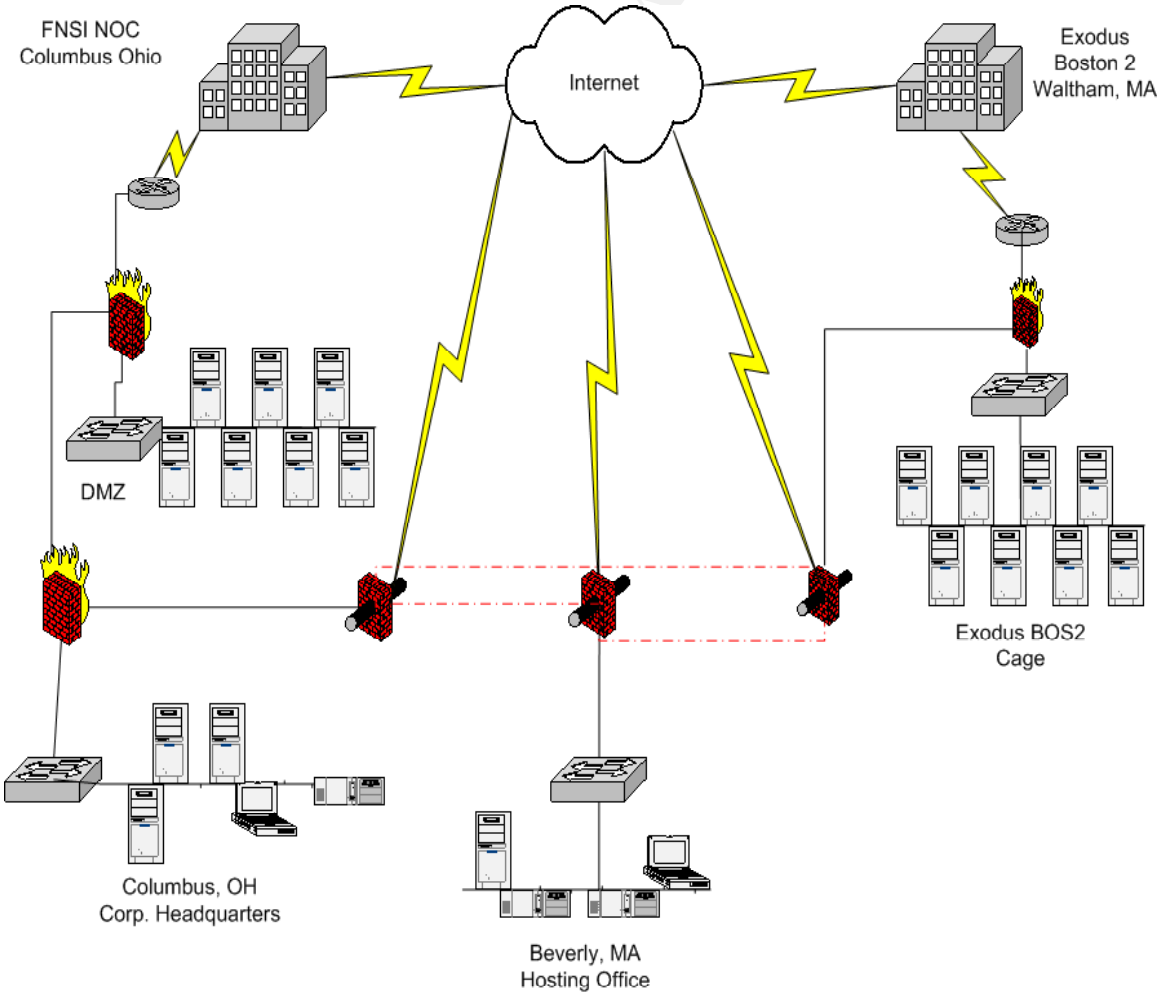
Global Information Assurance Certification Paper

Advanced Incident Handling and Hacker Exploits
Practical Assignment for Thomas Smit,
GCIH v1.5c
Option 1:
"Illustrate an Incident"
Incident "Nimda"

EXECUTIVE SUMMARY

Incident: (n) An occurrence or event that interrupts normal procedure or precipitates a crisis. (dictionary.com)

This paper describes a recent incident that occurred across the entire internet, as well as our company. The company is, at current, split across two parts of the United States. The corporate headquarters, including Human Resources, accounting, sales, IT, and development is located in central Ohio. My team, which is responsible for production operations, is based out of Boston. Production machines are currently located at a facility owned by Exodus, whereas all other company machines are housed in the Ohio facility. The company model is that of a Hosted Service Provider, providing selling solutions to numerous companies, across all aspects of commerce. A small team of three employees resides in the Boston area to administer the operations department. The three facilities, Columbus, Beverly, and Exodus are connected through a VPN tunnel across the net, thus allowing full connectivity to any company resource from any point in the network (see diagram).



I still remember the day clearly. The events of the past week were unbelievable at best. A week prior to the incident, almost to the hour, two airlines had crashed into the World Trade Center in New York City, a third into the pentagon, and an often un-mentioned fourth somewhere outside of Pittsburgh, PA. The country was on high alert after the events of September 11th, and the night before the 18th, newswires and underground sources buzzed with the electricity of an impending incident that would occur on the one week anniversary of the attacks.

I plugged my laptop into the network, and Black Ice went nuts. It was screaming about repeated character exploits against IIS. I chalked it up to a machine that was infected with an old version of Code Red in the Columbus office, and shot an email to the IT administrator in Ohio. Then I saw a Unicode exploit attempt. This was more than Code Red.

Four days later, the last of the remnants of a new worm, named Nimda, were cleaned off of the machines. All told, the total loss of man hours due to this worm was in the thousands. In the following sections of this paper, I will attempt to describe the events of the handling, and also, how the only person in the company who was trained to handle incidents, while being over 600 miles away from where the incident occurred, stayed calm and focused, followed procedures, and limited the damage as much as possible.

Preparation

Preparation: (n) The state of having been made ready beforehand; readiness. (dictionary.com)

Because of the geographical separation of the company, security preparation has been more than difficult. This security professional is employed out of the Boston office. As such, the policies and procedures set into place by me and my team are only applicable to the company assets that are located here. The team is not a member of IT, and therefore does not enjoy the freedom to dictate a corporate wide security policy.

Nevertheless, since I am the one with formal training, many of my colleagues turn to me for security related issues. Unfortunately, no other policies were (are) in place. There are no written procedures for building machines, no application restrictions, and although anti-virus software has been installed, its use is not enforced. However, there is a security policy that governs the assets at the Exodus facility. The following are excerpts from that security policy:

1.1. Virus and Worm Incidents

Although virus and worm incidents are very different, the procedures for handling them are very similar. The principal difference is in the initial isolation of the system and the time criticality. Viruses are not self-replicating, so virus incidents are not as time-critical as worm or hacker incidents. Time is a critical factor when dealing with a worm attack because worms are self-replicating and can spread to hundreds of machines in a matter of minutes. If you are not sure of the type of the attack, then proceed as if the attack was worm related.

1.1.1. Isolate the System

Isolate infected system(s) from the remaining COMPANY production network as soon as possible. If a worm is suspected, then make a decision whether to disconnect COMPANY production from the outside world. Network isolation is one method to stop the spread of a worm, but the isolation can also hinder the clean-up effort since COMPANY production will be disconnected from sites that may have patches. The COMPANY Hosting Operations Manager/Director must authorize the isolation of the COMPANY network from the outside world. **Log all actions.**

1.1.2. Do not reboot

Do not power off or reboot systems that may be infected. Some viruses will destroy disk data if the system is power cycled or rebooted. Similarly, rebooting a system could destroy needed information or evidence.

1.1.3. Notify the appropriate people

Notify the COMPANY Hosting Operations Security Engineer as soon as possible. If unable to reach him/her within 10 minutes, contact the backup person. The COMPANY Hosting Operations Security Engineer will then be responsible for notifying other appropriate personnel.

The COMPANY Hosting Operations Security Engineer will notify the COMPANY Hosting Operations Manager/Director as soon as possible. If unable to reach him within one hour (10 minutes for a worm attack), his backup person will be contacted.

1.1.4. Identify the Problem

Try to identify and isolate the suspected virus or worm-related files and processes. Before removing any files or killing any processes, take a snapshot of the system and save it securely (if possible, without rebooting the machine). A sample list of tasks to make a snapshot of a Windows NT system follows:

1) Dump all system log files to floppy if possible, otherwise, dump to local disk making sure not to infect another machine. This includes System, Application, and Security log files.
2) Capture all process status information in a file. Using the "tlist" command or something similar (srvinfo -s) can do this.

1.1.5. Contain the Virus or Worm

All suspicious processes should now be halted and removed from the system. Make a full image of the system using imaging software and store in a safe place (safe being defined as somewhere that the attack has not affected). The tapes/disks of the image should be carefully labeled so unsuspecting people will not use them in the future. Then remove all suspected infected files or worm code. In the case of a worm attack, it may be

necessary to keep the system(s) isolated from the outside world until all COMPANY production systems have been inoculated and/or the other Internet sites have been cleaned up and inoculated. **Log all actions.**

1.1.6. Inoculate the system(s)

Implement fixes and/or patches to inoculate the system(s) against further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system. If the virus or worm code has been analyzed, then assessing the damage is not very difficult. However, if the offending code has not been analyzed, it may be necessary to restore the system from backup tapes. Once the system is brought back into a safe mode, any patches or fixes should be implemented and tested. If possible, the virus or worm may be used to infect an isolated system that has been inoculated to ensure the system(s) are no longer vulnerable. **Log all actions.**

1.1.7. Return to normal Operating Mode

Prior to bringing the system back into full operation mode, you should notify the appropriate people by following the guidelines in 2.1.2. The users should also be notified that the systems are returning to a fully operational state. Hosting Operations engineers may be required to change users (customers) passwords. Before restoring connectivity to the outside world, verify that all affected parties have successfully eradicated the problem and inoculated their systems. **Log all actions.**

1.1.8. Follow-up Analysis

Perform follow-up analysis. This involves identifying, if possible, the method by which the problem was introduced and any mistakes made in isolating and eradicating it.

Management support for an incident handling capability has been lack-luster at best. Due to budgetary constraints and the "if it doesn't affect me, why should I care" attitude, information security has not been a large concern at our organization. However there is good news, after this recent incident, management's eyes have been opened to the fact that security is a major concern, and they have pledged to look into making things better. That being said, it's safe for the reader to leap to the next conclusion; that there is currently no incident handling team or organization in preparation for an incident occurrence. The most proactive the company has been is to send one employee to SANS' training, and having that employee subscribe to multiple internet news letters dealing with Information Security.

Below is a step by step analysis of total preparation in tune with guidelines proposed by SANS' publication Incident Handling Step by Step:

A. Establish Policy and warning banners (Overall: non-compliant)

Compliant

- Formal security policy in place that governs over production machines.
- Firewalls are monitored by log.
- Upstream provider FNSI has monitoring and security policies in place.

- No IDS installed in the corporate environment.
- No vulnerability scans of corporate network.
- No formal policy regarding corporate assets.
- No regular patch upgrades or software updates preformed on the corporate network.
- No remote employee policy or policy regarding laptops in place.
- No policy regarding outside communication.

Non-Compliant

- No warning banners posted anywhere.

B. Develop management support for an incident handling capability (Overall: Non-compliant)

Compliant

- SANS' trained employee has collected news articles and subscribed to many internet based mailing lists dealing with security.

Non-Compliant

- No one until now, has graphically illustrated an incident
- The company has not collected historical support, thus not calling to light the need for an incident team.

C. Select incident handling team members and organize the team (Overall: Non-compliant)

Compliant

- Only one qualified person in the entire company and they are not located at headquarters.

Non-Compliant

- No incident handling team exists, nor has there been any discussion regarding creating one.
- No Public Affairs Office exists.

D. Define incident handling team organization (Overall: Non-Compliant)

Non-Compliant

- No hierarchical organizational structure for a team when it comes to incident handling.
- No command post has been setup or utilized, no policy exists dictating that a command post can exist.
- Disaster recovery plan does not exist for corporate assets.
- No checklists or build documents exist for corporate assets.

