Global Information Assurance Certification Paper

Digging for KakWorms
Terri Cronk
February 20, 2001

Although many people refer to all malicious code that infects computers as a virus, there is a difference between a virus and a worm. A virus is a program that replicates itself and contains code that explicitly copies itself. A virus can "infect" other programs by modifying them or their environment like a call to an infected program implies a call to a possibly evolved copy of the virus. A worm is a program (or a group of programs) that is self-contained. The program is able to spread copies of itself (or segments) to other computer systems. A worm is also used to describe malicious software (malware) that propagates with no direct action by a user. There are host computer worms and network worms. Host computer worms are contained only in the computer they run on and only use network connections to copy themselves to other computers. With host computer worms, the original program ends after launching a copy on another host (so there is only one copy of the worm running somewhere on the network at any one time). Network worms have multiple parts, called segments, each running on different machines (and possibly performing different actions). They use the network for several communication purposes. Propagating a segment from one machine to another is only one purpose of a network worm.

In an article on ZDNet, "Top 10 Security Stories of 2000", The invisible worm called VBS/Kakworm, was listed as No. 10 for the year 2000. It was first detected on December 27, 1999. The Kakworm accounted for 3 percent more trouble calls than with LoveLetter according to Sophos. Still the worm has been around since the end of 1999, but it hasn't spread very fast and also hasn't caused much damage.

The worm attaches itself to the outgoing signature files in Microsoft Outlook Express. The KakWorm can also modify registry files and shut down Windows. The worm infects computers by taking advantage of a flaw in Microsoft's Internet Explorer, Outlook and Outlook Express, but will only spread to computers that have Outlook Express installed. Kak is considered to be an automatic worm, which means that a user doesn't have to open the attachment for a computer to become infected. Just reading an email can exploit the Microsoft Active X control Scriptlet.Typelib that allows local files to be created or modified. It is unsafe to allow untrusted programs to access this control according to CERT. The KakWorm has many aliases, such as Wscript.KakWorm, VBS.Kak.Worm, Kagou-Anit-Krosoft, Kagou-Anti-Kro$oft, KakWorm.A-M, KakWorm.A and Kakworm.B, and is related to the BubbleBoy virus.

The KakWorm copies a file called KAK.HTA to the PC's hard drive and then renames the autoexec.bat file to AE.KAK. The worm then makes a new autoexec.bat file that runs the KAK.HTA file. Once the computer is rebooted, then the files execute. The KAK.HTA file runs the first of the month at 5:00 p.m. with the message "Kagou-Anti-Kro$oft says not today!". Other messages that will appear on some systems are "Driver or memory error", that shows up briefly when Windows starts, and "S3 driver memory alloc failed". After the message appears, the computer will shut down.

In order to protect your computer against KakWorm, there are several precautions to take. Microsoft has provided a patch to fix this particular security hole at http://www.microsoft/technet/ie/tools/scrpteye.asp. It is also important to have updated virus definitions with your anti-virus software since all currently known variants of the Wscript.KakWorm should be covered in most software packages. If you uninstall the Windows scripting host, this will prevent the spread of infection.

If you have been infected with the KakWorm the Symantec Knowledge Base has listed the following instructions to repair the damage that was done by the worm. There is a Wscript.KakWorm repair tool that was created by the Symantec AntiVirus Research Center and is considered, by them, to be the best method for repairing any damage done by the worm. The tool is available at http://www.symantec.com/avcenter/venc/data/wscript.kakworm.fix.html. Symantec offers two solutions for using their tool.

Solution 1 removes the worm from within Windows using the following steps:

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 entry from the registry.
6. Uninstall the Windows scripting host.
7. Delete files from Quarantine (found in Norton AntiVirus).
8. Clear deleted items folder.
9. Install the Microsoft patch.
10. Follow the instructions for what to do after installing the Microsoft patch.

Solution 2 removes the worm mostly in MS-DOS mode using the following steps:

1. Start computer in MS-DOS mode.
2. Remove the worm entry from the autoexec.bat file.
3. Remove the worm-infected files in MS-DOS mode.
4. Remove the worm entry from the registry.
5. Uninstall the scripting host.
6. Delete worm-infected files from Quarantine (found in Norton AntiVirus).
7. Clear deleted items folder.
8. Install the Microsoft patch.
9. Follow the instructions for what to do after installing the Microsoft patch.

In order for the above solutions to work, the following steps must be taken after the Microsoft patch has been installed. According to the Symantec Knowledge Base, the following steps must be taken each time your anti-virus software detects an email that has been infected with the 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 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 the email, contact them and let them know that their system is infected with this worm.

In closing, Wscript.KakWorm is a worm and it spreads by using Microsoft Outlook Express. This worm will attach itself to all outgoing messages that use the Signature feature in Outlook Express. The worm needs three files to deliver its payload; .hta, .reg, and .bat. The worm exploits a security hole known as "Scriptlet TypeLib". Even though computers that run Microsoft Outlook or Outlook Express can be infected, only Outlook Express can spread the infection. There is a lot of information about the KakWorm on the Internet and several solutions on how to prevent, repair and maintain systems that have been infected with the worm.

References:

Lemos, Robert. "Top 10 Security Stories of 2000" December 24, 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2668051,00.html

Vamosi, Robert. "Kak Worm Threatens IE5 and Office 2000 Users" May 12, 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2567767,00.html?chkpt=zdnnrla

Sullivan, Bob. "Beware the Mass-marketing 'kak' Virus" May 26, 2000. URL: http://zdnet.com/zdnn/stories/news/0,4586,2578234,00.html?XMTFORCEDIALUP=TRUE

"What is the Wscript.KakWorm?" Symatec Knowledge Base. 2000020318071406. December 15, 2000. URL: http://service1.symatec.com/SUPPORT/nav.nsf/pfdocs/2000020318071406

"VBS_KAKWORM.A" Trend Micro Virus Encyclopedia. URL: http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=VBS_KAKWORM.A

"VBS_KAKWORM.A-M" Trend Micro Virus Encyclopedia. URL: http://www.antivirus.com/vinfo/virusencyclo/default5.asp?Vname=VBS_KAKWORM.A-M

"VBS_KAKWORM.B" Trend Micro Virus Encyclopedia. URL: http://www.antivirus.com/vinfo/virusencyclo/default5.asp?Vname=VBS_KAKWORM.B

"Exploitation of "Scriptlet.Typelib" ActiveX Control" CERT Incident Note IN-2000-06. June 6, 2000. URL: http://www.cert.org/incident_notes/IN-2000-06.html