GIAC
CERTIFICATIONS

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 permited 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

Exploit in Action, A W32/Nimda Outbreak

Gregory Edwards
Option 1 – Exploit in Action, Version 2.1

This paper is to fulfill the research paper for the SANS GCIH Class. The topic is:
Exploit in Action

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Part 1 – The Exploit

Name of Exploit/Attack, including CVEs

The incident described below was a W32/Nimda outbreak on 30 January 2002. W32/Nimda is a very dangerous email and network aware virus/worm that uses a number of different vulnerabilities to assist in its spread through Microsoft Windows based computers. There are a number of CVEs for the vulnerabilities that must be patched to protect against the W32/Nimda virus. Primary sites for information on these CVEs include the Mitre CVE page (1.1), the Security Focus website (1.2) and various Microsoft TechNet articles (1.3). Some of the CVEs (more fully described below) include: CVE-2001-0154, CVE-2000-0630, CVE-2000- 0631, CVE-2000-0884, CVE-2001-0338, CVE-2001-0339, CAN-2001-0246, and CAN-2001-0332.

Operating Systems Under Attack

The computer systems under attack were on TCP/IP version 4 networks that had a number of computers on them. The computers under attack were a combination of Microsoft NT4.0 SP4, NT4.0 SP6 and Win2000 SP1. The Win2000 SP1 were new systems that had just been delivered and had all recommended Microsoft Security Patches installed before other software was loaded or before the computers were deployed. There were also a number of Unix boxes but they were not at risk from this event. There were about 10k computers at this site. The corporation as a whole has over 100k computers in its Intranet.

Protocols/Services/Applications

W32/Nimda uses a variety of means to spread on Microsoft Windows 95, 98, ME, NT and 2000.

W32/Nimda tries to infect Microsoft Windows computers that use Internet Explorer 4.0 or 5.x via “Incorrect MIME Header can Cause IE to Execute E-Mail Attachment” vulnerability MS01-020 and is also known as CVE-2001-0154.

W32/Nimda tries to infect other Windows computer across a network via attacks on shares.

Yet another way W32/Nimda tries to spread itself to other computers is to utilize a backdoor installed by W32/CodeRed.c as a means of spreading itself.

W32/Nimda uses Microsoft Internet Information Servers to spread itself. To protect IIS servers there are several patches for several vulnerabilities. In the first

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MS00-044 MS Cumulative Patch for IIS has two CVEs, CVE-2000-0630 for IIS 4.0 and 5.0 and CVE-2000-0631 for IIS 3.0, 4.0 and 5.0. The first vulnerability allows an attacker to obtain parts of the source code by addition of a +.htr to the URL. The second is a script from IIS 3.0 that a Denial of Service attacks on an IIS server.

Another is MS00-078 Microsoft Web Folder Transversal vulnerability. It has CVE CVE-2000-0884 which allows attackers to read files outside the web root and possibly execute commands via UNICODE character encoding.

And IE5.5 SP1 systems also need to apply MS01-027. There are four CVEs listed: CVE-2001-0338 in which IE 5.5 and prior can be tricked into trusting untrustworthy web sites, CVE-2001-0339 which allows the attacker to force the display of a URL on the address bar that is different than the URL of the site being visited, CAN-2001-0246 which allows the attacker to read some client files via a variant of the "Frame Domain Verification" vulnerability, and CAN-2001-0332 which is also a variant on the "Frame Domain Verification" vulnerability.

Brief Description of exploit to show how it works

The W32/Nimda virus is a modern "merged vector" virus that uses a number of vulnerabilities in its attempt to spread and infect additional computers.
W32/Nimda propagates via several different methods:

- As an email-aware virus (like W97M/Melissa)
- As a network-shares aware virus (like W32/FunLove)
- As an upload to Microsoft IIS web servers that has not been patched against the Unicode Directory Traversal vulnerability.
- By finding un-patched holes created by a prior Code Red II infection.
- By putting infected .eml files on servers (IE5.x will execute these if not patched)

Names of different variants of exploits

The W32/Nimda virus can be found with the following names and variants (note, a ' ' is before the @ sign to avoid the document editor thinking that the name is an URL) from different vendors:

AVP/Kaspersky Lab 1.4 http://www.viruslist.com/eng/viruslist.html?id=4261
I-Worm.Nimda
I-Worm.Nimda.E

F-Secure 1.5 http://www.fsecure.com/v-descs/nimda.shtml
Nimda
Nimda.c

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Nimda.d
Nimda.e

Norton AntiVirus 1.6
http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html
W32.Nimda.A@mm
W32.Nimda.C@mm
W32.Nimda.D@mm
W32.Nimda.E@mm
W32/Minda @MM

AVX Command Central 1.7 **http://support.centralcommand.com/cgi-bin/command.cfg/php/enduser/std_adp.php?p_refno=010918-000005**
Win32.Nimda.A@mm

Computer Associates 1.8
http://www3.ca.com/Solutions/Collateral.asp?ID=1132&PID=128
Win32.Nimda.E (CA)

Sophos 1.9 http://www.sophos.com/virusinfo/analyses/w32nimdaa.html
Code Rainbow
Nimbda
W32/Nimda-A @mm (primary version)
W32/Nimda-B @mm (minor variant)
W32/Nimda-C @mm (minor variant)

McAfee 1.10 http://vil.mcafee.com/dispVirus.asp?virus_k=99209&
W32/Nimda.a @MM
W32/Nimda.b @MM (PE packer packed, files are PUTA!!.SCR and PUTA!!.EML) (NAI lists no .c version)
W32/Nimda.d @MM (filenames changed: README.EXE→SAMPLE.EXE, MMC.EXE→CSRSS.EXE & ADMIN.DLL→ HTTPODBC.DLL)
W32/Nimda.e @MM (very similar to D version)
W32/Nimda.eml (files are executed if read (web page or email) by un-patched Internet Explorer)
W32/Nimda.f @MM (very similar to D version)
W32/Nimda.g @MM (very similar to D version)
W32/Nimda.gen @MM
W32/Nimda.htm
W32/Nimda @MM

References

References are found in the Bibliography at the end of this document.

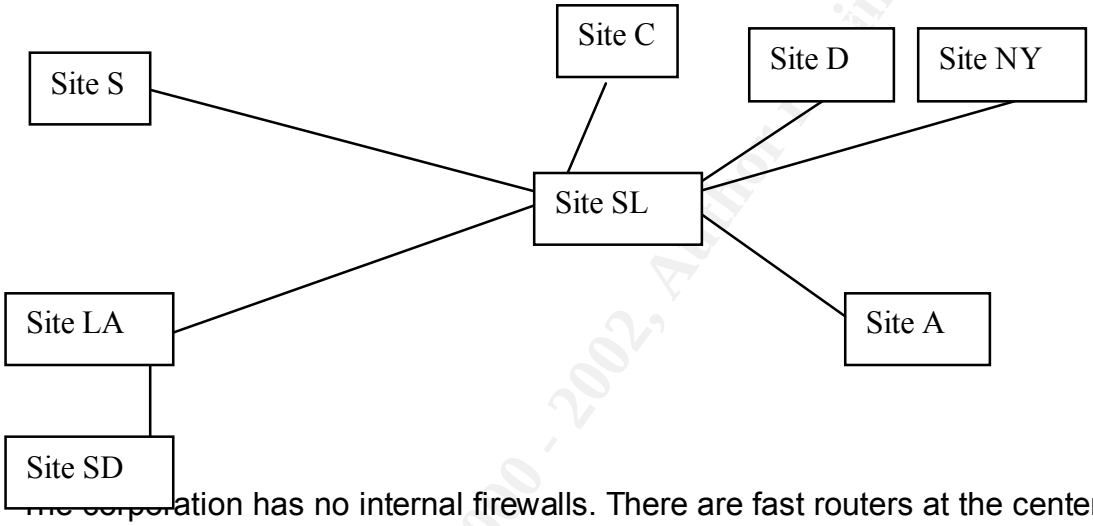
© SANS Institute 2000 - 2002, Author retains full rights.

Part II – The Attack

Description and diagram of network

The site that was attacked was one of a number of sites at the corporation. This site, site D, has about 10,000 computers. The corporation has about 100,000 computers as a whole. Site D is connected to the corporate intranet via a single connection at site SL. As can be seen, almost all corporate intranet traffic passes through Site SL. Internet firewalls for the Corporations are found at Sites S and A.

Major Corporate Sites and Network Connections



The corporation has no internal firewalls. There are fast routers at the center of all major sites. Subnets are served either by hubs or switches. At some sites the switches are remotely configurable; at other sites they are dumb. Most sites use DHCP for desktop IP addresses. Email servers are at each of the sites shown above. With the exception of the single link between Site SL and Site D none of the above network matters in understanding this event.

Site D has about 10,000 computers on a network. The only point of connection to the rest of the corporate network is through Site SL. If that link is lost Site D is disconnected from the rest of the corporate network. There are a number of subnets at site D, some for workstations, some for servers, and some mixed. The subnet computers are also a mixture of Microsoft Windows (various), Unix, and a few Macintosh computers. For this event only the Microsoft Windows computers were involved.

As with many sites in the corporation, the network maps for Site D were not available for the AntiVirus Incident Team (AVIT) during the event and the network operations center was unable to provide a physical address for a given IP address and was not able disconnect a (known infected) IP address from Site D at the local subnet switch.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

As shown below the infections were limited to (IP numbers changed from real to 10.xxx for this paper) subnets 10.22.193.xxx and 10.22.194.xxx. It was later found that on these two subnets were a mixture of desktop and server computers running Microsoft Windows 4.0 SP4, SP6a, and Windows 2000 SP1. No Unix or Macintosh computers were involved in this incident. The Windows 2000 systems were new installs in the past two weeks with all patches applied before connection to the corporate network and before user software was installed. This was later found to be one of the problems as some users installed Microsoft *Front Page* which in turn reinstalled IIS. Since IIS had been removed for security reasons, no IIS patches were, or could have been installed.

Protocol descriptions

W32/Nimda is a modern "merged" virus/worm with a number of means of propagation, including:

- Infected Email read by Internet Explorer 4.0 or 5.x
- Infected Web pages read by IE 4.0 or 5.x, most commonly from IIS
- Spread by Shares like W32/FunLove
- Use of existing Code Red II backdoors
- IIS Uploads
- IIS Downloads to IE

During this attack NO W32/Nimda infected emails were seen. Share spreads were suspected but not observed. No Code Red II backdoors were used (Code Red problems had been removed from the Site D network earlier). Later analysis of this incident showed that the infection vectors were limited to IIS → IE and IE → IIS, or in other words, port 80 http uploads and downloads.

Web http protocols consist of text transfer (the URL) from the IE browser to the IIS web server. The IIS web server would, if given a simple request, send the contents that make up the requested URL webpage back to the IE Browser. This can consist of text, .jpg and .gif images, and more complicated data structures. The material returned may include Java, JavaScript, or other code to execute on the IE browser. In more complicated requests the IIS server may have to interact with databases or other servers to gather and preprocess the information requested in the URL.

How exploits works

There are two exploits that occurred in this incident to allow W32/Nimda to move to new computers:

- IIS → IE
- IE → IIS

The other vectors that W32/Nimda uses to spread were not found in this event.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

IIS → IE
In the first case an infected IIS server can attack an IE browser via an infected email or an infected web page through the "Incorrect MIME Header can Cause IE to Execute E-Mail Attachment" vulnerability MS01-020. It is also known as CVE-2001-0154. When the IE browser visits the infected page or tries to read an infected email, the attack program is executed without informing the user. The exploit comes from the showHelp() function which bypasses default IE security and opens .chm files, even if the file is on a remote host. The "shortcut" command allows the .chm file to execute an arbitrary file, thus allowing a method for infection. See SecurityTeam's article IE5 allows executing arbitrary programs via .chm files 2.1.

IE → IIS
In the second case an infected machine can attack an IIS server by being browsed to the IIS server from an infected IE browser via the Unicode exploit or by using a backdoor created by Code Red II. In this incident all the Code Red II holes had been patched before the event occurred.

The Unicode exploit is based on replacing Unicode characters with certain not-allowed characters. For example sending the following http request to an un-patched IIS web server:
http://xxx.xxx.xxx.xxx/scripts/..%c0%af../winnt/system32/cmd.exe?c+dir+\:\
will result in the directory of d:\ being displayed on the user's browser. To run something else replace the material after the '?c'. See Guofei Jiang's paper (2.2) for more examples. It is that simple. And it works on Microsoft Windows NT 4.0 with IIS 4.x and Microsoft Windows 2000 with IIS 5.x.

Description and diagram of attack

This was a real incident. Much of what we though was happening during the incident was later shown to be inaccurate, but it was useful in finding, containing, and eliminating the infections. This is covered in detail in Part 3 below.

What was later determined to have happened:

1) A user was infected at home from the Internet. We never found out if it was from email viewed with Microsoft Internet Explorer or from an infected web site viewed with Microsoft Internet Explorer.

2) The antivirus signature files on the user's system were months out of date. Almost any antivirus signature file dated after the middle of September 2001 would have provided protection (note, the corporation provides the same antivirus engine used as the corporation to all employees for use at home at no charge).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3) The user connected to the Site D intranet via a VPN connection. In other words, the computer at home became part of and was “on” the Site D network.

4) Most of the computers at Site D had up-to-date antivirus engines and signature files, but a few had become “lost” over time and had out-of-date antivirus systems.

5) There had been extensive upgrades to computers at Site D. The facility had been switching from one remote update (software distribution) system (SMS) to a newer update system. Computers with the new update system had the newest antivirus system on them and were updated as needed. These systems also had their antivirus system tuned to report all infections and attempts at infections to a central corporate antivirus reporting system. This system is described below.

In addition, many of the older computers at Site D were in the process of being replaced by new Windows 2000 based computers. These new machines had Service Pack 1 and all Microsoft Security Patches installed. In order to provide additional security, IIS was removed from all desktop systems as desktops did not need to be web servers. All of this was done before the computers were deployed to the users. Once the computers were deployed user software was installed. Some users had Microsoft Front Page installed, which in turn re-installed IIS. Since IIS had been carefully uninstalled before the patches were applied, the newly re-installed IIS had no security patches.

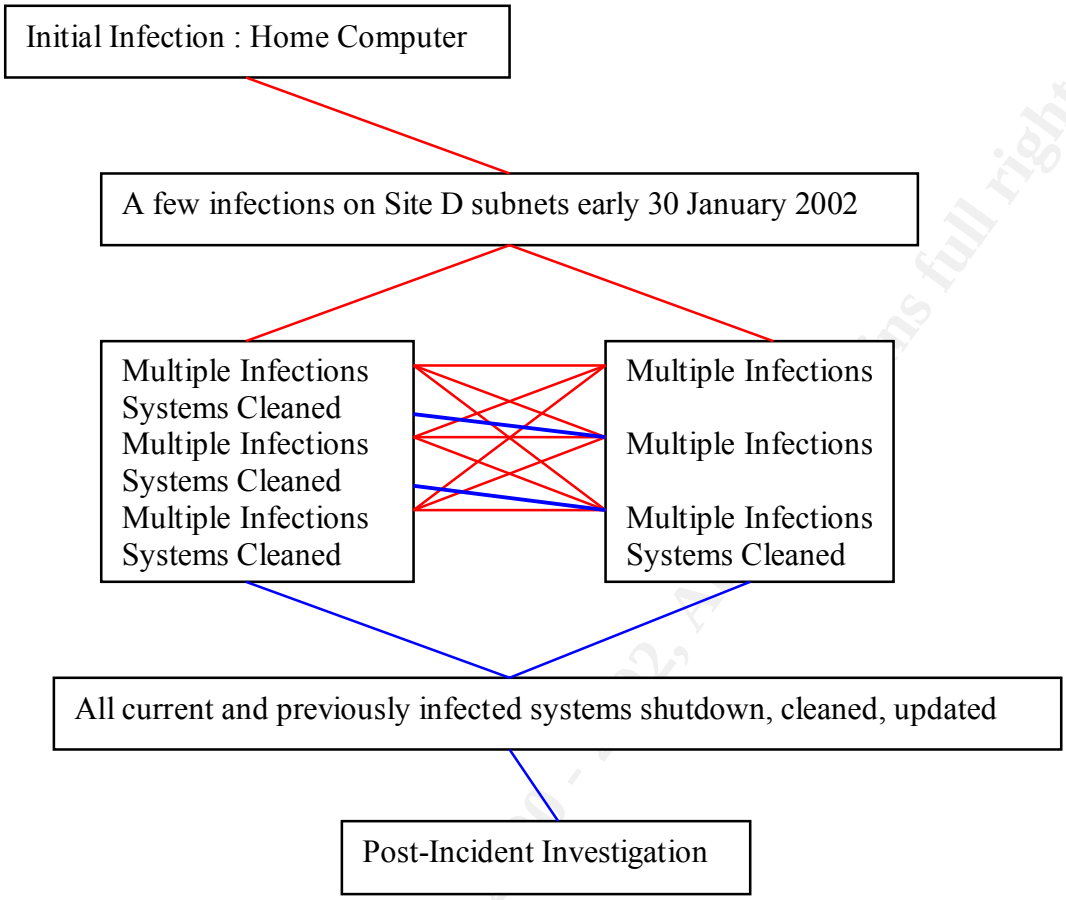
6) The home computer that was infected with W32/Nimda proceeded to attempt to infect computers at the Site D network. For several days it was un-successful at this. Finally on 30 January 2002 it managed to infect several other computers on two Site D subnets. These machines tried to infect other computers at Site D. Most of the other computers had up-to-date antivirus systems and patches and did not get infected but did report the attempts to the central antivirus system.

7) Local desktop support was activated to find the infected computers. Most computers could be found, however several could not. These missing machines led to additional machines being infected. Some machines that were cleaned became re-infected, because it was not realized at that time that Microsoft Security Patches needed to be installed again for systems that had Front Page installed.

Looking at the infection trail after the event appears to be a somewhat crazy ping-pong game in which multiple copies of W32/Nimda virus were being bounced from paddle (computer) to paddle (computer) with the desktop support team running about trying to safe the infected machines (remove the paddles or put glue on them) but were sometimes unable to physically find the systems and sometimes did not fix the infected machines correctly as they did not know that they also needed to reinstall the Microsoft Security patches.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The Incident Events Timeline



A new kind of analysis chart, the Tracking IP chart (discussed in Part 3) finally showed what was going on (ping-pong) and how to fix the problem (shut down all the current and previously infected machines, take them off the net, and fix/patch them all before allowing them back).

Tracking IP Chart

10:30pm	10pm	9:30pm	9pm
10.22.193.2	10.22.193.77	10.22.193.15	10.22.193.2

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

10.22.193.77	10.22.193.15	10.22.193.2	10.22.193.15
10.22.193.15	10.22.193.2	10.22.193.77	10.22.193.71
10.22.193.192	10.22.193.37	10.22.193.71	10.22.193.192
10.22.193.37	10.22.193.192	10.22.193.192	10.22.193.37
			10.22.193.85
			10.22.193.77

During this whole event the corporate IDS team was looking for W32/Nimda signatures transmissions between Site D and Site SL and the corporate AV analyst had an automatic audio alarm set to alert him if there were any email W32/Nimda infections. No cases of either were found, so Site D was never removed from the corporate intranet.

Signatures of the attack

Antivirus detection signatures are covered in detail in Part III below.

Web server logs will see the following patterns after W32/Nimda attempts to enter on Port 80 (source 2.3 http://www.cert.org/body/advisories/CA200126_FA200126.html)

```
GET /scripts/root.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET
/msadc/..%5c../..%5c../..%5c/..\xc1\x1c../..\xc1\x1c../..\xc1\x1c../win
nt/system32/cmd.exe?/c+dir
GET /scripts/..\xc1\x1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc0/../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc0\xaf../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc1\x9c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir
```

Snort signatures for detecting W32/Nimda are (from Snort.org, 2.4 http://www.snort.org/article.html?id=31)

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 \
(msg:"WEB-IIS multiple decode attempt"; \
flags:A+; uricontent:"%5c"; uricontent:".."; \
reference:cve,CAN-2001-0333; \
classtype:attempted-user; sid:970; rev:2;)
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 \
(msg:"WEB-IIS msdac access"; \
flags:A+; uricontent:"/msdac/"; nocase; \
classtype:bad-unknown; sid:1285; rev:1;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 \
(msg:"WEB-IIS _mem_bin access"; \
flags:A+; uricontent:"/_mem_bin/"; nocase; \
classtype:bad-unknown; sid:1286; rev:1;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 \
(msg:"WEB-IIS scripts access"; \
flags:A+; uricontent:"/scripts/"; nocase; \
classtype:bad-unknown; sid:1287; rev:1;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 \
(msg:"WEB-IIS cmd.exe access"; \
flags: A+; content:"cmd.exe"; nocase; \
classtype:attempted-user; sid:1002; rev:1;)

alert udp any any -> any 69 \
(msg:"TFTP GET Admin.dll"; \
content: "|41 64 6D 69 6E 2E 64 6C 6C 00 6F 63 74 65 74|"; \
classtype:successful-admin; sid:1289; rev:1; \
reference:url,www.cert.org/advisories/CA-2001-26.html;)

alert tcp $EXTERNAL_NET 80 -> $HOME_NET any \
(msg:"WEB-MISC readme.eml autoload attempt"; \
flags:A+; content:"window.open(\"readme.eml\""; nocase; \
classtype:attempted-user; sid:1290; rev:2; \
reference:url,www.cert.org/advisories/CA-2001-26.html;)

alert tcp $EXTERNAL_NET 80 -> $HOME_NET any \
(msg:"WEB-MISC readme.eml attempt"; \
flags:A+; uricontent:"readme.eml"; nocase; \
classtype:attempted-user; sid:1284; rev:3; \
reference:url,www.cert.org/advisories/CA-2001-26.html;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 \
(msg:"WEB-FRONTPAGE /_vti_bin/ access";flags: A+; \
uricontent:"/_vti_bin/"; nocase; classtype:bad-unknown; \
sid:1288; rev:1;)
```

How to protect against W32/Nimda

The basic protection against W32/Nimda and similar viruses is to use a good antivirus engine and keep it up to date AND install security patches as recommended by the vendor of the operating system.

All the antivirus vendors update files after mid-September 2001 provide protection against W32/Nimda, for example (from AV vendor's websites-URLs above). Examples include:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Sophos since September 2001
Symantec since 18 September 2001
F-Secure (formerly Datafellows) 18 September 2001

The patches required for protecting Microsoft Windows systems (Macintosh and Unix computers are not at risk) include:

Microsoft Windows TFTP Exploit
Protection is provided by blocking port 69 which is used by TFTP (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/isa/deploy/isanimda.asp)

Microsoft NetBios Shares Exploit
Protection is provided by blocking all NetBios traffic (ports 137-139)
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/isa/deploy/isanimda.asp

Microsoft Internext Explorer 5.01, 5.5 and 6.0 (not 5.01 SP2 or 5.5 SP2)
MS01-020 Incorrect MIME Header can Cause IE to Execute E-Mail Attachment vulnerability
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

Or install MS01-027 (which includes MS01-020)
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-027.asp

Microsoft Internet Information Server (IIS)

Code Red II Backdoor Vulnerability can be eliminated by applying/installing/running any one of the following:

MS01-033 Unchecked Buffer in Index Server ISAPI Extension
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

Or

MS00-044 MS Cumulative Patch for IIS (4.0 and 5.0)
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp

Or

Windows NT Security Roll-up Package 26 July 2001
http://www.microsoft.com/ntserver/nts/downloads/critical/q299444/default.asp?Fi

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

nishURL=%2Fdownloads%2Frelease%2Easp%3FReleaseID%3D31240%26redirect%3Dno

Or

IIS Lockdown Tool (default mode)
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp

Or

URLScan tool (default ruleset)
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/urlscan.asp

Or

The **"Web Server Folder Transversal"** vulnerability can be fixed by applying any of the following:
MS00-057 "File Permission Canonicalization" in IIS 4.0 and 5.0
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-057.asp

Or

MS00-078 "Web Server Folder Transversal" in IIS 4.0 and 5.0
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-078.asp

Or

MS00-078 "Web Server File Request Parsing" IIS4.0 and 5.0
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-086.asp

Or

MS01-026 Cumlative Patch for IIS 14 May 2001 for IIS 4.0 and 5.0
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-026.asp

Or

MS01-044 Cumulative Patch for IIS 15 August 2001 for IIS 4.0 and 5.0
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Or

Windows 2000 SP2 16 May 2001
http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/default.asp

Or

Windows NT 4.0 (with SP6a applied) Security Update 26 July 2001
http://www.microsoft.com/ntserver/nts/downloads/critical/q299444/default.asp?FinishURL=%2Fdownloads%2Frelease%2Easp%3FReleaseID%3D31240%26redirect%3Dno

Or

IIS Lockdown Tool v2.1
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp

Or

URLScan Security Tool
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/urlscan.asp

IIS systems also need MS01-020 (above) to protect against spreading W32/Nimda once infected by email.

File Shares on all Microsoft Windows systems need special attention to avoid W32/Nimda infections. High quality Administrator accounts passwords should be employed, and all un-needed shares should be removed. The Microsoft Personal Security Advisor (for WinNT4.0 and W2K) could assist, but this has been replace by the Microsoft Baseline Security Analyzer in April 2002
http://www.microsoft.com/technet/security/tools/Tools/mbsahome.asp

There a few things that Microsoft could do to improve security. First note that sometimes installing a later Microsoft patch uninstalls an earlier one. This may leave the computer vulnerable to a new W32/Nimda attack or another problem. Second Microsoft has many security patches and tools. Writing secure code in the first place, having a uniform easy path for patches (and no need to reinstall a patch just because a later patch uninstalled the first patch), and providing update tables showing which patches are superceded would help. Having accurate patch checking tools would also help (see recent articles in Bugtraq, NTBugtraq

© SANS Institute 2000 - 2002, Author retains full rights.

and elsewhere for more on this problem). The third thing that Microsoft could do is to not have surprise installs of problems like IIS when the user thinks that only Front Page is being installed.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Part III Incident Handling Process

The Incident Handling Process - Preparation

Current AntiVirus System

The current antivirus system is based on the following axioms:

Viruses are a threat to the Company.
Multiple layers of antivirus protection are critical for protection.
Analysis is cheaper than desktop support.
Use differential support; only help those who need it.
Infected users are >victims<, not guilty crooks who need to be arrested, which means there is no need to involve lawyers, police, etc..
Good reports (good analysis) are critical to keeping management support.

Below I will show how they do this, and then describe the incident in question.

Management Support

Management support was obtained after the w97M/Melissa event several years ago. Management is carefully informed of AVIT activities by the reports described below. The AVIT team and its members have won a number of internal corporate awards for their activities.

The Antivirus Team

The antivirus team is a virtual team consisting of three groups. The core team includes a project lead, an analyst, and a research/test sub-team. They solve virus problems daily. The extended team members handle virus incidents at their sites, work with the test sub-team on testing and distributing new updates, and other tasks as needed. Lastly, the antivirus team uses subject matter experts when needed. These are often system administrators, Microsoft Exchange email administrators, firewall administrators and network engineers. Most members of the antivirus team work only part time on virus problems. The company's antivirus team is distributed throughout dozens of sites around the US. The core team is based in four different locations, separated by 400 to 2500 miles. Many members have never met each other!

The team project lead handles the management interface, budget, and is also an incident handler. The analyst analyzes all reported virus infections at the company every day, and determines who needs assistance and who is the local antivirus support person. In addition, he prepares the weekly and yearly reviews and is the backup incident handler. The research/test team tests new engines and the weekly Virus Information Files (VIF) update files from the current Desktop Antivirus System vendor (this has been found to be very important) to make sure that they do not crash the systems. This team also tests new viruses against the current antivirus engine. The core team meets twice a week by telecom/Microsoft NetMeeting. Core team members also interact with the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

desktop deployment teams, desktop support teams, vulnerability analysis team, email server teams, the Viruswall Antivirus System/PMDF team, and so forth. The extended team, and people from other teams are invited to weekly meetings to discuss current and future virus problems. The current Desktop Antivirus System often has a support person attend these telecoms.

In 2001, the AntiVirus Incident Team (AVIT) handled major 13 incidents. An incident is defined as an event where they had to activate the full AVIT team to handle the viruses and prevent their spread. They won 12 of these incidents, meaning that the company did not have to shutdown email or other network services for any sites. In one, the W32/Goner virus outbreak, AVIT didn't fully win. In that case it was necessary to shut down part of the company's email system for part of one night. Other than that the company never had to stop email in 2001, and the AVIT limited damage to only a few dozen or less systems for every virus outbreak. For many of the problem viruses that were in the popular or technical press in 2001, the team blocked the viruses from infecting >any< desktop or server.

The Antivirus System

The current antivirus system for protection from Internet viruses has three basic detection layers, each of which are multipart (there are some critical non-detection layers, like reporting, which are also described below). In addition, there are defenses in place for email that bypass the normal port 25 connection between the company and the Internet. The volume of mail, the number of desktops covered, and a rough count of viruses is shown here:

Outermost layer - 500k emails/week to and from the Internet,
most viruses are blocked here.
Email viruses typical day 0-2 viruses per million emails
(125,000 users, ~4 million emails/day nationwide)
Desktop viruses typical day 10-20 infected files
(25,000+ desktops/servers nationwide)

The company's outermost layer of antivirus defense at is a two-part defense using PMDF relays (3.1) http://www.process.com/tcpip/pmdf.html and a general purpose antivirus engine at the firewall. The multiple SMTP email relays are fully meshed to provide for failsafe operation and load control for the roughly 500,000 emails passing between the company and the Internet every week.

PMDF and the viruswall Antivirus System combine to provide protection at the layer closest to the Internet. In the first step the PMDF checks to see if the "Subject" line is typical of a known problem virus, for example for the virus W32/Klez.e (3.2) http://securityresponse.symantec.com/avcenter/venc/data/w32.klez.e@mm.html , is likely to have one of the following subject lines:

Document End
Happy Lady Day

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

From
Eager to see you
and VBS/LoveLetter @MM has a subject line of
ILOVEYOU
while W32/Hybris.gen @MM is famous for a subject line of:
Snowhite and the Seven Dwarfs - The REAL story!
Email with these subject lines are discarded without further processing. The matched words are in the PMDF configuration file (which is a system wide filter file). To add new subject lines requires a recompile and restart of the PMDF. Thus it is recompiled only when there is great need.

In the second step, PMDF removes attachments considered too dangerous. There are over 70 different file extensions used by viruses to carry executables (.jpg and .gif are not two of them). Industry Best Practices calls for blocking executable extensions (.exe, .vbs, etc.) to the extent practical (performance may suffer if too many types are blocked). The blocking is done via a Unix script, which can be updated dynamically. Therefore PMDF can easily block new attachments when needed. When an email has an attachment blocked, the email is sent on to the addressee, but with a new attachment saying that a dangerous attachment was stripped off. This message does not comfort the addressee and needs to be improved.

After going through the two PMDF antivirus steps, the email attachments are examined a third time by the viruswall antivirus engine. The general purpose antivirus engine provides a more complete check for viruses that the PMDF missed. The general purpose antivirus engine is normally updated by new virus identity files (VIF) daily. The VIFs are applied soon after receipt. There are "monthly" engine upgrades in addition to the daily VIFs. AVIT has not had a problem with the viruswall general purpose antivirus system VIFs or monthly engine updates. The vendor has been very good in providing timely support for protection against new dangerous viruses. The only complaints about the vendor are from the administrators who sometimes have to get up to apply the new VIFs at 2:00AM!

There are three other ways for virus-infected email to enter the company: Programmatic Connections, Virtual Private Networks (VPN) connections and web based email. Programmatic Connections are network connections between the company and other companies such as partners, customers, and subcontractors. All Programmatic Connections have a firewall and have antivirus email scanning for attachments to prevent email viruses from entering. To prevent email viruses from entering the company network via VPN connections (home and on the road) a Desktop Antivirus System is provided (described below) for VPN users. The company now blocks all known Web based email providers (Yahoo, HotMail, and many others). Management agreed to this blocking when AVIT showed them the cost of web-based email virus attacks in 2001. Without the records AVIT keeps, AVIT could not have convinced management to allow this blocking.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The middle layer of antivirus defense at the company is an antivirus engine running on the Microsoft Exchange servers. These are currently running a generation behind as the newer version has to use the new Microsoft Exchange API (Application Program Interface). This new API does not allow easy reporting of the names of infected users. Without the names of the infected users, it is NOT possible to block or even find email infections. The email antivirus system used is an antivirus product designed to run on Microsoft Exchange. The only problems AVIT has had have been some "leakage" of email when the Exchange servers are very heavily loaded. In these cases some email, sometimes with viruses, are passed through without being checked for viruses. Because the company has a multilayered antivirus defense, the company antivirus system catches the viruses that leaked through later on the desktops. The company's antivirus system assumes that sometimes an antivirus level misses some viruses. That is why there are multiple levels, with some levels using antivirus products from other vendors. This diversity in vendors and products is very useful in reducing the number of problem virus incidents.

The email antivirus engine provides the information needed for a good antivirus system. When a virus is found it is placed in a quarantine folder and a message is sent to a special mailbox, *Alerts, email-virus*. The message includes: date/time the virus was detected, the server on which the virus was detected on, who sent the virus, and identification of the virus. How this data is used is shown below.

The innermost level of antivirus defense at the company is the Desktop Antivirus System on desktops and server antivirus software on Microsoft Windows servers and Unix servers. They are using a combination of old generation and new generation desktop antivirus systems. All sites are supposed to be at the current generation antivirus system., but some upgrades have been delayed. The old antivirus system can be used with central reporting, but only a minimum of information is provided. The current generation antivirus system provides a wealth of information which allows much more advanced antivirus management. This is described below.

Analysis Methods Before the Event

The first step in analyzing virus infections is to collect the data! AVIT has found that when users report their own infections, less than 1% of the actual infections are reported. Automatic machine reporting is *critical* for an accurate understanding of viruses at the company.

Data is collected by different systems according to the abilities of the antivirus engines. In the outermost antivirus system plus PMDF layer, only the viruses that viruswall antivirus system catches is processed. A summary of each infected email is put in a special Microsoft Exchange email mailbox. This data is processed in the weekly report in a manner similar to that of the viruses caught in the Exchange server (described below). The data on the viruses that the PMDF

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

relays kill or block are not captured at this time. The viruswall Antivirus System/PMDF team is trying to justify to management the extra hardware needed to record this data.

There are over 100 Microsoft Exchange email servers in the company. All emails with viruses caught by the Email Antivirus System on these servers are put into special quarantine folders and a summary is placed in a special email box. The contents of that box are analyzed as needed, normally on a daily basis but the data is analyzed more often during a virus incident. The Email Antivirus System is updated as needed with new VIF files, normally once a week. Up to a few dozen errors may be generated during updates. These error reports (and all reports of EICAR) are removed before the virus analysis processing is done.

The basic analysis methods use pivots and correlation as shown below. Currently the analyst is using Microsoft Excel but AVIT may switch to a database due to Excel's 65k line limit.

First the analyst selects the data from the Microsoft Exchange folder and pastes it into a Microsoft Excel spreadsheet. It must be noted that the *To:* column in the Email Antivirus System report is misleading. It comes from the message sent back to the sender saying that their email was infected and that their message didn't go through. Users almost always ignore this message, except when they immediately try to send another infected email to the user. The spreadsheet below shows typical (but created) raw data.

The date and time that the infected mail was found is in the *Received:* column, which is the first column. The second column, *To:* has the name of the sender of the virus infected email. Since the sender of the virus infected email is being sent a message stating that they sent a virus, this is not the *From:* column. The third column, *Subject:* lists the virus name. The last column records on which Microsoft Exchange server the Email Antivirus System had found the virus. Note that this is the Exchange server that the virus was found on, which may or may not be the server that the victim uses to send email. Therefore it is not possible to simply total up the results in the *From*: column to see which sites are sending the most email with virus infections.

Example-1 raw email reports

Received	To	Subject	From
Fri 3/15/2002 5:12pm	Johnson, Paul	Alert - Virus @97M/Marker.go	Email Server01002
Fri 3/15/2002 4:01pm	Smith, Tim	Alert - Virus @97M/Marker.gen	Email Server01099
Fri 3/15/2002 3:59pm	Johnson, Paul	Alert - Virus @97M/Marker.go	Email Server01002
Fri 3/15/2002 2:20pm	Jones, Karl	Alert - Virus @97M/Class	Email Server01008
Fri 3/15/2002 9:43am	Smithson, Tom	Alert - Virus @97M/Ethan.q	Email Server01023
Fri 3/15/2002 5:01am	George, John	Alert - Virus @97M/Ethan.q	Email Server01038
Fri 3/15/2002 4:13am	Ransome, Ian	Alert - Virus @97M/Footer.gen	Email Server01002

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The first step in processing the email infections is to clip all the infection records (1 line per record) for the reporting period from the Alerts, Email-Virus folder and paste this into a blank spreadsheet. This is the data for the current reporting period. The reporting period is normally once a day for average conditions but which may be as short as 15 minutes during a virus incident.

AVIT then does two analysis processes with this data. In the first process they want to see who has been infected with this virus before, or who has a history of virus infections. Then color the background with a vivid color:

Example-2 Colored New Data

Received	To	Subject	From
Fri 3/1/2002 1:20pm	Jones, Karl	Alert - Virus @97M/Wrench.gen	Email Server01008
Mon 2/11/2002 7:43am	Smithson, Tom	Alert - Virus @97M/Ethan	Email Server01023
Wed 6/9/02 7:32am	George, John	Alert - Virus @97M/Ethan.fam	Email Server01038
Fri 3/15/2002 5:12pm	Johnson, Paul	Alert - Virus @97M/Marker.go	Email Server01002
Fri 3/15/2002 4:01pm	Smith, Tim	Alert - Virus @97M/Marker.gen	Email Server01099
Fri 3/15/2002 3:59pm	Johnson, Paul	Alert - Virus @97M/Marker.go	Email Server01002
Fri 3/15/2002 2:20pm	Jones, Karl	Alert - Virus @97M/Class	Email Server01008
Fri 3/15/2002 9:43am	Smithson, Tom	Alert - Virus @97M/Ethan.q	Email Server01023
Fri 3/15/2002 5:01am	George, John	Alert - Virus @97M/Ethan.q	Email Server01038
Fri 3/15/2002 4:13am	Ransome, Ian	Alert - Virus @97M/Footer.gen	Email Server01002

After opening the historic record of all previous email viruses spreadsheet (which first must have previous highlight colors removed), paste the colored data at the end of that spreadsheet. Then select all of the data and sort by *User Name*, resulting in a list like this:

Example-3 New Reports Sorted In

Received	To	Subject	From
Wed 6/9/02 7:32am	George, John	Alert - Virus @97M/Ethan.fam	Email Server01038
Fri 3/15/2002 5:01am	George, John	Alert - Virus @97M/Ethan.fam	Email Server01038
Fri 3/15/2002 5:12pm	Johnson, Paul	Alert - Virus @97M/Marker.go	Email Server01002
Fri 3/15/2002 3:59pm	Johnson, Paul	Alert - Virus @97M/Marker.go	Email Server01002
Fri 3/1/2002 1:20pm	Jones, Karl	Alert - Virus @97M/Wrench.gen	Email Server01008
Fri 3/15/2002 2:20pm	Jones, Karl	Alert - Virus @97M/Class	Email Server01008
Fri 3/15/2002 4:13am	Ransome, Ian	Alert - Virus @97M/Footer.gen	Email Server01002
Fri 3/15/2002 4:01pm	Smith, Tim	Alert - Virus @97M/Marker.gen	Email Server01099
Mon 2/11/2002 7:43am	Smithson, Tom	Alert - Virus @97M/Ethan	Email Server01023
Fri 3/15/2002 9:43am	Smithson, Tom	Alert - Virus @97M/Ethan.q	Email Server01023

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Starting at the top or bottom of the historic virus infection spreadsheet scroll to the other end stopping whenever a colored bar is found (historical correlation) Use of vivid colors allows very fast scrolling without missing an entry. Examine the infections around each colored entry looking for other infections of the same or different viruses for that user.

If none are found (Tim Smith) assume that the Email Antivirus System on the Microsoft Exchange email server has killed that virus and no assistance is needed. If a previous virus infection is found (John George, Tom Smithson), or if the infection happened several hours apart on the same day (Paul Johnson) then AVIT needs to send a desktop support person to assist in cleaning the infected computer. If the person has been infected two or more times by the same virus then they can estimate how likely it is that the infection came from the same source, If only 10% of the current infections are VIRUS-X, and this person has been infected twice in the past by VIRUS-X, then the likelihood that the repeat infection was NOT from the same source is 10% * 10% = 1%, thus there is a 99% chance that the victim was re-infected from the same virus reservoir. If the desktop support team does not find that virus infected reservoir and clean it, they will have to go back and clean that computer again and again until the computer and the infecting reservoir is cleaned.

If the victim has had prior virus infections, but normally from different kinds of viruses, then AVIT needs to find out what kind of job that person has that causes them to be infected so often. Maybe they are receiving bids or resumes or press releases from outside people. These documents are much more likely to be infected than internal documents. This worker may need extra help in understanding how viruses operate and how they could better defend their systems.

A more difficult problem is finding where the victim is physically located. The analyst uses all available databases in the company, but some days it seems that half the victims have no phone numbers, and often no city or state information. The problem is that there is no checking to see if the data is updated in the databases for new hires or when people are moved to another office. There are many errors in these databases. If AVIT cannot locate the victim they sometimes just cut off their email account or network access. Then AVIT can locate them when they call for assistance.

A few useful tools AVIT has developed for email viruses are as follows. AVIT has had old computers set up in the offices of the core team members. The email system on these computers is set to the mailbox to which the notices of infected emails are sent. When an infected email arrives the email client rings a bell. When an AVIT member hears 5, 10 or more rings in a minute the team member knows that a problem is happening. From timed tests, if the victim's phone number is in a standard database, AVIT can identify an email virus outbreak,

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

identify the victim, call the victim, and if they are at their desk have them disconnect their computer within one minute of the outbreak occurring.

A related tool counts the infected emails in a two-minute period. When the two-minute counter sees too many infected emails in the counting period, it automatically locks out the victim's account. Alternatively, the people on the core team use a tool provided by the email team to lockout an infected user via a web page. The victim can have their email restored only when a desktop support person calls the support desk and verifies that the virus has been removed. With the above methods and tools, pure email viruses have not been a problem for months.

There are currently two desktop reporting systems and one server reporting system. The old Desktop Antivirus System allowed limited reporting. What data AVIT could collect was put into a web page each day. When double clicked it opened into a spreadsheet. Analysis was then done similar to the above email analysis. The company has now deployed the current Desktop Antivirus System to over 26,000 desktops. The current Desktop Antivirus System provides more useful data on infections than the earlier system. All the data can be accessed via a spreadsheet or database. AVIT has changed the current Desktop Antivirus System column order and column names to make them more usable. The system also does not show the known Desktop Antivirus System errors or EICAR. EICAR is a test file that current antivirus systems report as the EICAR virus test file. It is not a virus. It is named after the European Institute for Computer Anti-Virus Research institute). AVIT has a way of accessing EICAR test files if needed to see if the system is working. What is left is good, useful data. Unlike the old Desktop Antivirus System or email data, this spreadsheet has all of the pasted infections data in it. The first step in analysis is to color the period of interest, clip a copy of the new data into a new spreadsheet for pivoting, and sort in the colored records in the original spreadsheet. The data is now sorted and scrolled through by Internet Protocol (IP) and System Name as some sites use Host Configuration Protocol (DHCP). However it has been found that DCHP addressed computer systems are fairly static and the IP addresses seldom change. The rest of the data in this spreadsheet is processed as above, resulting in the following example. Column 1 shows the *Source IP* address, column 2 the *Date* that the infection was found, column 3 the *Virus Name*, column 4 the *System* name and column 5 the *User* name. The current Desktop Antivirus System provides additional information including Engine version, VIF version, Antivirus Engine version, etc., but this is enough for this example.

Current Desktop Viruses
Example 2 sorted

Source IP	Date	Virus Name	System	User
10.22.193.199	4-Feb-2001	JS/IEStart.gen.c	FORD002.77	Ng, David
10.22.194.010	21-Feb-2001	JS/Seeker.I	FORD002.291	Tyne, JD

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

10.22.194.21	21-Feb-2001	JS/IEStart.gen.c	FORD005.223	Jones, Tim
10.22.193.243	21-Feb-2001	W97M/Marker.c	FORD005.98	Rogers, Steven
10.22.193.003	17-May-2001	JS/IEStart.gen.c	FORD002.92	Jones, Tim
10.22.193.023	1-Nov-2001	W32/Nimda.htm	FORD002.723	Jones, Tim
10.22.194.233	1-Nov-2001	W97M/Class	FORD003.99	King, George
10.22.193.005	5-Nov-2001	JS/Seeker.gen.h	FORD002.431	Smith, Brian
10.22.193.145	5-Nov-2001	W95/CIH.remmants	FORD005.02	Jones, Tim
10.22.193.241	13-Nov-2001	JS/Exploit	FORD002.97	Mills, Charlotte
10.22.193.003	14-Nov-2001	JS/IEStart.gen.c	FORD002.92	Jones, Tim
10.22.193.134	14-Nov-2001	W32/Magistr.b@MM	FORD002.21	Jones, Tim

And after sorting by IP (or by System or User):

Example 5: Sorted by IP

Source IP	Date	Virus Name	System	User
10.22.193.003	17-May-2001	JS/IEStart.gen.c	FORD002.92	Jones, Tim
10.22.193.003	14-Nov-2001	JS/IEStart.gen.c	FORD002.92	Jones, Tim
10.22.193.005	5-Nov-2001	JS/Seeker.gen.h	FORD002.431	Smith, Brian
10.22.193.023	1-Nov-2001	W32/Nimda.htm	FORD002.723	Jones, Tim
10.22.193.134	14-Nov-2001	W32/Magistr.b@MM	FORD002.21	Jones, Tim
10.22.193.145	5-Nov-2001	W95/CIH.remmants	FORD005.02	Jones, Tim
10.22.193.199	4-Feb-2001	JS/IEStart.gen.c	FORD002.77	Ng, David
10.22.193.241	13-Nov-2001	JS/Exploit	FORD002.97	Mills, Charlotte
10.22.193.243	21-Feb-2001	W97M/Marker.c	FORD005.98	Rogers, Steven
10.22.194.010	21-Feb-2001	JS/Seeker.I	FORD002.291	Tyne, JD
10.22.194.21	21-Feb-2001	JS/IEStart.gen.c	FORD005.223	Jones, Tim
10.22.194.233	1-Nov-2001	W97M/Class	FORD003.99	King, George

The pivot spreadsheet is processed to produce a report showing viruses by IP (Total lines removed):

Example 6, Current Infections Pivoted to show Source IP, Virus Name, and Count of Viruses

Source IP	**Virus Name**	**Total**
10.22.193.003	JS/IEStart.gen.c	2
10.22.193.005	JS/Seeker.gen.h	1
10.22.193.023	W32/Nimda.htm	1
10.22.193.134	W32/Magistr.b@MM	1
10.22.193.145	W95/CIH.remmants	1
10.22.193.199	JS/IEStart.gen.c	1
10.22.193.241	JS/Exploit	1
10.22.193.243	W97M/Marker.c	1
10.22.194.010	JS/Seeker.I	1
10.22.194.21	JS/IEStart.gen.c	1

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

10.22.194.233	W97M/Class	1
Grand Total		**12**

Here AVIT can see where the attacks are occurring, what viruses are causing problems, who is having multiple different viruses in a reporting period, what sites have no reports (and hence need to be checked to see if the system is still working, i.e. why no attacks from 10.22.195 subnet?), etc. This system works very well in general, but AVIT had problems with it in January 2002, as explained below.

The Server reporting system is similar to the desktop reporting system. Currently it only provides reports for one site but as the bugs are worked out AVIT hopes to have it reporting all sites at our company nationwide. Viruses are often found on servers that backup user data. AVIT has found that when an effective antivirus system is deployed at a site, there has been a drop of a third or more of certain types of viruses found.

It is necessary to test all the reporting paths if viruses are not found for those sites. Several times when it was thought that there were no reports because there were no viruses, it was later found out that there were many viruses but that the system was broken and not reporting viruses. If in doubt, use the EICAR virus test file. Always test, check, and double check reporting systems. Do not assume that the system is working!

Virus Reports, Daily, Weekly, Yearly

Virus reports for desktop Microsoft Windows 95, 98, NT, ME, etc. are obtained from the old Desktop Antivirus System in a manner similar to the Email Antivirus System reports from Microsoft Exchange email servers, i.e. old Desktop Antivirus System provides only a small amount of useful information. While it is harder to extract useful information from the old Desktop Antivirus System than from the current Desktop Antivirus System, enough information is obtained that, with care, a cost effective antivirus program can be run. The key is to use the historical data. Always keep all past records and compare these historic records with the current report. In this manner a user's past infection record is patently obvious.

AVIT configured the antivirus system to report all infections to a central server. This server packages the data and places it in a .csv (comma separated values, a Microsoft Excel readable format) file that is accessible via a web page. The data is updated every two hours and a new .csv file is created every day. Double-clicking on the web page entry brings up the virus infections report for that day.

AVIT has one web page for Microsoft Windows 95 (and the few 98 and ME systems at the company), one for desktop Microsoft Windows NT, and one for

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Microsoft Windows NT/W2K servers. The latter two web pages are similar to the Windows 95 system except that almost all the desktop NT systems have been converted to the current Desktop Antivirus System (and thus there are few reports) and the servers use a command line scanner. But the data format for analysis is very similar.

As with the email system, the daily reports are examined for quality. The virus data (after errors, EICARS, etc. are removed) is colored a vivid shade, placed in the historical files (one each for Win95/98, NT Desktop, and NT Servers), and sorted in. A quick scan down the list finds the new infections, which are quickly compared with the historic record. After running the historical correlation there are several possible results:

Minor virus, first time infections
Minor virus, multi-day infection
Two or more different viruses, first time, single day
Two or more different viruses, multi-day
Very dangerous virus, first time or multi-day (does not matter)

AVIT does nothing with a minor virus on a first time infection. It is likely that the antivirus system caught the virus, killed it, and the infection is cured. It is not cost or time effective to send desktop support to rescan the disk, even with remote administration tools. It will take about 30 minutes for a remote clean and in general there is usually nothing that needs to be done. This policy of doing nothing is a great cost savings. It reduces desktop support costs by about 90% and with the follow-up policy for multi-day infections, provides good protection. In fact, through use of this policy, desktop virus infections have dropped from dozens a day to many days having no infections at all! Be lazy, it can save money! It can make you a hero with management!

When a minor virus is found that is a multi-day infection, take the time to examine several aspects of the historical correlation. As shown in the email virus analysis it is possible to determine in cases of re-infection where the reservoir of infections is likely to be. With this clue and discussion with the victim it is possible to find the infection reservoir and clean it. If cleaning out a virus is not done completely and properly the first time, money and time are lost in repetitive cleanings, as well as exposing the company to an active spreading virus. Do NOT be lazy in this case.

When the victim has had many days of repeat infections and desktop support has checked the antivirus system on that computer and it is working correctly, then this is a case where a user either does not care about viruses or likes viruses and wants to play with them. This is generally resolved by a discussion with her/his manager. In one case a manager kept turning off his antivirus system on over four dozen days during a year. The solution was to have the Vice President of his division speak with him. This is the only, I repeat ONLY, case

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

where one should treat the victim as ANYTHING other than a victim. Even in these cases however always be polite. NEVER act like cops making a drug bust.

If two or more different viruses are found on a system and it is a first time infection on that system, normally contact the user and ask if he has any idea what happened. This is not considered a problem as the antivirus system on the computer probably handled the infections. What is of interest is how multiple viruses arrived together: old backups, an old computer that was infected and placed back in service, from someone else's floppy disk or another cause. In several of these cases analysis may have found a machine that needs but does not have an antivirus system installed. In this case AVIT generates a ticket for desktop support to install antivirus on the computer that does not have one, clean the infected files, and resolve the problem.

If analysis sees a pattern of multiple different viruses over several different days it is likely that the user has a job that brings them into contact with viruses. AVIT may need to provide better protection for this user before they become a victim again. The infection route could be resumes, proposals, bids, letters with other companies, etc. These viruses are probably not arriving via the normal email route (if they were the viruses would have been caught earlier in the system). Other methods for the viruses to arrive include by physical means (US mail, FedEx, UPS) or electronic (unknown programmatic connections, modems, and downloads from web sites) means. Discussion with the victim can usually identify the route of the infection and then a plan to aid the victim from future infections.

A very dangerous virus is defined as one that can spread quickly, or spread stealthily, and in either case, cause great damage. Examples include W32/Nimda (see above), W32/Goner, W32/FunLove (3.3) http://vil.nai.com/vil/content/v_10419.htm, etc. With these viruses AVIT takes NO chances. Desktop support is sent to that system to make sure that the antivirus system is fully up to date, rescan the system, try to determine where the virus came from, make sure that the virus did not get backed up and that the infection will not happen again.

It is important to note that you should *always save all valid data forever.* It will be useful. To be sure it is sometimes worthwhile to reset the record for historical correlation. Examples include when the antivirus system has a major update. When a major update of the antivirus system is done typically many old hidden viruses are found. Because of this the existing problem viruses are mostly removed. Part of the reason for keeping the old data for historical correlation goes away. But at some point someone will ask a question that can only be answered by re-examining the old data. So always keep the old data. And it is always fun to have management call and request an urgent special report and either be able to give it to them while they are on the phone or tell them that it is in the weekly report you sent them a few days ago! This really happens several times a year.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Daily, Weekly, and Yearly Reports and Reviews
Daily, Weekly, and Yearly reviews are generated from the above datasets. They have different uses and audiences. Color is used heavily to aid in understanding, but fancy graphs are not given. It is best to let the numbers speak for themselves. If charts are needed, prepare them, but generally these charts can become confusing with the amount and kinds of data being presented. Read the book "The Visual Display of Quantitative Information" by Edward R. Tufte (1.1) for further details.

The daily reports are *operational*. They let the local desktop support teams know who needs assistance and what kind of assistance is needed. The negative report, reports indicating the site has no viruses for the day, is also useful as it lets the local teams know that there are no viruses and more importantly, by seeing that viruses are caught elsewhere, know that the antivirus system is working and they really have no viruses. There are two daily reports, one for email viruses and one for desktop/server viruses. The daily email antivirus report goes to all sites and to the email and core antivirus team members. In it is a summary of the past day's viruses, and details (virus, previous infections, victim name, phone number, column, building, city, state, country, etc.) of the day's problems. When needed there are reports of new viruses or other items of interest. The desktop/server report is similar but also includes the numbers of viruses by site. Due to the way the email viruses are found (generally on the Microsoft Exchange server at the *To:* end) it is not easy to list where the senders are). For sites that request it trouble tickets are generated for desktop support to resolve the problems.

The weekly reports are review, not operational reports. They contain a summary of all the virus events at the company for the past week and notes about any famous or in-the-news virus events. This report is widely read, especially when a virus has been in the popular press that week. There are a number of parts. The first section of the weekly virus report is mostly text, the second is mostly spreadsheets. The third section has the backup spreadsheets. The third section is not included in the email (or the email would be megabytes in size) but a path to the shared folder is given containing these spreadsheets. The weekly report is sent to everyone on the daily report and to everyone who asks to be on the list (more than might be expected) and goes in the directorate weekly activity report.

The text forepart of the weekly virus report starts off with a brief summary of the past week. This is followed by a list of viruses that are new to the company that have been found in the past week. The third paragraph gives the count of viruses that the Antivirus Vendor lists as high or medium threat (as I write this there are two of Medium risk, according to the Antivirus Vendor), along with the URL http://www.antivirus.com/trendsetter/virus_report/ to allow readers to see the Antivirus Vendor virus analysis for themselves. Then comes a one-sentence

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

review of the current risk from viruses inside and outside of the company's viruswall. The text section ends with a note on how to obtain access to all the virus infections spreadsheets that are generated.

The brief summary of the past week is important. It is a *sound bite* snippet that, if properly presented, is remembered. Through this it is possible to present not only information about viruses, but also try to educate the readers of the report about computer security ideas and principles. One bite a week and after several months the readers end up knowing more about computer security than they expected!

The spreadsheet section of the weekly reports has four spreadsheets: *Viruses at the Company as a Whole, Email viruses for the past week, Desktop/Server viruses for the past week*, and *Internet viruses for the past week.* These spreadsheets show not only the viruses for the past week, but also the past 4 to 8 weeks to allow comparison with recent weeks. For longer term comparisons the full spreadsheets can be accessed as mentioned above.

The first spreadsheet, *Viruses at the Company as a Whole,* is a summary of the rest of the spreadsheets. It has weeks horizontally and virus infection categories vertically. The infection categories are: *email infections, email-help sent, Current Desktop Antivirus System infections, Current Desktop Antivirus System help-sent, Current Desktop Antivirus System infections for City A, Current Desktop Antivirus System infections for City B, etc., Viruswall Antivirus System viruses blocked, and old Desktop Antivirus System desktop and server infections*. Since not all of the sites have 100% current Desktop Antivirus System coverage yet there is also a vertical column giving the rough percentage of coverage for the different current Desktop Antivirus System cities. Below this there are some notes as to the color codes and historical notes on systems that are in the old spreadsheets but not current reports. The color codes are Virus Outbreak (Red background, white text), Viruses this week mostly found during upgrades/conversions (purple background, black text), viruses found due to conversion and outbreak (purple background, white text). Months are color coded with one color per month to aid in understanding and there is horizontal color-coding to group email, current Desktop Antivirus System, Viruswall Antivirus System, and old Desktop Antivirus System data.

The second spreadsheet is called *Total Email Viruses by Week through most recent*. The columns are: *Week, Viruses Found, Systems Infected, Help Sent, and Most Common Viruses* (4 columns). The first row gives a total for the year 2002 to date. Further down on the full spreadsheet are totals for 2001, 2000, and so on as far back as AVIT has data. In the *Most Common Viruses* columns the hazard level of the viruses are color coded with the most dangerous being RED, the next ORANGE, and the least dangerous viruses GREEN. Only the past month or two of data is shown in the weekly report. All the previous data is in the backup data folder. This spreadsheet is built on another spreadsheet that is not

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

posted to the weekly report but is in the backup data folder. This spreadsheet has one row per virus (alphabetical order by the current Desktop Antivirus System vendor naming standards) and one column per week. There is a column to indicate how dangerous the virus is, a column to sum all incidents with this virus back through 1998, and a column to sum the virus for the current year. The monthly columns are color coded to aid in understanding and to help avoid data entry mistakes. Summation at the end of each week is compared with the weekly pivot data to make sure there are no data entry errors.

The third spreadsheet is: *Total Current Desktop Antivirus System Viruses Found by Week through most recent*. Its format is almost the same as the *Total Email Viruses by Week* spreadsheet, as is the backup spreadsheet that is used to generate this one almost the same as the backup email virus spreadsheet. The one difference of interest are estimates of the current numbers of desktops that can report each week (now about 26,000) and the number of viruses that AVIT thinks came into the company via web downloads (typically about 33%) for that week. AVIT hope to use this information to justify the expense of checking all web downloads for viruses.

The fourth spreadsheet is *Internet Viruses Captured at the Firewall in Email* and is from the Viruswall Antivirus System antivirus engine. The format is similar to above but they also have another table that shows the percentage of viruses that week by category, i.e. *Joke viruses, Classic DOS viruses, Windows 95 viruses, Word 95 Macro viruses, Word 97 Macro viruses, Excel viruses, Power Point viruses, VBS viruses, Worms and Trojans, Unix viruses, Macintosh viruses*, and *Unclassified viruses*. So far, Macintosh and Unix viruses always show 0 viruses found.

The yearly report (which may be issued several times during the year but always in early January) is part of a weekly report but also shows how well the company did in the past year (compared to AVIT records from 1998 on) and for other companies. The purpose of this report is to show how AVIT is doing and to review AVIT mistakes and where AVIT might do better. It also alludes to the cost of damages that viruses cause worldwide and to what it would cost the corporation to lose email for just a day due to viruses (tens of millions of dollars would be lost).

The two main tools for analysis, historical correlation via color and pivots, are described above. These tools are critical! They not only save time over searching lists by hand/eye, these methods are fast, allow methods for double checking results, make it easy to generate additional results (i.e. are antivirus engines and VIF files up to date?), and make it easy to do new analysis as needed. The analyst could not do this job without historical correlation and pivots. They are very useful. If you don't use them already please learn how as they are really helpful.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Emergency Communication Plan
The AVIT team have a number of means for emergency communication, including work, home, pager, cell phone numbers, work and home email address, etc. In addition through the Enterprise Service Desk (ESD) they can reach almost anyone who works for the corporation at work or at home 7x24. The Emergency Communication Plan is tested almost every week with various incidents.

Easy Reporting System
The easiest reporting system is have the machines do the work, not the users. All email in the corporation are checked automatically. Over 26,000 desktops are checked automatically. In addition all core team members have their names, phone numbers, and email addresses on the AVIT web page and are known by the ESD. I have received 17 requests for help or information on viruses and hoaxes today alone!

Conduct Training for Team Members
The AVIT conducts some training classes for team members (2 in the past 2 weeks), but with viruses found every day, there is less need for "hands-on" incident training. We do, however, use new viruses and vectors as a practice vehicle.

Establish guidelines for Inter-Departmental Cooperation
AVIT has not established special guidelines for inter-departmental cooperation. Only two members of AVIT are members of the same department! We do inter-department cooperation every day without special guidelines.

Pay Particular Attention to Relationships with System Administrators
AVIT pays particular attention to system administrators. Several people in the AVIT team are system administrators (and others members of the ESD). In addition AVIT team members work daily with system administrators, visit them, and attend meetings with them.

Develop Interfaces to Law Enforcement Agencies and other Computer Incident Response Teams
AVIT has very good relationships with the local physical site security officers. These officers are required to have good relationships with all LEAs. This has been tested in several incidents in the past year and has been found to be working well. The AVIT has good relationships with LEAs and the FBI. AVIT is weaker in relationships with other CIRTs and should improve in this.

The Incident Handling Process - Identification

The incident started at 4:54am PST on 30 January. It was realized to be a problem at 9:12am PST during the normal morning virus analysis. At 11:45am AVIT realized through many automated reports that the problem was growing

© SANS Institute 2000 - 2002, Author retains full rights.

and a special virus attack analysis report was sent to the site. By 1:23pm PST the company's AVIT was activated, one member of the AVIT core team began acting as Incident Handler, and management informed that a virus incident was occurring at one site. A full timeline is below.

The virus was identified through the central virus reporting system (described above in the Preparation section) during the normal morning report. If the virus had been a fast spreading email infector it would have been noted within 10 seconds after a spew started. The primary countermeasures, checking email and network traffic outside of Site D worked, but there were no W32/Nimda attacks outside of Site D (we did find two other W32/Nimda email infections at other sites during this period as well as dozens of other email, desktop, and server viruses, so we know that the system was working).

Detailed log files, analysis sheets, etc. are shown in the containment system below.

Since the corporation has a policy of treating all virus infections as an "illness" and not a hostile act, there was no collection of evidence, no chain of custody, no affirmations. The corporation does do this in other cases and the internal procedures are known.

The Incident Handling Process - Containment

The systems that were found to be infected with W32/Nimda were located (if possible) and repaired. Repair included remote logon (if possible) and remote cleaning of the system with the corporate standard antivirus system, followed by reloading and updating the local antivirus.

As the AVIT is a virtual team, there is no "jump kit" (a "jump kit" is a set of hardware, software, and other tools taken when an Incident Handler travels to the scene). The local desktop support team also did not need a "jump kit" as they used their everyday tools. Site D has about 10,000 computers and generally has a few viruses every day. With no intention of legal actions, there was no need to maintain a low profile. As the team has had vast experience handling viruses, the team knew to be very careful in not allowing their systems to be contaminated with compromised code. AVIT worked closely with the local desktop support team. The team also worked with users when possible. The local Site D management and system administrators were "in the loop" and assisting as needed during the event. As this was a known virus, not a break-in, there no need to change passwords.

Below is a record of all the emails sent from AVIT to the Site D team and an overview of the incident. AVIT had much better tools to "see" the problem.

© SANS Institute 2000 - 2002, Author retains full rights.

The W32/Nimda Incident

The incident started at 4:54am PST on 30 January. It was realized to be a problem at 9:12am PST during the normal morning virus analysis. At 11:45am AVIT realized that the problem was growing and a special virus attack analysis report was sent to the site. By 1:23pm PST the company's AVIT was activated and management informed that a virus incident was occurring at one site. A full timeline is below.

The primary problem with this incident was that desktop support could NOT physically find some of the machines, and it was suspected that some of the machines were being infected by other "hidden" computers. Only about half the computers at the site had been upgraded to current Desktop Antivirus system and had centralized reporting. Therefore it was only possible "see" the virus infections from half the infected machines. And desktop support couldn't find the "hidden" machines physically or by IP address. How to find and handled the "hidden" computers and the machines that could not be "physically" found is discussed in a following section and is one of the main purposes of this paper. The methods used to "see" the viruses in desktops, servers, and email are described above. The tools of historical correlation and pivot tables are very powerful and critical for this company's antivirus activities.

The first W32/Nimda@MM virus found in this event was at 20:54GMT on 29 January 2002, the last was at 20:50GMT on 31 January. During that time period AVIT found 5765 infected files on 32 different machines on 20 different Class C subnets at that site. There were two other W32/Nimda infections during this period in two other states that may or may not have been related. AVIT found NO W32/Nimda spreading in the corporate Email antivirus system (and AVIT had found W32/Nimdas before this event and afterwards). AVIT also found a large number of other viruses in this period. The probable cause of the other virus infections was that a large number of machines had been converted to the current Desktop Antivirus System that day from the old Desktop Antivirus System. The other reported viruses that were due to the upgrade. It is not known if the upgrade "tickled" dormant W32/Nimda viruses to become active. It is also thought that there were non-upgraded systems (AVIT could only obtain virus reports from upgraded systems) that were infecting and/or re-infecting the reporting systems. Most of the infected files were "owned" by the normal system user. However 4 of the 32 were "owned" by SYSTEM.

Four kinds of W32/Nimda viruses were found, but only two of the five thousand plus infections were in the .htm form (and they were the W32/Nimda infections found in this period at sites in other states) and only 169 W32/Nimdas were in the .eml forms. The rest were in the W32/Nimda.gen@MM form or the W32/Nimda@MM form. There were 447 infected files of the W32/Nimda@MM form and on the same machine there were 115 infections of the W32/Nimda.gen@MM form. There were four machines that had the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

W32/Nimda.eml form and the W32/Nimda.gen@MM form. In all four cases they had about the same number (within a factor of 5) of each form. None of the three different forms of W32/Nimda were among the first or last infections. None of these 32 machines had had a W32/Nimda or any other virus reported before. Of the 20 subnets three had two infected machines, two had three infected machines, and one had five infected machines.

Nimda seems to spew in clumps of time over a two to twenty minute period and then go dormant for a ten or twenty minute period. The histogram below shows the number of clumps of spews for different IP addresses. This chart is useful in predicting how often a system may continue to be a problem if not fixed. Most of the computers spew for one or two clumps of time (21 of 32 systems), while six systems spew for 3 to 6 times, and the remaining five spewed up to 21 times. The size of each spew varied from one or two infected files to hundreds. Analysis did not show any other patterns.

Clumpiness of New Infected Files

Number of Clumps of Infected files	Number of Systems
1	16
2	5
3	2
4	1
5	1
6	2
7	0
8	0
9	1
10	0
11	0
12	1
13	0
14	0
15	0
16	0
17	1
18	1
19	0
20	0
21	1
Total	31

© SANS Institute 2000 - 2002, Author retains full rights.

During the postmortem, AVIT found that all the antivirus engines were up-to-date and all but one of the weekly VIF files on the infected machines were up-to-date.

The analyst noticed that a number of the machines had further infections exactly seven days later. Four of the machines in this incident had later infections; others in other incidents. In some cases there were also infections at day 14 and 21. This had not been noticed before. It was also not seen in any vendor reports. A later review showed that this re-infection at one week intervals was common with many virus cases, not just with Nimda. Users seem to do things that get them infected often at about the same time and on the same week day in many weeks. Since the times slightly vary, but not the day of the week, this activity is probably not from a script. This result allows prediction of probable future attacks on victims at one week intervals after a known event. Unless the sources are found and cleaned, the victim is likely to be re-infected again and again. This may be new.

Timeline of Events All times are GMT (=Z) unless stated otherwise

29 January 2002
2054 – First W32/Nimda infections at the site, downloaded via IE, infections were deleted
2131 – Second computer infected with W32/Nimda, downloaded via IE, infection was deleted
2134 – Third computer infected with W32/Nimda, downloaded via IE, infections were NOT deleted, first spew of infections begins at a rate of about 5 infected files found/per minute until 21:50Z.

30 January 2002
0022 Fourth W32/Nimda infection, NOT downloaded via IE, infections deleted

9:12am PST = 1712Z Morning report states “Better check this one. Several dozen infections reported, only one deletion. This computer may still have infected files”. As later analysis shows there were a number of systems infected with W32/Nimda in which the antivirus engine deleted the infected files. Only the third computer did not delete all the files and needed assistance. At this point there were no theories as to where the virus came from or why it was spreading.

11:45am PST = 1945Z Message sent to site stating: “These are newer than my report, and there are several dozen infected files on these two machines. You might wan to clean this one up ASAP if it is not done already.

Thanks!”
Below this was detailed information from the spreadsheet including time, IP, virus, infected file and full path, result of what the antivirus engine did, computer name, user name.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1:23pm PST = 2:23Z Eight machines infected with W32/Nimda.

2:07pm PST = 2207Z Reported more viruses and infected computers

3:18pm PST = 2318Z Another similar report

31 January 2002
4:07pm PST = 0007Z email sent to site requesting them to call the analyst

4:12pm PST = 0012Z email from site to analyst saying that they couldn't reach the analyst as he was on the phone. The problem was that the analyst did not have a second phone line.

4:13pm PST = 0013Z another report, this time with a large number of infections. We are beginning to think that the infection was spreading from systems that had no antivirus on them or a defective copy of the old antivirus system. The problem became one of finding those systems that were spreading the infection and then cleaning the viruses on them.

4:41pm PST = 0041Z The antivirus team was given the ability to perform email lockouts. Under normal conditions only the email team could "turn off" email for a user as permissions to do this would allow someone not to use the system to accidentally damage the Microsoft Exchange servers. The remote email team and the virus analyst had recently moved to a new building and were seated together. The email team realized that the AVIT needed the ability to lock infected users out of email quickly and had generated a tool that allowed those authorized and authenticated to prevent infected users from sending any new email (email in the queue would not be blocked by this tool). During this W32/Nimda event the email team made some small but very useful changes to the email lockout tool. The antivirus team at the site under attack had not been given this ability before. This was the first time the email lockout tool had been used in an incident and it was quite useful.

4:51pm PST = 0051Z Email to management
"Folks

Site D is having a major W32/Nimda outbreak, almost all cases via http (no email viruses). New tools are VERY useful. They are trying to set up a tie line. They do not need help now but it is welcome. I'll send the phone number once I get it."

~5pm PST = 0100Z Incident telecom established. The telecom had the Incident Handler, the virus attack analyst, a virus knowledgeable person from the Enterprise Service Desk (ESD), the Intrusion Detection System (IDS) team, and the local site team. Note that it has been found that it is very useful to have people in the ESD who are experienced with viruses providing support and not just who ever is available. If a new-to-viruses ESD person is brought in to the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

operation, have them in listen mode for 30 minutes or so first to get used to events before having them provide assistance. Sometimes ESD people who are not used to viruses over react. The IDS team is useful in that they could "see" that there were no W32/Nimda attacks going across the corporate intranet outside of Site D.

5:14pm = 0114Z Another large report sent out, this time for the first time in addition to the semi-raw analysis of the infections, the infected systems were listed, along with their infected files. Six infected systems were found on six subnets with four to forty two infected files per system.

5:24pm = 0124Z A full report was sent, showing all sites for the past 36 hours, and all viruses, not just W32/Nimda. Analysis shows that the outbreak is limited only to Site D and that there are no other virus outbreaks any place else in the corporation during this time period.

5:34pm = 0134Z Another report on Site D, now showing system names of infected computers as well as IP addresses and total files infected.

5:39pm = 0139Z This update was the 5:30 update, 4 machines infected, 42 new files infected. The update took 9 minutes to compute and write.

6pm PST = 0200Z Special report, showing web servers only (based upon identification from Site D), not from scanning.

6:07pm PST = 0207Z Resent 6pm update to new person at ESD, added them on to the circular email list for this event.

6:23pm PST = 0223Z It is now almost 9:30 EST and the on duty Incident Handler, who lives in the East Coast, turned over the Incident to an analyst, who will now serve as both Incident Handler and analyst. Incident is in a steady state mode and does not appear to be expanding.

6:44pm PST = 0244Z The 6:30 report showed 9 machines infected in the past 30 minutes, 110 infected files. Report now shows data by IP, system name, user name, and is sent in Excel and as plain text (for one person who couldn't view the Excel file on his computer).

7:15pm PST = 0315Z In the 7pm update 176 viruses were found on 5 computers.

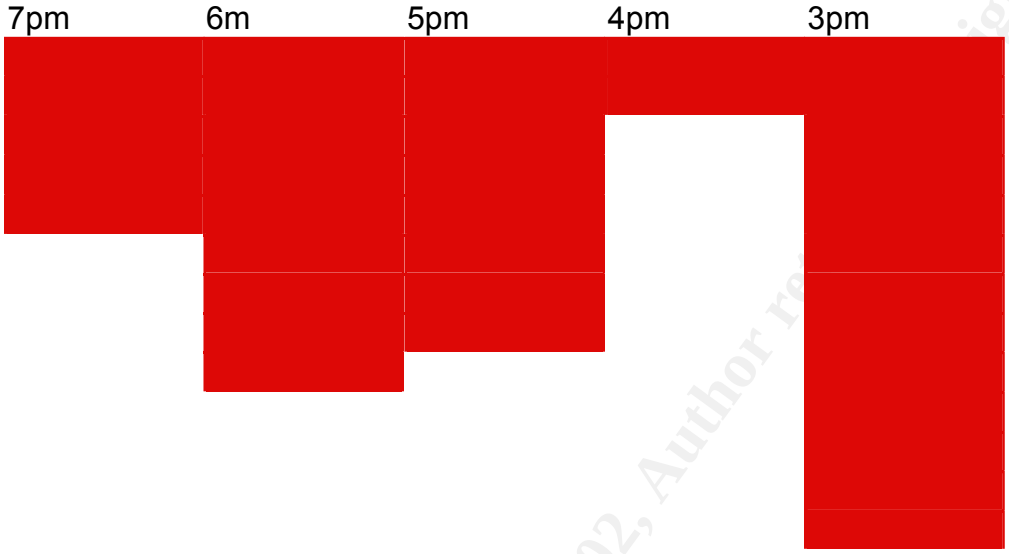
7:26pm PST = 0326Z The first version of the Chaos chart sent out. This showed the number of infected machines by hour from 3pm to 7pm. The purpose of this chart was to see if the problem was increasing or decreasing. The chart showed neither, from any past set of data and it was not possible to predict how many machines would be infected in the next time period. This was useful to gauge

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

how much effort would be needed that night and how many people might be needed to be called in (Site D is two hours East of PST).

Chaos Table

# of Infected Systems \ Time



7:31pm PST = 0331Z Chaos chart extended back to 8am.

7:41pm PST = 0341Z The 7:30pm update showed five infected machines and 168 files. Format and content layout was the same as the 7pm chart.

7:55 Site D IT Vice President talked to the team. Asked if email to and from the site should be turned off. Team said to keep the email flowing, between IDS monitoring and email virus monitoring there was no need to block email. Stopping email would have cost the company an enormous amount of money and the incident team did not want this cost to be incurred. AVIT argued that there were no email infections going on and that AVIT had multiple ways to detect any spread from Site D. Finally the VP agreed that Site D would not be disconnected unless AVIT found major spreading infections from Site D.

8:13pm PST = 0413Z The 8pm update showed four machines infected with 108 infected files. Chaos chart extended to 8pm.

8:28pm PST = 0428Z full list of all W32/Nimda infected machines at Site D sent out, 2671 infected files so far in this incident

8:49pm PST = 449Z The 8:30pm update showed 185 W32/Nimda infections on 6 computers plus one W32/SirCam virus infection

© SANS Institute 2000 - 2002, Author retains full rights.

9:24pm PST = 0524Z The 9pm update showed 289 viruses on 7 computers. The Chaos chart was also updated,

9:35pm PST = 0535Z Email sent out confirming the phone number for the new tie line as the old telephone number had only been reserved for a certain period of time and that time had run out. Only four people were now on the call, but it includes the an IDS team member. They are watching with their tools, as was the analyst with his tools, for possible breakout of W32/Nimda to other sites.

9:44pm PST = 0544Z The 9:30pm update found 5 infected machines and 179 infected files. Chaos chart also updated.

10:17pm PST = 0617Z The 10pm report found 5 machines with 197 infected files. The Chaos chart was updated, and a new Track-by-Infector chart, covering 8pm to 10pm by half hour, was sent to 7 people. Title of email was "New chart, let's talk!"

10:48pm PST = 0648Z Update found 5 infected computers with 230 viruses. The Chaos chart was extended and the Tracking by IP chart was extended. A note was included:

> "As can be seen from the chart below most of the infectors for the past 4 hours have been from just 5 computers. If the team can shut down those computers then most of the problems that AVIT can see with the current tools will be over."

The note on current tools was because the current Desktop Antivirus System had only been deployed to about 50% of the computers at Site D. The remaining 50% of the computers had no centralized reporting of viruses and AVIT could not "see" if they were infected. See conclusion, they weren't.

Tracking IPs Chart – Systems with the most infections are on top.

10:30pm	10pm	9:30pm	9pm	8:30pm
10.22.193.2	10.22.193.77	10.22.193.15	10.22.193.2	10.22.193.192
10.22.193.77	10.22.193.15	10.22.193.2	10.22.193.15	10.22.193.15
10.22.193.15	10.22.193.2	10.22.193.77	10.22.193.71	10.22.193.84
10.22.193.192	10.22.193.37	10.22.193.71	10.22.193.192	10.22.193.2
10.22.193.37	10.22.193.192	10.22.193.192	10.22.193.37	10.22.193.85
			10.22.193.85	10.22.193.77
			10.22.193.77	10.22.193.71

When this was realized, AVIT partly shutdown the incident. The ESD kept the tie line open (they work 7x24), the IDS standby person set his alarms to wake him up if there was a problem and went to sleep (he monitors from his home). And the local site team shutdown the above computers and went home to sleep. Full cleanup was worked in the morning.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1 February 2002Z = 31 January PST
2:13pm = 1013Z Report said: “No viruses found in the current reporting period from Site D! No W32/Nimda, no nothing!

Good Going!”

End of Incident

The Incident Handling Process - Eradication

Eradication consisted of remoting into the system (if possible) and cleaning or killing the virus, followed by updating the antivirus engine. Eradicating W32/Nimda is on almost every antivirus vendor’s webpage.

The root causes for the problem were:

Home user with infection VPNd into the network. The corporate antivirus team detected the problem but did not know how to identify that the system was VPNing in nor how to contact the user at home. This has been corrected.

Another reason for continued reinfection was that many of the machines had been set to move *infected files to a quarantine folder* on the computer, only there was no quarantine folder and the antivirus engine did not create one! This has since been corrected.

The symptoms were automated virus reports from many machines. AVIT had had a number of W32/Nimda events and incidents before and knew the vulnerabilities. The corporate IDS team was asked to monitor certain vectors to insure that W32/Nimda was not spreading via vectors that AVIT could not monitor (shares). With internally proven W32/Nimda removal tools and a good software update system it was possible to be sure that all the updates and backups were W32/Nimda-free.

The Incident Handling Process - Recovery

The desktop systems that were infected were already or were about to be converted to a new update system that allowed a central server to “push” any and everything needed to the systems. The gold master was updated to correct the settings of the antivirus program and to force an update of IIS security patches after the users had installed any software that might add risk, i.e. - Microsoft Front Page. These methods insured that systems were restored to the desired state. Local system management verified that the restored and improved system met local needs.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The system as a whole was never "taken down", only a few computers. Once the "ping-pong" effect was stopped and the *Front Page* problem identified and fixed, these machines were cleaned, updated, and returned to service.

The local team learned more about how to use the central reporting system.

The central team developed better alerting tools including one that gave a simple "quick look – red/green" status for all sites desiring this information.

The corporate antivirus team, AVIT, and the corporate Vulnerability Alert team, VAT, are now working more closely together.

One of the problems in the incident was that AVIT had no way of identifying VPN users. VPN users are a problem as these machines may not be owned by the corporation, their IP address changes more often, and the users probably are not at work and therefore the standard corporate whitepages would not have a working phone number for them.

Monitoring for virus infections is 7x24 at the corporation. Several extra checks were made in the days that followed, but no special problems were found.

The Incident Handling Process - Lessons Learned

AVIT has an existing Lessons Learned process. It could probably be improved however. No one person is assigned to the task. Generally the project lead does the Lessons Learned. The Lessons Learned is not done by AVIT the day of or the day after the event. We should improve on this. AVIT has few special forms for Lessons Learned and is not yet using SANS forms. Everyone involved is invited to review the document. No consensus is reached by AVIT (core and extended) members in Lessons Learned. AVIT sometimes conducts a Lessons Learned meeting. We should probably do this more often. An executive summary is sometimes created by AVIT. We should do better on this. The AVIT Lessons Learned report is sent to management. AVIT is weak in implementing Lessons Learned lessons and should improve here.

In processing the infection a few problems were found and lessons were learned:

1) Every person working the call virtually (Incident Handler, Analyst, ESD support, local team) needs at least two phone lines.
2) A local person should stay on the phone at all times. The virtual team cannot provide useful support if they are not in contact with the local team (if only the virtual team could identify which machines were infected).
3) AVIT needs a better way of having backup so team members can sleep. This is not the first incident at the company where AVIT had no backups for many team members (note, AVIT has three people who have handled

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

a number of incidents, this is almost enough Incident Handlers. AVIT does not have enough analysts.).

4) The SANS Incident Handling (IH) process might want to consider having a position of analyst and researcher (for new viruses or exploits). AVIT has found these positions very useful in the past. One cannot do Incident Handling at the same time as researching a problem or analyzing the data (except for low workload time periods).
5) Obtain a list of all IP subnets for a site before an event. Be sure to also obtain the IP address of all VPN connections.
6) Develop a way to find all the active computers on a subnet under attack and what ports they have open (i.e. obtain permission ahead of time to do network probes and port scanning with Nmap).
7) An antivirus system cannot work right if not properly configured. Test, test, and retest.
8) When upgrading users to new computers, scan for old viruses on all systems before transferring the data, files to the new computer.

During the incident the ability to do analysis on desktop computers greatly improved. Previous major incidents had all been with email viruses. The Email Antivirus System antivirus product on the Microsoft Exchange servers is good, but did not provide the amount of data that the current Desktop Antivirus System did. The initial reports were based upon what was possible, needed, and worked with email incidents and did not consider the differences in a desktop event and the additional data. In addition the *Chaos Chart* and the *Tracking IPs* charts were useful.

Extra Material

Corporate IH Plan vs. SANS/DOE IH Plan

The following is a comparison of the SANS general Incident Handling Plan and the Corporation's antivirus informal Incident Handling Plan. The SANS plan is based on the DOE plan and has had many years of practical use and input from almost a hundred professional incident handlers. The SANS plan has six steps: *prepare, identify, contain, eradicate, recover, and lessons learned* (2.11). The Corporation has no formal plan. The SANS plan is designed for a team that travels to an incident and operates the plan locally. The Corporations AVIT uses a virtual team to deal with major virus outbreaks in dozens of sites in every state of the union at the same time. Virus outbreaks can spread very fast and the AVIT needs to react very fast. Under some conditions (not 7x24) the AVIT can detect an email virus outbreak, identify the user of the system infected, find their phone number, call them, and if the user is at that phone number, be talking to them and get them to remove the network connection of the infected computer all in under 60 seconds! This has prevented a number of minor virus outbreaks from growing into major incidents. The SANS plan seems aimed mostly at incidents

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

that have a limited number of systems under attack and incidents where this quick a reaction is not possible. The AVIT team has dealt with virus infections involving tens of thousands of viruses on hundreds of infected machines while trying to protect over a hundred thousand computers in many states and countries.

The SANS plan has six stages:

Preparation
Detection/Identification
Containment
Eradication
Recovery
Follow-up/Lessons Learned

If you consider the **preparation** stage to be AVITs normal daily antivirus activities, the Corporation is well prepared for what AVIT is able to do (see below for what AVIT does not do well). However SANS expands the preparation stage beyond this to include: *Policy, People, Data, Software/Hardware, Communications, Transportation, Space, Power and Environmental Controls, and Documentation*. AVIT, being a virtual team, does not need on-site capability for many of these. See below for Policy. The Corporation needs a few more people with experience. Communications needs some improvement, however most of the points that SANS makes in the section the company already follows. And AVIT has communications tests fairly often from the current Desktop Antivirus Vendor or normal communications or incidents themselves. The one point in communication preparation where AVIT is not ready is to have encrypted telephones and faxes. This is not needed for viruses and could be obtained fairly quickly if needed. SANS also pushes PGP and tests using PGP. The corporation is well prepared to detect viruses as it has an excellent email virus detection and, for those sites that have deployed the centralized desktop reporting system (now at about 26,000 desktops), a very good desktop virus detection system.

However the SANS *policy preparation stage* has some items in which the Corporation is weak in. In the Policy stage, while the corporation has good notification of Banners and policy on presumption of privacy, the corporation's preparation needs work elsewhere. The Corporation needs a better written policy on when the AVIT can remote into an infected computer when the user cannot be found to be asked. AVIT need a policy on active scanning of subnets to look for vulnerable/infected machines. An improved policy for notifying neighboring companies who might be affected is needed. When to contact Law Enforcement Agencies needs improvement and was a problem in one past event. How to handle user owned machines (at home connecting via VPN to the Corporate Intranet) that are actively infecting the company network has not been written, and also for contractors, customers, and other non-employees. Road warrior policy is also non-existent, as is what to do with viruses on extranet/partner-nets (other than disconnecting the network). This has caused problems in the past.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SANS recommends as part of preparation that management support for an incident handling capability be developed. AVIT has management support based upon our past track record, especially when compared with other similar companies abilities to handle viruses. However AVIT does follow SANS recommendations to gather and use news articles on incidents. This is done through the top "sound bite" of the weekly virus report where an interesting virus or computer security news items are published in each issue. A much longer weekly computer security newsletter is also published but not very many people read it. However all the articles of previous newsletters are saved and are computer searchable for stories to illustrate particular points. This has been used in the past.

SANS recommends that the team have support in the form of credit cards for equipment and other needed items for dealing with the incident, and a pre-defined set of rules and exceptions for what can and cannot be procured (tape drive? Food? Hotel rooms or RVs?) ahead of time. They also recommend that there be an incident handling drill to test this before an event happens.

SANS thinks that having users and administrators report possible problems should be easy and encouraged. AVIT does not do this but the corporation's employees seem quite willing to report hoaxes and possible viruses already. AVIT might want to make the AVIT web page easier to find…put it on the standard site home pages?

SANS recommends training for team members, especially if there has been no recent incidents. I agree, however most of the training that SANS considers necessary does not apply to virus incidents. SANS also recommends surprise drills to keep team members ready. This is something AVIT should consider if AVIT has not had a real virus incident for a month or so.

SANS points out that the help desk is a very important source of information, and can be very useful during an event. Encourage the help desk to report to the Incident Team anything that seems "funny". SANS also recommends developing close relations with the help desk. AVIT does this already, but AVIT could consider what else AVIT might want to do to improve relations. SANS also says that the Incident Handling team needs to maintain very good relationships with all system administrators. That AVIT should do proactive training with them and that in addition to encouraging them to perform regular backups, AVIT should identify who among the system administrators are very good at reading log files. After one incident where this was needed, I agree. Interestingly, SANS states that there are often problems when Incident Handling teams come from security departments instead of being a mixture of security and system administrators.

Prior connections with law enforcement agencies and Computer Incident Response Teams need to be developed. This includes knowing whom to contact

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

in the local police department computer crime office and the local FBI cybercrime team, and finding out what they are interested in working on. Ditto for CIRTs.

The company has a requirement for Physical Security Managers to maintain excellent relations with local law enforcement officials and the FBI. From observation, this is true. AVIT has a good relationship with the Physical Security Managers at several sites and thus meets the SANS suggestion.

The rest of the SANS preparation items are not a problem for AVIT.

The second step in the SANS plan is **detection**. The corporation has very good email virus detection and a much-improved desktop virus detection system. While the corporation needs to expand the desktop protection, what they have is very good and has proven itself already.

The third step is **Containment.** At this point in time the AVIT, with the assistance of the email team for large events, can quickly contain email virus outbreaks by removing the capability of infected users to send email. The email team can also remove existing infected email from the email queues and from uninfected users in-boxes. The team also has the ability to request (and this has been granted in 3 cases) that all email from a site be cut off or even the network be shutdown for a sites or all sites in the corporation. Desktop and server containment is not as strong but is reasonable, if the computers can be found. AVIT needs to improve it's ability to physically find machines given just an IP address and perhaps go even further (note, the AVIT does use the Network Operations Center (NOC) and network experts, as well as the network IDS team as needed).

Eradication is the fourth step. The local desktop/server support teams normally do this task. This has worked well in the past but it might be useful to provide them with more information. In particular AVIT should generate a standard practices document showing what steps should be taken for various viruses, when to let the antivirus engine clean the problem and when to format the disk drive and every other disk drive on that subnet.

Recovery comes next in the SANS plan. The AVIT informal plan is to continue monitoring and analysis until all the local problems have been cleaned up and no more problem viruses of this type has been seen for a while. This step has worked pretty well in all past incidents.

The last step is the **Follow-up**.

SANS has a Seven Deadly Sins list:

Failure to report or ask for help
Incomplete/non-existent notes
Mishandling/destroying evidence
Failure to create working backups

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Failure to prevent re-infection
Failure to apply lessons learned

The AVIT take on these sins is:

Failure to report or ask for help has not been a problem for the members of the AVIT team. The corporation reporting system has worked very well and no one seems to be afraid to ask for help. It should be noted that while users do not report viruses very well, machine reporting at sites that did use user reporting has found a more than 100-fold increase in viruses found once they switched to centralized machine reporting. Team members have always been willing to ask for and offer assistance.

Incomplete/non-existent notes is a problem for the AVIT team. In general AVIT does not keep them. While AVIT does not expect that the corporation will ever go to court over a virus case, having analyzed the emails and notes from the above case showed AVIT that AVIT could do a better job at Incident Handling.

Mishandling/destroying evidence is not a problem as AVIT has never had to handle evidence. However one of the team members has passed the CISSP exam and has taught evidence handling in several courses, and at least two of the core team members have lockable storage that could be used for evidence. In addition the team has close contact with police who can provide assistance with evidence if needed.

Failure to create working backups has not been a problem as the team has only handled viruses, not intrusions. Probably the AVIT should practice this for Windows NT, Windows 2000, and one or more forms of Unix.

Failure to prevent re-infection is hard to answer. AVIT has had re-infections, sometimes serious re-infections. Mostly this has happened because AVIT did not do enough research on the new virus. In particular the viruses that spread by shares instead of or in addition to email have had major re-infection problems. The new merged transit viruses (Code Red, W32/Nimda, Goner) make avoiding this mistake even more important in the future.

Failure to apply lessons learned is something AVIT has not done well. As AVIT has no list for each event of lessons learned, with notes on what was fixed and what still is not fixed, AVIT cannot consider that they have done what should have been done. Part of the reason is money, partly because AVIT did not have concurrence, and partly for unknown reasons. AVIT have also not had everyone involved in the postmortems.

SANS has a list of Emergency Action Points

Remain calm, don't hurry
Notify your organization's management, apply need to know, use out of band communications
Take good notes

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Contain the problem
Back up the system(s), collect evidence
Eradicate the problem and get back in business
Lessons learned

The corporations AVIT response:
Remain calm, don't hurry – this has not been a problem for the AVIT members, although some of the additional help has gotten a bit excited.

Notify your organization's management, apply need to know, use out of band communications – part one AVIT has had problems with, but AVIT probably has this mostly corrected. AVIT needs to better decide when to notify early and when to notify everyone on the list. The second item, need to know, does not apply in any incident so far. AVIT normally uses out of band communications as a virtual team, i.e. telephones. AVIT has used other methods as needed, including in one case a ban on any wireless phone usage.

Take good notes is a problem. AVIT has not been taking notes. Below I suggest AVIT add a recorder position, but even without it I expect them to take better notes in the future.

Contain the problem has worked when AVIT understood the problem. AVIT often needs to do more research. In the ExploreZip virus event the AVIT core team reported to the extended team on Day One that the virus could spread by the then new method of shares, but shares on Windows systems were not blocked for two more days and the corporation lost a lot of computers and unrecoverable data as a result.

Back up the system(s), collect evidence has not been an issue with AVIT as AVIT has not dealt with incidents where AVIT needed to backup systems or collect evidence.

Eradicate the problem and get back in business happened in each of the 13 incidents AVIT handled in 2001. Aside from the items mentioned here that could be improved, AVIT has worked very well.

Lessons learned is an action that AVIT could improve (see above). SANS recommends that the Incident Handler write the draft report as soon afterwards as possible and circulate it among the team members who worked that incident. They can either concur, make suggestions for change, or write a statement about what they disagree with.

SANS says that after the report has been reviewed then it is time to hold the *Lessons Learned* meeting. The focus of the meeting is to develop a consensus Executive Summary of the incident. SANS states that "*What is the most important thing for an Executive Summary to cover? How much has the*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

*organization saved by having an effective incident handling procedure!"(*2.10). AVIT seems only to hold somewhat unfocused Lessons Learned meetings with little follow-up. Other topics should include organizational or policy problems that interfered with the incident handling process.

The final step in the Lessons Learned process is to hold a follow-up meeting to discuss process improvement. This is not a blame game, but rather to review what might be done better. SANS notes that this is a hard place to avoid blaming people, but that this must be avoided.

I think the SANS methods for the *Lessons Learned* step is better than AVIT's and AVIT should modify the teams methods to include their better ideas.

Additional items SANS considers important that the Corporation does not now do:

Take good notes, who, what, where, when, why and how.

The corporation IH plan does not require notes. SANS recommends having a recorder for use, if possible a mini-disk. The corporation does not use that and in some locations forbids recording devices in the buildings. SANS recommends a still (not video) camera to photograph sites and screens of interest. The corporation does not use cameras, in deed, does not allow them in many sites.

SANS speaks of having a helper along side the Incident Handler, the corporation's virtual team seldom has two members within 300 miles of each other. At times it would be very helpful to have another body locally to assist.

SANS recommends enforcing a "need to know" policy. The corporation's antivirus plan does not, in general. Both are correct. SANS needs to consider possible legal action, they cover more than antivirus cases. The corporation's system is only for viruses (and Trojans, worms, RATS, and other malware). AVIT does not consider anyone a "bad guy". All people whose systems are infected are considered "victims". AVIT is never going to take the victims to court for normal viruses. If the corporation's AVIT were to be used for a non-virus event, then the SANS policy would be better to use.

SANS recommends using out-of-band communications. The corporation's plan in a major virus incident is to set up one to three telecoms (management, email technical, antivirus technical). Generally one person from each of the technical calls also joins the management line to provide cross team communication. The corporate antivirus team also uses email to exchange data, generally reports on systems/users who have been infected being sent from the analyst to the local teams (who will provide assistance).

Additional methods that may have been used or should be considered include:

Microsoft NetMeeting
http drop boxes

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

fax
PGP Encryption
Private ISP accounts
Cell phones

One member of the corporations AVIT uses Microsoft NetMeeting in many other projects and thinks that the AVIT would find this very useful. So far, no one else agrees.

For one major email virus incident when the corporation lost email for a while, http drop boxes were setup to transfer data and update VIF files. This worked very well and should be in standby for future events. It should be tested about once a week.

Most, but not all, sites at the corporation have a fax machine within a few hundred meters. Fax has not yet been used by the corporation but it could be if needed. The problem with fax is that the output is hardcopy and most people want to work with softcopy.

SANS strongly recommends PGP usage, based upon a warning they had to give on 1 April one year (that alert was considered an April Fool's joke by many). The corporation has PGP distributed widely, but is not using it now for virus incidents. It could be used, but has not been tested and it is not known if everyone on the team has it installed and configured correctly. So long as the team is just processing viruses this is probably not a problem.

The corporate AVIT team members have knowledge of many of their private ISP mailing addresses and could make use of them during an emergency.

SANS strongly recommends that each incident team member have a cell phone and several extra sets of batteries. The corporate AVIT team just recently obtained a second phone line in the office for the analyst. The corporation does not provide cell phones for team members. They do provide one-way text pagers. This has been of use, but cell phones would allow consultation if an incident happens when the team members are away from their computers. All that the pager can do is to make them aware of a problem.

Also useful would be

Recorder
Communicator to the rest of the company
More Backup Incident Handlers (AVIT has only 3 now, and
two of them are often on other incident jobs, "hands on" virus research, updated DAT file testing, DAT file prep and distribution, Internet research, incident analysis, and assisting other organizations.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Additional SANS Tools

SANS recommends prior preparation of a “go bag” with full incident handling and backup tools for any OS under consideration. This would include CDROMs of known good software, CDROM burner, laptop, cables, extra batteries, etc. since the corporate AVIT is a virtual team, a “go bag” is not needed.

© SANS Institute 2000 - 2002, Author retains full rights.

Bibliography

I have not included in the Bibliography all the URLs given above for the various Microsoft Security Patches or Antivirus Vendors W32/Nimda pages. These are in the document above

0 The most useful source for references for this paper, is, of course, Google, www.google.com

Part 1 – The Exploit

1.1 Common Vulnerabilities and Exposures http://www.cve.mitre.org/cve/

1.2 Security Focus http://online.securityfocus.com/search

1.3 Example Microsoft Technet article (a number of Microsoft Technet articles are referenced with full URLs in the text)
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp

AVP/Kaspersky Lab 1.4 http://www.viruslist.com/eng/viruslist.html?id=4261

F-Secure 1.5 http://www.fsecure.com/v-descs/nimda.shtml

Norton AntiVirus 1.6
http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html

AVX Command Central 1.7 http://support.centralcommand.com/cgi-bin/command.cfg/php/enduser/std_adp.php?p_refno=010918-000005

Computer Associates 1.8
http://www3.ca.com/Solutions/Collateral.asp?ID=1132&PID=128

CERT Alert
http://www.cert.org/body/advisories/CA200126_FA200126.html

NAI Virus Information Library W32/Nimda.htm entry
http://vil.nai.com/vil/content/v_99209.htm

Sophos 1.9 http://www.sophos.com/virusinfo/analyses/w32nimdaa.html

McAfee 1.10 http://vil.mcafee.com/dispVirus.asp?virus_k=99209&

Part II – The Attack

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.1 SecurityTeam's article IE5 allows executing arbitrary programs via .chm files
http://www.securiteam.com/windowsntfocus/5ZP0J000DQ.html

2.2 IIS Microsoft IIS Extended Unicode Vulnerability by Guofei Jiang
http://www.sans.org/newlook/digests/unicode.htm

2.3 CERT article on W32/Nimda attacks on Port 80
http://www.cert.org/body/advisories/CA200126_FA200126.html

2.4 Snort.org article on W32/Nimda signatures
http://www.snort.org/article.html?id=31)

Part III - Incident Handling

3.1 PMDF Relays http://www.process.com/tcpip/pmdf.html

3.2 Symantec W32/Klez.e subject lines
http://securityresponse.symantec.com/avcenter/venc/data/w32.klez.e@mm.html

3.3 NAI VIL on W32/FunLove W32/FunLove
http://vil.nai.com/vil/content/v_10419.htm,

© SANS Institute 2000 - 2002, Author retains full rights.