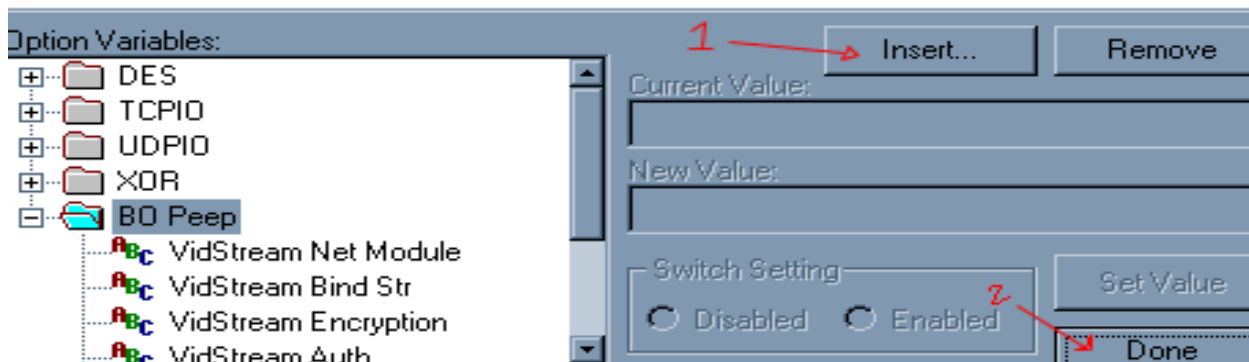
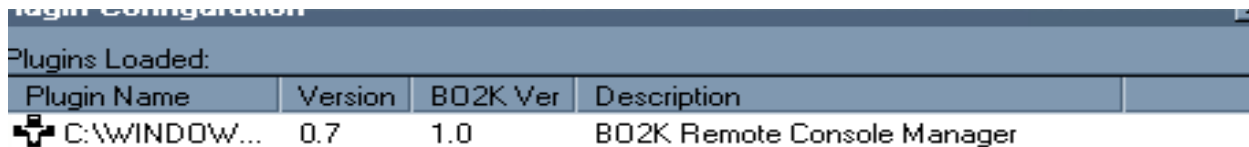
you are installing under Windows NT, BO2K copies itself into the c:\winnt\system32 directory (if permissions allow it to do so) and renames itself.

## Step Three: Start Up The Client

First start the client by running the tool. It should open, and maximize itself. First things first, we want to create a new server connection. So we click on the little computer button in the left hand side of the server list window at the bottom. This pops up a dialog where you can define the parameters of the machine that you want to contact. You'll want to put in a name for this connection (doesn't matter what it is) in the 'Name of this server' field. Next, put in the server's IP address:port pair. We have to specify the port, since we reconfigured the server, and didn't change the defaults for the client. So we type in aaa.bbb.ccc.ddd:18006, replacing the letters with the real IP address of the server. Connection type should be TCPIO, encryption should be XOR, and authentication should be NULLAUTH. When you're done, hit 'OK'.



One you've hit OK, the server command client pops up for this server. You can minimize and restore the server command client by double-clicking the server name in the server list box at the bottom.



## Step Four: Configure the Client

Since we installed the BO\_PEEP plugin in the server, in order to communicate with it properly, we need to install the same plugin into the client. To do this, we go to the 'Plugins' menu option and the choose 'Configure...!'.

This pops up a dialog to insert and remove plugins and configure basic setting, much like the BO2KCFG tool, but this time it's for the client. This dialog also doesn't modify any executables. It stores the configuration in the registry. So, we hit the 'Insert...' button and choose the bo\_peep.dll file. This adds the BO\_PEEP plugin and puts the options in the tree control below. We didn't reconfigure BO\_PEEP on the server side, so we won't have to configure it here. Just hit 'Done'.

# BACKORIFICE 2000 TUTORIAL

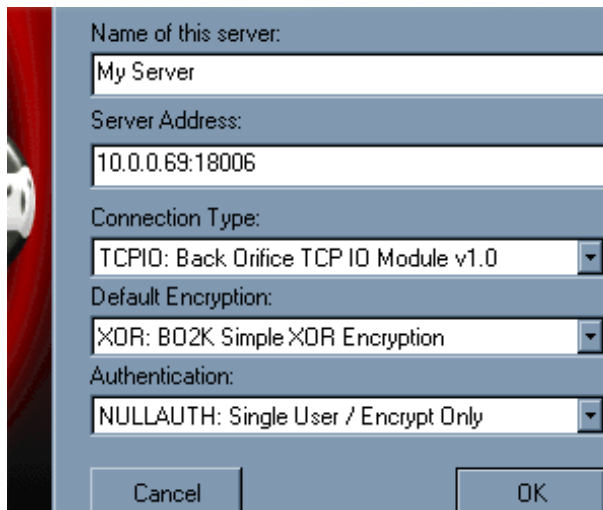
Mark E. Donaldson



## Step Five: Connect To The Server and Fool Around

Simply hit the 'Connect' button on the Server Command Client. It should sit there for a second, and then spit out the version number of the server it has connected to in the output window at the bottom of the command client. After connecting, you can pick commands out of the 'Server Commands' tree control. When you choose a command, the parameters for the command will appear in the right of the box. Some parameters are optional, as indicated by either brackets [], or something like (opt). All other parameters must be filled in with valid values.

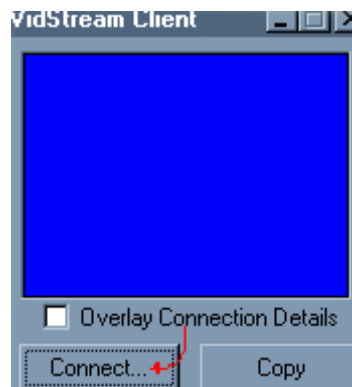
To send a simple ping command, open the "Simple" folder in the tree control, and click on the 'Ping' command. Now, click on the 'Send command' button. If the ping was successful, a ping reply message should be issued from the server, and will appear in the output window.



## Step Six: Try Using The Plugin

To use the plugin, go to the Plugins menu option, and you'll notice that there is now a 'BO Peep' submenu. This was added when you inserted the plugin into the client. Select the 'VidStream Client' sub-menu item. It should pop up a happy little blue box.

Before we can connect, though, we need to start the VidStream service on the server side. So we go



to the BO Peep folder in the server command client's command list, open it, and choose the "Start Vidstream" command. A number of options will appear. Type the value '8' into the FPS box. Type '160,120' in the 'Xres,Yres[,NET][,ENC][,AUTH]' box. Then hit 'Send command'. The server should respond, telling you what address you need to connect to in order to get the video stream.

# BACKORIFICE 2000 TUTORIAL

Mark E. Donaldson



Click on the connect button on the VidStream client, and you'll be presented with a connection dialog. The number in the box is the default VidStream port. Modify the address to include the appropriate IP address (as returned by the server). Such as: aaa.bbb.ccc.ddd:15151. All of the other options should be their correct defaults. Hit the OK button and you should connect. If you mistyped something, got the port/address wrong, or picked the wrong network type/encryption/crypto-key, then it won't connect. But it all goes well, you'll see a little window into the other machine's desktop.