

DOCUMENTATION & INSTRUCTIONS COMPILATION FOR

# Back Orifice 2000

BO2K freeware designed & written by cDc  
AND RELATED ADD-ONS, PLUG-INS, AND OTHER SOFTWARE

This compilation has been put together by the Non-Compiler.  
The Non-Compiler takes neither credit nor responsibility for the accuracy,  
potential usage (or misuse) of the information contained herein  
(however I do take full credit for all the work done in putting it together, and  
if [SETI@HOME](mailto:SETI@HOME) ever gets results, world peace erupts, or the 2<sup>nd</sup> coming happens,  
I would like to receive some credit for those as well! Thank you.)

All documentation contained herein is credited to the original authors  
in instances where this information is known.

## CONTENTS (as of 15 September 1999)

- Back Orifice – General Information (Sept. 1998)
- Data Fellows/F-Protect Virus Info: Description of BO2K
- Back Orifice 2000 – Tutorial (sort of...)
- Back Orifice 2000 FAQ
- Back Orifice 2000 Commands
- Butt Trumpet 2000 v. 1.2 and related FAQ
- Rattler Plug-in v. 1.0
- STCPPIO – Stealth TCP IO plug-in v 1.2
- CAST 256 Encryption Plug-In for BO2K v. 2.4
- BoTool - Remote Filesystem Browser and Registry Editor For BO2K Systems v. 1.0
- Liberator v. 1.11 Protection against BO2K
- Comparison of BO2K Security Plug-ins
- Listing of some available BO2K plug-ins, add-ons, etc.
- CDc Press Release “BACK ORIFICE 2000”



## What is BACK ORIFICE 2000?

**Control.** Back Orifice 2000 is the *most powerful network administration tool available* for the Microsoft environment, bar none.

Built upon the phenomenal success of Back Orifice released in August 98, Back Orifice 2000 puts network administrators solidly back in control. In control of the system, network, registry, passwords, file system, and processes. BO2K is a lot like other other major file-synchronization and remote control packages that are on the market as commercial products. Except that BO2K is smaller, faster, free, and very, very extensible. With the help of the open-source development community, BO2K will grow even more powerful. With new plugins and features being added all the time, BO2K is an obvious choice for the productive network administrator.

### Feature List

#### **General**

- Open source architecture ensures product development in the future
- Open source provides a trusted environment, and promotes security
- FREE. No price tag. Just download and install
- Easy installation on both client and server machines

#### **Client Features**

- Address book style server list
- Plugin extensibility
- Multiple server connections at once
- Customizable look-and-feel
- Session logging
- Native Server Support
- Keystroke logging
- HTTP filesystem browsing and transfer, with optional restrictions.
- Management of Microsoft Networking file sharing
- Direct registry editing
- Direct file browsing, transfer, and management
- Plugin extensibility
- Remote upgrading, installation, and uninstallation
- Network redirection of TCP/IP connections
- Access console programs such as command shells through Telnet
- Multimedia support for audio/video capture, and audio playback
- NT registry passwords and Win9x screensaver password dumping
- Process control, start, stop, list
- Multiple client connections over any medium
- GUI message prompts
- Proprietary file compression
- Remote reboot
- DNS name resolution

#### **Features Added By Plugins**

- Cryptographically Strong Triple-DES encryption
- Remote desktop with optional mouse and keyboard control
- Drag and drop encrypted file transfers and Explorer-like filesystem browsing
- Graphical remote registry editing
- Reliable UDP and ICMP communications protocols
- (COMING SOON) IPX/SPX, Telephony/Dialup, and IRDA communication protocols
- (COMING SOON) Scripting language for client and server-side automation
- Lots more coming soon!

## Description

Back Orifice is the most popular trojan at the moment. Since its release on DEFCON VI by Cult of the Dead Cow (cDc), it has spread extraordinarily fast around the globe. Well, Sir Dystic did a great job. Back Orifice is the most powerful trojan available at present. It is configurable for many special purposes by using plugins. The many options make it no easy toy for hacker kids however. One must know a lot to use this one right.

## Basics

Back Orifice hides itself from the task list when active. Upon infection, it installs itself in the Registry under the key HKLM/Software/Microsoft/Windows/CurrentVersion/RunServices, therefore launched by Windows upon system start. It copies itself into the <WindowsRootDir>\system directory, and then deletes the installer. The standard installer has an invisible icon.

You need to have Windows 95 or 98 to get infected. BO won't install itself on a NT system. This is due to the static usage of some system DLL's, which are not available under NT. For infection it is needed that you run the executable on your system. It is *\*not\** possible to get infected by just browsing the web or reading E-Mails. Theoretically. However, there are bugs in many Internet software packages, including Microsoft Internet Explorer, Microsoft Outlook Express and Netscape Communicator. Some bugs may allow someone to run arbitrary code on your machine without the need for your help. But these bugs are *\*very\** difficult to exploit, and this can only be done by a true hacker. Those attacking you with Back Orifice however usually are only kids playing superhacker, so you needn't get worried about those security bugs too much (Hmmm...but what about the authors? -ed.). But to be on the safe side please install the updates, service packs and bugfixes for the Internet software and for your Windows, available at [www.microsoft.com](http://www.microsoft.com) and [www.netscape.com](http://www.netscape.com) respectively.

## Tech

Back Orifice is fully configurable. The standard port is 31337, name is ".exe" and it uses no password. But this can all be configured. BO always places an entry in the RunServices section in the Registry, whether the configuration is valid or not. BO uses the UDP protocol for communication, which means that it is not locatable by a common port scan. It only responds to packets encrypted using the password it was configured to by the attacker. It has also the option to run plugins. These plugins can be written by anyone, and therefore is a BO server not limited to its standard functionality, but can easily be extended with other functions, known examples include sending a mail upon infection, and connecting to an IRC server and tell all the chatters there that the computer is infected, as well as a sophisticated network traffic sniffer. BO lends full control over the infected machine, including: application launch and control, directory and file mgmt, net connection and share mgmt, compression and decompression, HTTP server, keyboard log, screen capture, webcam capture, play sounds, ping, plugin mgmt, process mgmt, port redirection mgmt, Registry mgmt, resolve host, display dialog boxes, system information including cached passwords, lockup, reboot, TCP file send and receive.

There is the possibility to misconfigure BO so it will not copy itself to the system directory but stay where it is and run from there. The Registry entry in this case is not valid, which makes it harder to locate.

BO leaves a file called windll.dll in the system directory. This dll is used for hooking the keyboard and logging all keystrokes. Droppers are available, enabling anyone to package BO into another program, infecting the target upon execution of that program. The most powerful of these droppers, SilkRope 2.x, even encrypts BO, so it wont be located with a common file scan.



## F-SECURE VIRUS INFORMATION PAGES

**NAME:** BO2K  
**ALIAS:** Back Orifice 2000

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.

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 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.

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 filename, process name, process visibility and also NT-specific properties (NT service and host process names).

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 TUTORIAL (sort of...)**

**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* (do NOT click on the BO2K.EXE directly or you will infect yourself!) 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 then 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 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.

### **Add the BO\_PEEP plugin.**

1. To the right of the 'Plugins Loaded:' box, there is an 'Insert...' button. Click it.
2. When the 'Insert BO2K plugin' box comes up, choose `bo_peep.dll` and hit `O` pen.
3. 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 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. That's it. Wasn't very difficult, was it..?

### **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 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'.

**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.

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 if it all goes well, you'll see a little window into the other machine's desktop. Congrats!

Well that's it for the tour, you should be able to figure out lots of other things on your own!



## BACK ORIFICE 2000 FAQ

### General Topics

#### **1. What is BO2K? Where can I get it?**

You can get BO2K from the BO2K website in the downloads section at <http://www.bo2k.com> .

#### **2. Who wrote BO2K? Why was it written?**

BO2K was written by DilDog of the Cult of the Dead Cow. Many of the commands that BO2K comes with were directly ported from Sir Dystic's original Back Orifice source code. It was written with a two-fold purpose: To enhance the Windows operating system's remote administration capability and to point out that Windows was not designed with security in mind.

#### **3. Is this a 'hacker tool', or is it an 'administration tool'?**

This tool, like other tools you might have around the house can be used legitimately, or it can be used to harm people. You can take a hammer and beat people in the head with it. Doesn't mean we need to go around beating people in the head with hammers to teach them that they should watch out for maniacs wielding hammers. Imagine a whole world of people that don't know a hammer from sponge, let alone what a hammer is good for, and you'll find what situation we're in here. Hackers can use it to hack. Administrators can use it to make their lives a lot easier. Administrators, be responsible with this tool. End-users, don't trust random people on the internet, and they won't hit you with a hammer... Too bad it has to be this way, but Microsoft wasn't thinking of making the computer foolproof when they put together their operating systems.

#### **4. What is BO2K good for? What are the legitimate uses for it?**

Remote administration. Administration of many Windows boxes through encrypted channels. Performing common tasks on many machines without having to walk over to each and every one of them. Controlling a Windows machine that is many miles away with the kind of flexibility that UNIX users have enjoyed for decades, without a ridiculous VPN setup.

#### **5. How big is BO2K, anyway? Gimme statistics.**

Well, the BO2K server without any plugins installed is ~100K. Nice small footprint. The client software is ~500K. Large, bulky, MFC, GUI. That's why :). The whole suite will fit on a single 1.44MB floppy disk.

#### **6. Are there licensing terms for BO2K? How much does it cost?**

It costs nothing. Freeware. It's also open source. It's available under the GNU Public License. For end users, the license is simple. Use it, distribute it. Don't claim that you wrote it, because you didn't. We also aren't going to support the software. We don't have ANY manpower to do so. So, if you can't figure it out with everything we've put on this web site, you're shit out of luck. For developers, more detail about source code usage is available in the Developers Corner FAQ.

#### **7. What about the Triple-DES plugin? Tell me about export controls.**

The strong encryption provided by the Triple-DES plugin is only available in the United States. The US still has antiquated laws in place that keep citizens and corporations from exporting encryption that is already available in other countries anyway. The reasons why these export restrictions are still in place are beyond me. This probably stems from the fact that the US Government, on the whole, fears technology because they don't understand it. It would be in the best interest of America, for these laws to go away, and stay away. They only stifle scientific development, and free thought and speech.

### Compatibility Topics

#### **8. What does it run on? What do I need to use BO2K? Hardware requirements? Operating system?**

BO2K will currently run on Windows 95, Windows 98, Windows NT, and Windows 2000 systems. All of the various parts of the BO2K suite have been testing and found to be working on all of these platforms. It only runs on Intel platforms at the moment. Since everything is open source, hopefully more support for other operating systems and environments will be added.

**9. Will clients exist for other operating systems?**

Well sure, why the hell not. We did it for the UNIX command line client for the original BO. There were even a number of TCL GUIs for Back Orifice running around out there. We'll try to make a more concerted effort to collect what people develop and put it on the BO2K website.

**10. What about servers? Can I control a Mac from my Linux box?**

Well sure! Well.. not yet. But someday. There's no reason why the server couldn't be ported. To Mac, to Linux, to BeOS, to CP/M. Have fun. Develop and be prolific. We dare ya.

