Global Information Assurance Certification Paper

SANS Practical Assignment
GCIH Certification

Incident Illustration for DoS Attack in a Small Business Environment

By: Lane H. Melton, GSEC

Executive Summary

Technological development and capability is one of the fastest growing entities in the world today. This growth affects society in every facet of life. From military readiness, to healthcare, to agriculture, to monitoring our children at daycare, technology is around us. Due to this influx, we must rapidly change to meet the challenges it brings and utilize the capabilities it offers. For years now big business has made use of the Internet with its high speeds of data transfer and its ability to reach out to millions. And recently, "every day" people and traditional "Mom and Pop" business are now among the fastest to utilize the ever-present changing technology, but often with a heavy price.

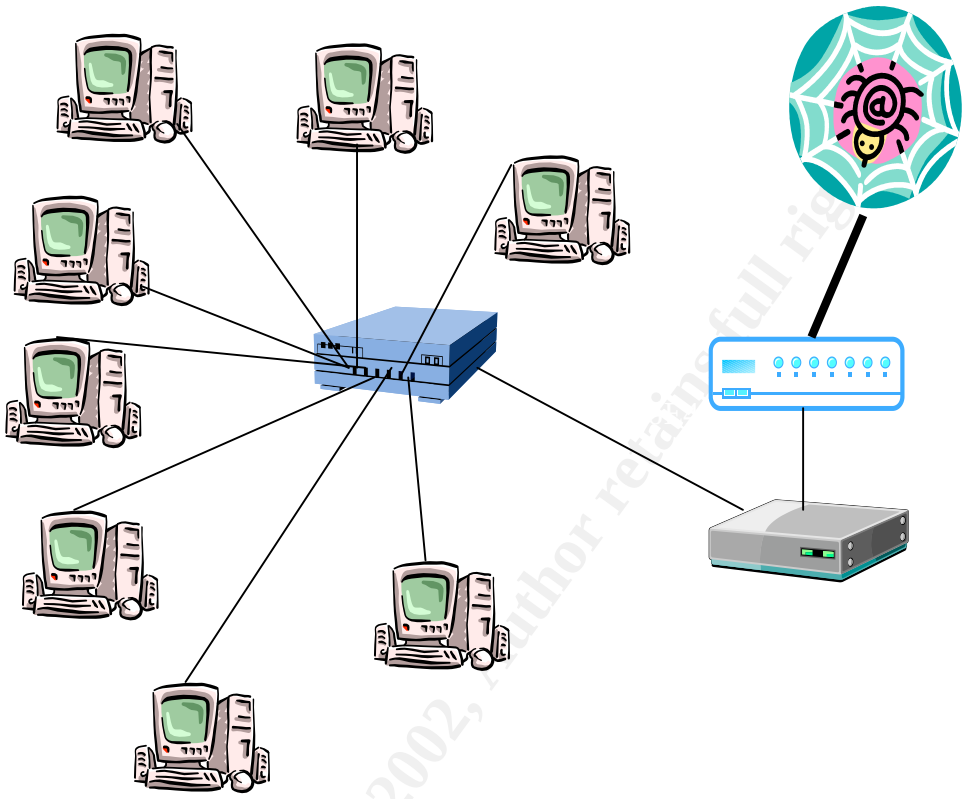
Big business having millions of dollars (we all know that is not necessarily allocated to the IT department) has the ability to research and implement new technology developments quickly and effectively. However, in the race to keep up and stay alive, small, more traditional businesses hear about new technology and do their best to implement it. These changes are often made on a "whim" and with little research or subject matter training completed. They implement new technology without knowing its full capabilities and pitfalls. Unfortunately, this creates a unique niche market for attackers to come in and bring small business to its knees.

Small businesses as well as home users are quickly becoming targets for attackers. While the reasons for attack vary, these businesses are unmistakably becoming victims at an alarming high rate. This paper will describe an incident of attack against a small, one owner business. It will demonstrate how the business handled the incident as compared to the six-step process of incident handling and will also it will also demonstrate deficiencies and improvements in their strategy.

The attack could be classified by two categories, first and foremost, a Denial of Service (DoS) attack and second, malicious code. The DoS attack caused the business PC to lock completely up and cease to operate. It was later discovered that the DoS was due to a malicious Java script. While Java Script is **not** malicious, it was used in a malicious manner and thus vaguely categorized as malicious code. The event occurred in a small business environment with no full time IT staff. I was not present at the incident location during the time of attack but was called in soon after it took place and rendered my services as a friend. This network consisted of eight PCs with file and print sharing connected to a hub in a star topology, then to a router/firewall and on to a cable modem. Each PC had the purchased version of Zone Alarm 2.6.88. Email was handled via a web-based account.

Figure 1 below, gives a basic outline for the network topology.

Figure 1 Network Topology



The Incident

On a regular basis, the small company accesses local news groups in order to obtain research on various products they deal with. These products are purchased by a very faithful following and are also in stiff competition with other similar products. Often the result is one group "bad mouthing" or degrading another manufactures product. During a news group fact-finding session, an employee clicked on what she thought was pertinent information. At that time a screen popped up using profanity and degrading their product. Immediately after the initial screen, over one hundred additional windows opened and completely locked the computer. The employee tried to move their mouse, click the "Start" button, and tried the "Windows" key on the keyboard to no avail. The PC was completely locked up. After alerting the business owner and his examination of the PC, it was turned off using the power switch. The PC was then rebooted and appeared to resume normal operation. However, the owner decided to turn off the PC for the rest of the day and I was contacted that evening after business hours. Again, I would like to reiterate that I was contacted as a friend and not as a purchased security service.

The following information documents how the six phases of incident handling were applied. This is very interesting because the company in general is technology savvy but has no experience in security. It looks like they gave it a pretty good shot but didn't quite make it.

Incident Index:

Incident Handling

Phase 1: Preparation

This small business had no full Information Technology person on staff and all network issues were the sole responsibility of the company owner. He would be categorized as a "power user". The owner also has final signoff on business operations (which includes the network). He reads articles and views telecast to keep up to date on the latest in technology, gadgets and information. Before installing the network, he researched security issues and determined that Zone Alarm, a router/firewall, and anti-virus software also needed to be implemented. While these products and features are fine in themselves, they are **NOT** defense in depth.

The following information will show the implemented network configuration, where it was suitable or lax and how it could have been improved.

Banners and Password Policy
There was no use of login banners or warning devices for unauthorized login. Password policy was lax at best. Passwords had no standard for alphanumeric style, length and expiration time.
Improvement: Implement Windows Resource Kit. This would have facilitated the creation and implementation of warning banners against unauthorized used as well as provided C2 security standards. It would also assist in identifying the lax password policy and provided recommendations for alphanumeric style, length and expiration.

Workstations
All workstations were loaded with Microsoft Windows 2000; factory install. Web browser was Internet Explorer 5.5 and was set for Medium-Low security. Mail program was Outlook Express 5.5 and was used only for accessing news groups. Email was handled by web-based products. Each node's C:\ drive was accessible by all other network nodes, which had full administrative privileges it.
Improvement: Check the critical downloads at Microsoft at [i]www.microsoft.com/windows2000/downloads/critical/default.asp for latest product updates, patches and security bulletins. Perform this check and implement at regular intervals on all network nodes. Service Pack 1 at a bare minimum should have been installed on each machine. This installation would have also updated attached applications for product updates such as Internet Explorer and Outlook Express. Windows Resource Kit would have also identified lax network permissions to all C:\ drives. Access to all drives should have been limited to a specific directory on the PC and allowed a minimal number of users.

Hub – Router/Firewall
The network was connected via a standard 10/100 hub, which in turn was connected to a router/firewall. The router/firewall was configured with the following specifications:

> *Network Address Translation (NAT)*
> Utilized one IP Address at the router/firewall. Hides all network components from the Internet.
> *Dynamic Host Control Protocol (DHCP)*
> Allocates "closed end" or "non portable" IP Addresses to all network components behind the router/firewall. Allocates the IP Addresses to components on an as needed basis. Set to expire ever 24 hours.
> *Logs*
> Disabled Mode.

Improvement: Router offered limited configuration ability; however did allow port configuration. Required PC and network services should have been identified along with appropriate ports. NAT is good and appropriate. Change DHCP to expire the IP Address ever two hours. Reset logs to log both incoming/outgoing traffic and to log to a separate server.

Zone Alarm 2.6.88
There are two main areas for configuration in Zone Alarm. They are Internet and Local or LAN Security. Internet security was set to the default "high". It enforces application privileges, has an Internet lock to block all traffic, blocks Internet access to Windows services such as file and print sharing, and hides all ports not in use. Local security enforces application privileges and Internet lock settings only, and Internet lock blocks only application traffic, and allows LAN traffic to access Windows services such as file and print sharing, and leaves computer and server applications visible to others on the network. Zone Alarm was also configured to allow full operation of Outlook Express and McAffee Virus Scan.
Improvement: Set local security to high and specifically allow services that are needed.

McAfee Virus Scan
Was installed on all network nodes. Virus definitions had been manually updated somewhat recently but were not absolutely current. The "Live Update" was not configured to retrieve virus definition files on a regular basis.
Improvement: Set "Live Update" to automatically update virus definition files. Establish date to purchase new software annually.

