

BubbleBoy Worm Infects PCs

Introduction

The BubbleBoy worm (a type of virus) resides in an HTML email message. The message in a BubbleBoy email consists of an HTML page with embedded hidden Visual Basic Script code that will be executed without notifying the user.

The worm can execute if the Microsoft Internet Explorer 5 security settings are set to medium or low.

BubbleBoy Technical Specifications

1. Uses Internet Explorer 5 to write the file "update.hta" in the windows startup directory
2. Disabling active scripting will defeat this worm.
3. Requires MS email programs: Outlook 98, Outlook 2000, or Outlook Express (ships with IE5)
4. Requires Windows 95/98; not WinNT
5. Worm replicates by sending itself to all addresses in all Outlook address books
6. Outgoing message is deleted after being sent to new addresses

Protection From BubbleBoy

1. Download Microsoft's "scriptlet.typelib/Eyedog" Vulnerability Patch, which will prevent the known vulnerability in the ActiveX control function.
2. Update anti-virus scanning programs, as appropriate, to detect and defeat the worm and "update.hta" file.

BubbleBoy Worm Characteristics

This is an Internet worm that requires Internet Explorer 5 with Windows Scripting Host installed (WSH is standard in Windows 98 and Windows 2000 installations). It does not run on Windows NT due to hard-coded limitations.

The Internet worm is embedded within an email message of HTML format and does not contain an attachment. This worm is written in VB Script. There are two variants; the .b variant is encrypted.

Microsoft Outlook & Outlook Express

In MS Outlook, this worm requires that you "open" the email. It will not run if using "Preview Pane".

In MS Outlook Express, the worm is activated if "Preview Pane" is used and the message is not actually opened.

Microsoft Security Update "Patch"

In both the above, if security settings for Internet Zone in IE5 are set to High, the worm will not be executed. The vulnerability exploited by this worm has been addressed by Microsoft with a security patch called the "scriptlet.typelib/Eyedog."

Installing this Internet Explorer patch will prevent the execution of this worm under default security settings.

We strongly urge applying this patch for all desktops running MS Internet Explorer.

How BubbleBoy Actually Works

After the Visual Basic Script executes, it writes the file UPDATE.HTA to the local machine and during the next Windows startup, the .HTA file is invoked. The UPDATE.HTA file is coded to do the following:

Change the registered owner via the registry to "BubbleBoy"

Change the registered organization to "Vandelay Industries"

Send itself embedded in an email message to EVERY contact in EVERY EMAIL ADDRESS BOOK of MS Outlook

Sets the registry key to indicate that the email distribution has occurred. (Email distribution will not be repeated.)

Method Of Infection

This worm creates the file "UPDATE.HTA" in the "C:\windows\start menu\programs\startup" folder. Upon Windows startup or restart, the worm code is invoked.

More Details

Additional details are posted to dgl.com/itinfo/1999/it991110.html.

