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
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Securing Microsoft Outlook by Dain Mullins

I was on the expressway, heading home from the office, when my heart actually stopped beating for a nanosecond. No, it wasn't the tourist in front of me slamming on the brakes. It was actually the radio, more specifically, the voice coming out of the radio. When I heard the name Anna Kournikova my ears perked up because I had actually received an email earlier that day that had *something* to do with the Russian tennis player. The reason my heart stopped was because I could not remember what I did with that email.

Did I open it? Did I forward it to my home email address? Hmmm. Did I infect my company's network? Oh no! Will I have a job tomorrow?

The reason that my heart started to pump again only a nanosecond later, was that I quickly remembered that I had taken a few minutes just the day before to make some network administrator *recommended* configuration changes to the Microsoft Outlook client that I use at work. I remember Don, the administrator saying that the changes would protect me from launching a worm but I was more worried that it would prevent me from receiving any more attachments. I had no intentions of giving up the funny little animations and movie clips that somehow turned up in my inbox each day! Don assured me that I wouldn't miss a single one, so I took him at his word.

He told me that Microsoft's Windows 95 or Windows 98 can be found on most of the PC desktops in the world. Everyday more of these computers are being connected to the outside world for both business and pleasure purposes. The use of electronic mail (email) has grown significantly and has become the number one method of exchanging messages worldwide. He said that most corporate workstation users and many at-home PC users find Microsoft Outlook satisfactory for their messaging and scheduling needs. He said they understand that Outlook connects to a mail server somewhere and transfers *out* the messages they wish to send to others and transfers *in* the messages others send them. Beyond that, there is little more, of which the average user of Outlook is aware, he continued.

"If an anti-virus program was loaded on their system when it was purchased, you can be fairly certain that the virus signatures are as old as the original install date." Even though they hear reports of worms and viruses from the customary media outlets and read the "subject lines" of the virus warnings they receive through email, they somehow think that they do not have to worry. They may be thinking, "Who'd want to send a virus to me?" But, the threat is very real. The fact that viruses are now headline news attests to their impact on our culture.

As an example, on Sunday, February 18, 2001, the Cincinnati Enquirer published a report on the ANNAKOURNIKOVA JPEG.VBS (VBS/SST) Internet worm as its front page, headline story. On that same weekend, the United States had to unleash its fighter pilots on Iraq in a continuing effort to maintain peace in the region. The curious thing is that

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

the report on the White House ordered bombing was placed on page six of the first section. Two years ago the worm story would have been lucky to find its home on page six.

I learned from Don that with the prevalence of infected email attachments and malicious code found embedded in the message itself, it is crucial that Outlook is configured in such a way to reduce the chance of getting a virus or worm and helping to propagate it over the Internet. I am offering the reader a chance to learn what I have learned about protecting my workstation and my company network.

The steps we take to secure Outlook will help us guard against viruses, worms and malicious HTML code. The steps involve the application of security related patches released by Microsoft, changing some default Outlook settings, some third-party utilities and some good old common sense.

Outlook Related Security Patches

I choose not to take up space describing all of the Microsoft security patches that pertain to Outlook, nor the step-by-step instructions necessary to install them. This is freely available from The Microsoft website, http://www.microsoft.com. Rather, I choose to address these patches from a different perspective. A perspective of what are some of the items that anyone considering the application of these patches would be wise to remember.

One significant thing to keep in mind when dealing with Microsoft Outlook patches is the fact that many of the files used by Outlook are shared components of Internet Explorer. So, the patches used to correct discovered vulnerabilities may be dependent upon which version in Internet Explorer you are using.

Microsoft released a patch for Outlook 98 and Outlook 2000 (with the Office Service Release 1 update) that disables many of the features that allow VBS/Loveletter and similar viruses to spread so quickly. The new patch makes it impossible to open program files in Outlook -- including VBScript .vbs files like those that spread Loveletter.