**11. What are the differences between BO2K and the original BO? Is it backward compatible?**

BO2K is an almost complete rewrite of the original Back Orifice. It sports a much heftier plugin architecture that can extend every little part of the system in any way. By default, BO2K comes with the capability to talk over TCP as well as UDP, and supports strong encryption through plugins. Commands have also been added, upgraded and fixed, especially in the areas of file transfer and registry handling.

**Running BO2K**

**12. How do I run more than one server at a time?**

You install two servers. Each with a different installation filename, and running on different ports. But, this is not suggested, as it is not necessary. BO2K servers can run on multiple ports and accept connections over any number of mediums at once. You only need one server to do everything.

**13. How can I tell if BO2K is running on my machine?**

Well, it depends. If you install it as Administrator on a Windows NT machine, you'll see it in the process list running as a service. Otherwise, there are no really good ways to tell if it's running. You will probably want to check your RunServices and Run registry keys as well as your startup groups to make sure that there isn't anything in there that you didn't specifically put in there (Good idea regardless!). If you don't understand what I just told you, go get the 10 year old kid down the street that 'knows computers' and get him to tell you. And give him a few bucks for it too, he deserves it.

**14. How can I tell if BO2K is running on someone else's machine?**

There's no good way to tell. Until someone finds a good way to tell. And then we'll make that not work any more. You shouldn't be able to tell if BO2K is installed remotely.

**15. So, I'm running BO2K. How do I get rid of it?**

Connect to the server with the client, and go to 'server control', and run the 'shutdown server' command with the 'DELETE' option. If you don't have the password, or you didn't mean to run it, you may have to get someone to help you hunt through your registry and startup groups to delete the appropriate registry keys. Don't install this program on your machine unless you really know what you're doing. And don't be dumb and let someone else put it on your system. Trust no one.

**16. What is a connect string (address, conn str, etc)?**

A connect string is a description of how you want to connect to a remote machine. It specifies a remote address (usually an IP address, but not necessarily), followed by the network type, the encryption type, and the authentication type. A typical example of a connect string is:  
192.168.55.20,TCPIO,XOR,NULLAUTH

**17. What is a binding string (bindstr, bind str, etc)?**

A binding string is a description of how you want to set up a listening service on the server machine. It specifies a binding characteristic (usually an IP port or an IP address:port pair, but not necessarily), followed by network type, encryption type, and authentication type. A typical example of a binding string is: 15380,UDPIO,3DES,NULLAUTH

**18. I'm using the BO Peep plugin and it seems choppy and slow, what am I doing wrong?**

You may be trying to send over a really big screen over a really slow network. Be aware that when VidStream starts up, it synchronizes by sending over the whole remote screen. That takes a while. If things lock up, wait for a little while. it'll come through.

### **BO2K Support**

#### **19. What support is available for BO2K? Can I buy support for my company?**

There is none. And you can't. You'll just have to get along. We don't have any personnel to sit around and answer questions or fix things.

#### **20. Where is the official BO2K documentation?**

On the BO2K website. <http://www.bo2k.com>. If you aren't reading this on the website, someone probably ripped this faq off. Go there for the newest info.

#### **21. I love BO2K, but I wish there was a feature to ...**

We love BO2K too. But we can't do everything. Feel free to send us suggestions though, and we'll take them seriously. Also, if you're a programmer, feel free to join all of the other developers that would like to write BO2K stuff, and write a plugin, or extend the server. Send us what you've done and if we like it, we'll put it in the next distribution.

#### **22. Where can I get plugins for BO2K? Are legacy BUTTPlugs supported?**

Right on the website. In the download area. There will probably be other places on the net that have BO2K plugins, and I'm sure you know how to use a search engine, so I bet you'll find them if you look. Legacy BUTTPlugs are supported in BO2K as well.

#### **23. Where can I ask questions and get them answered?**

Try IRC. Try UseNet. Try your friends. But don't send us email about support questions, because we'll just delete them.

#### **24. Are there IRC channels or UseNet groups for discussion of BO2K related topics?**

Not yet. There is a Cult Of The Dead Cow newsgroup at [alt.fan.cult-dead-cow](mailto:alt.fan.cult-dead-cow) that you can try asking questions on. As for IRC, there exists #bo and #bo2k on EfNet, but as usual, ugly 12 year olds have already cybersquatted those channels, set up 500 bots watching them, and then never say a damn thing on them. Way to go losers. Bug the people on these channels with your questions.

### **BO2K Security and Development**

#### **25. How do I know that I can trust BO2K on my network?**

First things first, BO2K (in the US, of course) uses strong encryption, making it a very difficult problem for system crackers to mess with your connections. BO2K is also very low profile, making it good for network surveillance. BO2K also comes with full source code available, so if you don't trust us, and want to see exactly what the software is doing, either take a look at it yourself, or have someone you trust do it for you.

#### **26. I don't believe you. Where is the source code?**

It's in the developer SDK download section. In the Dev Corner.

#### **27. How can I recover my password if I have physical access to the machine?**

You can find the server executable, open it up with the configuration tool, and look at the password. It's all plaintext in the executable anyway. Someday, that will change, when new authentication plugins are developed.

#### **28. I want to write plugins. Do I have to download all of the BO2K source?**

Nope. You only need to download the BO2K SDK. Go to the Dev Corner.

#### **29. Is there another FAQ for developers only?**

Yes. It's in the Dev Corner on the BO2K website. Go there and browse around.

.....

## **BACK ORIFICE 2000 COMMANDS**

### **Ping**

Send a ping to the server. If the server is connected/alive, it will respond.

### **Query**

Primarily sent by the client whenever it determines that it needs to synchronize itself with the server. Whenever a server-side plugin is added, the client sends this command to retrieve a new list of commands that the server is capable of. If you have auto-query turned off on the client, or you wish to synchronize the client, send this command to refresh things

### **Reboot Machine**

Reboots the server machine. Asks no questions. This will kill your connection to the server.

### **Lock-up Machine**

Makes the server machine completely unresponsive. The mouse will not move, and the keyboard will not work. Grinding halt. Also makes the BO2K server unresponsive and will kill your connection to the server after the protocol times out.

### **List Passwords**

Under Windows 95/98 this lists the passwords that are stored in the Internet Explorer password cache. If you've ever checked the 'Remember My Password' box, your password will be available here. Under Windows NT, it performs a PWDump-like password hash dump, suitable for import into L0phtCrack.

### **Get System Info**

Returns information about the system, including machine name and the capacity of the storage devices attached to it.

### **Log Keystrokes**

Captures the keystrokes that the user of the server machine types at the keyboard to a disk file. Also tells you what windows they typed the keystrokes into, so you can understand what they were doing.

Parameters: Disk File (Required) - The full pathname of the file to put the keystroke logs into.

### **End Keystroke Log**

Stops logging keystrokes.

### **System Message Box**

Puts up a dialog box on the server screen. The dialog box appears on top of everything else and makes a beep sound.

Parameters: Title (required) - The text to put in the title of the message box.  
Text (required) - The body of the message that is in the message box.

### **Map Port -> Other IP**

Binds to a TCP port and redirects all traffic to that port over to a different IP address. You can use this command to 'bounce' TCP connections off of the BO2K server.

Parameters: Server Port (required) - The TCP port number that is to be redirected.  
Target IP Address:Port (required) - The destination of the port redirection.

### **Map Port -> Console App**

Binds to a TCP port and redirects the standard input and output from a console application to the port. This can be used to simulate a 'remote shell'.

Parameters: Port (required) - The TCP port number on the server to put the console on.  
Full command line (required) - The full command line of the program that you wish to execute.

### **Map Port -> HTTP Fileserver**

Serves HTTP requests over A TCP port. The HTTP server allows you to browse the filesystem of the server machine and the local network neighborhood. The HTTP server can be 'rooted' at a particular directory in order to restrict which files people can download and browse through.

**Parameters:** Port (required) - The port number to put the HTTP server on.  
Root Path (optional) - The optional root directory of the browsable filesystem.

### **Map Port -> TCP File Receive**

Receives a file that is sent to the chosen port via a raw send (such as with Netcat), and dumps it directly to a file. Useful as a quick-and-dirty, unencrypted, file transfer method.

**Parameters:** Port (required) - The port number to receive the file on.  
Pathname (required) - The pathname to receive the file to.

### **List Mapped Ports**

Returns a list of which ports on the server machine are mapped to which services.

### **Remove Mapped Port**

Removes a mapped port, stopping whatever service it was providing. Use this to turn off a console app spawn, the HTTP fileserver, TCP File Receive, etc.

**Parameters:** Port (required) - the port that the service you wish to stop was spawned on.

### **TCP File Send**

Sends a file directly from the server to a target machine via TCP. Suitable for send a file to another server running the "TCP File Receive" port service.

**Parameters:** Source Port (optional) - The desired source port on the server from which to send the file data. If you do not choose a source port, one will be selected at random.  
Target Address:Port (required) - The target machine's TCP receive service address.  
Pathname (required) - The name of the file on the server to send to the remote machine.

### **Add Share**

Shares a machine resource on the server. Right now limited to drives/paths.

**Parameters:** Pathname (required) - The pathname that you want to share to the world.  
Share Name (required) - The name that you wish the share to be known as.

### **Remove Share**

Unshares a machine resource on the server.

**Parameters:** Share Name (required) - The name of the share that you wish to remove.

### **List Shares**

Lists which shares on the system are available and which paths/resources they map to. Also shows hidden shares.

### **List Shares on LAN**

Enumerates the shares on the server's local network. Like network neighborhood.

### **Map Shared Device**

Maps a share on a remote machine to a local drive letter. Much like 'mounting' a remote share.

**Parameters:** Local Name (required) - The local name of the shared device (Drive letter).  
Remote Share Path (required) - The UNC Pathname to the remote share  
Username:Password (optional) - The username/password pair used to share this device if the machine is in "share password" mode.

### **Unmap Shared Device**

Unmaps a share on a remote machine from a local drive letter. Much like 'unmounting' a remote share.

**Parameters:** Local Name (required) - The local name of the shared device.

### **List Connections**

Lists which machines are connected to the server, using shared resources.

### **List Processes**

Shows the process list for the server machine, with process names and process identifiers. Optionally on Windows NT, you can specify the name of an alternate Windows NT machine to dump the process table of remotely.

**Parameters:** Remote machine (optional) - The machine name of the Windows NT machine to retrieve the process table of.

### **Kill Process**

Abruptly terminates a running process on the server machine given its process ID. A list of process IDs is returned by the previous 'List Processes' command.

**Parameters:** Process ID (required) - The process ID of the process you wish to terminate.

### **Start Process**

Starts a process by running an executable file on the server.

**Parameters:** Pathname and arguments (required) - The command line of the program to execute.

### **Create Key**

Creates a registry key. Does not set a default value to the key.

