Global Information Assurance Certification Paper

W32/Fizzer.A-Analysis and Infection Prevention and Handling

Colette L'Heureux

GCIH v2.1 option #1

Table of Contents

Introduction

Hello, my name is Colette L'Heureux and I am a GCIH certification candidate. As a systems security specialist for my company I am notified by several different companies when new viruses are found to be in the wild. I'm also notified when new viruses are discovered, even when not in the wild, when they start spreading fast, the pager starts going off.

The W32/fizzer.a virus was first discovered on May 8th 2003 by F-secure. It was originally seen spreading rapidly via the Kazaa file sharing network in Asia. By May 12th, 2003, it was upgraded to one of the fastest spreading worms and considered a Level 1 security risk by F-secure. Trend Micro systems states they first discovered the worm on May 12th, 2003 and upgraded it to medium risk with high damage potential on the same day. Symantec first noticed the worm on May 8th, 2003 and listed it as a medium risk on May 12th, 2003.

Fizzer is one of the new hybrid viruses that have recently been seen popping up. This virus has its own e-mailer, a method to create IRC and AOL Instant Messenger accounts, to await instructions from its code writer to possibly launch a denial of service attack. It can also update itself by attempting to connect to a geocities website. It also attempts to disable any local anti-virus software it finds and it installs a keystroke logger to gather passwords and credit card numbers

Part 1: The Exploit

Name

From http://www.cert.org/current/current_activity.html#peido page

> **Win32/Fizzer Worm**
> *added May 12*
>
> The CERT/CC has received reports of a mass-emailing worm known as "Fizzer", "W32.Fizzer", or "Win32/Fizzer". It arrives via an email message in an attachment with an .exe, .pif, .com, or .scr extension. Upon opening the attachment, the worm uses various IRC networks to communicate with a remote attacker. This worm is also reported to contain a keystroke logger.
>
> The CERT/CC strongly encourages users to install anti-virus software, and keep its virus information files up-to-date.
>
> Users may also wish to consider:
>
> Filtering email attachments with the extensions listed above.
> Monitoring outgoing traffic for unexpected IRC connections

This worm/virus/exploit is known by several other names including but not limited to:

W32/Fizzer@MM
W32/Fizzer.A
Sparky
Win32.Fizzer
W32/Fizzer-A
WORM_FIZZER.A
Fizzer
Win32/Fizzer.A@mm
I-Worm.Fizzer
W32.HLLW.Fizzer@mm

The different names are caused by non-standardized naming conventions between the many different anti-virus product makers.

There is currently no CVE number assigned.

Vulnerable Operating Systems

The following operating systems are vulnerable to this virus/worm/exploit:

Windows 9x
Windows NT
Windows 2000
Windows ME
Windows XP

Protocols/Services/Applications

Fizzer targets many different services. First seen spreading through the Kazaa file sharing service, it then moved to email. When a computer becomes infected it attempts to connect to AOL Instant Messenger.

Fizzer uses the following ports either as method for infection or as a method to contact it's creator for further instructions:

1214 – Kazaa communication port (used to spread infection)
5190 – AOL Instant Messaging (used to listen for updates or instructions)
6667 – IRC Port (used to listen for updates or instructions)

Once Fizzer has infected a system it attempts to email itself with its own embedded email program. Fizzer targets the Outlook and Windows address books for address to send itself to.

Brief Description

Fizzer is a very complex hybrid virus with multiple methods of infection via Kazaa peer to peer file sharing and email attachments. It has multiple payloads that it delivers including a keystroke logger, a Trojan horse, several registry setting changes, a backdoor to AOL and several IRC channels. It also has the capability to be used for several other backdoors. It can kill some anti-virus software programs, update itself via the web and it even leaves a method to uninstall itself.

Variants

There are no known variants at the time of this writing.

References

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_FIZZER.A

http://www.sophos.com/virusinfo/analyses/w32fizzera.html

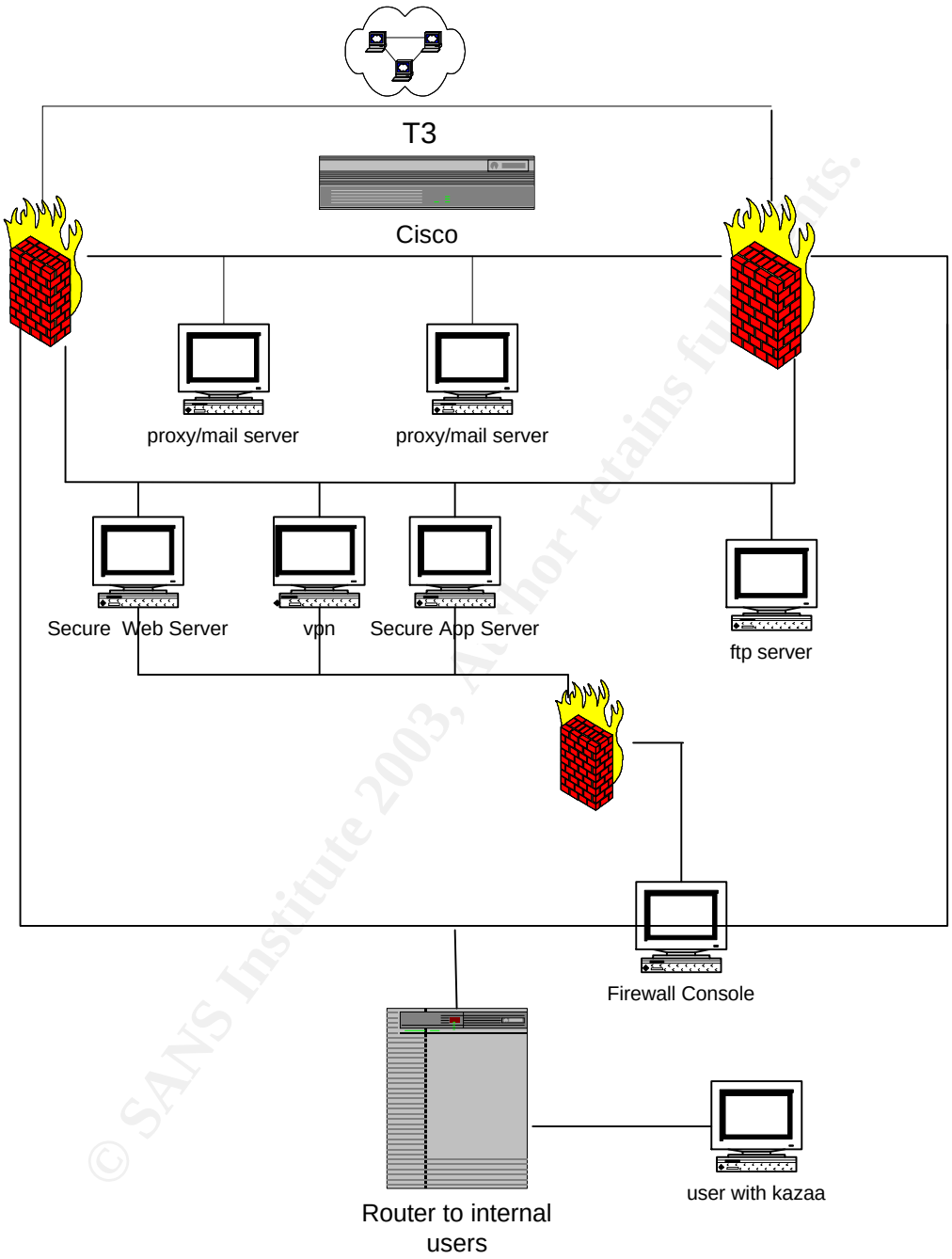
http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.fizzer@mm.html

http://www.cert.org/current/current_activity.html#peido

http://www.f-secure.com/v-descs/fizzer.shtml

Part 2: The Attack

Network Diagram



This diagram was modified from my graded GCFW practical (# 328) and the original can be found at http://www.giac.org/GCFW_400.php.

The end user who is running the Kazaa client is the focus of this attack. With Kazaa being the initial point of infection the virus then uses the user's outlook

address book to send itself through email The virus then drops a copy of itself back into the Kazaa share directories to replicate itself through the Kazaa system and open back doors through the firewall to the IRC channels and AOL instant messenger.

Protocol Description

To spread itself, fizzer uses two protocols. The Kazaa peer to peer file sharing protocol and the SMTP protocol.

According to RFC 821 the purpose of the SMTP (simple mail transport protocol) is to facilitate mail transport and delivery.

Kazaa is a distributed, self-organizing network and it also allows users to share digital media other than music. Peer to Peer protocol allows remote computers to connect to each other and create a shared network for the specific purpose of sharing files.

Fizzer does not use AOL Instant Messenger or IRC to spread infection but rather to update itself and receive instructions from it's creator.

How the exploit works

The Kazaa protocol when installed on a user's computer looks for a "supernode" (computer with the most amount of data to share and the fasted upload/download speed) when it finds that "supernode" it searches the shared files on that users computer and advertises what files are available for sharing on the local computer. All file sharing and finding takes place on port 1214. The Fizzer worm locates the Kazaa shared folder on an infected computer and copies itself there with random names. Any person who connects to an infected computer and executes files downloaded from its shared folder becomes infected with the worm.

When fizzer spreads through email the payload is the same and like all email borne viruses it relies on the user to open an attachment thereby executing the virus. The first infected machine received a copy of the worm via email with a subject line that reads one of the following:

I thought this was interesting...
rather psychedelic...
found this on the net, you might like it...
Damn it feels good to be gangsta.
The way I feel - Remy Shand
Paradigm Shift
WASSUP!
Know Thyself

I love you
Please discard if you don't like or agree with our present leadership...
little popup remover
B cannot remember
Yo, WASSUP, B?
an interesting program...
You might not appreciate this...
I think you might find this amusing...
check this out... hehehe
question...
see you tomorrow.
how are you?
you need to lose weight.
kind of simple, but fun nonetheless.
check it out.
I wonder what can be so bad
That it makes you want to die
I wonder what could be so tragic
Makes you want to take your life
You have your savior on the cross
While you sit on the throne
Put youself up on that cross
Put your savior on the throne
And I know
It's hard to take what's happening
Life is tough sometimes
It seem like there's no hope for you
Your life is worth more than you can say
It's hard to see beyond your pain
When you feel so dead inside
It's hard to see what you've been given
It's hard to find a hope in life

This is not a complete and exhaustive list of subject lines but rather an example of some it could contain.

This mail arrives in the user's mailbox with an attachment with a randomly generated name and an extension of:

.exe
.com
.scr
.pif

The name of the attachment is randomly generated using on of the following two formulas:

%Name%%Number%

%Word%

Fizzer collects e-mail addresses from Windows and Outlook Address Books on an infected computer and from different files in personal folders, cookie folders, the recently opened files folder and Internet cache directories.

The worm fakes sender's e-mail address in infected messages. It randomly composes fake addresses from its rather extensive internal list. The fake sender's e-mail address may be composed with a fake a name, a random number and one of these domains:

msn.com
hotmail.com
yahoo.com
aol.com
earthlink.net
gte.net
juno.com
netzero.com

The worm sends itself in e-mail messages to all the addresses it finds. The worm randomly selects subjects, bodies and attachment names from its large internal lists. The worm can use the names of innocent files from an infected system's hard disk for its attachment. Attachment extensions can be any .EXE, .PIF, .SCR or .COM.

The most impressive part of this worm is its payload. I have never seen such an extensive payload before. According to F-Secure the following is part of the payload:

Key logging Trojan

The worm records users' keystrokes and writes them into an ISERVC.KLG file located in the Windows folder. This file can be picked by a hacker, so he can get access to users' login names and passwords as well as to their confidential data.

AOL backdoor

The worm connects to AOL server on port 5190 with a random user name creating a bot. A hacker can establish a connection to the bot and control the behavior of the worm remotely.

IRC backdoor

The worm tries to connect to different IRC servers and create bots in a certain channels there. The author of the worm can use these bots to get limited access to infected systems. The worm has a long list of IRC servers in its resources. Here are some of the IRC server names that the worm uses:

irc.afternet.org
irc.dal.net
irc.eu.dal.net
irc.ablenet.org
irc.abovenet.org
irc.accessirc.net
irc.aceirc.net
irc.all-defiant.org
irc.allochat.net
irc.alphanine.net
irc.altnet.org
irc.amcool.net
irc.amiganet.org
irc.angeleyez.net
irc.aniverse.com
irc.another.net
irc.arabchat.org
irc.arabmirc.net
irc.astrolink.org
irc.asylum-net.org
irc.auirc.net
irc.aurosoniq.net
irc.auscape.org
irc.aussiechat.org
irc.awesomechat.net
irc.awesomechristians.com
irc.axenet.org
irc.aXpi.net
irc.ayna.org
irc.azzurra.org
irc.bahamutirc.net
irc.bappy.eu.org
irc.bdsm-net.com
irc.beyondirc.net

Additional backdoor capabilities

The worm has additional backdoor capabilities. It listens to ports 2018-2021 for commands from a remote host (the hacker's computer). The ports are used for the following purposes:

2018 - command port (sending/receiving commands)

2019 - file port (sending/receiving files)

2020 - console port (remote console)

2021 - video port (capturing video and sending it out)

The worm's author can access these ports with a specially made utility (client program of a backdoor), however the console port can be connected to with a Telnet application. A remote console gives a hacker access to an infected computer as if he was using it locally.

The worm can also start an HTTP server on port 81 to provide additional access to an infected computer.

