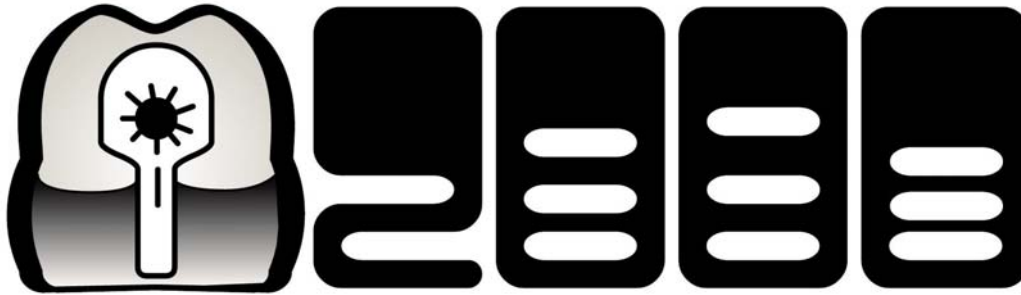


Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss



Back Orifice, or BO, is today's premier network administration tool for the Microsoft environment. It allows the network administrator to have complete power over a computer's functions, networks, registry, passwords, file system, and anything else. It in effect gives the administrator more power over someone's computer than the actual user. While the program does have great remote technical support potential, it also has more obvious destructive applications.

The program BO2K was written by DilDog of the hacking and phreaking group Cult of the Dead Cow and was based on the previous BO codes of SirDystic released in August '98 (also a cDc member). They provide this program absolutely free to download at their website www.bo2k.com. Not only does this program bring the abilities of the hacker into the next millenium, but it raises a number of moral and legal issues. Is Back Orifice legal? It certainly isn't ethical if it is used as a trojan horse virus to damage someone else's computer. The members of cDc liken its value to that of any 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...Hackers can use it to hack. Administrators can use it to make their lives a lot easier. " (bo2k faq)

So the members of cDc do concede that their creation of BO has dual purposes: "To enhance the Windows operating system's remote administration capability and to point out that Windows was not designed with security in mind."(bo2k faq) In true hacker fashion, cDc claims to be helping everyone out by displaying the security problems inherent in the microsoft operating system(windows 95, 98 or 2000), but are they doing more harm than good? Without a doubt.

With its small file size, stealth capability, configurability, and easy packaging BO has swept across the world. Many virus protection programs don't even pick it up yet. When used maliciously it is viewed as a trojan horse virus, in that it is packaged with a file or is a file that says it will do something else, not infect your computer, like an program or word document for example. The rumors that the virus is transferable through such attatched formats as JPG, GIF, BMP, WAV, and MP3 and currently spurious. A data file, such as an image or sound, is composed of binary data. This data is read in by an interpreter (for instance Photoshop, WinAmp, etc), which then outputs the data to your screen or speaker. No code is executed, therefore no executable can be attached. An executable file contains binary code that the computer executes in memory as a program. (www.netninja.com/bo/faq2k.html)

Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss



Back Orifice Applied

So what exactly can Back Orifice do? Well, what can't it do? It boasts a long feature list and an easy to use interface. Simply put, Back Orifice "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, and is more powerful than any other remote administration tool for Windows available on the market." (www.bo2k.com/release.html)

Each BO2K program comes equipped with the capability for remote keystroke logging, HTTP filesystem browsing and transfer (with optional restrictions), access to management of Microsoft Networking file sharing, direct registry editing, and direct file browsing, transfer, and management. And once the program is installed its easy to upgrade remotely or uninstall. The user can also redirect TCP/IP connections, access console programs such as command shells through Telnet, process NT registry passwords and Win9x screensaver passwords as well as all other cached passwords. BO2K allows multiple client connections over any medium, DNS name resolution, control over proprietary file compression, and provides multimedia support for audio/video capture, and audio playback. The remote user can also process control, start, stop, and list functions, create GUI message prompts, reboot, shutdown, or freeze the infected computer. The "client features" are an address book style server list, plugin extensibility, multiple server connections at once, a customizable look-and-feel, and complete session logging every time. (from www.bo2k.com/featurelist.html) While there have been programs before BO that have done similar things (like Netbus, for example), never has a program tied together so many features so well.