**Parameters:** Full Key Path (required) - The full path from the base of the registry to the key. The HKEY abbreviations are supported in the key path, for example: "HKLM\Software\Microsoft\Windows" is a valid key, where HKLM is an abbreviation for HKEY\_LOCAL\_MACHINE. Valid abbreviations are: HKCR, HKU, HKLM, HKCU, and HKDD.

### **Set Value**

Creates and/or sets the value of a registry key.

**Parameters:** Full Key Path (required) - The full path from the base of the registry to the key.  
Type:(Value Name):Value Data (required) - This string is comprised of three sub-parameters: Type can be one of B,D,S,M, or E. Value Name is the name of the value, and Value Data is the type-specific data to be stored in the key. Valid data formats follow:

*B - Binary data type: Value data is formatted as a series of hexadecimal bytes. Eg: B:(rubber ding dong):CD C3 13 37 12 34 56 78*

*D - DWORD data type: Value data is either a hexadecimal dword (preceded by '0x') or a decimal dword. Eg: D:(booga boo):16823049 or D:(booga boo):0xD34DB33F*

*S - String data type: Value data is an escaped C string. Valid escape sequences are the same as in C, such as \n, \r, \0, etc. Eg: S:(message):Bite my ass.\nYeah, you.*

*M - MultiString data type: Value data is a series of escaped C strings, separated by a null character. Eg: M:(twomessages):Bite my ass.\0Also, bite your own.\0*

*E - ExpandString data type: Value data is a regular string that performs environment variable expansion. Eg: E:(path):c:\\mybutt;d:\\yourbutt;%path%*

### **Delete Key**

Deletes a key from the registry. Deletes all values and keys underneath the target key as well.

**Parameters:** Full Key Path (required) - The full path from the base of the registry to the key. See above for description.

### **Delete Value**

Deletes a value from a registry key.

**Parameters:** Full Key Path (required) - The full path from the base of the registry to the key. See above for description.  
Value Name (required) - The name of the value within the key to delete.

### **Enumerate Keys**

Lists the single-level subkeys of a particular registry key.

**Parameters:** Root Key Path (required) - The full path from the base of the registry to the key you wish to enumerate subkeys of. See above for description.

### **Enumerate Values**

Lists the values of a particular registry key.

**Parameters:** Full Key Path (required) - The full path from the base of the registry to the key you wish to enumerate values of. See above for description.

### **Capture Video Still**

Captures a video image bitmap from a video capture device, such as a Quickcam, or external cameram, and saves it to a disk file.

**Parameters:** Device # (required) - The number corresponding to the video capture device to capture from. A list of capture devices can be retrieved with the 'List Capture Devices' command below.

Filename (required) - The full pathname of the BMP file to capture the video image to.

Width, Height, BPP (optional) - The width and height of the image to capture, along with the bitmap bit depth. Defaults are 640x480x16bpp.

### **Capture AVI**

Captures a motion video from a video capture device and saves it to the local drive (uncompressed).

**Parameters:** Device # (required) - The number corresponding to the video capture device to capture from. A list of capture devices can be retrieved with the 'List Capture Devices' command below.

Filename (required) - The full pathname of the AVI file to capture the video sequence to.

Seconds (optional) - The number of seconds to record to the AVI file. Default is 5 seconds.

Width, Height, BPP (optional) - The resolution of the video stream to capture, and the bit depth, Defaults to 160x120x16bpp.

### **Play WAV File**

Plays a WAV audio file through the system default mixer.

**Parameters:** Filename (required) - The full path name the .WAV audio file to play.

### **Play WAV File In Loop**

Plays a WAV file over and over again. User won't be able to stop the sound. To stop the sound, use the 'Stop WAV File' command below.

**Parameters:** Filename (required) - The full path name the .WAV audio file to play.

### **Stop WAV File**

Stops whatever audio file is being played through the default mixer.

### **List Capture Devices**

Lists the video capture devices in the system, giving each an index number to refer to them by.

### **Capture Screen**

Captures the desktop screen to a disk file. Like pressing printscreen, pasting into a paint program, and saving to disk.

**Parameters:** Filename (required) - The full path name of the file to save the screen image to.

### **List Directory**

Displays a directory listing of files, their dates and times of creation, and their sizes. Also shows attributes.

**Parameters:** Pathname (required) - The full pathname from the filesystem root to the desired directory.

### **Find File**

Given a directory and a wildcard file specification, recursively hunts down all files beneath or at the specified directory matching the filespec criteria.

**Parameters:** Root path (required) - The full pathname from the filesystem root to start searching at.  
Filename Spec (required) - The filename wildcard specification to match. Accepts standard '\*' and '?' wildcards.

### **Delete File**

Deletes a file via its full pathname.

**Parameters:** Pathname (required) - The full pathname from the filesystem root to the file to delete.

### **View File**

Views the contents of a text file through the command response window. Useful for browsing small text files.

**Parameters:** Pathname (required) - The full pathname from the filesystem root to the file to view.

### **Move/Rename File**

Moves a file from one pathname to another. Renames a file if the paths point to the same directory. Can be used to move a file across filesystems and networked machines.

**Parameters:** Pathname (required) - The full pathname from the filesystem root to the source file to move.  
New Pathname (required) - The full pathname from the filesystem root to the destination file.

### **Copy File**

Copies a file from one pathname to another. Can be used to copy a file across filesystems and networked machines.

**Parameters:** Pathname (required) - The full pathname from the filesystem root to the source file to copy.  
New Pathname (required) - The full pathname from the filesystem root to the destination file.

### **Make Directory**

Creates a directory. Will only create one directory at a time.

**Parameters:** Pathname (required) - The full directory name, ending in the directory to create.

### **Remove Directory**

Removes a directory. Will only remove one directory at a time and will not remove files within a directory.

**Parameters:** Pathname (required) - The full directory name, ending in the directory to create.

### **Receive File**

Creates encrypted/authenticated socket and receives a file over it. Uses a proprietary transfer protocol, but it's simple and its not FTP (pew!).

**Parameters:** BINDSTR,NET,ENC,AUTH (opt) - The ubiquitous BO2K binding string specification. Specifies which port, network protocol, encryption type, and authentication type. Any field can be left blank to use the defaults.  
Pathname (required) - The full pathname to the file that will be received.

### **Send File**

Creates encrypted/authenticated socket and sends a file over it. Uses a proprietary transfer protocol, but it's simple and its not FTP (pew!).

**Parameters:** Address(required)[,NET,ENC,AUTH] (opt) - The ubiquitous BO2K connect string specification. Specifies which address to connect to, also specifies network protocol, encryption type, and authentication type. Any field except address can be left blank to use the defaults.  
Pathname (required) - The full pathname to the file to send.

### **List Transfers**

Lists which transfers are active to which files over which ports. Lists transfers started with receive, send, or emit file commands.

### **Cancel Transfer**

Cancels a file transfer either in progress, or one that has not yet started. Cancels transfers started with receive, send, or emit file commands.

Parameters: Pathname (required) - The full pathname to the file associated with the transfer to cancel.

### **Freeze File**

Compresses a single file. Not compatible with the original Back Orifice Freeze File procedure, but employs slightly better compression this time.

Parameters: Pathname (required) - The source pathname from the filesystem root to the file to compress.

Output Pathname (required) - The output pathname from the filesystem root to the file to write the compressed output to.

### **Melt File**

Uncompresses a single file that has been compressed with "Freeze File". Not compatible with the original Back Orifice Freeze File procedure.

Parameters: Pathname (required) - The source pathname from the filesystem root to the file to uncompress.

Output Pathname (required) - The output pathname from the filesystem root to the file to write the decompressed output to.

### **Resolve Hostname**

Resolves a host name to a network address using a DNS query.

Parameters: Hostname (required) - The hostname string to resolve.

### **Resolve Address**

Resolves a network address to a hostname using a DNS inverse query.

Parameters: Address (required) - The network address to reverse-resolve.

### **Shutdown Server**

Shuts the BO2K Server down completely. The server will lose all connections and will be unresponsive (cause it isn't running!).

Parameters: DELETE option (optional) - If you fill this field in with the phrase 'DELETE', it will fully uninstall the BO2K server such that it doesn't run any more upon boot-up or login. Does not remove the actual installed file, however. It just won't run on startup.

### **Restart Server**

Shuts down and restarts the BO2K Server. Useful if you have made any configuration changes or if the BO2K server has been corrupted or is behaving strangely due to poorly written plugins or whatnot. The server will lose all connections but will remain responsive once it comes back up.

Parameters: Host process name (optional) - If you are running under Windows NT, and not as a service, you can choose to hop the BO2K server around between different processes' address space. This is of limited usefulness, but it does make you feel like the 'ghost in the machine'.

### **Load Plugin**

Dynamically loads an external BO2K plugin DLL. Runs all of the plugin initialization code and registers new commands with the server.

Parameters: Plugin filename (required) - The full pathname from the root of the filesystem to the plugin DLL you wish to load.

**Debug Plugin**

Dynamically loads an external BO2K plugin DLL using a more debugger-friendly loading method. This method requires that the DLL is a standard Windows DLL, but allows for debugger interaction with the plugin. For developers only.

Parameters: Plugin filename (required) - The full pathname from the root of the filesystem to the plugin DLL you wish to load.

**List Plugins**

Gives a list of which BO2K plugins are currently loaded.

**Remove Plugin**

Unloads a plugin via its plugin number. Plugin number is determined from the output of the "List Plugins" command.

Parameters: Plugin number (required) - The plugin number to unload as returned by the List plugins command.

**Start Command Socket**

Starts up a BO2K command socket that a client can connect to, authenticate with, and send encrypted commands to.

Parameters: [NETMOD][,ENC][,AUTH] (optional) - the network module, encryption, and authentication settings for the command socket. If any of these are left blank, defaults are used.  
[Bind Str] (optional) - The binding string for the command socket. This is optional, but is usually filled in. If it's not, then the default binding string is used.

**List Command Sockets**

Lists the command sockets that the BO2K server has made available. Lists socket information along with the internal 'command socket #'.

**Stop Command Socket**

Shuts down a BO2K command socket. This can be used to shut down all sockets, btw. And that's probably not a good idea.

Parameters: Command Socket # (required) - The number of the command socket to shut down, as returned by the 'List Command Sockets' command.



## BUTT TRUMPET 2000

### Remote E-Mail tool for Back Orifice 2000

BT2K - VERSION 1.2

by Brian Enigma

#### Overview

This DLL (with source code) is a plugin for Back Orifice 2000. It duplicates the functionality of the original Butt Trumpet plugin for the original Back Orifice, plus adds some more.

This plugin has been designed to send an email message to you, the administrator, after BO2K has been successfully installed on a client machine. It allows you to easily keep track of who is remotely administratable.

#### Installation

BT2K is strictly a server side plugin. There is no client component. To create a new server with BOred included perform the following steps:

- 1) Run bo2kcfg.exe
- 2) Create a bo2k server, following the BO2K directions (either using the wizard, or directly with the configuration tool)
- 3) Once you see the "BO2K Server Configuration" tool, you will need to click on "Open Server..."
- 4) Select the server you have, typically "bo2k.exe"
- 5) Click on "Insert..." under plugins
- 6) Select "BT2K.dll"
- 7) You will now see "Butt Trumpet 2000" in the plugins list
- 8) Configure the server, as listed below.
- 9) Select "Save Server"
- 10) Exit

The server is now ready to load on to a computer.

