

# Computer Virus Protection in Small Business

Chien-Lin Liu

LIS565 Information Systems Analysis and Design

Professor Dr. Neil Yerkey

Spring 2002

## Abstract

In today's small business environment, companies are in high demand with limited budget for unexpected security problems caused by computer virus. Especially, small companies have limited resources in IT departments; they have to use efficient computer virus prevention software to enforce their information security. Therefore, it is important to realize what computer viruses are, how they spread, and what devastation they would make, then IT employees can assess company's situation to purchase the suitable anti-virus software to match companies' needs. Thus, only understanding the attributes of viruses and the needs for virus prevention, IT departments are more likely to take appropriate steps to protect companies' security. This paper aims to point out computer virus's characteristics and goes on to the anti-virus software for small business.

## Computer Virus Protection In Small Business

Over the past several years, with dramatic development of computer technology and Internet, the computer viruses' problems have become the most threatened problem to business's security today. According a survey released by McGuire Research Services Inc., for Trend Micro, in Fortune 1000 companies, their computer managers indicated that the greatest threat they face to information security is computer viruses. (McGuire Research Services, Inc.). Moreover, in today's business environment, small firms may have only two or three employees in IT departments or may depend on outside consultants, small businesses have to use the efficient computer virus prevention to enforce their information security. Therefore, a complete consideration of small business's views about computer viruses in their characteristics about what virus is, how it spreads, is important for making the appropriate computer virus protection.

Where does the computer virus come from? "In the mid-eighties, the Amjad brothers of Pakistan ran a computer store. Frustrated by computer piracy, they wrote the first computer virus, a boot sector virus called Brain" (Therault, 1999, October). Since this simple action, today there are several tens of thousands of computer viruses around the world.

What is a computer virus? A computer virus is a type of executable program and it has two obvious characteristics: replication and payload. "The difference between a computer virus and other programs is that viruses are designed to self-replicate. They usually self replicate without the knowledge of the user." (Therault, 1999, October). "Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to just about any type of file and are spread as files

that are copied and sent from individual to individual.” (Trend Micro). Therefore, while the virus is active on the computer, not only can virus self-replicate itself as many as it could in the situation without computer users’ attention, but it can also copy itself to infect other files. In addition to self-reproducing, they also can run some damaging procedures before users being aware the destruction of their computer and data. And if the virus has not caused obvious damage yet, users without anti-virus software may not even be noted that computer virus exists in their computers.

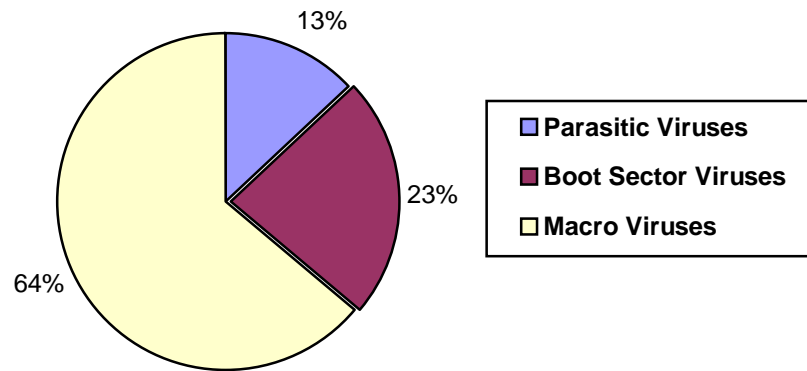
The second characteristic is payload. “While payload may only display messages or images, they can also destroy files, reform your hard drive, or cause other kinds of damage.” (Trend Micro, 1998). Users are not easy to be aware that viruses exist inside the computer system before the viruses’ payload happened. This “Payload“ action carries out the damage routine of computer virus. Payload may be displaying a joke, but the most devastating things coming with payload to companies are to lose the productivity in personal and machine and to destroy data that is stored in storage medium.