One of Back Orifice's main features is an open source architecture that is readily available to anyone who wants it. This ensures continued product development by members outside the group and lends itself especially well to the creation of new plug-ins. This source code availability also provides a trusted environment by letting all the prospective users see exactly what will be running on their machines.

While this program is already incredible with out the plug-ins, with the plug-ins the possibilities are greatly magnified. The standard XOR cryptography can be upgraded to the cryptographically stronger Triple-DES (3DES) encryption and recently way beyond that. The user can create an entire remote desktop with optional mouse and keyboard control of the infected computer. With the plug-in BOTool,

Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss

the administrator can perform drag and drop encrypted file transfers and have Explorer-like filesystem browsing or can do graphical remote registry editing.

One of the other plug-ins for Back Orifice is Silk Rope. This add-on binds your BO installer with a program of your choosing, saving the result as a single file. This allows the program to be given to people under a false guise and thus entirely covertly take control of their computer. This is also great for modifying single-file installs. Presently, the icon is the generic single-file-install icon (an opening box with a window in the background), but the Silk Rope authors are working on making it "steal" the icon from the original executable. So if you wanted to bind the BO installer program with another executable program, for instance, the entire merged file would take on the look of the legitimate executable. For now, the install icon can be changed with an icon utility such as Microangelo. This will let you select the icon that you want to represent the new merged file.

Saran wrap takes this deception one step further. It wraps BO to another program but after installing BO, will then run the other application too.

The plug-in ButtFunnel allows you to ping sweep for BO-Infected Computers THROUGH and infected computer. Thus, the ping sweep looks like its being ordered from the poor infected person and not the administrator.

ButtTrumpet will upon activation, will fire off an email to a predetermined SMTP server and email address (for instance, an anonymous remailer or a web-based email server). This way, victims could be infected via Usenet, without any knowledge ahead of time of who is being infected. A recently upgraded version automatically sends an email to you, the administrator, so that you can easily keep track of who is remotely administratable. Other similar programs are Rattler, RattlerSource, and RattlerClean.

The SpeakEasy plug-in is a simple, yet invisible, IRC client for BO. The basic functionality contained within Speakeasy is this: The administrator can initially set BO up with an IRC server, port number, and optional message. Once started, it attempts to connect to the IRC server until a connection can be established. It logs in with a random user name ("BO_" followed by 6 random letters) and then the channel #BO_OWNED is created/joined. An opening greeting is broadcast to the group and the user's IP address and message is repeatedly broadcast to the group every 2 minutes.

BOred will allow a BO administrator to turn a machine into not much more than a paper weight by removing the task bar and start menu through BO2K. These features can be easily switched off and on remotely.

Much has been made of the encryption for Back Orifice. The standard XOR encryption is not designed with security in mind. The 3DES cryptography option box is usually not available thanx to "our country's foolish and ignorant export laws." (BO2k Configuration Wizard) The three main encryption plug-ins available right now are the CAST256 plugin, the RC6 plug-in, and the STCPIO (which mutates the BO packets to make them untraceable). The best level of encryption easily downloadable all over the world is the IDEA algorithm plug-in which is 128 bits in length compared to TripleDES's 168.

The canadian encryption 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). "DES-like Substitution-Permutation Network (SPN) cryptosystem which appears to have good resistance to

Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss

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." As of now, this encryption has no known attacks, combining elements of both CBC and ECB modes for more improved security and easier transport and communication error tolerance. "CAST-256 is a 12-round Feistel cipher that has a blocksize of 128 bits and a keysize 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 8x32 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 keysize (256 bits) and has very good encryption / decryption performance." (<http://www.multimania.com/cdc/backorifice.html>) This same encryption program is packaged in the plug-in BO_serpent.

The RC6_Encrypt program claims to give the user the power to protect their BO2K session with 384-bit encryption.

The Stealth TCP IO encryption plug-in or "STCPIO" works when BO is configured to use the standard IO modules (TCPIO and UDPIO). Normally the network traffic can be easily identified as BO2K data. There exists 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.