#### Configuration

Configuration is relatively easy. Under the ServerConfiguration utility, look at the "Option Variables" tree. Toward the bottom, you should see a folder for "Butt Trumpet 2000." In this folder, you can set the following options (be sure to click on the "Set Value" button after typing in the new value):

- *Destination Email* - This is the address that automated messages are sent to. This can be the administrator account on your company's LAN. It could be your ISP email account. It could be a Hotmail account. If you are doing something "shady" with Back Orifice, you may want to consider using some anonymous remailers and Hotmail-like accounts.
- *Mail Server* - This is the mail server to use. It can be fairly tricky to find the proper value here. If you are using your ISP email account, put the ISP's mail server here (for instance mail.myprovider.com). If you are using a web-based email account, you must put in the address of their MAIL SERVER, and not their WEB SERVER. The unix-savy can use a tool such as "dig" to perform a DNS query for the service's MX record. The rest of you can try to find a similar tool for Windows (Good luck! I have yet to find one. Although, if you do happen to know of a port of "dig" for Windows, PLEASE let me know!) or use any of the following values\*:

hotmail.com	->	mail.hotmail.com
yahoo.com	->	mx1.yahoo.com
hushmail.com	->	www.hushmail.com
rocketmail.com	->	mta1.rocketmail.com
altavista.net	->	spool.globecomm.net
angelfire.com	->	mta1-mail.angelfire.com
juno.com	->	a.mx.juno.com
mailcity.com	->	mta5-mail.mailcity.com

*\*At the time of this writing, the above mail servers were correct. I cannot guarantee that they will be correct at any later date.*

ALSO: Be aware that some mail servers, in an effort to prevent spamming will only allow you to send to addresses that exist in their mail system. Unless you really know what you are doing, be sure that the mail server you use matches up with the email address you use.

- *Send Delay* - Defaults to 10 minutes. When the BO2K server is first started, it attempts to send a message. If it cannot send a message, it will repeatedly delay this amount of time and attempt a resend until the email message is successful. While this number can be as low as 1 minute, it is advised to keep it to 5 or 10 minutes--this causes less network traffic.
- *Repeat Process* –  
Disabled: Only one email message will ever be sent out from the BO2K'ed machine. Although you can manually send more using the "Debug:Resend Message" command).  
  
Enabled: A message will be sent each time the BO2K server is started. In other words, each time the computer is rebooted!
- *Message* - A piece of text to send in the notification message. Most likely, you will want to use it as a note to yourself. It will help you remember what computer or BO2K server sent the message. You can also use it as a reminder of what port and password the server uses. You can type whatever the hell you want here.

### Usage

As soon as Back Orifice 2000 is launched on the remote computer, the email action is performed. From the BO2K GUI, you can perform the following operations:

- *Debug:Show* - Displays the debug log of exactly what is going on with the plugin.
- *Debug:Clear* - Clears the debug log
- *Debug:Resend Message* - This will cause the remote machine to send an email message immediately. If you have the remote machine set up to send an email message only once, this will cause the machine to "forget" that it has done so. Hence, it will send again until successful.

### E-Mail

The email message that gets sent to you contains the following pieces of information:

- The logged in user's username
- The computer's name
- The date/time
- A custom message (see "Message" above in the configuration section)
- The IP address or addresses that are bound to the computer. A maximum of six will be displayed.

### Future Features

In the future, I would like to add the following features:

- Pull the dialup networking information from the registry. Basically, this will send the user's login name, dialup phone number, DNS settings, and possibly password in the email message.

### Links

BO2K is available at <http://www.bo2k.com/>

The latest version of BT2K is at <http://www.netninja.com/bo/>

Contact information is at <http://www.netninja.com/enigma/email.html>

### Change Log

Version 1.2 from 1.1

- Added a configuration parameter to determine the retry time value.
- Added checking so that if the local IP address is nothing or "127.0.0.1," then hold off sending.

- Added better error reporting during SMTP sending. If the send failed, you can connect via the debug command and see exactly why and where.

Version 1.1 from 1.0

- Modified the calls to the IP collection routine [myIP(char \*)], so that it is called each time a message send is attempted. The previous implementation only did this at startup. This resulted in dialup machines not being able to record their IP address (because it has not yet connected).
- Modified the internals of btWorkerThread(void \*) so that if the email send fails, it retries 10 minutes later. The old version retried every ten seconds (Yikes!). Yeah, I was tired and smoking crack.
- Modified the Debug:Resend command [CmdProc\_DebugResendCommand(...)] and the worker thread [btWorkerThread(void \*)] so that when a resend is requested and a worker thread is already running, instead of spawning a second worker thread, it simply zeros out the timer on the existing thread.

### **BACK ORIFICE BUTTPLUGS AND GOODIES FAQ (FREQUENTLY ASKED QUESTIONS)**

It seems the software I have written for Back Orifice has achieved quite a lot of popularity. Initially, I started writing personal responses to each person that had a question or comment about the plugins/goodies. Unfortunately, the time has come for me to use an automated system--the amount of mail I get each day about this software has gotten to be unmanageable.

If you wrote with a comment, thank you. I personally read each and every piece of mail I get (even though I cannot personally reply to all of it). If you wrote with a question, the answer will be in the following FAQ (I compiled the list of questions and answers from the messages I have received in the past week or two).

Thanks for showing an interest!

-E

Brian Enigma -----

<http://www.netninja.com/enigma.html>

"Painful pleasures turn to pleasing pain" -- Sir Edmund Spencer

### **Butt Trumpet**

Q: ....any question....

A: Before asking any questions, be sure to check if you have the latest version. At the time of this writing, 1.1 is the latest version number. Check <http://www.netninja.com/bo.html> for all updates and information!

Q: For some reason, BT is not sending out an email. I used the address of a web-based email system and my email address--or I used the address of my Internet Service Provider (ISP).

A1: Probably, the server you are using does not have a daemon listening for SMTP (email) traffic on port 25. This is a pretty typical situation. Just like web servers will usually have a "www.", mail servers will usually have a "mail." in front of them. For instance, hotmail uses "mail.hotmail.com." My ISP (let us call it "server.com") uses "mail.server.com."

A2: Some mail servers will not "forward" mail unless the source or destination is on that server. For instance, you would not be able to use "mail.hotmail.com" to get to "enigma@server.com." Conversely, you would not be able to use "mail.server.com" to get to "enigma@hotmail.com."

A3: BT might have already sent a message. If you feel comfortable using RegEdit, check for the key "HK\_Local\_Machine\Software\NinjaSoft\BT\RunSuccess." If it exists, then a message has already been sent (SOMEWHERE!). You will have to delete it and reboot the machine for BT to send another message.

Q: How do I get BT to send a message every time the user logs in?

A: See "A3" above. There is presently no automated way of doing this. In a future version, this will be an option.

Q: It still will not send a message

A1: Maybe you are not waiting long enough. BT waits about 5 minutes between retries, starting when you first turn on the computer (at which point most people do not have an internet connection. Maybe your timing is off?

A2: I would suggest checking your BOConfig install parameters. Be sure to call BT.DLL: \_start and be sure to use HOST,EMAIL as the parameter. Also, attach BT.DLL to the installer and have it copied to the system directory with the same name. Try connecting to the machine with BT installed. Invoke it manually (using the Plugin Launch command). The first argument is BT.DLL: \_start and the second is your HOST,EMAIL argument. See if an error message is returned. The plugin will return a "null string" if everything went well. If you get an error message involving a missing DLL, either (1) you have the wrong version, upgrade to 1.1 -or- (2) the victim has a problem with their TCP/IP DLL's (or does not have them installed).

A3: I do not know...it worked for me. It works for hundreds of other people. Maybe you are just weird. (Not that that is a BAD thing!)

### **SaranWrap**

Q: After setting up SaranWrap and testing it, my computer hangs

A: You probably used SaranWrap.EXE as the "real" program to run. (Did you copy SaranWrap.EXE to DATA2.Z? If so, you have a problem.). Try this: Find NOTEPAD.EXE and copy it to DATA2.Z (in the same directory as DATA1.Z and your, possibly renamed, copy of SaranWrap.EXE). Try testing again and it will work. Next time, rename some other .EXE file to DATA2.Z.

Q: When run, SaranWrap says "Cannot locate DLL xxxxxxxx.EXE"

A: Upgrade to the latest version. 1.0 had this problem on some machines. 1.1 has fixed it.

Q: Can I change the extension to something other than EXE?

A: Technically, yes...but probably, nothing would happen. The only way to run the program from a user interface (Explorer) is to let Explorer know that it is a program. [As an aside: through API calls, you can run a file with ANY extension as a program, but through Explorer, an email program, etc. it must have the proper extension]. Technically, you can use SCR (for screen saver, you can still double-click on it, but it won't run as a proper screen saver) or COM (no icon, but it will still run) or possibly a few others. DO NOT expect to be able to rename it to .WAV and have Media Player install it--that just will not work.

Q: After setting up SaranWrap and testing it on a Windows 95 system, someone goes to run the program on a Windows NT system. They get a Back Orifice error about "password enumeration." How do I make this stop?

A: This has been fixed in Silk Rope, but not yet in SaranWrap. I would suggest using Silk Rope instead.

### **Silk Rope**

Q: When I run SilkRope.EXE, I get an error message ("This file has been damaged or corrupted").

A: Read the directions. By itself, SilkRope.EXE does absolutely nothing (aside from spew out error messages). You **\*MUST\*** use SilkRopeBind.EXE to attach your Back Orifice installer and another .EXE program to SilkRope.EXE. Then you may rename SilkRope to whatever you wish and run it.

Q: After setting up Silk Rope and testing it, my computer hangs

A: You probably used SilkRope.EXE as the "real" program to run. (Did you type in SilkRope.EXE twice when running SilkRopeBind? If so, you have a problem.). Try this: Use SilkRope.EXE as the stub program, find NOTEPAD.EXE on your system and use that as the "real" program. Try testing again and it will work. Next time, use some other .EXE file in place of notepad.

Q: Can I change the extension to something other than EXE?

A: Technically, yes...but probably, nothing would happen. The only way to run the program from a user interface (Explorer) is to let Explorer know that it is a program. [As an aside: through API calls, you can run a file with ANY extension as a program, but through Explorer, an email program, etc. it must have the proper extension]. Technically, you can use SCR (for screen saver, you can still double-click on it, but it won't run as a proper screen saver) or COM (no icon, but it will still run) or possibly a few others. DO NOT expect to be able to rename it to .WAV and have Media Player install it--that just will not work.

Q: After setting up Silk Rope and testing it on a Windows 95 system, someone goes to run the program on a Windows NT system. They get a Back Orifice error about "password enumeration." How do I make this stop?

A: Upgrade to the latest version. This was fixed in 1.1.