Jump Kit
The company did not have a "Jump Kit".
Improvement: A jump kit is used to help in identification, eradication and recovery of an incident. At a bare minimum it should consist of a laptop running Win2K, Linux 7.0 and Nessus. This provides a Windows and Unix environment as well as an incredible scanner and vulnerability analysis tool. The laptop should be fitted with a CD-Burner and a Network Interface Card (NIC). The laptop should also have a gold disk for it should it be compromised during the investigation. It should also be hardened with the latest patches and service packs. In addition it is good to have at least five writeable CD's, five floppy disks, a notepad, pencils, a voice recorder, a boot disk and Ghost software. The Ghost software should be used to back up the "Incident" PC or system.

Security Policy
There was no written or understood policy to address information security or incident handling. Because of this small business environment, it would not be appropriate to establish huge incident handling teams and elaborate chain of commands for communications. However, it would be most appropriate to establish policy concerning security within the company and how a breach of security would be handled. This environment would benefit greatly by designating one or two individuals to have security as a collateral duty or hire a full time Information Technology/Protection person. In this case, the latter of the two was not an option.
Improvement: Establish a written security policy to identify the following:
Annual or semi annual employee training should be conducted concerning network security, web-site visitation, email and attachments, news group usage and emergency contact numbers.
Individuals responsible for security and incidents should be identified and their phone numbers provided to all employees.

Individuals responsible for security and incident handling should be adequately trained to handle them.
Identify individuals outside the organization and their phone numbers that should be contacted for legal issues. This should include but not be limited to the FBI, local/state law enforcement and legal representation. This category could also include help from outside sources that may have more expertise than what is "in house".
Identify a chain of communications for all incidents. Establish who should be contacted first, second and third etc…
Ensure there is a way to communicate. All parties involved in incident handling should be equipped with beepers and phones.

It is evident that the company was in a prime situation for breach of security. While there were a few good features like the personal firewalls and anti-virus software, the company as a whole was vulnerable. Defense in depth was not being practiced leaving opportunity for employees and outsiders to do harm.

Phase 2: Identification

The Identification Phase is used to determine weather an incident has happened or not and to determine the incidents nature. I was contacted the night of the incident and was told that something had happened to lock up a PC at work. After a brief description of the situation, I was asked to examine the PC the following morning. I had asked the business owner if the incident had affected other PCs within the company. He said no, that one was the only as far as he could tell. He did request that I get the "Incident" PC back up as soon as possible. [ii]His request fit the requirement of eradicating the problem and getting back to work listed in SANS Step-by-Step Incident Handling. I expected to arrive and find the network infected with Trojans, and at least half of their systems controlling the space shuttle. During the Identification phase of any incident, an individual should be assigned that is responsible for it. This establishes order, organization and control. I was asked by the owner to assist in the situation therefore making me responsible for the incident handling. This was really no different than in large organizations. There, the incident handler in charge is still subject to the authority of upper management, and board members. In this case, I had to clear all my intentions and activities with the business owner. I arrived the next morning with my jump kit (contents listed in Phase 1), and performed the following tasks:

Disconnected the "Incident" PC from the network
The "Incident" PC was eventually turned off after the incident occurred and was still powered down on my arrival. I went ahead and pulled the network cable.

Interviewed User
It was necessary to interview the individual using the "Incident" PC to determine if an incident had actually occurred. Given the description below, I determined that at least a minor incident occurred. It was described to me according to the following:

- Subject matter was selected from a news group pertaining to the company's product. When that information was clicked, immediately the screen was filled with web pages and the PC would not function any more. The company owner

was alerted and he made several attempts to operate the PC with no success. It was then powered down and restarted. No notice of specific information from a limited boot script was made and no outstanding information presented itself on reboot. The PC started and seemed to operate as normal, however it did seem a bit sluggish. The owner then decided that it should be turned off and wait until someone could be contacted that could help. It was at this stage of the description that I determined that at least a minor incident had occurred. I moved on to get the details.

Examine the log files of Router/Firewall
Using another PC, I examined the log and configuration files of the router/firewall. The router/firewall was standard and could be purchased at any electronics store. I also examined the configuration parameters for:

- Setup
- Password
- Status
- DHCP
- Log
- Advanced

Each section was properly configured and no unusual information was found. However, the log file was disabled. I asked the owner if he had initially enabled it and he said that he did not know. I enabled it after obtaining the owner's permission.