Although there are tens of thousands of computer viruses around the world, the majority of virus types are boot sector viruses, macro viruses, file infector viruses, and multipartite viruses. (See table 1)

Table 1. Virus classification statistics (Sophos, 1999, September)

Parasitic Viruses	Boot Sector Viruses	Macro Viruses
13%	23%	64%

**Figure 1. Virus Classification Statistics**



The first type of computer virus is the boot sector virus. “Until the mid-1990s, boot sector viruses were the most prevalent virus type, spreading primarily in the 16-bit DOS world via floppy disk. Boot sector viruses infect the boot sector on a floppy disk and spread to a user’s hard disk, and can also infect the master boot record (MBR) on a user’s hard drive.”(Trend Micro, 1998). The boot sector is the first program loaded into computer; computer cannot run any software without a boot sector. While the boot sector viruses exist in the MBR, they seek to modify every floppy disk’s boot sector that is inserted into computer. However, with the technology development, diskettes are gradually replaced by Internet and LAN in the role of files’ sharing. The boot sector viruses have become more rare. The famous examples of this type virus in Symantec Corporation web site’s “Online Virus Encyclopedia index” are Brain, Stone, Disk killer, Boot Killer, Boot-437, Boot Sierra.a, Zeus, Michael.b, Maji.2930, and Michelangelo. The advantage of this type virus is that it occupies the first sector and is not easy to detect and remove without using clean bootable diskettes and anti-virus software. On the other hand, today’s computers have seldom booted from diskettes, boot sector viruses have no longer have many opportunities like before to apply their advantage. For this reason, boot sector

viruses' advantage has become the main problem for them to spread today. The preventing method is to avoid using suspicious diskettes to boot computers.

The second type is macro virus. "A macro is an instruction that carries out program commands automatically." (Therriault, 1999, October). Many popular programs, for examples, Microsoft Word and Microsoft Excel, allow macro. Moreover, the documents that were created by applications that contain Macro function are shared and exchanged far more frequently in today's business offices by using Internet, LAN, and storage medium. For this reason, Macro viruses have been the most common type viruses. When word processing or spreadsheet documents that contain macro viruses are opened by users, those macro viruses can modify the application's startup files, for example, Normal.dot in Microsoft office, then any document that is used by users through those applications can become infected. Anti-DMV, Atom, Boom, Rainbow, Friendly, FormatC, Infezione, Parasite, Nuclear, Wazzu, and Hot are examples of Macro virus in Symantec Corporation web site's Online Virus Encyclopedia index. Being easy to create and having huge amount of applications supporting macro are the advantages of macro viruses. Thus, many applications supporting macro has become the anti-virus's difficulty to prevent the macro viruses' spreading. The useful way to prevent Macro virus infecting is that always to use anti-virus software to scan the document files that were created by Word, Excel, etc, before opening them.

File infecting virus is the third type of computer virus. "File infectors, also known as parasitic viruses, operate in memory and usually infect executable files with the following extensions: \*.COM, \*.EXE, \*.DRV, \*.DLL, \*.BIN, \*.OVL, \*.SYS." (Trend Micro, 1998). When users run a program that contain the file infecting viruses, those

viruses install themselves into computer memory and then start to infect other executable files. Without anti-virus software, the users' attentions might only raise by file infecting viruses' payload. The examples of file infecting virus are Sunday, Cascade, Jerusalem, Paradise.1840, Paris, Haddock, HellRaiser, Eastern Digital, Ranger, Red Star, Seat, Serena, Rust, Yankee, and Uruguay.<sup>7</sup>

The Multipartite viruses are the hybrid of boot sector viruses and file infecting viruses. The examples are Invader, Flip, Tequila, Galicia Boot, Indonesia Emas, Tchechen.mp.3420, Tchechen.1919, Hare.(b), One Half Boot, Emperor, Das Boot (b), DoRen Virsimul (b), and BadSectors.3174. Because the multipartite viruses contain the attributes from boot sector viruses and file infecting viruses, they can make the computers' infection more wide. The advantages of multipartite viruses are that not only can they hide in the computer's boot sector, but they also can exist in computers' memory to infect other files that are run or open by users.

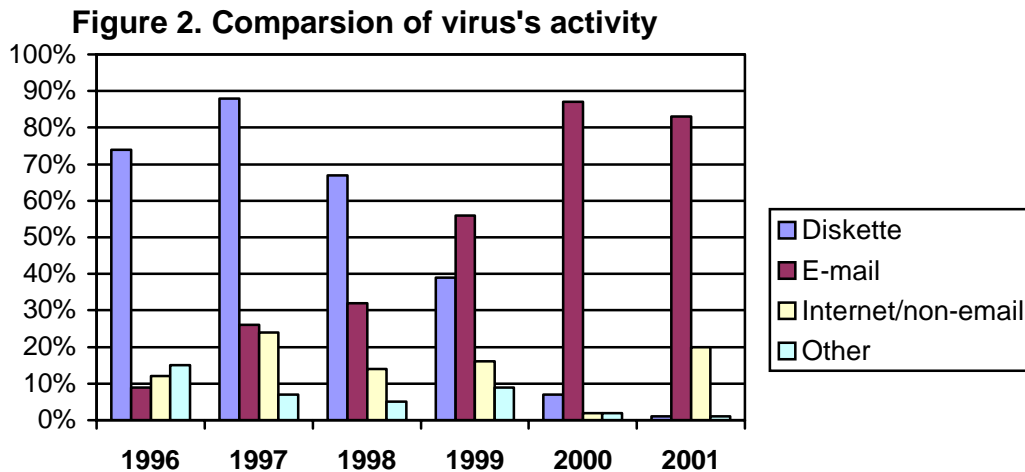
These four major types of computer virus, Boot sector viruses, Macro viruses, File infecting viruses, and Multipartite viruses, have been the most threats for today's business's security. However, the most spread out viruses are Macro viruses. Not only do they infect document files that were created by the most popular applications, like Microsoft Word, Microsoft Excel, etc, but it can also be written by only having few knowledge of computer programming.

After realizing what virus is, it is necessary to find out how they spread to computers. How do computer viruses spread? Floppy diskettes were the main spreading medium in several years ago, however, today the new virus distribution mechanisms, the Internet and e-mail, have made virus spreading faster than ever. According to the ICISA

Labs Virus Prevalence Survey 2001, from 1996 to 2001, the computer virus distribution could be separated into four major methods: Diskette, E-mail, Internet/non-email, and others. (See Table 2). From this survey (see Figure 2), it shows that the obvious changes of computer viruses distribution between diskette and e-mail. The most major computer virus distribution method in 1996 was diskette in 74% and only 21% were E-mail and Internet/non-email. With the time changing, in 2001 E-mail has grown to 83% and has become the most of viruses spreading method, but only 1 % viruses were spread via diskette. It became apparent that the most influential factor shown in this chart is that more and more infection of viruses is via the E-mail and Internet today. Therefore, it is more important to protect companies' message systems from viruses' attacks.

Table 2. Comparison of virus's activity between 1996-2001(Bridwell & Tippet, 2001, p. 26)

Source	1996	1997	1998	1999	2000	2001
Diskette	74%	88%	67%	39%	7%	1%
E-mail	9%	26%	32%	56%	87%	83%
Internet/non-email	12%	24%	14%	16%	2%	20%
Other	15%	7%	5%	9%	2%	1%