A different type of elusive program is BOwhack, a new version of BO created by ecoli_@hotmail.com. Basically "ecoli" has just tinkered with the program code of the original BO so that McAfee Virus Scan can't detect it by registering itself as system.exe in the Windows registry. Another program, Deep Throat, uses much of the BO source code but includes many more features (www.sohons.com/deept/index2.html)

There do exist programs that serve to counteract Back Orifice infections. The program BOFreeze allows those infected to extract some revenge by sending malformed data packets back to the client using the correct encryption key causing major problems for the BO client user. They can cause "strange and fabulous characters" to appear on the screen..."effectively disabling the client completely because its packet buffer becomes full, and with the GUI client - that just freezes up completely!!!"

Another countermeasure is the program Liberator. This program will free the infected from the Back Orifice virus. More and more virus protection programs are scanning for BO as a Trojan Horse and eliminating it. Other types of programs try to identify BO and then let the infected user turn the tables. BOmaze is one of these programs. It is able to simulate the Back Orifice server part. That means if someone comes along searching your computer for an installed Back Orifice server, he/she will be presented something like a Back Orifice server - a program that looks like a Back Orifice server - from the outside. Unlike the real Back Orifice server, BOmaze does not execute the commands from the client but shows them to you. Further more BOmaze gives you the possibility to send messages back to the client. So bomaze is a tool that shows you what people would do on your computer if they could. Another similar version of this program is called BackFire.

Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss

BOspy also lets you find out who's trying to hack into your computer using Back Orifice and what they're trying to do. The author of this program warns not to install the program if the file size is about 122k. This goes for all the Back Orifice Plug-ins and related files because of the possibility of the Back Orifice server being misnamed or silkroped. Anyway, this program listens on port 31337 (the default BO port) and tells you the IP of the hacker and the port of their BOGUI.exe. BO Spy can be set to automatically answer the hacker with a predefined reponse to the hackers requests. "If the hacker pings you, BO Spy will send back a pong. If the hacker requests your passwords, fake passwords will be sent to him. Also, you can type any message you want in the "Message to be Sent" box and send it to appear in his BOGUI."(www.multimania.com/cdc/backorifice.html)

Since Back Orifice has so much plug-in extensibility it only makes sense that it would have other GUIs also. The most popular non-standard cDc GUIs are BackEnd, DeepBO, and BOFacil (a BO for the Spanish language).



Applications

While some of the applications for Back Orifice are obvious others are not. It is easy for most people to see the humor in making a dialog window pop up with some derisive comment about the victim and then making the victim press "Ok" to accept the comment but exactly how far can someone go? Obviously people store a great deal of information on their computers and by running a simple keylog, the remote user can usually ascertain almost all the password and/or sometimes credit card information they desire. By accessing any file on the computer, the administrator also has a view of any ideas, projects, plans, computer organizers, address books, and phonebooks so in a business setting this program can wreak massive havoc or atleast leak possibly vital information. As the use of computers as a financial tool increases so too does the amount of damage BO can do. What if someone is into E-trading or banking? A simple snatched password and the remote user has access to all on-line accounts. The possibilities are endless. From the hackers point of view Back Orifice opens up an entirely new realm in bouncing from place to place to cover up tracks. A hacker can open their server connection to their Back Orificed victim, then use their computer as a starting point for mischief. Just another small step in the direction of anonymity for the hacker. However, "BO's data packets are recognizable and traceable. Countermeasures are in increasing use. If you poke around looking for open Orifices long enough, your ISP is going to receive a complaint -- more likely multiple complaints -- from other ISPs and/or individuals who have traced your transmissions.

Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss

Regardless how innocent your actual intent, your ISP is justified in assuming you're up to no good if you're using the BO client. You'll probably lose your account, even if you've done nothing remotely illegal."

(www.nwi.net/~pchelp/bo/bolaw.htm)



What People are Saying...

Since having opened up endless avenues for mayhem, Back Orifice has generated quite a buzz in the information technology world. A Microsoft Security Advisory website warns that "BO2K is a program that, when installed on a Windows computer, allows the computer to be remotely controlled by another user. Remote control software is not malicious in and of itself; in fact, legitimate remote control software packages are available for use by system administrators. What is different about BO2K is that it is intended to be used for malicious purposes, and includes stealth behavior that has no purpose other than to make it difficult to detect." (<http://www.microsoft.com/security/bulletins/bo2k.asp>) The members of Cult of the Dead Cow come back with the argument that BO2K's stealth feature is an OPTION, which is in fact disabled by default. Warnings by Microsoft can further be dismissed because Microsoft, as it happens, also has a remote administration tool for windows, a program called SMS (Systems Management Server). Not only does SMS have a nearly identical stealth feature, it also has almost all of the other features as well. Why then does Microsoft object? Because Back Orifice is free and the Microsoft SMS is not. Microsoft naturally wouldn't want to lose clientele so they do their best to debunk BO. The SMS's stealth feature is even explained in a Word document available from the Microsoft website:

"Of all the operations that Systems Management Server allows you to do on a client, remote control is possibly the most "dangerous" in terms of security. Once an administrator is remote controlling a client, he has as many rights and access to that machine as if he were sitting at it. Added to this, there is also the possibility of carrying out a remote control session without the user at the client being aware of it. Thus, it is important to understand the different security options available and also to understand the legal implications of using some of them in certain jurisdictions...It is possible to configure a remote control from a state where there is never any visible or audible indication that a remote control session is under way. It has been made this flexible due to customer demands ranging from one end of this spectrum to the other. When configuring the options available in the Remote Tools Client Agent properties, due notice must also be taken of company policy and local

Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss

laws about what level of unannounced and unacknowledged intrusion is permitted." (www.microsoft.com/smsmgmt/techdetails/remote.asp)

While Microsoft puts down Back Orifice it hypocritically employs many of its features. Microsoft is not the only company that puts out software similar to Back Orifice though. The capabilities of Back Orifice are closely comparable to Symantec's PC Anywhere, Compaq's Carbon Copy 32, or Artisoft's CoSession Remote 32. The Cult of the Dead Cow puts out a web page where they compare the three tools at www.bo2k.com/comparison.html. Back Orifice is the only free program and it is also smaller, faster, and much more extensible. And 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." Even if Back Orifice does have its obvious destructive capabilities it also has the same constructive applications as legitimate tools on the market today, and is in this way the best choice for network administrators.

Legality -- Trespassing

Back Orifice's legality is another question. According to the CFAA (Computer Fraud and Abuse Act), last revised in 1994, there are three types of trespasses. Fraudulent trespass, destructive trespass, and reckless trespass. Fraudulent trespass mainly deals with "phone phreaking" and the maintaining of something of value in the process. If two people are sending a file to one another and a third party intercepts the document, that third party could stand in violation of this type of trespass by fraudulently acquiring the file.

Destructive trespass is defined by intentionally damaging another computer's files, network, or data, and causing atleast \$1,000 worth of damage during the course of one year. This type of trespass is punishable by jail time of up to 5 years.

Reckless trespass is basically the same as destructive trespass with the addendum that the damage caused doesn't have to be intentional. Breaking of this law can lead to a maximum of 1 year jail time.

As for federal laws, it seems that unauthorized entry (unless into a government system) is actually not illegal, assuming its non-malevolent. However, each state has its own laws regarding the matter. Some states put in "catch-all" type clauses that can get anyone for even attempting access because of the vague wording. Most states, however, have laws similar to the CFAA.

Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss



Back Orifice in Action

Back Orifice also features easy installation on both client and server machines, just download and run the "setup.exe" program. A user will first want to configure the specifications of Back Orifice. Run the "Bo2kcfg.exe" tool which will let the user choose exactly which features to enable. The filename that Back Orifice installs itself as, the port the server listens on, and the password used for encryption can all be configured using the Bo2kcfg.exe utility. If the server is not configured, it defaults to listening on port 31337, using no password for encryption (packets are still encrypted), and installing itself as ".exe" (space dot exe). (www.multimania.com/cdc/backorifice.html)

To install the server the server simply needs to be executed. When the server executable is run, it installs itself and then deletes itself. This is useful for network environments where the server can be installed on a machine simply by copying the server executable into the Startup directory, where it will be installed, then removed. Once the server is installed on a machine, it will be started every time the machine boots. To get a victim, there are websites up (<http://members.xoom.com/Netraam/>) or you can simply ping someone to get their IP address. Once they are connected to you through the opened server connection to upgrade a running copy of Back Orifice remotely, simply upload the new version of the server to the remote host, and use the Process spawn command to execute it. "When run, the server will automatically kill any programs running as the file it intends to install itself as, install itself over the old version, run itself from its installed position, and delete the updated exe you just ran."

The program is then entirely functional through the "Bogui.exe" (or Back Orifice Graphical User Interface) application. In this window, the user has many command options to choose from. To check the connection status click on the little computer icon at the left of the screen. This brings up a window that asks you for the Name of the Server, the address of the Server, and then asks you to choose a connection type (UDPIO or TCPIO), an Encryption method (XOR is usually the only one available with out any plu-ins), and an Authentication device (which should be Nullauth). To connect to a known IP address just enter it in the Server address section and click "Ok". The next window will then allow you to connect to the address and spawn the program, starting the potential mayhem. Once connected the user is presented with a variety of options to choose from.

Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss

The simple commands are the "Ping" and "Query" commands. The first sends a ping to the server. If the server is connected/alive, it will respond. The query is usually 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.

The system commands are "Reboot Machine," "Lock-up Machine," "List Passwords," and "Get System Info." All of these are pretty self-explanatory. The reboot machine command causes the server machine to be rebooted, temporarily killing your connection to the server. Locking-up the machine makes the server machine completely unresponsive. The mouse will not move, and the keyboard will not work. It brings the entire system grinding halt. This will also kill the connection because the protocol times out. The list passwords feature lists the passwords that are stored in the Internet Explorer password cache on Windows 9x machines. This will return the passwords your computer has stored if you have ever checked the 'Remember My Password' box. "Under Windows NT, it performs a PWDump-like password hash dump, suitable for import into the L0phtCrack program." (Back Orifice FAQ, www.cDc.com) The Get System Info command returns information about the system, including machine name, speed, and the capacity of the storage devices attached to it.

The next set of commands are dedicated to keystroke logging. The "Log Keystrokes" function 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. This command needs the parameters to which you want the keylog saved to (in full path name form). To End logging Keystrokes choose the "End Keystroke Log" function. The "View Keystroke Log" feature opens the file which you have saved the keystroke logging session to for the administrator's viewing. And the "Delete Keystroke Log" deletes what was logged. This feature is especially helpful for finding out passwords not associated with Internet Explorer or for other reasons not stored in a system cache.

The GUI folder contains the command "System Message Box." Selecting this feature puts up a dialog box on the server screen. The dialog box appears on top of everything else and makes a beep sound. This feature provides laughs in many Back Orifice screen shots. The user must enter a title and a text and whatever is entered will pop up on the infected's screen. Some comical examples of this are at (<http://members.xoom.com/burnttoast/bo/index.html>)

The TCP/IP functions revolve around port mapping. These features can be used to "bounce" TCP connections off the BO2K server to hide your location. The "Map Port" command binds to a TCP port and redirects all traffic to that port over to a different IP address. To do this requires the TCP port number that will be redirected and the target IP address. The "Console App" will create a "remote shell" by redirecting the standard inputs and outputs from a console application to the port. Mapping an "HTTP Fileserver" will allow an administrator 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. The "TCP File Receive" program simply allows the administrator to transfer a selected file over a selected port. "List Mapped Ports" will return a list of which ports on the server machine are mapped to which services. And finally the "Remove Mapped Port" will do what it says, stopping whatever service it was providing. This often governs and stops all the other port mapping commands in service. "TCP File Send" sends a file directly from the server to a target machine via TCP. These features are some of the most widely used by hackers. The ability to grab files from an unsuspecting

Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss

infected server or even use the server as a starting off point for more hacking mischief is one of the reasons for BO's immense popularity.

The Microsoft Shared Networking folder (or M\$ Networking) contains the programs "Add Share," "Remove Share," "List Shares," "List Shares on LAN," "Map Shares on LAN," "Map Shared Device," "Unmap Shared Device," and "List Connections." The add share command shares a machine resource on the server (currently limited to drives/paths) and likewise, the remove share command unshares the resource. List Shares lists all the shares that are available on the system and which paths they corresponds to. List Shares on LAN restricts its list to the server's Local Area Network (i.e. network neighborhood). "Map Shared Device" maps a share on a remote machine to a local drive letter. This feature will require the shared file/system and the drive or location to which the client would like to map it. The "Unmap Shared Device" undoes this operation. The list connections command shows which machines are connected to the server using shared resources. Not only does the hacker now have access to your computer, but total access to every computer that has shared information with you.

List processes shows the process list for the server machine, with process names and process identifiers. The kill process Abruptly terminates a running process on the server machine given its process ID. In order to perform this operation a proper process ID is required. The start process command starts a process by running an executable file on the server. These Process Control features are what a hacker will use to run new programs or where a remote technical support administrator might perform a virus scan.

The Registry system gives the administrator access to reset keys and values. Create Key will allow the user to create a registry key. They do this by specifying the path "HKLM\Software\Microsoft\Windows", for example, where HKLM stands for "H Key Local Machine." This setting could be abbreviated using HKCR, HKU, HKLM, HKCU, OR HKDD. To set a value of a key the administrator can toggle the Set Value option. The type can be one of either B, D, S, M, or E, where B stands for Binary data type, D for DWORD data type, S for String data type, M for MultiString data type, and E for Expand String data type. A further description is given in the Cult of the Dead Cow's Back Orifice press release...

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%

The Delete Key function deletes a key from the registry and the Delete Value function deletes a value from a registry key.

The Multimedia capabilities are almost endless with BO. Everything from capturing video stills with a device like a Quickcam or other external camera to playing wav files at any point during connection. The picture grab function is even customizable upto what size picture you would like to take. The

Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss

administrator can also capture avi if the video capture device is connected and save it to the local hard drive. The default record length is 5 seconds and the dimensions are preset but everything is customizable. The administrator could also annoy the infected server by playing WAV files, or looping WAV files so the user won't be able to stop the sound. The administrator is the only one who has control over this with the Stop WAV File command. The List Capture Devices command retrieves a list of the video capture devices that are available, and the Capture Screen option saves the desktop screen to a disk file. This feature is very commonly utilized by the recreational hacker and displayed as a trophy of created mischief on various websites.

The File Directory lets the administrator look at all the files on the users computer and allows the administrator to view, copy, delete, move, rename, or even toggle the file's attributes. This directory also features a find file search feature, an option to create new directories, receive files (through an encrypted/authenticated socket using a proprietary protocol), send files (same transfer protocol), list all file transfers, and even cancel all pending or current file transfers.

The Compression tools are Freeze File, which compresses a single file, and Melt File, which uncompresses a single file.

The DNS options available are the resolution of the hostname, which uses a DNS query to yield a host name to a network address, and resolution of address, which resolves a network address to a hostname using DNS inverse query.

The server control functions give power to Shutdown the server, Restart the server, Load Plugins, Debug Plugins, List the Plugins, Remove Plugins, and play with the command sockets. Shutting down the server causes the machine to lose all touch with its network. Start Command Socket Starts up a BO2K command socket that a client can connect to, authenticate with, and send encrypted commands to. List Command Sockets Lists the command sockets that the BO2K server has made available (socket and number). And the Stop Command Socket shuts down a BO2K command socket.

"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.

"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."

Sources...

All images from <http://www.bo2k.com/indexnews.html> Back Orifice cDc Homepage

<http://www.cultdeadcow.com/tools/bo.html> Basic information, features list, gui image, download station...

Back Orifice 2000
The Ultimate Remote Network Administration Tool
by Thomas DeVoss

<http://www.nsclean.com/psc-bo2k.html> Privacy Software Corporation Security Advisory
Friday, July 16, 1999 BACK ORIFICE 2000 (BO2K) TROJAN HORSE PROGRAM

<http://www.cascade.net/bolinks2.html> BO Plugins, Screenshots and Fan Pages

<http://www.donkboy.com/html/bo.htm> Information on Back Orifice and Netbus, Tools, Processes, and Removal

<http://www.nwi.net/~pchelp/bo/bo.html> The Ultimate Back Orifice Page, contains absolutely everything

<http://www.microsoft.com/presspass/features/1999/07-08orifice.htm> Hackers Could Use "Back Orifice 2000" to Control Users' PCs

<http://www.multimania.com/cdc/backorifice.html>

<http://members.xoom.com/Netraam/>

<http://www.netninja.com/bo/index.html> Butt Plugs and Other Goodies, Saran Wrap, Silk Rope, Speak Easy...

http://www.phonelosers.org/back_orifice.html Tips on having fun with BO

<http://members.xoom.com/burnttoast/bo/index.html> Plenty of funny Screen Shots and Key Logs

email me... tomdevoss@aol.com