Global Information Assurance Certification Paper

Adv. Incident Handling
and
Hacker Exploits practical:

Investigation of the Bionet Trojan 3.1X (3.13-3.18)

Author: Rob Matthew

Version 1.5C – May 2001

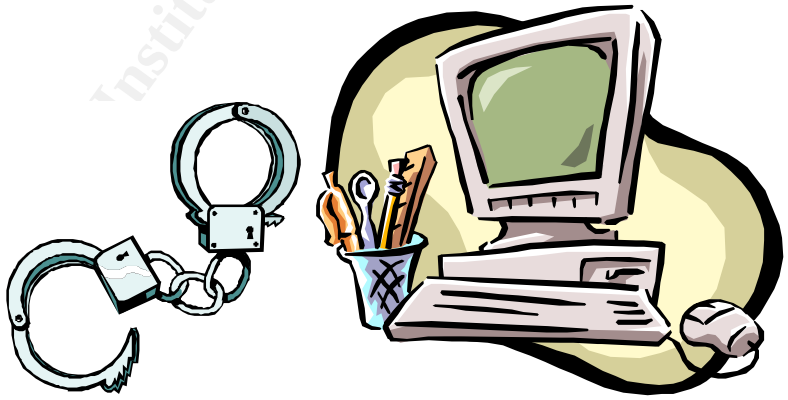

Table of Contents

Introduction

With the publicity of Back-Orifice, Subseven and other Trojan derivatives, malicious code writers have been 'one-upping" each other with new "Features" and stealth abilities. One such programmer is "Razmond", the original programmer of Bionet 1.X, in an effort to not be outdone he has totally rewritten Bionet and released it as Bionet 3.1X, what makes Bionet 3.1X so interesting is it's stealthing techniques. Most Trojan programmers play a game of leapfrog with anti-virus programs. As soon as a new variant of a Trojan is discovered in the wild, anti-virus programs identify its signature and include it in their updated databases, then the Trojan programmers redo their code thus changing its signature. Razmond does the same, however Bionet does something extremely simple and very devious at the same time. Bionet searches running programs in a windows OS and if it finds a match for any of its listed Anti-virus programs, personal firewalls or anti-Trojan program, it exploits a vulnerability in ***ALL*** windows environments via a function called "TerminateProcess()" . The function "TerminateProcess()" will unconditionally, without notification, terminate the running program. Once Bionet 3.1X has "Neutralized " these programs, it loads itself into memory and every 5 seconds rescans the operating system memory and registry looking for reloads of these programs.

Exploit Details

Name:

Bionet 3.1X, Versions 3.13-3.18 were released within the same week.

Variants:

Backdoor.Bionet [2], Backdoor.Bionet.314, Backdoor.Bionet.40a (though a 4.0 version hasn't even been coded yet). Last major release of Bionet was approximately 2 years ago.

Operating System:

Works on / against Windows 95 / 98 / ME / NT4 / 2000 / XP

Protocols/Services:

Bionet was written in Delphi and uses standard windows TCP/IP. Default Main port is 12349 with port 12348 being used for Data; Bionet is capable of using any of the 65,535 other user configurable ports.

Brief Description:

Bionet can be obtained from http://Bionet.mirrorz.com/ [1]. The latest released version is Bionet 3.18. Bionet includes 4 main programs and an optional Bio-lite program. The main programs are Client, Server, Editor and an optional DLL plugin (plugins\bnfun.dll) Bio-Lite is a trimmed down version of Bionet. Bio-Lite features a 7Kbyte executable Server program that uses TCP port 5000 [5], notifies the attacker via ICQ and is capable of having a file uploaded to it as well as executing a file locally.

Bionet has a similar feature set as SubSeven and BackOrifice, it's main "NEW" features include a total re-write of code, (which is not open source) and the ability to exploit a flaw in a windows functions call (called "TerminateProcess() which stops a running program without notification or normal shutdown). Bionet scans running services upon initial load, looking for common antivirus and personal Firewall programs, if any are found, Bionet will terminate those processes and load itself into ram in stealth mode (hidden from task bar and running services).

Example of Bionet features: [2] [3] [4]

Anti-virus/firewall evasion,	Attack target(s) by sending x number of IGMP packets
Schedule commands	Record sounds from server in real time
Deny Local Connections	Open ports only when connected to a network
View/ Kill running processes	Schedule when to activate the server,
Capture image from webcam	Shutdown, reboot, exit, suspend, power off;
Download/Upload files	Execute files remotely
Get cached and email passwords	Get list of ICQ UINS , AIM accounts & Passwords
IRC bot	Remotely download a file and run it

Email all logged keystrokes when the machine connects to the Internet.

Protocol Description

Bionet communicates via the SERVER.EXE" program on the victim(s) computer and via the "CLIENT.EXE" program on the attackers. Communication takes place via a predetermined TCP port and the "SERVER.EXE" can be password protected. The client communicates to the server via this port and all requests are processed from the server side and results are reported back to the client.

Bionet uses several standard methods to notify the attacker of a potential victim:

- ICQ Pager & ICQ Express notification
- Static IP Notification
- Customized ICQ notification message
- CGI Notification
- Email Notification

Description of variants

Bionet is not released with open source code. However, I have been able to find bits of his code that he has shared with his "CreW", to use in the coding of IRC BOTS. The majority of these IRC BOTS are less than 80% finished at this time (as per intercepted IRC channel conversations). Razmond has openly admitted to using Delphi to write Bionet and plans to continue using it, even though he has been getting some flack over Bionet's size.

So far Bionet and other similar Trojan programs (BackOrifice, SubSeven, and Netbus), all support the same basic annoying and dangerous features: The ability to upload, locally execute programs and locally compromise a computer's security features.

SubSeven and Bionet Similarities

Both SubSeven and Bionet release their code as Client / Server programs, which feature plugins and a simple readme.txt style, reference manual. Both are configurable with similar feature sets. Both use TCP ports only (Back Orifice can use TCP and UDP ports). Both can use stealth features when attempting to hide from the window's taskbar and running processes.