Q: When attaching a BO installer with an embedded plugin to a file with Silk Rope, the embedded DLL plugin gets copied to the SYSTEM directory, but the actual BO program does not. The user has to run the Silk Rope'ed program twice for everything to work properly.

A: I was only recently made aware of this and am not sure how wide-spread the problem is (or even the cause). I have never run across this problem, and am still researching it. If you have any additional information, please let me know. Also, if you have done this and have NOT had this problem, let me know--it will help me gather the number of working vs. nonworking situations and any special or funky circumstances that may be contributing.

### **Back Orifice**

Q: ....any question....

A: Try checking <http://www.cultdeadcow.com> or hang around in IRC.  
END

.....

## RATTLER V1.0

### Plugin For Back Orifice 2000

Copyright (c) 1999 by AdTropis - mataru@mail.airmail.net  
<http://wyrmssoft.tzo.net/rattler/>

Licensed under the GNU Public License (GPL)  
<http://www.gnu.org/copyleft/gpl.html>

### Introduction

Rattler is a Back Orifice 2000 plugin that sends e-mail messages to a specified user when the IP address of the Back Orifice host machine changes. This can be extremely useful for users who have Back Orifice servers running on dial-up machines and/or machines configured for DHCP.

### Files

The following files should be included in the Rattler plugin distribution zip file (Rattler10.zip):

Rattler.Dll - The plugin dll  
Rattler.Txt - This text file  
RattlerSrc.Zip - The source code to Rattle

The following files should be included in the Rattler source distribution zip file (RattlerSrc.Zip):

Rattler.cpp - Rattler C++ source  
Rattler.h - Rattler header file  
Rattler.def - DLL exports  
config.cpp - Config.cpp from BO2K SDK  
Rattler.dsw - Visual C++ workspace file  
Rattler.dsp - Visual C++ project file  
Rattler.Txt - This text file

If there are files missing, please refer to the official Rattler homepage to download the full distribution.

### Installation

Installation is a snap. Simply unzip the 'Rattler10.zip' file into any directory. Then copy the 'Rattler.Dll' file to your Back Orifice 2000 plugin directory. Now when you create server installation packages you can insert the 'Rattler.Dll' plugin into the server package.

If you want to tweak parts of Rattler (or whatever) simply unzip the 'RattlerSrc.Zip' file into a separate directory. A Visual C++ workspace file is included for easy development in Visual C++ 5.0/6.0.

### Plugin Configuration

When the plugin is inserted into a server installation package, there are several parameters that need to be set to ensure proper usage of the plugin. Each parameter can be accessed by using the Rattler menu Configuration parameters are listed below:

**BOOL**        **Run On Plugin Load:** Rattler will startup when the plugin is loaded

**NUMERIC**    **Query Delay:** Specifies the number of seconds to wait between each IP check

**STRING**     **Mail Host:** Specifies the SMTP (not POP!) mail host to use in order to send e-mail messages

**NUMERIC**    **Mail Port:** Specifies the port number of the SMTP mail host to use (probably won't need to change it)

**STRING**     **Mail From:** Specifies the name to use in the 'From:' field of the e-mail message

STRING	<b>Rcpt To:</b> Specifies the name to use in the 'To:' field of the e-mail message (must be a valid e-mail address!)
STRING	<b>Subject:</b> Specifies the subject of the message when an e-mail message is sent
NUMERIC	<b>Retries:</b> Specifies the number of connection retries when send an e-mail message
NUMERIC	<b>Retry Delay:</b> Specifies the number of seconds to wait between connection retries.
BOOL	<b>Notify On Startup:</b> If TRUE Rattler will send an e-mail after it has retrieved the first IP address block. If FALSE, Rattler will only send an e-mail after an IP address change has been detected.
BOOL	<b>Notify Local Hosts:</b> If TRUE Rattler will send an e-mail message for local network IP address changes (* see below for more on local networks addresses)
BOOL	<b>Use Debugging:</b> If TRUE Rattler will send messages to a debugging file (specified by 'Debugging File')
STRING	<b>Debugging file:</b> Specifies the location of the debugging file to use (* see below on debugging)

### Server-Side Configuration & Options

Rattler also allows for 'dynamic' configuration once it is loaded into the Back Orifice server. Once the Back Orifice server is started, just log into it with the client program and then you can change all of the Rattler options through the Rattler menu. Here is a list of the menu options:

<b>Status</b>	Shows the status of the Rattler plugin as well as the number of attempted messages and messages sent and the current state of the IP table. It also allows a user to manually send an e-mail message immediately.
<b>Configuration</b>	Shows the current configuration set for the Rattler plugin. Also allows the user to load the default configuration is desired.
<b>Config: Status</b>	Allows the user to shutdown or startup the Rattler service. Also allows for toggling the 'Run On Load' option.
<b>Config: Host</b>	Allows for configuration of the SMTP mail host to send mail to. The port and server name can be changed.
<b>Config: Users</b>	Allows for changing the names in the 'MAIL FROM' and 'RCPT TO' options
<b>Config: Subject</b>	Allows configuration of the subject to be sent in each e-mail that is sent by Rattler.
<b>Config: Options</b>	Allows the user to change the current connect retry count, the 'Notify Startup' option, and the 'Notify Local' option.
<b>Config: Delays</b>	Allows for changing the 'Query Delay' and 'Retry Delay' options.
<b>Config: Debug</b>	Allows for enabling/disabling debugging and changing the location of the debugging file.

All changes take effect immediately. However, when changing the 'Notify Local' option, a mail message will NOT be sent unless a local IP is changed or the user does so manually.

All options are also stored in the registry so that any configuration changes will be in effect the next time that the plugin is started. All options are stored under:

HKEY\_LOCAL\_MACHINE\SOFTWARE\WormSoft\Rattler.

### Client Side Operations

Rattler is a server-side-only plugin. There are no client options that can be set.

### How It Works

Basically the operation of Rattler is very simple. It simply obtains a block of IP addresses that correspond to the machine on which it is running. If there have been any additions to this IP table Rattler sends an e-mail message containing the current IP table to a pre-defined recipient.

By default Rattler does not send e-mail regarding changes to local network addresses. But just what is a local network address? Well, the first (and, hopefully, most obvious) is, of course, localhost (127.0.0.1). However, there are three other sets of network addresses that I call local:

10.0.0.0	MASK 255.0.0.0	Class A
172.16.0.0 - 172.31.0.0	MASK 255.255.0.0	Class B
192.168.0.0 - 192.168.255.0	MASK 255.255.255.0	Class C

These three network addresses are supposed to be used on LANs that do not have a direct connection to the internet. Therefore, I consider them local.

Of course, by setting the 'Notify Local' option to TRUE, changes to local network addresses will make Rattler send an e-mail message (this might be good for machines that are configured for DHCP).

### Debugging

You probably won't have to use the debugging option until you run into problems. Be prepared, though. The debugging option will generate a lot of messages, especially if the query delay is set to a low value.

If you use the debugging option and notice that there is a fault in the Rattler plugin, please let me know and I'll fix it as fast as I can.

### Development

The source code provided in the Rattler distribution is free for you to modify according to the terms of the GNU Public License. Feel free to make any changes you see fit. If you do make changes, please send them to me. I would very much like to hear your comments on my work.

The 'Rattler.Dll' file was compiled using Visual C++ 5.0.

### Conclusion

Thanks go out to The Cult of the Dead Cow for making Back Orifice as well as Brian Enigma for his work on Butt Trumpet 2000 (from which I got a few snippets of code).

Questions or comments? Please send me an e-mail: [mataru@mail.airmail.net](mailto:mataru@mail.airmail.net)

Enjoy!  
AdTropis

.....

## STCPIO STEALTHY TCP IO

### Plugin for Back Orifice 2000

Version 1.2, August 23rd, 1999

Copyright (C) 1999, Daniel Roethlisberger

#### Description

This is a plugin for the remote administration suite Back Orifice 2000 (BO2K) from the one and only, the Cult of the Dead Cow (cDc). Released at DEFCON 7, BO2K was subject to massive hype even weeks before the actual release of it.

When using the standard IO modules (TCPIO and UDPIO) that come with BO2K, the network traffic can be easily identified as BO2K data. There is security software around that can identify BO2K packets by traffic analysis.

Stealthy TCPIO (STCPIO) on the other hand generates traffic that is unidentifiable as BO2K traffic. This is extremely helpful if you run BO2K on a network with high end security software. With STCPIO, the software wont create bunches of false alerts when you administer a server using BO2K.

There is absolutely no way to identify a STCPIO packet as BO2K traffic for sure. So far, ISS have not come up with any way to do so.

#### What's New?

v1.2, August 23rd 1999 Strengthened security a lot at the cost of speed and 500 byte filesize.

v1.1, August 22nd 1999 Changed the key generation procedure for improved security.

v1.0, August 21st 1999 First release. Is a little too bulky yet for my taste.

#### Usage / Installation

Add the plugin to both the client and the server, be sure to configure matching packet header encryption engines and ports. You should now be able to select STCPIO from any IO module drop-down menu, and you can specify STCPIO in any IO module setting; where you specified TCPIO you can now use STCPIO.

***Please be sure to use STCPIO both in the client and the server, otherwise it wont work (surprise, surprise).***

I suggest using my CAST-256 strong encryption plugin along with STCPIO for top security.

#### Tech Stuff

Any BO2K traffic can be identified as such if sent through the standard TCPIO and UDPIO modules. The reason: they send a packet header (length field) \*unencrypted\* along the way. So when analysing sniffed traffic in a network, you can take the first DWORD of a packet, assume it the length of the following data, and if there is in fact exactly that much data following, you know it's a BO2K packet. This technique is used by the ISS network security software, and possibly others as well.

STCPIO does two things:

Firstly, it adds a random number of randomly generated bytes between the header and the data, enlarging the header by one byte (the length of the random data).

Secondly, but more importantly, it encrypts the whole header by XORing it with a special 5 byte header encryption key. This key is derived by encrypting the key string of the configured encryption engine with itself, and merging it down to 5 bytes.

The data length field is additionally XORed with a random key, which is sent in the packet after the random data, encrypted as well. This procedure makes identifying BO2K packets as such impossible, effectively hiding it from all network analysers, sniffers and similar security software.

There are three drawbacks however. Firstly, there is more overhead network traffic, that serves only stealth purposes. This amounts to between 0 and 255 bytes more per packet.

Secondly, STCPIO is a \*lot\* slower than TCPIO, due to the extra XORing and randomising code. And thirdly, the plugin enlarges the server considerably. This is due to the fact, that TCPIO and UDPIO are neither removable nor accessible by a plugin. STCPIO therefore has much code which is in TCPIO already, but cannot be accessed from a plugin. This could be changed by either incorporating STCPIO into the standard server completely, replacing TCPIO, or by removing TCPIO and UDPIO from the standard server and replace them by plugins of the same functionality. It is up to DilDog to decide so.

For details on how BO2K traffic can be detected, see the ISS X-Force's Security Alert on BO2K, which can be found at their website: <http://xforce.iss.net/alerts/advise31.php3>.