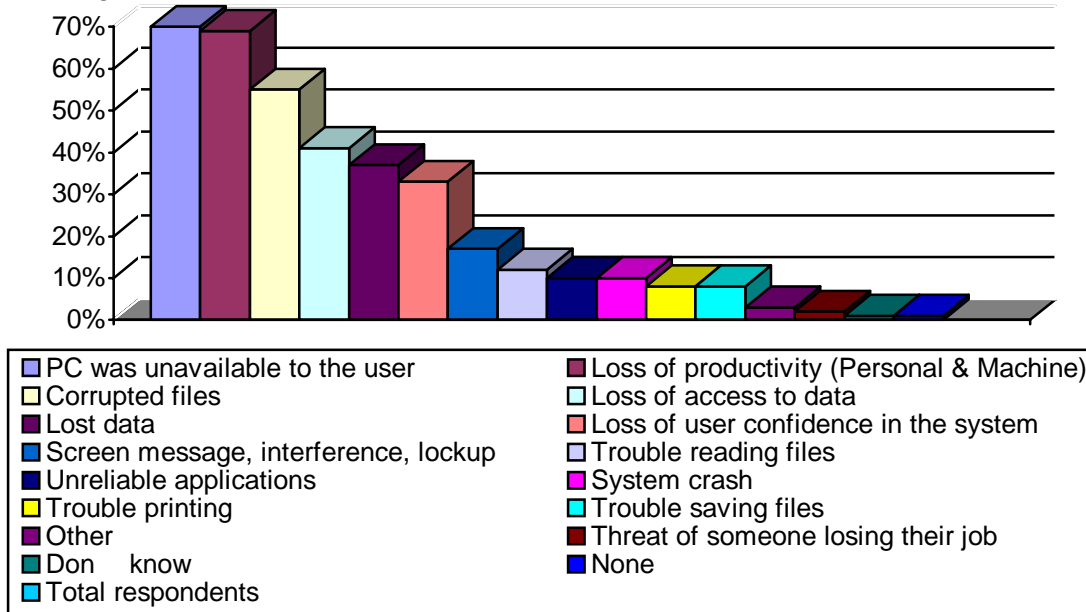
What effects do viruses have? In the ICSA Labs Virus Prevalence Survey 2001, from 1996 to 2001, (See Table 3, Figure 3) it showed that the top five responses from the survey participants are PC was unavailable to the user, loss of productivity (Personal & Machine), corrupted files, loss of access to the data, and lost data. The responses in “PC was unavailable to the user” that was the first impact in the survey has 210 votes and in 70% of respondents. The “loss of productivity in personal and machine” was the second place in 208 votes and 69% after “PC was unavailable to the user”. In today’s offices, employees cannot access to data and cannot use their computers could reduce the productivity of companies. On the other hand, viruses’ impacts can increase the companies’ cost. The third was “ corrupted files” in 165 votes and 55 % of respondents. “Loss of access to data” had 123 votes and 41 % in responses. “Lost data” had 111 votes and 37 %. Moreover, there were 100 votes and 33 % of respondents in “ Loss of user confidence in the system”. As a result, we could learn that the viruses’ impacts not only stopping users’ connections to computers, but also making users feeling no confidence to computer systems.

Table 3. Effects of viruses, 2001 (Bridwell & Tippett, 2001, p. 23)

<b>Answer</b>	<b>Frequency</b>	<b>%</b>
PC was unavailable to the user	210	70%
Loss of productivity (Personal & Machine)	208	69%
Corrupted files	165	55%
Loss of access to data	123	41%
Lost data	111	37%
Loss of user confidence in the system	100	33%
Screen message, interference, lockup	51	17%
Trouble reading files	36	12%
Unreliable applications	31	10%
System crash	29	10%
Trouble printing	24	8%

Trouble saving files	23	8%
Other	10	3%
Threat of someone losing their job	7	2%
Don't know	3	1%
None	2	1%
Total respondents	300	

Figure 3. Effects of Viruses. 2001



After realizing the attributes of viruses, IT departments can assess the companies' situation to make the appropriate step to design the viruses' prevention method and purchase the suitable anti-virus software. There are many anti-virus programs that IT departments can use to help their companies secured from viruses. But under the limited budget and resources in IT departments of small business, it should consider carefully to decide what kind of anti-virus applications are good for their small firms. According to the survey that took place by ICSA Labs (see Table 4), the top three anti-virus products are Network Associates, Symantec Corporation, and Trend Micro. Network Associates had the 150 responses and 50 % of total respondents using its anti-virus products. The second place was Symantec Corporation in 133 votes and 44 % of respondents. Trend

Micro was in the third place, having 33 votes and 8 % in respondents. In the Figure 4, it became apparent that the Network Associates and Symantec Corporation have occupied most of companies' anti-virus software market.

Table 4. Use of specific anti-virus products by frequency of response. (Bridwell & Tippet, 2001, p. 29)

Product	Frequency	%
Network Associates	150	50%
Symantec Corporation	133	44%
Trend Micro	23	8%
Computer Associates	17	6%
Command Software	10	3%
Don't know	4	1%
None	3	1%
Sophos, Inc.	2	1%
<b>Total respondents</b>	<b>300</b>	<b>&gt;100%</b>

Figure 4. Use of specific anti-virus products by frequency of responses

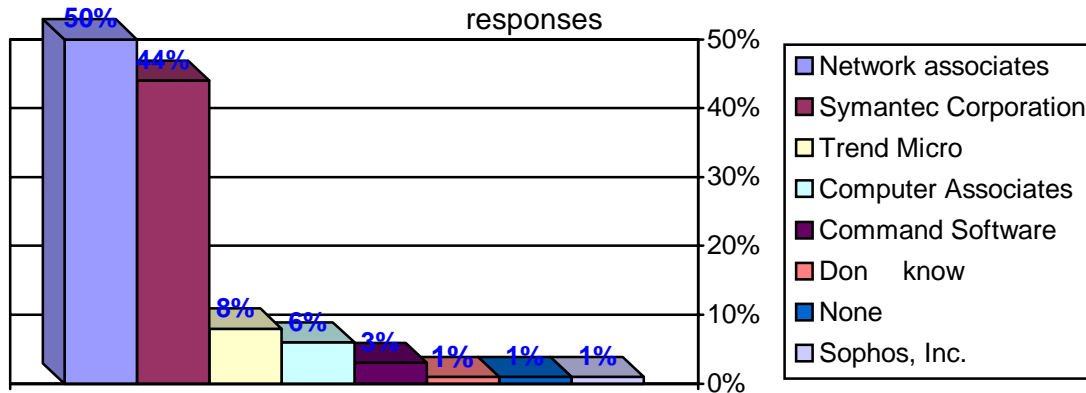


Table 5. Use of specific anti-virus products by number of PCs. (Bridwell & Tippet, 2001, p. 30)

Product	Total PCs	%
Symantec Corporation	316,015	42%
Network Associates	285,501	38%
Trend Micro	62,020	8%
None	49,000	6%
Computer Associates	26,772	4%
Command Software	9,554	1%
Don't know	5,150	1%
Sophos, Inc.	1,600	1%
<b>Total PCs</b>	<b>755,612</b>	<b>100%</b>

In Table 5, it showed that the similar results that based on the number of PCs. The products of Symantec Corporation were the most anti-virus products installing on the computers. As a result, the anti-virus products of Symantec Corporation and Network Associates have been total 80 % in companies' anti-virus market.

After understanding the characteristics of viruses and their distribution, IT departments in small firms can purchase suitable computer viruses prevention software for their companies. According the top three popular anti-virus products, the Table 6 is a comparison of anti-virus applications among Symantec Corporation, Network Associates, and Trend Micro. Besides the slightly differences in anti-virus function, the obvious differences are their prices. On the condition, a company having 100-computer, if this company want to buy anti-virus software for its 100 computers, it takes \$2,295 in Symantec Corporation's product—Norton AntiVirus Corporate Edition 7.6 and it also have to spend \$1,731 for second year's virus pattern update fee. Under the same condition, using Network Associates product, McAfee VirusScan ASaP, will take \$4.13 for per computer in every month. Therefore, it totally costs \$4,956 for 100 computers in a year. This would make small firms to consider their burden in purchasing McAfee VirusScan ASaP. The cheapest product among these three products is Trend Micro's Trend OfficeScan Corporate Edition. Trend OfficeScan Corporate Edition costs \$900 for companies' purchasing for 100 computers' licenses. From \$4,956, \$2,295 to \$900, those three products have apparent difference in the products' prices.

Those three products have the server, workstation, and e-mail protection. Norton AntiVirus Corporate Edition 7.6 and Trend OfficeScan Corporate Edition are the same Server-Client structure. But Trend OfficeScan Corporate Edition need a specific platform

OS in server---Microsoft Small Business Server 2000. Those two products have centralized real-time management and reporting. And in client platforms, they both support windows Me/98/95, windows 2000 professional/server, and windows NT 4.0 SP4.

Table 6. Comparison of anti-virus products

	<b>Symantec Corporation</b>	<b>Network Associates</b>	<b>Trend Micro</b>
<b>Anti-virus product</b>	<b>Norton AntiVirus Corporate edition 7.6</b>	<b>McAfee VirusScan ASaP</b>	<b>Trend OfficeScan Corporate Edition</b>
<b>Platforms (Server)</b>	Windows NT 4.0- SP5; Windows 2000 Server, Advanced server, Professional; windows XP Professional.	VirusScan ASaP doesn't install in specific Server. VirusScan ASaP is designed as an On-Access scanner. Therefore, it can be used on low volume, less-busy servers. McAfee recommend using NetShield on servers (as provided in MVD described above), which can be custom, configured for updating/upgrading and scheduling scans.	Microsoft Small Business Server 2000; Windows NT (minimum required: 4.0 w/SP3 or Windows 2000 or above), NetWare (supported versions: 3.12, 4.x, 5.x)
<b>Platforms (Client)</b>	Windows NT 4.0-SP4; Windows 2000 Professional, Server, Advanced Server; Windows XP Home, Professional Editon; Windows Me/98/95;	Windows NT 4.0-SP4; Windows 2000 Professional; Windows XP; Windows Me/98/95; IE 4.01 SP2	Windows NT 3.51/4.0; Windows 2000 Professional; Windows Me/98/95;
<b>Multiple platforms management</b>	Yes.( Windows, DOS, Netware)	No. (Windows only)	Yes. (Windows, DOS, Netware)
<b>Real-time protection</b>	Yes. (Including viruses spread via PDA synchronization.)	Yes.	Yes.
<b>E-mail protection</b>	Yes.	Yes.	Yes.
<b>Automatic Virus Pattern Update</b>	Yes.	Yes.	Yes.
<b>Unit Price</b>	\$22.95	\$4.13 (Per Month)	\$900
<b>Price-100 User</b>	\$2,295.00	\$4,956 (1 Year)	\$900
	2 <sup>nd</sup> year Upgrade insurance--\$1,731		

The McAfee VirusScan ASaP doesn't have the server-client structure that likes other two products. Its anti-virus program's server is in McAfee anti-virus center. Thus, this product depends on the Internet more than Norton AntiVirus Corporate edition and Trend OfficeScan Corporate edition. Therefore, it is suitable to the companies that have broadband connection to the Internet. Its advantage is, basically, the direct connection to McAfee Company and to get the virus alert early. Its disadvantage is the high price. This would make companies to think about the budget in anti-virus.

In conclusion, there are tens of thousands of computer viruses spreading around the world. Therefore, it is inevitable to face the most threat of computer security and to protect all valuable data that is stored in computers. After understanding the attributes of viruses and the needs for virus prevention, then according to the companies' conditions, small firms' IT departments can purchase the suitable anti-virus software with limited budget and affordable burden to match companies' needs in the most efficient effort to against computer viruses.

List of tables:

Table 1. Virus classification statistics (September 1999)

Table 2: Comparison of virus's activity between 1996-2001.

Table 3. Effects of viruses, 2001.

Table 4. Use of specific anti-virus products by frequency of response.

Table 5. Use of specific anti-virus products by number of PCs.

Table 6. Comparison of anti-virus products

List of figures:

Figure 1. Virus classification statistics (September 1999)

Figure 2. Comparison of virus's activity.

Figure 3. Effects of viruses, 200.

Figure 4. Use of specific anti-virus products by frequency of response.

Bibliography:

McGuire Research Services, Inc., (1995, August 30). *Report of Results from a Telephone Survey of 250 MIS Managers in Major U.S. Businesses.*

Therriault, Carole (1999, October). *An introduction to computer viruses.* Sophos.

Retrieved from the World Wide Web:

<http://www.sophos.com/virusinfo/whitepapers/videmys.html>

Trend Micro. *Virus Primer.* Retrieved April 3, 2002 from the World Wide Web:

<http://www.antivirus.com/vinfo/vprimer.htm>

Symantec Corporation. *Online Virus Encyclopedia index.* Retrieved from the World

Wide Web: <http://www.symantec.com/avcenter/vinfodb.html>

Bridwell, M. Lawrence, & Tippet, Peter. (2001). *ICSA Labs 7<sup>th</sup> annual Computer Virus Prevalence Survey 2001.* ICSA Labs.

Symantec Corporation. *Norton AntiVirus Corporate edition 7.6.* Retrieved from the

World Wide Web:

<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=23>

Network Associates. *McAfee VirusScan ASaP.* Retrieved from the World Wide Web:

<http://www.mcafee2b.com/services/virusscan-asap.asp>

Trend Micro. *Trend OfficeScan Corporate Edition.* Retrieved from the World Wide Web:

<http://www.antivirus.com/products/osce/>