Both SubSeven and Bionet were written purely for malicious / non-commercial applications with an emphases on covert remote control and data gathering capabilities. (BackOrifice and Netbus Pro, are Trojans that claim to be used for network management).

SubSeven and Bionet Differences

Bionet includes an ability to remove anti-virus, personal firewall programs or anti-Trojan programs. When configured for stealth mode, Bionet scan every 5 seconds for those running programs / processes and terminates them.

SubSeven's "SERVER.EXE" code size is approximately 70Kbyte packed, while Bionet's "SERVER.EXE" is approximately 260Kbyte when packed. The size difference hinders binding Bionet to another program for stealth delivery and hinders its download via slower links.

How the exploit works

The Bionet Trojan is usually distributed the same way that SubSeven and BackOrifice are distributed. Social engineering and creative presentation are used to deliver the Trojan to the victim, either by E-mail as an innocent looking executable or left on a Server for an unsuspecting user to download and execute. Once downloaded the "SERVER.EXE" will register itself as infected and available for control, via either E-mail, static IP notification, IRC-BOT or ICQ. Once the victim host has notified the attacker of its compromise, the attacker can take complete control of the victims PC to include logging every key stroke, sending cached passwords, manipulating files and executing attacks or probes locally. I personally have seen a version where an attacker bound the "SERVER.EXE" to

the “EDITOR.EXE” edited all documentation to show a new version, and then recompressed and redistributed the Trojan as a new release. When a would-be attacker (Script Kiddie) runs the “EDITOR.EXE” program, unnoticed to them an embedded “SERVER.EXE” is loaded on their system. While an attacker is using Bionet’s editor to configure their releasable “SERVER.EXE” their system is now turned into a zombie and susceptible to control.

Diagram

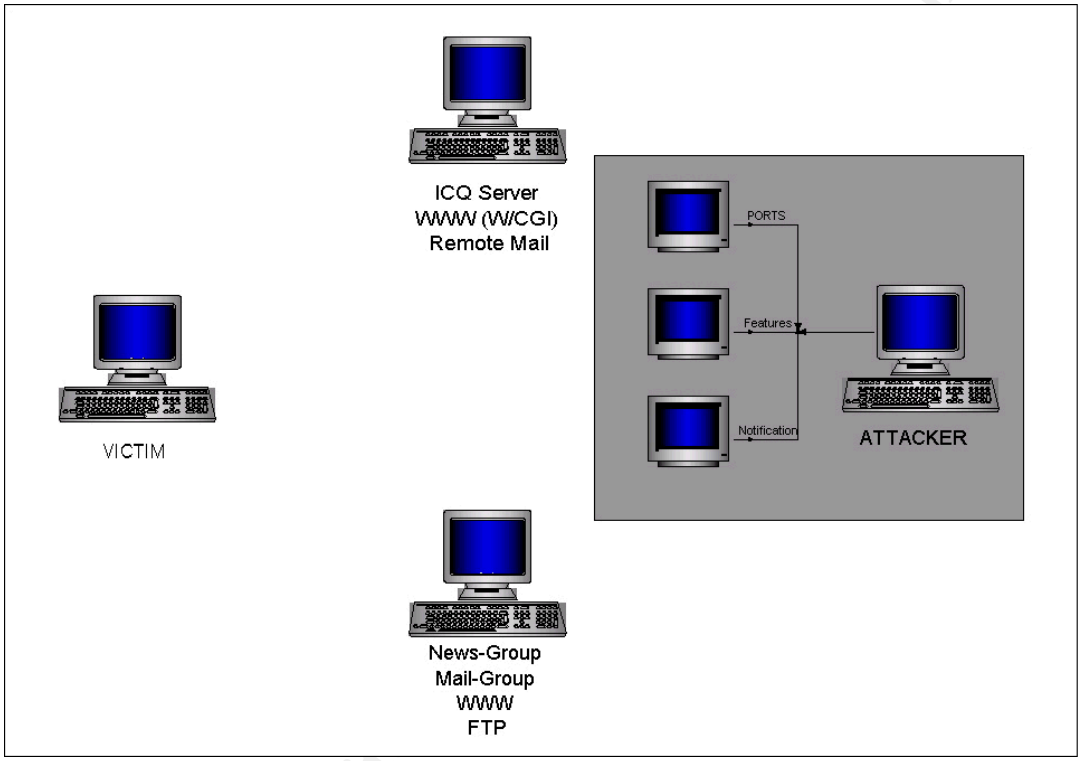

Figure 1. The attacker configures the “SERVER.EXE” with Notification, Channel options or stealth.

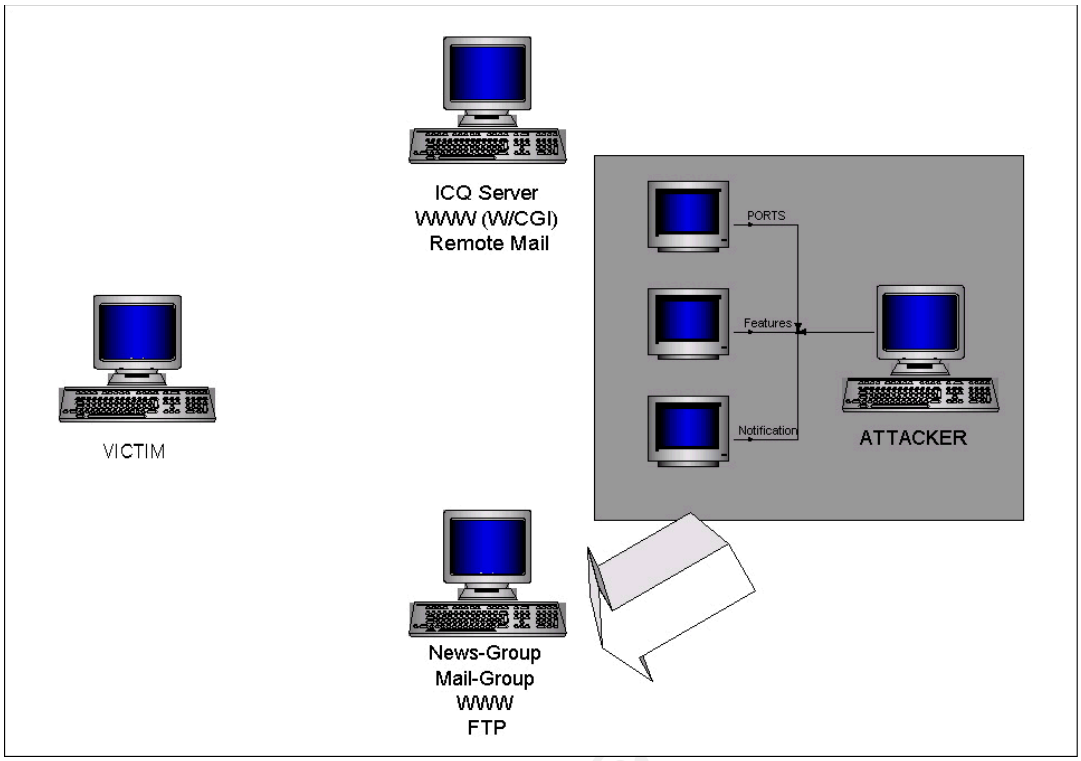

Figure 2. The attacker sends "SERVER.EXE" to A Newsgroup, E-mail Spam list, or FTP Server

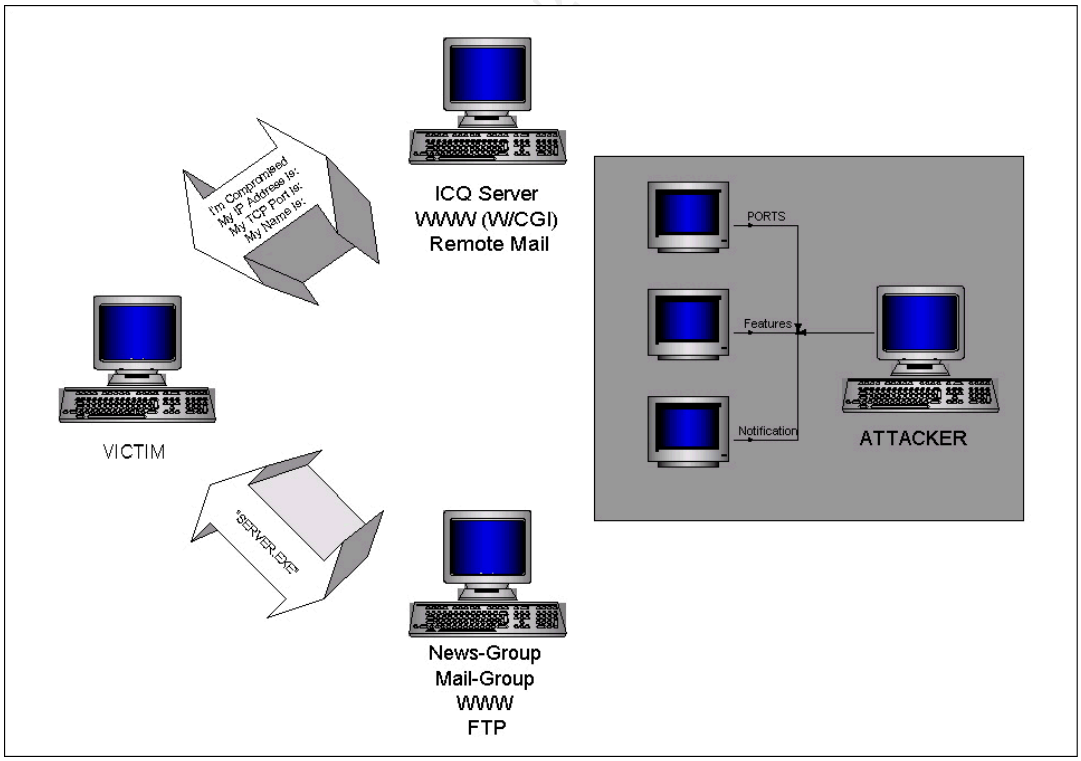

Figure 3. The Victim Downloads and executes the "SERVER.EXE" Notifies Attacker of Status

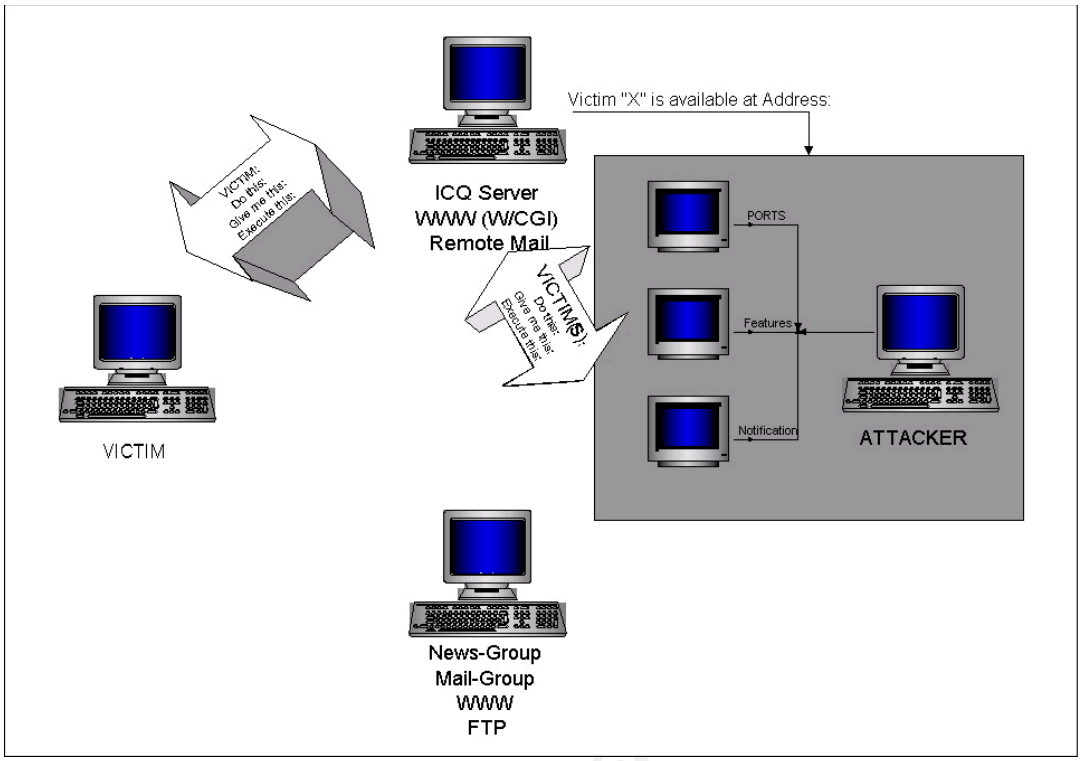

Figure 4. Attacker users IRC to stealthily control the victim

How to use the exploit

For ease of explanation and standardization the following verbiage will be used.

- "SERVER.EXE" The Bionet main Server program, though this can be any name an attacker chooses(Mcviegh-execution-mpg.exe., free-XXX-Passwords.exe.

- "CLIENT.EXE" The Bionet Client program, used to access the "SERVER.EXE".

- "EDITOR.EXE" The Bionet "SERVER.EXE" editing program. This is the program that all features are added or modified to the "SERVER.EXE" program.

Configuring the Server.exe

1. An Attacker downloads the latest version of Bionet. Once the attacker has it, he/she loads the editor and picks and chooses via a built in GUI which exploits they want to exploit on a potential victim. (This step determines the general size of the Executable.) From here, an attacker can choice stealth loading and configure when / how often they want the "SERVER.EXE" to be loaded (fig 1)

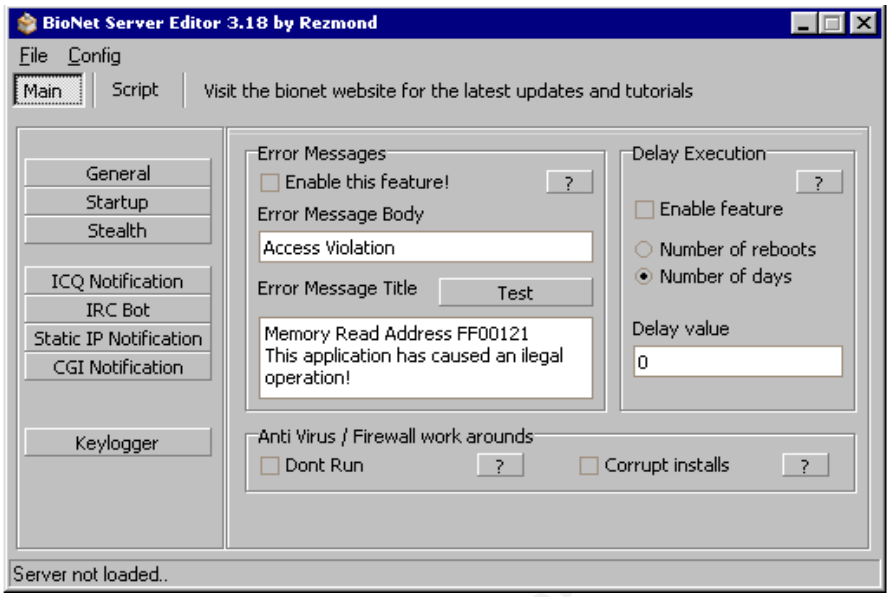

Figure 1. Bionet Server Editor

2. The attacker next chooses the method of loading and which port(s) to use. From here, an attacker can choose default load (port 12349) or a custom port. This is the port that the server will monitor and respond to client requests. An attacker will normally password protect the "SERVER.EXE", so other clients scanning a subnet will not be able to gain access. (*Fig2)* An advanced features option here is "The-joiner". "The joiner" is a mini exe file joiner. It is integrated into the builder and will allow you to join two files together. This can be used to join a simple game like winmine.exe (windows mine sweeper) with the server. Whoever runs the combined file will think they are just running winmine yet Bionet will also have been installed on their machine without their knowledge.

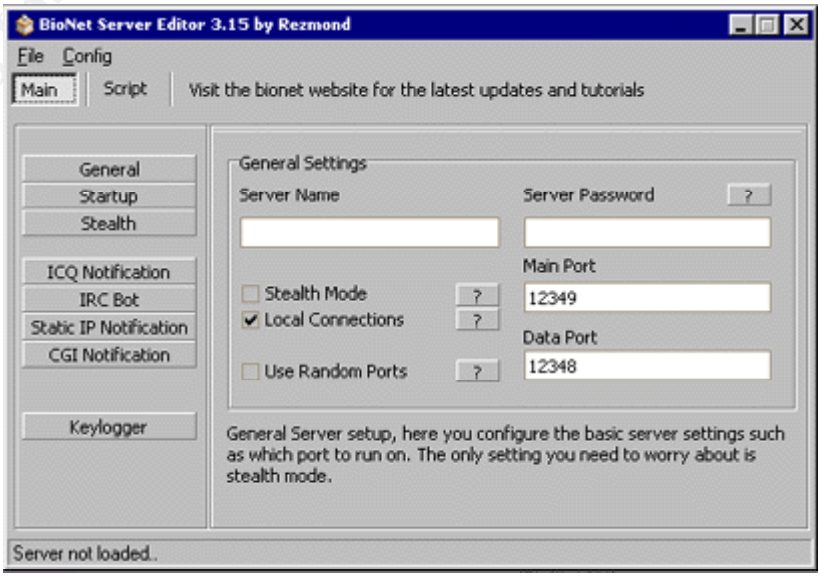

Figure 2. Server and port Settings

3. The last main configuration option is to decide how the attacker wants to be notified. Bionet supports several methods of notification, ICQ Pager & ICQ Express notification, Static IP Notification, Email notification, CGI notification and Customized ICQ notification messages to include: victims port number, Name, port used, and username (*Fig 3)*. Bionet also has built in support for an IRC BOT. The IRC BOT allows an attacker to configure the "SERVER.EXE" to automatically log into a private IRC channel. This is useful to an attacker who wants to collect a number of compromised machines and have them report for control centrally. This allows an attacker to launch DOS attacks and other attacks anonymously using a vast number of zombies with minimum effort . This places the aggregate bandwidth of 250+ hosts on 100+ different network provider pipes at his/her disposal. (*Fig 4)*