### **Legal Crap**

This software contains no strong encryption - it merely uses external encryption modules. Therefore this plugin constitutes no violation of the U.S. ITAR export regulations whatsoever.

### **License**

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

If you do redistribute or modify this plug-in, please let me know.

### **Thanx To...**

*DilDog - for answering (most) of my mails and for making BO2K possible  
the rest at cDc - for being the rest at cDc  
Maw~ and Ryan - for the developers talk  
Christian and Irwan - for the good bug reporting  
John, Graeme and the rest of the the crowd at alt.fan.cult-dead-cow - for keeping the newsgroup going*

### **Contact**

Daniel Roethlisberger  
E-Mail: <[admin@roe.ch](mailto:admin@roe.ch)>  
Web: [http://www.roe.ch/download/bo\\_cast.shtml](http://www.roe.ch/download/bo_cast.shtml)  
ICQ: 4646931

Get my PGP-Key with ID 0x8DE543ED at <ldap://certserver.pgp.com>.

**Visit the official BO2K site at <http://www.bo2k.com>.**

.....

## CAST-256 ENCRYPTION PLUGIN FOR BACK ORIFICE 2000

Copyright (C) 1999, Daniel Roethlisberger  
Version 2.4, August 3rd, 1999

### Description

This is a plugin for the remote administration suite Back Orifice 2000 (BO2K) from the one and only, the Cult of the Dead Cow (cDc). Released at DEFCON 7, BO2K was subject to massive hype even weeks before the actual release of it. This plugin adds *CAST6-256 encryption* capability to your BO2K, with or without CBC-Mode. The strongest available encryption for BO2K. As simple as that. Isn't that great?

### Security Considerations

CAST-256 offers the strongest encryption power known to Back Orifice 2000. CAST-256 uses user keys of 256 bits length (Comparison: TripleDES 168 bits, IDEA 128 bits). There are no known attacks against the algorithm. The plugin implements both ECB and CBC modes for either improved security (CBC) or more transport flexibility (ECB).

The Canadian algorithm CAST-256 is one of the candidates for the Advanced Encryption Standard AES, which will be the successor of the Data Encryption Standard (DES). I tested my CAST-256 implementation against the test vectors defined in RFC 2612 to ensure its validity, and I used the official MD5 reference implementation from RSA.

To sum it up: I would call CAST-256 absolutely secure at present and near future technology level.

### What's New?

v2.4, August 3rd 1999 - Using MD5 for determining initialization vector and abusing the initialization vector to XOR the data blocks in ECB mode. Improved security.

v2.3, August 1st 1999 - Password bug has been fixed. Cos I used Maw~'s faulty MD5 module, the password did not matter at all, dangerously. You should have me for being so stupid. I'm using the official implementation from RSA now.

v2.2, July 30th 1999 - Fixed eternally stupid bug disabling CBC-Mode. Updated old label returned by query. Silly me.

v2.1, July 29th 1999 - Support for passwords up to 256 chars long. Some bug fixes in MD5 module by Maw~ as well.

v2.0, July 28th 1999 - Did a complete implementation of CAST-256 from scratch (RFC) in place of CAST-128. First release. Great success. Scored 5 stars at bo2k.com, had hundreds of downloads in the first 24 hours.

v1.1, July 26th 1999 - Added CBC-Mode. Some bug fixes as well.

v1.0, July 25th 1999 - Used Norwegian implementation of CAST-128. Worked fine. I never released this version.

### Usage / Installation

Add the plugin to both the client and the server, be sure to configure matching key strings and check the CBC setting. You should now be able to select CAST from any encryption drop-down menu, and you can specify CAST in any Encryption setting. Please be sure to use CAST both in the client and the server, otherwise it wont work (surprise, surprise).

If you can't figure out how to add plugins I suggest you go to your local software store and acquire a copy of PC Anywhere [tm], so you wont have to coap with the tremendously difficult task of adding a plugin :-P

### ECB vs. CBC Mode

Many commonly used ciphers (e.g., IDEA, DES, Blowfish) are block ciphers. This means that they take a fixed-size block of data (usually 64 bits), and transform it to another 64 bit block using a function selected by the key. The cipher basically defines a one-to-one mapping from 64-bit integers to another permutation of 64-bit integers. CAST-256 uses blocks of 128 bits.

If the same block is encrypted twice with the same key, the resulting ciphertext blocks are the same (this method of encryption is called Electronic Code Book mode, or ECB). This information could be useful for an attacker.

In practical applications, it is desirable to make identical plaintext blocks encrypt to different ciphertext blocks. The Cypher Block Chaining (CBC) Mode does exactly that: a ciphertext block is obtained by first XORing the plaintext block with the previous ciphertext block, and encrypting the resulting value.

Thus the complete cypher stream is needed in order to decode. Any missing or displaced blocks and there's no chance of decoding it anymore. So if you are using unreliable means of transport, such as UDPIO, you should turn CBC Mode off.

### Algorithm

The CAST-128 cipher is described in "Constructing Symmetric Ciphers Using the CAST Design Procedure" by Carlisle Adams and in RFC 2144 "The CAST-128 Encryption Algorithm" also by Carlisle Adams. RFC 2612 "The CAST-256 Encryption Algorithm" offers an extension of the algorithm to key sizes up to 256 and block size of 128 bits.

The CAST encryption algorithm is a DES-like Substitution-Permutation Network (SPN) cryptosystem which appears to have good resistance to differential cryptanalysis, linear cryptanalysis, and related-key cryptanalysis. This cipher also possesses a number of other desirable cryptographic properties, including avalanche, Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), no complementation property, and an absence of weak and semi-weak keys. It thus appears to be a good candidate for general-purpose use throughout the Internet community wherever a cryptographically-strong, freely-available encryption algorithm is required.

CAST-256 is a 12-round Feistel cipher that has a block size of 128 bits and a key size of up to 256 bits; it uses rotation to provide intrinsic immunity to linear and differential attacks; it uses a mixture of XOR, addition and subtraction (modulo  $2^{*}32$ ) in the round function; and it uses three variations of the round function itself throughout the cipher. Finally, the  $8 \times 32$  s-boxes used in the round function each have a minimum nonlinearity of 74 and a maximum entry of 2 in the difference distribution table.

This cipher appears to have cryptographic strength in accordance with its key size (256 bits) and has very good encryption / decryption performance.

The 256 bit user key used by the CAST engine is constructed by  $\text{UserKey} = \text{MD5}(\text{string1} + \text{pwstring}) + \text{MD5}(\text{pwstring} + \text{string2})$ ; The Initialization Vector used by CBC/ECB modes is derived by  $\text{InitVect} = \text{MD5}(\text{string3} + \text{pwstring} + \text{string4})$ ; Whereby "+" denotes a concatenation.

### Legal Crap

Entrust Technologies / Nortel, under whose aegis the CAST algorithm was developed, have allowed free use of the algorithm for any purpose. RFC 2144, in which CAST-128 is described, states in paragraph 3:

*"3. Intellectual Property Considerations: The CAST-128 cipher described in this document is available worldwide on a royalty-free basis for commercial and non-commercial uses."*

RFC 2612, in which CAST-256 is described, states in paragraph 4:

*"4. Cipher Usage: The CAST-256 cipher described in this document is available worldwide on a royalty-free and licence-free basis for commercial and non-commercial uses."*

As this implementation was programmed using the RFC documents as guide and thus does not contain any code which was exported from the U.S., this plugin constitutes no violation of the U.S. ITAR export regulations.

I am a citizen of Switzerland, and my web server is located in Germany, so neither got anything to do with the US. But let's wait for Wassenaar - could change things a little to the worse :(

**License**

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

If you do redistribute or modify it, please let me know.

**Thanx To**

DilDog- for answering my mails and for making BO2K possible

the rest at cDc - for being the rest at cDc

Maw~ - for fixing the MD5 module very fast.

Graeme and the rest of the the crowd at alt.fan.cult-dead-cow for making information exchange possible.

Bernstein and the EFF - for having won a first law suit against the administration concerning the export regulations of crypto source code.

**Contact**

Daniel Roethlisberger

E-Mail: <admin@roe.ch>

Web: [http://www.roe.ch/download/bo\\_cast.shtml](http://www.roe.ch/download/bo_cast.shtml)

ICQ: 4646931

Get my PGP-Key with ID 0x8DE543ED at <ldap://certserver.pgp.com>.

Visit the official BO2K site at <http://www.bo2k.com>.

Over and Out

<<better than any handle>>



## SERPENT STRONG ENCRYPTION

### Plugin for Back Orifice 2000

Version 1.1, August 25th, 1999

Copyright (C) 1999, Daniel Roethlisberger

### Description

This plugin adds Serpent encryption capability to your BO2K, with or without CBC-Mode. The strongest available encryption for BO2K, exactly as secure as CAST-256, but a lot faster. Again: As simple as that. Isn't that great?

### Security Considerations

Serpent offers the strongest encryption power known to Back Orifice 2000. It is as secure as CAST-256. Serpent uses user keys of 256 bits length (Comparison: CAST-256 256 bits, TripleDES 168 bits, IDEA 128 bits). There are no known practical attacks against the algorithm. The plugin implements both ECB and CBC modes for either improved security (CBC) or more transport flexibility (ECB).

The British algorithm Serpent is one of the round 2 candidates for the Advanced Encryption Standard AES, which will be the successor of the Data Encryption Standard (DES).

I used a tested independant implementation of Serpent, and I used the official MD5 reference implementation from RSA.

To sum it up: I would call Serpent absolutely secure at present and future technology levels.

### What's New?

v1.1, August 25th 1999 Renamed to uppercase and fixed a bug causing it not to load on some systems.

v1.0, August 24th 1999 First release. Strong and fast encryption.

### Usage / Installation

Add the plugin to both the client and the server, be sure to configure matching key strings and check the CBC setting. You should now be able to select Serpent from any encryption drop-down menu, and you can specify "Serpent" in any encryption setting. Please be sure to use Serpent both in the client and the server, otherwise it wont work (surprise, surprise).

### ECB vs. CBC Mode

Many commonly used ciphers (e.g., IDEA, DES, Blowfish) are block ciphers. This means that they take a fixed-size block of data (usually 64 bits), and transform it to another 64 bit block using a function selected by the key. The cipher basically defines a one-to-one mapping from 64-bit integers to another permutation of 64-bit integers. Serpent uses blocks of 128 bits.

If the same block is encrypted twice with the same key, the resulting ciphertext blocks are the same (this method of encryption is called Electronic Code Book mode, or ECB). This information could be useful for an attacker.

In practical applications, it is desirable to make identical plaintext blocks encrypt to different ciphertext blocks. The Cypher Block Chaining (CBC) Mode does exactly that: a ciphertext block is obtained by first XORing the plaintext block with the previous ciphertext block, and encrypting the resulting value.

Thus the complete cypher stream is needed in order to decode. Any missing or displaced blocks and there's no chance of decoding it anymore. So if you are using unreliable means of transport, such as UDPIO, you should turn CBC Mode off.

