Global Information Assurance Certification Paper

Wolf in the Fold – Evolution of email viruses and worms…and countermeasures to deal with them.

Paul Goscinski
Assignment GSEC version 1.3
March 14, 2002

Introduction:

Even if your organization has a well-configured firewall, has educated users on the proper handling of email attachments, and is running virus protection software on your Personal Computers (PCs), email attachments can bypass the firewall and attack PCs whose users have used the default virus software installation. Computer Associates' "Top Ten Viruses of 2001", published in eWeek [i], shows that each of the top ten of 2001 were Internet email worms/viruses that carry attachments with the infectious agent. And it is not getting better. "ICSA Labs' 7th annual survey of 300 North American organizations found nearly 1.2 million incidents involving destructive computer code on approximately 666,327 machines during the 20 months from January 2000 through August 2001. Based on previous annual surveys, the data indicates an annual growth rate of approximately 20 virus encounters per month for every 1,000 PCs."[ii] CNET News went so far as to call 2001 "The Year of the Worm."[iii]

Email viruses are getting smarter and spreading more quickly. The new viruses build upon the successful techniques of earlier viruses to become more complex and spread faster. This paper will examine the most prevalent of last years' email viruses. It also includes a case study of an email virus attack of one of those viruses. To deal with this escalating threat, a multi level strategy was implemented to prevent future infections. One component of the strategy is scanning smtp mail traffic entering the network from the router using firewall independent gateway virus scanning software and automatic updates of virus definitions. The second component is virus-scanning software with automatic updates on the file servers. The third component is custom configuration of virus scanning software on the PC to thoroughly scan email attachments, using heuristic scanning. There are no substitutes for good backups to prevent data from being destroyed by either virus attack or equipment failure. The assumption is that backups are always the first line of prevention against data loss, and will not be covered here.

Recent Evolution of the Virus/Worm Threat:

Any discussion of Internet worms starts with the Morris worm. In 1988, Robert Morris unleashed the first Internet Worm[iv] on a fledgling Internet of only 60,000 plus computers and only 500 some networks. The worm infected up to 6,000 computers, or about 10 percent of the Internet at the time.[v] "Technologies such as firewalls, IDS and commercial anti-virus software were still years away."[vi] Most of the email worms described here are

really combinations of email viruses and worms, combining the characteristics of both. On the virus software sites you may find them classified as one or both, or sometimes classified as one with a subtype…primary type virus, subtype worm for example. The requirement for classification as a worm is a worm does not require user intervention to replicate.

According to an article in eWeek the beginning of this year, "The past 12 months have been one long coming-out party for the fast-spreading e-mail worm, several flavors of which ran amok on the Internet at various points…. Nimda and others ushered in the age of so-called blended threats: malicious programs that combine traditional virus like behaviors with other threats, such as the ability to infect machines through multiple means or launch a denial-of-service attack."[vii]

Before last year's crop of viruses is discussed, two older viruses deserve discussion because of their use of techniques that would be built upon further in 2001.

The "Melissa" macro virus used social engineering to coerce its' victims into opening the attachment. By mailing to recipients in the victim's Microsoft Outlook address book, the message appeared to have been purposefully sent by somebody you knew. Further, the body of the message read: "Here is that document you asked for ... don't show anyone else ;-) " The .DOC file attached contained the Word Macro virus.[viii] While not considered a worm because it required user intervention in opening the attachment, the speed at which it spread set it apart from other viruses that preceded it. The old advice of "Don't open email attachments from somebody you don't know" was no help in stopping "Melissa."

The "Love Letter" worm used social engineering techniques along with the default behavior of the Microsoft Windows operating system to trick users into opening the payload attachment. People couldn't resist opening a love letter from someone they knew…(again, the worm used the entries in the address book to propagate). The subject was "ILOVEYOU" and the message read, "kindly check the attached LOVELETTER coming from me."[ix] To disguise the file extension, which was .VBS or Visual Basic Script, the filename was padded with blank spaces so that it would be cut off and not displayed obviously on the screen. The "Love Letter" worm was the first to use file extension obfuscation.[x] "For people who use Microsoft Outlook and a product called Windows Scripting Host, simply previewing the message was enough to activate the virus."[xi] Instructions for disabling Windows Scripting Host are available on the Sophos website.[xii]

Of the top ten viruses of 2001, ranked by Computer Associates[xiii], variants of Badtrans, Sircam, and Magistr composed the top five. Hybris, Win95.MTX, Nimda.A, VBS.VBSWG.Generic and Goner.A rounded out the top ten, in that order. All of these had their payload contained as an attachment to email.

The BadTrans worm has its' payload distributed as an email file attachment and exploits two known vulnerabilities to replicate itself.[xiv] The first vulnerability is any program that uses vulnerable versions of Internet Explorer to render HTML, such as Outlook Express and Outlook, may execute the program as soon as the email message is viewed.[xv] The second vulnerability it exploits is using the default behavior of Windows operating systems to hide file extensions from the user, or file extension obfuscation, as discussed previously in the "LOVELETTER' worm.

Sircam is another virus that spreads through email attachments, and also potentially spreads through unprotected network shares.[xvi] The recipient may be tricked into opening the attachment because the file will appear without the .EXE, .BAT, .COM, .LNK, or .PIF extensions if the "Hide file extensions for known file types" is enabled in Windows.[xvii] As of this writing, based on Message Labs ranking of top viruses active on the Internet, Sircam.A is by far the most active virus on the Internet today.[xviii]

The Magistr Internet worm was discovered in early March, 2001. This worm incorporated several clever social engineering techniques to get users to open the payload attachment. Since it replicated using addresses in the email client address book, once again the email would come from someone you know. The subject line could be constructed from words and sentences that are found in .DOC and .TXT files in the system, so it could be a pertinent subject. Finally, it could attach Microsoft Word documents (.doc files), so it could send a real document along with an additional file, the payload.[xix] The Magistr-B worm followed in September, 2001, with enhancements. This worm will be covered in a case study later in this document.

The Hybris worm also had a payload in the form of a .SCR (screen saver) or .EXE (executable) file. The worm infects WSOCK32.DLL file, and when a user sends an email from the infected PC, the worm sends another email to the same recipient with a copy of the worm as an attachment. This worm differed in that it took leveraged the power of open mail relays to propagate itself and to make it difficult to trace the origins of the infections.[xx]

Win95.MTX is a virus that exhibits worm like behavior. The file attachments are usually .PIF (Program Information File…executable by Windows), .EXE or SCR. When it is run, it unpacks and drops a Trojan into the Windows directory. This virus is different in that it infects the system files by "entry point obscuring". This means that instead of infecting the "entry point" in the program or the header of .EXE files (typically the 512K, which has unused space left over), it can patch the program at almost any point inside its code. This makes detection more difficult, as the virus might not run right away, but only when a particular part of the .EXE program is executed.[xxi]

VBS.VBSWG.generic refers to a group of a worms created based on the code in the VBSWG kit (Visual Basic Script Worm Generator kit). The Anna Kournikova worm was of this group. This virus could trick recipients into opening the attachment, since the file

will appear without the .VBS extension if "Hide file extensions for known file types" is turned on.[xxii] This is the same trickery seen later in the SirCam worm, discussed previously.

The Goner worm comes as an email with a "gone.scr" (screen saver file) attachment as the payload. It propagates by mailing itself to all addresses in the Microsoft Outlook address book, and to all online users in the ICQ contacts list. This worm is different in that it searches out and kills processes associated with anti-virus and security software.[xxiii]

The Nimda worm aka the "Concept Virus" appeared in September 2001.[xxiv] The first section of the message contained no text, but the second section contained a binary executable file called Readme.txt. Because of a vulnerability described in CA-2001-06 (Automatic Execution of Embedded MIME Types), mail software running on an x86 platform using Microsoft Internet Explorer 5.5 SP1 or earlier (except IE 5.01 SP2) the payload is triggered by opening or previewing the message[xxv]. "The vulnerability could not be exploited if File Downloads have been disabled in the Security Zone in which the e-mail is rendered. This is not a default setting in any zone, however."[xxvi] This is easily changed in Outlook by selecting Tools | Options | Security and setting the Zone to Restricted Sites. The default setting is "Internet". This will keep the browser from rendering HTML mail from unregistered sites. Attachment Security on this screen should be set to high. There is a great advantage in spreading the virus without requiring user intervention for opening the attachment, and closing this vulnerability is an important step.

As this document was written, the latest email worm comes disguised as a security patch from Microsoft.[xxvii] It uses a file naming convention that Microsoft commonly uses to name patches, to lead recipients to believe it is a real Microsoft patch. This worm, called W32/Gibe, is like many others that preceded it, where a user must execute the attached file in order to be infected.[xxviii] There's just no end to it.