This patch will restrict you from opening many types of attachments including executables, batch files, and pcd files. The entire list is at the end of this paper. It will negatively affects many other features such as the Digital Dashboard. Also, when you create a mail merge to e-mail by using your Contacts folder, you receive a warning message which indicates that a program is trying to access your address book. OK. No big deal right? "Then you get a separate warning message for each e-mail message that you send and you must wait five seconds before you can confirm the send process. For example, if you generate a mail merge to e-mail that is being sent to 100 people, it takes over eight minutes and you must approve each of the e-mail messages every five seconds."

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

"There is no Uninstall utility on this patch. The files installed will become an integral part of your operating system and email client, and cannot be removed without risking damage to your operating system."

The main thing to remember is do not install any patches until you read the documentation and understand how it will affect the way you use Outlook. Make certain that those add-ins you have come to rely on will still do the same job for you after you have patched. Plus, it is possible to secure Outlook from the most common threats without patching, patching , patching.

Virus Threats

Enough cannot be said about having an anti-virus program on your PC and keeping the virus definition files current. I update my signature files several times a week.

According to Slipstick.com's Antivirus page, viruses can involve Microsoft Outlook in several ways:

A machine running an older version of Internet Explorer can receive a message from the Internet with a malformed header that either causes Outlook to crash or infects the system with malicious code. **The user does not need to open or preview the message.** Windows 2000 users with IE 5.5 are not protected and should go back to 5.01 SP1. For other operating systems, either IE 5.01 SP1 or IE 5.5 provides protection.

A machine running Outlook can become infected with a virus when a user who has not taken adequate security precautions opens a malicious HTML message or, in Outlook 98, views it in the preview pane. (In Outlook 2000, script on an HTML message cannot run in the preview pane.)

A user opens a virus-infected attachment received via an Outlook e-mail message. We used to think that attachments could never run automatically. However, as the Blebla virus showed, in certain HTML mail messages, attachments can run automatically if you are not properly protected.

Safeguarding Against VBS Email Worms

VBS or Visual Basic Script is often used to launch email worms. Because of Outlook's easy-to-use programming model, viruses can propagate themselves by using VBS to read the Outlook address books and send new virus-infected messages to everyone found there. These worms can be extra tricky to defeat because they seemingly come from a relative, friend or acquaintance.

These are the things that we need to do to help protect ourselves from VBS driven viruses. We want to disable Windows Script Hosting, change some default Outlook settings that open new emails automatically, turn off the preview panes in Outlook and modify a "file types" setting.

.1) To disable Windows Scripting Host

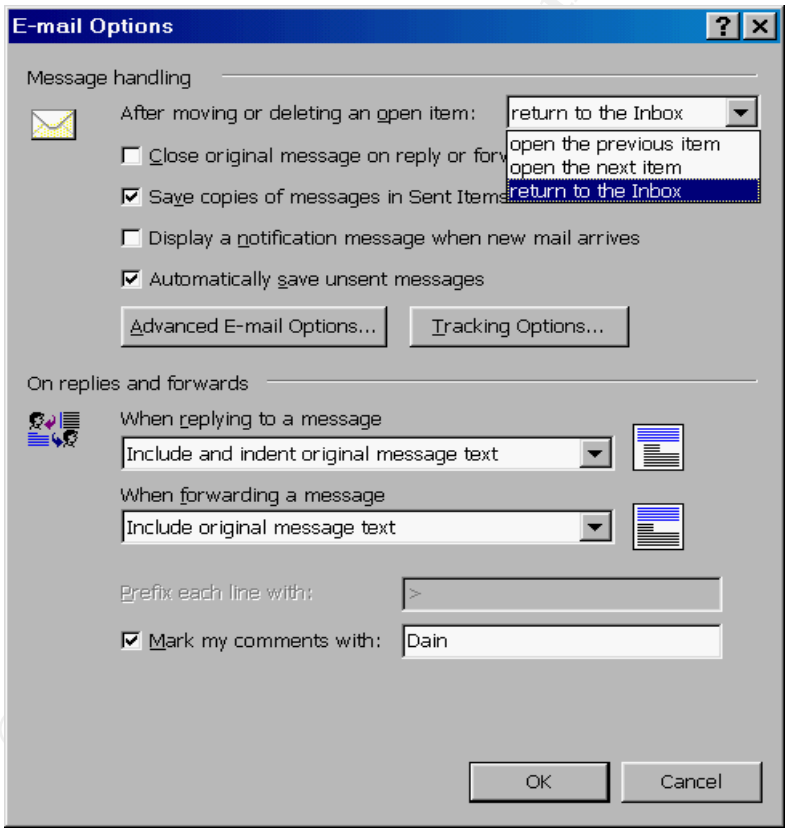
A) Open the Control Panel -> Click START, SETTINGS and CONTROL PANEL
B) Double-click the icon that reads ADD/REMOVE PROGRAMS

