# Global Information Assurance Certification Paper

# July 2001: Indicative of the "Year of the Worm"

David A. Shaffer
Version 1.2e

## Introduction

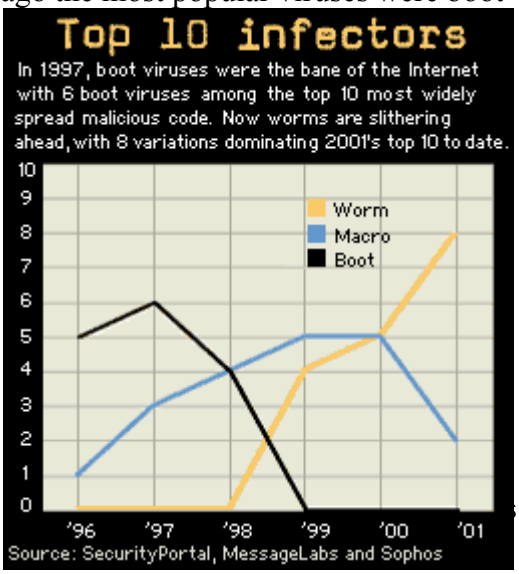
Each year, the American Institute of Certified Public Accountants (AICPA) identifies for its membership the top ten technologies affecting business. These technologies are reviewed and ranked by the AICPA Group of 100, a body of experts and leaders in the accounting technology industry. For 2001, the AICPA Group of 100 identified security as the number one technology affecting business. This was probably not surprising for members of organizations such as SANS but for small business owners security is often not a large blip on their radar screen. Especially when compared with other technologies on the list like bandwidth, XML, wireless communication and networking and database technologies.

One of the reasons why security issues have reached such a high profile as noted by the AICPA and many other businesses and security organizations is because of the incessant battery of viruses that are coded with each passing month. This paper is going to discuss the rise in attacks from worms. It will also discuss two worms making security headlines throughout the month of July 2001, the essence of their structure and how to neutralize the infections. Finally, this paper will look at preventative measures that can be taken by a company both at the perimeter and internal levels to help reduce the possible exposure to worms.

## "Year of the Worm"

CNET News.com has labeled 2001 the "Year of the Worm". The year started out with a bang…the VBS/AnnaKournikova virus was a worm that brought thousands of Internet mail servers to halt with its replicating scripts. This year has also brought us many variants of the popular Loveletter and Hybris worms that first surfaced in the year 2000.

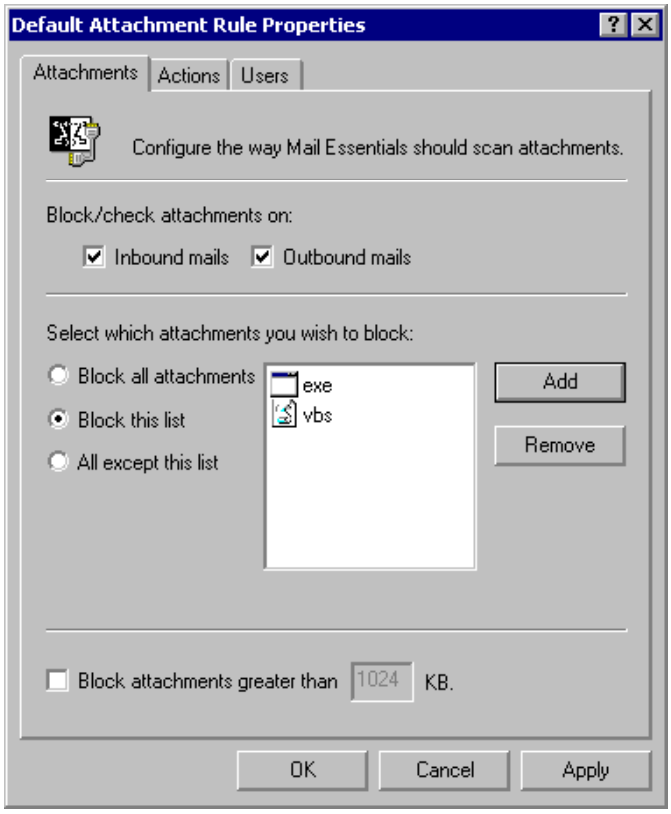
As the graph at right demonstrates, as few as four years ago the most popular viruses were boot sector viruses. The security community then saw the proliferation of macro viruses. Since the beginning of 2000 the worm has risen in popularity and currently now in mid-2001 is the most dominant virus breed. Today, worms fall into one of two classifications: the mass mailer or codependent type and the network-aware or loner type.




