Global Information Assurance Certification Paper

Donald Dick 1.55

Ryan J. Maglich
August 2000

Name: Donald Dick 1.55 with Last Updated GUI Component from Version 1.53
Location: http://people.alt.ru/computers/donalddick/
Variants: Back Orifice, SubSeven, Netbus
Operating Systems: Microsoft 95/98/NT/2000
Protocols/Services: TCP/UDP, SPX/IPX
Brief Description: Donald Dick is a tool that allows a user to control another computer over a network. It uses client/server architecture, with the server residing on the victim's computer. The attacker uses the client to send commands via TCP or SPX to the victim listening on a predefined port.

Protocol Description:

The Donald Dick client connects to the server machine via two different protocols, TCP and SPX. TCP/IP is the most widely used protocol for interconnecting computers among LANs and the Internet. Some of the advantages of using TCP/IP are that the protocol offers broad connectivity for different types of computers, support for routing of packets, and a centralized domain assignment for connections between organizations. Another of TCP's abilities is to correctly order packets when the computer receives them according to their sequence numbers. Two of the biggest drawbacks of TCP/IP are: 1) it is relatively slow compared to other protocols such as IPX, and 2) the cost and effort needed to setup connections between global networks. The difficulty in setting up network connections also derives from the limit on total number of available addresses. One of the advantages to using UDP is its ability to do checksumming of packets to make sure nothing was changed in transit. Although this secures the information in transit, it adds to the performance overhead causing many people to turn it off.

SPX is a reliable, connection oriented protocol for communicating between computers. One of the features of SPX is that it uses IPX as a datagram service. While IPX packets are unreliable, SPX adds a service of packet acknowledgement. With this technique, packets are not repeated unless there is no acknowledgement of receipt. Some other advantages include ease of setup and fast connections. One of the disadvantages of SPX/IPX is that there is no centralized network numbering scheme. This would allow different networks to use the same set of addresses for computers, increasing traffic collisions and incorrectly routing packets. Another disadvantage of IPX is that it requires all links of the network to be able to handle 576 byte packets, therefore packets are limited to this maximum for safety.

Description of Variants:

There are several variants to this type of trojan. The three more popular variations are Back Orifice from Cult of the Dead Cow, SubSeven by mobman, and Netbus by UltraAccess.net. Back Orifice (BO) offers the user the most options.

Some features that are in BO but not in Donald Dick are:

- Open Source Framework
- Plugin Extensibility
- Keystroke Logging
- Data Encryption
- Remote Keyboard and Mouse Control
- Network Redirection of TCP/IP Connections
- Plus Many More.

Some of the advantages to Donald Dick are:

- Ability to use the SPX Protocol. (BO has a plugin coming for this soon though.)
- Configurability of the Server to Avoid Detection.

Some of SubSeven's advantages include:

- Messenger Spies (Like AIM)
- Greater Control Over Keyboard
- Various Server Protections
- IRC Bots and Other IRC/ICQ Connectivity
- Plus Many More.

The advantages that Donald Dick has over SubSeven are the same as those listed for BO.

Netbus also has some advantages over Donald Dick:

- Plugin Extensibility
- Application Redirect
- Control Keyboard
- Plus Many More

The advantages that Donald Dick has over Netbus are the same as those listed for BO.

Back Orifice can be found at http://www.bo2k.com
SubSeven can be found at http://subseven.slak.org
Netbus can be found at http://www.netbus.org

How The Exploit Works:

The creation of the server software revolves around two files. The first file is the initialization file called ddsetup.ini, which contains the default settings for the server and installer. The second file is ddsetup.exe, which constructs the installer file based on ddsetup.ini file.

There are many pieces to the ddsetup.ini file that determine the server's/installer's overall actions, ability to be detected, and setup. The first section determines the default

ports for the SPX and TCP protocols. The setup file can specify multiple listening ports for each protocol or it can disable a protocol by not listing any ports. If the ports are prefixed with a "B", then this port is also a datagram listening port, which is used by ddsfind, a port scanning/trojan finding tool.