### Algorithm

The main advantage of the algorithm is speed, at strong encryption power. Serpent provides users with the highest practical level of assurance that no shortcut attack will be found. To achieve this, the designers limited themselves to well understood mechanisms, so that they could rely on the wide experience of block cipher cryptanalysis. They also used twice as many rounds as are necessary to block all currently known shortcut attacks. They believe that this is prudent practice for a cipher that may have a service life of 50 years and continue to protect legacy data for a further 50 years beyond that, if selected as the AES winner.

Despite these exacting design constraints, Serpent is faster than DES. Its design supports a very efficient bitslice implementation, and the current fastest C version runs at over 26 Mbit/sec on a 200MHz Pentium (compared with about 15 Mbit/sec for DES).

The 256 bit key used by the Serpent engine is constructed by  $\text{UserKey} = \text{MD5}(\text{string1} + \text{pwstring}) + \text{MD5}(\text{pwstring} + \text{string2})$ ;

The Initialization Vector used by CBC/ECB modes is derived by  $\text{InitVect} = \text{MD5}(\text{string3} + \text{pwstring} + \text{string4})$ ; Whereby "+" denotes a concatenation.

### Legal Crap

The developers and patent holders have allowed free use of the algorithm for any purpose. This implementation does not contain any code which was exported from the U.S. illegally, thus this plugin constitutes no violation of the U.S. ITAR export regulations.

I am a citizen of Switzerland, and my web server is located in Germany, so neither got anything to do with the US. But let's wait for Wassenaar - could change things a little to the worse!

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

If you do redistribute or modify it, please let me know.

Daniel Roethlisberger

E-Mail: <admin@roe.ch>

Web: [http://www.roe.ch/download/bo\\_cast.shtml](http://www.roe.ch/download/bo_cast.shtml)

ICQ: 4646931

Get my PGP-Key with ID 0x8DE543ED at <ldap://certserver.pgp.com>.

## **BoTOOL**

Remote Filesystem Browser and Registry Editor

For Back Orifice 2000 Systems

Version 1.0 - Copyright (C) 1999, L0pht Heavy Industries, Inc.

### **Introduction**

BoTOOL is a client-side plugin for Back Orifice 2000 that provides two functions:

- A remote filesystem browser with a familiar interface.
- A remote registry editor with a familiar interface.

The remote filesystem browser provides functionality to encapsulate the normally complex and commonly used BO2K functions to:

- List files/directories
- Move files/directories
- Copy files/directories
- Rename files/directories
- Examine and modify file/directory attributes
- Transfer files from client to server and from server to client (upload/download) using a secure encrypted/authenticated channel.

The remote registry browser provides the functionality to:

- List keys/values
- Add keys/values
- Modify values
- Delete keys/values
- Rename keys/values

### **Installation**

1. Copy the BoTOOL.DLL to a place where you won't forget about it. The place where you installed the BO2K client is a good idea.
2. Run the BO2K client, go to the plugins menu and hit the configure option. Insert the BoTOOL.DLL. You won't have to insert this plugin into the BO2K server, since it uses only native BO2K commands and communication protocols.
3. Click on the BO Tools folder in the configuration panel and set up your command channel net module/encryption/authentication options to the settings you use most often to connect to BO2K servers (just like the server command client settings). Set up the file transfer options to match those specified in the server's file transfer settings. This will not matter too much, since the server can tell the client which protocols to use.
4. Hit OK, go to the plugins menu and select the tool that you want to use and go for it. For the network address, use the same address/port that you've always used to connect to your server. Same encryption, same authentication.

**Notes** *These tools should be REALLY easy to understand. Pretty much everything has a 'right-click' menu. Upload and download may be confused if you are using TCPIO through an SSH tunnel. Here's how to do that, by the way...*

### **SSH Tunneling for BO2K:**

1. Set up 2 SSH tunnels between your client machine and your server machine. One for the port you've got BO2K running on, and one on another random port. If you don't know how to do this, don't ask me. Figure it out. Let's assume your BO2K server is on port 10000, and you have a ssh

- tunnel from 10000(local)->10000(remote), and your extra tunnel is on port 13131(local)->13131(remote).
2. Since you're connecting -through- the ssh tunnel, you'll point all your BO2K server connections to 127.0.0.1:10000.
  3. When you're using the BOTOOL file transfer stuff (upload/download), you should note that when the BOTOOL filebrowser client tells the server which file it wants to download, the server picks a random port and tells the client where to connect. It will tell the server to connect to its ACTUAL\_IP\_ADDRESS:PORT. This would be instructing the client to transfer the file without using the SSH tunnel.
  4. To enforce the tunnel, you have to tell the server to always use the same port, in this case, 13131. And you have to tell the client, to always connect to 127.0.0.1:13131, since the server will be giving BOTOOL a different address, and you want the filebrowser client to ignore that.
  5. So, you can do this with the Connect/'Transfer Options' menu item in the BOTOOL filebrowser client. In this scenario, we would uncheck 'RANDOM BINDING STRING', and set 'Always connect to:' to '127.0.0.1:13131'. We would set 'Binding String' to '13131'. And there ya go. File transfer from Windows to Windows encrypted via BO2K, reencrypted, authenticated and tunneled through SSH.

### Gratuitous Sigh

AAAAAAHHHH! It's like having a really easy and integrated SCP for Windows.

### TO-DO

I'd like to implement Windows NT native security to this module. This will mean that there needs to be an NT native security plugin written for the server to give it more COMMANDS that take files and objects and other stuff, and let you manipulate the access control lists and other aspects of object security. Anyone up to this? I could do it, but hey, I got a lot to do :)

Last updated 8/2/99

.....

## **LIBERATOR v1.11**

(c) by Daniel Roethlisberger.

All Rights Reserved Worldwide.

For updates and info please visit the official Liberator website:

<http://www.datacomm.ch/roe/download/liberator.html>

### **INFO - *The ultimate protection against Back Orifice***

No installation needed, just unzip into any folder and run it. Liberator detects and removes installed BO servers, monitors vulnerable ports and sends a warning message back to the attacker. It also has a file/directory scanning feature. When a server is encountered on the system, it is automatically removed, without rebooting your computer, and the configuration is saved. The port it was configured to is then added to the list of monitored ports.

If a BO packet is received, of which the password is unknown, Liberator will decrypt the packet anyway and send the attacker a message back. This is using a brute force attack on the received packet.

The message sent to any attacker is configurable by the user.

The features are not very well documented, I know. Sorry for that! But believe me: if you're running Liberator, you are pretty secure from Back Orifice, and lamers will have a hard time against you.

### **KNOWN PROBLEMS**

AntiGen 1.0 (and possibly later versions) by Fresh Software will generate a false alert if you let it check your system for trojans while Liberator is running. This happens because AntiGen checks if port 31337 is available. If Liberator monitors the standard BO port (i.e. if socket monitoring is activated), AntiGen will generate an alert. You can safely disregard this infection warning from AntiGen.

#### ***Shut down Liberator when using AntiGen.***

If you're living near the date frontier (ie. GMT +1200), Liberator thinks you're in GMT -1200 instead of +. But as very few people live there, I have no intention of correcting this one. BTW: I got no idea how either... :-)

I had problems sending large answers to the attacker, thus making it impossible to send both the interntional and Swiss legal notice and a custom text at the same time. Liberator will disable the custom text if both legal notices are selected.

### **COMING SOME TIME IN THE FUTURE:**

- o Better support for the BO droppers Saran Wrap and Silk Rope
- o Improved directory open dialog
- o Improved system check technique
- o BackAttack (flooding, IP spoofing, ...)
- o Using low-level network protocols instead of WinSock
- o Documentation :-)
- o Other cosmetics

### **LICENSE INFO**

This software is Freeware. You are free to use this software for non-commercial purposes. For commercial use, please contact me for a quote. The software is provided as is, with no warranty whatsoever. Use it at your own risk.

### **HISTORY**

Version 1.11, 04-Feb-99

- o Optimised the brute-force attack
- o Better reports to the user

Version 1.1, 03-Feb-99

- o Finally given up the idea of supporting other trojans as well - there are hundreds of them around, making it impossible to implement all of them
- o Fixed some problems with the date/time-stamp in the log
- o Minor bugfixes

Version 1.02, 02-Feb-99

- o Liberator is now FREEware, not Postcardware
- o Brute-force-attack against encrypted BO packets

Version 1.01, 02-Nov-98

- o Changes to the warning message.  
Includes now the IP of an attacker (tnx to Duffy for this one!)
- o Welcome message box (or is it a nag screen?) at first run time
- o Enhanced About dialog.
- o Minor bugfixes

Version 1.0, 02-Nov-98

- o Initial release

**AUTHOR**

Daniel "Roe" Roethlisberger

ICQ-UIN: 4646931

E-Mail: liberator@roe.ch

PGP Key: 0x8DE543ED at ldap://certserver.pgp.com

Web: <http://www.datacomm.ch/roe>

Liberator: <http://www.datacomm.ch/roe/download/liberator.html>



# BO2K Encryption Module Comparison

By Daniel Roethlisberger

## Overview

To make it possible to compare the encryption plugins available so far, I have compiled a table with as much information on the plugins as possible. For complete understanding of that data some basic knowledge will be required. To make it look better I marked advantages green and disadvantages red.

The following speed information is based on benchmarks run on a Pentium-II/266 under NT4. The TripleDES and Blowfish benchmarks were run by a US citizen, as I am not allowed to download these files due to the U.S. ITAR export regulations. To be able to still compare the results I scaled those results accordingly to the performance of the others.

Some of the information provided is depending strongly on my personal opinion, but is largely based on what crypto professionals say. If you feel I am terribly mistaken, please notify me by email.