Booted the PC
I arrived with Ghost software in order to make a backup of the system. Fortunately, they had a PC that was not being used. Using a boot disk and the software, I made a backup copy of the "Incident" PC. The backup process is usually performed during the Containment Phase; however, I felt it necessary at the time to perform a back up immediately. The PC was booted (disconnected from the network), with normal operation; it did search for a network connection though. The copied or "cloned" PC should be used to investigate the incident so as to preserve the original evidence trail should it be needed in a court of law. There was no abnormal operation to visibly demonstrate that the PC had been tampered with.

Examined the Logs of "Incident" PC
Windows Explorer, The Event Viewer and Zone Alarm Logs were examined.

Windows Explorer
On the C:\ drive were two unusual files in a FOUND.0000 directory. They were:

- FILE0000
- FILE0001

I opened FOUND.0000 and it had two files in it with the "Services" Icon that you would find under Control Panel – Services. Both files were 8 KB in size. I made copies of these files on a floppy disk. They would be examined at a later time.

The Event Viewer

Three areas were examined:

- The Application Logs revealed no unusual entries.
- The Security Logs were not auditing. (I noted in my notebook that this should be recommended to be turned on).
- The System Logs revealed only one, small discrepancy. There was a message stating that the computer was not able to renew its network address from the DHCP server and another stating that it was automatically configured using a "closed end" IP Addressed assigned by the machine. This is noted in the graphic below. The reason I made mention of this, is that it seems to have happened around the same time of the incident.

Event Type: Warning
Event Source: Dhcp
Event Category: None
Event ID: 1007
Date:
Time:
User: N/A
Computer: PC1
Description:
Your computer has automatically configured the IP address for the Network Card with network address XXXX. The IP address being used is XXX.XXX.XXX.XXX.
Data:
0000: 00 00 00 00 ....

This seems to be standard though when using Zone Alarm if that service (DHCP) is not preset to always on. An IP Address expires after a predetermined amount of time has passed and the DHCP server assigns a new one. If this action has not been specifically allowed in the Zone Alarm configuration, the IP Address will not be distributed. When this occurs, the network node will assign a "closed end" IP Address until one is accepted by the DHCP server. In this case, Zone Alarm had not been preconfigured to do so.

Zone Alarm Log

Once again all looked fairly normal with the exception of two things. The first being an occasional block of the "Incident" PC trying to access the Internet in an unauthorized manner or a server asking for server rights to the PC. This seemed consistent and normal in that environment. The second was that Zone Alarm picked up the event that would not allow the PC to renew its IP address. This is displayed in the graphic below.

PE,TIME/DATE	4:00 GMT,TCP/IP Services Application,0.0.0.0:0,N/A
PE, TIME/DATE	4:00 GMT,Windows Explorer,XXX.XXX.XXX.XXX:1029,N/A

ACCESS, TIME/DATE	4:00 GMT,Services and Controller app could not accept a(n) UDP Port 68 connection from XXX.XXX.XXX.XXX because Internet servers are blocked.,N/A,N/A
PE, TIME/DATE	4:00 GMT,Generic Host Process for Win32 Services,XXX.XXX.XXX.XXX:520,N/A
ACCESS, TIME/DATE	4:00 GMT,Generic Host Process for Win32 Services was unable to obtain permission for connecting to the Internet (XXX.XXX.XXX.XXX:Port 520); access was denied.,N/A,N/A
FWIN, TIME/DATE "INCIDNT TIME"	4:00 GMT,XXX.XXX.XXX.XXX:0,XXX.XXX.XXX.XXX:0,ICMP (type:3/subtype:2)
PE, TIME/DATE	4:00 GMT,Generic Host Process for Win32 Services,XXX.XXX.XXX.XXX:520,N/A
PE, TIME/DATE	4:00 GMT,Generic Host Process for Win32 Services,XXX.XXX.XXX.XXX:520,N/A
PE, TIME/DATE	4:00 GMT,Generic Host Process for Win32 Services,XXX.XXX.XXX.XXX:520,N/A
PE, TIME/DATE	4:00 GMT,Services and Controller app,0.0.0.0:0,N/A
PE, TIME/DATE	4:00 GMT,Generic Host Process for Win32 Services,0.0.0.0:0,N/A
PE, TIME/DATE	4:00 GMT,ZoneAlarm Pro,XXX.XXX.XXX.XXX:80,N/A

Here is an explanation of the log file according to Zone Alarm Help.

PE informs you that an application on your PC attempted to access the Internet.

FWIN informs you that the firewall blocked an incoming request to connect to your PC. It will also include the Date and Time, the Source IP Address and Port number, the destination IP Address and Port number and the transport, i.e., TCP, UDP, ICMP etc.