The worm has the ability to kill the tasks of certain anti-virus programs. It kills all processes with the following strings in their names:

NAV
SCAN
AVP
TASKM
VIRUS
F-PROT
VSHW
ANTIV
VSS
NMAIN

The worm can perform a DoS (Denial of Service) attack if it receives a specific command from a remote hacker.

Auto updating feature

The worm has the ability to update itself from a web site. It connects to a web site, downloads an update and saves it as UPD.BIN file in the Windows main folder. However, the web site with the updates for the worm is no longer available.

Uninstallation feature

The current variant of the worm can uninstall itself if a file with the following name is found in the Windows main directory:

Uninstall.pky

When the worm finds a file with this name, it kills all its tasks and removes its registry keys thus disinfecting a system.

Fizzer changes the windows registry setting in the following manner:
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"SystemInit" = "%windir%\iservc.exe]

where %windir% is the Windows main directory. As a result, the main file of the worm is activated for each Windows session.

Additionally, the worm modifies the text file startup string:

[HKEY_CLASSES_ROOT\txtfile\shell\open\command]
@ = "%windir%\ProgOp.exe 0 7 '%windir%\NOTEPAD.EXE %1'
'%windir%\initbak.dat' '%windir%\iservc.exe'

where %windir% is the Windows main directory.

It also drops at least the following 4 files:

ISERVC.EXE
INITBAK.DAT
ISERVC.DLL
PROGOP.EXE

The ISERVC.DLL file is a key-logging component and the PROGOP.EXE file is a pure dropper code. A dropper code file is code that constructs a multi-file virus into a single file so that it can “dropped” onto another system for execution. Before sending itself out, the worm re-assembles itself into a single file using this dropper.

A Unix “strings” command run against the encrypted source code of the virus comes back with the following recognizable words:

Sparky will reign.
mRich8
USER32.dll
WSOCK32.dll
WINMM.dll
AVICAP32.dll
SHLWAPI.dll
SHELL32.dll
FADVAPI32.dll

GDI32.dll
ole32.dll
IMAGEHLP.dll
MPR.dll
OLEAUT32.dll
WININET.dll
RASAPI32.dll
DispatchMessageA
TranslateMessage
GetMessageA
wvsprintfA
CreateWindowExA
RegisterClassExA
UnregisterClassA
DestroyWindow
MessageBoxA
SetWindowPos
GetDlgItem
CreateDialogParamA
GetWindowPlacement
ShowWindow
SendMessageA
SetWindowTextA
SetForegroundWindow
SetFocus
SetWindowLongA
CallWindowProcA
PostQuitMessage
SetTimer
KillTimer
SetCursorPos
GetWindowRect
GetForegroundWindow
ExitWindowsEx
ReleaseDC
DrawTextExA
GetDCEx
GetDesktopWindow
GetClientRect
GetDC
LoadImageA
GetSystemMetrics
EnumDisplaySettingsA
ChangeDisplaySettingsA
mouse_event
PostMessageA

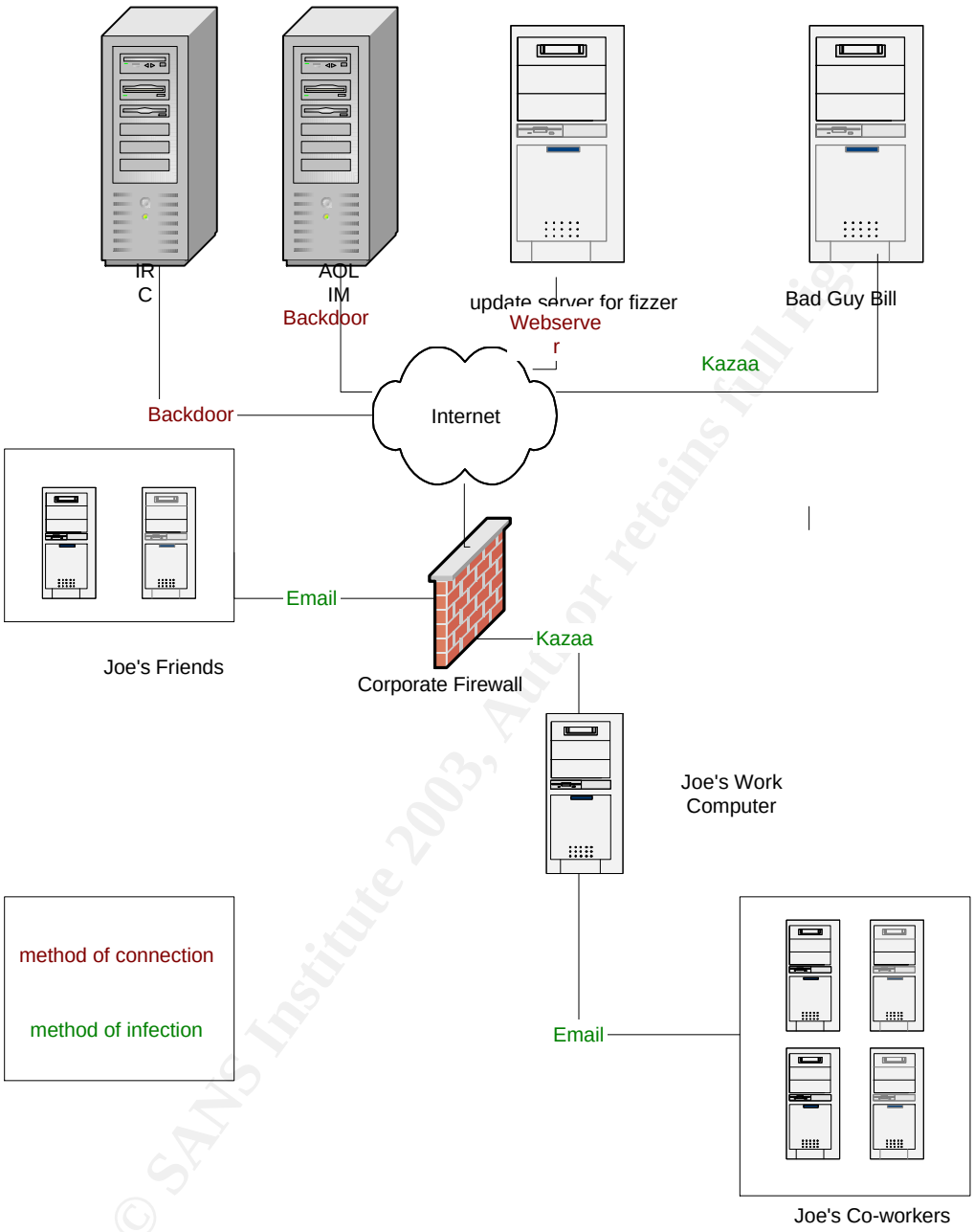
GetWindowThreadProcessId
WindowFromPoint
keybd_event
BlockInput
EnumChildWindows
GetWindowTextA
GetWindowDC
IsWindowVisible
PostThreadMessageA
PlaySoundA
mciSendStringA
mciGetErrorStringA
capGetDriverDescriptionA
capCreateCaptureWindowA
StrToIntA
StrToIntExA
SHGetSpecialFolderPathA
FindExecutableA
ShellExecuteA
StartServiceCtrlDispatcherA
SetServiceStatus
RegisterServiceCtrlHandlerA
AdjustTokenPrivileges
OpenProcessToken
LookupPrivilegeValueA
GetUserNameA
CloseServiceHandle
CreateServiceA
OpenSCManagerA
DeleteService
OpenServiceA
StartServiceA
ControlService
GetServiceDisplayNameA
RegCloseKey
RegQueryValueExA
RegOpenKeyExA
RegSetValueExA
RegCreateKeyExA
RegDeleteValueA
RegDeleteKeyA
RegEnumKeyExA
RegEnumValueA
SetROP2
DeleteObject
DeleteDC