## The BO2K Encryption Modules

	<u>SERPENT</u>	<u>CAST</u>	<u>RC6</u>	<u>IDEA</u>	<u>BLOWFISH</u>	<u>3DES</u>	<u>XOR</u>
<b>GENERAL</b>							
<b>Filename</b>	bo_serpent.dll	bo_cast.dll	RC6Encrypt.dll	IDEAEncrypt.dll	Blowfish.dll	bo3des.dll	
<b>Version</b>	1.2	2.6	0.2	2.0	1.1	1.0	1.0
<b>Filesize</b>	45k	38k	44k	45k	28k	24k	N/A
<b>Rating</b>	*****	*****	*****	*****	****	****	N/A
<b>Origin</b>	Switzerland	Switzerland	UK	UK	US	US	US
<b>Avail.</b>	international	international	International	international	US/Can	US/Can	
<b>ENCRYPTION ALGORITHM</b>							
<b>Name</b>	Serpent	CAST-256	RC6	IDEA	Blowfish	TripleDES	XOR
<b>Origin</b>	UK	Canada	US	Switzerland	US	US	US
<b>Avail.</b>	free, patented	free, patented	Eval., patented	free use	free use	free use	free use
<b>ALGORITHM DETAILS</b>							
<b>Encryption Strength</b>	very strong	very strong	Very strong	strong	Strong	Strong	Weak
<b>Encryption Key Size</b>	256 bit	256 bit	384 bit	128 bit	8 to 448 bit	168 bit	32 bit
<b>Block Size</b>	128 bit	128 bit	128 bit	64 bit	64 bit	64 bit	32 bit
<b>CBC/ECB Modes</b>	both	Both	both	both	ECB	CBC	ECB
<b>HASHING PROCEDURE</b>							
<b>Max Key String Len</b>	255	255	255	255	56	45	45
<b>Hashing Algorithm</b>	MD5	MD5	Tiger	Tiger	None	MD5	simple
<b>Algorithm Strength</b>	Good	good	good	good	n/a	flawed	poor
<b>Performance</b>							
<b>Startup/Shutdown Speed</b>	8695/sec	6172/sec	10752/sec	14084/sec	717/sec	426/sec	200000
<b>Encrypt/Decrypt Speed</b>	6944/sec	4219/sec	22727/sec	3333/sec	12987/sec	450/sec	62500/sec
<b>Combined Speed</b>	5347/sec	3571/sec	8695/sec	4524/sec	698/sec	289/sec	76923/sec

### Please Note

1. **Combined Speed** consists of a typical BO2K packet encryption or decryption procedure (startup, encryption, shutdown).
2. Any **encryption speeds** like ~3000 and higher are more than sufficient, as BO2K will never be able to send that many packets a second.
3. **XOR** packets can be decoded without any computing effort by exploiting a weakness
4. **BLOWFISH**'s key strings are not hashed for key generation, the entered string is directly used as the encryption key schedule, resulting in a reduced keyspace and thus impact on security
5. The plugins in the table are **sorted by author**, and although better modules are generally found in the left half and less secure ones in the right half, that fact is purely coincidental. I personally suggest using **Serpent**, **CAST-256** or **IDEA** for encryption as things are at the moment. **RC6** is very good as well, but once an AES finalist will be chosen, the evaluation period will expire and using RC6 might become subject to special licencing.

**BACK ORIFICE: LISTING OF SOME AVAILABLE PLUG-INS, ADD-ONS, AND RELATED PROGRAMS**

<b>Name</b>	<b>Author</b>	<b>Size</b>	<b>Download Location</b>
-------------	---------------	-------------	--------------------------

**Encryption Plugins**

- |                                 |  |       |   |
|---------------------------------|--|-------|---|
| <b>Blowfish Encryption v1.1</b> | <a href="mailto:talis@fusion-solutions.com">talis@fusion-solutions.com</a> | 30 KB | <a href="http://www.fusion-solutions.com/">http://www.fusion-solutions.com/</a><br><i>This is a export-restricted encryption plugin that provides strong fast encryption using the Blowfish algorithm.</i>  |
| <b>CAST-256 Encryption v2.3</b> | <a href="mailto:admin@roe.ch">admin@roe.ch</a>                             | 63 KB | <a href="http://www.roe.ch/download/bo_cast.shtml">http://www.roe.ch/download/bo_cast.shtml</a><br><i>This internationally available plugin provides strong encryption using the CAST-256 algorithm. The strongest encryption available for BO2K.</i>                         |
| <b>Serpent Encryption v1.2</b>  | <a href="mailto:admin@roe.ch">admin@roe.ch</a>                             | __ KB | <a href="http://www.roe.ch/download/bo_cast.shtml">http://www.roe.ch/download/bo_cast.shtml</a><br><i>This internationally available plugin provides strong encryption using the Serpent algorithm. The strongest encryption available for BO2K and faster than CAST 256.</i> |
| <b>IDEA Encryption v0.4</b>     | <a href="mailto:maw@wynne.demon.co.uk">maw@wynne.demon.co.uk</a>           | 32 KB | <a href="http://www.wynne.demon.co.uk/maw">http://www.wynne.demon.co.uk/maw</a><br><i>This internationally available plugin provides strong encryption using the IDEA algorithm. A highly recommended download for people outside of the U.S. or Canada.</i>                  |
| <b>BO3DES v1.0</b>              | <a href="mailto:DilDog@L0phT.com">DilDog@L0phT.com</a>                     | 21 KB | <a href="http://secure.cultdeadcow.com:bo3des.zip">secure.cultdeadcow.com: bo3des.zip</a><br><i>Triple DES implementation in CBC mode. This plugin is only available for US download, but helps to secure a BO2K connection from end to end.</i>                              |

**Server Enhancement Plugins**

- |                   |  |       |  |
|-------------------|--|-------|--|
| <b>BT2K v1.1</b>  | <a href="mailto:enigma@netninja.com">enigma@netninja.com</a> | 40 KB | <a href="http://www.netninja.com/bo/index.html">http://www.netninja.com/bo/index.html</a><br><i>The Butt Trumpet 2000 plugin for BO2K. Once installed and started, this plugin sends you an email with the host's IP address.</i>                      |
| <b>BOred v0.1</b> | <a href="mailto:enigma@netninja.com">enigma@netninja.com</a> | 27 KB | <a href="http://www.netninja.com/bo/index.html">http://www.netninja.com/bo/index.html</a><br><i>The BOred plugin for BO2K. It is still in development, but will allow you to turn the BO'ed machine into not much more than a boring dumb terminal</i> |

**Client Enhancement Plugins**

- |                    |  |       |   |
|--------------------|--|-------|---|
| <b>BOTOOL v1.0</b> | <a href="mailto:DilDog@L0phT.com">DilDog@L0phT.com</a> | 76 KB | <a href="http://www.l0pht.com">www.l0pht.com</a><br><i>Provides a graphical file browser and registry editor to the BO2K interface. Makes common tedious BO2K tasks point-and-click simple.</i> |
|--------------------|--|-------|---|

**Multi-Purpose Plugins**

- |                     |  |       |   |
|---------------------|--|-------|---|
| <b>BO Peep v1.0</b> | <a href="mailto:DilDog@L0phT.com">DilDog@L0phT.com</a> | 50 KB | <a href="http://bo2k.com:bo_peep.zip">bo2k.com: bo_peep.zip</a><br><i>This plugin gives you a streaming video (VidStream) of the machine's screen that the server is running on. Also provides remote keyboard and mouse accessibility.</i> |
|---------------------|--|-------|---|

**BO2K Enhancements That Aren't Plugins**

- |                          |  |        |   |
|--------------------------|--|--------|---|
| <b>Silk Rope 2K v0.9</b> | <a href="mailto:enigma@netninja.com">enigma@netninja.com</a> | 158 KB | <a href="http://www.netninja.com/bo/index.html">http://www.netninja.com/bo/index.html</a><br><i>Silk Rope 2K! Bind your BO2K server to an existing program. New and improved! Now features: a full graphical user interface for setup and an target date for infection.</i> |
|--------------------------|--|--------|---|

**Coming soon!**

- |                         |  |         |  |
|-------------------------|--|---------|--|
| <b>BOPEEP Plus v1.0</b> | <a href="mailto:DilDog@L0phT.com">DilDog@L0phT.com</a> | ? bytes | <a href="http://www.l0pht.com">www.l0pht.com</a> (not public yet)<br><i>BOPEEP Plus is an enhanced version of the BO-PEEP remote desktop access tool. Should make Windows feel more like X-Windows... More on this as news breaks.</i> |
|-------------------------|--|---------|--|

- |                     |  |         |   |
|---------------------|--|---------|---|
| <b>BOSCRIP v1.0</b> | <a href="mailto:DilDog@L0phT.com">DilDog@L0phT.com</a> | ? bytes | <a href="http://www.l0pht.com">www.l0pht.com</a> (not public yet)<br><i>Scripting language support to automate tasks on both the BO2K client and the BO2K server. Perform timed operations of common functions and script together actions.</i> |
|---------------------|--|---------|---|

*Note: Check the BO2K website for up-to-date listings.*

**BACK ORIFICE 2000**  
**Show Some Control**

**THE CULT OF THE DEAD COW RELEASES BACK ORIFICE 2000**

**Press Contact:**

The Deth Vegetable, cDc Minister of Propaganda  
[veggie@cultdeadcow.com](mailto:veggie@cultdeadcow.com)

[July 10, Las Vegas] Today at Defcon 7, the CULT OF THE DEAD COW (cDc) unveiled its latest networked remote administration tool called Back Orifice 2000. This program is the most powerful application of its kind and puts the administrator solidly in control of any Windows-oriented network. Back Orifice 2000 evolved from Back Orifice - a pun on the Back Office server suite from Microsoft - released at last year's Defcon. So, you want to know more about this application?

- Back Orifice 2000 provides safe, secure, remote administration.
- Runs under Windows NT as well as Windows95/98
- Utilizes strong cryptography to ensure secure network administration
- Has extended plugin architecture to allow for greatest flexibility
- Is completely open-source and made freely available under the GNU Public License
- More powerful than any other remote administration tool for Windows available on the market

"It's a totally professional tool. Essentially it sews together Microsoft networks in ways that were never possible before," says Mike Bloom, Chief Technical Officer for Gomi Media, Toronto. "BO2K is a control freak's dream and the strong crypto feature gives the legitimate administrator a level of confidence that just didn't exist before. It's one kickass app."

Back Orifice 2000 was written by cDc code monster, DilDog, with input from Sir Dystic, the originator of Back Orifice. "When it comes to administering Windows networks, the most problematic thing has always been the lack of powerful remote control. Unix administrators have enjoyed remote logins for decades, and with the dawn of tools like Secure Shell (SSH), Unix systems can be securely administered from anywhere in the world. Windows needed it too. Now that we've enhanced the Windows administration experience, we hope that Microsoft will do its best to ensure that its operating systems are robust enough to handle the control we've given to them", said DilDog.

If last year's release of Back Orifice is any indicator, Back Orifice 2000 will be a huge success. The first generation app caused quite a stir with the hacking community and the press. The webmaster for the CULT OF THE DEAD COW reported a whopping 300,000 downloads from the primary and mirror sites, and predicts that Back Orifice 2000 will move briskly into the Microsoft networking environment.

That's good news for network administrators but not the best news for Microsoft. System administrators will have at their disposal a professional open-source application, free of charge. Unfortunately for Microsoft, Back Orifice 2000 could bring pressure on the software leviathan to finally implement a security model in their Windows operating system. Failure to do so would leave customers vulnerable to malicious attacks from crackers using tools that exploit Windows' breezy defenses.

Back Orifice 2000 is available for download free of charge from <http://www.bo2k.com/>

---

The CULT OF THE DEAD COW (cDc) is the most influential group of hackers in the world.

Formed in 1984, the cDc has published the longest running e-zine on the Internet, traded opinions with large software companies, and entered numerous dance competitions.

We could go on, but who's got the time?

For more background information, journalists are invited to check out our Medialist at <http://www.cultdeadcow.com/news/medialist.htm>.

Cheerio.

"Microsoft", "Windows", "Back Office", "Software", "Desk", and "Leviathan" are all trademarks of the Microsoft Corporation.

Blah blah blah, give it a rest already.

**"cDc. It's alla'bout style, jackass."**

Whew! Finally! And just as I ran out of room, too! - the Non-Compiler.