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

C) Click the tab that reads WINDOWS SETUP
D) In the components window, click ACCESSORIES
E) Scroll to the bottom of the Accessories components window and make sure that WINDOWS SCRIPTING HOST is not checked. If it is, click the box to remove the check mark.
F) Click OK twice and close Control Panel

2) To change the setting that opens the next unread email as you move or delete a new email:

A) Open Outlook
B) On the toolbar, find TOOLS and click it.
C) On the drop down menu, find OPTIONS and click it. It opens the OPTIONS dialog box on the PREFERENCES tab. Right where we want to be.
D) Click the button that says E-MAIL OPTIONS...
E) Under MESSAGE HANDLING, the first line (After moving ...) needs to be modified.
F) Click the down arrow and select RETURN TO THE INBOX as shown here:



G) Next, remove the check from DISPLAY A NOTIFICATION MESSAGE WHEN NEW MAIL ARRIVES
H) Click OK two times to return to Outlook.

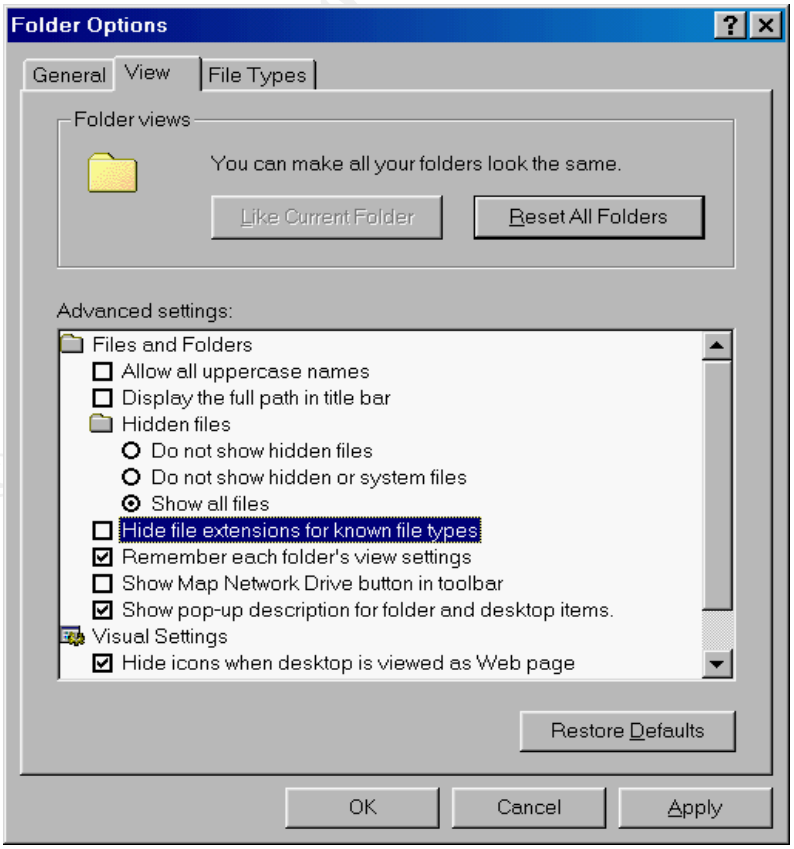
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3) To turn off Outlook's Preview Pane:

A) Open Outlook
B) Find VIEW on the toolbar and click it.
C) In the drop down menu, locate PREVIEW PANE and AUTO PREVIEW
D) If either or both of these are engaged, the icon next to their label will be depressed. If depressed, click it to disengage. Do this for both PREVIEW and AUTO PREVIEW.
E) You can install Chilton Preview on your Windows 98 PC which will preview your mail without activating any Visual Basic Scripts or HTML. Chilton Preview does not leave you vulnerable to a malicious HTML mail message. Note that Outlook 2000 never runs a script from HTML messages in the built-in preview pane. Download it from http://www.slipstick.com/files/chilton.zip.