The next section takes care of setting a password for the server to prevent unauthorized access. This section is followed by a setting, which will determine if the installer for the server will keep the settings of the previous installer when launching the server. After the installer is run, it has the ability to erase itself from the disk even though the default is to leave the installer alone.

The next main section details how to notify the attacker of the status of the server. The default setting specifies that no notification is sent, but logs can be sent by email, ICQ (although this was not implemented in the current version), or stored in a file local to the server. The log sent to the client contains the address of the victim for easy setup of the client. The server can send logs once during installation, when the server is started, or when the server crashes.

Following the notification setup is the section specifying the server name and loader name for Windows 95/98 and NT/2000. The default names for Windows 95/98 are nmiopl.exe, oleproc.exe, tsdm.dat, pnpmgr.pci, intld.vxd, and vmldr.vxd. The default names for Windows NT/200 are lsasup.exe, pmss.exe, samcfg.exe, and bootexec.exe. These files can be found in the \windows\system or \winnt\system32 directories, respectively. Also, all of the names must be 8.3 format. The names are difficult to detect because they resemble possibilities for names of real applications.

The next section lists the registry keys for the trojan for both Windows 95/98 and NT/2000. The default key, under HKEY_LOCAL_MACHINE, is System\CurrentControlSet\Services\VxD\VMLDR (or sometimes INTLD) for Windows 95/98. The default key for Windows NT/2000 is under HKEY_LOCAL_MACHINE at System\CurrentControlSet\Control\Session Manager. These keys are not removed when the installer is removed, unless the server is on a Windows 95/98 machine and the key is a VxD key. The value name for the server's parameters stored at these keys, defaults to dpdata. To use the Windows 95/98 loader's key to store server parameters then the key name must match the vxd file name. The last registry setting involves setting a value name for non-volatile chat storage and specifying a global event name for the server.

The last section allows for the specification of an Access Control List file name. This setting only concerns Windows NT/2000 NTFS file systems. The default listing is shdmp.dat. As shown by all the possible settings, the trojan can be hard to detect by simple file name scanning. Another layer of abstraction in the server is that the installer creator has the ability to change the byte order of the server, making it possible to bypass virus scanners.

The second file concerning the creation of the installation file is ddsetup.exe. This is the executable that actually creates the trojan installation program based upon the settings in ddsetup.ini. The output is a file called ddick.exe. This file can be renamed to whatever the attacker wishes, such as "KernelBufferOverflowPatch.exe".

There are two possible ways for the client to talk to the server. The simplest way to connect to the server is through the GUI client; the other method is to use the command line utilities. Please note that when looking at the GUI Client that the interface

has not been updated since version 1.53; the GUI uses version 1.55 of the client code with a non-updated version of the interface.

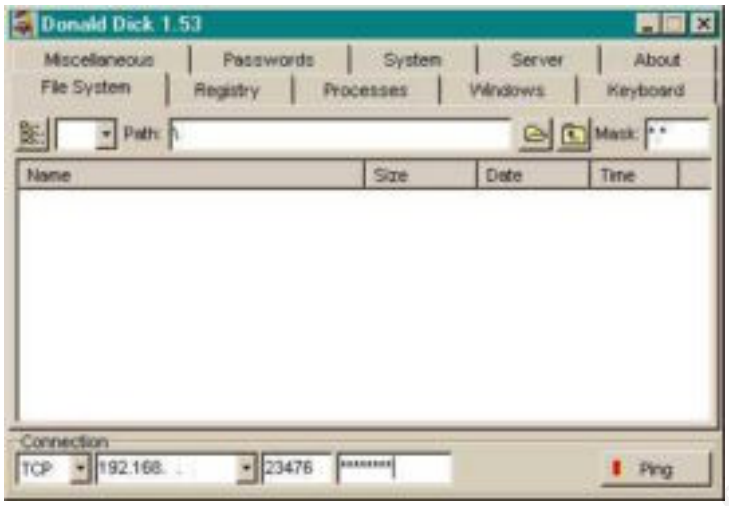


Figure 1

Figure 1 displays the overall layout of the GUI client. The bottom of the window allows the user to select the protocol, IP address of the server, the listening port and the password to connect to the server. When the user wants to connect to the server, the Ping button is pushed, when the connection is established, the light will turn green.

