# Global Information Assurance Certification Paper

Royal Canadian Mounted Police | Gendarmerie royale du Canada

## Executive Summary

As part of my certification in the GIAC Advanced Incident Handling and Hacker Exploits, I have been tasked with describing an incident in which I took part. I work in the Royal Canadian Mounted Police (RCMP) Technical Security Branch (TSB), which is part of the Technical Operations Directorate. TSB is organized on a functional basis to satisfy client demand for professional advice and guidance in numerous areas pertaining to physical and information technology security. The branch is divided into eight sections responsible for supporting five major functions: physical security, information technology security, incident response, investigative assistance and counter-technical intrusion. This document describes a real incident that was reported by a gentleman who wishes to remain anonymous. For simplicity reasons, I will refer to him as Joe Public.

## Six Stages of Incident Handling

The six stages of incident handling are preparation, identification, containment, eradiation, recovery and lessons learned. A short description of each step follows.

## 1. Preparation

Preparation is the first stage of incident handling. It is important to identify qualified people to join the incident handling team, organize a command post, and to develop management support for your team.

The section I work in is the Incident Response Section of the Technical Security Branch. It is staffed with IT Security consultants with a variety of specialized expertise in information technology security. Members possess broad academic and practical backgrounds in various areas of information technology, including computer hardware, software, communications and operations, and are extensively trained in accepted administrative, personnel, physical and technical security principles, to provide government departments with comprehensive security reviews and consultative services in the field of information technology security.

The Incident Response Section provides an incident reporting phone line and an incident handling Internet email service that respond to reports of computer incidents affecting the federal government of Canada. We have a 24 hour / 7 days a week hotline. We share on-call responsibilities after hours, with the RCMP's National Operation Centre which includes responding to calls, checking anti-virus vendor sites for newly discovered viruses, and sending advisories or alerts regarding these newly-discovered viruses if deemed necessary. We generally only handle incidents pertaining to the federal

government of Canada, but on occasion we do receive requests for help from the general public through our website. If at all possible, we try to answer these requests, but our priorities lie with the government of Canada departments.

I have included a screen shot of our original Technical Security Branch (TSB) website, which includes our email address and phone number for incident response. We have just hired a consultant who will be redesigning our entire TSB web site to give it a whole new look and feel. (See diagram 1 – RCMP TSB original website)


**Diagram 1 – Technical Security Branch original website**

Once an incident has been reported, we record the pertinent information in a database application called HEAT. There are four sections to the HEAT record to be completed, namely:

- Call Log Section;
- PIRS & Details Section;
- Assignment Section; and
- Journal Section

a) The Call Log is where we enter all the information pertaining to the client (victim) including the client type (private citizen, private business, government department,

RCMP department, etc), their name, organization, title, city, province, phone numbers, and email address. A leader is assigned to the incident and a call type is assigned. The incident is then assigned a priority number (1 meaning high and 3 meaning low), with a start date, file number, and offence type. A short description of the incident is also entered. (See Diagram 2 - HEAT Call Logging Section on next page).

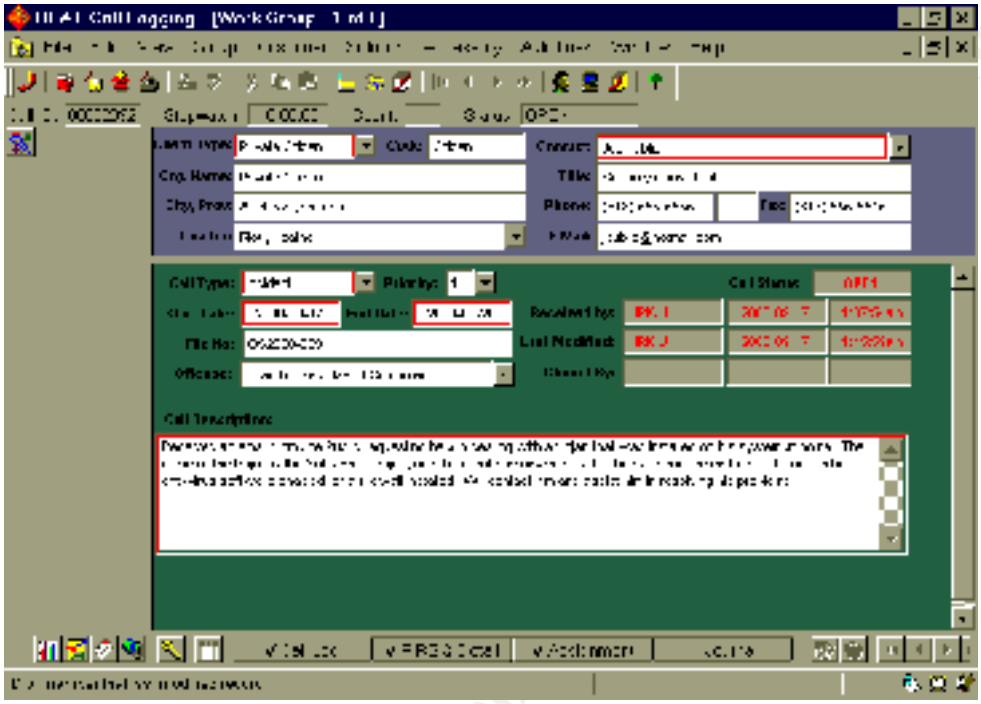


**Diagram 2 – HEAT Call Logging Section**

b) The PIRS & Details section is filled out by police investigators. Due to the high sensitivity of this section I cannot provide any more details.

c) The team leader then assigns other team member's tasks to be completed. (See diagram 3 – HEAT Assignment Section)

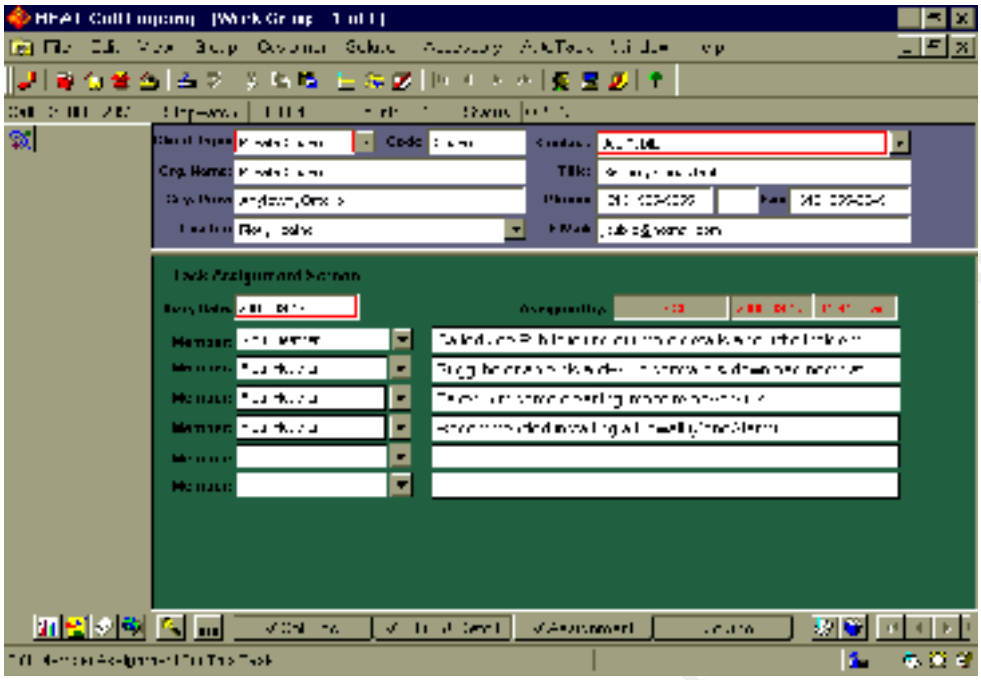


**Diagram 3 – HEAT Assignment Section**

d) During the incident investigation, each team member assigned to the incident can create a journal entry explaining details of each step of the incident. This is done in the fourth section of the HEAT record. It is basically just a notepad for entering further information. The database application also allows you attachments, i.e. email, documents, logs, etc. to each record. We usually attach all information we have regarding the incident to the HEAT record, and print and file a hard copy of each document as well.

Once the incident has been completed, we close the HEAT record and print a copy to be filed with the other documentation on the incident. We use this database to generate different types of statistical reports on the incidents we handle.

Incidents that are reported during normal working hours come in either through the incident response phone line or into the incident response email. The phone line and email account are checked regularly to ensure a prompt response to the incident.

After normal working hours our incident response phone line pages the person who is on call. The on-call person is provided with a pager (with an extra AAA battery), a cell phone (with extra battery, car plug-in, and wall chargers), and a binder, which contains call lists, organizational charts, checklist, procedures, and pager & cell phone manuals.

All of our RCMP computer systems that can be accessed from the outside have a warning banner in place.

We have just recently implemented a contingency plan, which was prepared for the Y2K rollover. This included establishing policies, creating emergency call lists, establishing

methods of informing people quickly (i.e. by email, fax, phone, cell phone or pager), and establishing interfaces with system administrators, other law enforcement agencies and computer incident response teams. We placed copies of passwords, encryption keys, call lists and call tree information in an offsite location, and made sure that at least two incident team members knew the location of this information. Presently, we do not have a jump bag at our disposal, but we are seriously thinking of putting one together since attending the SANS Advanced Incident Handling and Hack Exploit Course. The jump bag when assembled should include a small tape recorder, binary backup, forensic software, fresh backup media, CDs with binaries, windows resource kit, small hub, laptop with dual operating system, call lists and cell phone.

## 2. Identification

Identification is the second stage of incident handling. The event is analyzed by the assigned incident handler to determine if it is an actual incident. The definition of an incident (taken from SANS course notes Mon-4 Incident Handling: Step-by-Step and Computer Crime Investigation) is as follows:

*An incident refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event.*

We are careful to maintain a provable chain of custody at this point. (i.e. not deleting files, identifying every piece of evidence, and controlling access to the evidence). This is done by completing an exhibit report and placing a date, time, and initial of person who received evidence in permanent marker on the evidence.

In the case that I am presenting in this document, an email arrived after working hours from Joe Public (victim did not want to be identified) stating that he was having problems with his Pentium III 600 mHz computer (running Windows 98 second edition). He was advised by a friend to scan his hard drive for viruses with his PC-Cillin anti-virus software (which he installed when he purchased the computer but unfortunately had never enabled). His anti-virus software determined that his computer was infected with the SubSeven Trojan. (See Diagram 4 – Altered email from Joe Public – sent from a friend's machine)

| |
|---|
| From : "Joe Public" <JPublic@hotmail.com> |
| To: "Incident" <incident@magma.ca> |
| Subject: Virus |
| Date: 2000,09,17,Sunday 10:05 AM |

Good Morning

After spending many hours trying to figure out what happened to my fairly new Pentium III 600 mhz machine, I am requesting the advice of your incident response team. I was on the internet without my PC-Cillin anti-virus software enabled, and I have somehow gotten a virus on my machine. I am guilty of downloading a lot of games from sites, and have a lot of jokes sent to me through emails. A friend of mine advised me to scan my hard drive for virus. My anti-virus software shows I have a SubSeven Trojan. My computer is not working properly at all, and anytime I try to run any application I get errors. I am not sure what to do. Could you please contact me at:

555-5555 Telephone

555-5545 Fax

Thanks, Joe Public

**Diagram 4 – Altered email from Joe Public sent from a friend's machine**



**Phone Call to Joe Public – Sunday September 17th, 2000 11:45 AM**

I called Joe Public to find out more details about the incident. I asked him what operating system he was running and what sort of symptoms he was seeing as a result of this Trojan. He was running Windows 98 second edition, and was having problems running any applications. He said that he had scanned his C: drive with PC-Cillin and found the Trojan. He then tried to clean the virus with his anti-virus software but was not successful in doing so. I was sure at this point that an incident had occurred as his anti-virus software had confirmed a virus had been found. Since this was not a government incident I was not obligated to respond to this incident, but I decided to see if there was anything I could do to help him. I reviewed the information gathered from Joe Public and used the Internet to search for information regarding the SubSeven Trojan.

The definition of a Trojan horse is as follows: (taken from SANS – Tue-4/Wed-4 Computer and Network Hacker Exploits: Step-by-step, Parts 1 & 2, page 303)

*A Trojan horse is a program that looks innocuous, but is really sinister.*

Trojans are executable programs meaning when you open the file, it will run and perform some action(s). In the Windows environments, executable programs have file extensions like .exe, .vbs, .com, .bat, .pif, .scr, .lnk, or .js. Multiple extensions are also seen sometimes with Trojans. (i.e. Loveletter-for-you.txt.vbs). Joe Public could have received this Trojan any number of ways. (i.e. via email, on ICQ or downloaded from a site.)

**Description of the SubSeven Trojan**

I found the following information on the Internet regarding the SubSeven Trojan. The first variant of the SubSeven Trojan was first discovered in May of 1999. It was written by an individual known as MobMan. The SubSeven trojan currently affects Windows 95/98 operating systems. This backdoor is usually distributed under different names via newsgroups and emails. The package contains two or three programs. One of the files should be installed on a "server" machine. Once the server program is installed the client can take control over the victim's computer. The client is a powerful remote administration tool similar to NetBus. It has many remote controlling abilities. (See below for list of 113 capabilities of the initial version of SubSeven)

The client is also capable of stealing passwords and reading keyboard keys pressed on the server since the last boot. The third program in the package is a utility that can be used to configure the server program. It is possible to patch the server with any executable so it looks as if a user received a valid file instead of the trojan.

The server configuration program also configures the way the server is installed. To install itself the server can use the Windows registry file. It can also change the C:\WINDOWS\WIN.INI or C:\WINDOWS\SYSTEM.INI files so that the server runs on starting Windows. The client portion of the software has a nice looking GUI. (See next page for screen shot of the client version of the SubSeven Trojan.)


**Diagram 5 - Client Version of SubSeven**

The following is a screenshot of information obtained by the client portion after it attached to a PC that was compromised with the server portion. Note: it reflects information about the compromised system.

**Diagram 6 – Info obtained by client portion after attaching to a PC that was compromised**

The next screenshot shows the "EditServer" utility. This is the utility that allows the hacker to customize the "server" portion of the trojan. The server portion of the trojan is configured, and then sent to the victim.

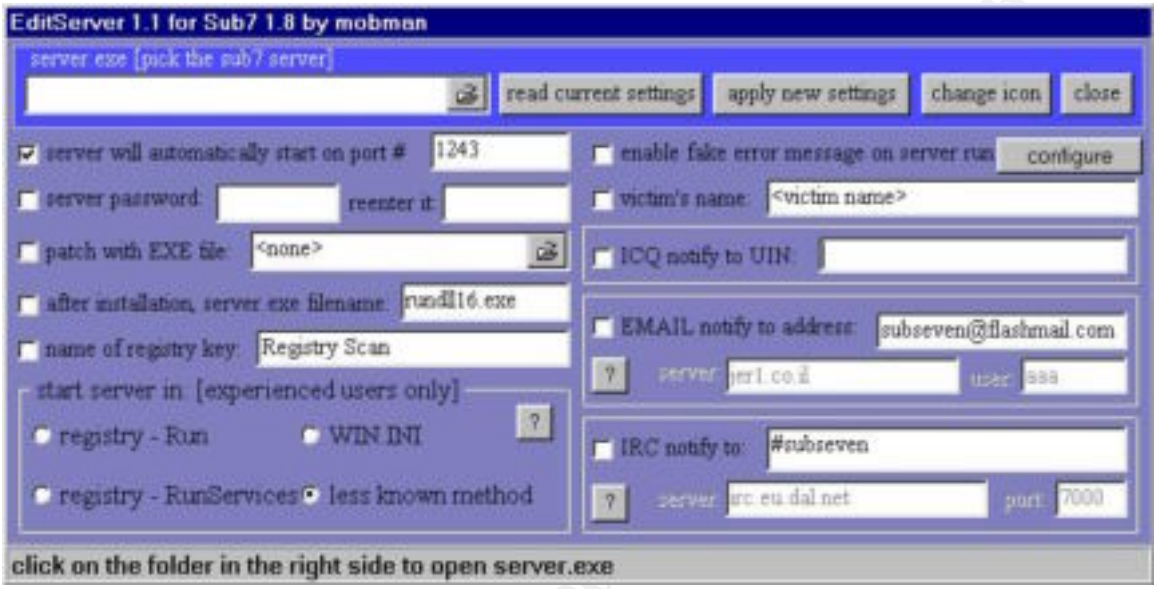



**Diagram 7 – EditServer utility**

SubSeven can be a bit difficult to remove due to the fact that the server portion can be configured to rerun itself automatically from any of four places each time the system has been rebooted. The server portion can have any name, and is found in the WINDOWS directory, with one of the following names:

1) server.exe (328kb)
2) rundll16.exe (328kb)
3) systray.dl (328kb)
4) Task_bar.exe (328kb)

The second file is found in the WINDOWS\SYSTEM directory, with one of the following names:

1) FAVPNMCFEE.dll (35kb)
2) MVOKH_32.dll (35kb)
3) nodll.exe (35kb)
4)watching.dll (35kb)

The default TCP Ports 6711 and 6776 are generally used, but a third TCP port is used in the establishment of the connection between the "client" and "server". This third TCP port can be configured to be anything, although it's commonly seen as TCP port 1243 or TCP port 1999.

The server portion of the trojan can be configured by the hacker to rerun itself each time the system is rebooted due to an entry in one of the following four locations:

1) an entry on the "shell=" line in the SYSTEM.INI file. (Note: most likely place)

2) an entry on the "load=" or "run=" line in the WIN.INI file.

3) under
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

4) under
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

## Capabilities of the SubSeven Trojan

Here is a list of 113 capabilities of the initial version of SubSeven. (obtained from the F-Secure Virus site):

### Fun Manager

1. Open Web Browser to specified location.
2. Restart Windows.
3. Reverse Mouse buttons.
4. Hide Mouse Pointer.
5. Move Mouse.
6. Mouse Trail Config.
7. Set Volume.
8. Record Sound file from remote mic.
9. Change Windows Colors / Restore.
10. Hung up Internet Connection.
11. Change Time.
12. Change Date.
13. Change Screen resolution.
14. Hide Desktop Icons / Show
15. Hide Start Button / Show
16. Hide taskbar / Show
17. Opne CD-ROM Drive / Close
18. Beep computer Speaker / Stop
19. Turn Monitor Off / On
20. Disable CTRL+ALT+DEL / Enable
21. Turn on Scroll Lock / Off
22. Turn on Caps Locl / Off
23. Turn on Num Lock / Off

### Connection Manager

1. Connect / Disconnect

2. IP Scanner
3. IP Address book
4. Get Computer Name
5. Get User Name
6. Get Windows and System Folder Names
7. Get Computer Company
8. Get Windows Version
9. Get Windows Platform
10. Get Current Resolution
11. Get DirectX Version
12. Get Current Bytes per Pixel settings
13. Get CPU Vendor
14. Get CPU Speed
15. Get Hard Drive Size
16. Get Hard Drive Free Space
17. Change Server Port
18. Set Server Password
19. Update Server
20. Close Server
21. Remove Server
22. ICQ Pager Connection Notify
23. IRC Connection Notify
24. E-Mail Connection Notify

### Keyboard Manager

1. Enable Key Logger / Disable
2. Open Key Logger in a remote Window
3. Clear the Key Logger Windows
4. Collect Keys pressed while Offline
5. Open Chat Victim + Controller
6. Open Chat among all connected

### Controllers

1. Windows Pop-up Message Manager
2. Disable Keyboard
3. Send Keys to a remote Window

### Misc. Manager

1. Full Screen Capture
2. Continues Thumbnail Capture
3. Flip Screen
4. Open FTP Server
5. Find Files
6. Capture from Computer Camera
7. List Recorded Passwords
8. List Cached Passwords
9. Clear Password List
10. Registry Editor
11. Send Text to Printer

### File Manager

1. Show files/folders and navigate

2. List Drives
3. Execute application
4. Enter Manual Command
5. Type path Manually
6. Download files
7. Upload files
8. Get File Size
9. Delete File
10. Play *.WAV
11. Set Wallpaper
12. Print *.TXT*.RTF file
13. Show Image

### Window Manager

1. List visible windows
2. List All Active Applications
3. Focus on Window
4. Close Window
5. Disable X (close) button
6. Hide a Window from view.
7. Show a Hidden Window
8. Disable Window
9. Enable Disabled Window

### Options Menu

1. Set Quality of Full Screen Capture
2. Set Quality of Thumbnail Capture
3. Set Chat font size and Colors
4. Set Client's User Name
5. Set local 'Download' Directory
6. Set Quick Help
7. Set Client Skin
8. Set Fun Manager Skin

### Edit Server

1. PreSet Target Port
2. PreSet server Password
3. Attach EXE File
4. PreSet filename after installation
5. PreSet Registry Key
6. PreSet Autostart Method:
   Registry: Run
   Registry: RunSevices
   Win.ini
   Less known method
7. PreSet Fake error message
8. PreSet Connection Notify Username
9. PreSet Connection Notify ICQ#
10. PreSet Connection Notify E-Mail
11. PreSet Connection Notify IRC Chan.
12. PreSet IRC Port
13. Change Server *.exe Icon

## 3. Containment

Containment is the third step in Incident Handling. The goal of containment is to keep the problem from getting worse. I quickly but thoroughly reviewed the information gathered from Joe Public was well as the information that I obtained from the Internet, and called Joe Public. The first recommendation that I made to him was to disconnect his computer from the Internet (ensuring he had physically unplugged his computer from the phone line.) I asked him if he had any backups from which he could restore his system, but the only backups he had were some WordPerfect documents he had saved to diskette. Normally, if this had been a government incident, we might deploy a small team to survey the situation, then secure the area, and review the information that was provided from the identification phase. We make every effort to keep the system pristine. I also recommended that he change all the passwords on his system as the hacker probably acquired knowledge of them.