E. Develop an Emergency Communications Plan (Overall: Non-Compliant)

Non-Compliant

- No call list or method if informing people exists
- There is currently no call tree to notify anyone in the company of an incident
- Passwords to switches/firewalls as well as administrative passwords to the network are not shared with anyone outside of IT. If access is not previously granted, it will not be granted in a time of emergency.

F. Conduct training for team members (Overall: Compliant)

Compliant

- Training in the form of SANS' training as well as Cisco/Microsoft training has been given to the sole team member.
- In turn, I have had seminars within the company discussing basic security principals such as password management, very basic security terms, and identification of easy ways that my co-workers can help.

G. Develop interfaces to law enforcement agencies and Computer Incident Response Teams (Overall: Non-Compliant)

Non-Compliant

- No contact has been made with law enforcement or a CIRT.

H. Jump bag (Overall: Compliant)

Compliant

- A jump bag has been prepared in the Boston office containing a spare laptop with both Linux and Windows 2000 on it, a small hub, a tape recorder, a spare cell phone and extra batteries, and also other items. However, no such jump bag is prepared in the corporate office.

If basic preparation is a strong foundation for advanced incident handling, then this company does not have the foundation necessary. There is no set line of communications, training schedule, or company wide guidelines. However, one cannot assume that since he is unprepared, that he cannot successfully handle himself during an incident.

Identification

Identify: (v) to ascertain the origin, nature, or definitive characteristics of. (dictionary.com)

9:00 AM EST

Tensions were high. Everybody was worried about security threats. I plugged my laptop into the network and noticed a high amount of traffic for a Tuesday morning. I checked blackice and noticed "Repeated Character" attempts from multiple machines on the Columbus network. I fired off a quick email to our IT staff in Columbus warning them that a few of their machines were infected with Code Red. Then I saw a Unicode exploit. I quickly opened up IIS logs on my local machine, which had already grown to over a megabyte, and saw this:

```
X.X.X.X - - [18/Sep/2001:10:16:47 -0400] "GET /scripts/root.exe?/c+dir HTTP/1.0" 404 287 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:48 -0400] "GET /MSADC/root.exe?/c+dir HTTP/1.0" 404 285 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:48 -0400] "GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404
295 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:49 -0400] "GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404
295 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:49 -0400] "GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 404 309 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:50 -0400] "GET
/_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 404 326 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:50 -0400] "GET
/_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 404 326 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:50 -0400] "GET
/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/sy
stem32/cmd.exe?/c+dir HTTP/1.0" 404 342 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:51 -0400] "GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 404 308 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:52 -0400] "GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 404 308 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:52 -0400] "GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 404 308 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:56 -0400] "GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 404 308 "-" "-"
X.X.X.X - - [18/Sep/2001:10:16:56 -0400] "GET
/scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 400 292 "-" "-"
```

```
X.X.X.X - - [18/Sep/2001:10:17:00 -0400] "GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 400 292 "-" "-"
X.X.X.X - - [18/Sep/2001:10:17:00 -0400] "GET
/scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 309 "-" "-"
X.X.X.X - - [18/Sep/2001:10:17:01 -0400] "GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 404 309 "-" "-"
```

I hit the books. Obviously it was using a wide range of exploits. First I checked Security Focus' incident mailing list. Questions were flying about; some offering that this was the long awaited "Code Blue[1]." I tried the usual sites, MSNBC, CNN, US Today. Unfortunately, these sites were devoted to the attacks that had occurred the week before. Knowing that the typical news sources were not going to be a help, I started scouring the internet for anything that could help. Slashdot had an article[2] about it, not knowing exactly what it was or where it was coming from though. All of the information that Slashdot had provided (including off-site links) had fallen victim to the "Slashdot Effect[3]", and couldn't be reached.

10:30 AM EST

Our worst fears had come true. After shutting down all the IIS machines in Columbus, the worm was still propagating. We had also found that the machines that were infected were experiencing Dr. Watson errors (seg. fault/core dump) on explorer.exe and iexplore.exe (internet explorer). Around this time, we also received a page. Drive space on one of the machines had filled up, apparently also caused by the worm. By 11:00 AM we had traced two more means of propagation. First, and also the most obvious, was that it was using an email routine similar to Melissa. It was also propagating itself through some other means, which was still unknown. We believed that the third method had something to do with the EML files that were being dropped on the machines, but we still couldn't figure out how or where these files were coming from.

11:24 AM EST

The following email from Olle Segerdahl hit the incident mailing list at Security Focus.

We've all just been hit by a VERY aggressive worm/virus.

Quick analysis indicates that it propagates itself in
a number of different ways:

Through use of IIS UNICODE direcory traversal coupled
with the recent IIS .dll privilege escalation attack.
It uses SMB/CIFS and TFTP to get the worm payload.

Through MAPI mails (probably to all of addressbook).

Other ways of spreading may be possible, but we haven't
yet had the time to properly analyse the worm/virus.

It seems to share "c:\" via SMB/CIFS as "c$" and
the worm/virus also adds the "Guest" user and "Guests"
group to the local "Administrators" group....

---

[1] A re-work of the famous Code Red worm
[2] http://slashdot.org/article.pl?sid=01/09/18/151203
[3] Slashdot Effect: http://ssadler.phy.bnl.gov/adler/SDE/SlashDotEffect.html

Interesting strings in binary:

Concept Virus(CV) V.5, Copyright(C)2001 R.P.China

SYSTEM\CurrentControlSet\Services\lanmanserver\Shares\Security
share c$=c:\
user guest ""
localgroup Administrators guest /add
localgroup Guests guest /add
user guest /active
open
user guest /add
net

More info as we come upon it.....

/olle

This email had given us the information we needed to go forward with containment. By 1:00 PM that afternoon, the worm had been named Nimda and the incidents.org had moved from "peace-time" to a level of "full heightened alert."

Containment

Contain: (v) to halt the spread or development of. (dictionary.com)

Damage assesment was difficult at best. As reports rolled in on the mailing lists, I tried to keep communications open between the Columbus staff and myself. We knew that it affected IIS through multiple, previously discovered exploits. We also knew that it was spreading through network shares.

Trying to use the machines was also difficult. The worm infected explorer and Internet Explorer making it impossible to browse the machine since IE is such an integral part of the OS.

Our network bandwidth utilization was rapidly increasing while the worm was propagating through the building. Like Code Red before it, not only did it scan all machines on an infected machine's subnet, it was also creating a denial of service attack against servers on the network due to the high amount of HTTP port probes. Couple that with the DoS caused by hard drives filling up with EML files, and our network didn't have a chance.

Throughout all of this going on, we still had users executing attachments in email and infecting their own machines. This no doubt added to the bandwidth utilization.

Based on the information above, as well as information obtained from the mailing-list at Security Focus, at approximately 1:10 PM we decided to remove all machines (infected and clean) from the network in Columbus. The threat was considered large enough to warrant the downtime. Unfortunately, that also removes me from the incident handling, because I could no longer remote desktop into the machines. However, the decision was made to allow me to remain as part of the incident handling team, only remotely. My last mandate before the network was shut down was that the infected

machines should not be rebooted. I watched the machines drop off the network one by one, until all that was left was myself and the IT engineer in Columbus.

Because our mail server in Columbus had been hit and the subsequent removal of all machines from the network, the corporate office was without outside contact. The decision was made that I would be the point of contact for outside information, and that a single line of communications over AOL Instant Messenger[4] between me and the IT engineer would be left open.

No backups were made of any of the systems. Due to the nature of the incident, it was decided that a backup of each system would not be necessary. Most of the systems by this time had filled up with replication EML files and since the incident was world wide, we found very little motivation in performing a backup for future use. By the end of the day Tuesday, the worm's spreading had been contained within our network. It had been decided that myself and the IT engineer would not stay throughout the night, because even though the entire company was affected, production systems were still running unaffected and removal instructions had not be found or created by anyone yet. Wednesday would be a long day of trials of recovery.

Eradication

Eradicate: (v) To root out; to destroy utterly; to extirpate; as, to eradicate diseases, or errors. (dictionary.com)

The cause of the incident was tracked down to an unsuspecting user, who had IIS running on his laptop. He had carried Code Red into the company on his laptop, and hadn't patched his system afterwards. That Tuesday morning, he had been infected with the Nimda virus at home, and then carried it into the office. We later found also that the mail server, running Exchange and Outlook Web Access had also been hit from the outside. It's hard to justify punishing an unknowing user for not patching his system, when the IT department is guilty of the same crime.

By Wednesday morning, anti-virus companies had released up to date virus definition files for their products. However, most of the .data files only allowed users to block new infections; there was still no easy way to remove the virus from an already infected machine. Through trial and error, the IT engineer and I came up with the following removal procedure:

- Stop all services possible
- Use a virus scanner that cleans the virus from a remote machine on all volumes
- Do a second scan and you shouldn't get any hits
- Double check the system.ini and wininit.ini for explorer.exe load.exe -dontrunold
- Power off instead of shutdown
- Power up disconnected from the network and log in locally
- Install anti-virus software locally and scan again
- Apply patches
- Reboot connected to the network

[4] AIM: a very popular Instant Messenger client produced by AOL, http://www.aim.com

It was later that day that Jeff Isherwood sent removal instructions[5] to the Incidents mailing list at Security Focus. It was only then did we realize that there was a lot more cleaning that needed to be done. Specifically, Nimda set a lot of registry parameters that we didn't even realize. All told, 50 machines were infected with Nimda in our company. Mostly NT Server and Windows 2000 Server machines, but a handful of user workstations were also hit. The decision was made that instead of following Jeff Isherwood's steps, that IT would begin wiping the machines and reinstalling from scratch. This time however, IT was sure to patch all the machines that they were building.

As machines came back onto the network, I ran Nessus and nmap scans against them, verifying that they were in fact patched with the latest updates and also that any unwanted ports had been closed. It was also decided by IT at this time that ports outbound would start to be blocked at the firewall, most notably TFTP and NetBIOS.

Recovery

Recover: (v). to regain a normal or usual condition. (dictionary.com)

Fortunately, most of the machines that were infected were web servers. It was easy for IT to rebuild these machine from scratch, and just drop the code back onto the machine. Also fortunate was the fact that our main Clearcase[6] machine was not hit, and our vob[7] was not affected by the worm.

User workstations were another matter entirely. Most of the workstations hit were laptops with Windows 2000 Professional on them. In Microsoft's never ending attempt to make things easy for the end user, IIS is installed by default in Professional, Server, and Advanced Server. For the workstations that weren't infected before we pulled them off the network, IT went around to each station and applied the necessary patches. For the machines that were infected, the decision was made to also wipe those machines, rebuilding from scratch.

The mail server, which was the only mail server, was also infected. Early on in the process, IIS was stopped on the machine so that no one could use one of the many exploits that the worm opened up to piggy-back in on. Since the decision had been made to wipe all infected machines, we manually rebuilt another mail server and transferred all mailboxes to it. A quick WINS/DNS change and everyone could once again access their mail. We then rebuilt the original mail server and applied all necessary patches.

Once the web servers were back online, we had our QA department perform a battery of tests against the machines. This was an enormous help, as it told us many things. By validating that the servers were indeed working correctly, QA helped us determine that the firewall, which had been tweaked, was still correctly setup, that the machines were not serving any errant code, and that the servers were reconfigured properly once they were brought online by the IT department.

---

[5] See appendix A.

[6] Rational Clearcase (http://www.rational.com) – Clearcase is a source management tool that is used in development.

[7] Vob – a clearcase database, where all checked in code is stored.

By late Thursday afternoon, the decision was made to slowly start bringing user machines back onto the network. By close of business Friday, all operations at corporate were restored to normal.

45 users downtime for @ 24 hours = 1080 lost man hours
Average salary = 60,000/@30 dollars per hour
Total loss = @32, 400 dollars

Follow Up/Lessons Learned

Hindsight: (n): understanding the nature of an event after it has happened**.** (dictionary.com)

We scheduled a meeting for that Friday afternoon, to discuss the incident and actions taken over the past days. It was stipulated going into the meeting that it was a follow-up meeting, and that the meeting would not be used to place blame or finger point in any direction. The meeting included the CFO, the CEO, the Director of IT, the IT engineer responsible for the machines, and the Director of Hosting and I, which were conferenced in from Beverly. I presented the group with the timeline of identification (almost exactly the same as in this paper), and we discussed what was good and what was bad about the whole situation.

- It was obviously realized that it was standard practice before this incident to not patch machines in Columbus. Although every admin instinctively should 'know' to patch his systems, there is now time set aside and the task is specifically assigned to one person.
- In the past, it has been the practice of the IT group to allow all outbound traffic through our firewalls. This has now changed, restricting outbound traffic as well as inbound traffic. NetBIOS and TFTP are only a few that have now been restricted.
- It was decided that someone in Columbus must become trained in the security arena. Although most everyone in the meeting praised how much was able to be done remotely, it was still seen as a burden to have to rely on someone who didn't have physical access to the machines.
- Backup practices were discussed and it is now standard practice that all machines are backed up nightly.
- Overall company preparation was discussed, and while the company hasn't promised to fund any further training or security exercises, the need for a company wide security policy was felt by the CFO and CEO, and they have asked that I begin to prepare one as soon as possible.
- Questions were asked as to why the company assets at the Exodus data center were not affected by the worm, and also why someone in Boston was the first person to identify the issue that was occurring in Columbus. Since these questions pointed to blame more than anything else, the discussion was curbed with the understanding that the worm used exploits that were over a year old, and that the machines in Boston were patched against these exploits while the machines in Columbus were not.
- Procurement of a Columbus based IDS and vulnerability scanner was discussed.

However, again due to budgetary constraints, the idea was dismissed. We are currently looking at implementing a Snort IDS and regularly scheduled Nessus vulnerability scans.

- We discussed the possibility of setting up a remote syslog for NT box, and routing logging of all machines to this repository. This item alone would not have helped us with this incident, but we decided that forward thinking with regards to security was better than losing another thousand man hours.
- A disaster recovery plan has been created for business critical machines, including the mail server, the clearcase servers, and the production systems hosted at Exodus. This includes quarterly "recovery tests" in which staff will "act out" an incident and the following reactions and recovery to said incident.
- Outlook Web Access and the main Exchange server have been broken into two. Now if the machine housing the Outlook Web Access becomes compromised, the Exchange server will still be operational.
- I have moved under the Director of IT's jurisdiction. Too many issues arose during the handling that would not have been a problem if I were a member of the team that was responsible for those machines. Administrators are often protective of their network and this was one case where that over protectiveness was a hindrance rather a help.
- Build documents have been created for user workstations, specifying that IIS should be removed from all user workstations. Also, user training has occurred and all users in the company are now aware of how to update their machines by using Windows Update[8]. This has yet to been proven a "good idea."
- Users are no longer allowed to use Outlook Express to grab their external email from within the company's networks. This has been done by blocking port 110 outbound at the firewall for all users.

Conclusion

As a child growing up, I was a member of the Boy Scouts. I'm sure many share fond memories with me when I say this: "Be Prepared." These two words, the Scout Motto, have followed me from my childhood into my career and my handling of this incident. If ever there was a motto for incident handlers world wide, it would be "Be Prepared."

Following this incident, I've realized how unprepared I was as an individual and how unprepared my company was. Not only that, worms such as Nimda and Code Red have proven how unprepared the internet population is, including most major ISPs. In no other industry can someone use an exploit that is over a year old and bring that industry to its knees.

However, a lot of good has come of the recent cyber attacks. ISPs such as Road Runner and @Home have taken a large piece of responsibility, some even blocking port 80 on their network, or shutting down infected users' access.

The time has come to no longer tolerate ignorance when it comes to computer

[8] www.windowsupdate.com (Microsoft)

security. Education is the first step, preparation, the second.

Resources

http://www.securityfocus.com/news/253 - "Nimda Worm Hits Net"
http://abcnews.go.com/sections/scitech/DailyNews/nimdaworm010918_wire.html - "Internet Attacked by New Worm"
http://slashdot.org/article.pl?sid=01/09/18/151203 - "New (More) Annoying Microsoft Worm Hits Net"
http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html – Symantec Security Response.
http://www.trusecure.com/html/tspub/hypeorhot/rxalerts/tsa01024_cid177.shtml - TruSecure.

Appendix A

Removal:

Step 1) Cleaning up your registry keys, since it reg-hacks to hide itself, make sure you do this one FIRST.

The worm adjusts the properties of Windows Explorer, it accesses the following keys and adjusts them to affect system ability to show hidden files (mostly Win2K &ME), infected files will not be seen by the Explorer.

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]

Registry key values are created/changed to hide files:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden

The worm tries to create this key:
[HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces]

The worm also deletes all subkeys from this key to disable sharing security:
[HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Services\lanmanserver\Shares\Security]
[HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Services\lanmanserver\Share\Security]

Step 2) Remove "loader" settings to disable autorun on boot.
It modifies the SYSTEM.INI file in order to activate itself on every startup,
remove this line from SYSTEM.INI file and reboot the computer:

```
[boot]
shell=explorer.exe load.exe -dontrunold
```

Step 3) Remove the payload files. When executed, virus copies itself into several the Windows system directories. These files have system and hidden attributes set. It will overwrite any original files if they already exist.

Delete all the "worm dropping" files (original files which have been overwritten should be restored from backup)

MMC.EXE (in Windows directory, MS Mgmt Console - looks like worm can overwrite this file)
LOAD.EXE (in Windows' system directory)
RICHED20.DLL (in Windows' system directory)
ADMIN.DLL (in root folder of all local hard drives C:\, D:\, and E:\ etc...)
WININIT.INI (in Windows directory)

Also scan all local hard drives for any hidden RICHED20.DLL files and delete them.
Replace a clean RICHED20.DLL to system32 folder.

The worm also copies itself to the Temporary directory with random MEP*.TMP and MA*.TMP.EXE names, for example:

mep01A2.TMP
p1A0.TMP.exe
pE002.TMP.exe
pE003.TMP.exe
pE004.TMP
README.EXE
root.exe

To be safe, delete all files with .TMP extension from your local temporary directories:

\Temp\
\Windows\Temp\
\documents and settings\username\local settings\temp

(from f-secure)
The worm enumerates shared network resources and recursively scan files on remote systems. If the worm finds an .EXE file on a remote system, it reads the file, deletes it and then writes a new file where the worm body is placed first and the original EXE file is present as a resource. Later when this affected file will be run, the worm will extract the EXE file resource and run it. The worm checks the file name for 'WinZip32.exe' and doesn't affect this file if it is found.

The worm accesses [SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths] key reads subkeys from there and affects all files listed in the subkeys the same way it does affect remote EXE files (see above). The worm doesn't only infect WinZip32.exe file. Also the worm reads user's personal folders from [Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders] key and infects files in these folders as well.

Step 4) REBOOT

Step 5) Removing infected message files.
Delete all .EML files generated by the virus.
It creates .EML (mostly) or .NWS (occasionally) files with randomly selected names.

Step 6) Fixing Winzip
Completely REMOVE WINZIP from the system and Re-install after reboot.

Step 6) Cleaning the HTML Files.
Check all *.HTML, *.ASP, and *.HTM as well as files that have 'DEFAULT', 'INDEX', 'MAIN' and 'README' words in their filenames for the small JavaScript code referring to README.EML file and remove it or restore the affected files from a backup. This JavaScript code is located in the very end of affected files.

Search for file types above containing readme.eml, but pay close attention to the following default file names:

index.html
index.htm
index.asp
readme.html
readme.htm
readme.asp
main.html
main.htm
main.asp
default.html
default.htm
default.asp

Step 7) Removing Admin rights from GUEST.
Check if the GUEST account is in the ADMINITRATORS group; if yes, remove it from the group

Step 8) Fixing Shares.
check the sharing of the local disks & remove unnecessary shares, the virus enables admin shares on infected systems. To be safe, remove all shares from all local hard drives and renew these shares with correct access rights if needed. This needs to be

done because the worm affects share security. Check especially the \\localhost\c$ share rights.

Step 9) FIX THAT HOLE.

Apply the MS patches.

Internet Explorer 5.01:
http://www.microsoft.com/windows/ie/download/critical/q295106/default.asp

Internet Explorer 5.5:
http://www.microsoft.com/windows/ie/download/critical/q299618/default.asp

Microsoft IIS 4.0:
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

Microsoft IIS 5.0:
http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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 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 Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 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
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 New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event