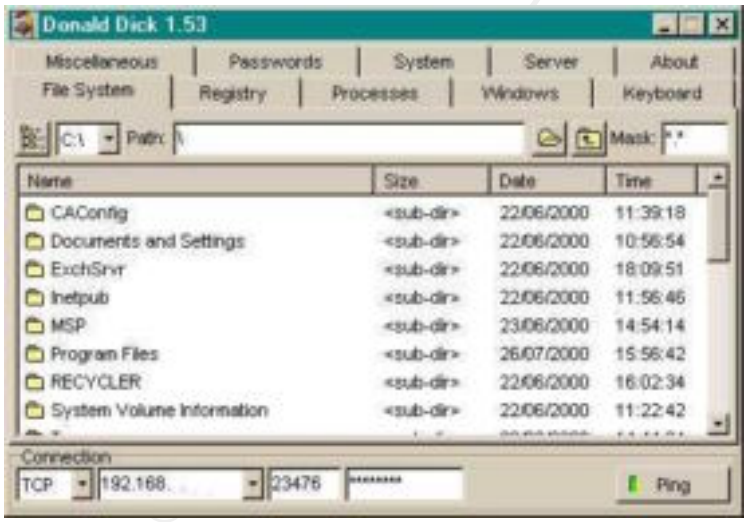


Figure 2

Figure 2 presents to the user information that can be retrieved from the server regarding the file system. From this window the client can copy, create, rename, and delete files, execute and start programs, send files to the printer, set the date and time of the file, and upload or download files. Also if the server is on a Windows 95/98 machine the client can set a folder to be shared. The client can select different drives and mask unwanted files or extensions to help limit the search for files.

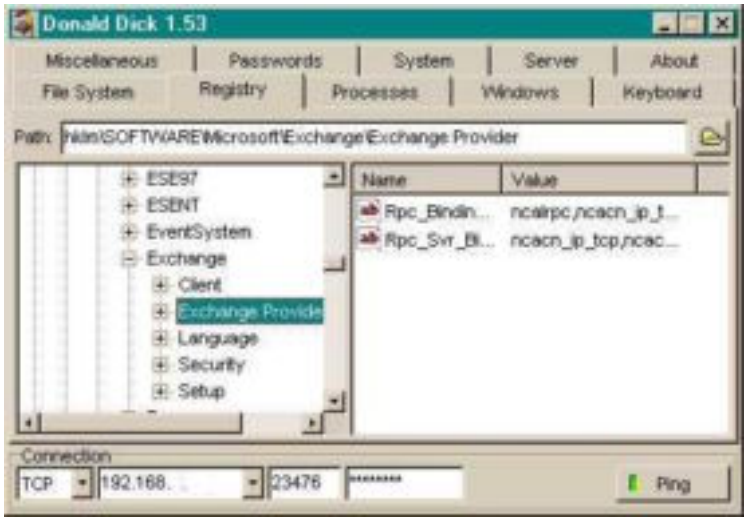


Figure 3

Figure 3 demonstrates the client's ability to obtain information from the registry. From here, the client can create subkeys or delete keys, as well as change, create and delete values or parameters.