4) Finally, let's make sure that your file associations are being properly displayed. By default, Windows hides file extensions for known file types. Since .VBS is a known file type, the worm ANNAKOURNIKOVA.JPEG.VBS is displayed as ANNAKOURNIKOVA.JPEG. We want it to be displayed with the .VBS extension so we recognize it for what it really is, a VB script, not a JPEG (image file).

A) Click START / SETTINGS / FOLDER OPTIONS
B) Click the VIEW tab
C) Under FILES AND FOLDERS, locate HIDE FILE EXTENSIONS FOR KNOWN FILE TYPES.



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

D) If there is a check mark in the box, remove it and click OK. If there is no check mark, click OK.

Back On The Highway

As I pulled off at my exit, I recalled Don saying it would only take a few minutes to make the changes in Outlook and he was right. It is surely better to take some time to do a little preventative maintenance now, than to have to pick up the pieces after one of these viruses hit you. Now that my heart has returned to its regular beating pattern, I can concentrate on getting around the tourist in front of me.

Resources

http://officeupdate.microsoft.com/2000/articles/olMalformedHeader.htm
Author's name and date is not stated with article

http://www.slipstick.com/antivirus.htm
Author's name and date is not stated with article

http://www.myhelpdesk.com/Jumpoff/Jump.asp?Fid=0&JumpTo=http://officeupdate.microsoft.com/downloadDetails/outptch2.htm
Author's name and date is not stated with article

Vamosi, Robert "Basic Steps to protect your PC from viruses"
http://www.zdnet.com/zdhelp/stories/main/0,5594,2425285,00.html

Stewart, Bruce "How to Protect Against Computer Viruses"
http://www.zdnet.com/zdhelp/stories/main/0,5594,2248291,00.html

http://www.ca.com/virusinfo/faq.htm
Author's name and date is not stated with article

Morris, Evan "Update to A Viral Survival Checklist" June 2000
http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=8778

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

Attachment Security

Systems running this patch will no longer be able to open or save the following types of files if they are attached to an Outlook message. The attachments will still be in the messages, and other programs or Outlook add-ins may be able to access them, but they will be invisible to Outlook itself.
If you try to forward a message containing one of these files, Outlook strips the attachment from the forwarded copy.

File extension	File type
.ade	Microsoft Access project extension
.adp	Microsoft Access project
.bas	Visual Basic class module
.bat	Batch file
.chm	Compiled HTML Help file
.cmd	Windows NT Command script
.com	MS-DOS program
.cpl	Control Panel extension
.crt	Security certificate
.exe	Program
.hlp	Help file
.hta	HTML program
.inf	Setup Information
.ins	Internet Naming Service
.isp	Internet Communication settings
.js	JScript Script file
.jse	Jscript Encoded Script file
.lnk	Shortcut
.mdb	Microsoft Access program
.mde	Microsoft Access MDE database
.msc	Microsoft Common Console document
.msi	Windows Installer package
.msp	Windows Installer patch
.mst	Visual Test source files
.pcd	Photo CD image
.pif	Shortcut to MS-DOS program
.reg	Registration entries
.scr	Screen saver
.sct	Windows Script Component
.shb	Shell Scrap Object
.shs	Shell Scrap Object
.url	Internet shortcut
.vb	VBScript file
.vbe	VBScript encoded script file
.vbs	Visual Basic Script file
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Script Host Settings file

Source: www.microsoft.com

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

Last Updated: April 30th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS