



December 2000

Issue 7

## Inside This Issue

- 1** Be Aware of Christmas Virus
- 2** Safe Computing Guide
- 7** Alert
- 11** Top News
- 12** Calendar of Events

Published by  
Hong Kong Productivity Council  
Information Technology Division

Sponsored by Innovation & Technology Fund

# HKPC SECURITY BULLETIN

## Be Aware of Christmas Virus

You must receive a lot of e-cards as Christmas is coming. However, please be careful when you open these e-cards because the virus may come as an attachment in it.



When approaching the holidays, new viruses developed on Internet are found and they disguise themselves as Christmas or News Years greetings. W32.Navidad, W32.Music and VBS.JeanA@mm are the examples.

Below list the information of viruses for your reference:

Virus	Description	Payload
<b>W32.Music</b>	A worm that runs only on Windows 95 and Windows 98 systems	<ul style="list-style-type: none"><li>• Modify window registry</li><li>• Sends email according to address book</li></ul>
<b>VBS.JeanA@mm</b>	A worm spreads via Microsoft Outlook.	Opens Microsoft Outlook and sends itself to up to 50 recipients in the address book of the infected user.
<b>W97M/PRILISSA</b>	An auto spammer and spreads quickly by using the Microsoft Outlook	<ul style="list-style-type: none"><li>• sends an email to address list in Outlook</li><li>• Format Hard Disk</li></ul>
<b>W32/NAVIDAD.A</b>	E-mail worm which spreads through (Microsoft Messaging API)MAPI Outlook	<ul style="list-style-type: none"><li>• No EXE files could be started and;</li><li>• Mass Mailing may hang the mail server</li></ul>
<b>W32/BELEBA.B</b>	An Internet worm which implements an I-Frame exploit in HTML in order to run and propagate.	Retrieve all of the e-mail addresses from within the Windows Address Book and creates a new message to send to each address
<b>W32HYBRIS</b>	E-mail worm contains components in its code and these components can be upgraded from an Internet Web site	Mass Mailing may hang the mail server
<b>W32/PROLIN</b>	The worm sends a copy of itself "CREATIVE.EXE" as the attachment to everyone in the Outlook address book	Moves all the JPG and ZIP files to the root directory and renames each of these files.

# Safe Computing Guide

At the moment, your system is connected to a network and/or to the Internet, you are probably benefiting from productivity- and life-enhancing information access services. Sending and receiving emails, chatting online with friends, surfing the Internet via web browsers, and downloading data or program files are a few of the most common activities that also expose systems to malicious code threats like computer viruses and Trojans.

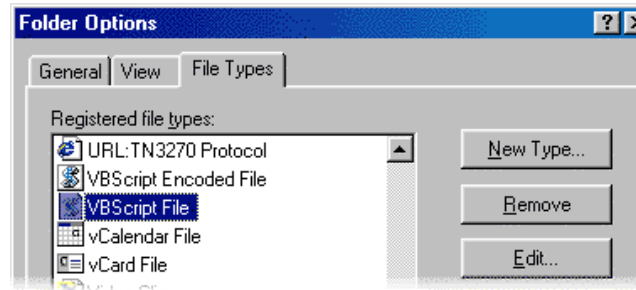
The power of today's computer can as easily access useful information as make you the dupe of viruses that hide in email attachments. It is too easy to inadvertently trigger today's sophisticated viruses that will immediately mass-mail themselves out to, and infect all your friends', customers and colleagues' computers. The real-world global virus outbreaks like W97M\_Melissa, VBS\_Loveletter (a.k.a. LoveBug), VBS\_Fireburn, W97M\_Resume and VBS\_Newlove have shown how effective malicious code technology can be. There are more than 50,000 viruses today, new viruses come out daily, any of them could be the next LoveBug virus!

To reduce the risk of virus infections, and of inadvertently triggering or spreading them to other people, Trend Micro would like to share some easily implemented "safe computing" practices. Put these into effect on your machine today and they will help keep you using today's advanced computer information access technology without falling prey to viruses and other malicious code!

To make your system more robust, follow these practices outlined below to set up and configure your system. The general idea is to make it difficult or impossible for viruses to run.

## Disable the Windows Scripting Host Functionality

This is to prevent Visual Basic script viruses like VBS\_LoveLetter from running, so that they cannot activate, spread or cause damage to files. A typical PC does not need Windows Scripting Host (WSH) to function normally. You can always change your mind later and reinstall WSH by repeating these steps and re-selecting "Window Scripting Host" checkbox.



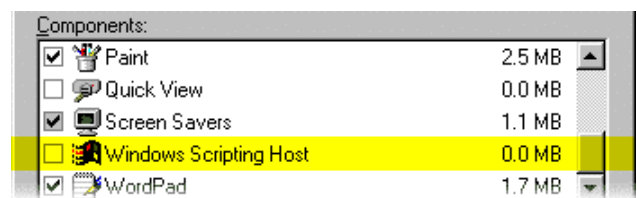
### Windows 98 systems

WSH is installed by default when you install Windows 98 or Internet Explorer 5. To prevent scripts (or .VBS files) from running:

- Open the Control Panel by selecting "Start", "Settings" and then "Control Panel".
- Double click on "Add/Remove Programs"
- Select the "Windows Setup" tab



- Double-click on "Accessories"
- Unmark the "Windows Scripting Host"
- Click the "OK" button



### Windows 95 Systems

Windows 95 systems do not come with the Windows Scripting Host. However, the WSH is installed automatically when you install Internet Explorer 5 or above. To disable scripts (with the extension, .VBS) from running on Windows 95 systems:

- Start "Windows Explorer"  
(To do this, select "Start", "Programs" and then "Windows Explorer". Please note, this is not the same as Internet Explorer.)

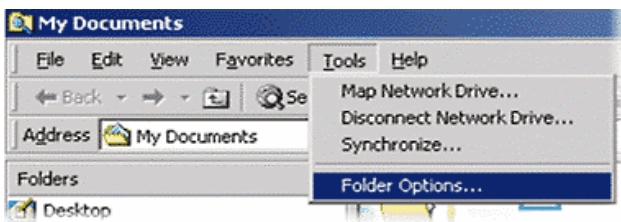
- b. Select "View" then select "Option"
- c. Select the "File Types" tab
- d. Search and select "VBScript Script File"
- e. Click "Delete" and then confirm the removal by selecting "Yes"

**Windows 2000 Systems**

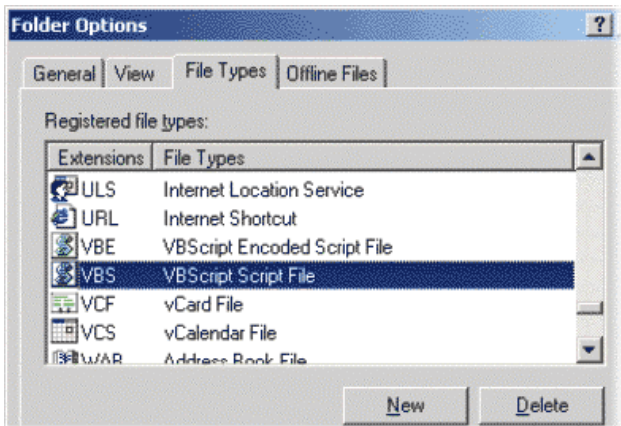
The Windows Scripting Host is installed by default on Windows 2000 systems.

To disable scripts (with the extension .VBS) from running on Windows 2000 systems:

- a. Start Windows Explorer
- b. Select "Tools" then "Folder Options"



- c. Select the "File Types" tab
- d. Search and Select "VBScript Script File"
- e. Click "Delete" and then confirm the removal by selecting "Yes"

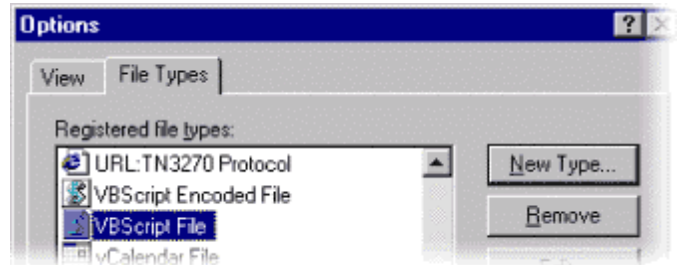
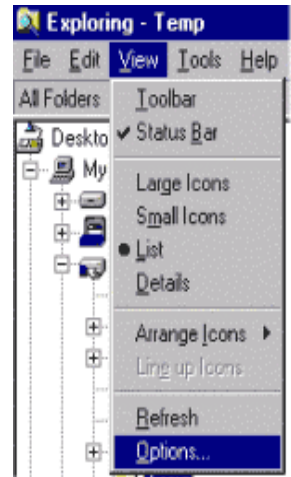


**Windows NT 4 Systems**

Windows NT 4 systems do not come with the Windows Scripting Host. However, the WSH is installed automatically when you install Internet Explorer 5 or above.

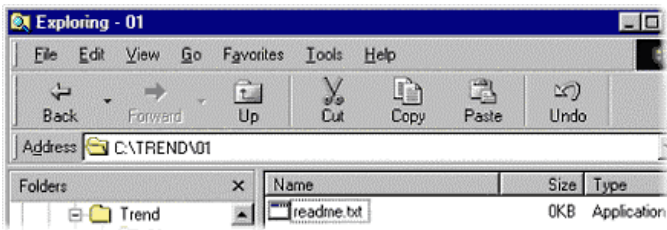
To disable scripts (with the extension .vbs) from running on Windows NT 4 systems:

- a. Log on with Administrator's right
- b. Start Windows Explorer
- c. Select "View" and then "Options"
- d. Select the "File Types" tab
- e. Search and Select "VBScript File"
- f. Click "Remove" and then confirm the removal by selecting "Yes"



**Do Not Hide File Extensions of Known File Types**

All Windows operating systems, by default, hide the known file extensions in Windows Explorer. This feature can be used by virus writers and hackers to disguise malicious programs as some other file formats, such as text, video or audio files. For example, a malicious program file named "readme.txt.exe" is displayed as "readme.txt" in Windows Explorer (see illustration below). Therefore users are often tricked into clicking the "text" file and then into inadvertently running the malicious file.



To avoid this confusion, you are recommended to change the Windows Explorer setting to "Not hide the File Extension of known File Types." This can be achieved by clicking on one of the following files, and saving it to your local hard drive, then double-clicking on the file to run:

**Windows 95, 98 and NT 4 users:**



NotHideFileExt\_Win9598NT4.reg

**Windows 2000 users:**



NotHideFileExt\_Win2000.reg

Afterwards, files will be displayed with the complete file extension as shown:



**Important Notice:** There are still some file extensions, which the Windows operating system will always hide, such as the shell scrap files with the extension .shs.

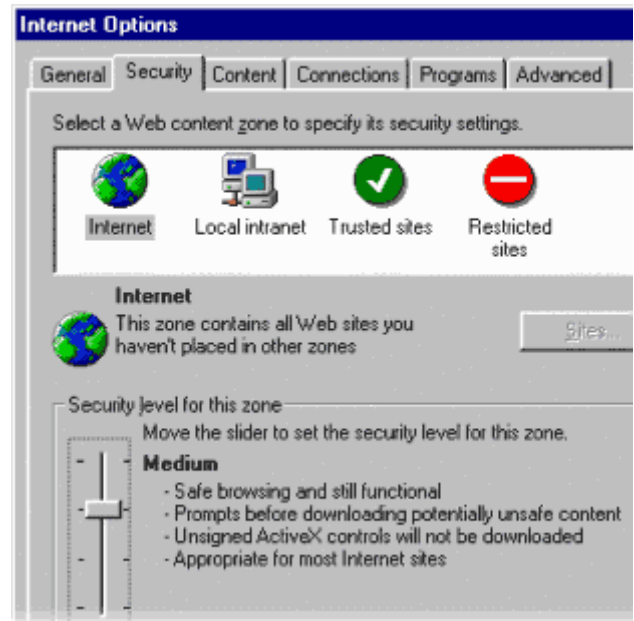
## Set Internet Explorer Security to at Least "Medium"

By default, the Internet Explorer Security Setting is set to "Medium." However, Trend has seen many systems

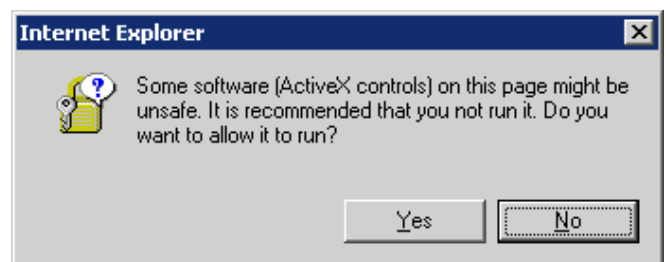
where the security system was changed to "Low" by a virus, Trojan, or hacker.

In this regard, we encourage every user to ensure that their security setting is set to at least "Medium", as this will reduce the risk of accidentally running a malicious file.

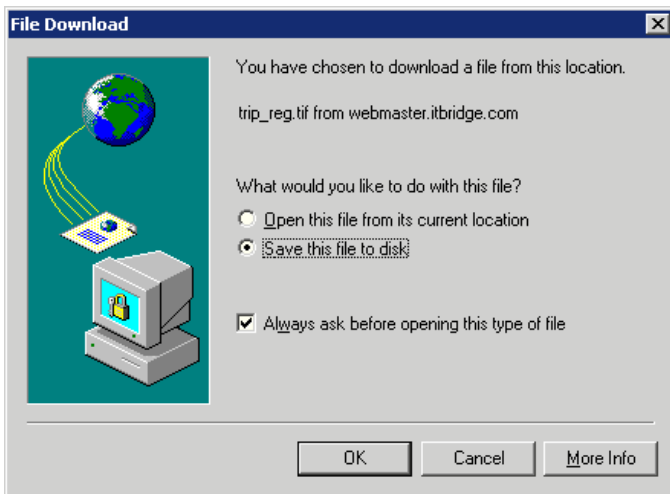
At the "Medium" security level, Internet Explorer 5 will prompt users before running potentially unsafe content.



Internet Explorer 5 or above will also display a warning message before running any Active-X controls (as shown on the picture below).



We also advise that users always save files to the local hard drive and then scan them with an up-to-date antivirus product. If you don't have an antivirus product or your product is out of date, please feel free to use Trend Micro's free on-line scanner HouseCall at <http://housecall.antivirus.com>



To automatically change the Internet Explorer 5 Security Setting to "Medium", please run the following registry file:



### Require a Prompt Before Opening Mail Attachments

(applies to Microsoft Outlook and Outlook Express users)

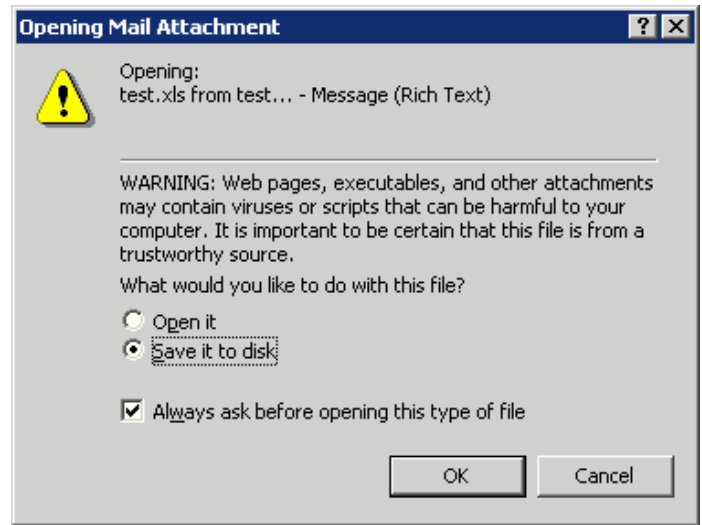
We have seen many viruses activate because users were double-clicking on incoming email file attachments. In this regard, we advise that Internet users save files to the local hard drive and then scan them with an up to date antivirus product (instead of double-clicking over the incoming email file attachments).

To ensure that your system automatically prompts you to save files, please click on the file below, and save it to your local hard drive, then double-click on the file to run:



Afterwards, your system will prompt you with a warning even if you accidentally click on an email attachment or read an email that has some embedded scripts. This

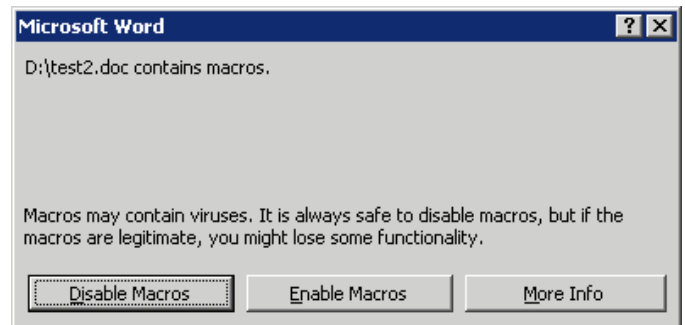
registry fix applies to Word documents, Excel sheets, Excel charts, PowerPoint files and HTML files.



### Enable Macro-virus Warning in MS Office 97 & 2000

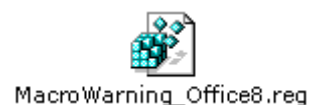
(applies to Office 97 and 2000 users)

By default, Microsoft Office products display a macro warning before Office documents are opened that contain macros.



However, many of the known macro viruses disable this setting to avoid being detected. To ensure that you have the macro warning enabled, please click on one of the following files below, and save it to your local hard drive, then double-click on the file to run:

Microsoft Office 97 (a.k.a. Office 8.0) users:



Microsoft Office 2000 (a.k.a. Office 9.0) users:



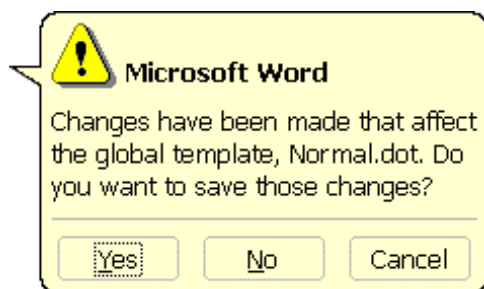
MacroWarning\_Office9.reg

If you are not sure if macro content that you encounter is safe, we advise to use the "Disable Macros" option.

## Prompt Before Saving Changes to the Global Template

(normal.dot - applies to Word 97 and Word 2000 users)

Since almost all macro viruses attempt to modify the global template (normal.dot) before closing the active Microsoft Word session, we advise everyone to make sure that Microsoft Word will prompt before any changes are being made.



While this action will not stop all macro viruses, it will help to identify potential malicious code.

If you are not sure what to do, select the "No" option and email a copy of such files to Trend Micro's virus doctors at [virus\\_doctor@trendmicro.com](mailto:virus_doctor@trendmicro.com). They will inspect suspicious files or documents to determine if they contain malicious macros. To automatically make the change to Word 97 or Word 2000, please click on one of the following files below, and save it to your local hard drive, then double-click on the file to run:

Word 97 (a.k.a. Word 8.0) users:



TmplateSavePrompt\_W8.reg

Word 2000 (a.k.a. Word 9.0) users:



TmplateSavePrompt\_W9.reg

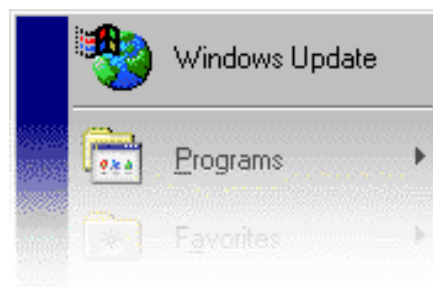
## Apply All the Latest Microsoft Security Updates

In order to close security holes that have been discovered since Windows was shipped and installed, we advise everyone to visit the Microsoft Update Website at <http://windowsupdate.microsoft.com>.

Please follow the on-line instructions on how to update your system. Security updates will help prevent hackers from accessing your system and prevent viruses from running on your system.

Windows 98 or Windows 2000 users can also use the Windows Update feature to get all the latest security updates.

Simply click "Start" and then select "Windows Update"



## Conclusions:

Safe Computing Practices mainly make it more difficult for malicious code to enter or execute on client systems. Nevertheless, the recommended safe computing practices are not intended to replace currently updated antivirus software.

Users whose systems have been attacked by viruses or Trojans can tell stories about what a hassle they can be at minimum – or about the important data they may have lost. In general, most viruses are mere nuisances, but every once in a while a new virus comes along that uses a new technique and causes major computer problems or threatens data or data security.

These Safe Computing Practices will add a protective layer of defense to prevent viruses from running inadvertently. ☺

Re-printed from Trend Marco. Incorporated.

**ALERT**

Date / Source	Common Name	Operating System / Vendor / Platform	Vulnerability System	Impact	Patches / Workarounds / Solutions (Please check instructions carefully on related web site before applying the solutions)
<b>Virus</b>					
2000/11/01	Sonic	Microsoft Windows	Microsoft Windows	<ul style="list-style-type: none"> <li>* It sends copies of itself via email and</li> <li>* The backdoor contains several task such as               <ul style="list-style-type: none"> <li>- Download/Upload files.</li> <li>- Get/Set server info.</li> <li>- Kill the server program.</li> <li>- Get user and OS info.</li> <li>- Display message.</li> <li>- Get cached passwords.</li> <li>- Capture screen.</li> <li>- List process.</li> <li>- Copy/Move/Delete/Rename /Execute local file.</li> <li>- Get WINDOWS directory.</li> </ul> </li> </ul>	New virus definition is available from anti-virus vendor to detect and remove this worm.
2000/11/13	Win32.Navidad	Microsoft Windows	Microsoft Windows	No EXE files could be started and Mass Mailing may hang the mail server	New virus definition is available from anti-virus vendor to detect and remove this worm.
2000/12/02	W32.Prolin.Worm	Microsoft Windows	Microsoft Windows	<ul style="list-style-type: none"> <li>* Upon executing CREATIVE.EXE, the worm writes a copy of itself to the local system in these folders:               <ul style="list-style-type: none"> <li>-C:\creative.exe</li> <li>-C:\[WINDOWS FOLDER]\TEMP\creative.exe</li> <li>-C:\[WINDOWS FOLDER]\StartMenu\Programs\StartUp\creative.exe</li> </ul> </li> <li>* The worm moves all the JPG and ZIP files to the root directory and renames each of these files by appending the text "change atleast now to LINUX" to the file extensions;</li> <li>* The worm drops a text file into the root directory with the file name: messageforu.txt</li> </ul>	New virus definition is available from anti-virus vendor to detect and remove this worm.

Date / Source	Common Name	Operating System / Vendor / Platform	Vulnerability System	Impact	Patches / Workarounds / Solutions (Please check instructions carefully on related web site before applying the solutions)
<b>Bugs, Holes &amp; Patches</b>					
2000/11/03	"Netmon Protocol Parsing" Vulnerability	Microsoft Windows	Microsoft Windows NT 4.0 Server, Terminal Server Edition, Enterprise Edition, Microsoft Windows 2000 Server, Advanced Server, Datacenter Server, Systems Management Server 1.2 & 2.0	Allow a malicious user to gain control of an affected server.	Apply the patch provided by Microsoft: * Microsoft Windows NT 4.0 Server and Windows NT 4.0 Server, Enterprise Edition: <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25487">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25487</a> * Microsoft Windows NT 4.0 Server, Terminal Server Edition: To be released shortly. * Microsoft Windows 2000 Server, Advanced Server and Datacenter Server: <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25485">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25485</a> * Microsoft Systems Management Server 1.2: <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25505">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25505</a> * Microsoft Systems Management Server 2.0: <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25514">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25514</a>
2000/11/06	"ActiveX Parameter Validation" Vulnerability	Microsoft Windows	Microsoft Windows 2000 Server, Professional, Advanced Server, Datacenter Server	Allow enable a malicious user to potentially run code on another user's machine.	Installation the patch released by Microsoft. <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25532">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25532</a>
2000/11/06	HP-UX dtterm misuse	HP9000 systems	HP9000 systems running HP-UX releases 11.00, 11.04, 10.20, 10.24, and 10.10.	Users can gain unauthorized privileges.	Apply patches as listed below and change permissions where patches are not yet available. <a href="http://itrc.hp.com">http://itrc.hp.com</a>  For HP-UX release 11.00: PHSS_22320, HP-UX release 11.04: PHSS_22548, HP-UX release 10.20: PHSS_22319, and do <code>chmod(1)</code> (below), HP-UX release 10.24: PHSS_22546, HP-UX release 10.10: not yet available, do <code>chmod(1)</code> 's (below).  Until patches are available the vulnerability can be removed by setting the permissions as follows: 10.10: <code>chmod 555 /usr/dt/bin/dtterm</code> <code>chmod 555 /usr/vue/bin/dtterm</code> 10.20 <code>[/usr/dt/bin/dtterm fixed in PHSS_22319]</code> <code>chmod 555 /usr/vue/bin/dtterm</code>

Date / Source	Common Name	Operating System / Vendor / Platform	Vulnerability System	Impact	Patches / Workarounds / Solutions (Please check instructions carefully on related web site before applying the solutions)
2000/11/03	"Indexing Services Cross Site Scripting" Vulnerability	Microsoft Windows	Microsoft Indexing Services for Windows 2000	Allow a malicious web site operator to misuse another web site as a means of attacking users.	Install the patch released by Microsoft.  Microsoft Indexing Services for Windows 2000 <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25517">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25517</a>
2000/11/20	"Exchange User Account" Vulnerability	Microsoft Windows	Microsoft Exchange 2000 Server CDs without "Rev. A" stamped on the CD on the line below the Part No.  Microsoft Exchange 2000 Enterprise Server CDs without "Rev. A" stamped on the CD below the Part No.	Could potentially allow an unauthorized user to remotely login to an Exchange 2000 server and possibly other servers on the affected computer's network.	The Manual procedure can be found from: <a href="http://www.microsoft.com/technet/security/bulletin/fq00-088.asp">http://www.microsoft.com/technet/security/bulletin/fq00-088.asp</a> The Tool can be downloaded from: <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25866">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25866</a>
2000/11/22	"Web Server File Request Parsing" Vulnerability	Microsoft Windows	Microsoft Internet Information Server 4.0 & 5.0	Enable a malicious user to run operating system commands on an affected web server.	Install the patch released by Microsoft.  Internet Information Server 4.0: <a href="http://www.microsoft.com/ntserver/nts/downloads/critical/q277873">http://www.microsoft.com/ntserver/nts/downloads/critical/q277873</a> Internet Information Services 5.0: <a href="http://www.microsoft.com/Windows2000/downloads/critical/q277873">http://www.microsoft.com/Windows2000/downloads/critical/q277873</a>
2000/11/22	"Domain Account Lockout" Vulnerability	Microsoft Windows	Microsoft Windows 2000 Professional, Service Pack 1 Microsoft Windows 2000 Server, Service Pack 1 below the Part No. Microsoft Windows 2000 Advanced Server, Service Pack 1 Microsoft Windows 2000 Datacenter, Service Pack 1	Allow a malicious user to use repeated attempts to guess an account password even if the domain administrator had set an account lockout policy.	Install the patch released by Microsoft.  <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25606">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25606</a>

Date / Source	Common Name	Operating System / Vendor / Platform	Vulnerability System	Impact	Patches / Workarounds / Solutions (Please check instructions carefully on related web site before applying the solutions)
2000/11/24	Red Hat Linux modutils Vulnerability	Red Hat Linux	Red Hat Linux 6.2 - i386, alpha, sparc  Red Hat Linux 6.2EE - i386, alpha, sparc  Red Hat Linux 7.0 - i386 7 Red Hat Linux 7.0J - i386	A local user can, without proper authorization, execute arbitrary code with elevated (root) privileges.	Install the patch released by the software manufacturer. Please visit our web-site for more details. <a href="http://www.hkpc.org/itd/infosecurity">http://www.hkpc.org/itd/infosecurity</a>
2000/11/27	"ASX Buffer Overrun" and "WMS Script Execution" Vulnerability	Microsoft Windows	Microsoft Windows Media Player 6.4  Microsoft Windows Media Player 7  The ".ASX Buffer Overrun" affects Windows Media Player versions 6.4 and 7.  The ".WMS Script Execution" affects only Windows Media Player version 7.	Could potentially enable a malicious user to cause a program of his choice to run on another user's computer.	Install the patch released by Microsoft.  Windows Media Player 6.4: <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26069">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26069</a> Windows Media Player 7: <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26079">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26079</a>
2000/11/30	Red Hat Linux Netscape HTML Buffer Overflow	Red Hat Linux	Red Hat Linux 6.0 (i386, alpha, sparc), 6.1 (i386, alpha, sparc), 6.2 (i386, alpha, sparc), 7.0 (i386, alpha)	Through the execution of arbitrary code a malicious remote website could gain root access.	Install the patch released by the software manufacturer. Please visit our web-site for more details. <a href="http://www.hkpc.org/itd/infosecurity">http://www.hkpc.org/itd/infosecurity</a>
2000/12/01	Multiple Denial-of-Service Problems in ISC BIND	Systems running ISC BIND & name servers derived from BIND	Systems running Internet Software Consortium (ISC) BIND version 8.2 through 8.2.2-P6 Systems running name servers derived from BIND version 8.2 through 8.2.2-P6	Domain name resolution services (DNS) can be disabled on affected servers from arbitrary remote hosts.	Install the patch released by the software manufacturer. Please visit our web-site for more details. <a href="http://www.hkpc.org/itd/infosecurity">http://www.hkpc.org/itd/infosecurity</a>

# TOP NEWS



**November 8, 2000**

## 'Mafiaboy' to plead guilty to hacking major Web sites

The 16-year-old Montreal-area high-school student known as Mafiaboy has agreed to plead guilty to a series of attacks on major Internet sites including CNN.com, Yahoo.com Inc., Amazon.com Inc., eBay.com Inc., Dell.com and others in February, according to prosecutor Louis Miville-Deschenes.

A sentencing hearing was set for Dec. 8. The teenager could face up to two years in prison and a fine of \$1,000 Canadian dollars (approximately U.S.\$650), the prosecutor said. *(from ComputerWorld)* 🗨️

**November 8, 2000**

## The new age of hacktivism

Politicians may not pander to them and experts may discount their opinions, but online vandals are getting the message out about what they think is important: Increasingly, that's politics.

On the eve of the U.S. elections, vandals defaced the home pages of the Republican National Committee, placing a spirited pro-Gore diatribe in its place. The Democratic National Committee said its site was subjected to repeated attacks. *(from ZDNet News)*. 🗨️

**November 10, 2000**

## Christmas virus causes mild clamor on the desktop

The email virus, being called "Navidad," infects Microsoft's Outlook email application, arriving as a reply when a person sends a message to an infected computer. If the attachment, "NAVIDAD.EXE," is run, a message in Spanish reads: "Never press this button." If the button is pressed, a further message reads: "Feliz

Navidad. Unfortunately you have given in to temptation and will lose your computer."

Although the virus has yet to do anything more than pester its victims, an antivirus researcher at security company McAfee.com, said the attachment could bring down a mail system if enough programs are run and are sending out response emails to all the addresses within the system. *(from CNET News.com)* 🗨️

**November 20, 2000**

## Morocco's Government Internet Site Attacked by Hacker

A hacker broke into Morocco's Finance Ministry's Web site for the first time at the weekend but caused no damage, an official said Monday.

Web surfers or potential investors visiting the site at [www.mfie.gov.ma](http://www.mfie.gov.ma) found a message in bad French saying the cover page had been hacked by "NetOperat." The tainted page maintained a link with the ministry's original Internet site stressing the server was not corrupted and invited authorities to protect their system better. *(from Yahoo)*. 🗨️

**November 21, 2000**

## Ms, hacker secretive about meeting

Microsoft last week met with Dimitri, the Dutch hacker who recently mocked the software giant by hacking into one of its Web servers twice within one week.

Earlier this month Dimitri hacked into the same Microsoft Web server twice, the second time after Microsoft had said the security hole was patched.

According to experts it's the first time ever Microsoft has met with somebody who has hacked into a Microsoft Web server. *(from IDG.com)*. 🗨️

**November 28, 2000**

## Yahoo deliver encrypted email

As [first reported](#) in August, Yahoo is providing its email encryption option through a deal with ZixIt, a Dallas-based email encryption company. Yahoo will route

encrypted email through ZixIt's [SecureDelivery.com](http://SecureDelivery.com) Web site.

Yahoo and ZixIt representatives declined to comment on the public availability of the service and would not say whether it was an across-the-board launch or a temporary test. (from *CNET News.com*). ☺

#### November 29, 2000

#### VeriSign, Microsoft unveil XML Net security protocol

Microsoft Corp. and VeriSign Inc. today unveiled an XML-based online security standard aimed at allowing easier integration of digital signatures and encryption for e-commerce.

The protocol, called the XML key management specification (XKMS), uses the relative simplicity of XML to implement two key aspects of secure electronic commerce, according to the companies. (from *ComputerWorld*). ☺

#### December 1, 2000

#### Hacker breaks into Brazilian president's e-mail account

A municipal police officer has been arrested and charged with breaking into the electronic mail account of Brazilian President Fernando Henrique Cardoso and sending messages in his name to other government officials, federal police officials said Thursday. (from *Yahoo*). ☺

#### December 4, 2000

#### NASA hacker pleads guilty

The man accused of breaking into NASA computer systems pleaded guilty Friday in federal court in exchange for a recommendation for a reduced sentence.

The plea agreement recommends a sentence of eight to 14 months. Maximum sentencing guidelines on these charges, according to court documents, allow for a combined sentence of 27 years in prison, more than \$700,000 in fines and up to double the loss of the victims or twice Torricelli's financial gain -- whichever is greater. (from *ComputerWorld*). ☺

## CALENDAR OF EVENTS



#### PERSONAL SECURITY SEMINAR

PLACE 4/F., EXHIBITION HALL, HKPC BUILDING, 78 TAT CHEE AVENUE, KOWLOON TONG  
 DATE 9 DECEMBER 2000  
 FEE FREE  
 TIME 14:30PM – 18:00PM  
 ENQUIRY 2834 2228

#### ASIA PACIFIC SOFTWARE ENGINEERING PROCESS GROUP (AP-SEPG) AND INTERNATIONAL SOFTWARE DEVELOPMENT & MANAGEMENT (ISD&M)

PLACE THE FOUR SEASONS BALLROOM, NEW WORLD RENAISSANCE HOTEL, 22 SALISBURY ROAD, KOWLOON  
 DATE 14 - 15 DECEMBER 2000  
 FEE HK\$3,200  
 TIME 9:00AM – 17:00PM  
 ENQUIRY 2788 5911

### FOR FURTHER INFORMATION, PLEASE CONTACT

Tel: (852) 2788-6060

Fax: (852) 2788-5878

e-mail: [infosecurity@hkpc.org](mailto:infosecurity@hkpc.org)

Web Site: <http://www.hkpc.org/itd/infosecurity>



**Hong Kong  
Productivity Council**  
香港生產力促進局