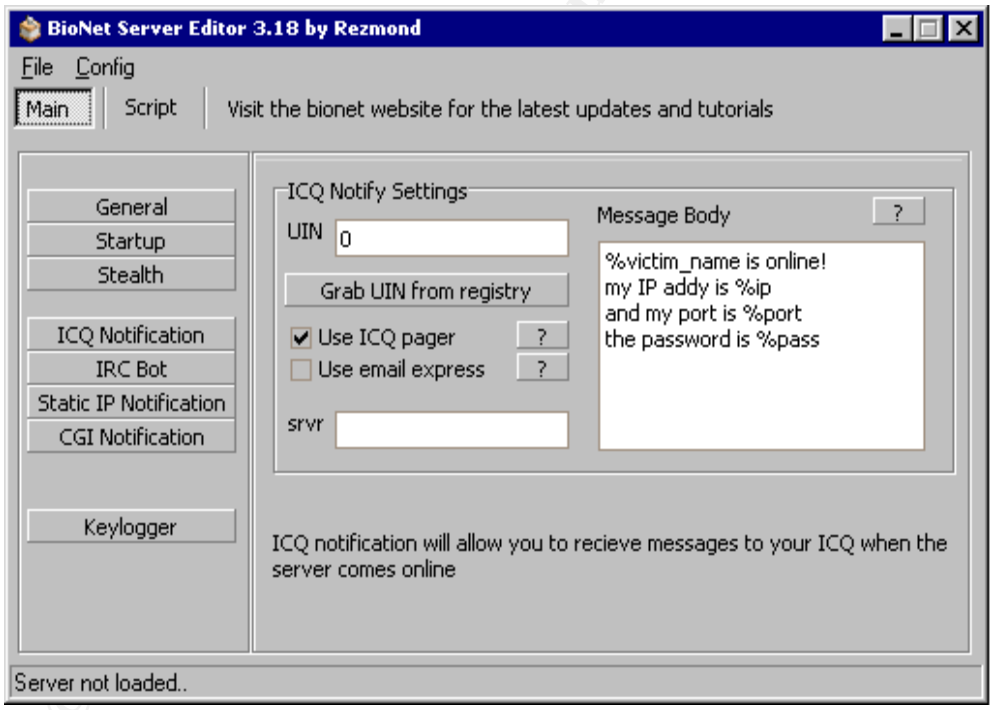

Figure 3. ICQ Notify Sessions

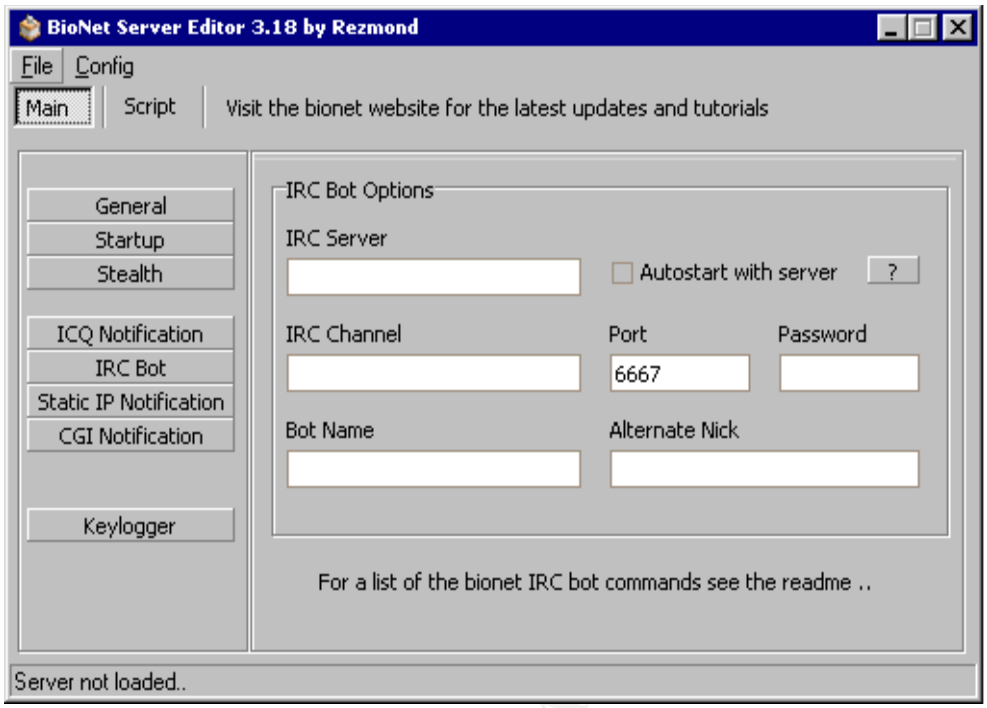

Figure 4. IRC BOT

Distribute Trojan

Once an attacker has customized his "SERVER.EXE" the next phase is getting the malicious code to End-users. This is where social engineering comes into play. Social Engineering as defined by Kevin Mitnick: [7] "The object is to get information or access to systems that are normally only used by privileged users." In the realm of Trojan horses and Social Engineering, an attacker wants an unsuspecting user to download (bring into) and locally execute (run / load /store) the malicious code. Trojan distribution via Social Engineering can:

- Offer something that a user wants, but doesn't want to pay for (i.e. click here, to download passwords to pay sites), or offers something that no one else has, as the following article shows:

  13 & 14 June 2001 Morbid Curiosity Yields Trojan [8]
  Computer users who thought they were downloading a bootlegged video of Timothy McVeigh's execution were actually being tricked into installing the Subseven Trojan Horse program on their computers. The program, which affects only computers running Windows operating systems, allows crackers to remotely control infected machines.