## 4. Eradication

The fourth step, eradication, is probably the hardest step of all. You must completely and safely remove all of the malicious code. Since we already knew the name of the virus that had infected the system, it was just a matter of completely removing the Trojan from his system. From talking to Joe Public, I discovered he had already tried to remove the virus with his anti-virus software but unfortunately he did not get all the files cleaned properly (either that or the anti-virus software did not detect all the files that were infected). I found some good manual removal instructions for the SubSeven Trojan from an anti-virus site (see Appendix A - SubSeven Removal Instructions) and faxed him the instructions. Unfortunately, this did not totally fix the problem. I decided since it was a fairly new machine and he did not have many programs installed on it yet, the best way to eradicate the trojan was to re-install the operating system from the original CD. I asked him if he was confident in doing this install, and he said he would give it a try. Since he had a bootable diskette already made, I suggested that he format the hard drive and reinstall Windows 98. This step went extremely smoothly until he could not find his Product ID code to bring Windows 98 up. Once he located this code, and entered it, the system booted clean. He had to reinstall the drivers for his video card and sound card, but other than that, Windows 98 was back intact.

## 5. Recovery

The first thing I asked Joe Public after he reinstalled the operating system was to change all his passwords on the system. This helps prevent unauthorized users from getting access again. I also recommended that he install McAfee Anti-virus software, as this is

what we use at work, and it is fairly reliable. I reminded him of the importance of updating his anti virus dat and superdat files. I stressed that this must be done on a regular basis. I then asked him to apply all the patches to his system, reinstall his browser and critical updates before returning to the Internet. I reminded him that the intruder entered his system through a hole and the best way to avoid this is to close as many holes as possible.

After all the critical updates were done on his operating system, and his anti-virus software was updated and enabled, I recommended that he install a personal firewall. (See Appendix B – Personal Firewall Information). He agreed to try ZoneAlarm and he downloaded the application and installed it on his machine.

He then reconnected his telephone line to his computer and once again began to surf the web. ZoneAlarm kept a good eye on the intruders trying to get into his system. If only he had taken the time previously to learn about safe web surf perhaps he would not have been in this predicament.

I asked him to monitor his system closely for a few weeks to see if there would be any more malicious activity. He has agreed to report back to me in the event of another attempted attack.

## 6. Lessons Learned and Follow Up

The PC was brought back online the same day as the email was sent in. The following recommendations were faxed to Joe Public to avoid further infection.

1. Never use features in your programs that automatically preview or get files. (i.e. disable preview mode in Outlook or other mail utilities)
2. Never download from sites that are not considered reputable or from people you don't know.
3. Always beware of hidden file extensions. Unhide extensions to view the whole file name.
4. Remember that anti-virus software is only effective if you download dat and superdat files on a regular basis, and even then, some new viruses can sneak through.
5. If you receive something questionable from a friend via email, always make sure you know what is in the file before opening it.
6. A personal firewall when configured properly helps ward off unwanted intruders and can alert you when an application wants to attach to the Internet.
7. Always apply all the critical patches and upgrades to your operating system and applications.
8. Close all unused ports!

When I was convinced that the incident had been completed, I closed the HEAT record and attached this paper to the HEAT record. I then printed a copy of this document to circulate amongst our incident response team, and filed an original copy.

**For at least one operating system involved in the incident, show the process used to assess and contain, including screen shots and operating system commands. In this section you should describe your jump kit, and all the tools that you used.**

The operating system that was compromised was Windows 98 Second Edition. The anti virus PC-Cillin was responsible for the detection of the Trojan, but did not clean the system properly. Since the victim could not run anything on his system, it was impossible to get actual screen shots of the events. Had this of been a government incident, with sensitive information being compromised, there would have been a different assessment done to decide how to handle the situation.

The machine that was compromised was fairly new and did not have any sensitive information on it.

The victim was responsible for the format of his C: drive and the installation of the windows 98 operating system.

As mentioned earlier in the report, we do not have a jump kit available to us at the present time, as we are generally only the first level response to an incident. We are however, considering putting together a jump bag in the near future.

One valuable tool I used to assess and contain the incident was the Internet. I checked for information regarding the Trojan on many anti-virus sites to evaluate how to safely remove it.