FWOUT informs you that the firewall blocked an outbound request from your PC to an outside location. Like the others it will include Date and Time, the Source IP Address and Port number, the destination IP Address and Port number and the transport, i.e., TCP, UDP, ICMP etc.

Examined the Browser settings of "Incident" PC

The browser being used at the time of the incident was Internet Explorer by Microsoft. Most of the settings were default. However, there were two settings that raised red flags. First, Active X was activated and allowed. Second, Java was activated and allowed. There was no prompting set and they were allowed as needed.

After looking at the browser and the resounding red flags, I thought it would be a good time to look at the two files that had been graciously captured by the system for me to view.

The first file I opened was FILE0000 in Word Pad. It was an explanation of what the file was along with some code. The code was garbled and could not be read. The graphic below displays the file contents. The code explanation within the file described the code as a "crapplet". [iii]http://info.astrian.net describes a "crapplet" as "A worthless applet, esp. a Java widget attached to a web page that doesn't work or even crashes your browser". Ah, seems we are getting somewhere now. That definition seemed to fit the description of what happened during the incident. With Java turned on, this seemed to fit perfectly. The explanation of the Java code itself said it would crash the browser. As shown in the graphic below, the code uses several graphics from different web sites. Apparently, something was added to the code because it not only locked up the browser but locked up the PC as well.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
<HTML>
<HEAD>
   <TITLE></TITLE>
   <META NAME="GENERATOR" CONTENT="Mozilla/3.0b6Gold (Win95; I)
[Netscape]">
</HEAD>
<BODY
background="http://www.meat.com/textures/img/a051.jpg"
TEXT="#000007" BGCOLOR="#000000" LINK="#0000EE" VLINK="#551A8B"
ALINK="#FF0000">

<CENTER><P>
<HR><APPLET code="Starfield3.class" width=296 height=150
ALIGN=CENTER><PARAM name="numimages" value="8"></APPLET></P></CENTER>
<h3>
<P>Give this crapplet a shot. I'm not sure how vicious it really is
because
I got tired of crashing my computer in order to refine it. It might not
even work anymore, who knows. It works best with MS Internet Explorer
(with
the Java plugin, natch) for two reasons:</P>

<UL>
<LI>The Images load <I>much</I> faster. It's not even funny. Ten times
faster wouln't be a bad estimate.</LI>

<LI>It seems to crash a bit more spectaculary when you click on the
Crapplet.
Netscrape boringly performs the proverbial &quot;illegal
operation&quot;
quite quickly. MSIE freezes up the screen and proceeds to absolutely
<B><FONT COLOR="#FF0000">flog
</FONT></B>your hard drive. It's fun.</LI>

<LI>The Just-In-Time compilation seems to make a slight difference.
Sorta.
Maybe?</LI>
</UL>

<P>To make things &quot;fair&quot; I give you a 50/50 chance. Half the
time it will actually take you to the SMT page when you click on
```

```
it,
the other half it will crash. If you just want to see the hostile
performance,
feel free to click on the applet a whole bunch of times, but you might
as well wait for the images to load, cuz they're groovy, and the applet
will go wacko if you try to leave the page before the animation
starts.</P>

<P>Somebody try this on mac/linux/or (God help us) Win 3.1. Let me know
if anything interesting happens. I'm also kinda curious to see how fast
it runs on a slow machine, but my turbo button isn't connected.</P>

<P>Does anyone have that hostile Javascript code? Might as well throw
that
on this page to see what the combo is like.</P>