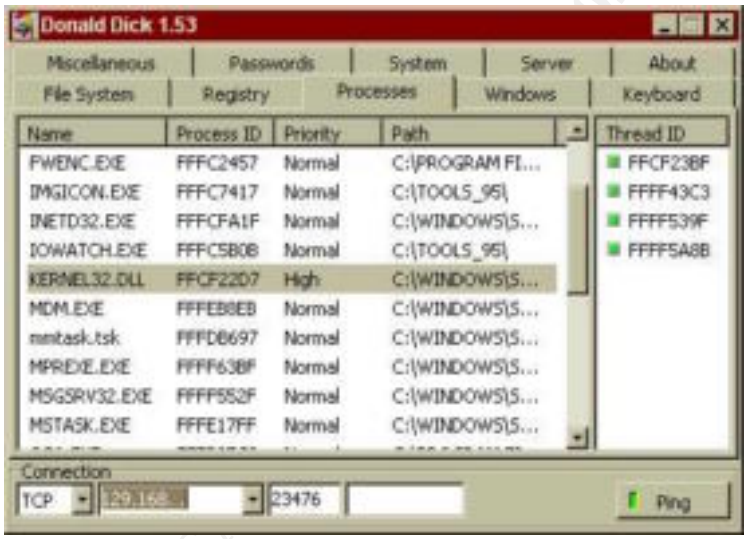


Figure 4

Figure 4 allows the client to view what processes what running on the server machine. The client has the ability to kill, change priorities, and create new processes. The threads can be suspended, killed, and resumed by right clicking each one listed for a process. Depending on which version of Windows the server is running, the results will vary. Figure 4 demonstrates the server being hosted on a Windows 98 machine. If the server were running on a Windows NT machine the information would be more cryptic with entries appearing like:

?????x?? 000003AC Normal <No Path>

The possibilities for controlling the processes remains the same, but distinguishing which process you want to control is more difficult.

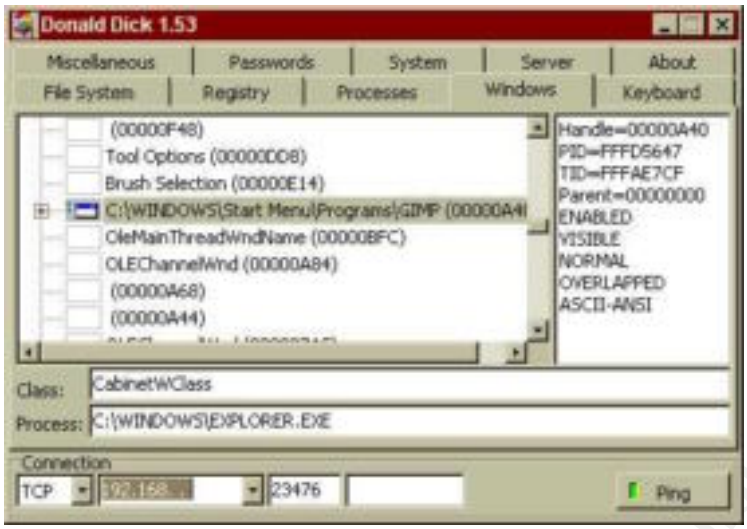


Figure 5

Figure 5 allows the client to view the window processes and their attributes. The client has the ability to close any window with a right mouse click. From this screen it is also possible to get a screen capture or a window capture.

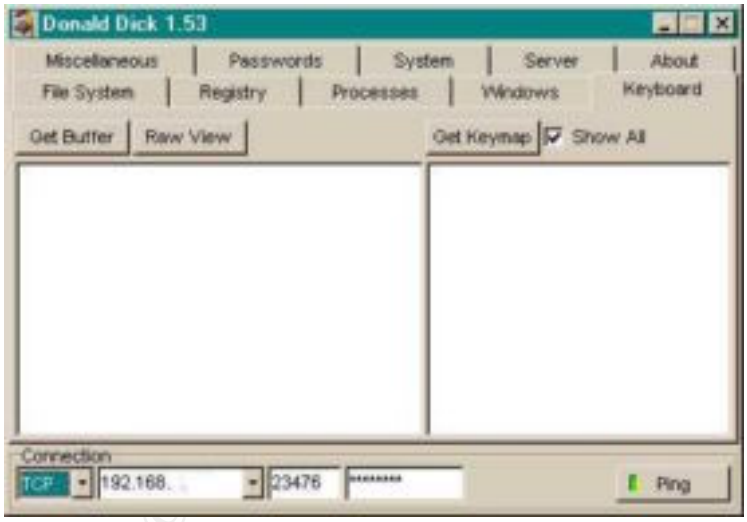


Figure 6

Figure 6 shows a feature for grabbing keystrokes. This ability has not yet been implemented for Windows NT in version 1.55. If the server is running on a Windows 95/98 machine, the client can simulate keystrokes, remap keys, disable keys, and view keyboard input.