**For at least one operating system involved in the incident describe in detail the process used to back up the system. This should include descriptions of the hardware, commands, and any problems that you ran into.**

Due to the fact that the machine was fairly new, and there was not a lot of information stored on the hard disk, it was decided to reform the C: hard drive. The user had already backed up his wordperfect documents, so there was nothing on the system that he wanted to save.

I have included the procedures that Joe Public used to re-install Windows 98 Second Edition on his machine.

1) With FDISK he deleted all the partitions on the machine

2) With FDISK he created a brand new partition that he made ACTIVE

3) He then reboots his machine from his clean bootable floppy. This bootable floppy gave him access to his CD ROM drive.

4) With the Windows 98 Second Edition in the CD ROM drive, he ran SETUP and the setup program took him through several standard screen.

5) After Windows 98 Second Edition was installed, the only problem that occurred was Joe Public could not find his Windows 98 Product ID number to enter. Windows 98 will not let you continue until this is entered.

6) After searching high and low, he found the book with the Product ID on it, and enters the Product ID number.

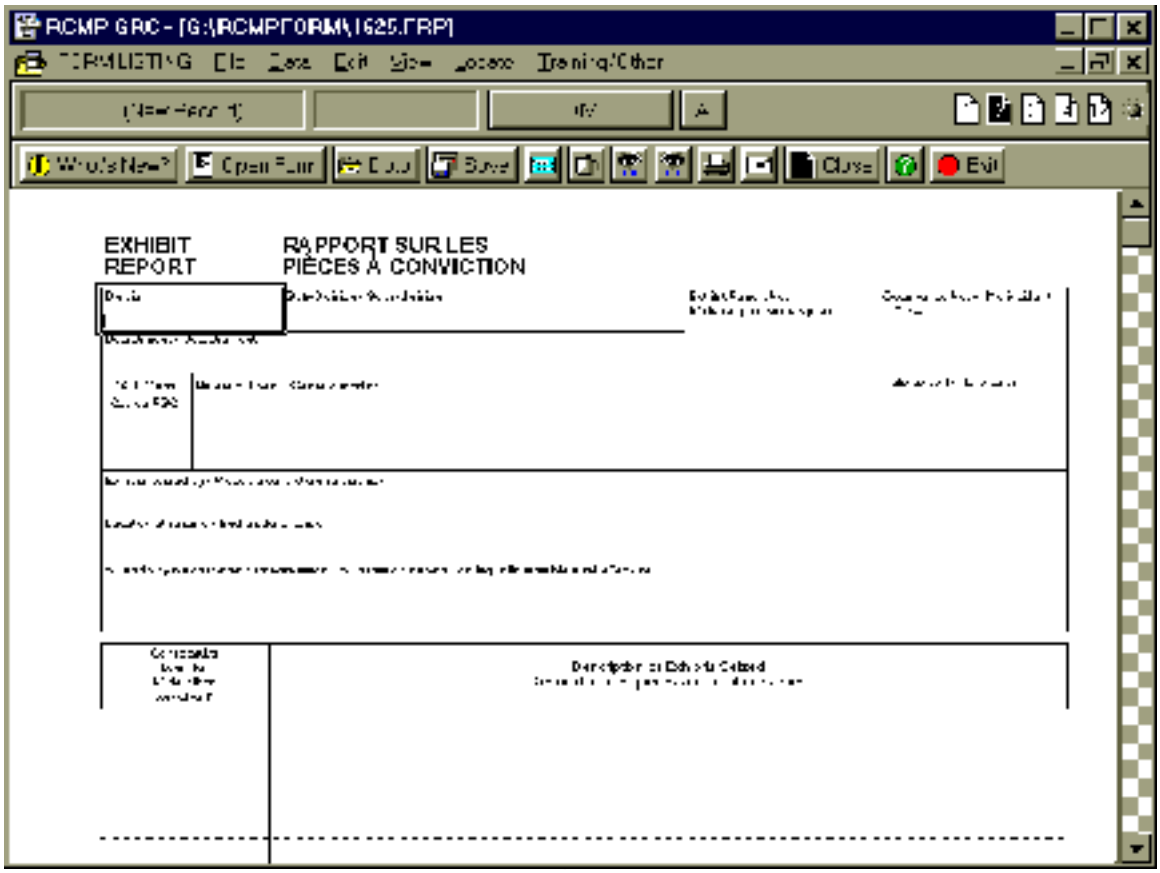
7) Windows had a hard time detecting some of this more advanced peripherals such as his advanced RAGE 128 video card and SoundBlaster Live card.

8) Both the RAGE 128 video card and SoundBlaster Live has to be reinstalled with the proper OEM drivers that came with the cards.