NOTE:  This page isn't that good if you don't have java.
<CENTER><P>
<HR></P></CENTER>
</h3>
</BODY>
</HTML>
```

The second file I opened was identical to the first with the exception of Java and HTML script at the bottom of the page. This information is listed below. I am not a Java expert but it appears that an HTML page list a table of sorts, which displayed Java code messages. I was not entirely sure, so I opened the file in a browser. The code below is what I found in addition to the description above. The code basically uses graphics from other sites and creates a table for users to input information which can be used for ill purposes.

// Away img = 'src="http://XXX.XXX.XXX.XXX/icon_messenger2.gif"'; msg = L_IsAway_Text; break; case 34: // Away img = 'src="http://XXX.XXX.XXX.XXX/icon_messenger2.gif"'; msg = L_IsAway_Text; break; case 50: // On the Phone img = 'src="http://XXX.XXX.XXX.XXX/icon_messenger3.gif"'; msg = L_IsBusy_Text; break; case 66: // Out To Lunch img = 'src="http://XXX.XXX.XXX.XXX/icon_messenger2.gif"'; msg = L_IsAway_Text;

break; } if (Page=="CONF") { ret = ' ' + pUser.FriendlyName + '

'; } else if (Page=="IB") { ret = ' '; } else if (Page=="RM") { ret = ' ' +

msgFromName.value +" + msg +"; } else { ret = ' ' + pUser.FriendlyName + "; } return ret; } function DoInboxIM() { var DataTable; var State = MsgrObj.LocalState; if (isStateOnline(State)) { DoUsers(); DataTable = document.all.MsgTable; for (i=1; i< DataTable.rows[i].cells[2].innerHTML='
' { else } DataTable.rows[i]

' } } else if ((UserNotOn[E] != null) &&
(DataTable.rows[i].cells[2].children[0].tagName=="TABLE")) {
DataTable.rows[i].cells[2].innerHTML =
DataTable.rows[i].cells[2].children[0].rows[0].cells[0].innerHTML; } } } } } function
DoAddressesSubmit() { if ("undefined" == typeof(MsgrObj)) { //the object wasn't
created return; } var DataTAble; var State = MsgrObj.LocalState; if
(isStateOnline(State)) { DoUsers(); DataTable = document.all.msngrdata; for
(i=0;i<=2;i++) { if ((DataTable.rows[i].cells[3].children[0].checked) &&
(DataTable.rows[i].cells[3].children[0].disabled==false) &&
(AllUsers[DataTable.rows[i].cells[2].children[0].value]==null)) {
DoSilentAdd(DataTable.rows[i].cells[2].children[0].value) } } } } function
CheckAddressInput() { var CB = this.parentElement.parentElement.cells[3].children[0];
if (ValidateEmail(this.value)) { if (AllUsers[this.value] == null) { CB.disabled=0; } else
{ CB.disabled=1; } } else { CB.disabled=1; } } function DoAddresses() { var
DataTAble; var State = MsgrObj.LocalState; if (isStateOnline(State)) {
document.all.msngrH.innerHTML="**'+L_AddToMy_Text+'**"; DataTable =
document.all.msngrdata; for (i=0;i<=2;i++) {
DataTable.rows[i].cells[2].children[0].onchange=CheckAddressInput; if
(DataTable.rows[i].cells[2].children[0].value) {
DataTable.rows[i].cells[3].innerHTML='<input type=checkbox disabled>'; } else {
DataTable.rows[i].cells[3].innerHTML='<input type=checkbox disabled checked>'; } } }
document.addr.alias.focus(); } function DoSaveAddress() { var DataTAble; var State =
MsgrObj.LocalState; if (isStateOnline(State)) { DoUsers(); DataTable = document.all.msngrdata; for (i=1;i
'+L_Add_Text+E+L_MyMessList_Text+"; } } } } function DoSaveAddressSubmit() { if
("undefined" != typeof(MsgrObj)) { if (isStateOnline(MsgrObj.LocalState)) { for (var
i=0;i<document.domsgaddresses.elements.length;i++) { var e =
document.domsgaddresses.elements[i]; if ((e.name != 'allbox') &&
(e.name.match(/msngr/)) && (e.checked)) { DoSilentAdd(e.value); } } } } } function
DoSilentAdd(email) { var list = MsgrObj.List(0); var services = MsgrObj.Services var
NewUser = MsgrObj.CreateUser(email,services.Item(0)); list.Add(NewUser); } function
DoABIM() { var DataTable; var State = MsgrObj.LocalState; if (isStateOnline(State)) {
DoUsers()

With that examined, I had a theory and a couple of questions. My theory was that an HTML page was loaded and that it crashed the PC by overloading its memory. My first question was, did the Java code load any other applications on the PC, secretly sending information to a remote location. Second, was the PC set up as a pawn or a jump to control other PCs? I presented this option to the owner of the company along with options for loading an IDS on the network. He did not want this done at the present time, nor did he feel the need for me to connect an external sniffer to the network. I did do a vulnerability scan and the results are listed in Phase 4 of this paper.

CERT has developed a "Windows NT Intruder Detection Checklist" which can be found at [iv] www.cert.org. This checklist involves a fifteen-step process for examining various components of your system. Some of the steps I followed were to examine log files, check for odd users and accounts, check for unauthorized shares, check for changes in user or computer policies and examine all machines on the local network concerning items in the checklist. These steps were applied to all nodes on the network and they showed no signs of an invasion, except that one.

Evidence Collection
It is absolutely crucial that all evidence such as the scripts and logs listed above be documented and kept pristine. Attorneys and experienced handlers can assist in developing a policy for collecting evidence, however the owner in this case did not choose to notify anyone else but me.

Copies of files, printouts, photographs, voice recordings and reports should all be kept confidential and controlled by a small group of individuals. The evidence should be kept in a controlled environment such as a safe or guarded room. There should also be procedures established for all authorized individuals to sign in or out when viewing or working with the evidence. The owner and I were the only authorized persons to enter the room.

In this incident I voice recorded all my findings. They consisted of the procedures I used to examine the log files and give a verbal description of what I found. User interviews were also recorded with the permission of the individual being interviewed. I also made a copy of the files that were recovered on to a CD-ROM. I maintained a copy of them and gave a copy to the owner of the company. I made copies of my voice recordings and gave them to him as well.

Notification
Notification of evidence findings to the appropriate management will also assist in moving forward with the investigation. Alerting them as to what was found keeps all concerned parties aware of what is going on and aids in effective communication. The owner was with me most of the time. However he did have to leave several times when I needed to discuss an issue with him. This made steady progress difficult. This issue is further discussed in the Lessons Learned section of this paper.

Phase 3: Containment

The Containment Phase is used to stop the incident from proceeding or causing further damage. At this point the an incident handling team will come in, secure the incident area, prohibit the incident from proceeding any further and collect the evidence. This also involves making backups of the compromised system and changing administrative passwords. In this incident, a backup had already been performed. This was done because the PC was shut down after the initial incident on-set. I felt that additional damage might occur to the PC should it be rebooted. By implementing the backup in the identification phase, the original state of the machine was captured.

One other key factor in containing an incident is to see if the incident has spread to other systems. Router and system logs were collected during the Identification Phase. They were reviewed again for accuracy with no additional details found.

Phase 4: Eradication

The purpose of the Eradication Phase is to purge, remove, abolish, or kill the cause of the incident. Several steps to follow to ensure eradication:

Determine The Cause And Symptoms Of The Incident

The problem was a combination of a malicious Java script or "crapplet" and employee security training.

Performed a Vulnerability Analysis

Using Nessus, a vulnerability analysis was performed resulting in the following information:

Nessus Scan Results

Warning found on port netbios-ns (137/udp)

. The following 6 NetBIOS names have been gathered :
XXX = This is the computer name registered for workstation services by a WINS client.
XXX = Workgroup / Domain name
XXX
XXX = Computer name that is registered for the messenger service on a computer that is a WINS client.
XXX
XXX = Computer name that is registered for the messenger service on a computer that is a WINS client.
. The remote host has the following MAC address on its adapter :
"MAC ADDRESS"
If you do not want to allow everyone to find the NetBios name
of your computer, you should filter incoming traffic to this port.
Risk factor : Medium

Information found on port general/udp

For your information, here is the traceroute to XXX.XXX.XXX.XXX :
XXX.XXX.XXX.XXX

Warning found on port general/tcp

The remote host uses non-random IP IDs, that is, it is
possible to predict the next value of the ip_id field of
the ip packets sent by this host.
An attacker may use this feature to determine if the remote
host sent a packet in reply to another request. This may be
used for portscanning and other things.
Solution : Contact your vendor for a patch
Risk factor : Low

Warning found on port general/icmp

The remote host answers to an ICMP timestamp
request. This allows an attacker to know the
date which is set on your machine.
This may help him to defeat all your
time based authentifications protocols.
Solution : filter out the icmp timestamp
requests (13), and the outgoing icmp
timestamp replies (14).
Risk factor : Low

This file was generated by[v] Nessus, the open-sourced security scanner.

The information recovered from the scan was documented and removed during the Recovery Phase using the Windows Resource Kit and the C2 standard.

Remove the Cause/Improve Defenses
Malicious files were removed and employees were trained on a newly developed security policy.
The security policy included:

- Passwords – Should have an expiration date, be alphanumeric, and be no less than eight characters.
- User rights – If shared drives must be used, users may only have access to certain folders and not the entire drive and no services. The guest account should be disabled and the administrator account renamed.
- Antivirus Software – Live Update should be configured to automatically check and update virus definitions files and the product should be updated completely once a year. Full system virus scans should be scheduled to run regularly.
- Appropriate News Group Use – Only click on news group information that appears from a logical source. Do not choose one with garble in the "from" name. Do not open attached files.
- Browsers Settings – Implement High Security and turn off Active X and Java components or prompt the user before using them.
- Email Attachments – Only open email and attachments from a trusted source.
- Incident Handling – Should an incident occur, unplug the cable from the network and immediately call for assistance. The contact information and numbers are to be made available to all employees. All employees will be trained who to contact during an incident. Individuals responsible for incident handling were to be given phones and pagers.
- PGP – Should be installed on all PC on the network to protect and encrypt vital data. Backups should be performed on a regular basis of the file server.
- Zone Alarm – Services on the PC and those vital to Internet usage were identified and configured in Zone Alarm as well as the PC. All others were turned off.
- IDS – Snort and its capability was discussed. The owner decided to delay the implementation of it. (Against my advice).

Phase 5: Recovery

The primary focus of the Recovery Phase is to get the system back up and running. In this instance we concentrated on three issues:

Restore The System
The owner and I discussed how to ensure the system was absolutely safe. Based on his sole decision, I rebuilt the system from the ground up. I feel that after removing the malicious files and installing the appropriate service packs, the system would have been safe. However, I rebuilt the system from a low level format to production. This also included an installation of Service Pack 1 and The Window Resource Tool Kit. New Anti-virus software was installed and configured for "Live Update" for virus definition

files. Virus scans were set to run on a regular basis. Zone Alarm was also configured for High security and allowed services that were needed.

Ensured It Is Safe For Use Or Validated
To ensure that the system was safe, we ran a Nessus scan on the system again which reported no problem. We also ran a full system virus scan on all network notes with reported no problems. Using the Windows Resource Kit we also brought all network nodes into C2 compliance.

Put Back Into Operation And Monitor
The system was reconnected to the network. Before this however, I recommended that an IDS be placed on the system. This would have been a good watchdog for future detection of network security problems. The owner declined the implementation of an IDS, temporarily. He did ask me to come back and install one at a later date.

CERT offers a very similar list of information for recovering from both a Windows and a UNIX system compromise. The overall steps are as follows:

1. Consult the security policy
2. If no policy consult with management
3. Document all steps
4. Regain control
5. Analyze the intrusion
6. Contact relevant sites like CERT for incident reporting
7. Recover from the Intrusion
8. Improve the security of the system and network
9. Reconnect to the internet
10. Update the security policy

This paper can be read in detail at [vi]www.cert.org/tech_tips/win-UNIX-system_compromise.html.

The SANS Institute offers complete courses on incident handling which is the foundation of this paper as well as successfully recovering from this documented incident.

Phase 6: Follow Up

The primary focus for the Follow Up Phase is to compile what happened, evaluate it, and make recommendations for improvement and to learn from experience. After any incident it is important to immediately start compiling the events of the incident for a report. This should thoroughly document the entire incident from the cause to the end result of recovery. All parties in the incident handling should have a part in creating this report. Once written the report should be reread by all involved to reach general consensus and submitted to management for review. Also the security policy should be changed or amended to reflect the newly implemented security. In this case, the owner did not want a written report nor wanted to report the incident to an agency like SANS. He did not want the publicity. However, we did use the evidence we collected along with

the changes we made to the network and "Incident" PC to develop a new security policy and train the staff on it.

On evaluation of all the evidence, symptoms and problems, I concluded this was the most basic denial of service attach. However this could have been quite serious. Typically, this is classic of Trojan infestation. By clicking on the news group, this could have downloaded a file to the pc, which was activated when it was rebooted. An example of this is Back Orifice 2K (BO2K). One safeguard against this happening is good virus software, kept up to date, and scans everything before permitting a download.

One last time before I left, I used the command ipconfig/all and netstat with the following switches – ae, an, and ar. The result revealed no unusual of unexpected information.

Lessons Learned

I believe I learned the most from this incident. Several factors came into play. I have always looked at things from a technical point of view. This incident helped me realize that I needed a generic plan to deal with small business aspects as well as technical issues. A security policy is a key factor. Often there is no policy. Often small businesses don't realize the need for one. This incident helped the owner and me to understand that there is a crucial need for one and how it can help recover and protect.

Lessons learned also include chain of custody procedures. In this small business environment, there was no chain of custody at all. It consisted of one link – the owner. He was consumed with the business operations and could not devote the appropriate time to the network and security. For the same reasons, communications were not optimal during this incident. For most of this incident, he was looking over my shoulder. However, there were many times that he had to attend to other things and could not assist me. No one else was authorized to make appropriate decisions. I also did not know who I could discuss certain issues with concerning my findings. This has led me to develop a generic chain of custody form that includes names and numbers for network administrators, managers, sign off authority and public relations people. Even in a small environment, these positions can be assigned as collateral duty and make the flow of information much smoother.

Works Cited:

[i] www.microsoft.com/windows2000/downloads/critical/default.asp for downloads, July 09, 2001
[ii] "Incident Handling Step by Step", The SANS Institute, Page 4, Copyright 1998 The SANS Institute
[iii] http://info.astrian.net "crapplet". July 09,2001
[iv] http://www.cert.org/tech_tips/win-UNIX-system_compromise.html. July 09, 2001
[v] http://www.nessus.org, July 09, 2001
[vi] http://www.cert.org/tech_tips/win-UNIX-system_compromise.html. July 09, 2001