BitBlt
SelectObject
CreateCompatibleBitmap
CreateCompatibleDC
GetDIBits
GetDIBColorTable
GetObjectA
StretchDIBits
GetSystemPaletteEntries
CoCreateInstance
CLSIDFromProgID
CoGetClassObject
CoInitialize
CoUninitialize
MakeSureDirectoryPathExists
SearchTreeForFile
WNetCloseEnum
WNetEnumResourceA
WNetOpenEnumA
WNetGetLastErrorA
InternetGetConnectedState
RasEnumEntriesA
RasEnumConnectionsA
RasHangUpA
RasDialA
GetProcAddress
LoadLibraryA
FreeLibrary
Sleep
HeapAlloc
GetProcessHeap
HeapFree
HeapSize
ExitProcess
GetModuleHandleA
GetLastError
CreateMutexA
SetLastError
InterlockedExchange
LocalAlloc
LocalFree
SetUnhandledExceptionFilter
FormatMessageA
lstrcmpiA
lstrcmpA
MultiByteToWideChar

WideCharToMultiByte
CreateFileA
CloseHandle
GetFileSize
SetFilePointer
WriteFile
ReadFile
FindClose
FindFirstFileA
DeleteFileA
CopyFileA
GetDriveTypeA
GetLogicalDriveStringsA
FindNextFileA
LocalUnlock
LocalLock
GetCurrentThreadId
GetLocalTime
GetSystemTime
GetCommandLineA
GetModuleFileNameA
GetCurrentProcessId
OpenProcess
CreateProcessA
GlobalFree
GlobalUnlock
GlobalLock
GlobalSize
GetVersionExA
GetComputerNameA
GetDateFormatA
GetTimeFormatA
GetTickCount
MoveFileA
DuplicateHandle
SetStdHandle
CreatePipe
GetStdHandle
GetCurrentProcess
SetConsoleCtrlHandler
SetConsoleTitleA
AllocConsole
ResetEvent
CreateEventA
WaitForMultipleObjects
SetEvent

TerminateProcess
FreeConsole
ExpandEnvironmentStringsA
GetCurrentDirectoryA
FreeResource
LockResource
LoadResource
SizeofResource
FindResourceA
EndUpdateResourceA
UpdateResourceA
BeginUpdateResourceA
MoveFileExA
GetSystemInfo
ResumeThread
CreateThread
TerminateThread
KERNEL32.dll
DrawDibClose
DrawDibDraw
DrawDibOpen
ICImageCompress
ICImageDecompress
MSVFW32.dll
RtlZeroMemory
RtlMoveMemory
kernel32.dll
SocketWindow
Ver: %u.%u, High Ver: %u.%u
PSAPI.DLL
KERNEL32.DLL
%s: %s
FILE
Could not update module.
Could not open file.
PADDINGXXPADDINGPADDINGX

Description and diagram of attack



Joe uses Kazaa at work because the connection speed is better, his network shares have more available space then his computer at home, but most importantly he uses it at work because the firewall is not tightened down properly. Ok, let's face it they really need to do a firewall rule review where Joe works because they have several really big holes and lots of open ports. But that discussion is really for a different practical.

Joe logs into Kazaa and gets connected to the supernode owned by bad guy Bill. Bad guy Bill, hereby referred to as just plain “Bill”, is sharing a new file called “Cool Tunes”. Joe really likes cool tunes and decides he wants to hear whatever this music maybe so he downloads “Cool Tunes” to his local machine. What Joe does not know is that Bill has placed a super new, extremely harmful virus known as W32/Fizzer on his Kazaa shares and called it “Cool Tunes”.

Joe then launches the “Cool Tunes” file he downloaded. Upon launching, Fizzer does the following:

1. Drops 4 files
2. The file containing the instructions executes
3. It deactivates your anti-virus software
4. Installs a key stroke logger
5. Opens a connection to AOL instant messenger
6. Opens a connection to 1 or more IRC channels
7. Mails itself to everyone in the outlook address book
8. Searches the system for other email addresses to mail to
9. Opens a web server connection to the update server
10. Drops a copy of itself in the Kazaa shares
11. Updates the Windows Registry
12. Drops an uninstall program on the system
13. Starts listening on parts 2018, 2019, 2020, 2021 for instructions
14. If the virus find a copy of itself on the system already it will execute the uninstall program

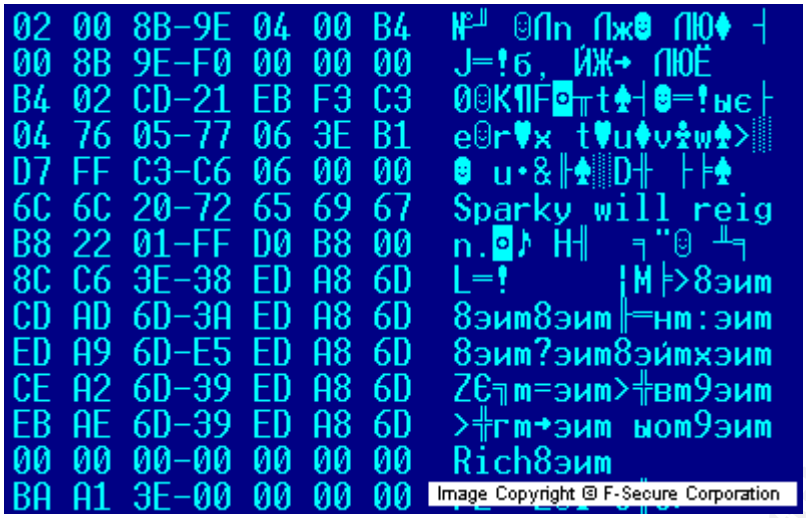
With the emailing and placement of itself in the Kazaa shares it has then managed to attempt to spread itself to others.

Signature of attack

One signature of the virus is if you see an increase or start of traffic on the AOL IM and IRC ports. These ports are 5190 and 6667. Activity on these ports when not expected is a sure sign that one or more of your computer systems have become infected.

