



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at <http://www.giac.org/registration/gcih>

Steven A. Saunders
Advanced Incident Handling Practical
“Opening Pandora’s Box”

As an incident handler for a large global organization, I’ve seen just about everything from reconnaissance probes to multiple-system compromises. Normally, whenever a compromise report comes in to my office, it is either a defaced web page or some site that hadn’t kept up with the latest patches for their OS and got caught by some “script kiddies”.

Not long ago, I was assigned an incident involving one of our outlying sites. The initial report came in the form of a tip-off from law enforcement, which had seen one or more of my organization’s systems involved in an IRC session.

The incident would be a routine one, or so I thought. The deeper I delved into the evidence provided by the site’s network administrator, the clearer it became that “Pandora’s Box” had been opened.

The six phases of an incident are preparation, identification, containment, eradication, recovery and follow-up. The following paragraphs describe what was discovered through each phase.

Preparation. In this phase, an incident handler should be gathering necessary tools to adequately assess, evaluate and recover from an incident. Recommended tools include (but are not limited to) forensic software, CD’s with binaries for UNIX/Linux, a complete Windows resource kit, a laptop with dual OS, a contact list and phone book for the organization, a cell phone and some form of device to rapidly take notes.

Given that my organization has sites scattered around the world, it is cost-prohibitive to send members of my office out to most sites. Therefore, each site has a network security staff that functions as the on-site representatives for incident handling. My office directs the efforts of these representatives, who in turn report their results back to my office. Not only does this provide the capability of handling multiple incidents on a daily basis with minimal staffing, but it also emphasizes to network staff members at each site the need to know what is on their systems and keeping as up-to-date as possible on current vulnerabilities and patch levels. Only when absolutely necessary do members of my office go on-site to handle an incident.

As part of our role as “central dispatch” for incident handling, my office maintains an extensive list of documents and websites for ready reference. This list includes the websites of all major software vendors for hot fixes; the Security Focus website (www.securityfocus.com) for access to Bugtraq vulnerability reports, vulnerability discussion forums, forensics and vulnerability assessment

tools; and various hard- and softcopy documents generated by my organization and other affiliate organizations. These cover nearly everything from firewall policies and security directives to intrusion checklists and basic root compromise guidelines. Should any member of my staff actually need to go to a remote site to handle an incident, my local networking staff is capable of readily providing requisite hardware/software in support of incident analysis/recovery.

Identification. This phase consists of the identification of an incident. The primary incident handler is identified, and he/she looks for indications and warnings, ferrets out key pieces of information from end-users and systems administrators and fuses the information together to make an educated guess as to the whether or not an event is actually an incident.

All information gathered is carefully documented. Some bits and pieces, in and of themselves, may not be significant; but as the scenario plays out, the pieces will start to come together. Documentation is very important, should the case go to trial. It will also help to assess the situation after the fact when developing the final report on an incident. This is the time to begin evidence gathering; ensuring files are not deleted nor overwritten.

My office is not involved in the physical confiscation of systems or system components related to incidents. These functions are performed by law enforcement officials attached to my organization, so we do not have chain-of-custody procedures established. Only members of the CIRT team have access to files provided by sites reporting incidents, which are maintained in established directories for ready access. Backup copies are made daily onto floppy diskettes, which are maintained in locked cabinets when not actually in use. Any hardcopy evidence generated by CIRT members, including personal notes, is placed in clearly marked folders and is maintained in locked cabinets when not actually in use.

Clear, concise and timely communications play a key role. Appropriate personnel should be contacted as soon as possible. Remaining calm is important for maintaining control of the situation.

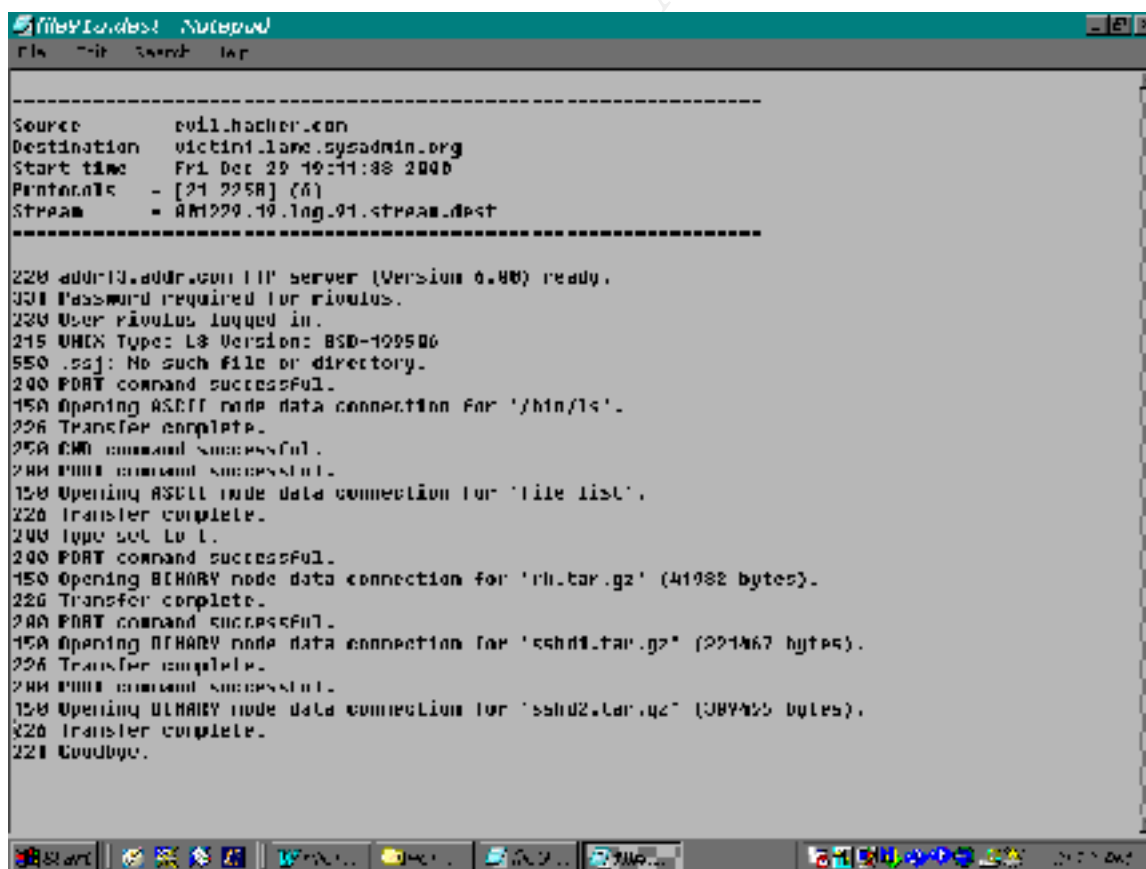
On January 18, 2001, while processing incoming event reports from various sites, my office received a tip-off from law enforcement, stating that one or more of my organization's systems had been seen in an IRC session. One of my co-workers contacted the network administrator of the site in question, requesting that she investigate the accuracy of the information provided and report back to my office.

The next day, I opened an email report from the network administrator confirming that they had been compromised since before the beginning of the year. This site is primarily involved with research, and has a working relationship with several commercial and educational organizations. The report had several files

attached (including FTP server logs and JIDS capture logs of FTP and IRC traffic) as amplifying information.

According to the report, an authorized user was working late on December 29, 2000, on a research project with a co-worker. This authorized user needed to send a 10MB file his system, which was located in a different building. The system that this file resided on did not have any form of secure copy utilities nor secure communications software (such as SSH) installed. The user, well aware of established security policies and the risk that he was taking, opened an FTP session with his own system. After sending his logon name and password in unencrypted format, he transferred the file to his system. The user stated that he was going to change his password in the morning to avoid possible compromise.

Unknown to anyone, the system that was being used had been compromised earlier and had a sniffer running on it. This system (which was running an unpatched version of RedHat 5.2) was compromised a couple of days earlier via the WU-FTP Site Exec vulnerability. Within an hour, a foreign hacker used the sniffed logon name and password to access the system that the 10MB file was FTP'd to, and installed a root kit, as shown below:



```
-----
Source      evil.hacker.com
Destination victim1.lame.sysadmin.org
Start time  Fri Dec 29 19:11:38 2000
Portname    - [21 2258] (6)
Stream      = RM229.19.log.01.stream.dest
-----

220 addr13.addr.com FTP server (Version 0.80) ready.
331 Password required for rivulus.
230 User rivulus logged in.
215 UNIX Type: L8 Version: BSD-100500
550 .gz: No such file or directory.
200 PORT command successful.
150 Opening ASCII mode data connection for '/bin/lc'.
226 Transfer complete.
258 CWD command successful.
200 CWD command successful.
150 Opening ASCII mode data connection for 'file list'.
226 Transfer complete.
200 Type set to I.
200 PORT command successful.
150 Opening BINARY mode data connection for 'rl.tar.gz' (41982 bytes).
226 Transfer complete.
200 PORT command successful.
150 Opening BINARY mode data connection for 'ssh1.tar.gz' (221467 bytes).
226 Transfer complete.
200 CWD command successful.
150 Opening BINARY mode data connection for 'ssh2.tar.gz' (1087425 bytes).
226 Transfer complete.
221 Goodbye.
```

This root kit, which was later identified as "Eggdrop", installed a sniffer, trojaned up to 13 different services and opened six different ports for telnet access. The

intruder then created a couple of bogus login accounts (authorizing root level access, of course) and installed an IRC client, which was downloaded from bitchx.dimension6.com. Utilizing the nickname "Atm0sfear", the intruder logged into several IRC sessions on various channels in the Undernet.org domain, apparently to brag about coming from one of my organizations systems.

Further into the report, it was identified that "Atm0sfear" compromised three additional boxes in the same manner while he/she was chatting online. After compromising each box and installing BitchX, he/she would start up another connection to the same channels in Undernet, indicating that another one of the site's systems was compromised.

As I had worked with the network administrator of the reporting site on a couple of previous incidents, I knew that she was familiar with what actions would be required. I contacted her to confirm that the compromised boxes had been removed from service and that full system backups of each box were in progress. I also inquired as to the possibility of further compromise of their network(s) by either "Atm0sfear" or another hacker. She stated that she would check into it and report back to me.

A couple of days later, the network administrator sent me an email stating that she found additional activity indicating several attempted and successful compromises of other systems in their network(s), via anonymous FTP login. Review of provided log files revealed that this site was utilizing FTP daemons written by several different vendors, many of which did not have continuing technical support. As an example, one system was running an FTP daemon written for an older version of Novell NetWare that had not been actively supported in over 6 years (see below):

```
UI Jan01 Notepad
File Edit Format View Help

-----
Source      = evil.hacker.org
Destination = victim4.lame.sysadmin.org
Start time  = Mon Jan 01 08:11:52 2001
Protocols   = [1058 21] (6)
Stream      = 010101.08.log.396.stream.init
-----

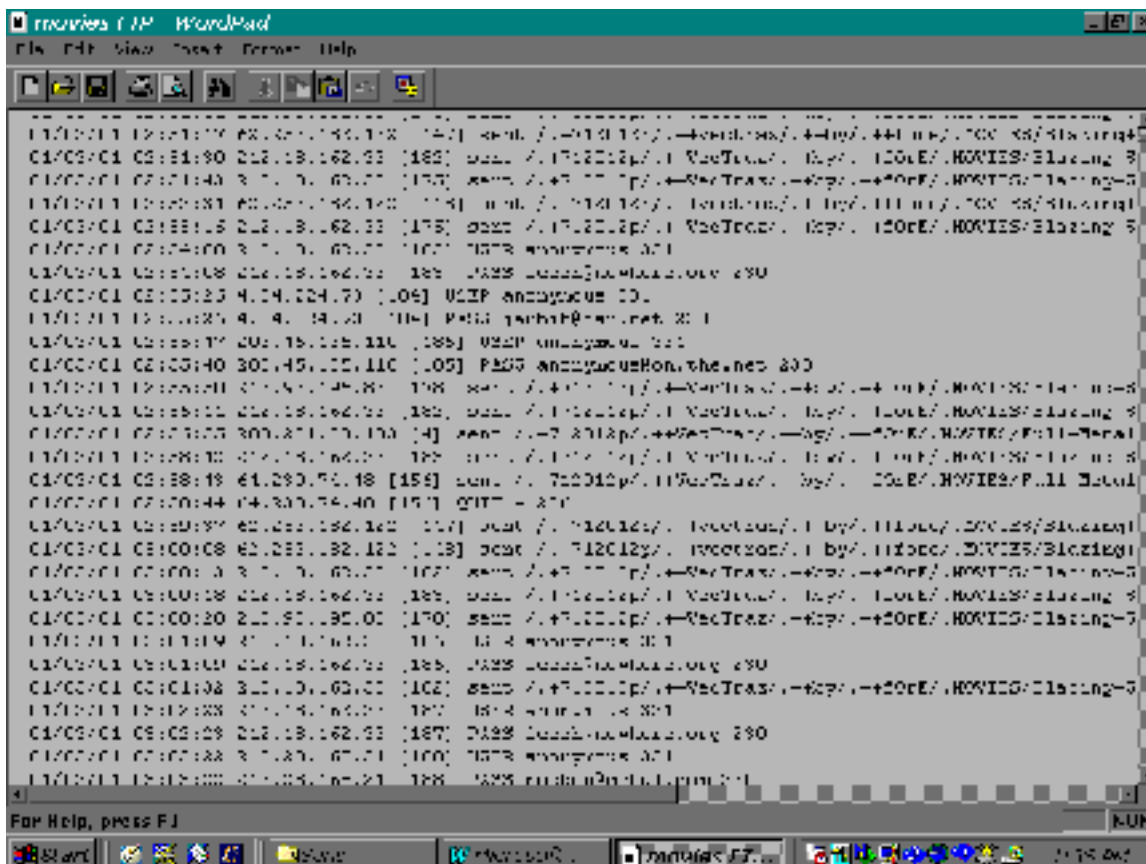
USER anonymous
PASS quest@here.com
CWD /pub/
CWD /public/
CWD /pub/incoming/
CWD /incoming/
CWD /_vti_pvt/
CWD /
CWD /uplnad/

-----
Source      = victim4.lame.sysadmin.org
Destination = evil.hacker.org
Start time  = Mon Jan 01 08:11:52 2001
Protocols   = [21 1058] (6)
Stream      = 010101.08.log.396.stream.dest
-----

220 victim4(FTP Server for NO 3.11 (v1.0), (c) by HellSoft.
331 Anonymous login OK, send id as password.
230 User logged in.
250 Current directory: /USLH/11/
550 Cannot change directory (No such file or directory).
550 Cannot change directory (No such file or directory).
550 Cannot change directory (No such file or directory).
550 Cannot change directory (No such file or directory).
550 Cannot change directory (No such file or directory).
```

These log files identified a total of 24 systems that the intruder attempted to log into via anonymous FTP. Of these, the intruder was able to garner anonymous access to seven systems and one networked printer. On one of the systems accessed, the intruder copies several raw data files to a commercial network that provides free shell accounts to users. The most notable compromise was one system accessed via anonymous FTP and used as a repository for pirated versions of popular DVD movies:

© SANS Institute



As for the other five systems and the networked printer, the intruder was able to travel outside of the FTP home directory, but was unable to create any files or directories.

Containment. In this phase, an on-site team is deployed to survey the situation. As stated earlier, my organization utilizes the network administrators of remote sites as our on-site representatives while my office functions more as “central dispatch” (similar to Carnegie-Mellon’s CERT/CC). I directed the network administrator to ensure that all compromised systems were removed from their network(s), each system had full system backups performed on new media and that the backups were available for delivery to law enforcement if and when required.

I then notified one of the law enforcement agents that are co-located with my office of the situation. I provided them with all available information, including a summary of what was known, and what actions were taken. In turn, they provided me the name and telephone number of the agent closest to the compromised site, who would be in charge of law enforcement efforts involved in this case. I passed this information to the site’s network administrator and told her to expect contact from the agent-in-charge.

The next step in the investigation of this incident was to ensure that no other systems were compromised. As the reporting site had over 3500 systems installed, this task was going to take some time; especially since these systems ran varied operating systems and the majority of these did not have standard configurations. To make matters worse, many of the systems were supplied by researchers from various universities and were configured for functionality over security. The network administrator and I decided to initially concentrate on the two subnets on which the compromised systems were connected. This reduced the number of systems significantly, as only 75 to 80 systems were involved. Fortunately, no further signs of compromise were found on these systems.

From this point, the search was expanded to include systems on other subnets that maintained a trust relation with the compromised subnets. For each system on these subnets, the network administrator and her staff verified the MD5 checksums of all services that were being trojaned by the root kit used by the intruder, looked for traffic on unusual ports and ensured that no unauthorized user accounts had been added.

Finally, a review of system firewall logs for the entire facility was conducted, keying on activity on unusual ports and activity outside of normal working hours. Again, no sign of further compromise was noted. The entire scope of the compromises had finally been defined.

While the network administrator and her staff were inspecting their networks, I began to wade through the dozens of JIDS capture logs and system log files that were provided, looking for clues that would identify the source of the compromises. During this process, I discovered that we had captured the login names and passwords of two free shell accounts that the intruder had initiated FTP sessions to – one session to download the Linux root kit, the other to upload raw data from one of the compromised systems.

A series of traceroutes, nslookups and whois executions revealed the IP's, hostnames, mailing addresses and point-of-contact information on both of the shell accounts. The logon name used by the intruder for one of the FTP sessions looked like a URL, so I plugged the login name to a web browser, and found copies of the files that were exported from one of the compromised systems. I immediately passed this information to law enforcement.

Continuing my review of log files, I discovered that the pirated movie files were coming from an IP registered to an evangelical organization in Washington state. I contacted the network administrator for that organization and queried him as to the nature of the system that was identified. The system in question was their email server, which was discovered to have a default installation of Microsoft Exchange loaded. I informed him that he could very well have an anonymous FTP server running on his system without his knowledge and asked if he would investigate this and report his findings to me.

About an hour later, he called me back, and confirmed that they did, in fact, have an anonymous FTP server running. He also informed me that an IP out of Romania had been on his system and had sent the movie files from there. After getting the Romanian address from him, out of professional courtesy, I recommended that he disable the anonymous FTP service, perform a full backup of his system and contact his local FBI office for further investigation.

Going back to my review of log files, I noted the IP address that I was given by the evangelical organization had attempted several telnet sessions to various systems on the compromised networks, and was also noted in captured IRC chat sessions. On a hunch, I went back to the shell account I had visited earlier, and noted that the account was registered to an individual in Romania. Certain that I had discovered the true source of the compromise, I informed law enforcement of my findings.

Eradication. In this phase of incident handling, the cause(s) and symptom(s) of an incident is determined using information gathered during the identification phase. Improvements to the security posture of the network(s), such as tighter firewall policies, installation of router filters and/or re-addressing and renaming compromised systems should be considered. A vulnerability assessment should be performed on recovered systems prior to placing them back into service.

After piecing together the entire scope of the compromise, I contacted the network administrator to discuss issues regarding elimination of the vulnerabilities that were exploited during this incident. Given what her staff had recently gone through, I was more than a little surprised to hear how resistant her executive staff would be to any proposed changes in their security profile.

Her reaction to my first recommendation was pessimistic. I recommended the elimination of anonymous FTP services on all systems on their networks, and that unique logon names and passwords be required for all users. The network administrator stated that they had roughly 7000 users on their networks, and that a large number of them were transient from various universities and commercial organizations. She further stated that the networking staff was not large enough to be able to cope with the additional workload of daily updating user profiles for FTP services on their networks.

My counter-offer on this issue was met with a little more optimism: establish a single server to handle all anonymous FTP requests. In this manner, her site could maintain the functionality requested by her users; yet establish a stronger defense against compromise. I further recommended that, in accordance with established policies dictated by my organization, they limit the number of world-writeable directories within the server.

My next recommendation was all but blatantly shot down. I recommended that they shut down all unnecessary/unused ports at their firewall(s), to include telnet, HTTP, identd, finger and other well-known exploitable ports. Her response to this recommendation was about as negative as the response one would get when making the same recommendation to a network administrator out of the .EDU community.

My remaining recommendations were met with enthusiastic support. These recommendations were: mandating that all systems on their networks, including transient ones, had some form of secure copy and communications services (such as scp and SSH) installed; install filters at their border routers to only allow access to their networks from known authorized domains; and to request a vulnerability assessment of their network via ISS Internet Scanner from my office's network security staff. This last recommendation was made to provide the network administrator clear identification of additional vulnerabilities in her networks and recommended defense strategies to mitigate possible exploitation of the same.

Recovery. When recovering from system compromises, my organization's policy is to have victimized sites reload operating systems from known good media (preferably from original install disks, if time permits), apply all applicable patches provided by the operating system's website, then replace data files from backups taken prior to the date and time of compromise. In the event of suspected/actual password compromise, all passwords on each system affected are to be changed immediately. Once the system is reloaded, full operability testing is performed offline to verify that the system is stable. After completion of this testing and the system has been certified as secure, the system can be placed back onto the network and resume normal operations, while monitoring for backdoors or other suspicious activity that may have escaped earlier detection.

Follow-up. At this phase, the final report regarding this incident was developed and sent to the network administrator of the victimized site for review and concurrence. Once she agreed with the content and wording, the report was promulgated through official channels, along with an executive summary.

The lessons learned discussions from this incident included non-availability of essential security services running on systems, poor security policies and practices, non-standardization of data transfer services and required patches to known vulnerabilities not being installed when made available by vendors. Our lessons learned included the following:

- a. ***Non-availability of Essential Security Services:*** In reviewing the chain of events of this and previous incidents throughout the organization, it is obvious that several remote sites do not have secure communication services, such as SSH, available on all systems. Recommend

developing and implementing changes to current policies regarding standard software installation practices to address this issue.

- b. **Poor Security Policies:** This incident is indicative of a disturbing trend that is becoming apparent over time. We are frequently discovering networks at remote sites within the organization that do not have adequate security policies installed on their firewalls. Recommend development of standardized firewall security policies to be implemented throughout the organization.
- c. **Poor Security Practices:** This incident might have been avoided, had a user not exported a required file to another system via non-secure communications. Recommend refresher training, in the form of an organizational bulletin via email, be sent to all users. Code the email to notify network security staff when each user opens the email.
- d. **Non-standardization of Data Transfer Services:** It has been noted too many times that data transfer services from multiple vendors are being used within the organization. This practice increases the chances that a given vendor either no longer supports the data transfer service or that a critical patch to an identified vulnerability might be missed. Recommend the development and implementation of a standardized list of authorized vendors for data transfer services throughout the organization.
- e. **Lack of critical patches being installed:** It is becoming increasingly noticeable that critical patches that are readily available are not being installed. A system of checks and balances needs to be developed concerning network administrator's responsibilities. The problem appears to be that upper management is usually not technically aware enough to know what questions to ask. Recommend developing a quarterly "hot topics" list, which addresses the agenda which management can use to assist in information security.

Executive Summary

On January 18, 2001, CIRT team was notified by law enforcement that four IP's belonging to the lame.sysadmin.org domain was seen in various IRC channels, in direct opposition of established organizational policies. The CIRT team contacted the network administrator in order to confirm this information. The network administrator discovered that an unknown individual utilizing evil1.hacker.org, evil2.hacker.org, and washington.evangelical.org had compromised these four systems. Actual source of activity appears to originate from Romania.

Actual date of compromise was traced back to December 29, 2000, when an authorized user transmitted a 10MB file from a system within the site to

victim1.lame.sysadmin.org via FTP. SSH was not used because it was not installed on the sending system. Evidence suggests that the sending system was compromised at an unknown earlier date and time, as a sniffer was found on the system.

Because the existence of a sniffer on the sending system was unknown, the intruder was able to garner the unencrypted logon name and password and use them to gain initial access to victim1.lame.sysadmin.org. After initial access, intruder installed a root kit, trojaned various services, added additional logon names and passwords with root access permissions, and installed a copy of BitchX, a popular IRC client. Intruder then utilized the trust relationships between systems to compromise three additional systems the same way. All four systems were used by intruder to access IRC to brag about his exploits.

Intruder also identified seven systems and one network printer that had anonymous FTP services running. One of the systems accessed had eight raw data files exported to a shell account on a commercial ISP, the other was used to store pirated DVD movie files. The five remaining systems and the network printer that were accessed via anonymous FTP did not allow intruder to create files or directories. No further compromises of systems in the lame.sysadmin.org domain were noted.

The network administrator was directed by CIRT team to remove affected systems from service, perform full system backups on new media, and have them ready for delivery to law enforcement. Upon release of affected systems by law enforcement, the network administrator commenced recovery procedures as recommended by CIRT team. When recommended recovery procedures were completed, systems were certified secure and placed back into service.

Recommend increased security awareness training for users, removal of anonymous FTP services on all systems, standardization of data transfer services and tighter firewall restrictions be implemented ASAP.