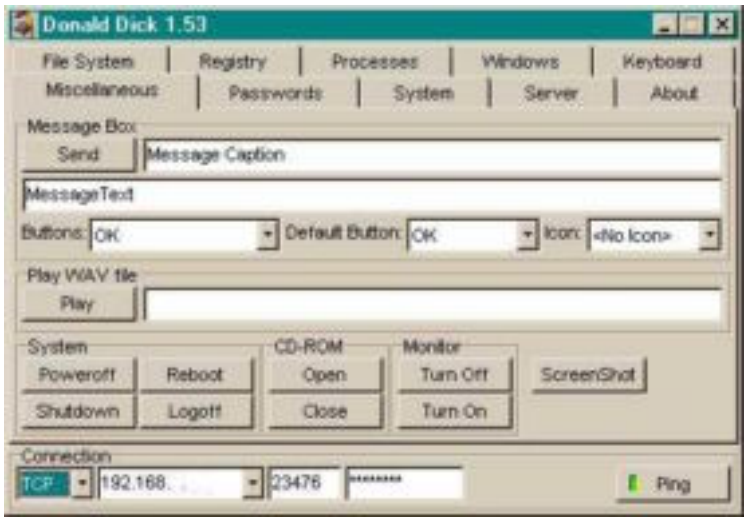


Figure 7

Figure 7 displays the capabilities found on the miscellaneous tab. The message box allows the client to send various warnings, questions, and information to the user. The client can specify the message and it's caption, along with various buttons. When the victim clicks on the buttons provided by the message box, the response is returned to the client. The client also has the capability to play wav files on the server's machine. The bottom third of the window allows the client to take control of the machine itself. The client can logoff users, reboot or power off the machine, open or close the CD-ROM, turn the monitor on and off, and grab a screen shot.

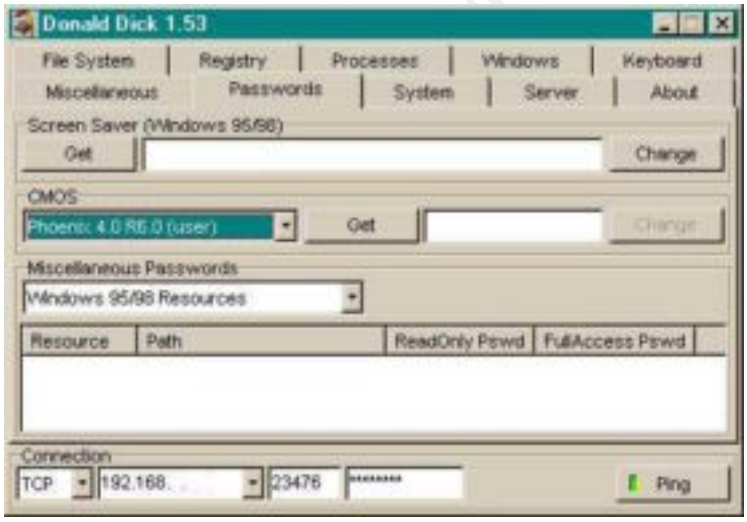


Figure 8

Figure 8 demonstrates the client's ability to grab and set passwords. When the client is installed on a Windows 95/98 machine the screen saver password can be obtained and changed. If the motherboard uses the Phoenix 4.0 R6.0 CMOS, the BIOS password can be obtained and changed too. In the bottom of the window, the server can

obtain passwords from various Windows 95/98 resources, CuteFTP, Windows Commander, and from FTP FAR Manager.

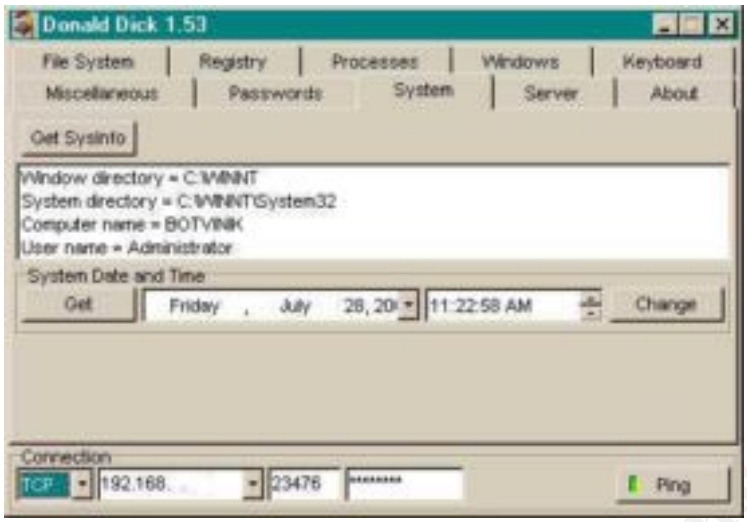


Figure 9

Figure 9 shows the information the server obtained about the host computer. With this information the client will see on what operating system the server is running, along with the name of the computer and who is currently logged on locally to the server. The client also has the ability to obtain and change the system date and time of the server computer.

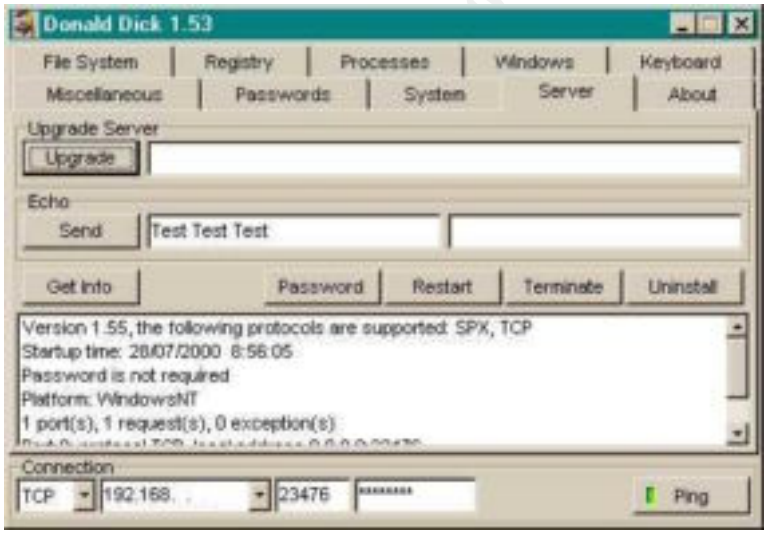


Figure 10

Figure 10 presents the client with a command line connection to the server. The same commands that are used with the CLI are used to upgrade the server through the GUI. The client can also send information to the echo port to test connectivity. The final portion of the tab obtains information about the server itself. The client can see the

version of the server, uptime, whether a password is needed, the host OS, IP addresses and ports. Finally the client can set the password for the server, as well as restart, terminate and uninstall the server.

Figure 11

Figure 11 demonstrates the About tab. This presents to the client the authors and the email address to use to contact the authors.

The next way to connect from the client to the server is by using the command line interface. Anything that is possible through the GUI is possible through the CLI. The format for the CLI is:

> <protocol> <address> <port> "<options>" <command> [<param1> < param2>….<paramN>]

The protocol parameter is either 0 for SPX or 1 for TCP. The address parameter is the address of the server machine and the port parameter is the port the on which server is listening. The options parameter allows the client to set delays for commands, specify the number of times to repeat the command and provide a password to access the server. A few examples of the commands are: SETPASS, TERMINATE, CREATEDIR, REMOVEDIR, GETPID, KILL, RUN, REGKEY, REGSETVAL, GETWINDOW, MSGBOX, SCREENSHOT, CLOSECD, MONON, and PLAY. There are many more commands and parameters listed in the readme.txt file that is supplied with trojan software.

A few example commands are:

1. To upload a file:
   client.exe 1 w.x.y.z 23476 "p=<password>" UPLOAD "c:\remote\file.exe" local_file.exe
2. To get info:
   Client.exe 0 220481132A7 0 "" INFO

3. To open CD-ROM tray 10 times but delay 10 seconds before execution and 20 seconds after execution:
   Client.exe 1 w.x.y.z 23476 "r=10 d=10000 D=20000" opencd

Another utility that comes with the trojan software is DDSFIND. Each server can have up to two datagram listeners for IPX and UDP protocols. The DDSFIND utility can send datagram packets to a specific host or a range of hosts and wait for a reply. The command line for this utility is:

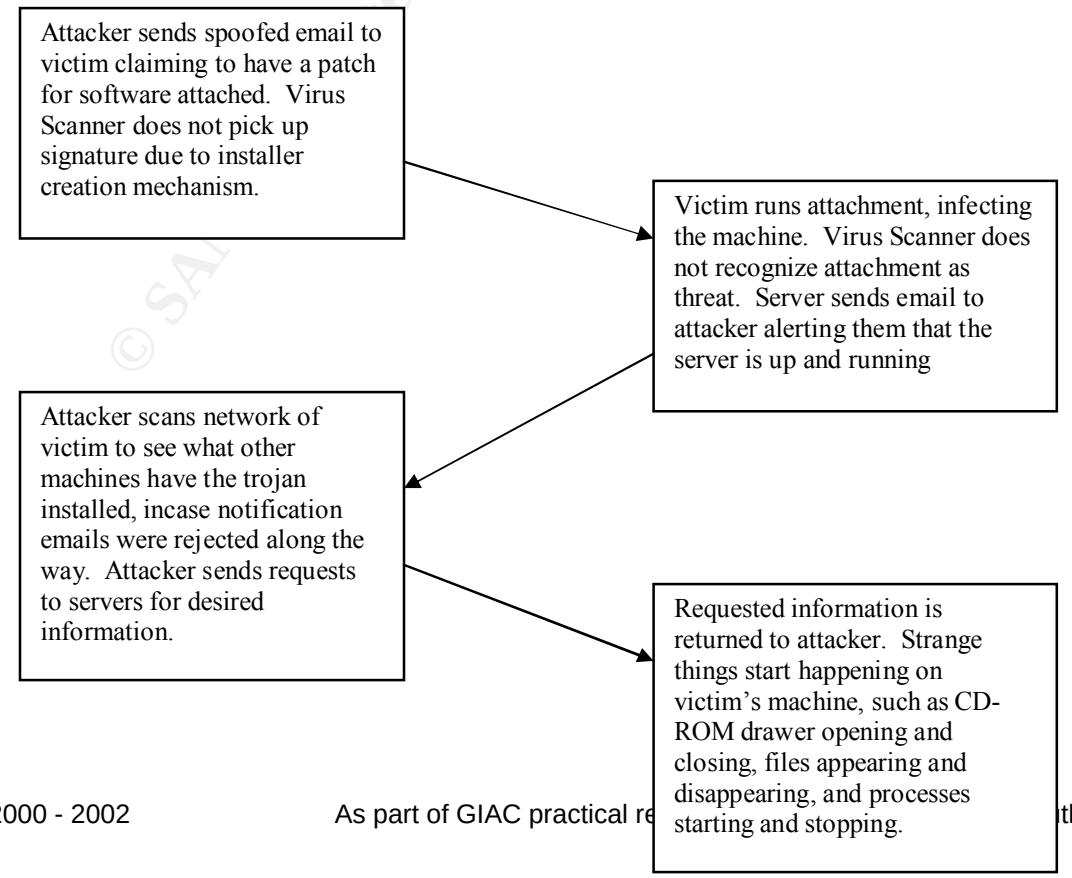
<protocol> <address> <port> <count> [<timeout>]

The protocol parameter is either 0 for IPX or 1 for UDP. The address parameter is either the IPX/SPX address or IP address and can also be a broadcast address. The port parameter must match the settings in the ddsetup.ini. The count parameter is the number of address to scan sequentially. The default timeout is 5000ms, with the minimum value being 1000.