The only other thing that could be considered a distinct signature for this virus is that the ISERVC.EXE file contains the 'Sparky will reign.' string in its header, as shown in the screenshot provided by F-secure

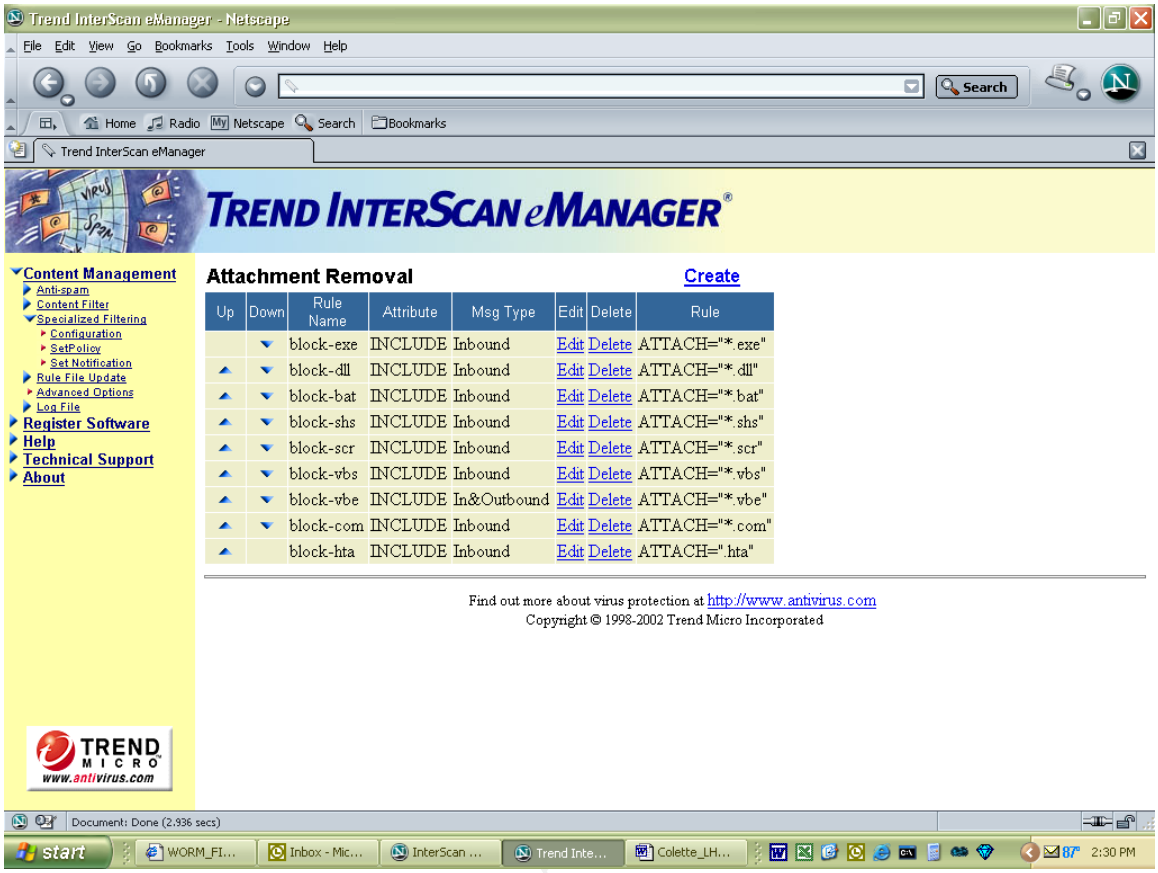
http://www.f-secure.com/v-descs/fizzer.shtml



How to protect against Fizzer

There are two ways to prevent Fizzer from getting to your company. The first is to not allow the Kazaa protocol through your firewall. In other words block all inbound and outbound traffic on port 1214.

The second way to prevent this virus from entering is to not allow emails with executable attachments in. You could do this by blocking the entire email or simply stripping off the attachment and forwarding the body of the email to the recipient. I have found that the Trend's eManager application can easily be set up to strip attachments by file type as seen in the following screenshot:



Executable attachment stripping has the added benefit of protecting you from email borne executable virus attachments while waiting for your anti-virus software to update.

You can not completely prevent an infected internal system from spreading this virus unless you do not allow outbound or intra-company mailing. However, you can reduce the risk of this virus by tuning the firewall to not accept traffic on the AOL IM port (5190) and the IRC port (6667). This will prevent the virus from being able to open these channels and reduce your risk of backdoors being available.

Part 3 The Incident Handling Process

Preparation

Joe's company has a few countermeasures in place but still is extremely unprepared for a true emergency. The most impressive countermeasure they have in place is a very complete and extensive guide to log review.

Every day during working hours there is one person who is dedicated to watching logs such as the system logs and firewall logs for all machines in the DMZ. This person also watches the NIDs device logs. Overnight and on weekends this work is turned over to Symantec's managed security services. This service provides Joe's company with the following services:

- Delivers 24x7, real-time monitoring and management of firewalls, intrusion detection systems, virtual private networks, and other security products
- Enhances an organization's information security posture through continuous monitoring and management, expert analysis of log data, and immediate response to potential security threats
- Provides rapid, cost-effective resolution of security problems from security operations centers around the world
- Uses a proprietary technology platform to aggregate and analyze data from heterogeneous security devices to quickly identify and defend against threats
- Offers organizations a real-time view of their enterprise security posture
- Ensures optimal protection of mission-critical assets by providing analysis and commentary needed to adjust defenses against emerging attacks
- Smoothes out the volatility in resource demands and costs typically associated with managing information security
- Protects existing technology investments with broad, vendor-neutral support

More information about this service can be found at:
http://enterprisesecurity.symantec.com/SecurityServices

The company has a network intrusion device (NID) in place in the DMZ but since Kazaa, Instant Messenger and IRC are well know traffic flows and not considered anomalous the device would not have been tripped by the fizzer worm.

The company has a profile of an incident handling team but it has never been tested. The profile for this team consists of two members of the IT security group, senior staff from each of the four technology groups (web, mainframe, windows and Unix), one auditor, one member of the company's legal council and a corporate communications specialist. When an incident does occur all involved parties will report to the Manager of Business Continuity.

For this incident the following people were first to be called: The two IT security people, the window's staff, the web specialist, Unix specialist (they also maintain the firewall software), the communications specialist. The first call came from Symantec alerting the security staff of suspicious traffic approximately 20 minutes after it started. The 20 minute delay occurred when Symantec was verifying that they were seeing anomalous traffic patterns and while they checked their worldwide database for similar patterns.

Joe's company has several policies and procedures in place handling an incident. Following is an excerpt:

Incident handling
Each incident may require additional treatment and may alter the handling based on its intensity and practice. The steps below create a base containment strategy. It is the Incident Manager's (IM) duty to plan and coordinate accordingly. These steps assume that an incident has been reported and identified.

Point of Contact
The end user, business partner, external customer, or other means of notification has taken place. An abnormal situation has occurred that raises speculation. The on call engineer is notified using one of the communication mechanisms stated in the Incident Communication portion of this document. Once the point of contact is established the process of combating the particular incident begins.

Identification
A critical component in the response of any compromise is to identify the systems, which are affected, and the level of priority that needs to be applied.

Containment
Once the priority level has been established it is critical to reduce the extent of the attack. Systems which have been identified as being compromised or infected must be contained from other systems on the network. This may include the disconnection of the machine from the network or major production services turned off. Rapid response is critical to minimizing the impact of the attack. Physical access should be restricted and audited. Members of the Infrastructure Incident Response Team (IIRT) have full understanding and abilities to shutdown and hardware of software components that they feel has been or is in danger of being compromised.

Eradication
Knowledge of the level of the attack has been established and the removal process starts. Archive file(s) that pertain to the attack for further examination. Clean and reformat any media that requires attention and insure that the backup media is not affected

Identification

This incident was first seen by Symantec's managed security services at 6 pm. They watched the traffic that suddenly started on ports 6667 and 5190 for 20 minutes while also searching for similar traffic from the corporations they watch. Upon noticing a rise in this type of traffic distributed across several platforms and corporations they contacted the emergency contacts at Joe's company. The new traffic pattern was identified from reports by many anti-virus companies as that of W32/Fizzer.a. The traffic was spotted in the active firewall logs for the company.

At 6:20 pm the two security specialists for the company were paged. Upon notification of the potential problem the security specialists contacted the Manager of Business Continuity. The two security people arrived back in the office within 20 minutes of being paged with the manager arriving 10 minutes later. They assembled in the prearranged location to asses the situation.

Prior to 6 pm that evening the logs showed that port 6667 had never been used before and port 5190 was only used during business hours. Based on what was known about Fizzer the security people looked for traffic on port 1214. They discovered that Joe was processing a lot of traffic through this port and that the increase in traffic to the two other ports could also be traced back to Joe's machine.

At this point, based on the defined procedures, the manager on hand declared a medium incident and called back on site the firewall/Unix, windows/exchange, and web services incident personnel. A phone call was placed to the communications representative and auditors to inform them if the situation since the incident has occurred after hours it was deemed unnecessary for the auditor and communications persons to come on site. Joe's Company defines a medium incident as the following:

> ***Medium***
>
> Production or Development Platform(s) that affect 10 – 50% of the enterprise functions: Development servers, Backup server, Internal web environment, and single user workstation.
>
> Level of support: Incident reported to on call personnel. On call contacts necessary individual(s) pertaining to a specific platform. Situation is confined to a single machine or process, and has little affect on production functions. Situation is eradicated and level of service is returned to normal within 60 minutes. Incident is reported to the IIRP email alias and recorded on the IIRP Incident spreadsheet for historical information.

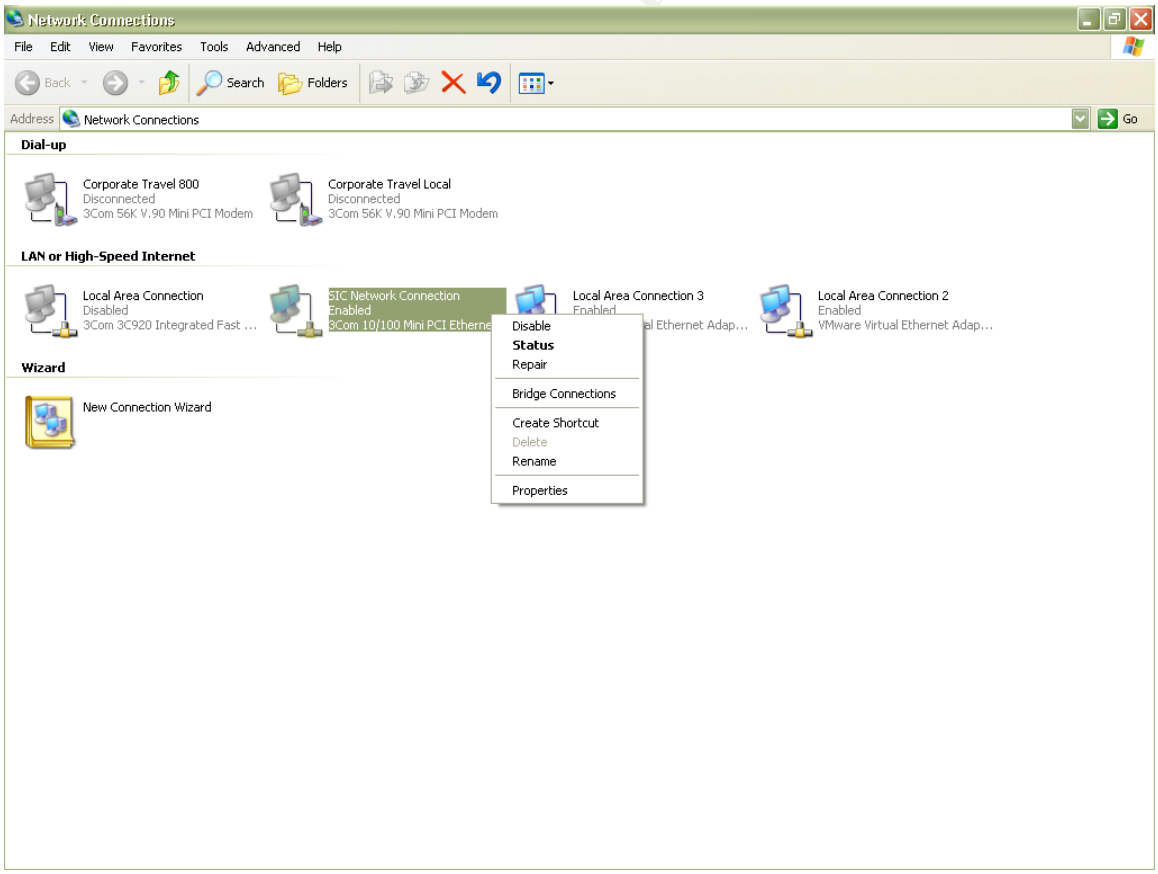
After the Manager and Security people have assembled, they went to the point of infection, Joe's computer. They explained the situation and told Joe he could go home for the day and that they would need to rebuild his computer before he could get back on the network. They then removed Joe's computer from the network and waited for the rest of the team to assemble.

Containment

After taking possession of Joe's computer the handling team removed the computer from the network effectively stopped the connections to AOL and IRC and preventing the sending of more infected emails.