- Act as E-mail from a file-sharing friend that has a new utility for them to try.
- Embed the Trojan in an innocent looking program or game. (winmine.exe)

- Embed the Trojan in a commercial package that is being illegally distributed

Victim Activates Trojan [3]

The first thing that Bionet does upon execution via stealth mode is to scan running processes looking for known anti-virus, personal firewall and anti-Trojan programs. If any of the following filenames are found it is they are automatically terminated.

AVP32	AVPCC	AVPM	AVP32	AVPCC
AVPM	AVP	NAVAPW32	NAVW32	ICLOAD95
ICMON	ICSUPP95	ICLOADNT	ICSUPPNT	IFACE
ANTS	Anti-Trojan	iamapp	iamserv	FRW
blackice	blackd	zonealarm	vsmon	WrCtrl
WrAdmin	cleaner3	cleaner	tca	MooLive
lockdown2000	Sphinx	VSHWIN32	VSECOMR	WEBSCANX
AVCONSOL	VSSTAT			

Next Bionet scans the registry for references to installed, but not running anti-virus and personal firewall programs:
HKEY_LOCAL_MACHINE\Software\WRQ\IAM\Installation Info\
HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoute\
HKEY_LOCAL_MACHINE\Software\McAfee\McAfee Firewall\
HKEY_LOCAL_MACHINE\Software\MooSoft Development\The Cleaner\
HKEY_LOCAL_MACHINE\Software\Signal 9 Solutions\ConSeal PC Firewall\

Every 5 seconds Bionet repeats this process and terminates any re-activated anti-virus, personal firewall or anti-Trojan programs.

After Bionet has disabled a Victim's anti-virus, personal firewall or anti-Trojan software it loads itself into memory and makes changes to the registry to ensure it is reloaded every time the victim's computer is loaded. Bionet makes the following window's registry entries:
HKEY_LOCAL_MACHINE\software\GCI\Bionet 3.\LibUpdate\LibUpdate.exe

* The default server name (LibUpdate.exe) and the default registry entry name can be anything the attacker chooses.

The following key is created by the Bionet server to make it autostart every time windows starts:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
WinLibUpdate="C:\Windows\libupdate.exe -hide"

where C:\Windows\ is the path to your Windows directory.
** Note LibUpdate.exe can be any name the attacker chooses.

After Bionet makes these changes to the registry to ensure its loaded every time windows is loaded, Bionet notifies the attacker of its infection via any combination of its configurable notification options:
ICQ Pager & ICQ Express notification, Static IP notification, Customized ICQ notification message, CGI notification or Email notification. Bionet has Variables in its notification fields. These variables allow the attacker to customize the messages being sent from each victim, thus allowing them to build a large, manageable cluster of zombies.

Message Variables

There are many message variables in a notification message, having one of the following variables in the body of the message will replace that variable with that data. For example %IP gets replaced with the victims IP address.
Key variables>>

Variable	Description
%ip	The ip[s] of the server
%port	The server port
%pass	The server password. blank if none
%victim_name	Name of the server.
%version	The version of the server.
%computer	Computer name (if on a network)
%user	User name (windows registerd username)
%mode	The server mode (server is in debug mode ? or stealth mode
%lf	Line feed (indicated the start of a new line)

Examples of using the above key variables >>
A victim is infected with Bionet on port 12349. The victim's IP address is 100.100.100.100, the victim's name is Mobman and the server version is 3.15 if the attacker used. "Victim : %victim_name is online with IP : %ip on port %port. Server version: %version." as the content of the notification message, it would result in a notification message with something like this:
Victim : Mobman is online with IP 100.100.100.100 on port 12349 Server version: 3.15

An attacker now has a victim's IP address, port number the "SERVER.EXE" is listening on, and name of their computer. Only thing left for the attacker to do is to take Control of the victim.

Control Victim

Standard configuration for Bionet once activated and connected to the

internet, is to send a notification message via any combination of ICQ, CGI, Static IP, IRC or E-mail to the attacker with it's name, IP address and port used. Now than an attacker has a victims IP address and TCP port info all they have to do is decide if they want "one on one" or "one on many (IRC-BOT)" remote control.

One on one remote control

One on one remote control allows an attacker to establish a virtual connection to a victims computer via their Bionet client and the victim's Trojan "SERVER.EXE" program, on an agreed upon TCP Port. Once an attacker has a virtual connection to a victim's computer he / She can:

- **Remotely update server** – Upload Bionet's latest "SERVER.EXE"

- Get system information - Processor, peripherals, memory, O/S, Etc.
- **Remotely install an application-** Install rootkits, or other tools
- File manager- Hunt for Financial, proprietary, or damaging info.
- Task list- Shows any specialized programs running.
- Clipboard viewer- View data they are working / manipulating.
- **Registry editor-** VERY Dangerous, causes mayhem in windows.
- ***Chat functions***- Send Alert, Erroneous Instructions, False info.
- **Key logger –** Record keystrokes, Account #'s, Passwords, PGP-Keys.
- *Mouse controller*- Change speed, motion type of pointer.
- *Display manager*- To include resolution, background and desktop.
- *Printer manager*- Add /delete / modify printers or paper-eject.
- Webcam control – Unauthorized remote surveillance, Peeping-Tom
- Audio / MIC control – Unauthorized surveillance, eavesdropping.
- Screenshot capture – See what victim sees, account #'s password, Etc.
- Internet Explorer cache viewer – See what they have visited and seen.
- *Internet Explorer start page modifier*- Where IE loads first (pay sites).
- *Open/close CD-ROM*- Gremlins, bad when playing a game.
- *Change screen saver*- Type what is displayed, when it occurs.
- *PC speaker player*- Change volume, left-right (maybe damage).
- **Password stealer** – To include cached internet passwords, Logins.
- *Remote shutdown/reboot*- Very annoying, Gremlins.
- *DUN manager* – Change connection rates.
- **IGMP attack launcher-** Victim looks like the initiator of an attack.
- **Port redirector-**Tunnel through firewalls or relay data to another host.
- *Plugin manager*- For adding future "Feature Enhancements".
- File finder - Hunt for Financial, proprietary, or other damaging info.
- **Port scanner** Victim looks like the initiator of a probe.

- **Highlighted features can be Critical / Damaging to Victim**.

- *Italics features can be annoying to Victim.*
- Underlined Features are for Data-gathering, Covert-ops, or Financial gains

One on Many remote control

One to many remote control is usually accomplished by configuring the Bionet "SERVER.EXE" to automatically log into an IRC channel, register itself and await commands. This feature allows an attacker to amass a large number of infected machines (Zombies) a.k.a. an Army of Zombies, and provides the attacker with the opportunity to direct all their (Victims) resources at fixed locations. I.e. an attacker has 250+ infected hosts from 100+ different network providers, automatically log into an IRC server under the channel name of "BIO-Zombies". In the middle of the night the attacker connects to the IRC channel and, using his private password, logs in and issues a single script which is received by ALL Zombies on that IRC channel, instructing them to do a DDOS attack against www.Someone.com. . This places the aggregate bandwidth of 250+ hosts on 100+ different network provider pipes at his/her disposal.

An Excerpt from Steve Gibson's [9]

"The Strange Tale of the Attacks Against GRC.COM"

by Steve Gibson, Gibson Research Corporation

The Attack Profile

We know **what** the malicious packets were, and we will soon see (below) exactly how they were generated. But we haven't yet seen where they all came from. During the seventeen hours of the first attack (we were subsequently subjected to several more attacks) we captured 16.1 gigabytes of packet log data. After selecting UDP packets aimed at port 666 **. . .**

I determined that we had been attacked by 474 Windows PC's.

This was a classic "Distributed" Denial of Service (DDoS) attack generated by the coordinated efforts of many hundreds of individual PC's.

Where do these machines reside?

Who owns them?

Who are their ISP's?

What sort of users are running Windows PC's infested with potent Internet attack Zombies?

A determination of the network domains hosting the attacking machines revealed the following, hardly surprising, cast of Internet end user service providers:

104	Home.com	5	inreach.net	3	Voyager.net
51	rr.com	5	telus.net	3	lvcm.com
20	aol.com	5	gtei.net	3	co.uk
20	mediaone.net	4	tpo.fi	2	cdsnet.net
17	uu.net	4	rcn.com	2	enter.net
14	btinternet.com	4	isoc.net	2	cgocable.net
14	shawcable.net	4	uswest.net	2	knology.net
14	optonline.net	3	dialsprint.net	2	com.au
14	ne.jp	3	a2000.nl	2	fuse.net
9	chello.nl	3	grics.net	2	lrun.com
9	ntl.com	3	linkline.com	2	dialin.net
8	videotron.ca	3	eticomm.net	2	bellsouth.net
7	ad.jp	3	prestige.net	2	psnw.com
7	psi.net	3	warwick.net	2	pacificnet.net
6	uk.com	3	supernet.com	2	tds.net

Domains hosting two or more security-compromised, attack Zombie, Windows PC's

(The balance of the 474 Windows PC's not represented above were scattered across a multitude of domains, one machine apiece.)

It probably comes as no surprise that the top two U.S. residential cable-modem Internet service providers — **@Home** and **Road Runner** — provide Internet connectivity to the host machines most often sought by malicious hackers for the installation of bandwidth flooding Zombie attack Trojans.

While I was monitoring several online hacker hangouts (with the aid of custom spy-bots I created for the purpose — more on that below), I often overheard hackers referring to various lists of "cable Bots" and saying things like "Heh, but how many of his Bots are cable?"

It is clear that the "cable Bot" — a remote control Zombie program installed on a high bandwidth, usually on, Windows machine — has become a highly sought-after resource among malicious "Zombie/Bot running" Internet hackers.

This Excerpt more than underlines the capabilities of "Ready Made" Trojans with built in IRC-BOT capabilities.

Signature of the attack

To simulate a victim – attacker relationship I set up a mini network consisting of:

Victim PC: 800Mhz Windows 2000, 256 megabytes of RAM and 20 gigabyte hard-drive.
Attacker: 650MHZ windows 98, 64 megabytes of RAM and 6 gigabyte hard-drive.

PC's were connected to a 100 Megabyte switched internal network with an IP network address of 192.168.1.X. The 100-megabyte full duplex switch is connected to an internal firewall / NAT router, which is connected to an XDSL modem, connected to the Internet. ICQ via the Internet was used for notification.

Attacker command and control was accomplished via internal network

Prior to delivery and execution of "SERVER.EXE" **netstat –na** was run on the victim's machine. (Note: Netstat output was edited to be more manageable) *(fig 5)*

NETSTAT –NA prior to infection

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:53	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:119	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1029	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1030	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1033	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1035	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1037	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1038	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1041	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1755	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3372	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7007	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7778	0.0.0.0:0	LISTENING
UDP	0.0.0.0:1032	*:*	
UDP	0.0.0.0:1034	*:*	
UDP	0.0.0.0:1036	*:*	
UDP	0.0.0.0:1039	*:*	
UDP	0.0.0.0:1042	*:*	
UDP	192.168.1.110:138	*:*	
UDP	192.168.1.110:500	*:*	

Figure 5. NETSTAT –na prior to Trojan

Delivery of Bionet Trojan was accomplished by Joining "SERVER.EXE" to a freeware game and sent via E-mail to the victim. Victim executed

(ran) the "Trojan-game.exe" attachment and I (the attacker) was immediately notified of the compromise. Bionet sends all of its data unencrypted. The Server sends an initial notification to the attacker's e-mail address, ICQ address or IRC address. For this example I'm using an ICQ notification method. *(fig 6)*

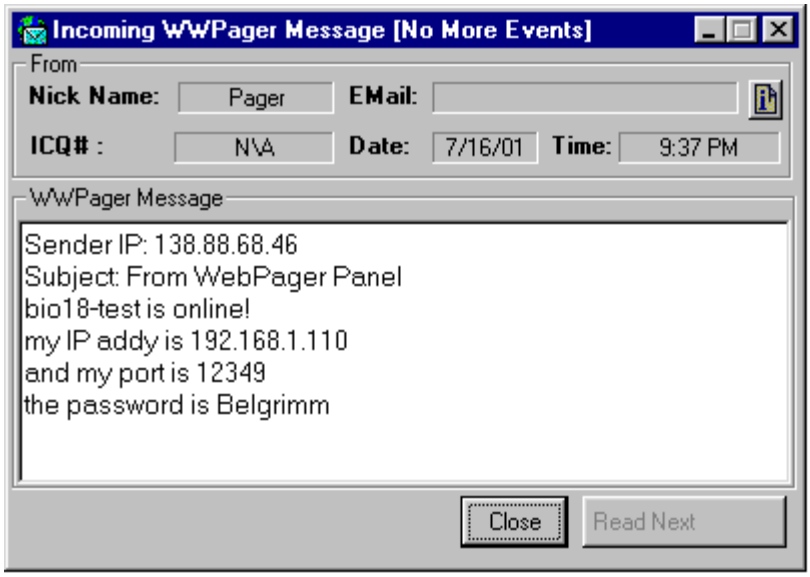

Figure 6. Bionet "SERVER.EXE" ICQ notification message.

Once notified of Victims Name, IP address, port being used and Password, I loaded up the client and initiated connection. The following is an NETSTAT-na screen. (Note Netstat output was edited to be more manageable.) *(fig 7)*

NETSTAT –NA after infection

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:7	0.0.0.0:0	LISTENING
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:119	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1029	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1030	0.0.0.0:0	LISTENING

```
TCP    0.0.0.0:1033           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1035           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1037           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1038           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1040           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1041           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1755           0.0.0.0:0              LISTENING
TCP    0.0.0.0:9853           0.0.0.0:0              LISTENING
TCP    0.0.0.0:12348          0.0.0.0:0              LISTENING
TCP    0.0.0.0:12349          0.0.0.0:0              LISTENING
TCP    192.168.1.110:139      0.0.0.0:0              LISTENING
TCP    192.168.1.110:12349    192.168.1.9:1496       ESTABLISHED
UDP    0.0.0.0:7              *:*
UDP    127.0.0.1:1026         *:*
UDP    127.0.0.1:1027         *:*
UDP    127.0.0.1:1031         *:*
UDP    192.168.1.110:53       *:*
UDP    192.168.1.110:137      *:*
UDP    192.168.1.110:138      *:*
UDP    192.168.1.110:500      *:*
```

Figure 7. NETSTA-na after Trojan infection

Even though the Bionet "SERVER.EXE" was configured for stealth and does not show up on the windows task bar NETSTAT shows an TCP 192.168.1.110:12349 192.168.1.9:1496 ESTABLISHED connection. Also note that there are no UDP connections established, further proof that BIONET is TCP only and not UDP.

How to protect against it

Bionet, Like other Trojan programs before it, relies on end-users to execute them. Thus, most delivery methods for Trojans rely on social engineering or deceit (Trojan buried in a game or desired program). Very often end-users rely on their anti-virus software or personal firewall to catch all malicious programs or rely on nothing. The biggest problem with relying on software is the "leap-frog" effect between anti-virus programs and malicious programmers, as soon as one gets the upper hand the other releases a newer, more feature rich product. With the constantly changing nature of computer's, operating systems and malicious software, the following recommendations are submitted

- Run anti-virus *and* personal firewall software on *all* networked or Internet connectable hosts.
- Check *at least* twice a month for anti-virus and personal firewall updates, and *install* them!
- Configure firewall to only allow known applications access and to limit ports out.

- Keep operating system patches and security updates current.
- Configure Internet access to be on a "need to access only", not continually on. If you are not accessing the Internet, you should not have a continuous open connection to it.
- Take all alerts seriously. Burglars case a target prior to breaking in, Hackers do the same.
- If your anti-virus or personal firewall stops working, investigate *WHY* and fix it.
- Never run an unsolicited program that has been E-mailed to you, especially if it offers you something for nothing, or free access to a pay site.

If you have been infected with the Bionet Trojan, you can use a Trojan removal program such as BOCLEAN 4.07 [6] or other Trojan removal program. To manually remove Bionet 3.X from your system, you will need to run Regedit [4]. Bionet stores assorted configuration information under the key:

```
HKEY_LOCAL_MACHINE\software\GCI\Bionet 3.
```

With the default server name (LibUpdate.exe) and the default registry entry name, the following sub-key is created by the Bionet server to make it autostart every time windows starts:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
WinLibUpdate="C:\Windows\libupdate.exe -hide"

** Note Bionet 3.1X allows the attacker to change the
name of libupdate.exe to whatever they want, so be wary
of any –hide options that your machine auto loads.
```

You must remove the registry sub-key first. It will not be possible to remove the program file while the server is running and you may also be prevented from shutting down the computer. A reboot is required to restart the machine without the Bionet server being reloaded. At this time the file pointed to in the registry can be removed without further risk. The Bionet Trojan, like most others, will not be visible to the Windows task-listing program. You must note the filename referred to in the registry and manually remove each occurrence of it the same way.

Additional information

[1] Bionet Support site: [July 2001]
http://Bionet.mirrorz.com

[2] F-Secure Computer Virus Information: [June 2001]
http://www.f-secure.com/v-descs/Bionet.shtml

[3] MISCHEL Internet security: Analysis of Bionet 3.12: [2000]
http://www.mischel.dhs.org/Bionet312analysis.asp

[4] Dark Eclipse Software, Bionet 3.1X write-up: [2000 2001]
http://dark-e.com/archive/trojans/Bionet/313/index.shtml

[5] Dark Eclipse Bio-lite write-up: [2000, 2001]
http://dark-e.com/archive/trojans/Bionet/lite10/index.shtml

[6] Boclean: [2001]
http://www.nsclean.com/boclean.html

[7] Mitnick teaches Social Engineering: [July 17, 2001]
http://www.zdnet.com/zdnn/stories/news/0%2C4586%2C2604480%2C00.html

[8] 13 & 14 June 2001 Morbid Curiosity Yields Trojan: [June 13 2001]
http://news.bbc.co.uk/hi/english/sci/tech/newsid_1386000/1386606.stm

[9] The Strange Tale of the Attacks against GRC.COM: [July 4, 2001]
http://grc.com/dos/grcdos.htm