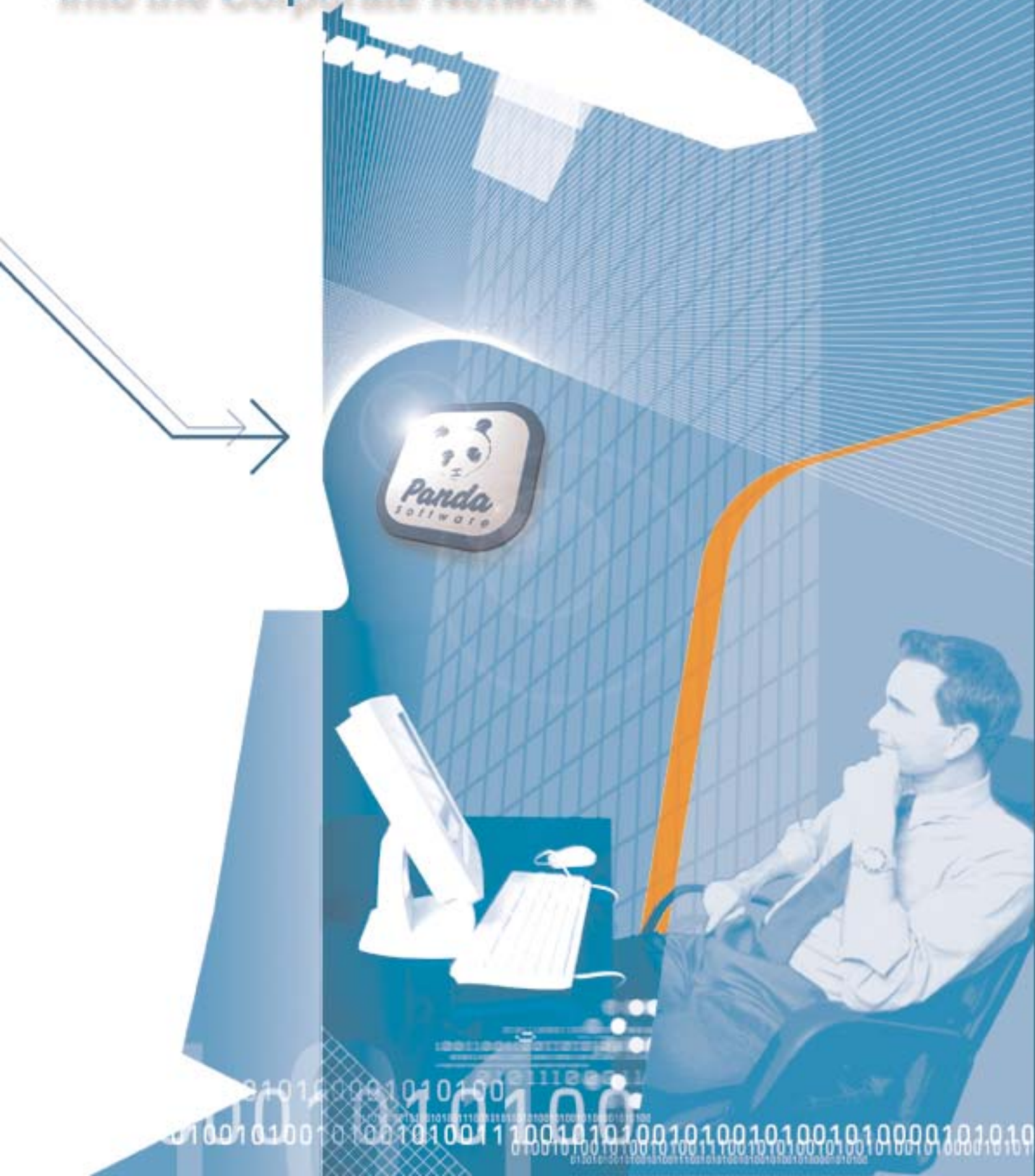


White Paper

Virus Entry Points into the Corporate Network



Virus Entry Points into the Corporate Network

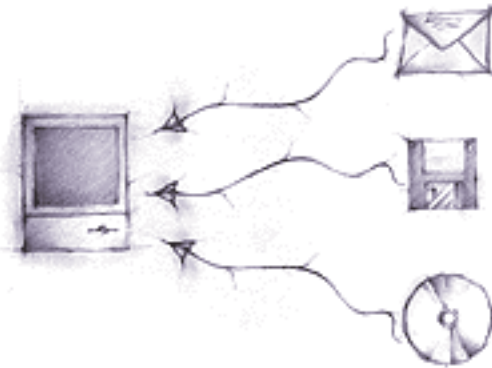
Contents

Most Common Virus Entry Points	page 3
Internet	page 3
E-mail	page 4
Web pages	page 6
File transfer (FTP)	page 7
Downloads	page 8
Newsgroups	page 8
Removable Disk Drives	page 8
Networks	page 9

Most Common Virus Entry Points

In order to correctly evaluate your anti-virus needs, one must look at where viruses enter a computer and/or a computer network. Below is a summary of virus entry points.

The first question that you should ask yourself is: How do viruses get into a computer, or attack it? If you know the answer to this question you can prevent infection by protecting all of these possible virus entry-points.



The most common entry-points used by viruses are the following:

Internet

- E-mail
- Web pages
- File Transfers (FTP)
- Downloads
- Newsgroups

Removable disk drives

Computer networks

- **Internet:** The Internet is becoming the most popular means of obtaining information, sending and receiving files, sending and receiving news, or downloading files. The Internet has become, by far, the biggest virus entry-point. All of these operations are based on transferring information and the inter-connection of millions of computers all over the world. This means that as well as data, you may well be receiving a hidden virus. Infection via the Internet may be produced through a number of different means, including the following:

E-mail

Web pages

File transfers (FTP)

Downloads

Newsgroups



Some of the possible virus entry-points via the Internet

- **E-mail:** Documents and files can be sent and received via e-mail in the form of attachments. These files could be infected. When an infected e-mail message is opened and the file it contains is run or opened, the computer that has received the message will become infected. The most important characteristics of infection via e-mail are as follows:
 - *Increased replication and propagation capacity.* The virus can spread to thousands of computers throughout the world in just a few minutes.
 - *Storage of messages.* Messages are stored in a special database (for example, PST files), which are difficult to scan using an antivirus program that is not designed specifically for e-mail systems.
 - *Increased connection capacity.* It is possible to send and receive messages between any types of computers/platforms.

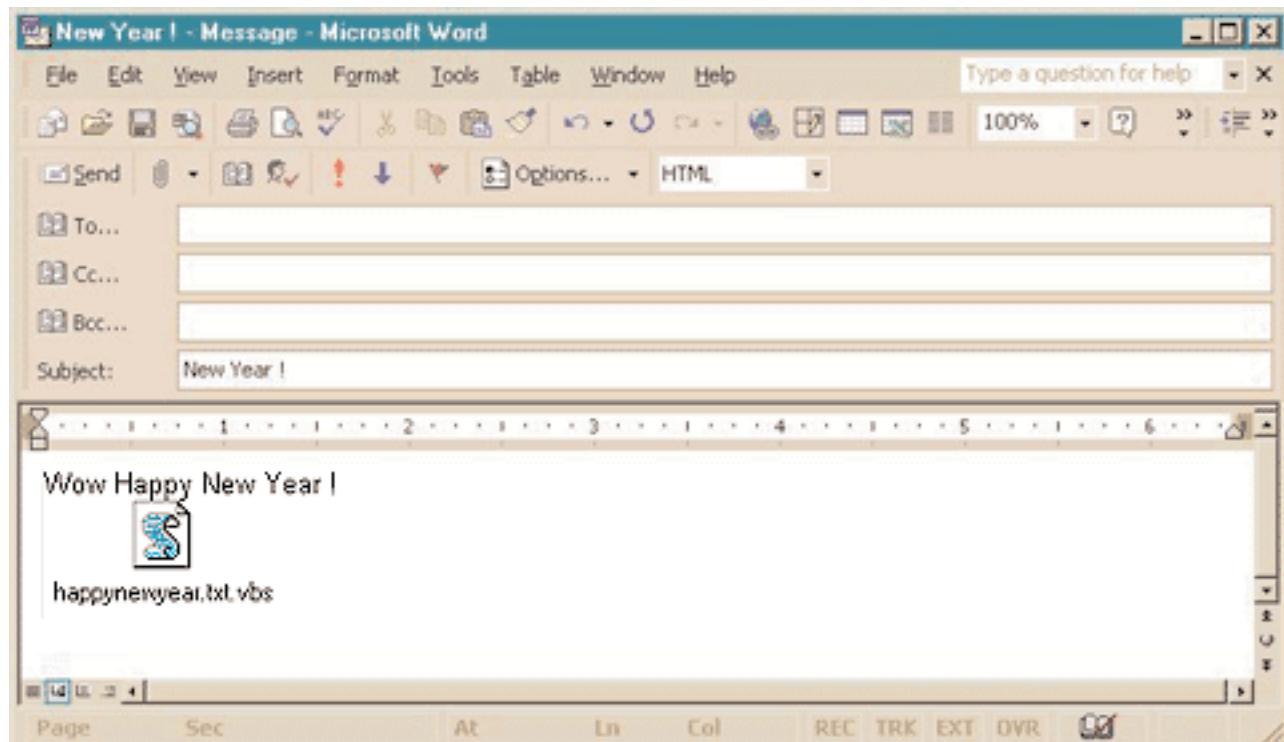


Viruses can hide in apparently inoffensive e-mail messages

Every day, millions and millions of e-mail messages are exchanged throughout the world. The time that it takes to reach the recipient is minimal. In addition, an e-mail message can

be sent to a large number of recipients at the same time. This makes e-mail particularly popular with virus authors: It is an extremely fast way of spreading and reaching a large number of recipients. In addition, viruses nowadays can produce an infection and have the capacity to send themselves to other computers without the affected user even realizing it. In this case, the recipients of the virus could be all of the people included in the e-mail Address Book of the infected computer.

In most cases, infections transmitted via e-mail are not carried out when the message is opened, but on opening or running an infected file included in it. However, there are exceptions. Some viruses, the minority, can carry out their infection when the mail message is opened (without the attached file needing to be executed).



E-mail message sent by the VBS/Tqll.A virus. (This message has been received and opened with Microsoft's Outlook 97).

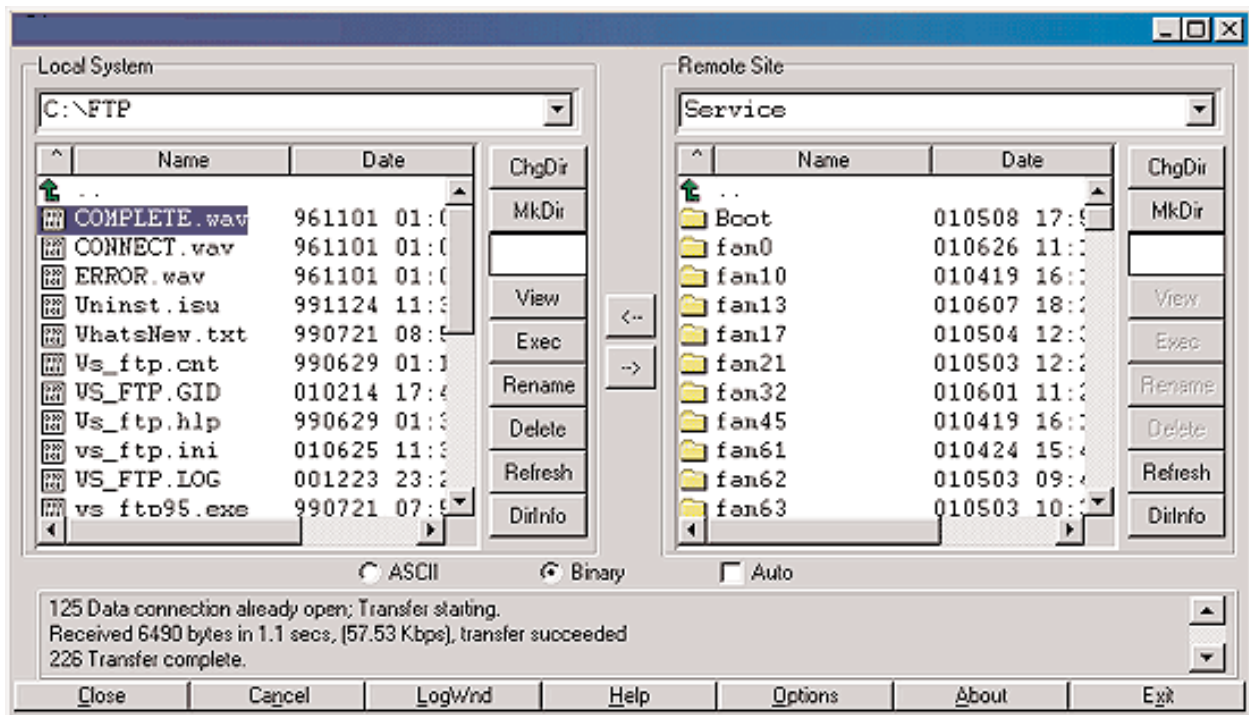
In order to avoid infection via e-mail, the following advice should be considered:

- Install an antivirus product that is designed to scan e-mail.
- Do not open suspicious files, messages from unknown senders, messages which contain strange texts, etc.
- Do not run or open files included in suspicious mail messages.
- If you think a message may be infected, delete it and inform the sender.

- **Web Pages:** The majority of pages visited on the Internet are text files or images written in a language known as HTML. However, they may also contain programs known as ActiveX controls and Java Applets. These may be infected and therefore infect the visitor to that page. If one of these pages includes a virus in HTML code that includes sections of dynamic code (which executes programs, or carries out certain operations), you could become infected simply by visiting the page.

When browsing Web pages, any flaws in your browser can be exploited through ActiveX Controls, Java Applets, HTML code and/or JavaScript, as well as through other methods. All of these can enable viruses to 'sneak' into a computer.

- **File transfer (FTP):** The term FTP stands for File Transfer Protocol. Through this protocol it is possible to place documents (upload) on any computer in the world or copy files from any computer to your own (download). When a file is downloaded, it is copied directly from a certain place to your computer. The downloaded files could, of course, contain a virus that would infect your computer.



Accessing a directory for a file transfer (FTP), through a FTP client called WS_FTP LE (Limited Edition).

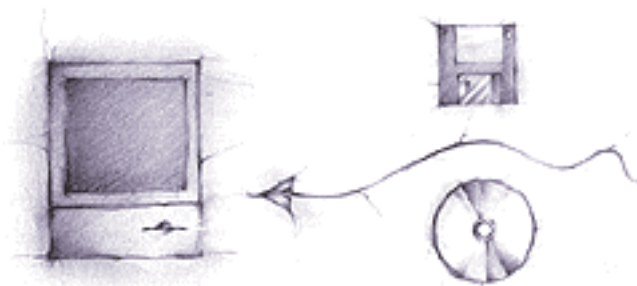
Some of the most common operations carried out by users on the Internet are downloading programs (shareware), documents, etc; in addition to downloading software from specific sites. For this reason, it is very important that you only download files from

sites that are well known and reliable.

- **Downloads:** Although downloading files from the Internet is similar to file transfer (FTP), it is not the same. Through FTP you can upload as well as download files, whereas through downloads you can only obtain files (which will be copied from a website to your computer). Although in general, these downloads are safe and virus free, it is possible that the downloaded file could be infected. There are some sites that are specially prepared for downloading software or IT utilities.
- **Newsgroups:** Through this service it is possible to debate a topic with anyone in the world or receive e-mails featuring the latest information on a topic of your choice. These newsgroups work in a similar way to a notice board. Users post their comments, questions, or notes about certain topics and other users can respond, give their opinion, clear up questions, etc. These messages could contain an infected document that could install a virus in your system.

With newsgroups you run the same risk of virus infection. When you connect to a newsgroup, files containing the recent articles are downloaded (in the same way as e-mail). These files could also be infected.

- **Removable disk drives:** Disk drives are storage devices on which data is stored in the form of files or documents. These disk drives enable documents to be created on one computer and then used on another. Among these types of storage devices are floppy disks, CD-ROMs, and Zip and Jazz disks, removable disk drives, and other new emerging storage formats. If any of these are infected, the other computers on which they are used will become infected. E-mail messages can also be stored in these storage devices, which may also be infected.

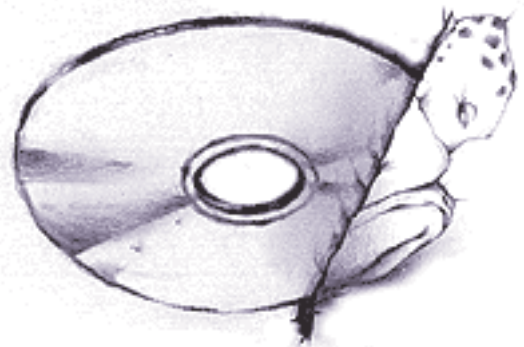


Viruses can use floppy disks, CD-ROMs and removable drives to enter computers.

Floppy disks (or other extractable disks) can store programs, files, Web pages (HTML), e-mail messages with attached files, compressed files, etc. Any of these elements could be infected. Similarly, what is known as the boot sector of the disk could also be infect-

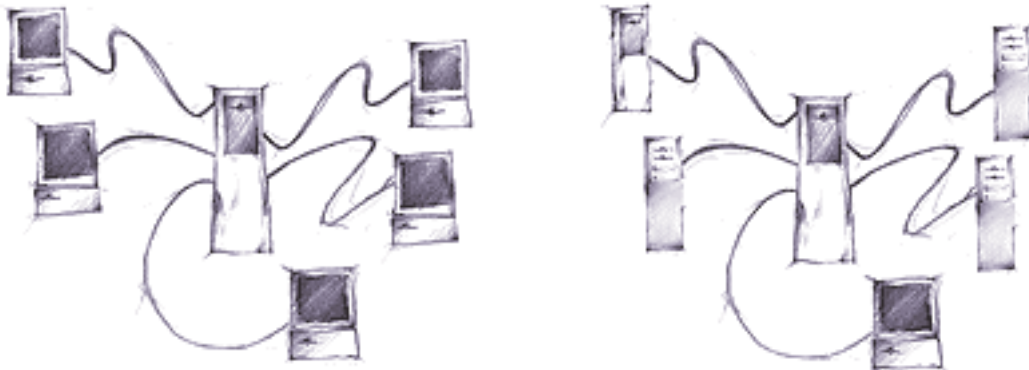
ed with a boot virus. Although it still happens, infections produced from floppy disks have decreased significantly. This method of spreading viruses has given way to much quicker means of propagation, such as e-mail.

Although in general CD-ROM drives can only read the content of a disk but cannot write on them, nowadays it is possible to read and write (record) on a CD-ROM. This, along with the large quantity of information that they can store has led to a large number of infections. In addition, many computers can be booted from a CD-ROM. This option can also lead to an increase in the number of infections.



Viruses can also enter computers through CD-ROMs

- **Networks:** Each computer that forms part of the network can connect to all other networked machines. Through this system it is possible to transfer information from one computer to another and/or access the information stored in one of them from the rest. If the information (programs, files, documents, etc.) that is accessed or transferred from one computer to another were infected, the computers that accessed this computer (or those involved in the transfer), could also be infected.



Viruses can also get into networks through workstations and/or servers

These connections can be local and/or remote, allowing computers and laptops to connect via cable, an Intranet, modem, etc. In short, this means that the network can be accessed from multiple points. You only need to consider a single computer and the means through which a virus can enter it, then multiply this by the computers in the network and mobile machines (such as laptops) that can connect to this network in order to get an idea of the myriad ways through which viruses can enter a network.

Conclusion:

To conclude, below is a table representing how the different infection entry-points used by viruses have changed over the last six years. It is evident that the most popular means of infection amongst virus writers at present is e-mail, having increased from 9% of all virus infections in 1996 to 83% in 2001.

Source of Virus	1996	1997	1998	1999	2000	2001
E-mail Attachment	9%	26%	32%	56%	87%	83%
Internet Downloads	10%	16%	9%	11%	1%	13%
Web Browsing		5%	2%	3%	0%	7%
Don't Know	15%	7%	5%	9%	2%	1%
Auto Software Distribution	0%	2%	1%	0%	0%	2%
Other Vector	0%	5%	1%	1%	1%	2%
Diskette: other	21%	27%	21%	9%	2%	1%
Diskette: From Home	36%	42%	36%	25%	4%	0%
Diskette: Sales Demo	11%	8%	4%	2%	0%	0%
Diskette: Wrapped SW	2%	4%	2%	0%	0%	0%
Diskette: LAN mgr/spvr	1%	3%	1%	0%	0%	0%
Diskette: repair/service	3%	3%	3%	2%	0%	0%
Diskette: malicious person	0%	1%	1%	0%	0%	0%
CD: software distribution	0%	1%	2%	0%	1%	0%
Total Respondents						300

(Source: ICSA Virus Prevalence Survey, 2001)

The Solution:

The total solution to virus problems is to have disk-resident virus protection at every point of your network, including on your desktops, your email server such as Exchange Server or Groupwise, and on all points of your network perimeter, including your Firewall, your Proxy Server, and on any Linux Email Servers such as Sendmail and Qmail.

In today's corporate IT environments, it is not enough to just have protection on the desktops, for instance. Similarly, it is not enough to just have protection on just your servers either. Users will check their Hotmail or Yahoo accounts through a browser, or may use

both Outlook and Outlook Express for different accounts. Like having a lock on every single door to a house, it is vital to guard every single potential network entry point against viruses.

About Panda Antivirus Products

Panda Antivirus offers a suite of exceptional antivirus products for networks of all sizes. Our products will protect your network from virus threats at every single potential entry point.

Panda Antivirus Enterprise Suite is complete network protection, designed to enable your company to meet today's virus threats head on. It's a scalable and integrated antivirus that offers uniform protection for networks regardless of their size or topology.

Its technology blocks all unwanted virus traffic, with state-of-the-art features that protect all entry points of a computer network. These features include truly automatic daily signature file updates, centralized antivirus administration, the latest generation heuristic scan engine to block unknown malicious code, content filtering, and customized virus warnings.

It is essential to ensure that all communication entering and leaving the company is 100 per cent virus-free. Panda Antivirus Enterprise Suite protects all points of the network, including desktops, email servers such as Exchange Server, Lotus Notes or Groupwise. And Panda PerimeterScan (which is included with Panda Antivirus Enterprise Suite or can be purchased separately) protects all points of the gateway, including firewalls, proxy servers, and Linux email servers such as Sendmail and Qmail.

Our highly-qualified team of Tech Support experts are available 24 hours a day, 365 days a year at no additional cost to you. Panda also offers your company customized services to suit your particular needs. Unlike many other antivirus companies, Panda Antivirus does not charge extra for phone Tech Support for corporate sites.

For a quote on Panda Antivirus for your network, **call toll-free at (800) 603-4922.**

Or try a free demo of Panda Antivirus Enterprise Suite to test it on your network. To download now, go to: <http://www.pandasecurity.com/demo.htm>