## Mass Mailer Worms

Mass mailer worms are sometimes referred to as codependent worms because they require an action by the user or victim in order to propagate the worm. In this manner, mass mailer worms resemble a Trojan Horse because an action is required to set the worm in motion. The most common way for mass mailer worms to replicate is through email attachments. The email lures the computer user into executing an attachment by promising something in the attachment that arouses great curiosity. The person then clicks on the attachment and the mass mailer spamming itself to all of the user's address book entries continues the propagation. Defense against these worms is a simple as not triggering the replication by opening the worm's attachment. Easily said, but some of the message "traps" are so alluring that even savvy computer users will unwittingly release the worm by attempting to open the attachment. Therefore, merely training users to not open emails with attachments from people they don't know is not an adequate defense against mass mailer worms. For defense in depth, not only should the user population be trained about the risk of these types of worms, but an email gateway should be put in place that profiles incoming emails to see if they have any of the characteristics of mass mailer worms. The gateway will then quarantine any emails that it profiles as suspicious, so that the system administrator can then examine and destroy them or release them to the user if they do not appear to meet the mass mailer worm profile. The majority of mass mailer worms prey on Microsoft email clients Outlook and Outlook Express.

One email gateway product I have used frequently and can highly recommend is "Mail Essentials" by Gfi. Of the nineteen excellent features, there are two that are most relevant to this discussion. The first is email content checking/filtering. With this feature you can quarantine all emails with dangerous attachments before they reach the intended recipient. As demonstrated in the screen shot at right, the default file type attachments that are blocked are "exe" and "vbs". However Mail Essentials is very flexible and will let a system administrator add any file type they want. Therefore, if "mp3" files are responsible for occupying large amounts of disk space, the system administrator can quarantine these types of attachments also. In addition, there is an option to restrict by size. Another bonus is that Mail Essentials can scan for script coding in the message body, adding another layer of protection.




The second feature is Mail Essentials' ability to automatically remove Word macros and HTML scripts. If the application detects a Microsoft Word file attachment that contains a macro it will strip off the macro before it sends the email to the recipient. This will neutralize the threat of the macros. Even more impressive is the application's ability

to disable scripts in HTML email. Since the ability to send email in HTML format has become popular, hackers have been able to embed triggers in HTML code that could possibly release viruses or worms without alerting the recipient to the damage being done. This application detects these scripts in the HTML code and disables them before forwarding the mail to the mailbox, thereby securing the piece of mail.
I recommend that a gateway application such as this be used *in addition* to virus protection because it helps protect against threats that the virus engines have yet to be updated for and it provides another layer of defense, as it scans for types of attachments and not particular virus characteristics.

**Network-Aware Worms**

Network aware worms are sometimes referred to as "loner" worms. This is because, unlike mass mailer worms these network-aware varieties can bypass the user to exploit a security hole in the operating system, such as unprotected, shared drives or weaknesses in software applications such as FTP. Once the target machine is infected, the worm will scan the Internet for other machines that are vulnerable that it can infect. The best defense against this type of worms is to apply all security updates released by the developers, look for open network shares and clamp them shut and use perimeter devices such as a reliable and properly configured firewall.

**July 16th 2001: Enter CodeRed**

On July 16th a new worm appeared on the scene that immediately captured the interest of the anti-virus research community because there is no piece of its code that is saved in any files that can be scanned by anti-virus software. The code is executed directly from memory.
The CodeRed worm has two payloads. Damages that can be caused by this worm are:

1. It will spawn multiple threads and utilize bandwidth causing a denial of service.

2. It will spawn multiple threads causing system instability and may be responsible for a system crash.

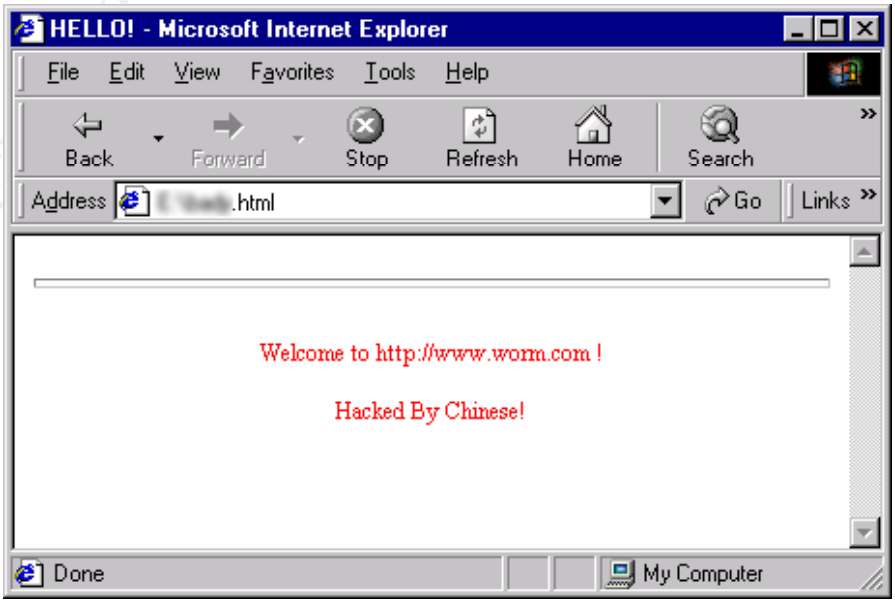
One of the most concise and easily understood technical descriptions of the CodeRed Worm processes of infection and replication is by Ryan Permeh and Marc Maiffret of eEye Digital Security:

> The .ida "Code Red" worm is spreading throughout IIS web servers on the Internet via the .ida buffer overflow attack that was published weeks ago.
>
> The following are the steps that the worm takes once it has infected a vulnerable web server.
>
> 1. Setup initial worm environment on infected system.
> 2. Setup 100 threads of the worm
> 3. The first 99 threads are used to spread the worm (infect other web servers).

-The worm spreads itself by creating a sequence of random IP addresses. However, the worm's randomization of IP addresses to attack is not all together random. In fact there seems to be a static seed that the worm uses when generating new IP addresses to try to attack. Therefore every computer infected by this worm is going to go through the same list of random IP addresses to try to infect. The "problem" with that is that the worm is going to end up reinfecting systems and also end up crossing traffic back and forth between hosts to end up creating a denial of service type affect because of the amount of data that will be transferred between all the IP addresses in the sequence of random IP addresses. The worm could have done truly random IP generation and that would have allowed it to infect a lot more systems a lot faster. We are not sure why that was not done but a friend of ours did pose an interesting idea... If the person who wrote this worm owned an IP address that was one of the first hundred or thousand etc. to be scanned then they could setup a sniffer and anytime and IP address tried to connect to port 80 on their IP address they would know that the IP address that connected to them was infected with the worm and they would therefore be able to create a list of the majority of systems that were infected by this worm.

4. The 100th thread checks to see if it is running on an English (US) Windows NT/2000 system.

-If the infected system is found to be a English (US) system then the worm will proceed to deface the infected systems website. That means... the local web servers web page will be changed to a message that says Welcome to http://www.worm.com !, Hacked By Chinese!. This hacked web page message will stay "live" on the web server for 10 hours and then disappear and never appear again unless the infected system is re-infected by another host.




-If the system is not an English (US) Windows NT/2000 system then the 100th worm thread is also used to infect other systems.

5. Each worm thread checks for c:\notworm

-If the file c:\notworm is found, the worm goes dormant.

-If the file is not found then each thread will continue to attempt to infect more systems.

6. Each worm thread will now check the infected computers time.

-If the time is between 20:00 UTC and 23:59 UTC then the worm will proceed to

use this thread to attack www.whitehouse.gov. The attack consists of the infected system sending 100k bytes of data to port 80 of www.whitehouse.gov therefore potentially performing a denial of service attack against www.whitehouse.gov.
-If the time is below 20:00 UTC then this worm thread will try to find and infect new web servers.

In testing we have calculated that the worm can attempt to infect roughly half a million IP addresses a day and that was a rough estimate made from using a very slow network.

As of writing this document (July 18 6:49pm) we have had reports from administrators that have been probed by over 12 thousand unique hosts. That basically means at least 12 thousand hosts have been infected by this worm.

In testing we have seen that sometimes the worm does not execute correctly and will continue to spawn new threads until the infected machine crashes and has to be rebooted. We have not been able to isolate the cause of this behavior.

Within two days over 12 thousand web servers were infected (Permeh). The most astonishing fact concerning CodeRed is that Microsoft released a patch for this vulnerability a month before it was exploited via CodeRed. System administrators must subscribe to published alerts like those from Cert.org or Sans.org that contain alerts for the latest patches and updates for the software products they are responsible for. It is critical that these updates are applied as soon as the vulnerability is detected and the alert is tendered. It is the responsibility of the IT management to insure that procedures and policies are in place that require security updates to be applied as soon as they are released. In the busy, multiple-priority days of the front line IT specialists and administrators, it is easy to put patches on the to-do list and press forth with "more urgent" user requests, especially when the patches/updates require rebooting of the company's server(s).

Since this worm operates from system memory it is possible to remove it by rebooting the web server, however this is not recommended because the probability or reinfection is high. The recommended procedure is to take the system offline and apply the patch from Microsoft that corrects the vulnerability. Another recommended procedure is to install Service Pack 6a from Microsoft as it addresses many other security updates with one application. Some of these updates may have possibly been overlooked as singular releases.

**July 17th 2001: Enter SirCam**

The W32/SirCam worm found its way into the Internet community on July 17, 2001. By July 24th it was the number one reported virus on McAfee's website with over 144,000 infections reported in 24 hours (McAfee).

It was immediately observed that this worm had some unique characteristics. It copies itself to the recycle bin of the infected computer. Most anti-virus software does not scan the recycle bin

so Sircam has a great place to hide. It has mass mailer capabilities and is also network-aware so that it was coded to be a hybrid—it can replicate both ways. Technically, it is a worm and a virus because it replicates exactly like a worm does but also has the capability to perform attacks on the computer system like a virus does. SirCam also contains its own Simple Mail Transfer Protocol (SMTP) engine which facilitates the mass mailing capabilities of the worm. Interestingly enough, there is a bug in the program, which does not allow it to replicate under Windows NT or Windows 2000.

The damages that SirCam can cause to an infected host computer are:

1. There is a payload trigger such that on October 16th a file deletion payload is triggerd.
    a. If the file deletions occur, or after 8,000 attempts at execution, a space-filler payload is triggered.
2. Payloads
    a. Mass Mailing – the worm grabs a document from the host PC and mails it to all of the addresses in the address book.
    b. Deletes files - There is a 1 in 20 chance of deleting all files and directories on C:. This only occurs on systems where the date is October 16 and which are using D/M/Y as the date format. Always occurs if attached file contains "FA2" not followed by "sc".
    c. Degrades Performance – There is a 1 in 50 chance that the worm will cause the C: drive to fill by adding text to the file c:\recycled\sircam.sys.
    d. Releases Confidential Information – it exports into the body of the worm a random document from the infected computer's hard drive.

The comprehensive technical description of this worm is referenced at the SARC.com website:

> This worm arrives as an email message with the following content:
>
> Subject: The subject of the email will be random, and will be the same as the file name of the email attachment.
> Attachment: The attachment is a file taken from the sender's computer and will have the extension .bat, .com, .lnk or .pif added to it.
> Message: The message body will be semi-random, but will always contain one of the following two lines (either English or Spanish) as the first and last sentences of the message.
>
> Spanish Version:
> First line: Hola como estas ?
> Last line: Nos vemos pronto, gracias.
>
> English Version:
> First line: Hi! How are you?
> Last line: See you later. Thanks

Between these two sentences, some of the following text may appear:

Spanish Version:
Te mando este archivo para que me des tu punto de vista
Espero me puedas ayudar con el archivo que te mando
Espero te guste este archivo que te mando
Este es el archivo con la informaci=n que me pediste

English Version:
I send you this file in order to have your advice
I hope you can help me with this file that I send
I hope you like the file that I sendo you
This is the file with the information that you ask for

When run, the worm performs the following actions:

1. It creates copies of itself as %TEMP%\<File name> and C:\Recycled\<file name>, which contain the attached document. This document is then run using the program registered to handle the specific file type. For example, if it is saved as a file with the .doc extension, it will run using Microsoft Word or Wordpad. A file with the .xls extension will open in Excel, and one with the .zip extension will open in your default zip program, such as WinZip.

NOTE: The term %TEMP% is the Temp variable, and means that the worm will save itself to the Windows Temp folder, whatever its location. The default is C:\Windows\Temp.

2. It copies itself to C:\Recycled\Sirc32.exe and %System%\Scam32.exe.

NOTE: %System% is also a variable. The worm will locate the \System folder (by default this is C:\Windows\System) and copy itself to that location.

3. It adds the value

Driver32=%System%\scam32.exe

to the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows\CurrentVersion\RunServices

4. It creates the following registry key:

HKEY_LOCAL_MACHINE\Software\SirCam

with the following values:
FB1B - Stores the file name of the worm as stored in the Recycled directory.
FB1BA - Stores the SMTP IP address.
FB1BB - Stores the email address of the sender.
FC0 - Stores the number of times the worm has executed.
FC1 - Stores what appears to be the version number of the worm.
FD1 - Stores the file name of worm that has been executed, without the suffix.

5. The (Default) value of the registry key

HKEY_CLASSES_ROOT\exefile\shell\open\command

is set to

C:\recycled\sirc32.exe "%1" %*"

This enables the worm to execute itself any time that an .exe file is run.

6. The worm is network aware, and it will enumerate the network resources to infect shared systems. If any are found, it will do the following:
Attempt to copy itself to <Computer>\Recycled\Sirc32.exe
Add the line "@win \recycled\sirc32.exe" to the file <Computer>\Autoexec.bat
Copy <Computer>\Windows\Rundll32.exe to <Computer>\Windows\Run32.exe
Replace <Computer>\Windows\rundll32.exe with C:\Recycled\Sirc32.exe

7. There is a 1 in 33 chance that the following actions will occur:
The worm copies itself from C:\Recycled\Sirc32.exe to %Windows%\Scmx32.exe
The worm copies itself as "Microsoft Internet Office.exe" to the folder referred to by the registry key:

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Explorer\
Shell Folders\Startup

8. There is a 1 in 20 chance that on October 16th of any year, the worm will recursively delete all files and folders on the C drive.
This payload functions only on computers which use the date format D/M/Y (as opposed to M/D/Y or similar formats).

Additionally, the payload will always activate immediately, regardless of date and date format, if the file attached to the worm contains the sequence "FA2" without the letters "sc" following immediately.

9. If this payload activates, the file C:\Recycled\Sircam.sys is created and filled with text until there is no remaining disk space. The text is one of two strings:

[SirCam_2rp_Ein_NoC_Rma_CuiTzeO_MicH_MeX]
or
[SirCam Version 1.0 Copyright ¬ 2000 2rP Made in / Hecho en - Cuitzeo, Michoacan Mexico]

10. The worm contains its own SMTP engine which is used for the email routine. It obtains email addresses through two different methods:

It searches the folders that are referred to by the registry keys

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Explorer\
Shell Folders\Cache

and

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Explorer\
Shell Folders\Personal

for sho*., get*., hot*., *.htm files, and copies email addresses from there into the file %system%\sc?1.dll

where ? is a different letter for each location, as follows:

scy1.dll: addresses from %cache%\sho*., hot*., get*.
sch1.dll: addresses from %personal%\sho*., hot*., get*.
sci1.dll: addresses from %cache%*.htm
sct1.dll: addresses from %personal%*.htm

It searches %system% and all subfolders for *.wab (all Windows Address Books) and copies addresses from there into %system%\scw1.dll.

11. It searches the folders referred to by the registry keys:

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Explorer\
Shell Folders\Personal

and

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Explorer\
Shell Folders\Desktop

for files of type .doc, .xls, and .zip, and stores the filenames in %system%\scd.dll. One of these files will be appended to the worm's original executable and this new file will be sent as the email attachment.

The From: email address and mail server are taken from the registry. If no email account exists, then the current user name will be prepended to "prodigy.net.mx", eg if the current user logged on as JSmith, then the address will be "jsmith@prodigy.net.mx". Then the worm will attempt to connect to a mail server. This will be either the mail server taken from the registry, or one of

prodigy.net.mx
goeke.net
enlace.net
dobleclick.com.mx

The language used for the mail depends on the language used by the sender. If the sender uses Spanish, then the mail will be in Spanish, otherwise it will be in English. The attachment is chosen randomly from the list of files in the scd.dll.

Removal of the worm is easily completed by using the removal tools created by SARC and by McAfee. There is a manual removal process that was developed however it is unwieldy and requires many registry edits and therefore is not recommended.

Although SirCam is not receiving as much public attention as the CodeRed Worm, it has the potential for great damage. SARC initial estimates by researchers said that it could reach over 100,000 infected systems(SARC). The popularity of this worm reached its peak on July 25th 2001 where the infection level was much greater than the initial estimates. SirCam is a future danger in that it remains a model for future mass mailing and network-aware worms.

**Additional Prevention Measures**

There are a number of countermeasures that can be taken at the workstation level to help thwart worms. These are particularly effective in a small business environment where there is less emphasis on security and where perimeter defense is less likely.

- Remove the Visual Basic Script file extension from the registered file types list – Some worms can propagate only if the .vbs extension is registered with the system. This can be accomplished by selecting "folder options" under the "view" menu in my computer. Locate the .vbs extension and remove it. It is unlikely that the average user would ever have a need for this registered file type.

- Disable windows scripting host – Windows scripting can be exploited by some worms . The original intent was to automate Windows tasks. The average user

will likely not be affected by disabling Windows scripting. The easiest way is to access "Add/Remove Programs" in the control panel. Choose the Windows setup tab and then select "Accessories". Make sure the check box for Windows Scripting Host is unchecked.

- Disable email scripting in Outlook/Outlook Express – Outlook 98 and later supports email scripting which can open vulnerabilities just by reading email. Disabling this feature in the security section of Internet Explorer properties can harden the workstation.

- Install all security updates – Monitor Microsoft's security sites or subscribe to Microsoft's security bulletin list to receive the very latest news about security and all Microsoft products. Install updates at the workstation level as soon as they are released.

- Train the users to exercise caution with email attachments – Make it part of user orientation or new employee orientation to never open attachments in emails from someone the user does not know.

## Conclusions

Data security and access is compromised daily by the many threats that are being coded by the hacker community. The popularity of worms has reached epic proportions in 2001 as evidenced by CNET News.com proclaiming 2001 as the "Year of the Worm". There are many countermeasures that can and must be taken by system administrators and information technology professionals. The most important is the training of IT staff to recognize the magnitude of these threats and put company policies and procedures in place to minimize the damage that these worms cause. It is also imperative to understand the ways in which these worms penetrate and replicate in computer systems. An understanding of defense in depth is critical to neutralizing the damage. It has been demonstrated how security alerts and the subsequent system patches, along with firewalls, email gateways and virus protection can dovetail to form a defense which can effectively minimize the damage to company systems and stop the propagation of the worms.

The most susceptible to these threats is small businesses. Just as these companies are more likely to ignore proper software licensing due to a lack of education, they are more likely to ignore proper data security due to what is perceived as a non-threatening situation. Or they perceive it to be an unnecessary expense compared to IT dollars that need to be invested into infrastructure or equipment upgrades. If the security certified community and its advocates such as SANS reach out to the small business owners and managers and strive to educate them about the importance of company security and security training it will help prevent the rapid replication of threats such as CodeRed and

SirCam. With the fast majority of business in the global economy being of the "small business" variety, education and training are the keys to controlling these threats and raising the productivity and revenues of all those concerned.

**References:**


**Lemos, Robert "Fast-spreading code is weapon of choice for Net vandals" March 15, 2001**
**URL:** http://news.cnet.com/news/0-1003-201-5125673-0.html
**Delio, Michelle "Love Bug, SirCam Neck and Neck" July 23, 2001**
**URL:** http://www.wired.com/news/technology/0,1282,45476,00.html

**AICPA Toptech**
**URL:** http://toptech.aicpa.org/techs/

**Computer Associates Virus Information Center**
**URL:** http://www.ca.com/virusinfo/virusalert.htm#CodeRed

**Sophos**
**URL:** http://www.sophos.com

**MessageLabs**
**URL:** http://www.messagelabs.com/

**Gfi**
**URL:** http://www.gfi.com/

**Permeh, Ryan; Maiffret, Marc "Full analysis of the .ida "Code Red" worm" July 17, 2001**
**URL:** http://eeye.com/html/Research/Advisories/AL20010717.html

**McAfee**
**URL:** http://www.mcafee.com/

**Symantec AntiVirus Research Center**
**URL:** http://www.sarc.com/avcenter/venc/data/codered.worm.html
**URL:** http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html