GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Back Orifice 2000 (BO2K) – The Insider Threat

GCIH Practical Assignment
Option 1 – Exploit in Action
Version 2.1a (revised Jan. 20th, 2003)

By Rob Ferrill
June 13, 2003

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Contents

EXECUTIVE SUMMARY 3

PART 1 – THE EXPLOIT 4

Name 4

Operating System 4

Protocols/Services/Applications 4

Brief Description 5

Variants 5

References 5

PART 2 – THE ATTACK 5

Description and diagram of network 5

Protocol description 7

How the exploit works 8

Description and diagram of the attack 13

Signature of the attack 16

How to protect against it 19

PART 3 – THE INCIDENT HANDLING PROCESS 20

Preparation 20

Identification 21

Containment 32

Eradication 34

Recovery 36

Lessons Learned 37

References 37

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

EXECUTIVE SUMMARY

This paper was written as partial fulfillment of the GIAC Certified Incident Handler Certification (GCIH), version 2.1a, revised January 20th, 2003, option 1 Exploit In Action. I have chosen to write about an incident I was involved with at work so this is going to appear very sanitized. The incident involved two employees at a Fortune 500 company who worked at a remote WAN site. One was an IT support person and the other was his manager, the data coordinator for the site. IT support for this company is mainly done from the corporate office, however there are needs for full-time or contracted IT support personnel in the field since this company has offices all over the United States. During an interview after the incident, the individuals claimed they wanted to ease their burden of supporting large numbers of PC's by downloading and installing an open source remote control application thereby allowing them to manage desktops from their offices. In this particular case, it happened to be a popular trojan program called Back Orifice 2000. The use of unauthorized software, especially those of a malicious nature, is against corporate IT policy. Not only is there a policy against installing unauthorized software, but the help desk and corporate IT support staff already maintain multiple remote control applications at their disposal for desktop support (i.e. Symantec's PCAnywhere).

It was obvious from the onset of this incident that these gentlemen were not experienced hackers but were the types that know enough to be dangerous. The incident began when our Virus Administrator was reviewing daily logs and discovered that Trend anti-virus detected the trojan on one of the computers involved and tried to delete it. After being notified by the Virus Administrator of this activity, the IT Security staff reviewed the logs of our linguistic analysis software (the Vericept View product) and retrieved the actual web sites that were visited during their search for hacker and trojan tools. In addition to the searches for trojans and hacker tools, the individuals involved also conducted web searches to find out how to disable the Trend anti-virus software. This was initiated in an attempt to determine how to install Back Orifice 2000 without the Trend virus protection software interfering. The Vericept product analyzes all traffic at the ingress and egress points of our corporate network for pattern matches in a contextual manner. The Yahoo searches these individuals were conducting showed up in Vericept under the "Hacker Research" category.

At this point, we immediately had the hard drives from the two computers involved shipped back to the IT Security department at corporate headquarters for forensic analysis. The analysis of the hard drives was completed using a commercial forensic analysis tool called Encase.

Due to the countermeasures already in place to prevent this type of incident from happening, this event never became a full-blown incident where the attacker was

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

actively using the trojan to exploit systems. Therefore, I will have to discuss a few "what-if's" in order to explain what could have happened and how this trojan really works.

PART 1 – THE EXPLOIT

Name

The exploit discussed in this paper is a trojan called Back Orifice 2000 or BO2K. According to the advisory released by the ISS X-Force on this trojan, the Common Vulnerabilities and Exposures (CVE) project has assigned the name CAN-1999-0660 to this issue. They also state that there is a standard associated with the entry which is: IAVT 1999-T-0002: Back Orifice 2000 Technical Advisory. In searching CERT's website it doesn't appear that there was ever an advisory released regarding this trojan. There was however a vulnerability note released on the original version of this trojan. The original CERT number assigned to the original Back Orifice trojan was CERT Vulnerability Note VN-98.07.

Operating System

The operating systems that this trojan runs include all service pack and patch levels of the following:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Professional
- Microsoft Windows XP
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows 98 Second Edition
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Workstation 4.0

It should also be noted that BO2K currently runs on Intel platforms only but since the source code is open to the public it could conceivably be ported to other platforms and/or operating systems in the future.

Protocols/Services/Applications

The protocols used by this trojan are either TCP or UDP and the ports that it uses are completely configurable. The default port for the base program is TCP port 54320. The default ports for the bo_peep plugin include TCP port 15151 for the VidStream module and TCP port 14141 for the Hijack module. These will be explained in more detail later in this paper. The communications can be encrypted with an XOR algorithm (which is easily decrypted) or a triple DES algorithm.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Brief Description

According to BO2K author, Dildog (a member of the well-known hacking group "Cult of the Dead Cow – CDC" dildog@users.sourceforge.net), this trojan is an open source freeware tool that provides a legitimate method for remote administration of Windows platform boxes including remote control over encrypted channels (you can use XOR or triple-DES encryption). The program has several stealthy type features that have caused many in the security industry to question the integrity of the author. The covert operations allowed by the trojan make this ideal for hackers to hide their activity. The writer designed Back Orifice 2000 so you cannot see it running as a process in the process list unless you install it yourself while logged on as administrator.

Variants

Back Orifice 2000 is itself a variant of the original trojan called Back Orifice, but the newer version is a complete rewrite. Listed below are the alias names:

- BO
- CDC-BO
- BOSERVE
- BOCLIENT
- Orifice
- Hacktool
- Back_Orifice

References

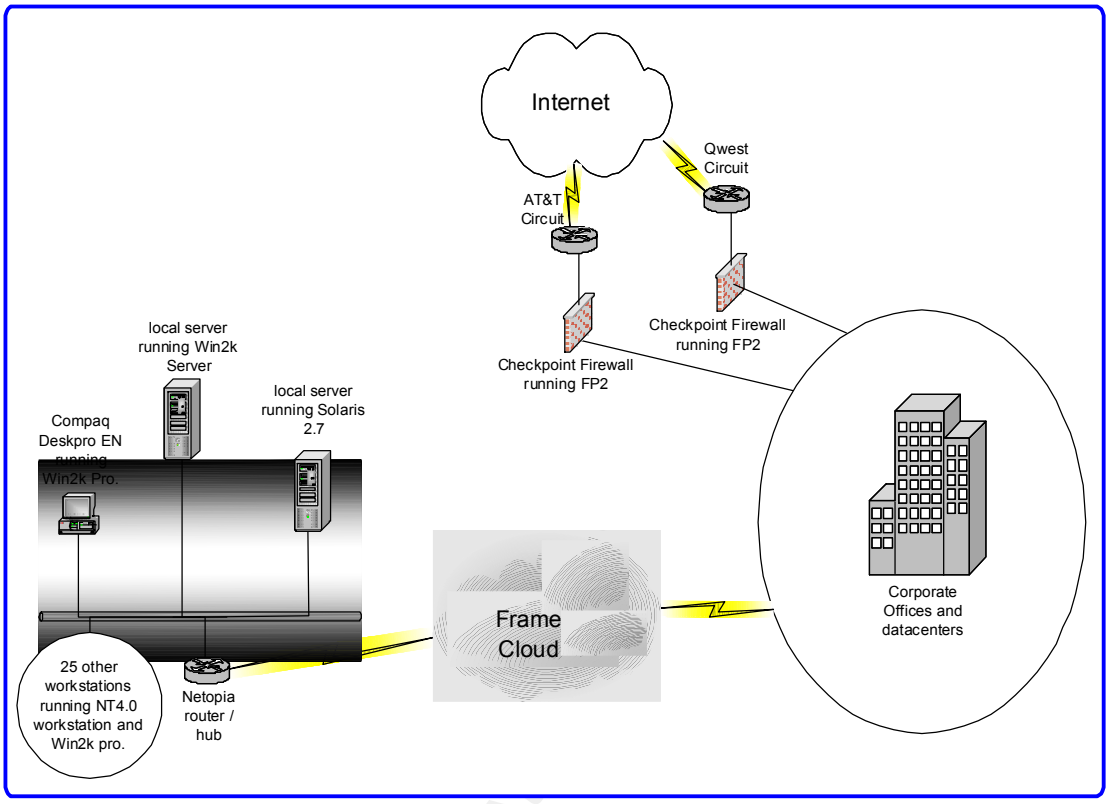
http://www.bo2k.com
http://prdownloads.sourceforge.net/bo2k/bo2ksrc_1.0.zip?download
http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?id=advise31
http://www.antivirus.com/vinfo/security/sa071299.htm
http://www.norton.com/avcenter/venc/data/back.orifice.2000.trojan.html
http://zdnet.com.com/2100-11-501114.html
http://news.com.com/2100-1001-228208.html?legacy=cnet

PART 2 – THE ATTACK

Description and diagram of network

The network upon which this incident took place consists of a corporate campus with dual ISP connections and 1700 remote offices all across the country that have frame relay WAN circuits back to the corporate office for Internet access. This design allows for centralized monitoring of all traffic to and from the Internet. The WAN sites are connected to one of seven regional routers at various locations across the country. The drawing below does not depict the entire corporate network but shows only the remote office where the incident occurred.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



The remote offices each have a flat LAN design (i.e. one class C network with a router that connects to a frame relay network). While only limited filters exist between WAN sites or between a WAN site and the corporate office, this incident could have affected almost any computer on the enterprise network. With this design, virus infections have the potential to run rampant and affect the entire company rather than being isolated by a more secure network design.

The Netopia router that connects this particular WAN site to the frame cloud is a model R5320 and is running a code release of 4.8.2. The frame circuit is running a full T1 or 1.544 mbps. This router does not have any filters or ACL's on it and contains merely a default route pointing it to the Corporate office. In order for users at this WAN site to access the Internet, they have to go through the Corporate office and out the Checkpoint Firewall and then out the Nortel BLN Internet router.

The firewalls run on a Nokia IP530 appliance which runs a proprietary OS called IPSO and it is version 3.6 FPS4. The firewall software running on the Nokia is CheckpointNG running feature pack 2. The policies on these firewalls are proprietary in nature to the Corporation and will therefore not be shown. Since almost everything in the screen shot would have to be sensitized, it is pointless to include it.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

One of the conditions for gaining access to the Internet for any type of service or protocol requires RADIUS authentication against the Active Directory in the Windows 2000 Domain. This means that your userid must exist in a particular group within the Active Directory, or you will not be authenticated through the firewall to access the Internet. There are a few services that are allowed outbound without authenticating: ftp, ntp, and telnet. There are also specific applications that have been allowed outbound connections to business partners on custom ports.

It should also be noted that inbound access through either of the firewalls is limited to the following:

- HTTP/HTTPS for access to corporate web servers
- SMTP for inbound email
- DNS for DNS updates
- FTP for access to corporate FTP servers

The routers between the firewalls and the Internet are Nortel BLN-2 routers running version 15.3.0.0 code. There are no outbound filters on these routers but there are several inbound filters that do things like block traffic from Asia and block traffic to broadcast addresses, etc. These inbound filters are not relevant to the discussion so I won't list each one of them.

Protocol description

BackOrifice2000 does not exploit a protocol or service. There are default ports that the program uses for the client-to-server communications but these are configurable and can be changed to any TCP or UDP port from 1 to 65,535. The default port for the base program is TCP port 54320. The default ports for the bo_peep plugin include TCP port 15151 for the VidStream module and TCP port 14141 for the Hijack module.

TCP and UDP both operate at layer four in the OSI (Open Systems Interconnection) model. In laymen's terms, this client-server program (BO2K) operates, in essence, like any other application, aside from the fact that it will work over TCP or UDP. Most applications use one or the other. For example, a web server listens or TCP port 80 and a client machine connects to this port with a browser to see web content or run web applications. This is the same with Back Orifice 2000. The server portion of this application listens on a pre-defined port and the client portion connects to the server with a custom built graphical user interface.

Obviously if an attacker wants better results from this application, they would choose to use TCP over UDP because of its reliability. TCP is a connection oriented transport layer protocol that provides end-to-end reliable communications. It is considered reliable because the application data is broken into segments to be passed to the IP layer. It is called connection oriented

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

because a connection is established between two computers and remains in tact until the data to be exchanged by the applications on both ends has occurred. The TCP connection is established with a three-way handshake. This handshake consists of a syn packet from the source, a syn-ack packet from the destination, and an additional ack pack from the source and the connection is established. TCP is responsible for ensuring that the data is divided into packets that are transmitted via IP (which contains the source and destination information and is responsible for the actual delivery of the data) and then reassembled on the other end. TCP also provides a checksum mechanism whereby any changes in the data during transit will alter the checksum and cause a re-transmission.

When a packet of data is sent, a timer will start and wait for an acknowledgement from the destination host that the data has been received. If an acknowledgment is not received from the destination before the timer expires, retransmission of the packet will occur and the timer will be longer this time. RFC 793 found at http://www.ietf.org/rfc/rfc0793.txt explains the transmission control protocl (TCP) as well as the three-way handshake.

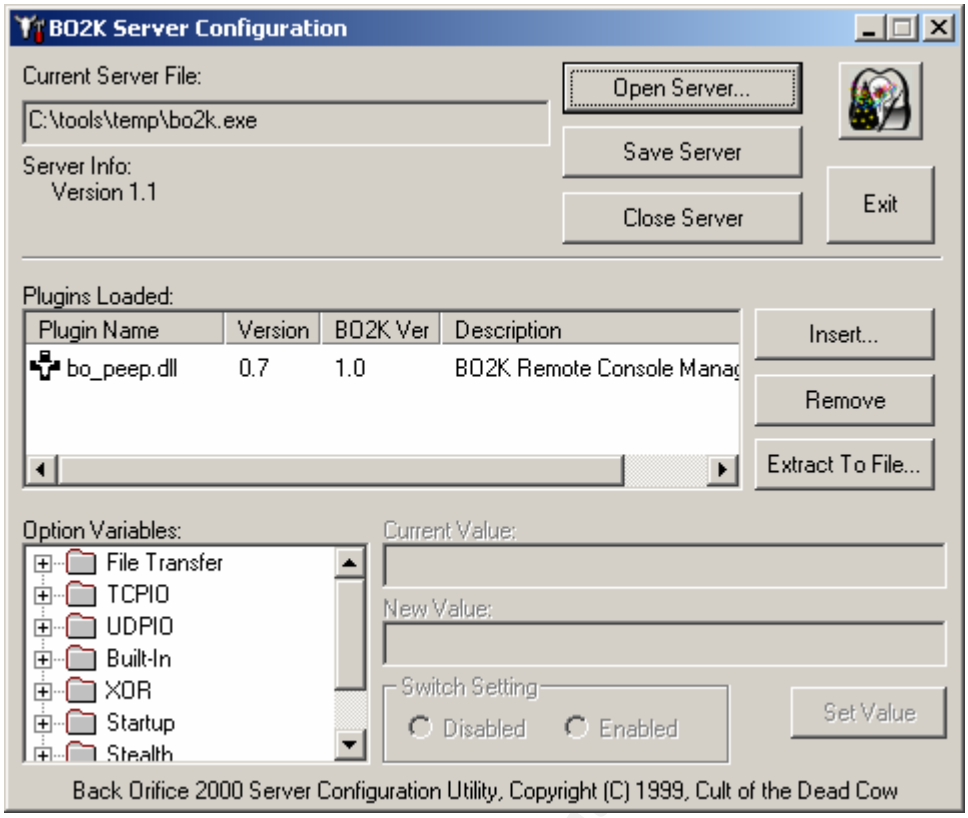
The other alternative for the Back Orifice 2000 communications would be to use UDP, which is considered a connectionless protocol and is much less reliable than TCP. In contrast to TCP, UDP provides very little in the way of error recovery when transmitting data. It is primarily used for broadcasting messages over a network. Also, UDP does not provide the service of dividing a message into packets and reassembling it on the other end like TCP does. Due to the fact that UDP also does not provide sequencing of packets that the data arrives in, the application using UDP must be able to make sure that the entire message has arrived and in the intended order. UDP is protocol 17 in the list of Internet Protocols found in RFC 762 (http://www.faqs.org/rfcs/rfc762.html). The user datagram protocol is defined by RFC 768 which can be found at http://www.faqs.org/rfcs/rfc768.html.

How the exploit works

Once an attacker downloads the compressed application files and unzips them, the first thing to do is configure the server by running the BO2Kcfg.exe file. It will bring up a configuration screen to set the parameters for the server executable. There will also be a window for setting the plug-in configurable items. The plug-in loaded in this example is called bo_peep. Most of this info can be found at http://sourceforge.net/docman/display_doc.php?docid=7864&group_id=4487

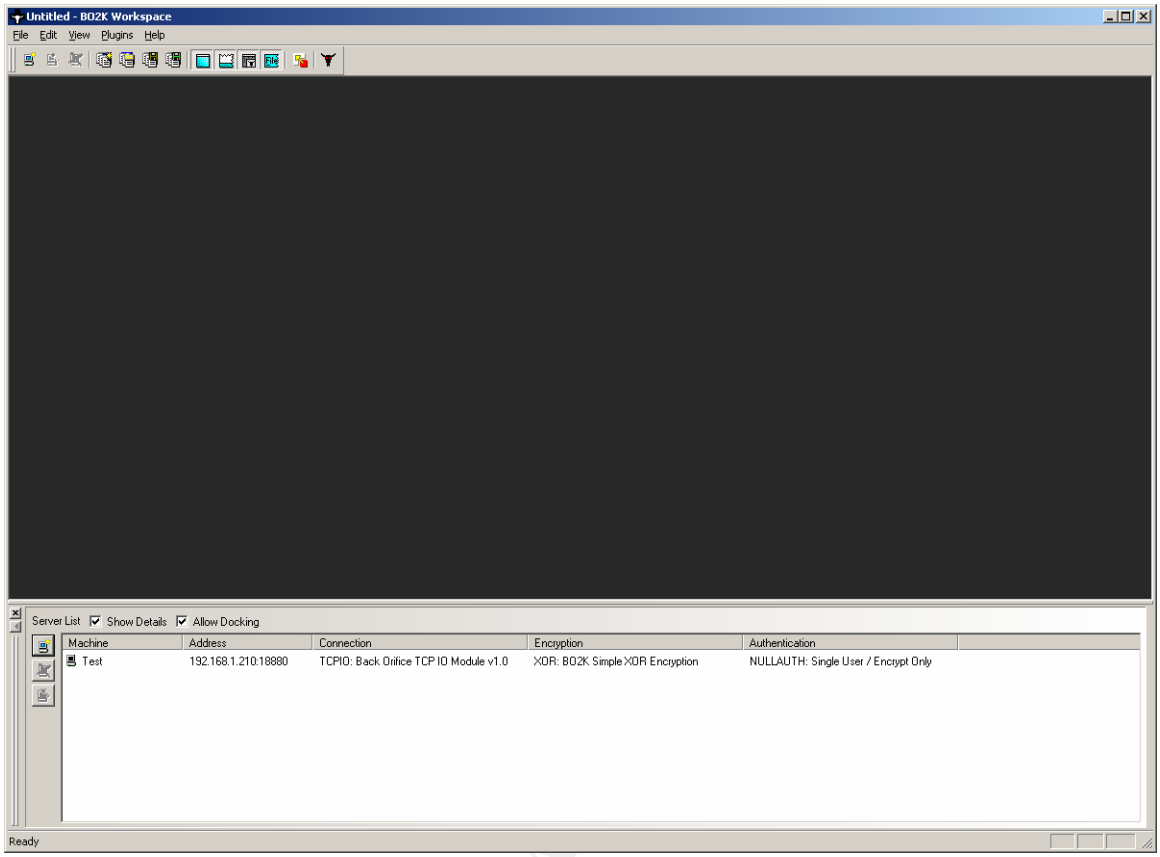
See below:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



When the server is configured as desired, the Save Server button should be clicked. At that point, the executable has to be copied over to the target machine and executed. The suggested methods for moving the executable to the target machine are IRC, Instant Messaging, or email. Once it is on the target machine, the server must be executed to work. It can be configured to use any TCP or UDP port and can also be configured to use XOR or 3DES encryption if you have the non-exportable version. An attempt was made to test this without encryption turned on and was unsuccessful in connecting to the server. Once you have run the executable on the server, you can then connect to it with the client application (BO2Kgui.exe). See screen shot below:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

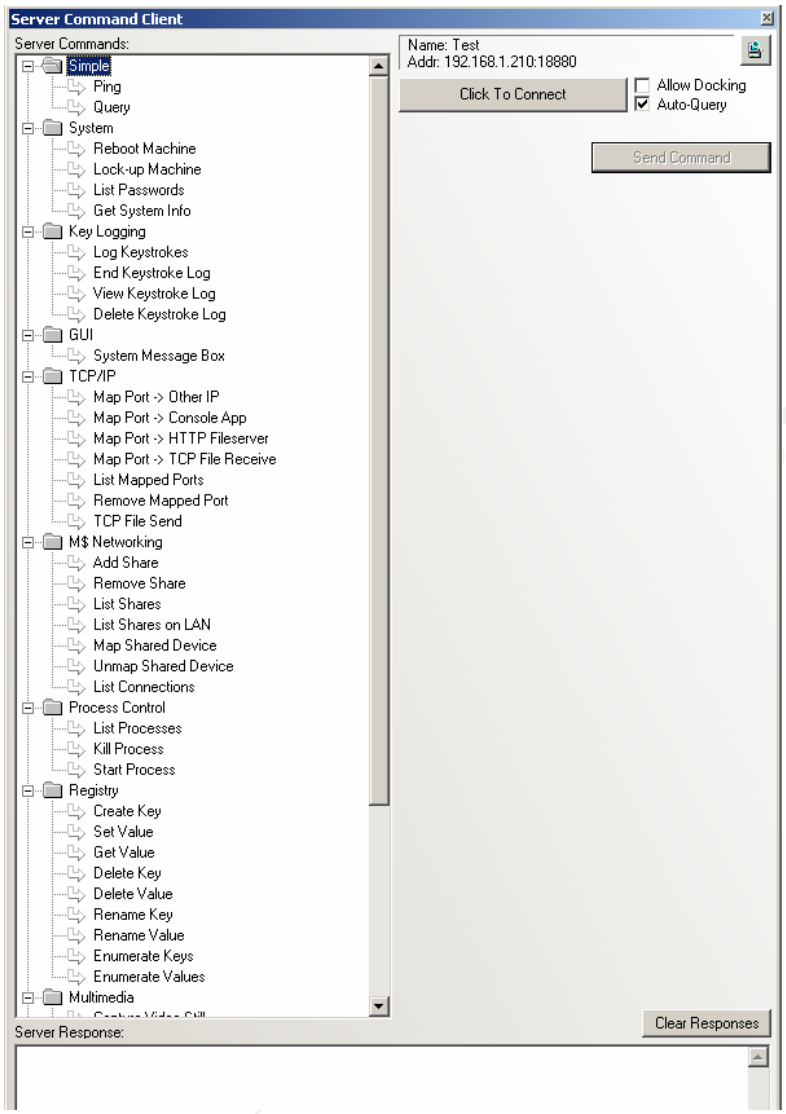


The buttons on the toolbar at the top are from right to left, new server, edit server, delete server, new workspace, open workspace, save workspace, save workspace as, activate color gradients, toggle status bar, toggle server list, toggle screen reader menus, client plug-ins setup, and about.

The buttons on the toolbar down the left hand side are new server, edit server and delete server.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

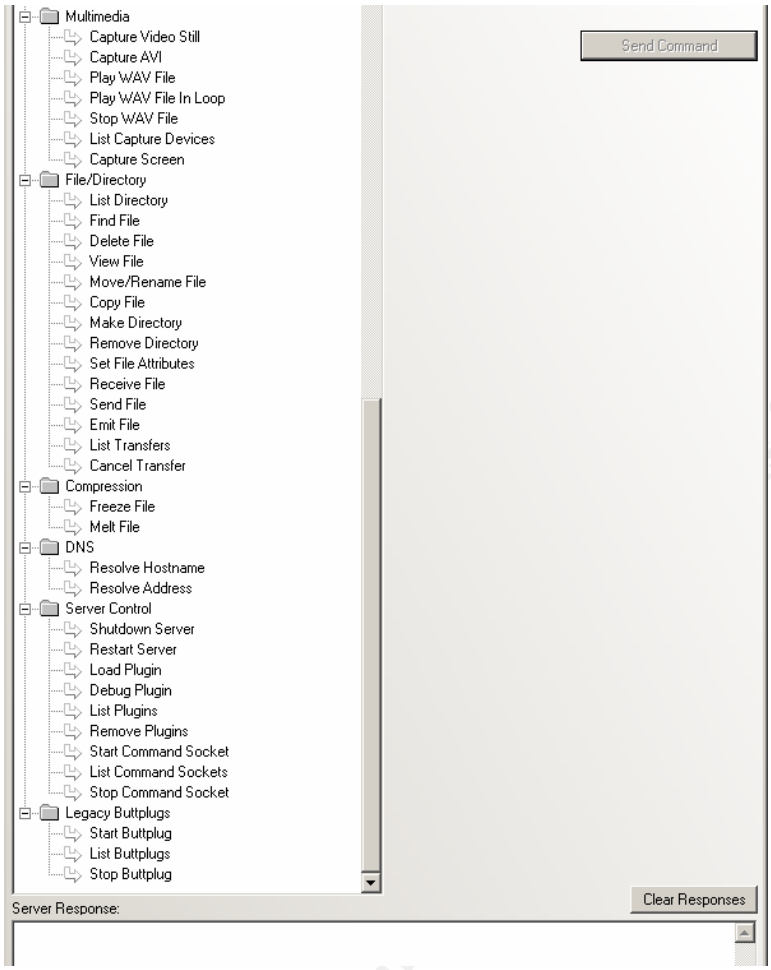
Once you connect, you will see the following list of commands that you can run against the server machine:



© SANS

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

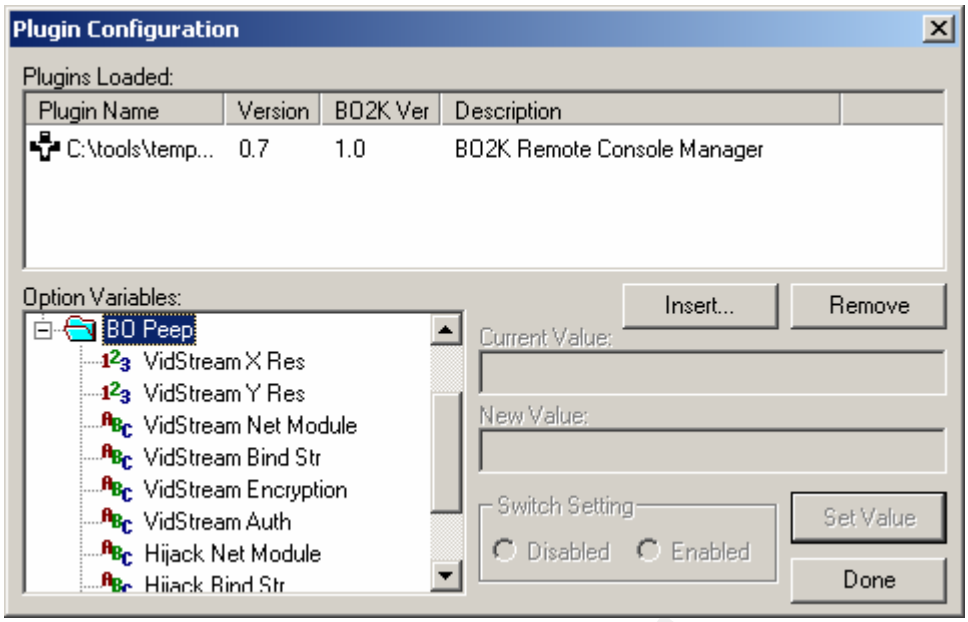
Here's the bottom half of that screen:



Once successfully connected to the server from the client, any of the commands seen in the above screen shots can be run and even more if you have plug-ins installed. In addition, the bo_peep plug-in can do remote monitoring of the server screen as well as remote control. The writer called the remote monitoring component a Hijack module.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

See below:



You can set the video stream to whatever resolution you like. The default settings are 160 by 120, which is a pretty small window, and is also cumbersome to manipulate. For testing purposes, I set mine to 640 by 480. The higher resolution will consume more bandwidth, which could be a factor over the Internet, but in a lab setting with both machines on a 100mb hub, it should not be a problem. The default TCP port for the VidStream module is 15151, and the default port for the Hijack module is 14141, which are both configurable.

Description and diagram of the attack

1. Although the ports used in the implementation of this trojan are configurable, it does default to TCP port 54320. Below we have some actual packet captures of this trojan horse application in action. As you can see from the following packet captures, the attacker had the BO2K server listening on port 18880. Notice in the first three packets the typical three-way handshake indicating that they configured their app to use TCP instead of UDP. I will also provide the packets in a table format that is a little easier to read. The first format is tcpdump output. Also the payload is not displayed for these packets due to the fact that they are encrypted and it appears non-readable in ASCII format.

09:51:06.331200 192.168.1.210.4154 > 192.168.1.100.18880: S [tcp sum ok] 2838015814:2838015814(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) (ttl 128, id 46682, len 48, bad cksum 0!)

09:51:06.335369 192.168.1.100.18880 > 192.168.1.210.4154: S [tcp sum ok] 5346503:5346503(0) ack 2838015815 win 8760 <mss 1460,nop,nop,sackOK> (DF) (ttl 128, id 41370, len 48)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

09:51:06.335955 192.168.1.210.4154 > 192.168.1.100.18880: . [bad tcp cksum 3764!] ack 1 win 64240 (DF) (ttl 128, id 46683, len 40, bad cksum 0!)

09:51:06.340934 192.168.1.210.4154 > 192.168.1.100.18880: P [bad tcp cksum 5177!] 1:18(17) ack 1 win 64240 (DF) (ttl 128, id 46684, len 57, bad cksum 0!)

09:51:06.565709 192.168.1.100.18880 > 192.168.1.210.4154: P [tcp sum ok] 1:226(225) ack 18 win 8743 (DF) (ttl 128, id 41626, len 265)

09:51:06.606225 192.168.1.210.4154 > 192.168.1.100.18880: P [bad tcp cksum eecd!] 18:62(44) ack 226 win 64015 (DF) (ttl 128, id 46685, len 84, bad cksum 0!)

09:51:06.938804 192.168.1.100.18880 > 192.168.1.210.4154: P [tcp sum ok] 226:315(89) ack 62 win 8699 (DF) (ttl 128, id 41882, len 129)

09:51:09.094470 192.168.1.210.4154 > 192.168.1.100.18880: . [bad tcp cksum fa63!] ack 315 win 63926 (DF) (ttl 128, id 46686, len 40, bad cksum 0!)

09:51:09.115290 192.168.1.100.18880 > 192.168.1.210.4154: P [tcp sum ok] 315:1711(1396) ack 62 win 8699 (DF) (ttl 128, id 42138, len 1436)

09:51:12.098865 192.168.1.210.4154 > 192.168.1.100.18880: . [bad tcp cksum 4c5d!] ack 1711 win 64240 (DF) (ttl 128, id 46687, len 40, bad cksum 0!)

	Source IP	Source Port	Dest IP	Dest Port	Size	Date	Timestamp	Info
1	IP-192.168.1.210	IP-4154	IP-192.168.1.100	IP-18880	66	3/31/2003	23:24.4	S=2838015814,L= 0,A= 0,W=64240
2	IP-192.168.1.100	IP-18880	IP-192.168.1.210	IP-4154	66	3/31/2003	23:24.4	S= 5346503,L= 0,A=2838015815,W= 8760
3	IP-192.168.1.210	IP-4154	IP-192.168.1.100	IP-18880	64	3/31/2003	23:24.4	Bad TCP checksum: 0x84A1, should be: 0xE8D8
4	IP-192.168.1.210	IP-4154	IP-192.168.1.100	IP-18880	75	3/31/2003	23:24.4	Bad TCP checksum: 0x84B2, should be: 0xFC03
5	IP-192.168.1.100	IP-18880	IP-192.168.1.210	IP-4154	283	3/31/2003	23:24.4	S= 5346504,L= 225,A=2838015832,W= 8743
6	IP-192.168.1.210	IP-4154	IP-192.168.1.100	IP-18880	102	3/31/2003	23:24.4	Bad TCP checksum: 0x84CD, should be: 0x52BC
7	IP-192.168.1.100	IP-18880	IP-192.168.1.210	IP-4154	147	3/31/2003	23:24.5	S= 5346729,L= 89,A=2838015876,W= 8699
8	IP-192.168.1.210	IP-4154	IP-192.168.1.100	IP-18880	64	3/31/2003	23:24.6	Bad TCP checksum: 0x84A1, should be: 0xE89B
9	IP-192.168.1.100	IP-18880	IP-192.168.1.210	IP-4154	1454	3/31/2003	23:24.6	S= 5346818,L= 1396,A=2838015876,W= 8699
10	IP-192.168.1.210	IP-4154	IP-192.168.1.100	IP-18880	64	3/31/2003	23:24.8	Bad TCP checksum: 0x84A1, should be: 0xE1ED

2. The following packet capture shows the attacking BO2K client running the command to list the processes running on the server. Again you will notice destination port of 18880 being used.

16:30:56.594805 192.168.1.210.4174 > 192.168.1.100.18880: P [bad tcp cksum fa4f!] 3217294120:3217294166(46) ack 6864719 win 64240 (DF) (ttl 128, id 47122, len 86, bad cksum 0!)

16:30:56.778180 192.168.1.100.18880 > 192.168.1.210.4174: P [tcp sum ok] 1:79(78) ack 46 win 8410 (DF) (ttl 128, id 47002, len 118)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

16:30:58.600335 192.168.1.210.4174 > 192.168.1.100.18880: . [bad tcp cksum dace!] ack 79 win 64162 (DF) (ttl 128, id 47123, len 40, bad cksum 0!)

16:30:58.613625 192.168.1.100.18880 > 192.168.1.210.4174: P [tcp sum ok] 79:834(755) ack 46 win 8410 (DF) (ttl 128, id 47258, len 795)

16:31:01.604684 192.168.1.210.4174 > 192.168.1.100.18880: . [bad tcp cksum dace!] ack 834 win 63407 (DF) (ttl 128, id 47124, len 40, bad cksum 0!)

	Source IP	Source Port	Dest IP	Dest Port	Size	Date	Timestamp	Info
1	IP-192.168.1.210	IP-4174	IP-192.168.1.100	IP-18880	104	3/31/2003	50:03.8	Bad TCP checksum: 0x84CF, should be: 0xD4C9
2	IP-192.168.1.100	IP-18880	IP-192.168.1.210	IP-4174	136	3/31/2003	50:03.8	S= 6864719,L= 78,A=3217294166,W= 8410
3	IP-192.168.1.210	IP-4174	IP-192.168.1.100	IP-18880	64	3/31/2003	50:03.9	Bad TCP checksum: 0x84A1, should be: 0x537C
4	IP-192.168.1.100	IP-18880	IP-192.168.1.210	IP-4174	813	3/31/2003	50:03.9	S= 6864797,L= 755,A=3217294166,W= 8410
5	IP-192.168.1.210	IP-4174	IP-192.168.1.100	IP-18880	64	3/31/2003	50:04.1	Bad TCP checksum: 0x84A1, should be: 0x537C

3. Finally, the attacker is seen connecting to the Vidstream and Hijack modules on the victim computer. You will notice the default ports 15151 and 14141 are being used and also the absence of the three-way handshake at the beginning since the session is already established. You will notice in packet 1 that port 14141 is being connected to on the server. This indicates that the Hijack portion of the BO Peep plugin is required to be activated first. Next you will notice in packet 4 that port 15151 is being connected to which is the Vidstream portion. This Vidstream portion is responsible for actually sending the video of what is being displayed on the server back to the client. The Hijack portion is used by the client to send commands to the server.

	Source IP	Source Port	Dest IP	Dest Port	Size	Date	Timestamp	Info
1	IP-192.168.1.210	IP-4176	IP-192.168.1.100	IP-14141	78	3/31/2003	05:39.3	Bad TCP checksum: 0x84B5, should be: 0x48BC
2	IP-192.168.1.100	IP-15151	IP-192.168.1.210	IP-4175	88	3/31/2003	05:39.5	S= 9392569,L= 30,A=3400458698,W= 8632
3	IP-192.168.1.100	IP-15151	IP-192.168.1.210	IP-4175	1518	3/31/2003	05:39.5	S= 9392599,L= 1460,A=3400458698,W= 8632
4	IP-192.168.1.210	IP-4175	IP-192.168.1.100	IP-15151	64	3/31/2003	05:39.5	Bad TCP checksum: 0x84A1, should be: 0xE04A
5	IP-192.168.1.100	IP-15151	IP-192.168.1.210	IP-4175	1422	3/31/2003	05:39.5	S= 9394059,L= 1364,A=3400458698,W= 8632
6	IP-192.168.1.100	IP-15151	IP-192.168.1.210	IP-4175	1518	3/31/2003	05:39.5	S= 9395423,L= 1460,A=3400458698,W= 8632
7	IP-192.168.1.210	IP-4175	IP-192.168.1.100	IP-15151	64	3/31/2003	05:39.5	Bad TCP checksum: 0x84A1, should be: 0xD542
8	IP-192.168.1.100	IP-15151	IP-192.168.1.210	IP-4175	1422	3/31/2003	05:39.5	S= 9396883,L= 1364,A=3400458698,W= 8632
9	IP-192.168.1.100	IP-15151	IP-192.168.1.210	IP-4175	107	3/31/2003	05:39.5	S= 9398247,L= 49,A=3400458698,W= 8632
10	IP-192.168.1.210	IP-4175	IP-192.168.1.100	IP-15151	64	3/31/2003	05:39.5	Bad TCP checksum: 0x84A1, should be: 0xD542
11	IP-192.168.1.100	IP-14141	IP-192.168.1.210	IP-4176	64	3/31/2003	05:39.5	S= 7805329,L= 0,A=3452544057,W= 7720
12	IP-192.168.1.210	IP-4176	IP-192.168.1.100	IP-14141	78	3/31/2003	05:39.6	Bad TCP checksum: 0x84B5, should be: 0x6D6C
13	IP-192.168.1.210	IP-4176	IP-192.168.1.100	IP-14141	78	3/31/2003	05:39.6	Bad TCP checksum: 0x84B5, should be: 0x2967
14	IP-192.168.1.100	IP-14141	IP-192.168.1.210	IP-4176	64	3/31/2003	05:39.6	S= 7805329,L= 0,A=3452544097,W= 7680
15	IP-192.168.1.210	IP-4176	IP-192.168.1.100	IP-14141	78	3/31/2003	05:39.7	Bad TCP checksum: 0x84B5, should be: 0x8667
16	IP-192.168.1.100	IP-14141	IP-192.168.1.210	IP-4176	64	3/31/2003	05:39.8	S= 7805329,L= 0,A=3452544117,W= 7660
17	IP-192.168.1.210	IP-4176	IP-192.168.1.100	IP-14141	78	3/31/2003	05:39.9	Bad TCP checksum: 0x84B5, should be: 0x3C6D

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

18	IP-192.168.1.210	IP-4176	IP-192.168.1.100	IP-14141	78	3/31/2003	05:40.0	Bad TCP checksum: 0x84B5, should be: 0x3146
19	IP-192.168.1.100	IP-14141	IP-192.168.1.210	IP-4176	64	3/31/2003	05:40.0	S= 7805329,L= 0,A=3452544157,W= 7620
20	IP-192.168.1.210	IP-4176	IP-192.168.1.100	IP-14141	78	3/31/2003	05:40.0	Bad TCP checksum: 0x84B5, should be: 0x3647

Once the initial client-to-server connection was established the victim box was completely controlled by the attacking BO2K client and there was almost no limit as to what could be done. See http://sourceforge.net/docman/display_doc.php?docid=12856&group_id=4487 for a complete reference of commands available to the client. This does not account for the enhancements made by plug-ins (see the url below for these) http://www.roe.ch/bo2k.shtml. Also, a favorite plug-in of the BO2K users involves the file browsing and registry editing from the L0pht plug-in called BOTOOL (see the following URL for info - http://www.winnetmag.com/Articles/Index.cfm?ArticleID=7256).

Signature of the attack

The signatures for Back Orifice 2000 in the ISS Site Protector application are not exactly open source, but they do give a few important details as seen below. To date I have been unable to find any open source signatures for Back Orifice 2000. It appears that the highly configurable and stealthy features (ports, protocols) in this trojan have kept the open source community from writing IDS signatures to detect this. The signatures listed below were developed by the ISS X-Force and were obtained from the documentation within the ISS Site Protector application:

Back Orifice 2000 allows complete remote administrative control (BackOrifice2K_TCP_Auth_Request)
About this signature or vulnerability
RealSecure Network Sensor: This signature detects TCP packets for which the first byte of the sequence number is a function of the packet length and where the remainder of the packet is composed of a character of value '69' (decimal). These packets indicate an attacker's attempt to locate an instance of the Back Orifice 2000 backdoor on a host.

Back Orifice 2000 allows complete remote administrative control (BackOrifice2K_TCP_Auth_Response)
About this signature or vulnerability
RealSecure Network Sensor: This signature detects TCP packets for which the first byte of the sequence number is a function of the packet length and where the remainder of the packet is composed of a character of value '0'. These packets indicate a positive response made by an infected host to BackOrifice authentication request.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Back Orifice 2000 allows complete remote administrative control (BackOrifice2K_TCP_Request)
About this signature or vulnerability
RealSecure Network Sensor: This signature detects TCP packets that match specific Back Orifice 2000 command packet sizes and specific Back Orifice 2000 argument lengths, as represented by the packet data, and where particular data bytes match Back Orifice 2000 command structures.

Back Orifice 2000 allows complete remote administrative control (BackOrifice2K_TCP_Response)
About this signature or vulnerability
RealSecure Network Sensor: This signature detects TCP packets that match specific Back Orifice 2000 command response sizes and specific Back Orifice 2000 argument lengths as represented by the packet data, and where particular data bytes match Back Orifice 2000 response structures.

Back Orifice 2000 allows complete remote administrative control (BackOrifice2K_UDP_Auth_Request)
About this signature or vulnerability
RealSecure Network Sensor: This signature detects UDP packets for which the first byte of the sequence number is a function of the packet length and where the remainder of the packet is composed of a character of value '69' (decimal). These packets indicate an attacker's attempt to locate an instance of Back Orifice 2000 on a host.

Back Orifice 2000 allows complete remote administrative control (BackOrifice2K_UDP_Auth_Response)
About this signature or vulnerability
RealSecure Network Sensor: This signature detects UDP Auth packets that match specific Back Orifice 2000 command response sizes and specific Back Orifice 2000 argument lengths as represented by the packet data, and where particular data bytes match Back Orifice 2000 response structures.

Back Orifice 2000 allows complete remote administrative control (BackOrifice2K_UDP_Request)
About this signature or vulnerability
RealSecure Network Sensor: This signature detects UDP packets that match specific Back Orifice 2000 command packet sizes and specific Back Orifice 2000 argument lengths as represented by the packet data, and where particular data bytes match Back Orifice 2000 command structures.
Back Orifice 2000 allows complete remote administrative control (BackOrifice2K_UDP_Response)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

About this signature or vulnerability
RealSecure Network Sensor: This signature detects UDP packets that match specific Back Orifice 2000 command response sizes and specific Back Orifice 2000 argument lengths as represented by the packet data, and where particular data bytes match Back Orifice 2000 response structures.

Back Orifice default installation (BackOrifice_Ping)
About this signature or vulnerability
RealSecure Network Sensor: This signature detects an attempt to locate systems running the "Back Orifice" backdoor. Unless the system responds, it is unlikely that it has been compromised. Back Orifice pings are among the most frequent kind of attack seen on the Internet.

Back Orifice default installation (BackOrifice_Request)
About this signature or vulnerability
RealSecure Network Sensor: This signature detects a command request to a "Back Orifice" backdoor. Unless the system responds, it is unlikely that it has been compromised.

Back Orifice default installation (BackOrifice_Response)
About this signature or vulnerability
RealSecure Network Sensor: This signature detects a command response from a "Back Orifice" backdoor. The system is infected with Back Orifice.

In the security advisory (http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?id=advise31) released by the ISS X-Force on BO2K, they give some detailed information on the packet structure and how to decrypt the XOR encryption key. See below:

The format of the BO2k packets is

[Length (4 bytes)][Data that is 'Length' long]

By looking for a series of packets that contain a 4 byte length (in little-endian byte order), followed by that length of data, you can detect all BO2k packets, regardless of the encryption used. This format is used on both the TCP and UDP transports.

To decrypt the packets using the XOR encryption, XOR the 4 bytes starting at offset 4 with the value 0x3713C3CD (0xCDC31337 in little-endian order). This will give you the XOR encryption key, which is generated from the XOR key configured by the user. You can then XOR that 4 byte key with the rest of the packet -- XOR it with the 4 bytes at

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

offset 8, 12, 16, etc. This will reveal a packet structure that is described in the BO2k source code.

How to protect against it

The best way to protect a computer from being infected by this trojan is to have anti-virus software installed and up-to-date with the latest virus signatures. The Vericept View product was also a tremendous asset in the identification of the hacker research that was done. The network security component of Vericept would have most likely recognized the trojan activity as well if this had been used to access a server via the Internet. Vericept and ISS Site Protector are the two components that monitor traffic flowing through the Internet gateways for the company and it's likely that Site Protector would also have recognized this trojan activity.

In a corporate setting, there are other methods to prevent unauthorized software from being installed. Assuming that most corporations these days have Win2k domains and that the workstations are members of the domain, the simplest method to prevent normal users from doing this is by not allowing them to be local administrators. Most applications these days won't install if you are not a local administrator. This may not apply in the case of certain trojans however since they might be able to affect critical files and services without admin access, especially if the machine has not been hardened in any way.

Another method to protect against unauthorized software from being installed is to deploy desktop firewalls throughout the organization that have application protection built-in. This will take a snapshot of applications currently installed on your computer, add them to the approved applications list, and then prevent other programs from being installed without the end-users approval. This would of course be pointless if you install the application protection after a trojan is already on your computer. The firewall would think that this trojan is an approved application and let it run without interference. Therefore, it's good to install this firewall after a thorough virus scan or either right after the OS has been installed and the machine has not yet connected to the Internet.

A third method that could be used in a corporate environment would be to apply group policies to all users in the domain (assuming you are running Windows workstations and a WindowsNT or higher domain). Group policies have some great benefits (including prevention of applications being installed) but do not work if users are allowed to logon with local user accounts and not forced to logon with domain accounts.

Intrusion Detection Systems, either open source or commercial versions, provide a great method for protecting networks against most attacks. Most IDS systems are signature based, just like anti-virus software, and therefore don't work properly if you don't keep the signatures updated. There are some IDS systems

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

that are anomaly based that use a baseline for normal network traffic and alert the security administrator whenever there is traffic "out of the norm". While these systems are by no means full-proof, they greatly enhance your chances for detecting traffic on your network that may be non-desirable, possibly illegal, and on occasion may affect business continuity.

It appears that some of the up and coming trends in the Intrusion Detection industry include such things as event correlation and Intrusion Prevention. Event correlation has been presented to me in two different ways.

One way is to take logs from a multitude of devices (router, firewall, IDS, servers) and consolidate them in one application. This way, you can actually see the progression of an event all the way through your network and validate that it was successful or not.

The second way that event correlation has been presented to me is to perform a vulnerability assessment against a host server and store that information in a database. Therefore, when an attack is seen on the network or locally against that host, correlation can occur to determine if this attack would even be successful. If it is determined that this host is vulnerable to a particular exploit and that exploit is actively being used to attack this host, then the IDS software would escalate the priority of this alert to the highest level. Conversely, if a host was known to be patched for a particular vulnerability and the IDS system detected that exploit being run against that host, then the IDS software would lower the priority on that event.

The up and coming Intrusion Prevention technology tries to take the IDS technology one step further by preventing the intrusion from happening rather than just detecting and reporting on it. At least one vendor that I know of, (Okena – recently purchased by Cisco) if not more by now, have host based technology that prevents intrusions all together. This software purports the ability to detect and prevent things like buffer overflows, trojans, port scans, SYN floods, etc. It's really quite remarkable what they've accomplished if it does all they claim it does. From what I've seen in articles from infoworld.com and informationweek.com, there are some loud praises being sung for this solution. It may be well worth the money, whatever they are charging.

PART 3 – THE INCIDENT HANDLING PROCESS

Preparation

In order to prepare for computer security incidents, the company has several countermeasures in place to thwart would-be incidents and / or hackers. Although this is not how the incident was actually discovered, the initial countermeasure that detected the beginning of the incident was the detection of hacker activity by the linguistic analysis engine of the Vericept View filter. This detected actual Internet searches done on Yahoo in which the suspect was

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

looking for the following keywords: "trojans", then "trojan horse download", then "trojan horse hacker download". Once they got the trojan downloaded to their local computer, the second countermeasure kicked in which is the corporate anti-virus solution. Trend Microsystems tried to delete the trojan as soon as it appeared in the local file system.

At the time this incident occurred, there were not any clearly defined written procedures at the corporation for handling computer security incidents. Also, the incident response team or CIRT was not in existence at the time of the incident. The individuals actually involved in the investigation included two information security engineers, the Director of Information Security, and the anti-Virus Administrator.

A few other methods of preparation should be discussed for this topic to be fully covered. The first is physical security. The company has taken physical security to a fairly high level with restricted access to two secured data centers, video surveillance throughout the corporate offices and a large staff of security personnel to man the gated entrance to the property and monitor the video cameras and front lobby.

The other method of preparation needing discussion is training or user education. I feel this is one of the most integral parts of a complete security solution. Your network is only as secure as the weakest link, which typically involves an unknowing, uneducated end-user opening an attachment they shouldn't or downloading some files they shouldn't. The company has an acceptable Internet/Email usage policy and a generalized security policy, both of which require signatures before the employee is given an NT account to access the network. The employee is also verbally made aware of some of the specifics in these policies during their first week of employment. During this week they are required to sit through several orientation classes that cover this material. However, there are no follow up classes that continue to educate users and these definitely need to be developed. Also, training of in-house IT staff is a must to insure that IT personnel are educated as to common security practices. It would be especially good if in-house developers / programmers were educated on secure programming practices. This would greatly enhance the possibility for more secure in-house applications.

Additionally, the company educates the end-users through a monthly newsletter published on the corporate Intranet. The S.A.F.E. (Security Awareness For Employees) section covers different topics each month to keep people on their toes regarding common practices. The articles cover such things as e-mail etiquette, password management, Instant Messaging, SPAM, etc.

Identification

Little confirmation was needed once we saw what had been downloaded to the individual's computer. Three main countermeasures exist in the company for

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

protecting corporate assets -- anti-virus, content filtering, and Intrusion Detection Systems. The anti-virus and content filtering solutions identified this incident immediately and it's likely the IDS solution would have caught it if this type of traffic had been flowing through one of our Internet gateways. Since the incident was controlled before the individuals had a chance to deploy this so called "remote administration software", our Intrusion Detection Systems were never tripped because the Internet gateways were not traversed with any packets related to this activity.

There were exactly five minutes between the time that Trend detected BO2K on the system and the time we received an email from the Virus Administrator. For the purposes of better understanding, userid1 correlates to the data coordinator – manager, and userid2 correlates to the IT support person. Here's the original email:

From: AV Admin
Sent: Tuesday, February 11, 2003 11:23 AM
To: IT Security
Subject: CPQxxxxxxxxxxx - Back Orifice
Follow Up Flag: Review
Due By: Friday, May 02, 2003 12:18 PM
Flag Status: Flagged

This looks like a hacker tool. What do you think?
-----Original Message-----
From: OfcScan [mailto:OfcScan]
Sent: Tuesday, February 11, 2003 11:19 AM
To: Virus Alerts

Virus Alert!!
TROJ_BO2K is detected on CPQxxxxxxxxxxx(userid1) in Default domain.
Infected file: C:\Documents and Settings\userid1.CPQxxxxxxxxxxx\Local Settings\Temporary Internet Files\Content.IE5\QPY3AFUF\BO2K_1_0_full[1].exe
Action: Clean Failed (Delete Failed)
Detection date: 2003.02.11 12:17:39

The computer involved in the incident was on the east coast, and the corporate office is in the central time zone, so there's a one-hour reverse differential from the Trend alert and the Virus Administrator's email. The userid in this alert belonged to the manager at the facility.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

For some reason at this point, the IT person decided to logon as himself and try the same thing. I suspect he thought the trojan was deleted by Trend. See the second Trend alert below:

From: AV Admin
Sent: Tuesday, February 11, 2003 11:25 AM
To: IT Security
Subject: CPQxxxxxxxxxxx - same computer, different user
Follow Up Flag: Review
Due By: Friday, May 02, 2003 12:20 PM
Flag Status: Flagged

Back Orifice
-----Original Message-----
From: OfcScan [mailto:OfcScan]
Sent: Tuesday, February 11, 2003 11:21 AM
To: Virus Alerts

Virus Alert!!
TROJ_BO2K is detected on CPQxxxxxxxxxxx(userid2) in Default domain.
Infected file: C:\Documents and Settings\userid2.CPQxxxxx\Local Settings\Temporary Internet Files\Content.IE5\29YFWRIL\BO2K_1_0_full[1].exe
Action: Clean Failed (Delete Failed)
Detection date: 2003.02.11 12:18:31

Here's another email from the Virus Administrator:

From: AV Admin
Sent: Tuesday, February 11, 2003 11:30 AM
To: IT Security
Subject: CPQxxxxxxxxxxx again
Follow Up Flag: Review
Due By: Friday, May 02, 2003 12:27 PM
Flag Status: Flagged

FYI:
We've had over 35 alerts for this computer so far, and it looks like it could be a hacker tool. A lot of these are getting deleted by Trend, but I thought y'all would like to know.
-----Original Message-----
From: OfcScan [mailto:OfcScan]
Sent: Tuesday, February 11, 2003 11:27 AM
To: Virus Alerts

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Virus Alert!!
TROJ_BO2K is detected on CPQxxxxxxxxxxx(userid2) in Default domain.
Infected file: C:\TEMP\BO2Kgui.exe
Action: Clean Failed (Deleted)
Detection date: 2003.02.11 12:24:03

One more email from the Virus Administrator later that afternoon showing the BO2Kgui.exe on the data coordinator's machine:

From: AV Admin
Sent: Tuesday, February 11, 2003 3:03 PM
To: IT Security
Subject: CPQxxxxxxxxx again
Follow Up Flag: Review
Due By: Friday, May 02, 2003 4:02 PM
Flag Status: Flagged

Just FYI...
-----Original Message-----
From: OfcScan [mailto:OfcScan]
Sent: Tuesday, February 11, 2003 3:02 PM
To: Virus Alerts

Virus Alert!!
TROJ_BO2K is detected on CPQxxxxxxxxxxx(userid1) in Default domain. Infected file: C:\Documents and Settings\userid1.CPQxxxxxxxxxxx\Desktop\INFO\ DOWNLOADS\BO2Kgui.exe Action: Clean Failed (Deleted)
Detection date: 2003.02.11 16:01:55

Attached below is a spreadsheet of the Trend virus logs regarding the computer in question:

VLF_VirusName	ActionResult	VLF_FileName	VLF_FilePath
TROJ_BO2K	Delete Failed	bo_peep.dll	C:\Documen~\userid2\Desktop\
TROJ_BO2K	Delete Failed	BO2K_1_0_full[1].exe	C:\Documen~\userid1\Local~\Tempora~\-
TROJ_BO2K	Delete Failed	BO2K_1_0_full[1].exe	C:\Documen~\userid1\Local~\Tempora~\
TROJ_BO2K	Delete Failed	BO2Kgui.exe	C:\Documen~\userid2\Desktop\
TROJ_BO2K	Delete Failed	bo_peep.dll	C:\Documen~\ userid2\Desktop\
TROJ_BO2K	Delete Failed	bo_peep.dll	C:\Documen~\ userid2\Local~\Tempora~\

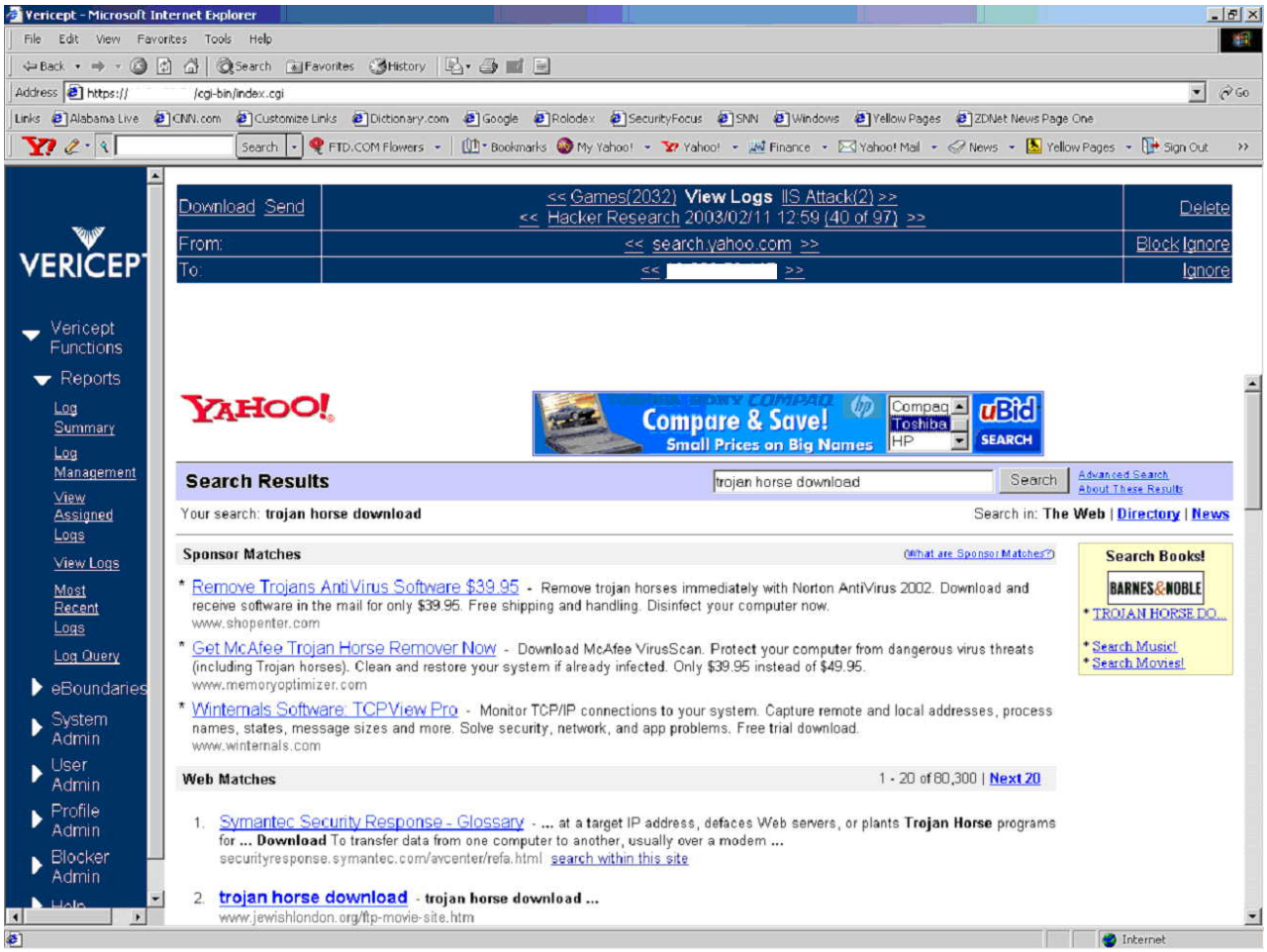
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TROJ_BO2K	Delete Failed	BO2K.exe	C:\Documen~\ userid2\Desktop\
TROJ_BO2K	Delete Failed	BO2K.exe	C:\Documen~\ userid2\Local~\Tempora~\
TROJ_BO2K	Delete Failed	BO2Kcfg.exe	C:\Documen~\ userid2\Desktop\
TROJ_BO2K	Delete Failed	BO2Kcfg.exe	C:\Documen~\ userid2\Local~\Tempora~\
TROJ_BO2K	Delete Failed	BO2Kgui.exe	C:\Documen~\ userid2\Desktop\
TROJ_BO2K	Delete Failed	BO2Kgui.exe	C:\Documen~\ userid2\Local~\Tempora~\
TROJ_BO2K	Deleted	bo_peep.dll	C:\TEMP\
TROJ_BO2K	Deleted	BO2K.exe	C:\TEMP\
TROJ_BO2K	Deleted	BO2Kcfg.exe	C:\Documen~\ userid2\Local~\Tempora~\
TROJ_BO2K	Deleted	BO2Kcfg.exe	C:\TEMP\
TROJ_BO2K	Deleted	BO2Kgui.exe	C:\Documen~\userid1\Desktop\Info\Downloa ~\
TROJ_BO2K	Deleted	BO2Kgui.exe	C:\TEMP\
TROJ_BO2K	Delete Failed	BO2K.exe	C:\Documen~\ userid2\Local~\Tempora~\---
TROJ_BO2K	Delete Failed	BO2Kcfg.exe	C:\Documen~\ userid2\Local~\Tempora~\---

Below are actual screen shots from the Vericept View product that show the Yahoo search results:

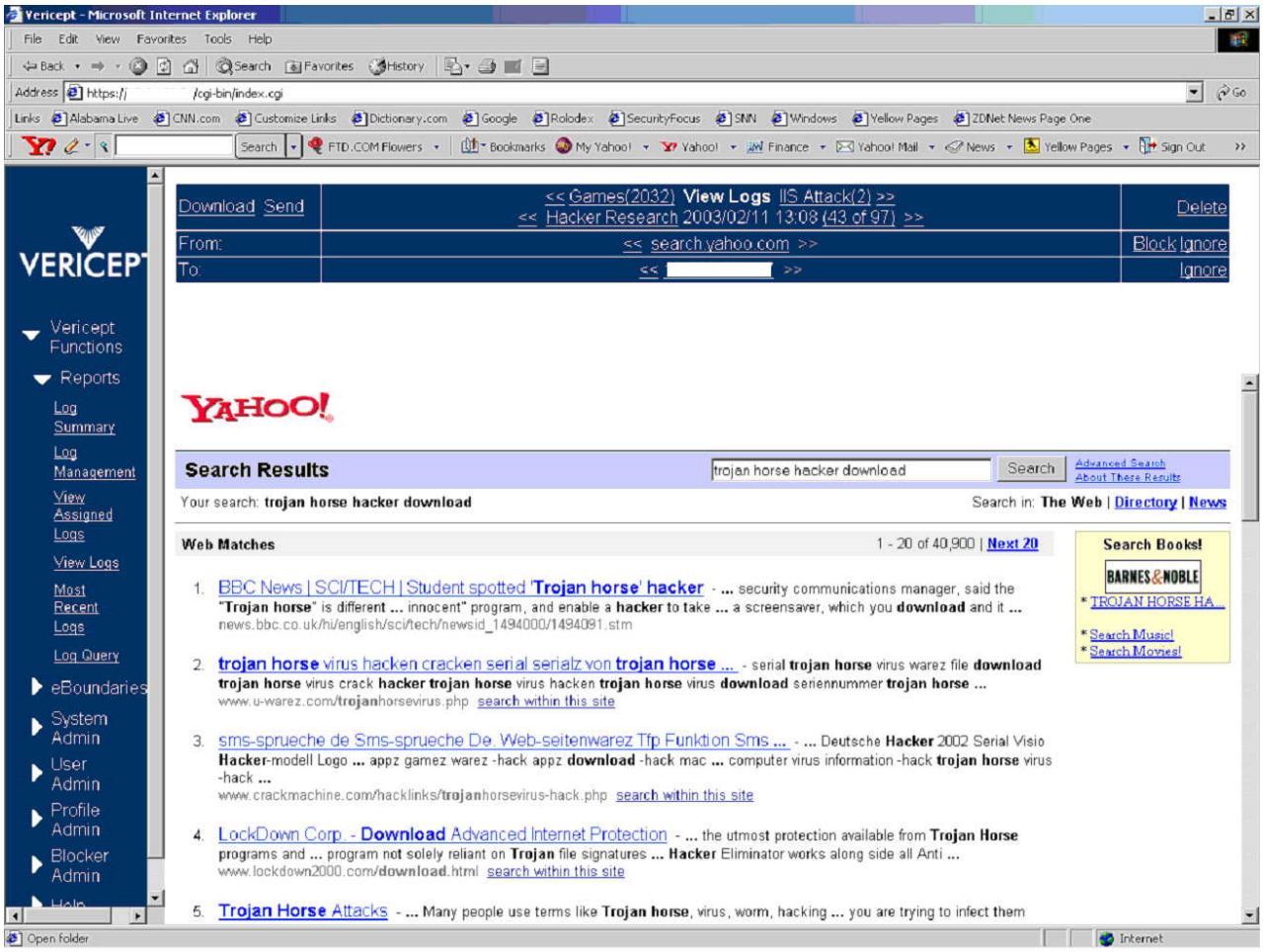
© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



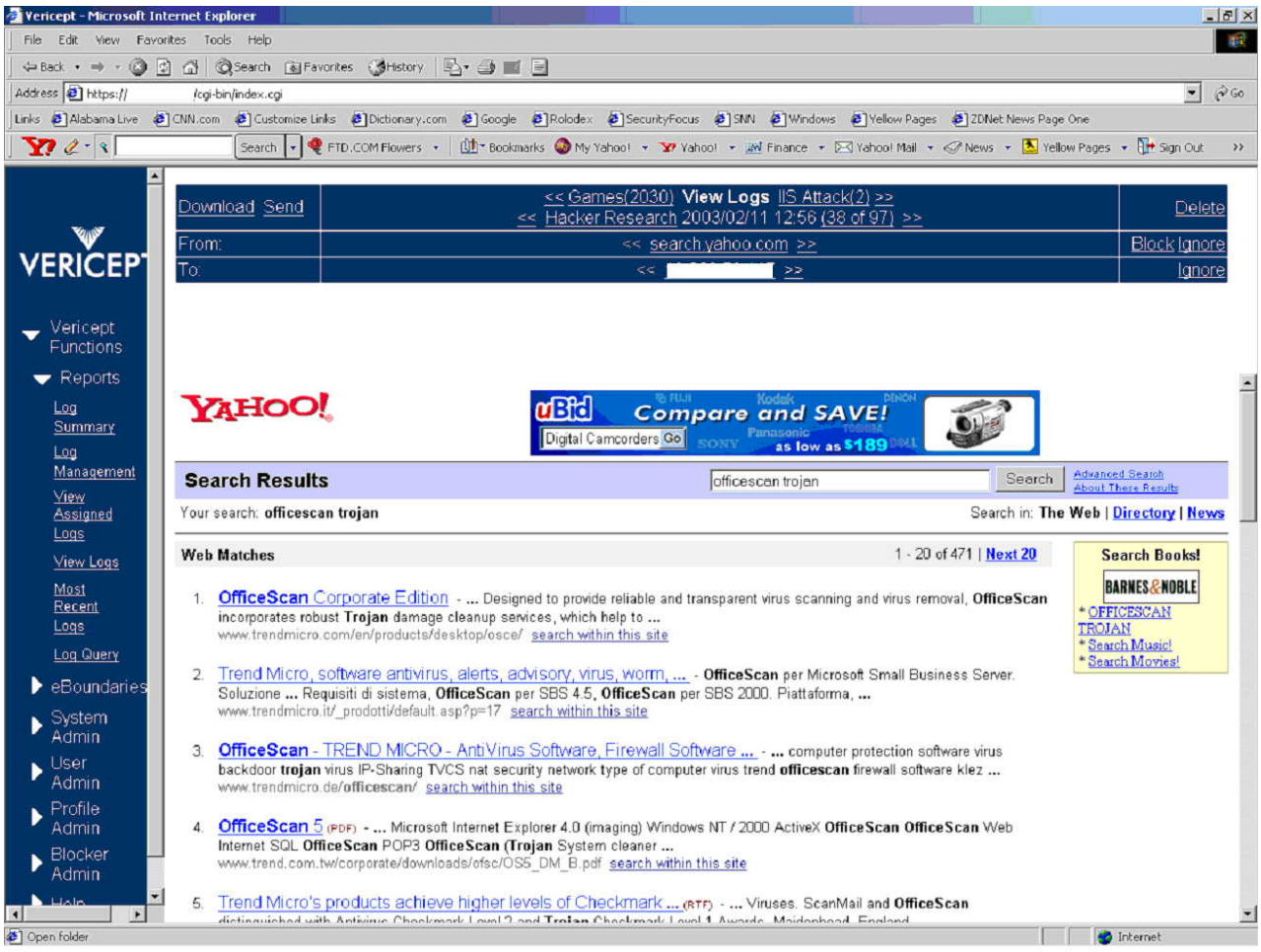
© SANS Institute 2003,

As part of GIAC practical repository. Author retains full rights.

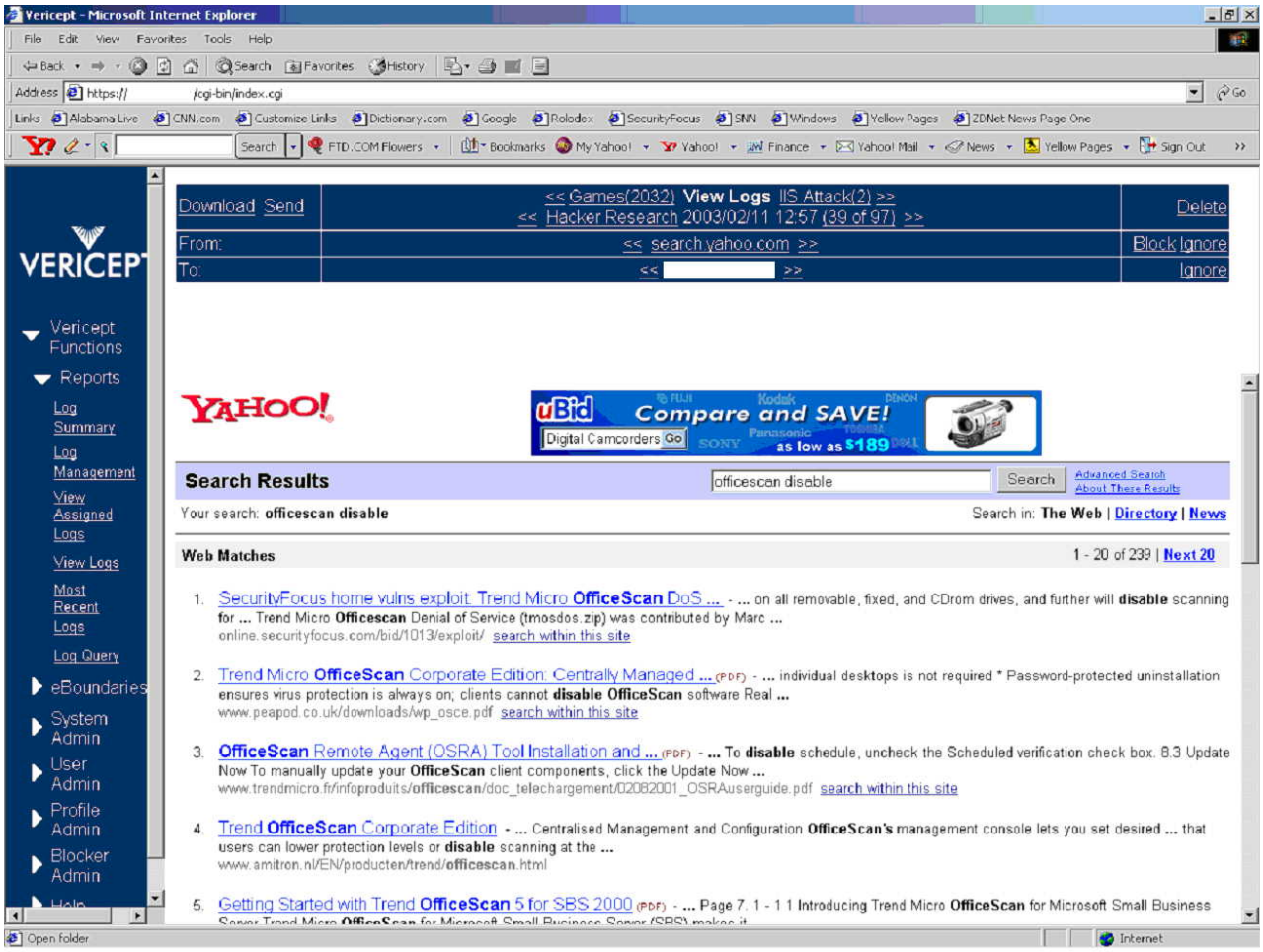


Below are the screen shots from Vericept that show where they tried to find out how to disable the Trend anti-virus software:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Since the Director of IT Security for the company was on vacation when the incident occurred the Security Engineers investigating the incident were not able to get the hard drives shipped until three days had passed. The incident occurred on a Tuesday, and the Director of IT Security returned to work on Friday of that week. He immediately addressed the issue with the Office manager at the remote facility and the Human Resources Director. This resulted in the two employees immediately being placed on administrative leave until the matter could be resolved. The Directory of IT Security immediately instructed to isolate the computers involved away from other staff and had the hard drives removed and shipped overnight to the corporate office.

Since there were actually two separate IP addresses that showed up in Vericept as accessing the BO2K.sourceforge.net website, we had both drives shipped to the house of the Director of IT Security for Saturday delivery. Once the drives arrived, we began a forensic analysis of the drives with Encase. The chain of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

custody procedures were non-existent at the time since there was no incident response policy in place, and the original hard drives were used for evidence.

Below are the images that Encase discovered on the data coordinator's hard drive relating to the trojan:

Images

1) Drive 0\C\Documents and Settings\xxxxx.CPQxxxxxxxxxxx\Local Settings\Temporary Internet Files\Content.IE5\UPAJ0XQP\linuxpic[1].gif



2) Drive 0\C\Documents and Settings\xxxxx.CPQxxxxxxxxxxx\Local Settings\Temporary Internet Files\Content.IE5\QTANKPS5\header[1].gif



3) Drive 0\C\Documents and Settings\xxxxx.CPQxxxxxxxxxxx\Local Settings\Temporary Internet Files\Content.IE5\QTANKPS5\BO2K10pic[1].gif



4) Drive 0\C\Documents and Settings\xxxxx.CPQxxxxxxxxxxx\Local Settings\Temporary Internet Files\Content.IE5\UPAJ0XQP\cdclogo1[1].gif



5) Drive 0\C\Documents and Settings\xxxxx.CPQxxxxxxxxxxx\Local Settings\Temporary Internet Files\Content.IE5\QTANKPS5\screen1[1].gif

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



6) Drive 0\C\Documents and Settings\xxxxx.CPQxxxxxxxxxxx\Local Settings\Temporary Internet Files\Content.IE5\QPY3AFUF\BO2Kscr[1].jpg



It should also be noted in this Identification section that several steps should be considered when gathering information on a compromised Windows NT/2000 machine. There can be valuable forensic data retrieved from the compromised computer which is considered volatile. The reason that this data is volatile is because it reflects the current state of the system (including physical memory, virtual memory, caches, network connections, running processes, etc.) and is subject to change. If the compromised machine were rebooted before the specifics of this volatile data were collected, each of the previously cited examples would or could all be drastically different. There are other considerations to deal with as well:

- Is the intruder still currently accessing the box?
- Did the intruder leave behind any "booby traps"?
- Has the compromise affected system operations?
- Should law enforcement be involved?

There are many freely available tools to investigate the volatile data on compromised systems. These tools need to do things such as:

- List shares on the system
- Terminate selected tasks or processes
- Create a copy of the Event Viewer Logs
- Display all file system activity in real time

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Display all registry activity in real time
- Display what files are open by which processes
- Display all DLLs that are currently loaded including path and version
- Generate checksums of files and provide verification
- Map application processes to the ports they listen on

This is just a beginning to the many tasks that need to be accomplished on a compromised system. Another thought to remember is that the system could actually have a rootkit installed which compromises the kernel of the system. Therefore, any information obtained from a system with a rootkit would be deemed suspect but noteworthy (Scambray, McClure & Kurtz).

Containment

Since the incident response procedures for the company did not exist at the time of the incident, there was obviously no jump kit available to conduct the investigation with. The steps taken to contain the issue were grossly inadequate in retrospect. It was three days after the incident actually occurred that the individuals in question were suspended from work. If they truly had malicious intentions, they could have done irreparable damage in that time.

Being that these individuals were apparently not experienced hackers as previously stated, it appears we are lucky that they were scared enough by the Office Manager to at least temporarily discontinue this type of activity. The IT support person ended up being terminated, the data coordinator kept his job. This was a decision from executive management and therefore not within the jurisdiction of the Director of Security.

As for containing the damage, a ping sweep of the LAN involved was conducted to determine which hosts were up. Below are the commands done for this scan using nmap:

```
[root@xxxxxxxx root]# nmap -e eth0 -sP a.b.c.d/24
results excluded for sanitization purposes.
Nmap run completed -- 256 IP addresses (34 hosts up) scanned in 97
seconds
```

A port scan of the two computers that were involved with the incident was then conducted. Below are the commands done for this type scan using nmap:

```
[root@xxxxxxxx root]# nmap -e eth0 -sS a.b.c.d
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on xxxxxxxx (a.b.c.d):
(The 1538 ports scanned but not shown below are in state: closed)
Port       State       Service
135/TCP    open        loc-srv
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

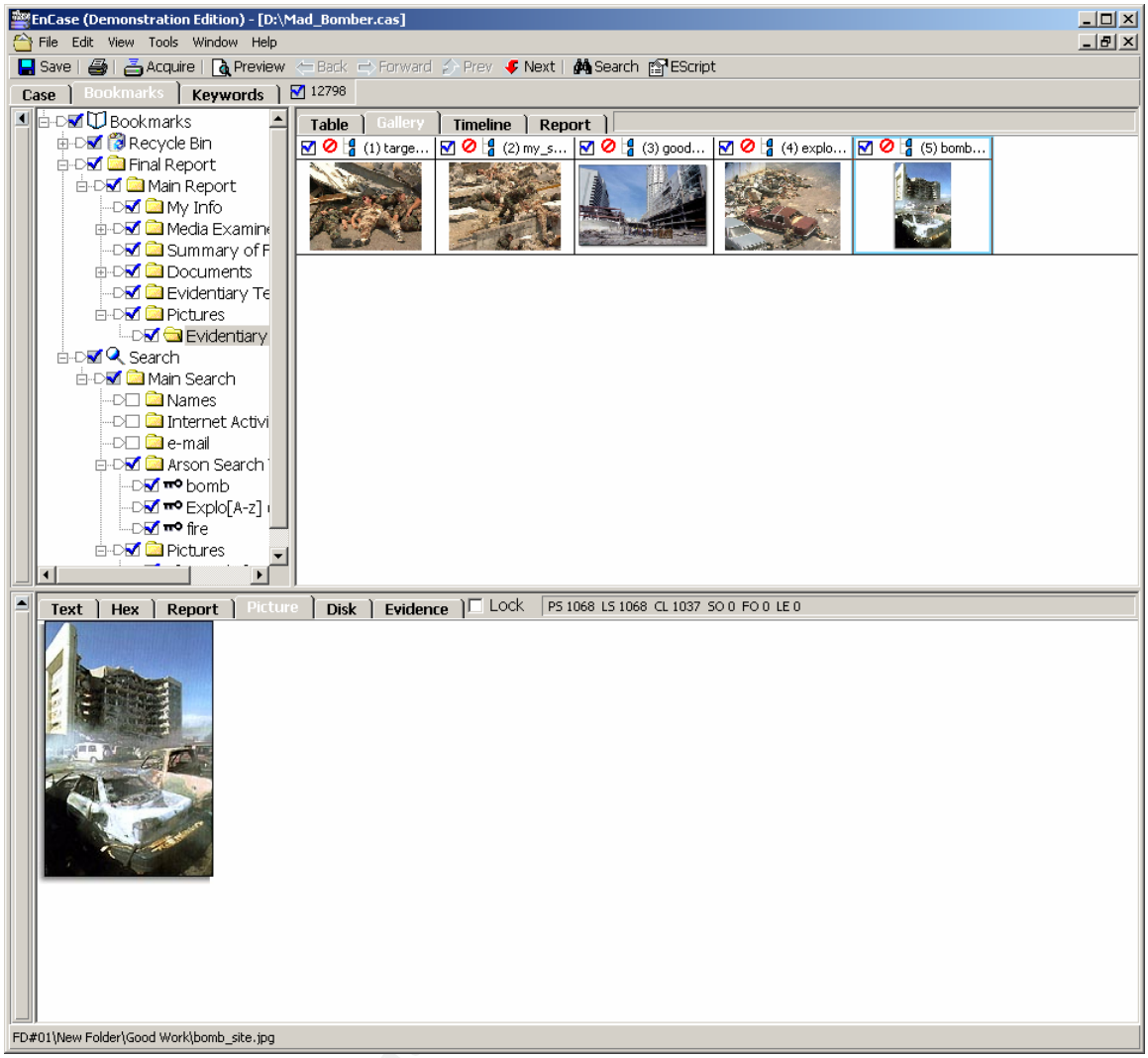
```
139/TCP    open       netbios-ssn
445/TCP    open       microsoft-ds
1025/TCP   open       listen
Nmap run completed -- 1 IP address (1 host up) scanned in 6 seconds
```

```
[root@xxxxxxxx root]# nmap -e eth0 -sS a.b.c.d
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on xxxxxxxx (a.b.c.d):
(The 1538 ports scanned but not shown below are in state: closed)
Port       State      Service
135/TCP    open       loc-srv
139/TCP    open       netbios-ssn
445/TCP    open       microsoft-ds
12345/TCP  open       NetBus
Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds
```

For posterity, we will note here that the Trend anti-virus product listens on TCP port 12345 for management purposes. Therefore this host is not infected with NetBus.

Also, the only backup copies of the drives being investigated were made using the acquire function from the Encase enterprise forensics tool. Encase allows an investigator / examiner to acquire evidence without altering or damaging the original. This was done by connecting a laptop running encase to a desktop where the suspect drive was plugged up via a crossover Ethernet CAT5 cable. Encase has three methods to acquire evidence (or copy the hard drive). The first is through a cable connected to the parallel ports on both machines, the second is through a crossover Ethernet cable, and the third is through a FastBlock device. The FastBlock device is more or less an IDE cable that allows a much faster file transfer rate. Once you have the suspect hard drive connected to a computer, you boot the machine from an Encase bootable floppy, load the network drivers for the model NIC you have, and then connect from the laptop using the Encase GUI. Encase has very nice features built-in for creating evidence files (including only the relevant data instead of the entire hard drive) as well as creating tons of notes for future reference. Below is a screen shot of the Encase application interface in demo mode:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

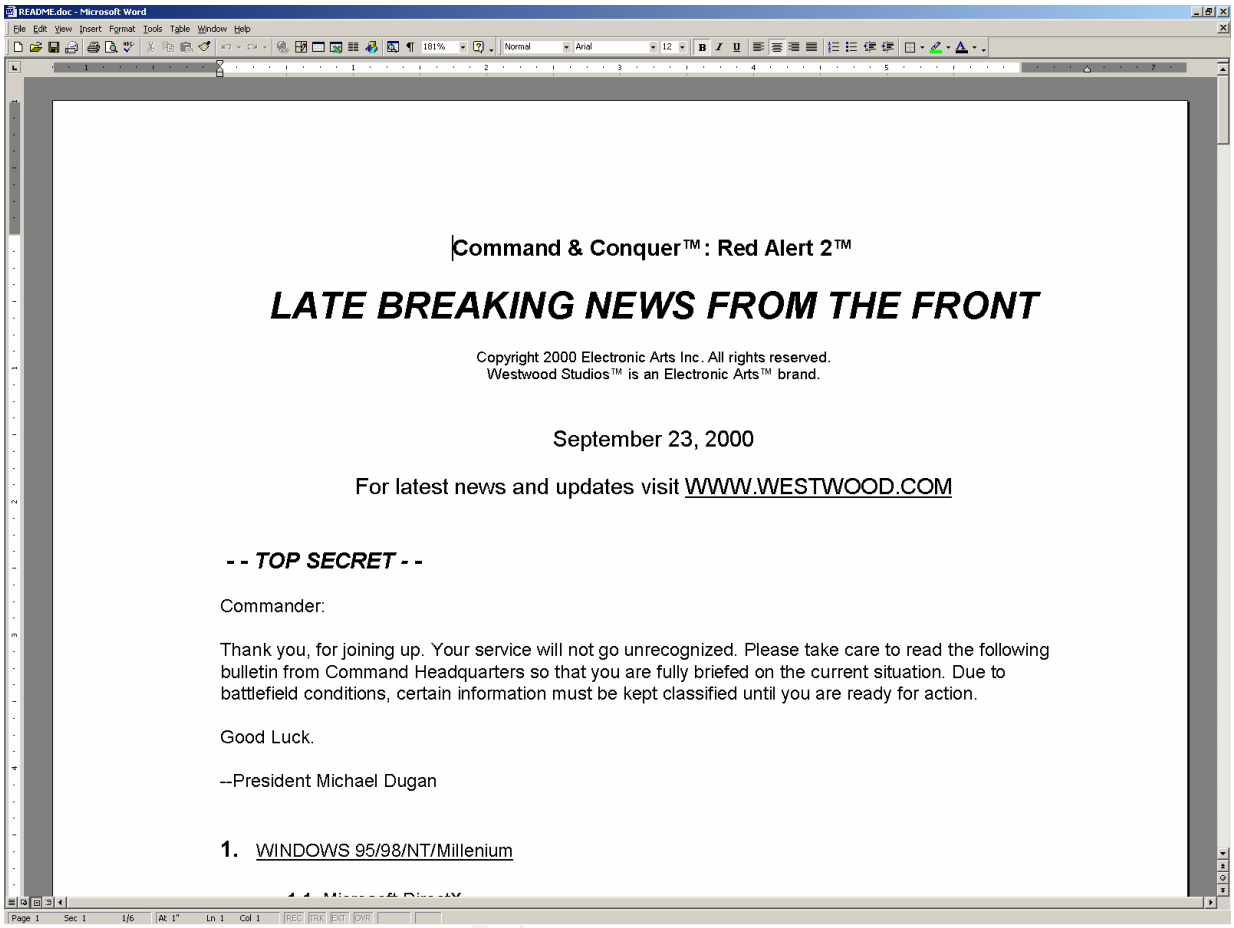


Eradication

Once we obtained the evidence from the hard drives in question and terminated one of the would-be hackers, the drive belonging to the IT support person was simply re-imaged with a corporate desktop image using Symantec's Ghost corporate edition and shipped back to the remote office. The drive belonging to the data coordinator did not actually have the BO2K files on it anymore so it was sent back to the user so they wouldn't lose all of their work data. A recommendation was made that this individual be terminated due to his involvement in this incident as well as other evidence found on his computer related to non-business activity. See the image below:

Installed Application: Red Alert 2
Display Name: Command & Conquer Red Alert 2

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.


README.doc - Microsoft Word

Command & Conquer™: Red Alert 2™

LATE BREAKING NEWS FROM THE FRONT

Copyright 2000 Electronic Arts Inc. All rights reserved.
Westwood Studios™ is an Electronic Arts™ brand.

September 23, 2000

For latest news and updates visit WWW.WESTWOOD.COM

- - TOP SECRET - -

Commander:

Thank you, for joining up. Your service will not go unrecognized. Please take care to read the following bulletin from Command Headquarters so that you are fully briefed on the current situation. Due to battlefield conditions, certain information must be kept classified until you are ready for action.

Good Luck.

--President Michael Dugan

1. WINDOWS 95/98/NT/Millenium

A potential root cause of this incident could be the lack of user education / training in this corporate environment. There are no existing training programs in-house that deal with even the lowest level of computer security. The only thing done in this manner is a requirement to sign an “Acceptable Use Policy” (AUP) during orientation to the company. We also point out to the employees through in-house memoranda or informative “blurbs” on our corporate Intranet about the existing IT policies that they can read via the Intranet as well.

I suspect that if there were training programs in place to educate the users on things like unauthorized software, hard-to-guess passwords, etc., the overall security posture of the company would improve dramatically. It should be assumed that few people read the fine print on all the documents that have to be signed during employee orientation. Employees should be bombarded with standard operating procedures regarding computer security basics during orientation or continuing education provided by HR or the IT security department.

A large majority of the people who make up the executive management teams of corporate America fail to see the importance of promoting computer security awareness to their employees. Maybe they do not see the “big-picture” of how

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

such incidents can affect the company. When a major virus outbreak occurs or a major break-in occurs and there is significant downtime to computer systems that are involved with generating revenue, they may see the necessity for end-user training as well and other security countermeasures needed to protect the company.

Recovery

Once again we see the lack of policy causing steps to be overlooked or not completed. The hard drive from the IT support person who was terminated actually got re-imaged from a corporate desktop image so we didn't worry about it. However, the hard drive from the data coordinator was not re-imaged and was basically sent back into service "as-is". There were no steps taken to further secure this system other than verbally warn the individual in question. There have been subsequent port scans of this network to look for any odd ports that may be listening for connections (especially since this trojan can run on any TCP or UDP port).

Interestingly Back Orifice 2000 was discovered around the same time frame at another remote office in a different state, on a floppy disk. We port scanned the computer as well as the entire LAN at that office and also searched the hard drive of this machine and did not find any traces of BO2K. This is a much smaller office, and the names of managers were rather hard to come by. This incident is still under investigation. With limited security staff and facilities all across the country, incident response is not as easy as one would like it to be. Below is the email from the Virus Administrator regarding the Trend alert at the second remote office:

From: AV Admin
Sent: Tuesday, February 11, 2003 12:21 PM
To: IT Security
Subject: BO2K Again
Follow Up Flag: Review
Due By: Friday, May 02, 2003 1:16 PM
Flag Status: Flagged

Here's another one. On a floppy this time.

-----Original Message-----
From: OfcScan [mailto:OfcScan]
Sent: Tuesday, February 11, 2003 12:16 PM
To: Virus Alerts

Virus Alert!!
TROJ_BO2K is detected on xxxxxxxx(yyyyyyyy) in Default domain.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Infected file: A:\boserv.exe
Action: Clean Failed (Delete Failed)
Detection date: 2003.02.11 13:24:29

Lessons Learned

Numerous lessons have been learned from this incident. Possibly the most significant benefit from this entire ordeal is that it pushed management to realize the need for a formal written Computer Security Incident Response Policy with documented procedures to follow and forms to fill out. Of course, everyone knows this policy is a fluid document that may change with each incident but, it's a beginning point.

One of the biggest lessons personally learned throughout this investigation was the need for working copies of the evidence. Being an inexperienced handler, I accidentally booted my computer with the hard drive from one of the suspect computers. I intended to boot off of the Encase floppy disk and run Encase on the drive to gather forensic data, but instead I booted up and immediately got messages like "found new hardware", etc., etc., which inadvertently changed or modified many files on the drive and effectively destroyed any chance of honestly using this drive in a court case as evidence.

One of the most positive things we learned was that our anti-virus solution, although not deployed company wide, seems effective at the job it was designed for. We also realized the wonderful benefits of the Vericept View product and it's very capable linguistic analysis engine for picking out the needle in the haystack for us.

If this had been a normal domain user, we would hope they would not be privy to local administrator passwords on corporate workstations. This would prevent them from installing unauthorized software. However, one of the most challenging security problems in this company is lax control over the password to the local administrator account on corporate workstations. As we image machines with software like Ghost, this password gets replicated to practically every remote office. We've actually been discussing in the last few days how to devise a script or two so that we could change this password across the board. Considering this company has 1500 or so remote offices, this is no small task.

References

Back Orifice 2000 Documentation – Command Reference
http://sourceforge.net/docman/display_doc.php?docid=12856&group_id=4487

Back Orifice 2000 FAQ
http://sourceforge.net/docman/display_doc.php?docid=12704&group_id=4487

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

BO2K 1.0 Quick and Simple Tutorial
http://sourceforge.net/docman/display_doc.php?docid=7864&group_id=4487

Back Orifice 2000 Official Press Release
http://www.bo2k.com/release.html

A Note on Product Legitimacy and Security
http://www.bo2k.com/legitimacy.html

Back Orifice 2000 Feature List
http://www.bo2k.com/featurelist.html

Deane, Joel, ZDNet News, Back Orifice 2.0 Going Legit
http://zdnet.com.com/2100-11-501114.html

Ulricksen, Drew, ZDNet News, Back Orifice 2000 Not to be Feared
http://zdnet.com.com/2100-1107-515130.html

Original ISS Security Alert #31
http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?id=advise31

Martinez, Michael J., Hunting BO2K
http://abcnews.go.com/sections/tech/DailyNews/bo2k990712.html

How to Determine if Back Orifice 2000 Virus is Installed on Your Computer
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B237280

Symantec's Back Orifice 2000 trojan Description
http://www.norton.com/avcenter/venc/data/back.orifice.2000.trojan.html

BOTOOL – L0pht Plugin for b02k
http://www.winnetmag.com/Articles/Index.cfm?ArticleID=7256

Scambray, Joel, McClure, Stuart, and Kurtz, George. Hacking Exposed: Network Security Secrets and Solutions. Berkeley: Obsborne/McGraw-Hill, 2001.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.