Global Information Assurance Certification Paper

Robert V. McMillen Jr.
GIAC Level One Security Essentials Course

Back Orifice 2000 Overview

Back Orifice 2000 (BO2K) is advertised as "a best-of-breed network administration tool, granting sysadmins access to every Windows machine on their network. Using Back Orifice 2000, network administrators can perform typical desktop support duties without ever leaving their desk [5]." But is it really an administrative tool? Why would an administration tool provide stealth installation techniques?

This paper provides a general overview of the program, to include its stealth installation capabilities. The intent is to help Windows 9X and NT users identify BO2K's existence on a system, and provide recommendations to avoid infection.

Overview [1]

BO2K is a remote control utility with extensive capabilities that can operate on Windows 9X and Windows NT systems using a client/server model. The server is installed on the desired victim or remote system, and the client is located on the local system. Some of the key and most dangerous feature are:

- Plugins – These can add encryption capability and hide the BO2K server within a legitimate program making the server invisible. When the legitimate program executes, BO2K is installed without the user knowing.
- Multiple server connections – One BO2K client can control several BO2K servers simultaneously. This feature could assist in distributed denial of service attacks.
- Keystroke logging – The client can access everything the victim is typing on the keyboard (e.g. username and passwords, e-mails, etc.).
- File sharing – The client can remotely share files, directories, or disks on the server.
- Registry – Total control of the server's registry.
- File browsing and transfer – The client can browse the file system as if he or she were sitting at the server.
- Remote installation, upgrade, and removal of server.
- Port and Application redirection – Allows the client to execute programs on the server system. The server can also be used as a hop to another victim by redirecting the client's commands to another system. This would

make it look as if the server were performing the attack.

- Password dumping – Copy passwords from the registry and/or cache.
- Process control – Allows the client to start, stop, and list server processes.

BO2K can use any TCP or UDP port for its client/server communications, but it uses TCP 54320 or UDP 54321 by default. Once the system is infected, the server opens a UDP and/or TCP port, and waits for the client to initiate and establish a connection.

Installation (1, 2, 3)

BO2K can be configured to hide itself within the system. By default, the server will edit the registry by adding the UMGR32.EXE key to the following key:

Window 9X - \\HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\
WINDOWS\CURRENT VERSION\RUNSERVICES

Windows NT - \\HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\
WINDOWS\CURRENT VERSION\RUN

The file will be located in the *<SystemRootDir>\SYSTEM* directory in Windows 9X or the *<SystemRootDir>\SYSTEM32* directory in Windows NT. However, the server configuration tool can rename this file in order to hide it within the system directory, registry, and task manager.

Identification (1, 2, 3)

In order to identify BO2K on the system, the user must either have antiviral software installed or be familiar with the services the system provides.

Currently, antiviral software can detect the existence of BO2K on the system. However, there are two problems.

- The user must maintain current viral definitions on the system by periodically downloading the latest definitions from the software company's web site. At times, new viral definitions are posted daily!

- Finally, BO2K is open source software; therefore,

anyone with the time and skill to modify the code can change the signature of the Trojan, thereby making the viral software useless.

Familiarity with system services will go a long way. The system administrator should be aware of the services each system offers and how they communicate with the world (e.g. port number and protocol). The following command will list listening and established connections on the system:

---

c:> netstat –an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:54320	0.0.0.0:0	LISTENING
TCP	10.10.30.33:137	0.0.0.0:0	LISTENING
TCP	10.10.30.33:138	0.0.0.0:0	LISTENING
TCP	10.10.30.33:139	0.0.0.0:0	LISTENING
TCP	10.10.30.33:54320	0.0.0.0:0	LISTENING
UDP	0.0.0.0:135	*:*	
UDP	10.10.30.33:137	*:*	
UDP	10.10.30.33:138	*:*	

If the system displays the default listening ports (TCP 54320 or UDP 54321) or an unexpected listening port, the registry keys mentioned above should be examined. This system may be compromised because most legitimate services appear between ports 1 through 1023.

Avoiding Infection

The first, and possibly the most preventive countermeasure, is not to execute e-mail attachments that are executable (end with .exe).

Next, Protect the network with a statefull firewall. With rules to allow only inbound traffic initiated by the legitimate network, the attacker will not be able to establish a connection to an infected system (unless the attacker is inside the firewall).

Establish a procedure for downloading and updating existing anti-viral software on a regular basis.

If possible, acquire a tool such as RegSnap that will allow the system administrator to take system “snap shots”

prior to installing the system on the network. Then, regularly, take new "snap shots" and compare them in order to find illegitimate additions or modifications to the registry [4].

In conclusion, BO2K is an extremely dangerous software program, and should not be allowed to run free on the network. By ensuring the network contains the latest viral definitions and employing security in depth such as filtering at the border routers, protecting the network with statefull firewalls, and adding intrusion detection agents throughout the network, a system administrator should be able to keep BO2K from infecting the network.

References:

1. cDc. "Back Orifice 2000 Documentation & Instructions Complilation." 13 September 1999. URL: http://www.bo2k.com

2. Elnitiarta, Raul and Wason Han. "BackOrifice2K.Trojan." 11 Jul 1999. URL: http://www.norton.com/avcenter/venc/data/back.orifice.2000.trojan.html

3. McAfee. "Back Orifice 2000 Virus Profile." 15 July 1999. URL: http://vil.mcafee.com/dispVirus.asp?virus_k=10229&

4. McMillen, Robert. "SubSeven Program Documentation." 29 June 2000. URL: http://www.sans.org/y2k/practical/Robert_McMillen_gcih.doc

5. Vranesevich, John. "Does The Dead Cow Stink?" 8 July 1999. URL: http://www.antionline.com