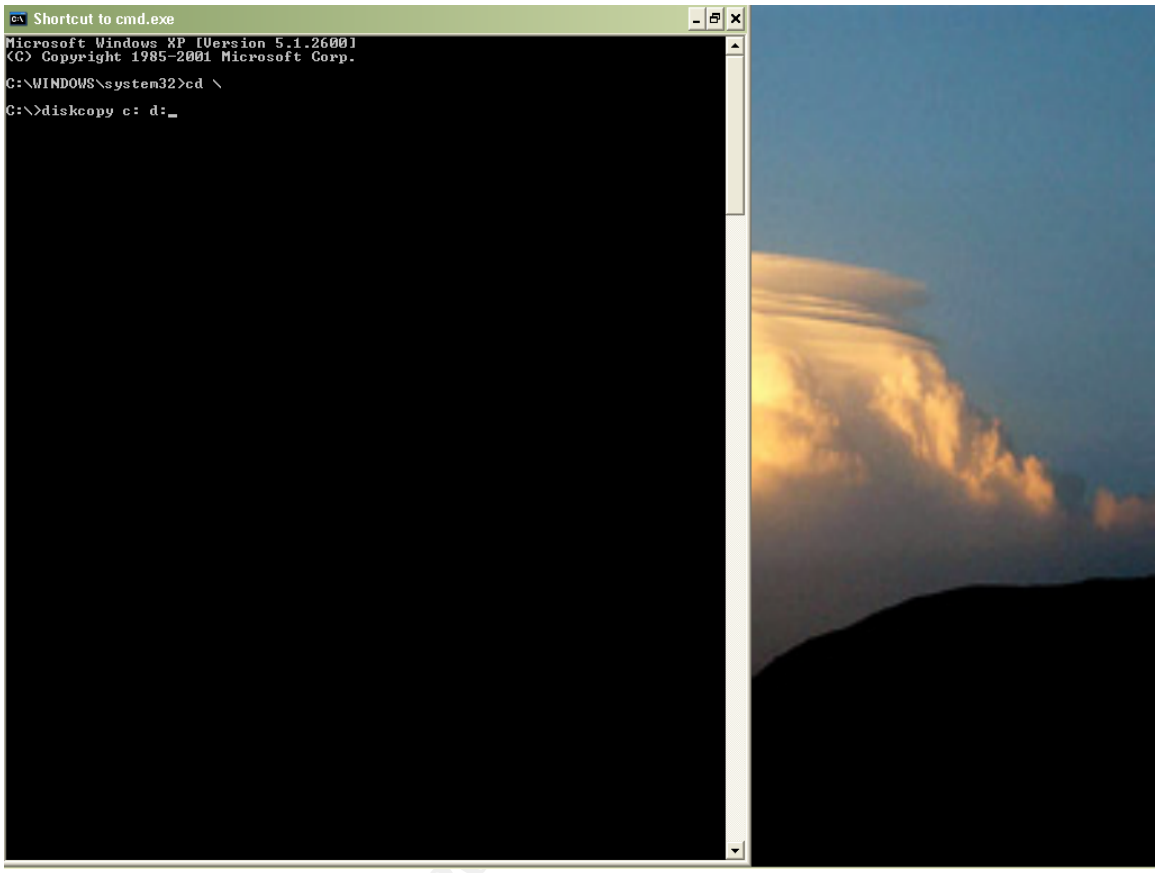
To take the computer off the network the following was done:

1. Right click on the "My Network Places" icon on the desktop
2. Click on properties
3. Find the interface in question and right click on it
4. Click on disable

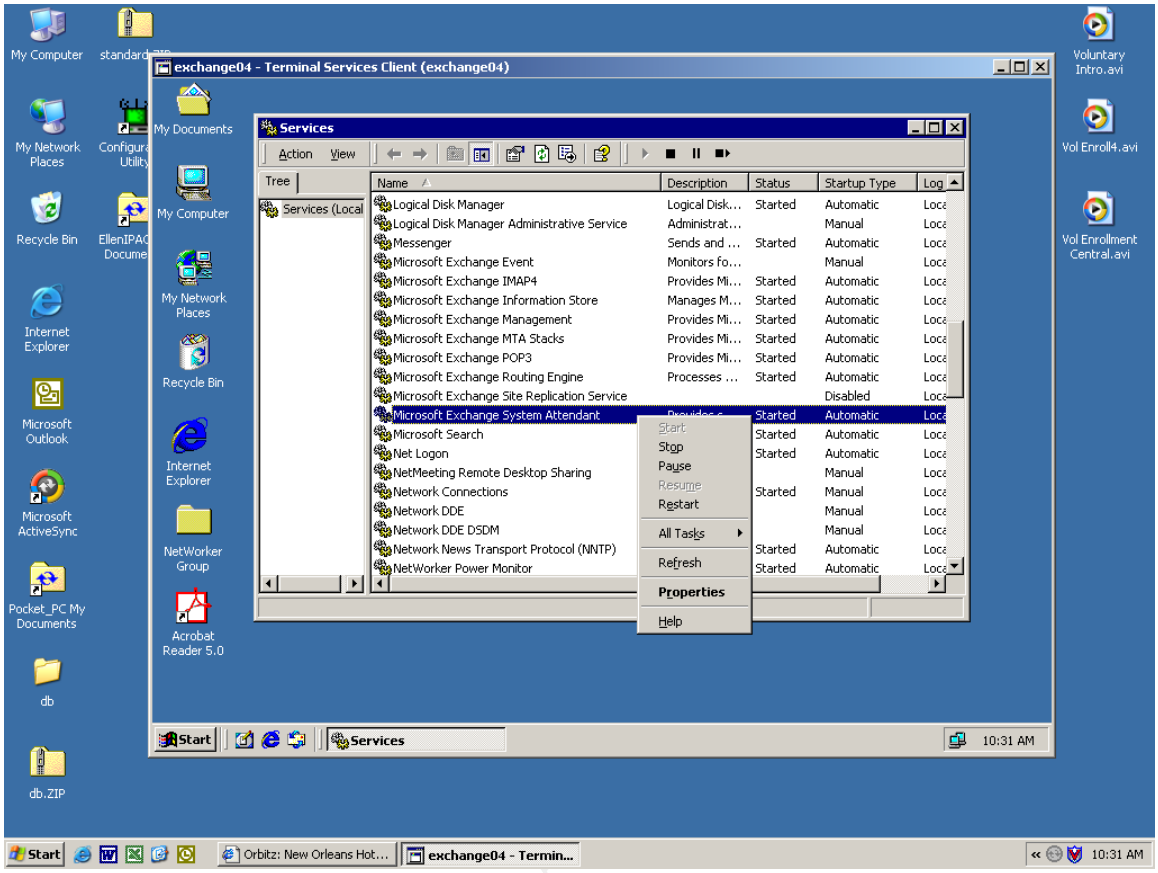


After taking the computer off of the network the handling team would get a spare external drive from the jump kit (all contents will be detailed shortly) attach it to

the computer in question and from the command line copy the infected disk to a backup copy.