9) After the OS was installed, Joe Public installed all the other relevant software that he required (Browser, Anti-virus, Firewall, etc.).

**Describe in detail the chain of custody procedures used, any affirmations, and a listing of all evidence.**

The chain of custody procedures begins by filling out an exhibit report that is stored electronically on our form flow application. When an exhibit is brought in, the time, the date, and the initials of person who received it, is written in an inconspicuous place on the exhibit. This is done in permanent marker so that it cannot be altered or erased. Each exhibit is stored in a plastic bag that has a label on it identifying when it came in, what it is, who has handled it, and signatures of people (with data & time) who have handled it in order to maintain continuity. The label also contains where the exhibit came from, and any other identifying marks such as serial numbers, model numbers, etc. All exhibits are in a secure room and locked away at night. (See Form 1625 - Exhibit Report)






## Appendix A - SubSeven Removal Instruction

Due to the fact that the server portion of the SubSeven trojan can be configured to be loaded automatically from one of four locations, you'll need to look in all of the locations. A word of warning, please read the instructions carefully when editing the registry.

The first and second locations to check are:

1) the WIN.INI and

2) the SYSTEM.INI files

To check these locations follow the steps below:

Step 1.
Click START | RUN
Type SYSEDIT and press ENTER

Step 2.
Click on the SYSTEM.INI file and look at the "shell=Explorer.exe" line under the [boot] section. There should not be anything to the right of it. However, if yours looks like "shell=Explorer.exe Task_Bar.exe", then Task_Bar.exe is the server portion of the trojan.

Delete Task_Bar.exe from the line, save the changes. Skip to the END.

Step 3.
Click on the WIN.INI file and look at the run= and load= lines under the [windows] section. Note : it is common to have legitimate programs on either of these lines. You should look at the name of the file that appears on the line and compare it to those mentioned previously.

If you find one, delete it from the line, save the change. Skip to the END

The third and fourth locations to check are in The Registry. You will need to run regedit to edit the registry. To do this follow the instruction below:

Step 1.
Click START | RUN
Type REGEDIT and press ENTER

Step 2.
In the left window, click the "+" (plus sign) to the left of the following:
HKEY_LOCAL_MACHINE
Software
Microsoft
Windows
CurrentVersion
Run

Step 3.
In the right window, look for a key that has a Value that loads one of the files listed above. If you don't find a file as listed above, it might mean that the server portion was renamed to something else. Note the names of any suspicious files.

What you will need to do, is open Windows Explorer and go to the WINDOWS directory. Locate each of the suspicious files that were referenced within the right

window of regedit. When you find the file that's 328Kb in size. You've probably found the renamed server portion of SubSeven.

Step 4.
Return to the registry and in the right window, highlight the key that loads the file and hit the DELETE key. Answer YES to delete the entry.

Step 5.
Exit the Registry and reboot your computer.

Step 6.
After the computer has restarted, open Windows Explorer

Step 7.
Go to the WINDOWS directory and look for the suspicious file. Once you've found the file, DELETE it.

Step 8.
Exit Windows Explorer. With any luck, SubSeven has been removed.

## Appendix B – Personal Firewall Information

ZoneAlarm provides essential security for any computer connected to the Internet, especially those with always-on DSL or cable modem connections. ZoneAlarm protects you from malicious programs, like Spyware and Trojan horses, by allowing you to control your computer's Internet traffic and how applications access the Internet.

ZoneAlarm's Dynamic Firewall can block attempts to connect to your computer from the Internet. High Security Level makes your computer invisible from the Internet so you won't be a target for hackers and intruders. Security levels provide the most convenient way to configure the firewall, without requiring you to program protocols and ports.

When an application on your computer tries to access the Internet, ZoneAlarm makes sure it has your permission first. This ensures that a rogue program will not sneak your important data out onto the Internet.

ZoneAlarm appears as a panel on your Windows desktop, shown below. You can also interact with ZoneAlarm using the Desk Band Toolbar.


**Diagram 8 – ZoneAlarms control panel**

ZoneAlarm can be downloaded at http://www.zonelabs.com/zonealarm.htm

## References:

SANS – http://www.sans.org/newlook/home.htm

ZoneAlarm – http://www.zonelabs.com

McAfee Anti-Virus – http://www.mcafee.com

F-Secure Virus Information Pages - http://w.europe.f-secure.com/v-descs/subseven.htm

**Completed September 20, 2000 by Heather Riou of Incident Response Section, Royal Canadian Mounted Police**