A few example commands are:

1. To scan IP range from w.x.y.z, 50 addresses:
   Ddsfind 1 w.x.y.z 23476 50
2. To get list of servers in IP network w.x.y.0:
   Ddsfind 1 w.x.y.255 23476 0
3. To get list of servers in local network using IPX protocol:
   ddsfind 0 FFFFFFFFFFFF 0x9015 0

Diagram Of How The Exploit Would Work:



Signature Of The Trojan And How To Protect Against It:

Because of the ability to change many of the features of the trojan, it is difficult to track down the malicious files. The first place to search for the occurrence of a trojan is by running the command "netstat –an" and looking for unusual open ports. The default for the Donald Dick trojan is either 23476 or 23477 depending on the version. The lines would appear as:

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:23476	0.0.0.0:0	LISTENING
UDP	0.0.0.0:23476	*.*	

The next preventive measure would be to analyze the registry for unusual entries. The Donald Dick trojan only adds one line to the registry and hides itself by appearing to be a valid entry. One way to limit the installation of the server is to control write access to the Registry and to either \windows\system or \winnt\system32 depending on the version of the operating system that is hosting the server. The usual place for the entry is:

Windows 95/98:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\<Key Name>

Windows NT/2000:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\<Key Name>

A similar measure would be using a file-monitoring program such as Tripwire. This would allow the victim to look for files that have mysteriously changed, uploaded or disappeared. Another tool to search for and detect trojans is the TAMU Suite from Texas A&M University. TAMU is available at:

ftp://coast.cs.purdue.edu/pub/tools/unix/TAMU

When the trojan starts up, the process adds its name to the process list. Daily monitoring of which processes are running on a user's machine will help the victim recognize when something unusual is running. The time to watch for unusual processes is when an email attachment is launched. Often the trojan will come in the form of a believable email attachment; e.g. the I Love You Virus. One of the difficulties with this trojan is that anti-virus programs have trouble detecting it. The installer creator, ddsetup.exe, has the ability to rearrange the internals of the installer, making antiviral signatures difficult to produce.

Another tool to help prevent the client/server connection would be to use a personal or corporate firewall. The corporate firewall would help protect corporations from scans or connections originating from the Internet. A personal firewall located on each machine would be more effective because it could block traffic from the Internet as well as local LAN attacks.

The final countermeasure would be to watch for strange network traffic. The key traffic to watch for are connections to external unknown mail servers. The trojan has the

ability to send messages to the attacker by connecting to external mail servers. The mail will contain the IP address of the victim's machine.

How To Remove The Trojan:

1. Click Start, and go to Run. In the box, type regedit and click OK.
2. When regedit starts, you will see a file-like tree on the left-hand panel. Open the folders to follow the path:
    Windows 95/98:
        HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\ VMLDIR\
        (If the VxD program is different, such as INTLD, you will have to change your path.)
    Windows NT/2000:
        HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\
3. At the end, click on the final key once (VMLDIR or SAMCFG depending on the situation), and the right hand panel should change.
4. Look on the right hand side for the key:
    StaticVxD = "vmldir.vxd" (or intld.vxd)
5. In the LEFT panel, right click on VMLDIR (INTLD, or SAMCFG, etc.), and choose delete. This should remove the whole folder from the VxD section.
6. Close regedit and reboot your PC.
7. After you reboot, you still need to delete the trojan program itself.
8. The default Windows 95/98 trojan is at C:\WINDOWS\System\vmldir.vxd (or whatever Static VxD is equal to, such as intld.vxd) and can be deleted through Windows Explorer, or simply by going into My Computer. For Windows NT the default trojan is at C:\winnt\system32\lsasup.exe.
9. Once you find the file, right click on it and choose Delete. Then empty your recycling bin.

Additional Information:

The Official Web Page:
    http://people.alt.ru/computers/donalddick/

Maximum Security, Second Edition. Anonymous. SAMS Publishing. 1998. Pages 236-252.