Once this is done the handling team will need to take the exchange server off line to prevent the spread of fizzer through emails. This is done through a GUI on the server and it looks like this:



Once the exchange server has been taken off-line a full level 0 backup is run using Legato Systems backup services. There are no screen prints for this process. For details on this application please see: http://portal2.legato.com/products/networker/modules/exchange.cfm

For this incident the handling team's jump kit includes the following items:

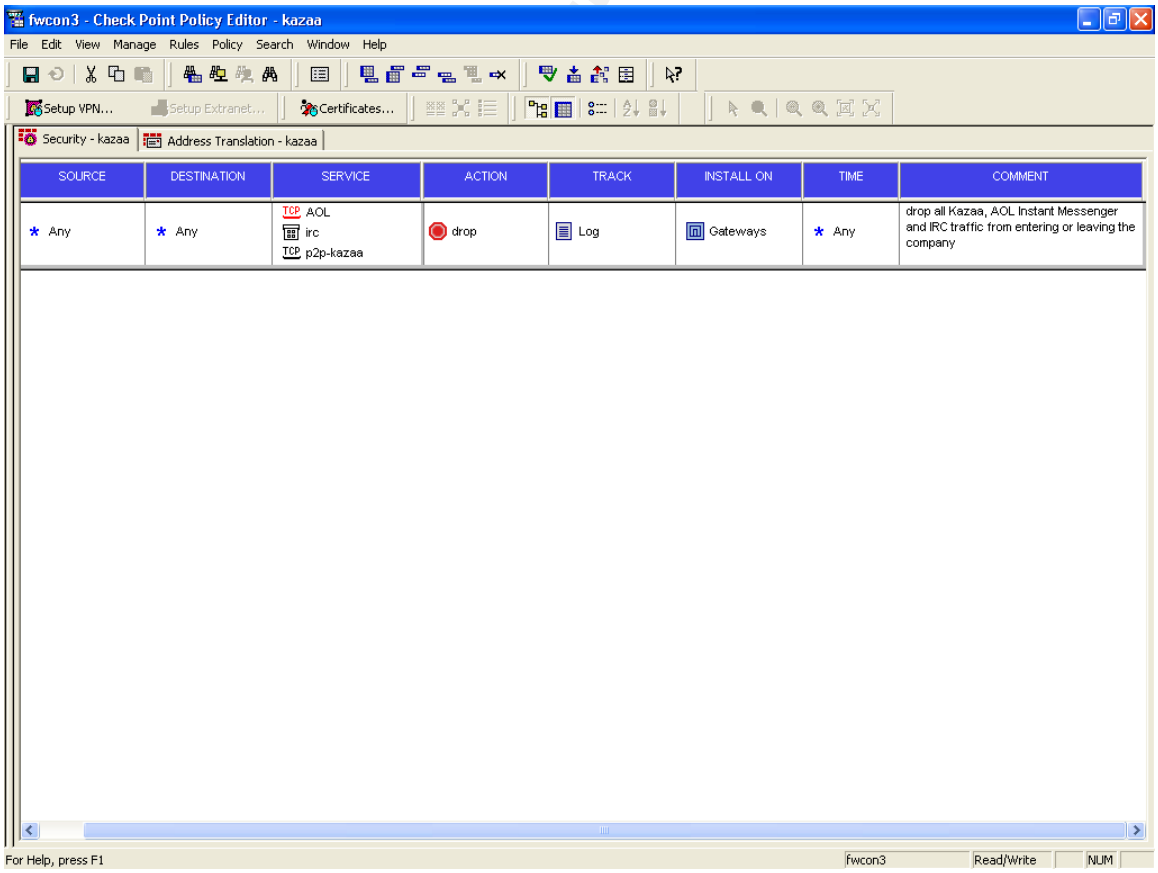
- Note pad and pens
- Tape recorder
- Spare hard drives (internal and external) formatted for both Unix and Windows architectures
- Scsi cables (fast wide and scsi2 both internal and external)
- USB external hard drives and zip drive
- Polaroid camera
- A whiteboard with printing capabilities
- Laptops configured with all flavors of window's and Unix operating systems used by the company

Eradication

As described in an earlier section Joe's computer became infected via the Kazaa P2P file sharing protocol. After he was infected the computer opened several back door connections to outside services and replicated itself via email by sending copies of itself to everyone in Joe's email address book and any other documents Joe may have had with email addresses in them. This means that Joe's machine is infected as well as the company's email server, in this case exchange 2000.

To remove all sources of current infection and potential infection three things must be done. First on Joe's computer a fresh burn of the XP operating system needs to be produced and used to replace his current hard drive. This removed the infection and also removes the Kazaa software Joe should not have been using in the first place. Second the exchange server needs to be searched for all emails with executable attachments. To do this we would use a tool provided my Microsoft called Microsoft Exchange Mailbox Merge program or exmerge. Details about this utility can be found at:
http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b174197

The last server that needs to be fixed is the firewall. A new rule needs to be added to block traffic to and from Kazaa, AOL IM and the IRC channels. For a CheckPoint NG firewall that rule would look like this:



A follow up to the eradication process would be for corporate communications to send a notification to all employees that the ports and services used by Kazaa, AOL IM and IRC chat have been blocked. This email should also state that further attempts to use these services will not be allowed.

Recovery

Because this incident occurred after work hours and the actual infection was limited to one machine the only recovery needed was on Joe's desktop machine. This limited recovery was achieved by giving Joe's computer a new hard drive with the standard, base corporate build that all employees start out with.

There was no recovery needed on the exchange server only the removal of the emails with infected attachments and there was no recovery on the firewall just an additional rule that needed to be added.

Lessons Learned

The biggest lesson learned by the company is that they need to do more of everything. They got lucky this time around and the infection and damage was very limited.

The company needs to do tests of the incident handling team and while they did a good job during this incident they need more practice. The company needs to review the posted policies and procedures for what type of traffic will and will not be allowed on their networks. The company needs stated and supported disciplinary actions that will be enforced should the policies and practices not be followed. The company needs to review their firewall rules more frequently.

The company needs to educate the employees on what is and is not company property, including computer hardware, and what are acceptable uses for company assets.

Some positive lessons they learned were that the practice of stringent log review by internal employees and the monitoring 24x7 by an outside company works and that the response team can be put together rapidly if need be and function coherently when they need to.

Bibliography and Sources Used

Northcutt, Stephen, Computer Security Incident Handling. SANS Press. 2003

Incident Handing Step-by-Step and Computer Crime Investigation. Track 4 – Hacker Techniques, Exploits and Incident Handling – Day 1. SANS Press. 2002

http://www.microsoft.com

http://www.symantec.com

http://www.cert.org

http://www.incidents.org

http://www.f-secure.com

http://www.trendmicro.com

http://www.mcafee.com

http://www.legato.com

http://www.sophos.com

http://www.kazaa.com

http://www.rfc-editor.org

http://www.iana.org