Case Study:

Our organization had a properly configured firewall, using least privileges, for blocking unwanted network traffic. Every PC had current McAfee Viruscan software installed, and updates were downloaded to a local server. Our users were educated in the proper handling of email attachments; especially from outside sources or from people they did not know. Notifications of Virus software updates were posted on the Local Intranet page, with instructions for updating. Cautionary instructions for handling of email attachments were posted there, as well…including a list of file extensions to avoid opening in an email attachment.

In early September, a new variant of the Magistr virus was found. McAfee.com reported the virus on September 03, 2001 on their website.[xxix] However, an updated virus definition file from McAfee was not ready until September 12, 2001.

Symantec.com reported the virus on September 03, 2001 and had an updated virus definition file the following day on their website and by automatic download.[xxx]

Kaspersky Labs reported on it in a September 04, 2001 warning on their website – "Magistr makes Grand Return"[xxxi]:

Unfortunately, there were very few computers running Symantec anti-virus software at our site, as McAfee Viruscan is our office standard. The Network Associates virus definition file update would not be ready for two days, and on September 10, 2001, a Magistr.b virus originated from a parent office location.

The virus used ingenious social engineering to entice the victim to open the file attachment. The Subject is empty, or constructed of words found in .DOC and .TXT files on the hard drive of the victims' PC. Not just any words, but "sensitive" words from a list the virus writer created. In our case, it grabbed a DOC file concerning sensitive information about an employee, created a Subject line with the sensitive words, and attached the sensitive .DOC file, along with a second "payload" file .EXE or .SCR file and emailed it to the entries in the PCs address book.

As well trained and educated as the users were, this was too much to resist. It was an email from a supervisor, concerning another employee in the Subject line. It included a paragraph from the doc file with juicy info in the message body. The doc file itself as the first attachment. All relevant, real material…until the second file attachment, the payload.

The following details of the actual method of infection are from the Kaspersky Labs virus encyclopedia and website:

"The messages may have no body (no text in the message), or randomly constructed as well as a Subject (see above). The Attached file name variable. The virus looks in the system for a PE .EXE or .SCR file of up to 132K in length, infects it and attaches to the message. In some cases, the virus fails to infect the file, and an "infected" e-mail message exits a computer without an infected .EXE or .SCR file. In one out of five cases, the virus also attaches a .DOC or .TXT file that has been found in the system while the virus was scanning files for Subject and MessageBody texts. So, a randomly selected .DOC or .TXT file may escape from the system, possibly causing the disclosure of confidential information. All in all, the message the virus sends out of an infected PC contains the following: "strange" or empty Subject and message body .EXE or .SCR file (infected or clean) that is possible the message also have second attached file - .DOC or .TXT. While sending infected messages, the virus connects to one of three e-mail servers using SMTP protocol, and sends messages to there. In 4 out of 5 cases, the virus randomly corrupts a second letter in the sender name. The virus stores ten e-mail addresses of already infected users (a history of spreading - the 10 most recent e-mail addresses the virus spread from) in its body. While spreading, the virus compares a

victim's e-mail address with this list, and does not send messages to addresses that are already infected." [xxxii]

A user from a next door office came by and informed me that she thought she had a virus. A second call and a third followed quickly before I could investigate the first. It was obvious the system had been compromised, and to prevent further spread of the virus by email, I immediately logged onto the mail server and killed the sendmail daemon. That halted the spread of new messages dead in its' tracks. In a few minutes, I found that users were still opening messages that had already been delivered from the first onslaught. I killed the imapd daemons on the server, and temporarily disabled it by renaming it so that no users could start it, and that stopped further spread of the virus. See "Unix in a Nutshell – System V Edition"[xxxiii]. Further advice on recovering from an incident or intrusion is available on the CERT website.[xxxiv]

The next step was assessment of the damage, enumerating and quarantining of the infected machines. Once McAfee released an extra.dat virus definition file the following day (which is placed in the virus scan program directory on the PC), the infected PCs were cleaned and brought back up again. The mail server daemons were restarted, and we cautiously monitored and evaluated the incoming messages. The day after, McAfee Security released the full Virus definition file.

The First Line of Defense

The solution to preventing future damage is three levels of virus scanning, utilizing automatic updating of virus definitions and heuristic scanning. The first line of defense regard to the email worms was to catch them at the perimeter by employing firewall independent gateway virus scanning, along with automatic updates of virus definitions. McAfee Security has a number of Internet Gateway Protection Products [xxxv]. Since McAfee Viruscan is deployed at the desktop throughout the organization, since we run Solaris servers, because I had an idle Solaris box, and also because of the low price, the McAfee Webshield for Solaris Product was selected. This product not only scanned SMTP traffic, but also HTTP and FTP traffic as well.[xxxvi]

McAfee Security is not the only vendor with Internet Gateway Protection products, or email server protection products. A list of Anti-Virus software vendors is available on the CERT website.[xxxvii] The following are some of the alternatives:

Sophos has a gateway email product called MailMonitor for SMTP. They also have software for Microsoft Exchanges and Lotus Notes/Domino.[xxxviii]

Kaspersky Labs has anti-virus protection for various email gateways, including Microsoft Exchange, Lotus Notes/Domino, and Sendmail, Qmail, Postfix.[xxxix]

Panda Software makes products that protect Microsoft Exchange and Lotus Notes/Domino servers.[xl]

Symantec Corporation offers Norton Anti-Virus products for gateways, and for Lotus Notes/Domino.[xli]

Trend Micro is another company offering virus protection for the NT- or UNIX-based Internet gateways, scanning SMTP, FTP, and HTTP traffic.[xlii]

This covers the first component of the strategy. Either utilize mail server scanning software or scan smtp mail traffic coming out of the router using firewall independent gateway virus software, and automatic updates of virus definitions.

The Second Line of Defense

The second component is installation and configuration of virus scanning software on the file servers. McAfee offers a variety of products for file server protection.[xliii]

For Netware Servers, there is McAfee Netshield for Netware. Their product runs as a Netware Loadable Module (NLM) on the server and is configured to scan all incoming and outgoing files.

For NT Servers, there is McAfee Netshield for NT. It works in a similar fashion, running as a process on the server.

There is also a Viruscan UNIX version. This software runs as a process on the Unix box, and is listed on their website as a Unix desktop (not server) solution.

McAfee makes a Multi-platform Viruscan that runs on Windows 9x, NT and 2000. Using an NT box, and installing Samba[xliv] on the Unix servers it will allow you to access Unix file systems using the Server Message Block protocol (SMB) on the Windows box, and scan them using the McAfee Multi-Platform Viruscan software. In particular, the home directories of the users can be scanned on a recurring basis, because that is the most likely place viruses will be introduced into the system, via email. (The user's smtp email folders are stored in their home directories, except for the Inbox, which is stored in /var/mail).

The Third Line of Defense

The third component is custom configuration of virus scanning software to thoroughly scan email attachments on the personal computer. Refer to your software's instruction manual or website for customization instructions. McAfee 4.03 does NOT automatically

install email scanning for Internet mail. It must be done manually. This is addressed in McAfee 4.5 and higher.

"NOTE: The installation procedure outlined in the VirusScan User's Guide has changed. To install the VShield modules responsible for scanning your POP or SMTP Internet mail, for scanning your corporate cc:Mail system, or for filtering harmful ActiveX or Java objects and dangerous Internet sites, you must choose the Custom Installation option and select each of these components. The Typical or Compact installation will, however, install the VShield component responsible for scanning your MAPI-based email systems."[xlv]

In a nutshell, on the Setup Type screen, you must **click on the Custom radio button.** Click on Next. In addition to the three checked options, put a check in the box next to **McAfee WebScanX**.

These instructions for configuring McAfee 4.03 to scan Internet email are available on the McAfee on-line answer center:

"Clean Installation Instructions for McAfee VirusScan 4.0.3

1. Click the Next button on the Welcome to Setup screen.
2. Click the Yes button on the Network Associates Software License Agreement screen.
   NOTE: If a previous version of VirusScan is currently on the computer a screen will appear asking to remove the installed version. Click Remove to continue.
3. A screen will appear titled Setup Type. **Click on the Custom radio button.**
4. Click on Next.
5. In addition to the four options that are checked, put a check in the box next to McAfee WebScanX.
6. Click the Next button on the next four screens.
7. After the scan of system area is complete click on OK.
8. If you have already created an Emergency Disk click Cancel, otherwise, continue on with the Emergency Disk Creation Wizard.
9. Click on Yes or No at the What's New in McAfee VirusScan window.
10. Click the Next button.

Click on Finish to restart the computer.

Configure Download Scan and E-Mail Scan

1. Right-click on the VShield icon on the taskbar. The VShield icon will look like a red V surrounded by a blue shield.
2. A pop-up menu will appear.
3. Highlight Properties then click on Download Scan.

4. The Download Scan Properties dialog box will then appear.
5. Make sure the "Enable internet download scanning" checkbox is checked.
6. On the left side of the screen click on the E-Mail Scan icon.
7. Put a check in the "Enable scanning of email attachments" checkbox.
8. If you are using a standard Internet email program such as Microsoft Outlook Express or Netscape put a check mark in the "Internet Mail" Checkbox.
9. If you are running on a network that uses a Microsoft Exchange email server then put a check mark in the "Microsoft Exchange (MAPI)" checkbox. Otherwise, leave this box unchecked." [xlvi]

To have the program automatically update, you must perform some additional steps not outlined in the installation document on the McAfee Center:

1. Click Start
2. Click Programs
3. Click McAfee Viruscan
4. Click McAfeeViruscan Scheduler
5. Right click AutoUpdate
6. Click Properties
7. Click Configure
8. Click the folder Tab named Schedule
9. Check the Enable box
10. Click Daily
11. Click Randomize within 1 hour.
12. Click OK
13. Right click AutoUpgrade
14. Click Properties
15. Click Configure
16. Click the folder Tab named Schedule
17. Click the Enable box
18. Click Daily
19. Click Randomize within 1 hour.
20. Click OK
21. Close the window.

You're still not quite done. It you want to enable the heuristic scanning technology for possible, yet unknown viruses, you must complete some more steps. You'll need McAfee version 4.5 or higher.

"VirusScan's heuristic scanning technology evaluates the probability that a file or a macro might be infected by a new, unidentified virus. You can choose to use heuristic scanning to look for file-infecting viruses, macro viruses, or both." [xlvii]

To enable heuristic scanning of email.

1. Right click on the Virus Shield icon in the taskbar.
2. Click Properties
3. Click Email scan
4. In the Detection Tab, Click Advanced
5. Click the box "Enable Heuristics Sacnning"
6. Click the radio button "Enable Macro and Program file heuristics scanning.
7. Click OK.

To enable heuristic scanning of downloaded files:

8. Right click on the Virus Shield icon in the taskbar.
9. Click Properties
10. Click Email scan
11. In the Detection Tab, Click Advanced
12. Click the box "Enable Heuristics Scanning"
13. Click the radio button "Enable Macro and Program file heuristics scanning.
14. Click OK.

To enable heuristic scanning of system (inbound and outbound) files:

15. Right click on the Virus Shield icon in the taskbar.
16. Click Properties
17. Click System Scan.
18. In the Detection Tab, Click Advanced
19. Click the box "Enable Heuristics Scanning"
20. Click the radio button "Enable Macro and Program file heuristics scanning.
21. Click OK.

Be advised that heuristics scanning, particularly on System files, can degrade system performance. Enabling heuristics scanning on email and downloads has less of an impact on overall system performance, and is usually acceptable.

Conclusion:

It is imperative that the anti-virus scanning software stays up to date, and that other protective measures are followed.[xlviii] Manual updating of virus definitions in these times of fast proliferating viruses is no longer a viable option, and neither is relying on users to manually update their PCs. A multi level strategy is needed, including scanning mail traffic entering the local network using a gateway virus scanner that automatically downloads virus updates, as well as custom configuration of virus scanning software to

scan all email attachments on the personal computer, also configured for automatic updates. Heuristic scanning methods should also be used to stop malicious code before a specific virus is identified.

It appears that some Anti-Virus companies have gotten the message.

"Sophos plc. And McAfee Security, a division of Network Associates Inc., are taking different approaches to the problem of signature propagation but have one similarity: hands-off automation for network operators."[xlix]

The companies are taking different approaches. Sophos will write small updates for signatures to push to MailMonitor as soon as new viruses hit the Internet. Code to block messages containing certain text strings or subject lines for example. This will be combined with automated distribution of signatures and software updates. McAfee is offering improved peer-to-peer signature delivery. McAfee's design delivers small numbers of updates to certain machines in an organization, and these machines propagate to the rest of the organization's machines. McAfee will also offer automated distribution of virus signatures.

The McAfee approach should streamline the update process, rather than have all the machines in an organization trying to download the update from the McAfee site, and using up the organizations' Internet bandwidth. In either case, it is a step in the right direction.

---

[i] Rupley, Sebastian. "Top Ten Viruses of 2001." eWeek, January 1, 2002. URL: http://www.eweek.com/article/0,3658,s=712&a=20526,00.asp (March 4, 2002).
[ii] Krebs, Brian. "Computer Virus Infections Continue to Climb – Report." Newsbytes –The Washington Post, March 4, 2002. URL: http://www.newsbytes.com/news/02/174942.html (March 5, 2002).
[iii] Lemos, Robert. "Year of the Worm." March 15, 2001. URL: http://news.com.com/2009-1001-254061.html (March 13, 2002).
[iv] Kehoe, Brendan P. "Zen and the Art of the Internet." January 1992. URL: http://www.cs.indiana.edu/docproject/zen/zen-1.0_10.html#SEC91 (March 9, 2002)
[v] General Accounting Office. "Computer Security - Virus Highlights Need for improved Internet Management." June 1989. URL: http://www.worm.net/GAO-rpt.txt (March 12, 2002).
[vi] Fisher, Dennis. "Living with Worms, Viruses and Daily Security." EWeek. February 11, 2002. URL: http://www.eweek.com/article/0,3658,s=712&a=22612,00.asp (March 5, 2002).
[vii] Fisher, Dennis. "Viruses to Continue Their Assault on Net." eWeek, January 2, 2002. URL: http://www.eweek.com/article/0,3658,s=712&a=20523,00.asp (March 5, 2002).
[viii] CERT. "CERT® Advisory CA-1999-04 Melissa Macro Virus." March 27, 1999. URL: http://www.cert.org/advisories/CA-1999-04.html (March 13, 2002).
[ix] CERT. "CERT® Advisory CA-2000-04 Love Letter Worm" March 4, 2000. URL: http://www.cert.org/advisories/CA-2000-04.html (March 13, 2002).
[x] CERT. "CERT® Incident Note IN-2000-07. Exploitation of Hidden File Extensions." (June 19, 2000). URL: http://www.cert.org/incident_notes/IN-2000-07.html (March 13, 2002).
[xi] CERT. "CERT® Coordination Center Fights Love Letter Virus." May 4, 2000. URL: http://www.cert.org/about/loveletter5-2000.html (March 13, 2002).

[xii]Sophos Support. "Disabling Windows Scripting Host." URL: http://www.sophos.com/support/faqs/wsh.html (March 13, 2002).
[xiii] Computer Associates. COMPUTER ASSOCIATES RELEASES TOP 10 VIRUS LIST FOR 2001, WARNS OF INCREASINGLY COMPLEX THREATS IN 2002. December 27, 2001. URL: http://www3.ca.com/press/pressrelease.asp?id=1856 (March 13, 2002).
[xiv] CERT. "CERT® Incident Note IN-2001-14. W32/BadTrans Worm." November 27, 2001. URL: http://www.cert.org/incident_notes/IN-2001-14.html (March 13, 2002).
[xv]CERT. "Vulnerability Note VU#980499. Certain MIME types can cause Internet Explorer to execute arbitrary code when rendering HTML." March 29, 2001. URL: http://www.kb.cert.org/vuls/id/980499 (March 14, 2002).
[xvi]CERT. "CERT® Advisory CA-2001-22. W32/Sircam Malicious Code. July 25, 2001. URL: http://www.cert.org/advisories/CA-2001-22.html (March 13, 2002).
[xvii] CERT. "CERT® Incident Note IN-2000-07. Exploitation of Hidden File Extensions." July 27, 2000. URL: http://www.cert.org/incident_notes/IN-2000-07.html (March 14, 2002.)
[xviii] Message Labs. http://www.messagelabs.com/viruseye/ (March 13, 2002).
[xix]Kaspersky Labs. "I-Worm.Magistr." URL: http://www.viruslist.com/eng/viruslist.asp?id=4170&key=00001000130000100067 (March 12, 2002).
[xx]CERT. CERT® Incident Note IN-2001-02. Open mail relays used to deliver "Hybris Worm"" March 2, 2001. URL: http://www.cert.org/incident_notes/IN-2001-02.html (March 13, 2002).
[xxi] Computer Associates Virus Information Center. URL: http://www3.ca.com/Virus/Virus.asp?ID=9769 (March 13, 2002).
[xxii] CERT. "CERT® Advisory CA-2001-03. VBS/OnTheFly (Anna Kournikova)." February 12, 2001. URL: http://www.cert.org/advisories/CA-2001-03.html (March 13, 2002).
[xxiii]CERT. CERT® Incident Note IN-2001-15. W32/Goner Worm." URL: http://www.cert.org/incident_notes/IN-2001-15.html (March 13, 2002).
[xxiv]CERT. CERT® Advisory CA-2001-26. Nimda Worm. September 18, 2001. URL: http://www.cert.org/advisories/CA-2001-26.html (March 12, 2002).
[xxv] CERT. CERT® Advisory CA-2001-06. Automatic Execution of Embedded MIME Types." April 3, 2001. URL: http://www.cert.org/advisories/CA-2001-06.html (March 12, 2002).
[xxvi]Microsoft Tech Net. "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment." March 29, 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp (March 13, 2002).
[xxvii]Hackman, Mark. "GIBB Virus Poses as Microsoft Email." EWeek. March 8, 2002. URL: http://www.eweek.com/article/0,3658,s=712&a=23792,00.asp (March 13, 2002).
[xxviii]CERT. "CERT® Incident Note IN-2002-02. W32/Gibe Malicious Code" (March 12, 2002). URL: http://www.cert.org/incident_notes/IN-2002-02.html (March 13, 2002).
[xxix] Network Associates, Inc., URL: http://vil.nai.com/vil/content/v_99199.htm (March 4, 2002).
[xxx] Symantec Corporation, URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.magistr.39921@mm.html (March 4, 2002).
[xxxi] Kaspersky Labs, URL: http://www.viruslist.com/eng/index.html?tnews=1001&id=1198 (March 4, 2002).
[xxxii] Kaspersky Labs, URL: http://www.viruslist.com/eng/viruslist.asp?id=4170&key=00001000130000100067 (March 4, 2002).
[xxxiii] Gilley, Daniel and the staff of O'Reilly & Associates, Inc. Unix in a Nutshell – System V Edition. Sebastopol: O'Reilly & Associates, Inc., 1994.
[xxxiv] CERT. "Recovering from an Incident" November 28, 2001. URL: http://www.cert.org/nav/recovering.html (March 13, 2002).
[xxxv] McAfee Security. URL: http://www.mcafeeb2b.com/products/internet-gateway-protection.asp (March 4, 2002).
[xxxvi] McAfee Security. URL: http://www.mcafeeb2b.com/products/webshield-solaris/default.asp (March 4, 2002).

[xxxvii]CERT. "Computer Virus Resources." URL: http://www.cert.org/other_sources/viruses.html (March 14, 2002).
[xxxviii] Sophos. URL: http://www.sophos.com/products/software/mailmonitor/ (March 13, 2002).
[xxxix] Kaspersky Labs. URL: http://www.kaspersky.com/products.html (March 13, 2002).
[xl]Panda Software. URL: http://www.pandasoftware.com/ (March 13, 2002).
[xli] Symantec Corp. URL: http://enterprisesecurity.symantec.com/products/products.cfm?productid=64&PID=na&EID=0 (March 13, 2002).
[xlii] Trend Micro Corp. URL: http://www.antivirus.com/products/internet_gateway.htm (March 13, 2002)
[xliii] McAfee Security. URL: http://www.mcafeeb2b.com/products/file-server-protection.asp (March 13, 2002).
[xliv] Samba.org. URL: http://www.samba.org/ (March 13, 2002).
[xlv] McAfee Viruscan Documentation. Version 4.0.3 Whatsnew.txt.
[xlvi] McAfee Answer Center. http://www.mcafeehelp.com/ (March 12, 2002).
[xlvii] McAfee Viruscan Documentation. Version 4.03 Whatsnew.txt.
[xlviii] CERT. "Protecting Yourself from Email-borne Viruses and Other Malicious Code During Y2K and Beyond." December 28, 1999. URL: http://www.cert.org/tech_tips/virusprotection.html#III (March 13, 2002).
[xlix] Fisher, Dennis. "Anti-virus Makers Pushing Automation" eWeek, March 4, 2002. URL: http://www.eweek.com/article/0,3658,s=712&a=23496,00.asp (March 4, 2002).

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS