Global Information Assurance Certification Paper

Application of Defense in Depth Model Against Malicious Code

A look into designing an effective Enterprise System, and its Daily Administration

By
Kalo Milkoff
GSEC Version 1.4b
Submission Date: August 17, 2004

Summary

Malicious code has become an integral part of the IT life in the past several years. It is in the mainstream; new viruses are able to break major news stories due to their widespread footprint and ability to bring financial harm. How does one protect the enterprise against the vast variety of malicious code effectively, relying on predominantly signature-based software?

This paper will examine the types of malicious code IT administrators face today, and remedies available for effective mitigation of threats. An effective model would piece together technology, procedures and both manual and automated administrative effort. But, in order to devise such architecture against a moving target, one has to study and understand the adversary, and keep abreast of new developments. The following study is primary applicable to the Windows environment, however, it can be applicable to other Operating Systems. In addition, the term "virus" is used to refer in general to worms, Trojan horse programs and other malicious code.

A minimum protection for any computer system that is vulnerable to virus infection is to have up-to-date antivirus software running. However, the current virus definition database can only protect the system from known viruses. There are ad-hoc situations when a dangerous and active new virus is traversing the Internet, and the inability to update antivirus definitions on time could result in widespread infection of systems. If one only relies to signatures to detect and cure, then this strategy has clearly been defeated.

Types of Malicious Code

Macro Viruses

The macro viruses relate most often to Microsoft Office products and mostly Word. Ever since Microsoft included Visual Basic support in Word, and the rest of the Office suite, this enabled malicious code to integrate into files, thus creating ideal facade. Protection was enabled against macros, but this was later overcome by more sophisticated code. As a result of infection, damage is caused mostly to files with .doc, .dot, .xls, .xlt, .ppt, .pot and .mdb extensions and Office applications. If such a virus has destroyed files, there nothing that can be done to undelete them: the virus has not erased them, but it has inserted its own code.

As far as application damage, the best recourse is a reinstall, since no antivirus program deals with repairing a third party product.

Trojan Horses, including Spyware, Spybots, Hijackers, Adware, and Keyloggers.

Trojan Horses are small applications, auto-executing code, or “active content” that allow access to a penetrated computer to others without owner’s consent; they could set up file server and Keyloggers, or turn a system into a tool for Distributed Denial-of-Service attack. The most common type of Trojan is the remote administration type; they are Internet-borne and consist of two elements – host program and user program.

The host part is sent to the user under the disguise of an attached executable, in the case of an e-mail attachment, or via Java or ActiveX code that targets user’s web browsing. If such a code is allowed to infiltrate the host system, it loads in memory and allows remote access to the originator of the virus. It was possible to clean the host system simply by restarting the system with some older types of Trojan Horses; however, new variants create entries for themselves in win.ini, in the Startup folder, and in the registry.

The user program is employed by the originator of the malicious code, instructing the host program remotely. The level of access could start from registry modifications, manipulation and execution of files, accounts and passwords retrieval to moving of mouse cursor, and false messages. Classic representatives of this type of a program are Subseven, NetBus, Back Orifice.

Boot Sector Viruses

Boot sector viruses write their code onto the boot or system sector of the media they infect – floppies, hard disks, etc. This usually leads to Windows not being able to access or recognize these devices. It is important to note not to insert floppies or other writeable media into the system while infected, as their boot sectors will become compromised. In addition, it is possible to overlook media that could have been used while infected, and re-infect the system with this type of virus in the future; this makes scanning floppies a pre-requisite upon discovery of a boot sector virus.

BIOS Viruses

These types of viruses are capable of destroying hardware. By flashing the BIOS firmware and erasing its contents, they prevent the system from booting, resulting in a board replacement as a worst case scenario. BIOS viruses execute only upon system boot, so an infection does not mean an automatic BIOS flash; a system restart is needed.

Worms

Worms are the type of viruses that are most prevalent today in news headlines. They are and are distributed to unsuspecting recipients in an e-mail attachment and commonly disguised files with double file extensions, such as openme.jpg.bat, as Windows by default hides the last extension of a file. The recipient's e-mail address is usually harvested from an infected user's address book, spam list, or a web site, carrying random trivial text in the subject line, such as "Important message from <sender name>".

Another technique of worm writers is to utilize compressed attachments as carriers of malicious code. As .zip or .rar files carry no direct threat to the end user, they and are commonly allowed through without barriers by e-mail gateways. This social engineering approach relies on the end user to infect oneself from the curiosity of opening a provocative attachment.

Blended Threats

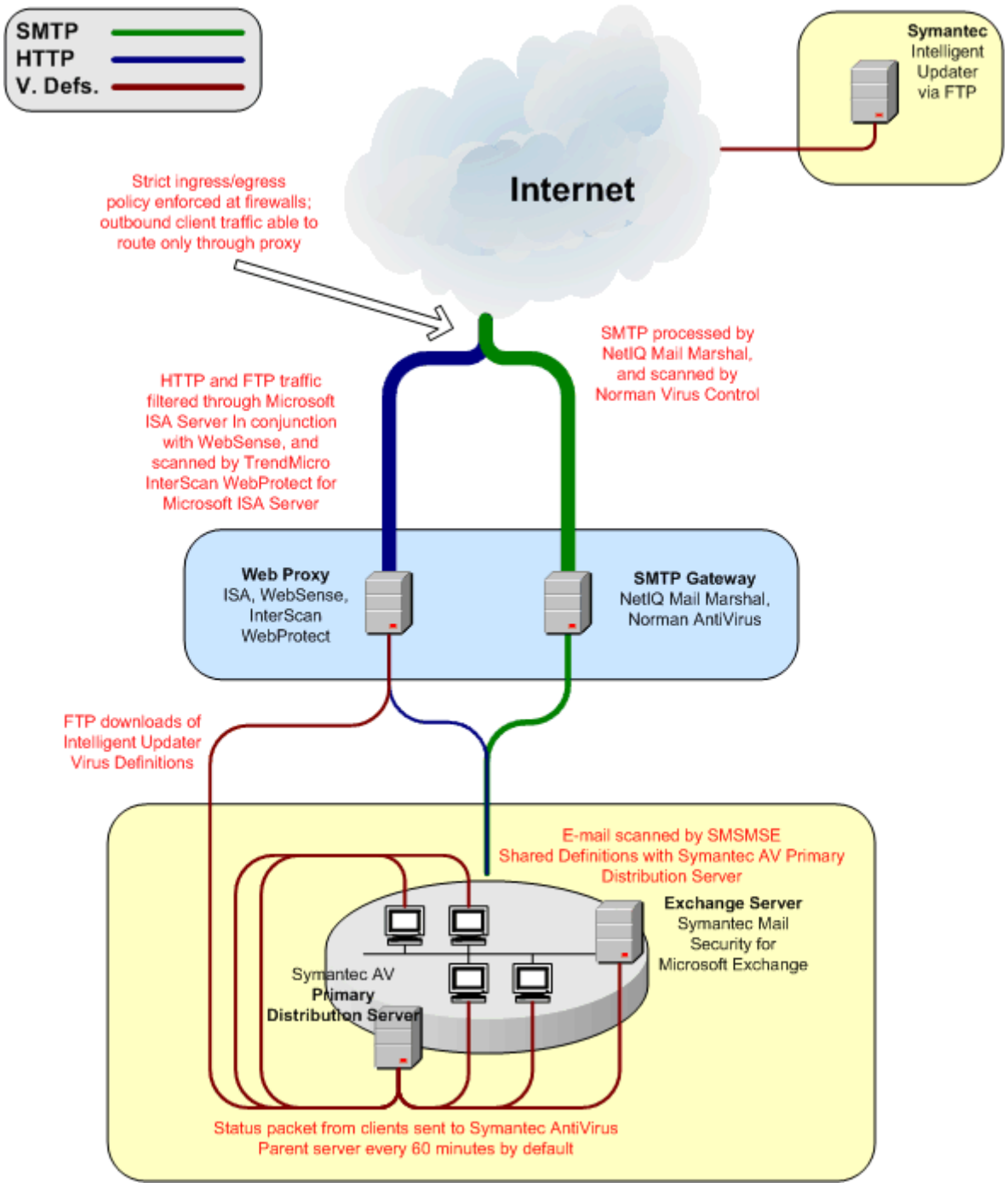
Blended threats are a combination of malicious code and vulnerabilities to launch a cyber attack. "A blended threat exploits one or more vulnerabilities as the main vector of infection and may perform additional network attacks such as a denial of service against other systems." (Chien, Eric and Ször, Péter). Methods of propagation include un-patched systems, e-mail, visits to compromised servers, backdoors left by previous viruses, and systems with open file shares. In addition to Usenet, more sophisticated and faster spreading worms use new vectors for infection, such as P2P networks, IM applications, wireless phones, and pocket PCs.

They share a number of characteristics:

- Can cause harm
- Use more than one attack method
- Require no user intervention to propagate
- Typically use several propagation methods
- Exploit vulnerabilities in un-patched systems

"Blended threats made up 54 percent of the top 10 malicious code submissions over the last six months of 2003.", and "may have resulted in up to $2 billion in damages." (Symantec, Symantec Internet Security Threat Report, March 14, 2004)

Simply utilizing a signature-based solution is not realistic, facing the level of threat at stake. Architecture needs to be put in place in order to match the right tools available against specific threats.



The Architecture

Following is as an illustration of the specific architecture can consist of.

Ingress and Egress Filters at the Edge

Strict ingress and egress filtering at border network infrastructure components, such as routers and firewalls. No traffic is allowed outbound if not routed though a proxy server, allowing only authorized activity across the network.

Internet Proxy Configuration

At the proxy server, HTTP and FTP traffic is filtered through Microsoft ISA Server in conjunction with an Internet filtering solution, such as Websense, and scanned for viruses by TrendMicro InterScan WebProtect for Microsoft ISA Server or Symantec Antivirus for Microsoft ISA Server.

Usage of Websense facilitates filtering against known harmful sites, as well as helps with shutting down traffic towards discovered new sites, serving malware. “90% of businesses suffered hacker attacks in the last year, 1 in 3 corporations have spyware on their networks”, and “45% of IT Managers reported that viruses have infected their company's network.” (Websense)

As an addition to the ability to filter unwanted web material, and content checking at the perimeter of your network, a scanner such as InterScan WebProtect for Microsoft ISA Server would detect in an user’s web traffic malicious code traversing via HTTP and FTP - it is no good having email anti-virus protection, if a user can download a Trojan from a website and infect your network via that vector.

The Ubiquitous E-Mail Gateway Virus Scanning Point

“Since 1999, the most dangerous viruses have been the rapidly spreading Internet and e-mail worms. Given the spectacular increase in the incidences of this kind of malicious code, Internet gateways (proxies, firewalls, mail servers) are expected to continue being the principal target for virus writers. For this reason, a sound corporate security policy should be centered on reliable protection for these gateways, making them the first line of defense.” (Summary of the ICSA Labs 7th Annual Computer Virus Prevalence Survey 2001).

Blocking e-mail attachments with the file extensions EXE, SCR, VBS, COM, BAT, or PIF at the e-mail gateway is just the beginning. These extensions are frequently carriers of viruses and SMTP is definitely not the proper avenue for their distribution. Some organizations allow only ZIP attachments, consider as an alternative. In light of recent usage of compressed files as payload carriers, a procedure can be instituted to notify users, and manually temporarily block ZIP files, until antivirus signatures have been updated.

Implement multiple virus engines at the gateway. As “There are four critical selection factors: Accuracy, Ease of Use, Administrative Overhead and System Overhead.”, antivirus software is selected based on a wide number of criteria (W. T. Polk & L. E. Bassham). Although a good virus engine usually detects all known viruses, it is a fact that a combination of virus engines and content security software increase the level and efficacy of recognition of known malicious code, than a single antivirus product.

The SMTP Gateway is even more powerful when anti-SPAM and content security software such as NetIQ’s Mail Marshal is present. Not only does it “Block viruses, malicious code, specified file types and Spam”, by using built-in antivirus software plug-ins, but “protects against wider threats than just viruses”. (Marshal Software). These threats include loss of reputation, based on the fact the company might become an attack vector, increased bandwidth due to large e-mails, intellectual property breaches, productivity issues, etc.

Host Scanners

Antivirus software on workstations should by far be a standard. Configure policies on client software to allow the least possible access to the end user, locking up real-time scan protection, and system scheduled scans, if available.

Utilizing real-time protection, both incoming and outgoing viruses are detected and either repaired or quarantined before they have an opportunity to spread. Real-time protection is critical with the usage of encrypted e-mail as the gateway antivirus software is not able to check encrypted traffic, mail for infected attachments, scan attachments, or stored encrypted files on shares.

If you image workstations, incorporate antivirus software in a standard baseline. Notwithstanding the existence of imaged baseline, periodically perform an audit to check if there are rogue workstations or laptops on the network with no antivirus software installed.

Set up e-mail alerts or other mechanism to communicate alerts for detected malware. Configure alerts to write to the event logs, and archive.

While it is possible that some servers might not be particularly vulnerable, based on their maintained level of security and user access, it is also strongly advisable to consider placing client antivirus software there, as well.

File share servers, and Microsoft Exchange servers are an example of good candidates. However, certain precautions need to be made. “Allowing Symantec Antivirus to scan certain parts of a mail server can cause unexpected behavior, problems, or even total data loss.” (Symantec). In Microsoft Exchange’s case, as well as for domain controllers in Active Directory, certain files and folders need to

be excluded from scanning, as damage to the databases or issues with directory replication could occur.

While the specifics of the host antivirus software architecture can vary, based on geographic, departmental, or other approach, automation is the key to success in keeping virus definitions up-to-date. Set up the best possible process to obtain updates regularly. In Symantec's case, if internal Live Update server is not a consideration, use Intelligent Updater, instead of standard Live Update downloads. Consideration here is given to the fact that Intelligent Updater is updated daily, as opposed to Live Update. But it requires a manual download. Implement a monitored script solution to get updates via FTP.

Deploy and Monitor a network Intrusion Detection System

Based on anomalous traffic, signatures, and unusual network activity as a clue, and before any other alert could trigger, such a system can give an early warning, if tuned properly. These types of systems will aid in port scan patterns that infected hosts employ shortly after they begin searching for targets. However, "the IDS is free to flag anything it deems unusual." (Farshchi); if normal behavior is not profiled to the specific environment, the intrusion detection system could be more of a hindrance, rather a contributor to the overall architecture.

Network Segmentation

Zero-day viruses represent a significant threat to large networks. More granular network segmentation is a possible defense, as it would limit the malicious code's proliferation by isolating it in specific network subnets. Workstations-populated subnets cannot directly communicate with server subnets, or between departments without some kind of a firewall device.

Host Application Firewall

For authorized remote access users, institute a standard that requires a client firewall installed in addition to antivirus. The mobility of laptops makes these types of systems more vulnerable to outside intervention, as opposed to office desktops. In addition to requiring the firewall for the privilege of using VPN services, the firewall needs to be enabled. There should not be an opportunity for the end user to disable the functionality of the firewall simply because of the mere inconvenience of a persistent unknown popup window, or perceived access and bandwidth issues. Proper configuration of the firewall should reduce the number of firewall-related popup windows to a minimum.

Instant Messaging

Have a tight grip on instant messaging software, such as Windows Messenger. If used as a business tool, deploy an enterprise-level solution, with proper levels of access, and prohibit anything else.

Security Updates

Patch your systems in a timely manner, and install application security patches for products such as Outlook. Blended threats rely on compromising un-patched systems, before an updated antivirus signature had been developed. In addition, vulnerability assessment software can be used to automatically identifying un-patched systems.

Abreast of Events

Stay up-to-date on trends in virus and security matters. Popular portals include http://www.incidents.org/, http://www.securityfocus.com/, http://www.symantec.com/avcenter/, http://www.uscert.gov/, http://www.auscert.org.au/, to name just a few. Subscribe to publications which can keep you current; many vendors provide up-to-the-minute security advisories and assistance based on their own research, being a member of their mailing list is mandatory.

Additional Policies

Adopt and enforce a no-open network shares policy.

Configure Windows to always show file extensions – either in a standard baseline, or through a GPO policy. This should resolve the double file extensions masquerade.

Consider using Active Directory GPO policies to remove unneeded Windows services; they are a security risk because the open port through which they communicate.

Training

Educate end users about security threats and what those threats mean, including issues such as double file extensions, to disregard suspicious e-mail, and not to open it even in preview pane, or follow web links in an unsolicited e-mail, etc.

Validation

Monitor feedback between components of your anti-virus architecture. If there is no user, or system feedback, your approach is bound to fail. Verify updated signatures on a daily basis, and setup an e-mail alert system to notify you if an update to virus distribution servers happens, or not.

The Response

Process and Guidelines

In addition to other policies that might already be in place, set up antivirus process and guidelines what to do if users suspect a virus incident, and basic steps that can be taken to help prevent the propagation of a virus and a potential damages it may cause. Excellent samples could be obtained from the SANS Security Policy Project, at http://www.sans.org/resources/policies/.

Basic steps need to be concise, not to confuse the end user with too much information, and in return achieve no feedback.

1. Physically unplug your system from the network. This will prevent the virus from spreading. Only attempt to power off your system, if you are unable to unplug the network cable.
2. Write down any information that may help to identify the virus, such as:
   a) The Subject of the email message you suspect triggered the infection (if you suspect it was triggered by email)
   b) The name of the person who sent the email/virus. Please, note that the virus might have automatically sent a copy of itself from another user's mailbox and they might not even be aware that their system is infected, or the virus could have spoofed the From: address with a legitimate one, even though the person, whose name appears as a purported sender might not be infected.
   c) A description of the activity on the system such as increased hard-disk activity/slow application response time, unusual pop-up, etc.
   d) The name of the file that you believe was responsible for the infection (either as an email attachment, a file on the system, a floppy disk or on the computer network)
   e) Any files that you believe may have been damaged by the virus
   f) Whether the system has the very latest antivirus software and definition files installed.
3. Shutdown and power off the system only if step 1 is not possible.

Once the initial steps have been taken to contain the spread of the virus, the incident must be reported to Information Security Office.

Response and Recovery Tools

Even with an elaborate architecture in place, it is a given that an infection will happen. The first and obvious action upon a suspected virus infection is following your own established processes and guidelines. Visit the response center of the vendor of your choice, such as http://securityresponse.symantec.com/, or http://www.sophos.com/downloads/ide/, and correlate available technical details

of recent malicious code with events that might be affecting the system in question. If a recognized activity occurs, adhere to vendor removal guidelines or use tools supplied.

Typical scenario is to validate that the virus definition signatures are updated on the system itself, restart Windows in Safe Mode, delete or clean virus carrier files, and reverse changes made to the registry. Study entries in the registry, in predictable locations, such as HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, and HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. If an irreparable damage has been made, then initiate restore from backup, if possible, or image workstation.

To assist in analyzing data for infection trends, examine and quarantine unknown viruses upon discovery, create a model desktop environment, complete with antivirus scanning tools, registry monitors, such as InCtrl5, application firewall, etc. Set up a virtual machine, such as VMWare's Workstation commercial product, available at http://www.vmware.com/products/desktop/ws_features.html, an excellent tool to build an isolated and recoverable sandbox.

Handling Network-Aware Malware

The majority of antivirus software has historically been short on support detecting Trojans, Spyware, Adware, Hijackers, Keyloggers, hostile Java applets and ActiveX components, etc., so where does one start investigating?

Determine the type of malware suspected. This is important, because the approaches to dealing with unknown viruses are different, depending on the type of Trojans, Worms, or other malware detected. Because of the danger of rendering a system unusable with a simple deletion of the offending file, a research into the type of malware is a must. This is where a standard system baseline is important, but even general knowledge into the types of expected processes should suffice.

Verify the applications that load upon startup first. Navigate to Start > Programs > Startup. If you find a shortcut to an application that you know you have not installed or cannot remember installing, and you are sure it is not among applications you use, this is a potential Trojan. Deleting the shortcut from the Startup folder is just one way to prevent future execution of the malicious application, as most Trojan applications place entries in the registry or win.ini, as well – a check there would yield more information. Besides the standard registry "Run" location choices, there are variants that create their own scattered entries elsewhere.

A multitude of tools exists in order to check for Trojan-related malicious logic; below are listed some free and effective basic ones, in addition to system scanners:

- A basic utility to check your startup settings is Msconfig.exe, the Windows System Configuration Utility from Microsoft. Available in older versions of Windows, it was not included by default in Windows 2000, but it is back in Windows XP. Windows 2000 users can use the Windows XP version, as msconfig is a stand-alone program, and runs on any computer. Type msconfig from Start > Run to load. Check the Startup tab for unusual startup items and their location.

- The freeware application Autoruns is an excellent, and much more elaborate alternative to Msconfig from Sysinternals, and available for download at http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml.

- Another freeware, intended for advanced users, is HijackThis – “a tool, that lists all installed browser add-ons, buttons, startup items and allows you to inspect, and optionally remove selected items.” (SpyChecker.com), and available at http://www.spychecker.com/program/hijackthis.html.

- Spybot S&D is a very effective scanner that allows you to automatically scan and remove Dialers, Keyloggers, Hijackers, Spyware, and Trojans, available at http://www.safer-networking.org/.

- Use the command-line TCP/IP Process to Port Mapper fport from Foundstone - www.foundstone.com/resources/proddesc/fport.htm. The utility "expands on the information you would see using the 'netstat -an' command, but it also maps those ports to running processes with the PID, process name and path. Fport can be used to quickly identify unknown open ports and their associated applications." (Foundstone). The output can be sorted by ports, application paths, etc., which greatly helps in identifying non-standard processes.

From understanding the danger at hand, to protection, detection, and response, I have briefly reviewed malicious logic threats to the health of computer systems, surveyed the daily administration, and design of an effective antivirus enterprise system, and discussed general security issues as they apply to viruses. While no one of the techniques examined is foul-proof alone, a layered combination of the tools described, together with administrative expertise, is capable of achieving significant progress in a battle against an ever changing adversary.

References:

1. Chien, Eric and Ször, Péter. “Blended Attacks - Exploits, Vulnerabilities and Buffer-Overflow Techniques in Computer Viruses”. URL: http://www.peterszor.com/blended.pdf. (August 3, 2004)

2. Symantec. “Symantec Internet Security Threat Report.” March 14, 2004. URL: http://www.symantec.com/press/2004/n040315b.html (July 29, 2004)

3. Websense. “Why Use Websense?” URL: http://www.websense.com/products/why/ (August 1, 2004)

4. Polk, W. T. & Bassham, L. E. “A Guide to the Selection of Anti-Virus Tools and Techniques.” National Institute of Standards and Technology Computer Security Division, March 11, 1994. URL: http://csrc.nist.gov/publications/nistpubs/800-5/select/select.html (August 1, 2004)

5. Bridwell, Lawrence M. and Tippett, Peter. “ICSA 2001 Virus Prevalence Survey.” ICSA Labs, a Division of TruSecure Corporation. URL: http://www.trendmicro.com/NR/rdonlyres/C490C780-DF65-43FB-9629-9A6EE23B804E/2770/icsavps2001.pdf (August 5, 2004)

6. Duigan, Adrian. “Product White Paper.” Marshal Software. Published May 2001. URL: http://www.flexnet.com/Email_Security_and_Filtering/Email_Security_And_Filtering/Mail_Marshal_SMTP/Downloads/avcs.pdf (July 26, 2004)

7. Symantec. “Considerations on installing Symantec or Norton Antivirus Corporate Edition on mail servers.” URL: http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2004062508305148?OpenDocument&src=ent_hot&dtype=corp&prod=Symantec%20AntiVirus%20Corporate%20Edition&ver=8.x&tpre= (July 23, 2004)

8. Farshchi, Jamil. “SANS Intrusion Detection FAQ: Statistical based approach to Intrusion Detection.” URL: http://www.sans.org/resources/idfaq/statistic_ids.php (August 7, 2004)

9. Merijn. “Product description.” SpyChecker.com. URL: http://www.spychecker.com/program/hijackthis.html (August 6, 2004)

10. Foundstone. “Product description.” URL: http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/fport.htm (August 6, 2004)