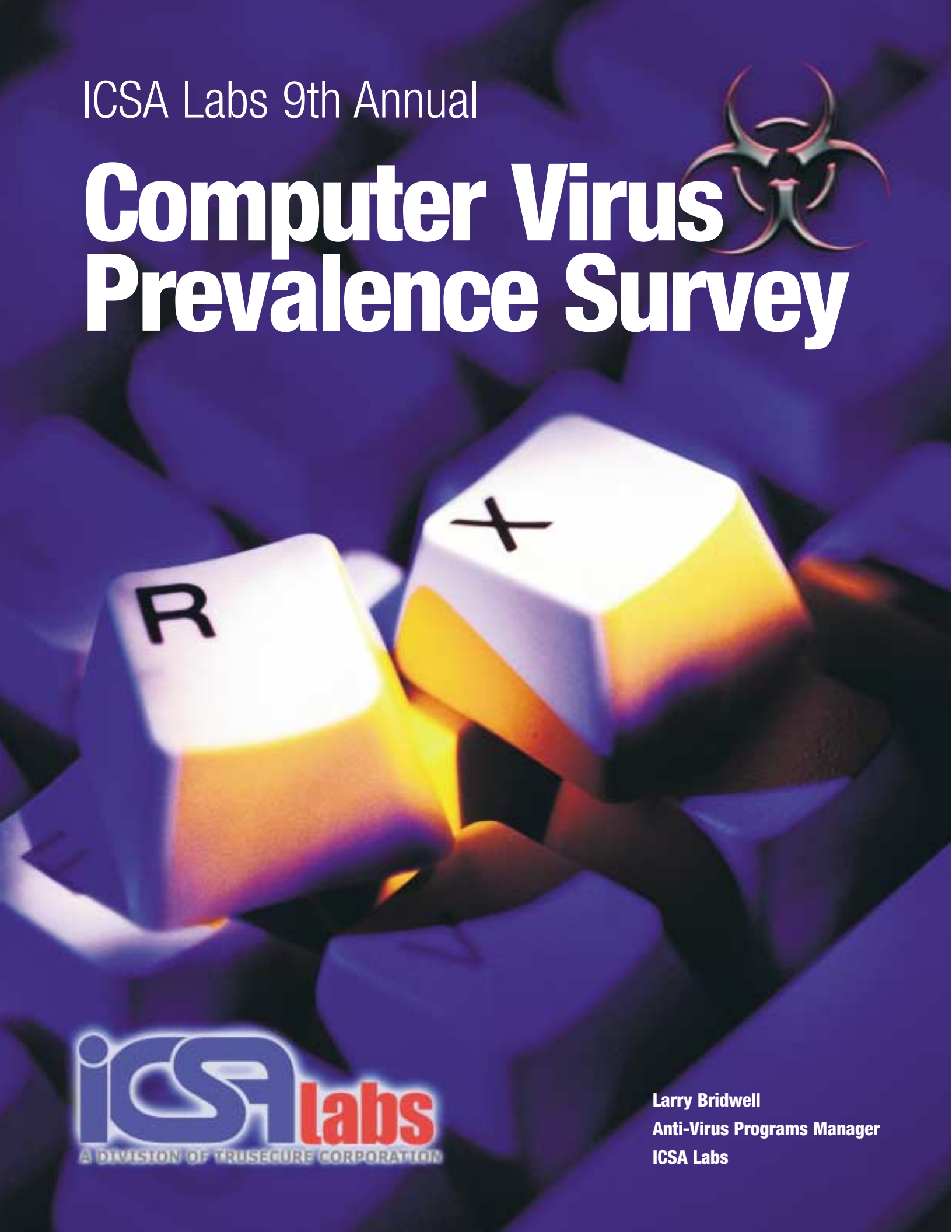
ICSA Labs 9th Annual

Computer Virus Prevalence Survey

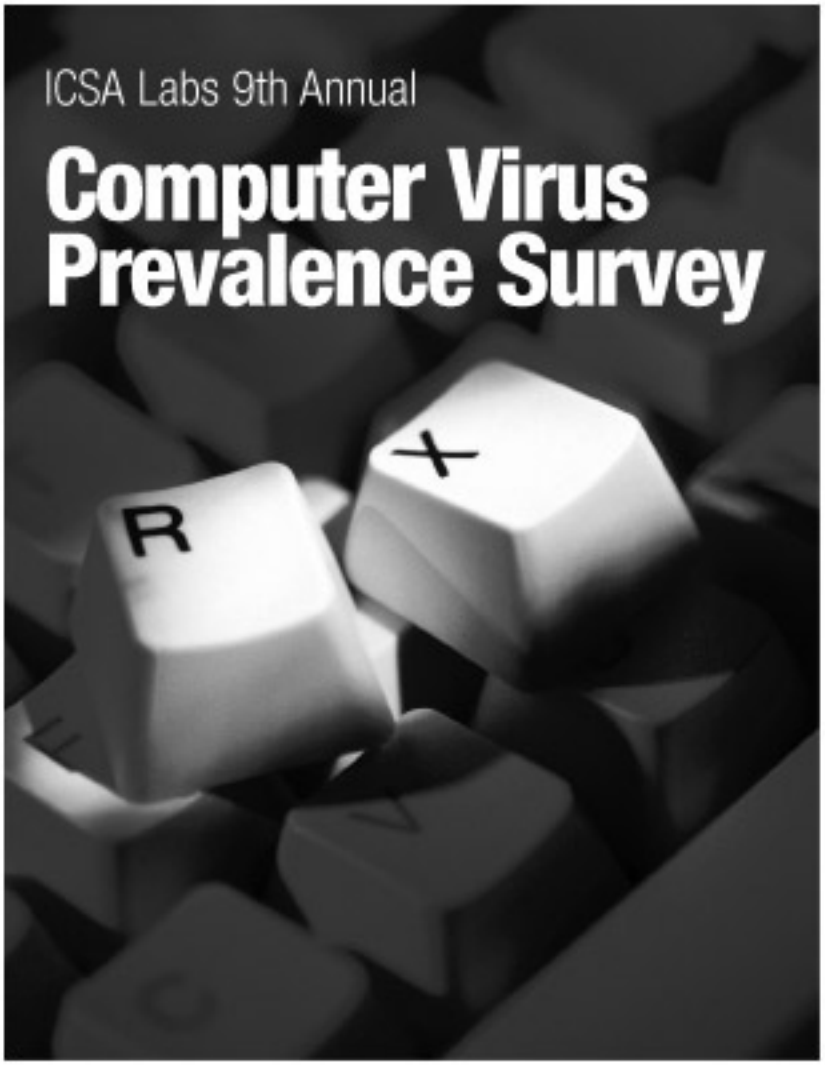


ICSA labs
A DIVISION OF TRUSECURE CORPORATION

Larry Bridwell
Anti-Virus Programs Manager
ICSA Labs

ICSA Labs 9th Annual

Computer Virus Prevalence Survey



GOLD SPONSOR
NETWORK ASSOCIATES

SILVER LEVEL
MICROSOFT CORPORATION

BRONZE LEVEL
ESET, LLC
TREND MICRO, INC.

EDUCATIONAL SPONSOR
MIS TRAINING INSTITUTE

ICSA labs
A DIVISION OF TRUSECURE CORPORATION

Larry Bridwell
Anti-Virus Programs Manager
ICSA Labs

Table of Contents

List of Figures

List of Tables

ICSA Labs Virus Prevalence Survey 2003

Executive Overview

ICSA Labs' annual Virus Prevalence Survey gathers data to measure the prevalence of computer viruses and malware in medium to large companies. The Ninth Annual Virus Prevalence Survey 2003 was organized by the ICSA Content Security Labs and the corporate sponsors who support the survey each year. Qualified respondents who work for companies and government agencies with more than 500 PCs, two or more local area networks (LANs), and at least two remote connections access the survey questionnaire and enter data over a secure connection. The data is collected, normalized, and analyzed. The annual report describes the existing computer virus problem and attempts to interpret trends of virus propagation and infection vectors, and explores possible risk mitigation methods.

HOW DID RESPONDENTS PERCEIVE THE EVOLUTION OF THE VIRUS PROBLEM?

Without a doubt, the respondents believe the problem is worsening. Twelve percent of this year's respondents felt the problem was *About the Same* or *Better* - and last year was considered a bad year! Eighty-eight percent of respondents felt the virus problem was either *Somewhat Worse* or *Much Worse.*

HOW COMMON ARE VIRUS ENCOUNTERS?

This year's sample of respondents reported more than 2.7 million virus incidents on more than 900,000 desktops, servers, and perimeter gateways. This translates to 201 encounters per 1,000 machines per month over the survey period from January 2003 through December 2003, with a rate of 108 infections per site per month by the end of the survey period, November - December 2003.

WHAT ARE THE CHARACTERISTICS OF VIRUS DISASTERS?

For this survey, a virus disaster had to meet the historical criterion of 25 or more PCs or servers infected at the same time with the same virus or a virus incident *causing significant damage or monetary loss to their organizations*. When the latter criterion was used, the respondents were asked to qualify the disaster, i.e. number of machines, loss of data, loss of productivity, revenue loss, etc. Based on this definition, 92 of the 300 qualified respondents reported incidents of disaster.

WHAT ARE THE EFFECTS OF VIRUS DISASTERS?

In the 2002 survey, 80 respondents reported a disaster while in 2003 that number increased to 92 reports of disaster. Another significant difference in 2003 was the return of the *Outbreak* virus incident. A major outbreak incident in the form of W32/Slammer kicked off 2003. Slammer was an automatic network worm that spread around the world in less than 15 minutes! The Internet traffic created by Slammer in its search for computers to infect caused considerable slowdown of the Internet and affected telecommunications and some financial networks. A handful of other outbreak incidents followed Slammer in 2003.

Another interesting point was that of the 92 reported disasters, there was at least one reported in each month – a first for our annual surveys. Disaster recovery time increased only slightly

from 23 person-days to 24 person-days. Interestingly, while recovery time increased only slightly, recovery costs increased a significant 23 percent. In 2002, respondents reported average recovery costs of approximately $81,000. This year that number escalated to almost $100,000. Historically, we have found that numbers we obtain from the technical person responsible for viruses is underestimated by a factor of seven or eight when considering both direct and indirect costs. With that proportional underestimation in mind, one could easily determine that the average company might have a much larger cost-per-virus disaster when considering both soft and hard costs.

HOW ARE ANTI-VIRUS PRODUCTS USED?

Almost all (98 percent) of respondents report that at least 90 percent of their machines are protected by anti-virus software products. The products protecting the majority of desktops, servers, and perimeter devices are those sold by Network Associates, Inc. and the Symantec Corporation.

Last year we saw virus protection of email gateways increase significantly with more than 90 percent of respondents reporting installation of anti-virus products. This year we see a slight increase to 94 percent reporting coverage of email gateways. At the same time, only 50 percent of respondents protect their firewalls, and 58 percent have installed anti-virus software on their proxy servers. This year's survey respondents also report that gateway filtering (blocking, quarantining, or stripping) of Email and attached files have increased to 88 percent.

ICSA Labs Virus Prevalence Survey 2003

Survey Objectives

The objectives of this project are to: examine the prevalence of computer viruses in mid- and large-sized organizations; describe the computer virus problem in computer networks, including desktop computers application and file servers, and perimeter devices such as firewalls, gateways, and proxy servers; and observe trends in computer virus growth, infection methodologies, and attack vectors. The scope of the survey report includes Intel-based or Intel-compatible PCs[1] at sites with more than 500 PCs, multiple LANs, and two or more remote connections. We surveyed only the commercial, government, and industrial business sectors.

Research Methodology

CONFIDENCE

Data is collected from 300 qualified respondents. The sample size provides an accuracy rate of ±6 percent with a confidence limit of 94 percent for questions that relate to the entire data sample.

SELECTION

We selected survey participants from a qualified list of sites with 500 or more PCs, two or more LANs, and two or more remote connections at that site. We also screened respondents to insure that they were the persons most responsible for computer virus protection within their organizations.

ROUNDING

Occasionally percentages will total more than 100 percent because some questions allowed for multiple responses. In some cases, rows or columns in tables may total either 99 percent or greater than 100 percent due to rounding. Likewise, charts or graphs may show less than 100 percent due to the exclusion of *Don't Know*, *Refused*, or *Other* responses.

PREVIOUS WORK

Some of the results of this survey can be directly compared with the results of five previous surveys:

A previous survey conducted for ICSA during Jan through Feb 2002
A previous survey conducted for ICSA during May through June 2001
A previous survey conducted for ICSA during May through June 2000
A previous survey conducted for ICSA during March through May 1999
A previous survey conducted for ICSA during March through May 1998
A previous survey conducted for ICSA during March 1997
A previous survey conducted for ICSA during March 1996

[1]Data gathered for Macintosh and other non-Intel servers and workstations may be referred to. However, they will only be considered anecdotal in this report.

Principal Findings

2003 Demographics

The 2003 survey represents a total of 962,278 desktops, servers, and perimeter gateways. The average site in the survey had 3,027 PCs (the median was 1,872) and 181 file and application servers (median was 68).

How Common Are Virus Encounters?

All of the companies responding to the survey experienced at least one virus encounter during the survey period.

These organizations experienced more than 2.7 million encounters during the 12-month period from January 2003 through December 2003. This translates to 201 encounters per 1,000 machines per month over the survey period with a rate of 108 infections per site per month by the end of the survey period. This rate continues the trend of an increase in infection rate each year. Most noteworthy is the marked increase in *encounters* versus actual infections. Further examination suggests that this difference is due to filtering and blocking viruses at the gateway before they can enter the network. We will discuss this in detail in the Discussion section at the end of the report.

In a comparison of the survey data for 1996 – 2003, Table 1 shows that from 1996 through 1998, virus encounters show a steady rise of approximately 12 virus inflections per 1,000 machines per month each year through 1998 and again from 1999 – 2001. However, from 2001 to 2003, that number remains flat, with only a slight increase in infections. We derived these data by determining the average of the infection rates reported for the two months immediately before collection of survey data. We selected the prior two months (November and December) for comparison because historically they produce the greatest accuracy in participant responses.

Survey Year	Nov. – Dec.
1996	10
1997	21
1998	32
1999	80
2000	91
2001	103
2002	105
2003	108

Table 1: Monthly rate of infection per 1,000 PCs

Figure 1 displays the data from Table 1 in a chart to give a graphical representation of the growth rate of virus infections. The rate spike from 1998 to 1999 specifically relates to the Melissa outbreak incident of 1999 and its mass mail payload.

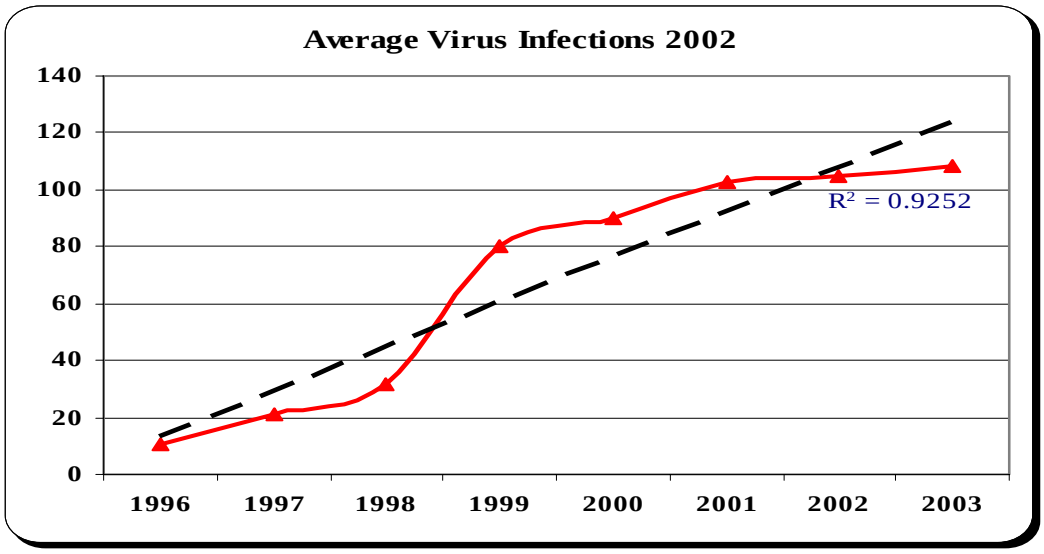


Figure 1: Encounters per 1,000 PCs per month

CHANCE OF A DISASTER

For the purposes of this survey, a virus disaster is defined as an incident in which 25 or more machines experienced a single virus at or about the same time. Due to the changes in virus infection and propagation vectors, we have expanded the definition to include virus incidents causing their organizations significant damage or monetary loss. Survey respondents were asked if their organizations had experienced a "disaster" during the survey period; 92 responded in the affirmative.

RESPONDENT PERCEPTION OF THE VIRUS PROBLEM

We asked respondents to express their opinion of the computer virus problem, and to respond on a scale of *Much Worse* to *Much Better*. Figure 2 below represents these answers. The respondents clearly believe that the problem of computer viruses in general was much worse in 2003 than in 2002. Of the respondents, only 12 percent felt the problem was about the same or better, the lowest percentage ever reported in this survey.

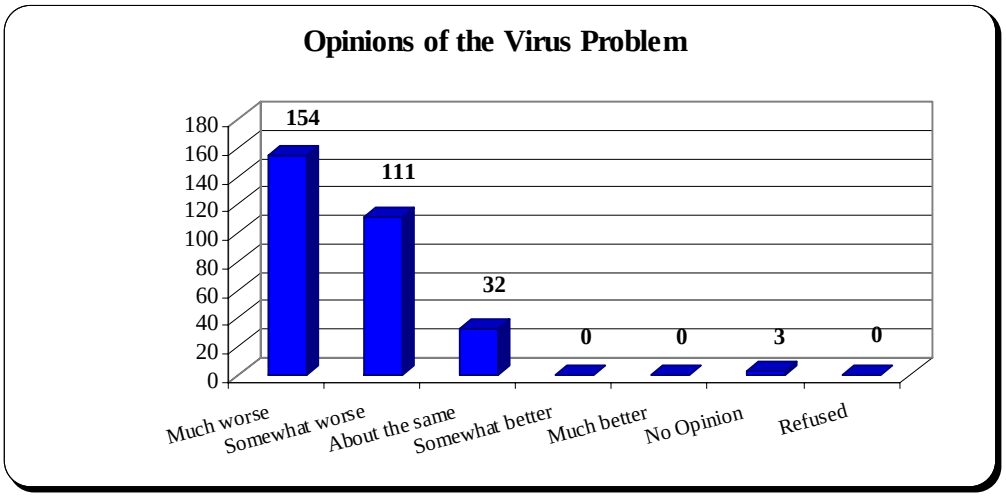


Figure 2 Opinions of the virus problem 2003

Detailed Findings

The Ever-Changing Picture of Computer Viruses and Their Prevalence

The primary objective of this work each year is to ask the question, "How has computer virus prevalence changed?" The findings detailed below offer insights into several significant changes in computer viruses. These include not only growth in prevalence, but also growth in the severity of payloads, consequences of infection, and changes in attack vectors. These detailed findings will also help us determine the risks posed by computer viruses .

VIRUS ENCOUNTERS VERSUS VIRUS INFECTIONS

As reported above, virus encounters continue to rise. Figure 3 below gives us a picture of the survey period January 2003 through December 2003.

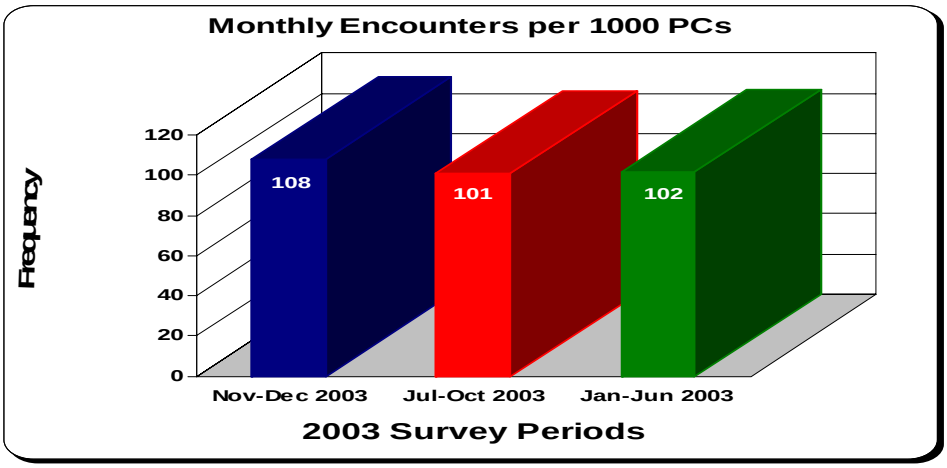


Figure 3: Encounters per month, 2003

TOP REPORTED VIRUSES

As we have noted in past years, certain viruses are more likely to spread than others are. Factors that determine whether a virus is likely to spread include the virus *type,* the infection *vectors,* and virus *payload.* Viruses such as mass mailers continue to grow in prevalence while others, such as simple macro viruses, are in decline and still others, like boot sector viruses, have all but disappeared. Respondents were asked which viruses affected their group. Due to the large number of known viruses and their many variants[2]; a lack of standardized identification scheme[3]; and, at times, poor record keeping, respondents were not always able to identify the viruses with certainty. In all instances, every effort was made to identify individual responses at least to the virus family name. In instances where exact names were not known, partial names were given, or virus types were given and the data was pooled as [*Type], unspecified.*

in contrast to 2002, 2003 saw a noteworthy increase in serious viruses and saw a significant number of virus *Outbreaks*. In fact, several viruses were reported in numbers sufficient to have made the Top 10 list in previous year's surveys that did not make it in this year's top viruses. Table 2 below presents the Top 10 reported viruses for 2003 by rank from 1 to 10.

The table shows virus encounters per month for the period January – December 2003. Note that of the Top 10 reported viruses, nine were either mailers or mass mailer viruses. The exception was Blaster, which was an automatic network-type worm and had the ability to connect to and infect computers over a network or Internet connections.

2003 Rank	Virus Name	Encounters
1	W32/Yaha	32
2	W32/Klez	29
3	W32/Mimail	22
4	W32/BugBear	18
5	W32/SirCam	12
6	W32/Sobig	7
7	W32/Dumaru	6
8	W32/Swen	5
9	W32/Lovgate	4
10	W32/Blaster	2

Table 2: Top viruses for 2003

[2] Over 70,000 known

[3] In 1991, a group of security experts known as the Computer Anti-Virus Researcher Organization (CARO), developed a computer virus naming scheme and it was dubbed the "1991 New Virus Naming Convention" (NVNC '91). This scheme promoted the now commonly used 'Family_Name.Group_Name.Variant' formulation as well as setting laying out guidelines for what NOT to use in naming viruses. While this scheme is being used by more companies with and with greater consistency than in the past, the fact is, there is no standardized identification or naming convention accepted and used by the entire anti-virus industry. There is research being done on this at this time.

Virus Disasters

Survey respondents were asked, "Has your group had a virus disaster anytime since January 2003?" Table 3 shows that 92 (31 percent) reported experiencing such an event.

Answer	Frequency
Yes	92
No	192
Don't know	16
Refused	0
Total	300

Table 3: Respondents experiencing virus disaster

Date of last virus disaster?

Respondents were asked the month of their most recent disaster. Table 4 presents these as a frequency distribution. This table is sorted by calendar year beginning with January 2003.

Month of Last Disaster	Response	%
January 2003	11	12%
February 2003	3	3%
March 2003	2	2%
April 2003	1	1%
May 2003	4	4%
June 2003	2	2%
July 2003	2	2%
August 2003	39	42%
September 2003	3	3%
October 2003	8	9%
November 2003	7	8%
December 2003	10	11%

Table 4: Date of most recent disaster

There were reports of at least one disaster in each month of 2003. Fifteen different viruses were responsible for the reported disasters. Notably, there were two separate "spikes," one in January 2003 and the other in August 2003. The January 2003 spike was undoubtedly due to the Slammer outbreak as well as the appearance of Lirva and the first SoBig variant. August 2003 was arguably one of the worst months for viruses since this survey began with Blaster, Nachi, and SoBig and Mimail variants appearing.

WHICH VIRUS CAUSED THE MOST RECENT DISASTER?

We asked the survey participants to identify the viruses responsible for their latest disaster. Table 5 lists these viruses, the frequency of response, and the total number of machines affected in the disaster. The list is sorted by number of machines affected.

Virus Name	Frequency	Machines Involved
W32/Blaster	12	129,087
W32/Slammer	16	84,921
W32/Sobig	6	23,761
W32/Klez	10	13,997
W32/Yaha	5	11,799
W32/Swen	7	10,760
W32/Dumaru	4	8,697
W32/Mimail	9	7,011
W32/Nachi	3	6,325
W32/Fizzer	2	5,768
W32/BugBear	5	4,987
W32/Lirva	2	4,732
W32/Sober	2	2,106
W32/SirCam	8	2,091
W32/Ganda	1	1,893

Table 5: Virus causing most recent disaster

HOW MANY MACHINES WERE INFECTED IN DISASTERS?

Based on the data above, Figure 5 below gives a graphical picture of the number of machines reportedly involved in the latest disasters. The total number of machines reported to be involved in disasters was 317,935.

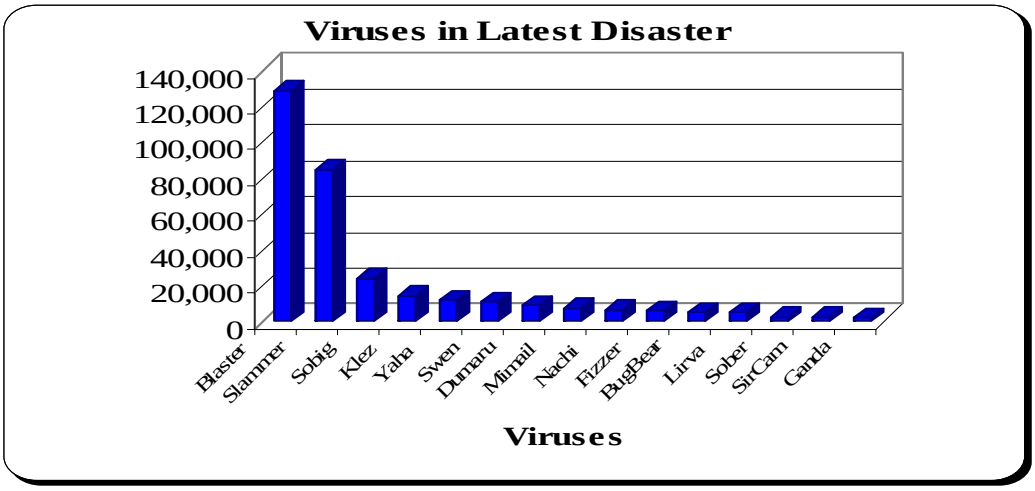


Figure 4: Viruses causing most recent disaster

What are the effects on victims of virus disasters?

HOW LONG WERE SERVERS DOWN?

Table 6 and Figure 5 show the pattern of responses on the question of how long servers were down after a virus disaster. Eighty-two (82) participants reported disasters with server involvement. The average server downtime reported was 17 hours. Fully 66 percent of responding companies reported downtime of ten hours or less.

Hours	Frequency	%
1	14	17%
2	9	28%
3	13	44%
4	4	49%
5	3	52%
10	11	66%
20	17	87%
30	4	91%
40	1	93%
50	1	94%
100	2	96%
200	2	99%
300	0	99%
400	1	100%
Total	82	100%

Table 6: Frequency distribution of server downtime

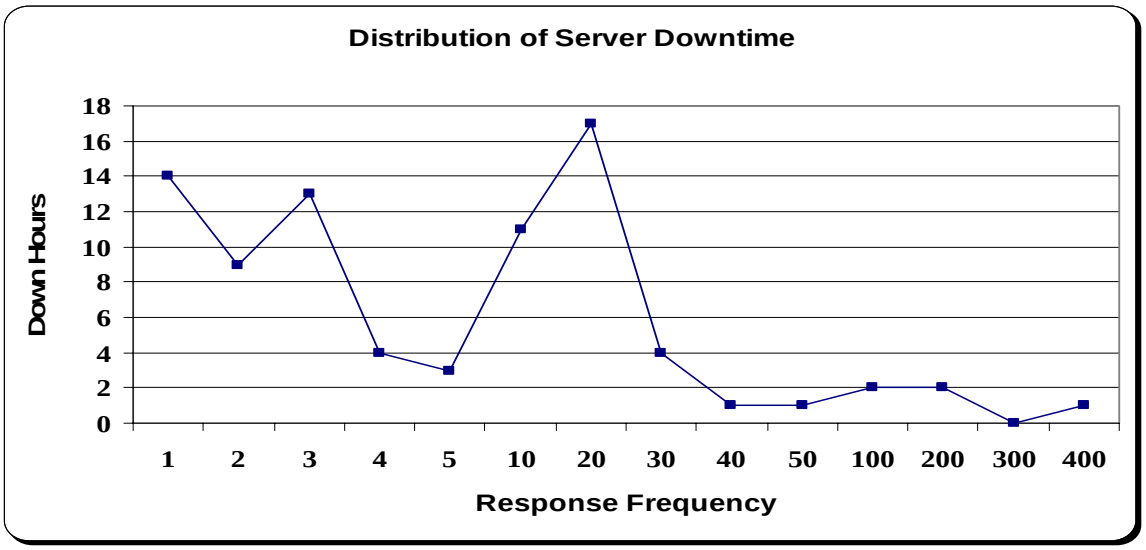


Figure 5: Frequency distribution of server downtime

WHAT WAS THE COST OF THE DISASTER IN PERSON-DAYS?

Respondents were asked how many cumulative person-days were lost during the disaster that affected their company. Table 7 is a frequency distribution of responses. Of those reporting disasters, 82 participants responded to this question. This number represents 89 percent of those reporting disasters. Of those responding, half of the respondents reported ten person-days or less. The median time for full recovery was 11 person-days and the average was 24 person-days.

Days	Frequency	%
0	3	4%
1	5	6%
2	3	4%
3	6	7%
4	5	6%
5	6	7%
10	13	16%
11	1	1%
12	3	4%
13	0	0%
14	1	1%
15	1	1%
20	13	16%
30	8	10%
40	3	4%
50	3	4%
100	4	5%
200	3	4%
300	1	1%
Total	82	

Table 7: Frequency distribution of person-days lost

Figure 6 show these results in a graphical representation. Note the two peaks at the ten- and twenty-day marks.

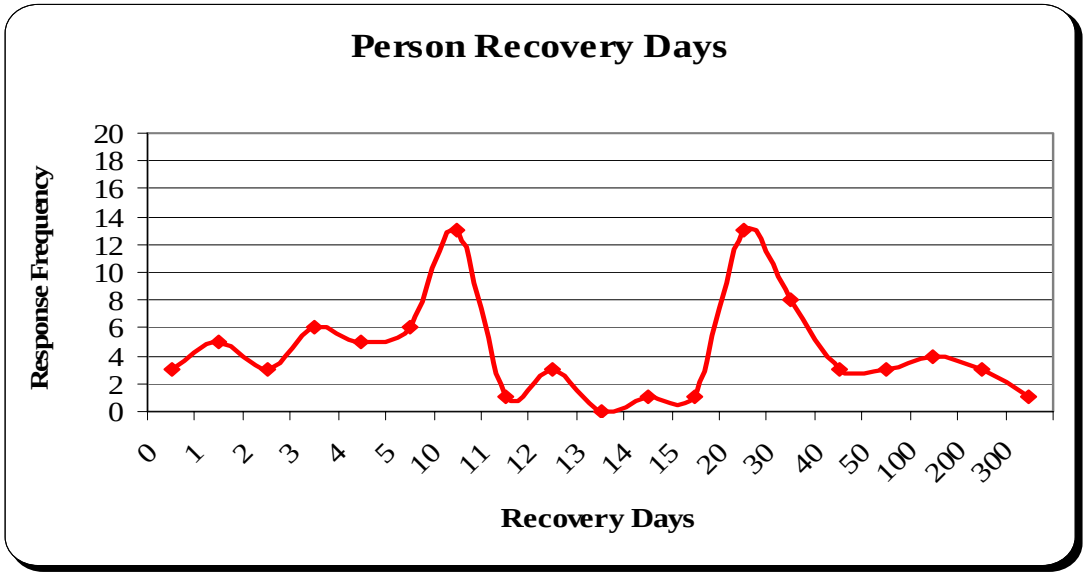


Figure 6: Loss in person-days due to disaster

What was the cost in dollars to your company?

We also asked respondents to estimate the cost in dollars for their latest disaster. Those responding were asked to consider ALL costs including such things as employee downtime, overtime to recover, lost opportunity, etc. Table 8 shows these responses.

Cost	Frequency	%
$2,500	2	2%
$3,000	0	0%
$5,000	12	15%
$10,000	19	23%
$20,000	9	11%
$30,000	9	11%
$40,000	6	7%
$50,000	5	6%
$100,000	8	10%
$200,000	4	5%
$300,000	1	1%
$400,000	1	1%
$500,000	1	1%
$1,000,000	3	4%
>$1,000,000	2	2%

Table 8: Frequency distribution of dollar costs

The average for dollar costs was more than $99,000. The median cost was $11,000 and the most frequent answer was $10,000. Again this year we see a large variance in the average, median, and most frequently stated costs due to three very large reports over $1,000,000 each. This is more easily recognized when depicted in Figure 7 below.

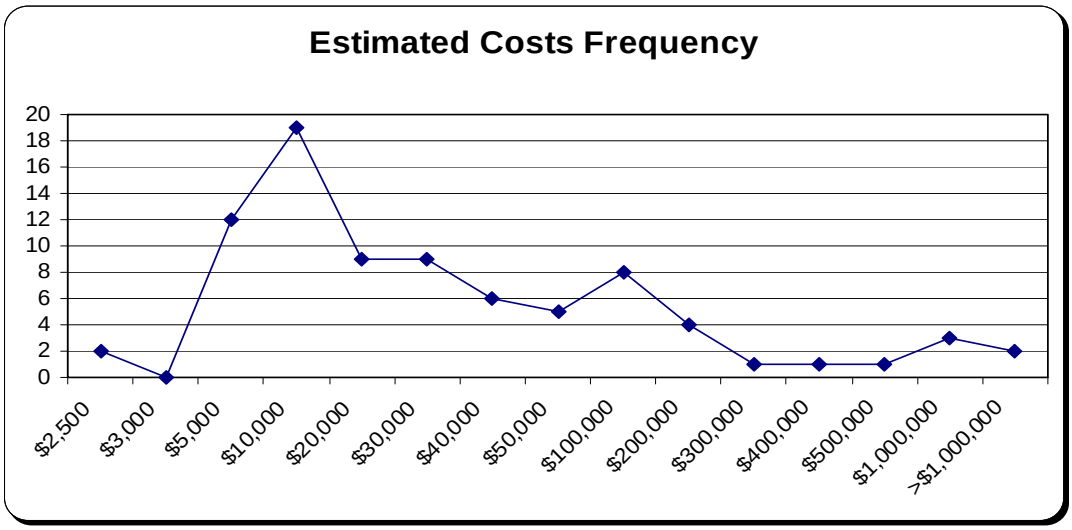


Figure 7: Distribution of dollar costs

Virus Impact

WHAT ARE THE ORGANIZATIONAL EFFECTS OF VIRUSES?

Virus disasters and incidents have organizational ramifications beyond the money, resources, and effort required to recover from such incidents. We asked the participants what organizational effects the latest disaster or incident had on the company or working group. Table 9 lists these data in decreasing order.

Response	Frequency	%
Loss of productivity	229	76%
PC was unavailable	201	67%
Corrupted files	175	58%
Loss of access to data	151	50%
Lost data	140	47%
Loss of user confidence	99	33%
Interference, lockup	54	18%
System crash	49	16%
Unreliable applications	41	14%
Trouble reading files	35	12%
Trouble saving files	22	7%
Trouble printing	17	6%
Threat of job loss	4	1%

Table 9: Effects of viruses

Respondents were allowed to choose as many effects as needed. Therefore, percentages add up to more than 100 percent. The data in this table is represented graphically by Figure 11 below.

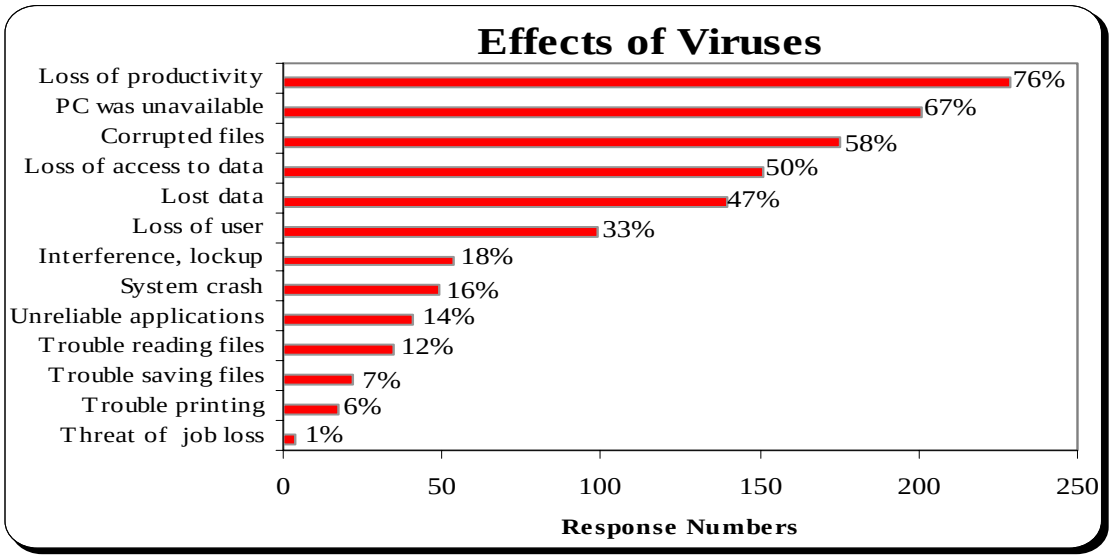


Figure 8: Effects of viruses

Where Do They Come From?

We asked respondents to identify the means of infection for their most recent virus incident, disaster, or encounter. Again, responses total more than 100 percent because participants were allowed to select more than one means of infection. Table 12 compares this year's responses to previous surveys.

Virus Source	1996	1997	1998	1999	2000	2001	2002	2003
Email Attachment	9%	26%	32%	56%	87%	83%	86%	88%
Internet Downloads	10%	16%	9%	11%	1%	13%	11%	16%
Web Browsing	0%	5%	2%	3%	0%	7%	4%	4%
Don't Know	15%	7%	5%	9%	2%	1%	1%	3%
Other Vector	0%	5%	1%	1%	1%	2%	3%	11%
Software Distribution	0%	3%	3%	0%	1%	2%	0%	0%
Diskette	71%	84%	64%	27%	7%	1%	0%	0%

Table 10: Sources of infection, 1996-2003

Respondents report that the email vector continues to be the primary means of virus spread. Also, note the continued increase in the Internet download and Web browsing vectors. There has also been a continued decrease in encounters through diskettes. It should be noted that even though diskettes have sharply decreased as a vector of virus spread, boot sector viruses still occasionally show up in incident reports.

Changes in Virus Distribution Mechanisms

To focus on the major changes in virus distribution vectors, we have grouped the various vectors from Table 10 into four categories: email, diskettes, Internet downloads, and Internet other. We compare the data from this year to data gathered in previous surveys. Figure 9 depicts these comparisons.

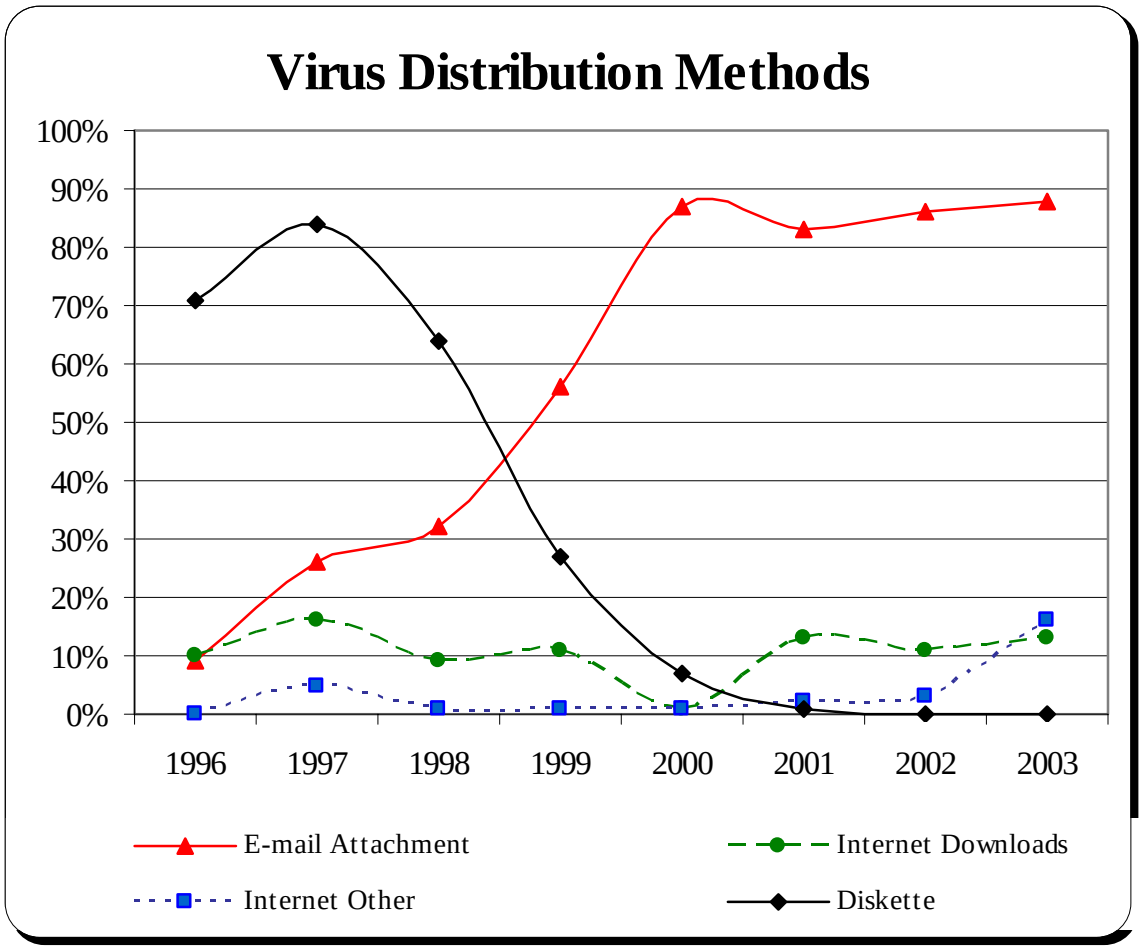


Figure 9: Virus encounter vectors

Usage of Anti-Virus Products

Overall Level of Usage

The survey also attempts to determine what percentage of desktops are covered by anti-virus products. The survey asks respondents, “How many desktops have anti-virus protection?”

This year, 98 percent of the 300 qualified respondents reported that at least 90 percent of desktop computers are protected with anti-virus software; 83 percent claimed 100 per cent protection. Table 11 gives a frequency distribution sorted by frequency of response.

Distribution	Frequency	Percentage
0%	249	83%
10%	45	15%
20%	2	1%
30%	2	1%
40%	2	1%
50%	0	0%
60%	0	0%
70%	0	0%
80%	0	0%
90%	0	0%
100%	0	0%

Table 11: Anti-Virus software usage

Figure 10 shows the same data expressed as the percentage of desktops that were covered by anti-virus products and includes the cumulative percentage covered.

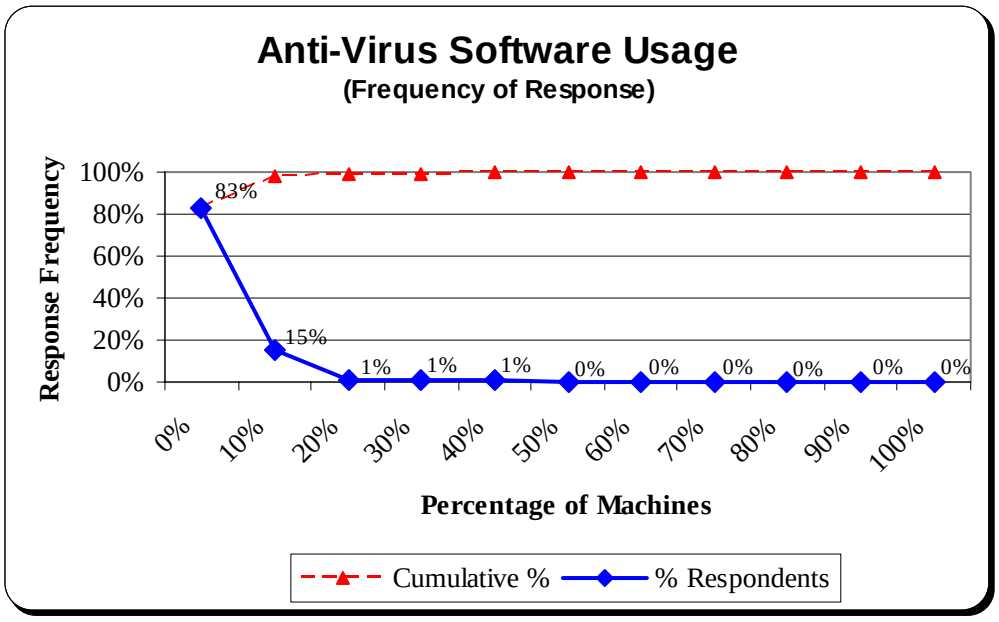


Figure 10: Desktop anti-virus usage

ANTI-VIRUS PRODUCTS DISABLED ON DESKTOPS

Participants were asked what percentage of desktops had anti-virus installed, but not running. Figure 11 represents the frequency of distribution in a graphical format.

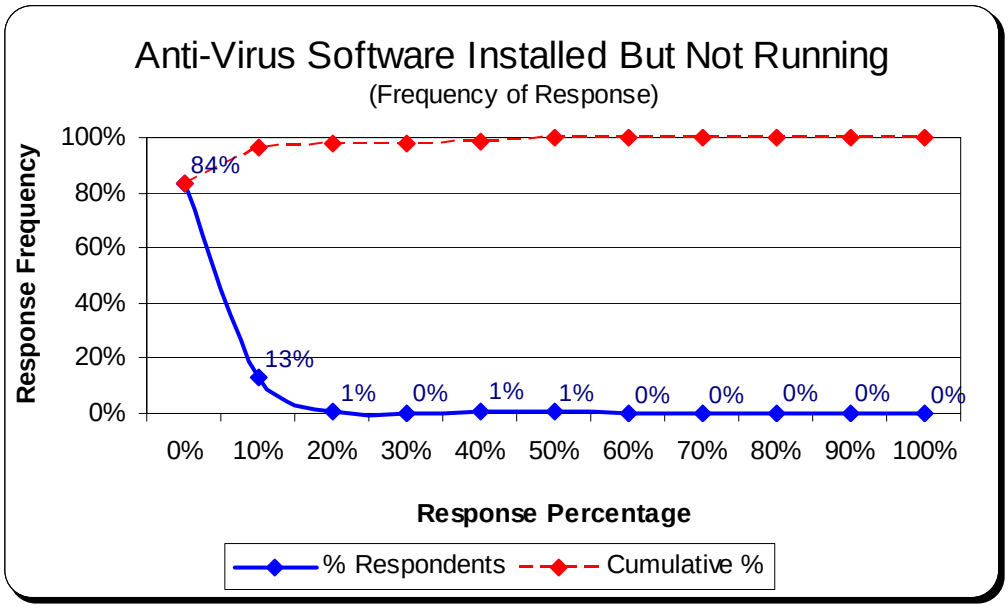


Figure 11: Desktops with anti-virus disabled

These data show that very few of the respondents felt that significant numbers of the desktops for which they were responsible had anti-virus products that were not running. Eighty-four percent answered that none of their desktops had non-functioning anti-virus products; over 97 percent claimed that no more than 10 percent were not running. If these reports are accurate it is indeed good news. However, based on previous survey results and observations of industry and user trends, this number seems somewhat optimistic.

ANTI-VIRUS PRODUCTS EMPLOYED ON DESKTOPS

Table 12 is list of anti-virus companies that make anti-virus products and reported usage of each company's products. The table gives both frequency of response and number of desktops. The frequency of response category may add up to more than 100 percent as some organizations use multiple products.

Product	Response Frequency	Frequency Percent	Desktops Response	Desktops Percent
Symantec Corp	142	37%	388,698	43%
Network Associates	131	34%	355,520	40%
Trend Micro	47	12%	89,437	10%
Computer Assoc	41	11%	47,691	5%
Command Software	11	3%	7,708	1%
Sophos, Inc.	10	3%	9,103	1%

Table 12 Desktop anti-virus products in use:

Symantec Corporation and Network Associates continue to maintain their market share (at least within the reports of this survey sample). However, their lead this year is not as great as

in past years. Figure 12 shows the graphical results of the survey taking into consideration only whether a respondent reported using one or more specific anti-virus products on the organization's desktops

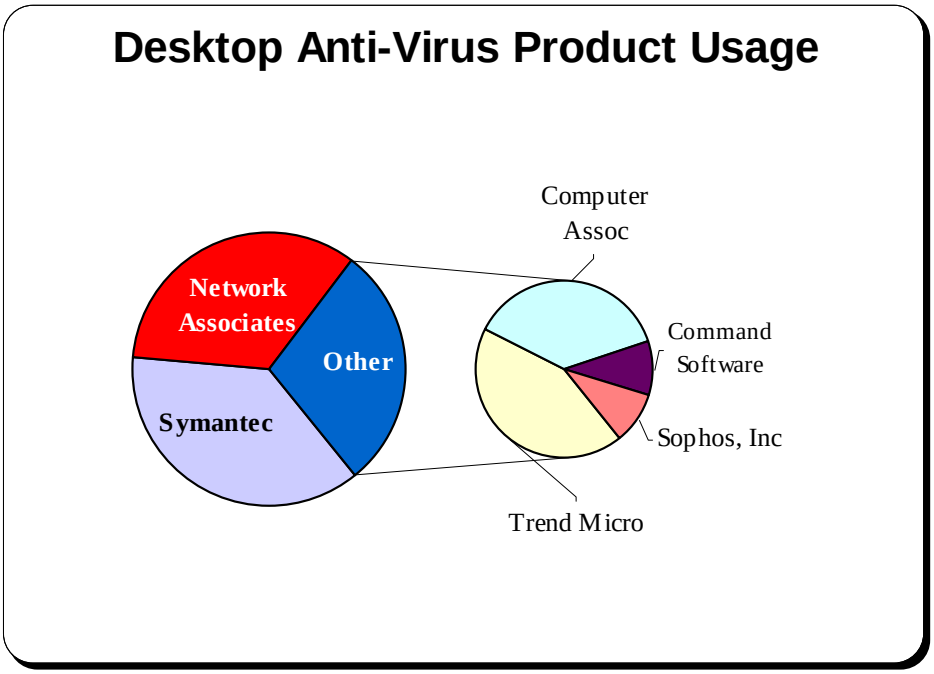


Figure 12: Desktop coverage by frequency of response

We also asked respondents what mechanisms were in use on their anti-virus-protected PCs. Table 13 shows their responses.

Method	Frequency
Users check diskettes and files for viruses	81
Anti-virus software scans hard drive for viruses every boot-up	278
Anti-virus software scans hard drive for viruses every login	225
Anti-virus software scans full time in the background	295
Other periodic anti-virus detection on the desktop	102
Other full-time anti-virus detection on the desktop	30

Table 13: Respondents using specific anti-virus methods

Survey responses show that most companies in the sample (89 percent) use full-time background virus protection at the desktop. In addition, 74 percent of companies scan desktops at boot-up. Figure 13 below shows this data as a graph.

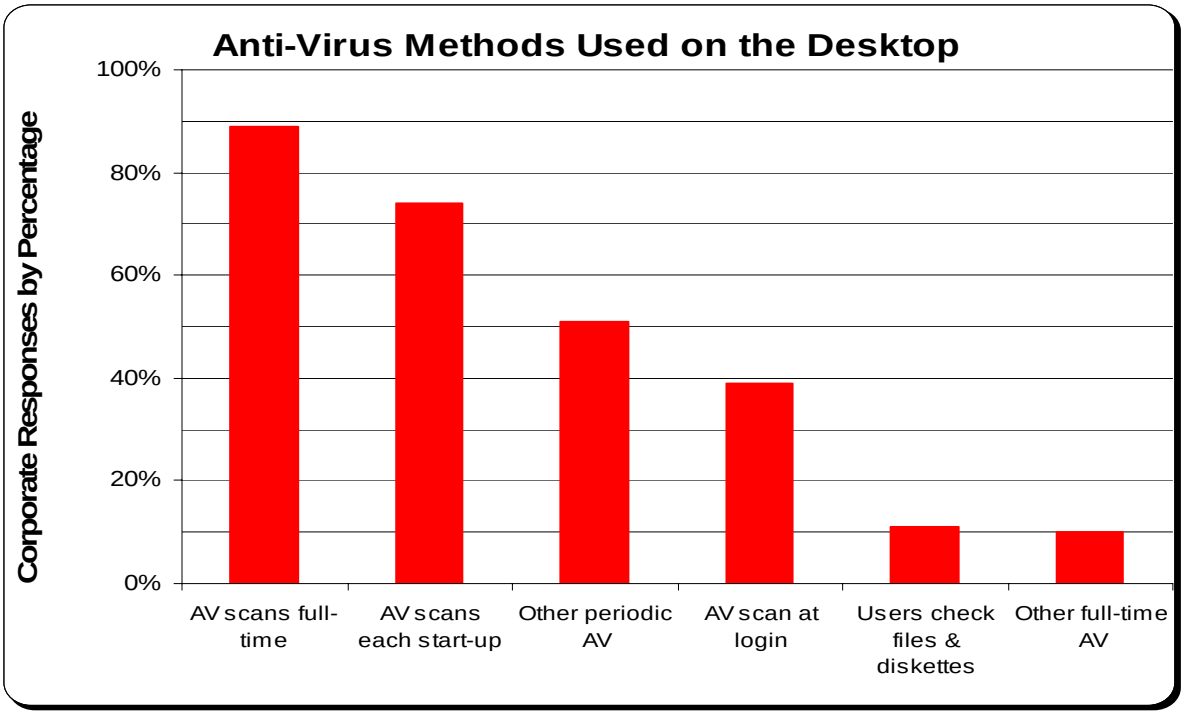


Figure 13: Anti-virus Methods Used

Perhaps even more interesting than the number of organizations using various methods was the number of PCs on which they applied these methods. Using the data detailing how many PCs for which each respondent was responsible, we computed the total number of desktops in the sample of respondents who gave numerical estimates of the usage of various methods. With that number, we were able to compute the proportion of desktops where they used those methods. Table 14 lists the total PCs using various methods.

Method	Desktops	Percentage
Anti-virus software scans for viruses full time in the background	835,979	89%
Anti-virus software scans hard drive for viruses every boot-up	695,083	74%
Anti-virus software scans hard drive for viruses every login	366,328	39%
Users check diskettes and downloads for viruses.	103,323	11%
Other periodic anti-virus detection on the desktop?	103,323	11%
Other full-time anti-virus detection on the desktop	93,930	10%

Table 14: PCs using specific anti-virus methods

SERVER ANTI-VIRUS METHODS

We also asked our respondents what anti-virus methods they used on file and application servers. Figure 14 shows the response for both the percentage of responding companies and the total number of servers using particular methods. Again, a clear majority (93 percent) depend on full time background virus protection

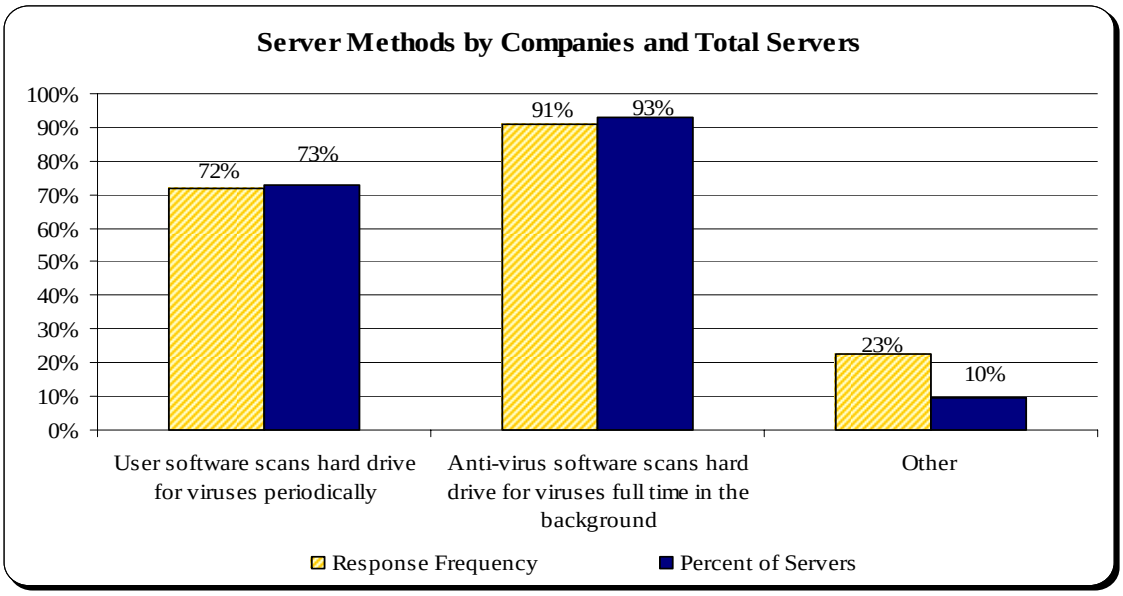


Figure 14: Anti-virus methods used on file servers

ANTI-VIRUS USAGE ON PERIMETER SERVICES

We asked respondents what percentage of their email servers, proxy servers, and firewalls were covered by anti-virus methods. Table 15 shows the results of their responses.

Coverage %	Email	Proxy	Firewalls
100%	281	177	151
90%	11	14	22
80%	2	2	0
70%	0	1	0
60%	2	0	0
50%	1	3	1
40%	0	0	0
30%	0	0	0
20%	0	0	1
10%	0	0	0
0%	3	103	125

Table 15: Perimeter coverage by frequency distributions

As has been the case since we began asking for this information, there is usually a bimodal distribution. Respondents report either no protection on perimeter gateway services or cover all of their perimeter services. Only a very small percentage claim percentages between 10 percent and 90 percent.

Figure 15 below charts the growth of reported perimeter protection since the 1997 survey. ICSA Labs began recommending full anti-virus coverage on perimeter gateways after the 1997 survey.

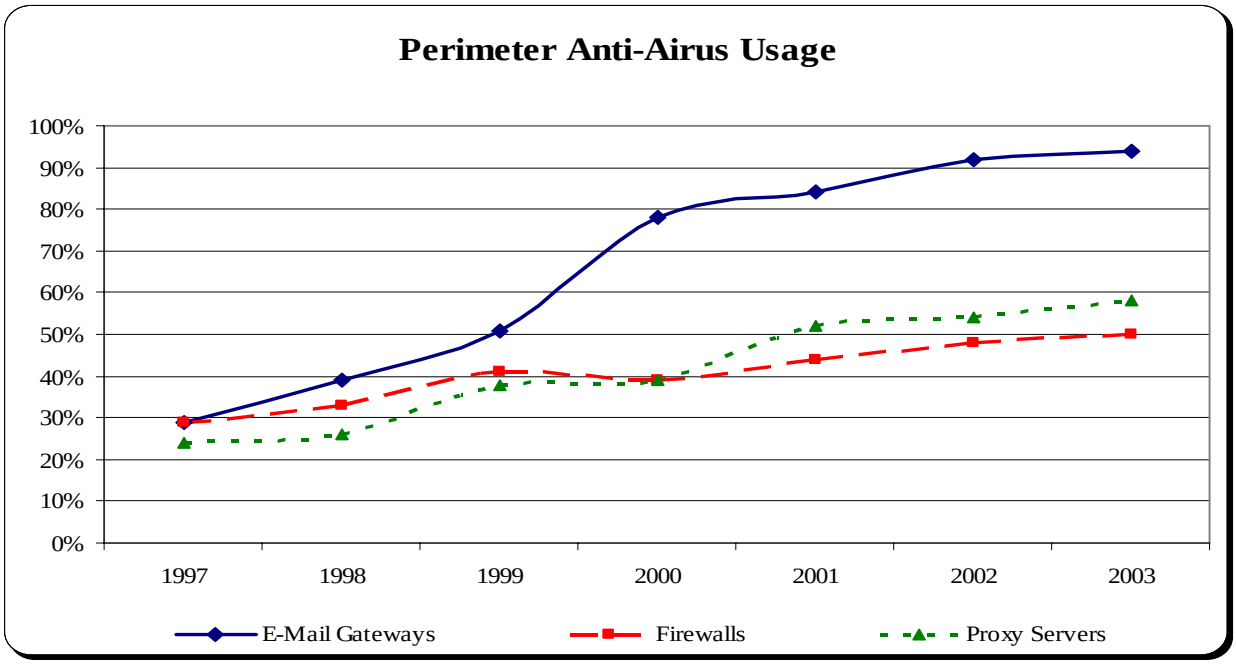


Figure 15 Comparison of perimeter anti-virus coverage, 1997-2003

The 2003 survey showed email gateway coverage finally reaching acceptable levels. This year we see a slight increase in that report from 92 percent to 94 percent coverage. However, firewall and proxy server protection still remain low with 50 percent and 58 percent coverage respectively. While perimeter protection is not a replacement for desktop and server protection, it is an important layer of protection and a key component necessary for a complete corporate virus protection strategy and it is gratifying to see its continued growth.

PERIMETER ANTI-VIRUS METHODS

We also asked respondents about the anti-virus methods used at their Internet perimeter. The following tables and charts represent their answers. Table 16 lists the responses by frequency, while Figure 16 graphs the usage of these methods by percentage.

Method	Frequency
Anti-virus software scans all messages in real time?	292
Block, filter, or quarantine email attachments by file type	264
Anti-Virus software scans message folders and databases?	212
Other anti-virus software protection methods used	10
Total respondents	300

Table 16: Anti-virus methods in use on email gateways

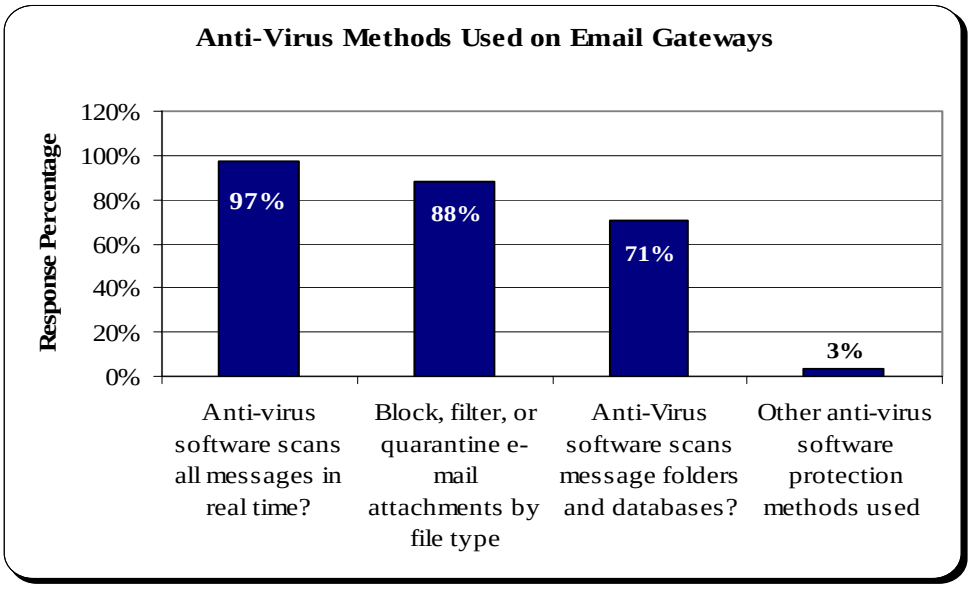


Figure 16: Anti-virus methods used on email gateways by percentage

Table 17 lists the responses for anti-virus methods used on proxy servers by frequency, and Figure 17 graphically depicts this in percentages of respondents.

Method	Frequency
AV scans all traffic in real time	149
Block, filter, or quarantine files by file type	130
Other Methods	11
Total respondents used	209

Table 17: Anti-virus methods used on proxy servers

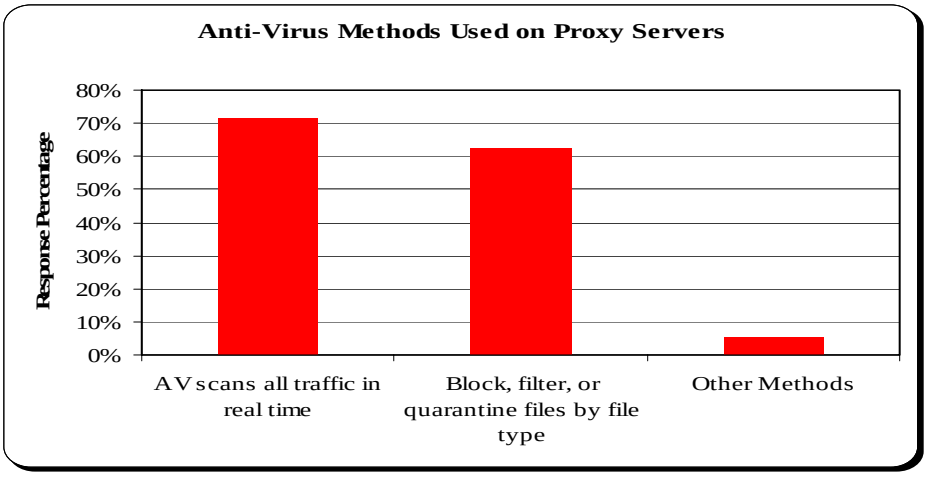


Figure 17 Anti-virus methods used on proxy servers by percentage

Table 18 lists the anti-virus methods used on the firewalls, and Figure 18 gives us a graphical representation of the method percentages of total respondents.

Method	Frequency	%
Block, filter, or quarantine files by file type	140	80%
Anti-virus software scans all traffic in real time	109	62%
Other anti-virus protection methods	9	5%
Total respondents used	176	

Table 18: Anti-virus methods used at the firewall

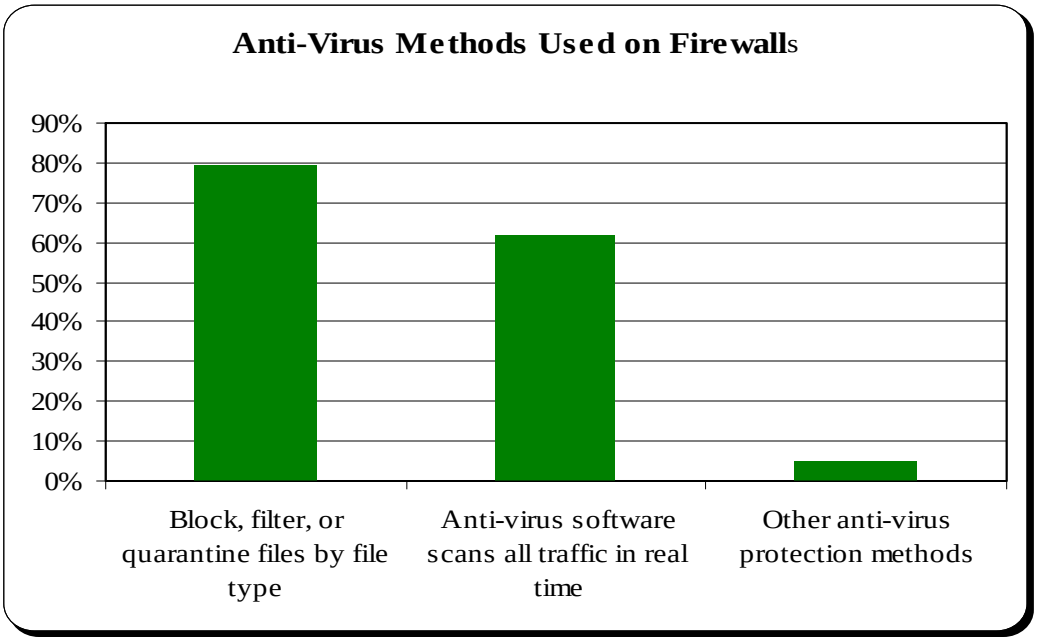


Figure 18: Anti-virus methods used at the firewall by percentage

Discussion Section

THE VIRUS PROBLEM IN COMPANIES CONTINUES TO GET WORSE

There is little doubt that the global virus problem is worsening. After a somewhat quiet year in 2002, 2003 arrived with a vengeance. Beginning with the Slammer worm in January, to Mimail and its many variants in December, we have seen one of the most eventful years ever for computer viruses.

For the 8th year in a row, virus infections, virus disasters and recovery costs increased. Virus infection rates increased only slightly from last year. For the last two years, infection rates have slowed to only a slight increase year over year. From 1996 through 1999, the virus infection rate approximately doubled. There was a significant spike in the 1999 survey due to

the March 1999 Melissa outbreak. After the 1999 spike, infection rates slowed to approximately 15 percent per year. In the last two surveys, we have only seen an increase of five infections per 1,000 PCs per month, from 103 infections per month in 2001 to 108 infections in 2003. While it is heartening to see the *flattening* of the infection rates, there was a dramatic up tick in total virus *encounters*[4]. In the survey, we differentiate between virus *infections*[5] virus *encounters*. Reports of encounters more than doubled from 1.2 million encounters per month in 2002 to 2.7 million encounters reported per month this year. This increase is undoubtedly due to the increased number of mass mailing viruses, internet worms, and their variants.

The reported number of disasters increased again. The survey of 2002 saw a slight drop in reported disasters and was due to the lack of *outbreak* incidents during the year. Respondents reported an increase from 80 reported disasters in 2002 to 94 reports of disasters this year. This really was not surprising. Last year we predicted that while we believed the rate of growth for desktop viruses appeared to have slowed, we also believed that both infection and disaster rates would continue to grow for the near term and we would continue to see increases in mass mailers, Internet worms, expanded connectivity and functionality. That prediction has proven to be accurate. This year nine of the Top 10 reported viruses were mass mailers and the other was the internet worm Slammer. Also, all of the viruses that were responsible for disasters were either Internet worms or mass mailer viruses. Both of these virus types tend to have staying power. This past year saw not only new viruses of these types, but they have remained active longer than other types, even after anti-virus products have included protection against them in their products.

VIRUS TYPES

As mentioned earlier, 2003 was a banner year for numbers of viruses and outbreak incidents. Several trends need to be addressed. The first three listed are continued items from last year.

1. The latest Internet worms and mass mail viruses have more "staying power." The latest Internet worms and mass mailers seem to stay virulent longer and spawn more variants.
2. There was a higher rate of infections per month over the entire survey period than in previous years. The survey asks about virus incidents over several time frames. This year's survey showed almost a constant high level of incidents across all periods. Corporations facing this constant high number of virus incidents must devote more time, personnel, and resources to protecting their systems. When infections do occur, it is taking considerably longer to disinfect systems and fully recover from them.
3. As predicted, boot sector viruses are missing from this year's reporting. While we cannot declare legacy viruses extinct, they do seem to be practically a non-factor in today's virus problem.
4. The trend of forging the From: address in emails distributing the viruses – we also saw this trend last year; it continues to be used in some of the most prevalent viruses this year.
5. Spammers and virus writers seem either to have joined forces or at the very least are using one another's techniques. One of the more notable examples is that of SoBig and its variants. Some elements found in these viruses are the ability to collect email addresses as well as setting up email and web servers on infected machines.

[4] The survey defines an encounter as an event or incident where viruses were experienced, detected, or discovered on any PCs, diskettes; or files or filtered, block or stripped from email.
[5] An infection describes an activation of the virus on the machine, media, or network.

PERCEPTIONS OF THE VIRUS PROBLEM

How respondents feel about the virus problem is consistent with reality. Eighty-eight percent of those surveyed feel that the overall virus problem is either *Somewhat worse* or *Much worse* than last year (which was considered a bad year). Only 32 respondents felt it was *About the Same*. This reflects the reality of their experience with Internet-enabled viruses and worms and the increase in total numbers of viruses and their speed of spread.

VIRUS DISASTERS AND COSTS

The severity of disasters continues to increase. While it is only taking slightly longer to recover fully from these disasters, the cost has increased approximately 23 percent. The average in 2002 was 23 staff days for full recovery. This year respondents reported 24 days for recovery. Cost impact increased significantly over last year, the largest single increase since we have been gathering these data. The average reported cost for a disaster this year was almost $100,000 ($99,900) versus $81,000 in 2002. These numbers alone are dramatic enough, but when we consider that respondents in our surveys historically underestimate costs by a factor of 7 to 10, the results can be staggering. Based on the dollars reported by the technical respondents, if both actual hard and soft costs are considered, it is not out of the question to find complete cost of recovery to be between $100,000 and $1,000,000 in total costs of recovery alone.

VIRUS DISASTER IMPACT:

For the eighth year in a row, our survey respondents report that viruses are not only more prevalent in their organizations but are also more destructive, caused more real damage to data and systems, and are more costly than in past years. This despite increases in their use of anti-virus products, improved updating and upgrading, better management of anti-virus systems. Corporations are spending more time, energy, and dollars in purchasing, installing, and maintaining anti-virus products without achieving their desired results.

Part of the reason for the increased cost of viruses is the impact they have on the business functions of a company. In years past viruses were nuisances and caused little real damage. Those days are long past. Today's viruses continue to escalate in all those areas that affect the function of organizations. Loss of productivity is by far the most important consequence of both virus encounters and disasters. At least 50 percent of the respondents list *Loss of productivity, PC unavailable, Corrupted files, and Loss of access to data* as the primary effect that viruses had on their organizations.

Why is this still the case? A primary reason is rapidity of spread. Corporations must deal with new attacks from Internet worms and mass mail viruses within minutes or at most a few hours of release. Today it is not uncommon for a virus to infect a large proportion of the machines on the Internet in a short period of time. For instance:

- ✓ File viruses took months to years to spread widely
- ✓ Macro viruses took weeks to months
- ✓ Mass Mailers took days
- ✓ Code Red took about 12 hours
- ✓ Klez went around the world in 2.5 hours

- ✓ Slammer affected the world in about 10 minutes!

Today the "threatscape" for viruses has shifted toward multifaceted and faster spreading attacks and infection mechanisms. With this shift comes the importance of mitigating the risk of new and previously-unknown viruses. Even though the current reactive anti-virus technologies are much faster at providing updates for known viruses, and their heuristics have improved greatly, known virus scanning is only a baseline. Corporations also need to look toward other virus protection such as better and finer grained heuristics, access controls, behavior blocking, change detection, filtering, and other generic technologies.

PROTECTION STRATEGIES:

The survey reports that anti-virus product usage is up at every level from previous years. Only firewalls and proxy servers show less than a 90 percent usage of anti-virus products. More than 95 percent of users report that desktop, server, and email gateway server usage has at least 90 percent coverage. With anti-virus product usage up, why do we continue to see the increases in infections, disasters, and costs?

Very simply, we must begin to think differently about virus and malware protection. Anti-virus products are and will remain an important part of the virus protection equation, but they are only a part of the solution. It is no longer enough to think of virus protection in terms of reactive technology. The example given above showing the increasing rapidity of virus spread is evidence that the use of anti-virus products, while necessary, is not enough.

Corporations need to adopt a more holistic protection philosophy that includes intelligent risk management, strong leadership, a comprehensive security policy, and the use of more generic protection techniques. ICSA Labs and TruSecure Corporation have recommended email gateway filtering and generic virus controls and procedures since 1997. Only in the last two years have we seen significant increase in the use of perimeter anti-virus but corporations are still slow in adopting the generic protection.. Generic controls exist that can be employed with minimal maintenance and manageable infringement on corporate business practices. For a number of years, TruSecure Corporation has published a list of these generic controls in its anti-virus policy guide.

These controls include such protections as file attachment filtering; specific configuration for various email clients, email servers, web browsers, and business applications such as word processors and spreadsheets; and various other controls that are generally easy to implement, require infrequent updates, and go unnoticed by the average user because of their transparency. However, their effectiveness is very good, especially when used in conjunction with and implemented within the corporate security policy. Research done by ICSA Labs and TruSecure Corporation in 2003 on Slammer, Blaster, SoBig, and more recently on MyDoom has shown that adopting the controls outlined in a two-year-old version of the aforementioned policy guide would have rendered these viruses ineffective[6]. Copies of these studies may be obtained by contacting TruSecure Corporation.

As another aspect of intelligent risk management, users should subscribe to an "early warning" service that warns system administrators as quickly as possible of the outbreak of new malicious code, vulnerabilities in operating systems and networks, and code that exploits

[6] A copy can be obtained from the TruSecure website http://www.trusecure.com/

these vulnerabilities. However, not all early warning systems are created equal. Ideally, the early warning service will not only advise of the threat or vulnerability, but will give some rating on severity and what actions to take in the short, mid and long term. In conjunction with such a service, it is imperative that organizations update their perimeter virus defenses within minutes of receiving such an alert.

In summary, ICSA Labs recommends the adoption of an Intelligent risk management solution to the virus problem.

1. Develop a comprehensive security policy.
    a. Publish the Policy
    b. Update it Regularly
    c. Enforce the policy
2. Adopt a Defense in Depth
    a. Install anti-virus software at all levels: desktop, servers, gateways, and the perimeter.
    b. Employ generic virus protections where possible; filtering, blocking, stripping attachments.
    c. Employee complimentary security programs such as desktop firewalls, host and network based intrusion detection, and prevention
    d. Consider Managed security services for email and anti-virus
3. Subscribe to an alert service
    a. Commercial
    b. Online lists: NTBugtraq, Bugtraq, AVIEN to name a few

Appendices

Appendix A: Survey Questionnaire

ICSA labs Virus Prevalence Survey Questionnaire

- Q1 How many computers (workstations, desktops, or laptops) are you responsible for in terms of virus knowledge, prevention, and software?
- Q2 How many file and application servers are you responsible for in terms of virus knowledge, prevention, and software?
- Q3 What percent of virus incidents in your group are you informed of or likely to know of?
- Q4 What anti-virus products are you using?
- Q4a Please indicate which anti-virus products you are running at the desktop PC level.
- Q4b Please indicate which anti-virus products you are running at the server.
- Q5 Please indicate which of the following anti-virus software protection methods are used on the desktop level by clicking on the appropriate box.
- Q6 What percentage of desktops have NO anti-virus software installed?
- Q7 What percentage of desktop have anti-virus software installed, but not running?
- Q8 Please indicate which of the following anti-virus software protection methods are used on the file server level by clicking on the appropriate box.
- Q9 What percentage of email gateways have full-time anti-virus software installed now?
- Q10 What percentage of proxy servers have full-time anti-virus software installed now?
- Q11 What percentage of firewalls have anti-virus software installed now?
- Q12 Please indicate which of the following antivirus software protection methods are used on the email gateway by clicking on the appropriate box. Also, please indicate how many servers use each method by typing a number in the box.
- Q13 Please indicate which of the following anti-virus software protection methods are used on the proxy server level by clicking on the appropriate box. Also, please indicate how many servers use each method by typing a number in the box.
- Q14 Please indicate which of the following anti-virus software protection methods are used on the firewall level by clicking on the appropriate box. Also, please indicate how many servers use each method by typing a number in the box.
- Q15 To the best of your knowledge, has a computer virus ever been discovered in any PC, diskette or file in your organization?
- Q16 How many virus encounters did you have during the survey period:
- Q17 Which viruses have affected your group's PCs during the survey period? How many times?
- Q18 Has your group had a virus disaster any time since January 2003?
- Q18a When was the month and year of your most recent disaster?
- Q18b What was the name of the virus in your most recent disaster?
- Q18c How long were any servers "down" while dealing with the disaster? (total server hours)
- Q18d Were EMAIL GATEWAYS shut down during the disaster? How long? (total gateway hours)
- Q18e Were PROXY GATEWAYS shut down during the disaster? How long?(total proxy hours)
- Q18f Were FIREWALLS shut down during the disaster? How long? (total firewall hours)
- Q18g How long did it take for your group to completely recover? (total person hours)
- Q18h How many person-days did the disaster cost your group? (total person hours)
- Q18i How many dollars did the disaster cost your group? (as much as possible include all costs including employee downtime, lost opportunity, IT costs)
- Q19 Which of the following effects occurred in your group with the most recent virus disaster or encounter? (Check all that apply)
- Q20 How did your most recent virus disaster or encounter come to your site? (Check all that apply)

Appendix B: Possible Biases

As with all surveys, there are potential biases that may affect the results of this report. We have taken all possible steps to reduce the effects of these.

RETROSPECTIVE STUDY

The most important bias is that this study is retrospective. That is, we asked respondents to answer questions about past events. Though most sites claimed to have formal tracking mechanisms in place, we believe that respondents describe the older events less reliably than they do when providing information about more recent events. Moreover, older events are often under-represented (forgotten) compared to more-recent events.

Finally, it may also be true that unpleasant events are less easily remembered than pleasant events, so that the past seems more positive than it actually was.

This bias might enhance the perception that things are getting worse.

CORRECTNESS

Some questions referred to issues with well-known right answers, such as questions about policy and virus protection. Other questions asked respondents about the correctness of their estimates (e.g. comparisons of actual virus infections to initial estimates).

In such cases, it is possible that respondents consciously or unconsciously adjusted their responses to look good to the interviewer or to reduce discrepancies between their actual behavior and the normative behavior they felt they ought to display.

This bias could overestimate correctness in such questions.

SITE SELECTION

The survey can be biased in favor of companies that have "computer virus experts" due to the initial site screening. Consequently, it might be true that sites that do not have such a person were under-represented in the survey.

It may also be true that these sites did not have such a person because the virus problem was minimal there.

This bias could show the problem as worse than it really is. Unfortunately, it could also be true that under-represented sites were worse off than the sites in the sample.

FAMILIARITY

The survey tried to estimate the chance that the respondent would actually know about every virus encounter at their site. Respondents were asked the question, "What percent of virus incidents in your group are you informed of or likely to know about?"

However, based solely on anecdotal experience of what happens to anti-virus reporting in organizations, we surmise that a remote employee who encountered a virus for which the appropriate actions were already well known (because of past experience) would be less likely to report the incident to the respondent.

Therefore, we think that common viruses may be under-reported compared with newer or less familiar viruses or those that have recently hit the headlines at the time of questioning.

Appendix C: Glossary of Common Terms in Anti-virus Discussion

The following are common terms used in discussions of anti-virus software:

Background Scanning:	Automatic scanning of files as they are created, opened, closed, or executed. Performed by memory resident anti-virus software. Synonyms: online, automatic, background, resident, active.
Behavior Blocking:	A set of procedures that are tuned to detect virus-like behavior, and prevent that behavior (and/or warn the user about it) when it occurs. Some behaviors that should normally be blocked in a machine include formatting tracks, writing to the master boot record or boot record, and writing directly to sectors. Synonyms: “dynamic code analysis”, “behavioral analysis.”
Boot Record:	The program recorded in the Boot Sector. All floppies have a boot record, whether or not the disk is actually bootable. Whenever you start or reset your computer with a disk in the A: drive, DOS reads the boot record from that diskette. If a boot virus has infected the floppy, the computer first reads the virus code in (because the boot virus placed its code in the boot sector), then jumps to whatever sector the virus tells the drive to read, where the virus has stored the original boot record.
Boot Sector:	The first logical sector of a drive. On a floppy disk, this is located on side 0 (the top), cylinder 0 (the outside), sector 1 (the first sector.) On a hard disk, it is the first sector of a logical drive, such as C: or D:. This sector contains the Boot Record, which is created by FORMAT (with or without the /S switch.) The sector can also be created by the DOS SYS command. Any drive that has been formatted contains a boot sector.
Boot Sector Infector:	Every logical drive, both hard disk and floppy, contains a boot sector. This is true even of disks that are not bootable. This boot sector contains specific information relating to the formatting of the disk, the data stored there and contains a small program called the boot program (which loads the DOS system files). The boot program displays the familiar “Non-system Disk or Disk Error” message if the DOS system files are not present. In addition, the program is infected by viruses. You get a boot sector virus by leaving an infected diskette in a drive and rebooting the machine. When the program in the boot sector is read and executed, the virus goes into memory and infects your hard drive. Remember, because every disk has a boot sector, it is possible (and common) to infect a machine from a data disk.
Boot Virus:	A virus whose code is called during the phase of booting the computer in which the master boot sector and boot sector code is read and executed. Such viruses either place their starting code or a jump to their code in the boot sector of floppies, and either the boot sector or master boot sector of hard disks. Most boot viruses infect by moving the original code of the master boot sector or boot sector to another location, such as slack space, and then placing their own code in the master boot sector or boot sector. Boot viruses, which also infect files, are sometimes known as multipartite viruses. All boot viruses infect the boot sector of floppy disks; some of them, such as Form, also infect the boot sector of hard disks. Other boot viruses infect the master boot sector of hard disks.
Companion Virus:	A program that attaches to the operating system, rather than files or sectors. In DOS, when you run a file named “ABC”, the rule is that ABC.COM would execute before ABC.EXE. A companion virus places its code in a COM file whose first name matches the name of an existing EXE. You run “ABC”, and the actual sequence is “ABC.COM”, “ABC.EXE”
File Virus:	Viruses that attach themselves to (or replace) .COM and .EXE files, although in some cases they can infect files with extensions .SYS, .DRV, .BIN, .OVL, OVR, etc. The most common file viruses are resident viruses, going into memory at the time the first copy is run, and taking clandestine control of the computer. Such viruses commonly infect additional programs as you run them. But there are many non-resident viruses too, which simply infect one or more files whenever an infected file is run.
In the Wild Virus:	A term that indicates that a virus has been found in several organizations somewhere in the world. It contrasts the virus with one that has only been reported by researchers. Despite popular hype, most viruses are “in the wild” and differ only in prevalence. Some are new and therefore extremely rare. Others are old, but do not spread well, and are therefore extremely rare. Joe Wells maintains a list of those he knows of to be “in the wild.”

Macro Virus:	A virus which consists of instructions in Word Basic, Visual Basic for Applications (VBA), or some other macro language, and resides in documents. While we do not think of documents as capable of being infected, any application that supports automatically-executing macros is a potential platform for macro viruses. Because documents are now more widely shared than diskettes (through networks and the Internet), document-based viruses are likely to dominate our future.
Master Boot Record:	The 340-byte program located in the Master Boot Sector. This program begins the boot process. It reads the partition table, determines what partition will be booted from (normally C:), and transfers control to the program stored in the first sector of that partition, which is the Boot Sector. The Master Boot Record is often called the MBR, and often called the "master boot sector" or "partition table." The master boot record is created when FDISK or FDISK /MBR is run.
Master Boot Sector:	The first sector of the hard disk to be read. This sector is located on the top side ("side 0"), outside cylinder ("cylinder 0"), first sector ("sector 1.") The sector contains the Master Boot Record.
Master Boot Sector Virus:	A virus that infects the master boot sector, such as NYB, spreads through the boot sector of floppy disks. If you boot or attempt to boot your system with an infected floppy disk, NYB loads into memory and then writes itself to the master boot sector on the hard drive. If the disk is not bootable, you see the DOS error message, "Non-system disk or disk error...". If the disk is bootable, the system boots to the A: prompt. Either way the system is infected, and there is no indication on the screen that this has happened. Once the hard drive is infected, NYB loads into memory each time the system is booted. The virus stays in memory, waiting for DOS to access a floppy disk. It then infects the boot record on each floppy DOS accesses.
On-Demand Scanning:	Synonyms: offline, manual scanning, foreground, non-resident scanning, scanning.
Polymorphic Virus:	A polymorphic virus is one that produces varied, yet fully operational, copies of itself in the hope that virus scanners will not be able to detect all instances of the virus.
Remove:	To remove or clean a virus means to eliminate all traces of it, returning the infected item to its original, uninfected state. Nearly all viruses are theoretically removable by reversing the process by which they infected. However, any virus that damages the item it has infected by destroying one or more bytes is not removable, and the item needs to be deleted and restored from backups in order for the system to be restored to its original, uninfected state. There is a gap between theory and practice. In practice, a removable virus is one that the anti-virus product knows how to remove. The term "clean" is sometimes used for remove, and sometimes used to refer to the destruction of viruses by any method. Thus deleting a file that is infected might be considered cleaning the system. We do not regard this as an appropriate use of the term "clean."
Resident:	A property of most common computer viruses and all background scanners and behavior blockers. A resident virus is one which loads into memory, hooks one or more interrupts, and remains inactive in memory until some trigger event. When the trigger event occurs, the virus becomes active, either infecting something or causing some other consequence (such as displaying something on the screen.) All boot viruses are resident viruses, as are the most common file viruses. Macro viruses are non-resident viruses.
Stealth Virus:	A virus that uses any of a variety of techniques to make itself more difficult to detect. A stealth boot virus will typically intercept attempts to view the sector in which it resides, and instead show the viewing program a copy of the sector as it looked prior to infection. An active stealth file virus will typically not reveal any size increase in infected files when you issue the "DIR" command. Stealth viruses must be "active" or running in order to exhibit their stealth qualities.
Trojan Horse:	A program that does something unwanted and unexpected by a user, but intended by the programmer. Trojans do not make copies of themselves, as do viruses, and seem to be more likely to cause damage than viruses.
Worm:	Similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all. Once a worm is executed, it seeks other systems to infect, then copies its code to them.
Zoo Virus:	A virus which is rarely reported anywhere in the world, but which exists in the collections of researchers.

Appendix D: TruSecure Anti-Virus Policy Guide

Version 3.7.0, October 2003

OVERVIEW

This policy guide is designed to deal with all current types of viruses known to TruSecure Corp. as of the revision date of this document and those expected in the next six months.

The policies are specifically designed to deal with web, HTML and script based viruses and worms like Code Red and Nimda:

- self-updating malicious code
- malicious code that has been compressed by a 32-bit compressing program
- active communication-enabled viruses, Trojans and worms (such as Happy99, Melissa, BubbleBoy, and LoveLetter) as well as those that may utilize vectors such as ActiveX and JavaScript(Kak.Worm)

- conventional macro viruses
- multipartite, parasitic, stealth, polymorphic viruses
- executable file viruses
- boot sector & partition table viruses

TruSecure Corp. policy suggestions are primary controls or synergistic controls. Primary controls are the most important and effective stand-alone preventative techniques and constitute TruSecure Corp.'s principal policy recommendations for organizations. Synergistic controls function in a way that is analogous to the military strategy of defense-in-depth, which provides for redundancy and failure of particular controls.

When operating alone, individual policies, controls or screens may have limited value, but synergistically can be quite effective. When used in conjunction with other synergistic controls, they behave according to Baye's theorem. Their cumulative effect improves with the use of each control. Their use enhances the effectiveness of other primary controls.

TruSecure recommends the use of all synergistic controls that a site can easily implement without infringing on other business productivity. This includes controls that are easily tolerated by particular groups or sub-groups in an organization, even though other groups may have less tolerance for these same controls. For any given site, it is common to be able to find synergistic controls that have very low infringement and maintenance costs. Furthermore, effective synergistic controls tend to require less frequent updates in order to maintain overall effectiveness.

> *We expect that many synergistic controls (below) will not be applicable to a particular site or for a particular group at a particular site. TruSecure Corp. does not encourage changing business practices in order to achieve these controls. Rather we encourage the use of all controls that can be easily applied to a given organization and all that can be applied to given sub-groups in an organization.*

Virus protection controls can be applied at various levels in an organization. Before macro viruses, there was no practical utility in any controls applied anywhere other than PC desktops[1]. With the advent of macro viruses, the utility of the application of some controls at the server level became evident. With the communication-enabled viruses, controls at places other than the desktop (especially the email and HTTP Proxy perimeter) gain additional value.

[1] For more discussion on the derivation and logic behind these statements, please see other support documents such as ICSA Labs anti-virus surveys, virus study, and virus cost models, available at www.trusecure.com.

ICSA Labs Virus Prevalence Survey 2003

TRUSECURE RECOMMENDED MALCODE CONTROLS

Implement as many of these as may be business- feasible within your organization.

DESKTOP SYSTEMS

TruSecure Corp. Recommended Primary Controls at Desktop Malcode Level:

1) ICSA Certified anti-virus software installed and running on at least 90% of desktop PCs[2].
   http://www.icsalabs.com/html/communities/antivirus/certifiedproducts.shtml
2) Subscribe to an alert service, such as *TruSecure and TruSecure Malcode List.*
3) If alert service is available, update desktop anti-virus software (virus signatures) at least monthly and be prepared to perform emergency updates within two hours of being notified by your alert service of a virus outbreak
   NOTE 1: *During recent outbreaks some anti-virus vendors have taken several hours to provide detection for virus outbreaks. It may be necessary to monitor your anti-virus vendor's web site for an update or contact your vendor to get an update as soon as it is available.*
   NOTE 2: *Updating virus signatures is not good enough if you are using outdated software, please be certain you are using the most up-to-date version of your anti-virus software.*
4) If alert service is not available, update desktop anti-virus software weekly, or as often as your anti-virus vendor provides updates[3].
5) Educate users on how to update virus signatures where the process is not centralized/automated.
6) Recommended desktop anti-virus software configuration:
   a. Full-time, background, real time, auto-protect or similar mode—ENABLED
   b. Start-up scanning of memory, master / boot records, system files—ENABLED
   c. Configure your AV to scan "all files." (***important, this may not be the default setting***)
   d. Logs should be ENABLED to log all desktop virus-related activity.
7) Recommended desktop security settings that relate to viruses.
   a. Ensure that all relevant Microsoft security patches and service releases are installed. (See Annex Two) for a list of such security patches and service releases
   b. See E-mail client primary controls (below)
8) Turn off the Operating System Windows Scripting Host
   a. Disabling WSH for Windows 95
      1. Open "My Computer."
      2. Select "View/Options."
      3. Find "VBScript Script File" from the "File Types" tab.
      4. Select "Remove."

[2] ICSA Labs virus surveys and cost models show a cost minimum when 90% of desktops have active protection with communications-enabled viruses. The same survey indicates that at upwards of 10% of machines with anti-virus products installed have the AV software turned off or other wise inoperable, therefore it is important to monitor AV protection to maintain this 90% coverage. This is up from 75% in v3.01 and earlier policy guides.
[3] Previous policy recommendations suggested quarterly updates when using alert capability or monthly updates without alert capability for macro level viruses and six month updates with alert capability, quarterly without, for pre-macro viruses.

5. If you get a confirmation dialog, select "Yes."

b. Disabling WSH for Windows 98

1. Click on "Start" button in the lower left corner of your desktop.
2. Move the cursor to "Settings" menu, wait a bit and when another menu appears, move the cursor to "Control Panel" and click left mouse button.
3. In the Control Panel window double click on "Add/Remove Programs" icon.
4. In the "Add/Remove Programs" dialog window click on "Windows Setup" tab.
5. Then put the cursor on "Accessories" and double click left mouse button.
6. A new dialog window will be opened. Use the slider or button controls to scroll down the list of accessories.
7. In the end of accessories list you will see "Windows Scripting Host" option. Click on the checkbox near this option to disable it (the "bird" or "check" sign disappears).
8. Click "Ok" button.
9. The Accessories dialog will be closed. In the "Add/Remove Programs" dialog window click "Apply" button.
10. Windows Scripting Host will be uninstalled from your system.

c. Disabling WSH for Windows 2000

1. Open "My Computer."
2. Select "Tools/Folder Options."
3. Find "VBScript Script File" from the "File Types" tab.
4. Select "Delete."
5. If you get a confirmation dialog, select "Yes."

d. Disabling WSH for Windows NT 4

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."

NOTE: Every time you update Windows or Internet Explorer, WSH will be reinstalled.

9) Configure Notepad to open .vbs files.

Notepad has no macro capabilities, so viruses won't execute or spread when opened this way.

a. To create this association in Windows 95, 98, or NT, so that *.vbs files will be opened in notepad.

1. Open My Computer or Windows Explorer and choose View, then Folder Options.
2. On the File Types tab, select the .vbs extension in the Registered File Types box and click Edit. (If you don't see the .vbs extension you can add it to the list of extensions and continue with the following steps.)
3. In the Edit File Type dialog box, select Open, in the Actions box and click Edit.
4. Enter the path to Notepad.exe in the Application Used To Perform Action field and click OK to exit all dialog boxes.

b. (*To do this in Windows 2000, you can follow the same steps, but you'll find the Folder Options menu item under the Tools menu instead, and use change, instead of edit.)*

Additional notes on desktop level policies:

1) Alerts to users, by installed antivirus products, are neither recommended nor discouraged. TruSecure Corp. marginally recommends turning user alerts "off," but turning system administrator alerts, logs, or other advisories "on."
2) Daily, startup, login, or other periodic scanning of hard drives or floppy drives has little incremental utility. TruSecure Corp. recommends these options be turned off as their user infringement normally outweighs their protective value.
3) User-driven scanning policies such as requesting users to scan floppies, downloads or hard drives are not recommended as they are generally more expensive and infringing than useful.
4) Write protection of floppies is probably still worthwhile, but not worth implementing new policy. There is little on the downside of a policy of write-protection, and although the incidence of boot sector viruses has declined dramatically over the last few years, it is quite likely that future Win32 viruses will seek out the boot sectors of floppies. It will be easier to simply keep doing the write protection than to try suddenly to re-train everyone.
5) Educating users to look for virus-like activity is not a viable policy.

TruSecure Corp. Recommended Synergistic Controls at the Desktop-Level:
(For items 1 & 2 specific recommended configuration settings are listed in Annex One)

1) Configure all instances of MS Word to save files as: Rich Text Format (*.rtf).

   NOTE 1**:** *Renaming the *.doc file to *.rtf is not useful. Files must be saved in *.rtf format but may be saved by any file name or extension.*

   NOTE 2**:** *The policy should allow users to save as *.doc type where needed to reduce the file size of complex documents, or for files that require macro use or other very advanced, embedded features use. Otherwise, all files should be saved, mailed, stored, and maintained as *.rtf files by default.*
2) ENABLE Macro Virus Protection in Microsoft Office Programs. (word, excel, powerpoint, access)
3) Seriously consider the use of add-in tool, which is designed to prevent double-click execution of e-mail attachments without challenge.
4) Further, consider the permanent blocking and/or quarantining of executable files as attachments, utilizing desktop mail client rules. (*see Outlook rules below*)
5) Make a policy to send and receive executables by compressing or encrypting them first, should there be a real need to send or receive an executable programs. This can also offer some protection against malicious code hidden by 32-bit self-compression, such as Explore.Worm.MiniZip.

For an example of an add-in tool, see:
Mail add-on to Outlook 97 home page with link to file:
http://www.microsoft.com/security/bulletins/mailaddon.asp
Actual link to file:
http://www.microsoft.com/security/downloads/attchwrn.exe

NOTE*:* *May not be effective for Outlook 98 or Outlook 2000 client –This software has not*

been tested for effectiveness by ICSA Labs.

4) Configure WordView or WordPad as default association with *.doc files.

NOTE: *This is probably not effective on all versions and service releases of Office, particularly as the document-centric model becomes more common, but there is little on the downside. (Document-centric means that, instead of the user having to decide what program they want to use to examine a file, the operating system examines the file internally, as opposed to just looking at the extension, and decides what program should be used automatically. This already happens for some versions of some applications)*

5) Make and distribute an end-user policy and educate users. *Never* double-click on unexpected e-mail attachments. If you receive a document or spreadsheet that you want to look at, manually open it with WordView, Wordpad or XLView. If the attachment appears to be an executable program, *never* run it, despite what the accompanying e-mail says, and no matter from whom it is from. It is now a common ploy for spreading viruses to make them appear they are from someone you know and trust. A viable policy is to ask users to never double click on an attachment unless they are expecting it.

6) Use AV software heuristic controls (in full-time background mode where available) – these work very well for macro viruses.

7) Set site attributes to READ ONLY for *.exe and *.dll in the %systemroot% directory. On Windows '9x machines, the usual directory is C:\Windows; on Windows NT and Windows 2000 machines, this is usually C:\WINNT. On Windows '9x machines this is done using the DOS command ATTRIB.EXE, on Windows NT and Windows 2000 machines, this is a permission setting. Set site attributes for WSOCK32.DLL to "read only."

8) Set AV product to alert or prevent changing of DOS Read-Only file attributes.

9) Store NORMAL.DOT (the default document template) in a protected folder on the file server or write protect and store it on the C: drive (i.e. set its "read only" attribute).

10) Create a copy of NORMAL.DOT, rename it and store it somewhere else on your computer, and create a batch file which runs from the AUTOEXEC.BAT, and which compares the two files. You can use a simple DOS command like FC (File Compare). NORMAL.DOT shouldn't change, unless you are making some sort of customizations. While viruses may still defeat the read-only attribute on NORMAL.DOT, it is unlikely they will find the renamed copy. This would provide a useful early warning that something had happened.

11) Make a copy of Winsock.DLL and Kernel32.DLL, store them and compare them the same way as the previous item, for the same reason. This would help protect against malcode like of Happy99, which modifies Wsock32. Kernel32.dll is another likely target for malicious code. Periodically, we will probably suggest other candidate system files, which are static -- and thus defendable -- and important -- and thus likely targets. Windows 2000 implements a feature called Windows File Protection. This feature ensures that any protected file which is replaced, for any reason by any means, is automatically recovered from a protected cache.

12) Consider use of an alternative word processor or office suite or limiting the use to certain users, providing other users with alternate applications. Remember that no product is bulletproof, and anything that becomes very popular is likely to be targeted.

13) Install the Microsoft Office Document Open Confirmation Tool
This tool can be used to help protect you by always requiring confirmation before opening any of the following Microsoft Office document types in Internet Explorer and Outlook:

http://office.microsoft.com/downloads/9798/confirm.aspx

E-Mail Client (Desktop) Applications

TruSecure Corp. Recommended Primary Controls at the E-Mail Client Level:

1) **Outlook:**
   a. Set Internet Explorer (IE) 4.x/5.x security settings in the Internet zone to "high"
   b. Set Internet Explorer (IE) 4.x/5.x security settings in the Restricted sites to "high"
   c. Set any other ActiveX controls and plug-ins, Java, and Scripting that are enabled to "prompt" or "disable."
   d. Customize IE settings (after setting to High) and disable ActiveX and Active Scripting, setting them to "disable" (strongest) or "prompt."

NOTE 1: *All versions of Outlook (except Outlook 97) rely on the Security Zone Security Settings from Internet Explorer (Tools, Internet Options, Security). Outlook lets you specify one of two zones to use as the security settings for dealing with e-mail messages (Tools, Options, Security). You can use the Internet Zone (default), or the Restricted Sites Zone (which is more secure). You should be using the Restricted Sites Zone. But, as configured by default, Restricted is not strict enough.*

NOTE 2: *IE versions must Update your IE Browser to ensure you're NOT running a browser that's vulnerable to MS01-020. You should be running IE 5.01 SP2, IE 5.5 SP2, or IE 6.0 to be sure you're not vulnerable, or apply the MS01-027 patch (which supercedes MS01-020). (IE 6.0 must perform full install to be protected)*
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-027.asp

To the Restricted Sites Zone you should add these restrictions:
1. Change Script ActiveX controls marked safe for scripting to disable / prompt
2. Change Active Scripting to disable or prompt
3. JavaScript settings should already be set to disable or prompt

NOTE 3: *RAMIFICATIONS of disabling Active Scripting probably include the inability of the machine to use the Microsoft automated path update systems. Ramifications of disabling ActiveX and JavaScript mostly relate to web browsing infringements. If a company wants its users to have the ability to use Microsoft's Windows Update feature, this may be overcome by including those pages in Internet Explorer's Trusted Sites Zone.*

   e. For Outlook '98 users, disable the Preview Pane on all folder views. Since Preview Pane is enabled by default, this must be done for every folder available to the user. It must also be done again each time a new folder is added. By default, Outlook 2000 prevents the use of Active Scripting in the Preview Pane, regardless of the Security Zone setting of the Outlook 2000 client. However, it may be recommended that all users use the AutoPreview feature rather than the Preview Pane for consistency within the company.
   f. Setting up rules in Outlook to automatically delete e-mails that contain embedded scripting:
      In Outlook 2000 or above;
      1. Select Tools, Rules Wizard.
      2. Click "New."
      3. Click "Next."
      4. Click "with specific words in the message header."

5. Click "with specific words in the subject or body."
6. In the Rules Description section of this panel, click on the "specific words" link in the "with specific words in the subject or message body" line.
7. Enter "Content-Type: text/html" beside the "Add" button, don't include the quotation marks.
8. In the Rules Description section of this panel, click on the "specific words" link in the "with specific words in the message header" line Enter "<jscript>", click "Add", enter "<vbscript>", click "Add", enter "<iframe>", click "Add", enter "<object", click "Add." Don't include any of the quotation marks.
9. Click Next.
10. Click "delete it."
11. Click "stop processing more rules."
12. Click "Finish."

2) **Outlook Express –** Disable Open and /or Preview panes. (Auto Preview which shows the first 3 lines of the message is probably ok and is certainly the safest of the three choices)
   a. Perform IE Security Zone settings as above.
   b. To disable the Preview Pane in Outlook Express:
      1. Select Local Folders, then on the Menu Bar select View | Layout |.
      2. At the bottom of the Dialogue Do not check Preview Pane.
3) **Netscape-** Disable JavaScript
   a. To disable JavaScript: On the Menu Bar select: Edit | Preferences
      1. On the left menu of the Dialogue Box Click Advanced.
      2. On the right side of the Dialogue Box, **Do Not Enable** JavaScript for e-mail and news.
      3. For maximum safety, also disable JavaScript for browsing.

   NOTE: *Be advised, however, that Netscape uses JavaScript as part of its Smart Update program and will need to be Enabled to take make use of this feature.*
4) **Other e-mail client** -- Disable Visual Basic Scripting or Java Scripting if utilized. Also, disable the use of IE for HTML viewing of e-mail if used by the client. (i.e. Eudora 4.x). If IE is on desktop, set as above.

TruSecure Corp. Recommended Synergistic Controls at the E-Mail Client Level:

1) Turn off auto-open attachments.
2) Configure for Plain text only.
3) Configure to challenge execution of all executables attachments, (see Annex Three.)
4) Configure to challenge opening of all executable files, (see Annex Three.)
5) Configure to challenge double click of all attachments.
6) Consider using non MS Mail application.
7) Do not store ALL_Company alias in local e-mail lists.

Network File and Print Servers

Implement as many of these as may be business-feasible within your organization.

TruSecure Corp. Recommended Primary Controls at Inside Server Level:

1) Run AV Scanner in full time, background, automatic, auto-protect or similar mode on any file server which potentially stores files which are potentially infect-able such as*.doc files, HTM files, and executables which run on desktops.

   NOTE: Daily or other periodic scanning has little value when auto-protect mode or similar full time mode is enabled.

2) Update server signature files monthly if alert service is available, weekly (or at maximum vendor rate) if no alert service is available.

TruSecure Corp. Recommended Synergistic Controls at the Inside Server Level:

1) Utilize centralized AV management
2) Use centralized desktop management
3) Manage Internet Explorer, Visual Basic Scripting and Java Scripting centrally

E-MAIL GATEWAYS, FIREWALLS, PROXY AND ANTI-SPAM TOOLS

Implement as many of these as may be buisness- feasible within your organization.

TruSecure Corp. Recommended Primary Control at the Gateway Level:

1) Install e-mail gateway anti-virus software configured for full-time active mode.
   a. Configure your anti-virus "Files List" to include scanning all files (most effective).
   b. If you determine not to configure for scanning all files, check (Annex Three) for a list of files that may be automatically invoked.
2) Filter all business-feasible file attachments (eg. *.exe, *.doc, *.dll and *.vbs) whether infected or not (See Annex Three.)
3) Filter all arriving (and departing if possible) e-mail traffic by subject line /header:
   a. Be prepared to rapidly adjust filtering rules, within 1 hour of notice for emergency alerts. *(See Annex Four for filtering rules for historical viruses spreading in the wild.)*
   b. For additional help with sendmail see: http://www.sendmail.com/blockmelissa.html
   c. For help with John Hardin's Procmail see: ftp://ftp.rubyriver.com/pub/jhardin/antispam/procmail-security.html
   d. For help with Innosoft's PMDFsee: http://www.innosoft.com/iii/pmdf/virus-word-emergency.html

TruSecure Corp. Recommended Potential Synergistic Controls at the E-mail Gateway Level:

1) Consider filtering all arriving and departing e-mail by spam threshold (greater than 40 identical messages blocked and source traced, if inside.)
2) Filter embedded from HTML traffic ActiveX and JavaScript ("<jscript>", "<vbscript>", "<iframe>", "<object.")
3) Convert HTML to RTF or TXT before reaching desktop.

TruSecure Corp. Recommended Potential Synergistic Controls at Proxy Gateway Level:

1) Filter all business-feasible file attachments (eg. *.exe, *.doc, *.dll and *.vbs) whether infected or not (See Annex Three.)
2) Filter embedded ActiveX and JavaScript ("<jscript>", "<vbscript>", "<iframe>", "<object.")

HUMAN FACTORS

Implement as many of these as may be business-feasible within your organization.

TruSecure Corp. Recommended Primary Control at the Human Factor Level:

None

TruSecure Corp. Potential Synergistic Controls at the Human Factor Level:

1) Educate users to consider e-mail attachments and links potentially dangerous and to treat them very cautiously. Specifically recommend education: Open only expected attachments and links from known and trusted sources. Delete or question all others before opening.
2) Warn users that even attachments from known sources could be infected. Most viruses spread using Outlooks Address Book so most likely a virus will come from a user you know that has you in their address book.
3) Keep system managers updated and informed. Links to hundreds of sites and related documents are available at http://www.icsa.net/virus.
4) Reinforce the message to users to never double click an e-mail attachment that is not expected. This policy is difficult since the affected malicious e-mail will normally come "From" a trusted person. Well-informed users can be taught that *.doc, *.exe, *.vbs, and *.hta extensions are the most likely to be dangerous. Desktop anti-virus software will normally work if it is kept updated and properly configured to operate full-time in the background.
5) E-mail containing Christmas card attachments, video, audio or other "fun attachments" and sexually-oriented attachments are likely to be the most exploited vector for this and similar viruses.

Other Notes:

Using software on your site different from the popular software on average sites in general is protective. Look for things about your site that change enough of your implementation of word processing, document file usage, e-mail, and other similar systems so as to not be identical to the average site.

ActiveX and JavaScript viruses have begun to materialize as real risks and have been experienced by the computing community. TruSecure Corp. believes that these vectors will worsen in the next months. Building defenses for them now will save the day when they become common. Viruses and worms dependent upon them may travel exceedingly fast -- much faster than an organization can be expected to update its anti-virus signatures and potentially faster than anti-virus companies can create and distribute signatures.

Use a security service like TruSecure which will provide, updated policies (updated at least quarterly for proven effectiveness), continuous alerts and information, emergency alerts and updates, and which will repeatedly measure and test the effectiveness of your sites implementation of these virus and numerous other security policies and practices. The service considers the malicious code risk as one of six risk categories (Electronic Risk (mostly hacking), Malicious Code Risk (mostly viruses), Privacy Risk, Downtime risk, Physical Risk, and Human Factors risk. Participation in the TruSecure program normally qualifies your organization for TruSecure site certification that often satisfies due diligence and audit requirements. The process is continuous and constantly improving and rapidly leads to effective security using the people and products already in your organization.

IT managers should subscribe to the TruSecure Malcode Mailing List
http://postal.trusecure.com/mailman/listinfo/tsmalcode This list posts "pre-alerts" significantly in advance of actual alerts and provides a way to communicate with TruSecure and ICSA Labs virus experts and other corporate TruSecure members.

Submit Suggestions: Please contribute your AV policy suggestions whether primary controls or supplemental / synergistic controls by sending e-mail to 'avpolicy@icsa.net.'

ANNEX 1: Recommended settings for Microsoft Office programs to increase virus protection.

For Office 97 programs:

Word 97

Tools /Options /General:
Do Check: [Macro virus protection]
Do Not Check: [Mail as attachment]
Tools /Options / Save:
Do Check: Prompt to save Normal template]
Do not check: [Allow fast Saves]
Do Configure: Save Word files as: Rich Text Format (*.rtf)

Excel 97

Tools /Options /General:
Do Check: [Macro virus protection]

PowerPoint 97

Tools /Options /General:
Do Check: [Macro virus protection]

Office 2000 Settings:

Word 2000

Tools | Macro | Security
Security level = High (default is high)
Trusted Sources = NO ONE
Do not check "Trust all installed add-ins and templates." (Default is checked)
Tools | Options | General:
Do Not Check: Mail as attachment
Tools | Options | Save:
Do Check: Prompt to save Normal template
Do not check: Allow fast Save
Do Configure: Save Word files as: Rich Text Format (*.rtf)

Excel 2000

Tools | Macro | Security
Security level = High (default is high)
Trusted Sources = NO ONE
Do not check "Trust all installed add-ins and templates." (Default is checked)

PowerPoint 2000

Tools | Macro | Security
Security level = High – (Default may be medium)
Trusted Sources = NO ONE
Do not check "Trust all installed add-ins and templates." (Default is checked.)

ANNEX 2: Recommended Security patches

E-mail Attachment Security Update for all versions of Outlook

This update prevented users from automatically executing certain file types, instead forcing them to save these file types to disk.

Download and install the following depending on the version of Outlook which you use;

Outlook '97 http://officeupdate.microsoft.com/downloadDetails/O97attch.htm
Outlook '98 http://officeupdate.microsoft.com/downloadDetails/O98attch.htm
Outlook '2000 http://officeupdate.microsoft.com/2000/downloadDetails/O2Kattch.htm
The following URL provides a fuller description of the update. The update prevents the automatic execution of .exe, .bat, .com, or .cmd file types.

http://support.microsoft.com/support/kb/articles/q235/3/09.asp

Microsoft Office SR-1

MS Office SR-1 provides further flexibility for Outlook 2000 than the previous versions. Included in SR-1 is an enhancement to the E-mail Attachment Security Update as described in;

http://support.microsoft.com/support/kb/articles/Q259/2/28.ASP

See the following for details.

http://officeupdate.microsoft.com/2000/downloadDetails/O2kSR1DDL.htm

Outlook 2000 SR-1 Update: E-mail Security

1. E-mail attachment security prevents users from accessing several file types when sent as e-mail attachments. Affected file types include executables, batch files, and other file types that contain executable code often used by malicious hackers to spread viruses.

2. Object Model Guard prompts users with a dialog box when an external program attempts to access their Outlook Address Book or send e-mail on their behalf, which are how viruses such as ILOVEYOU spread.

3. Heightened Outlook default security settings increase the default Internet security zone setting within Outlook from "Internet" to "restricted sites." In addition, active scripting within restricted sites is disabled by default. These security features help protect users from many viruses that are spread by means of scripting.

http://office.microsoft.com/downloads/2000/Out2ksec.aspx

Outlook 98 Update: E-mail Security

1. E-mail attachment security prevents users from accessing several file types when sent as e-mail attachments. Affected file types include executables, batch files, and other file types that contain executable code often used by malicious hackers to spread viruses.

2. Object Model Guard prompts users with a dialog box when an external program attempts to access their Outlook Address Book or send e-mail on their behalf, which are how viruses such as ILOVEYOU spread.

3. Heightened Outlook default security settings increase the default Internet security zone setting within Outlook from "Internet" to "restricted sites." In addition, active scripting within restricted sites is disabled by default. These security features help protect users from many viruses that are

spread by means of scripting.

http://office.microsoft.com/downloads/9798/Out98sec.aspx

Incorrect MIME Header Can Execute E-mail Attachment

A flaw exists in Microsoft Internet Explorer 5.01 and Microsoft Internet Explorer 5.5 that would allow a user to maliciously alter Mime types so that IE will handle them incorrectly. This would cause IE to launch the malicious attachments automatically when the e-mail is opened. The flaw would also work by getting a user to visit a malicious web page.

***NOTE**: Internet Explorer 5.01 Service Pack 2 is not affected by this vulnerability*.

Patch availability

Download locations for this patch

http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp

CLSID Can Hide True Extension of File

A user can maliciously hide the true extension of a file by adding a Class ID to the file name. This would cause the Class ID to not be seen in Explorer or Internet Explorer.

A CLSID looks like this:

{00000001-0000-0002-0002-0044534F4654}

If a malicious user renamed a file test.txt.{00000001-0000-0002-0002-0044534F4654} it would not be opened by notepad but by which ever program the CLSID referenced in the users Registry.

Mitigation:

It may be possible to filter the body of incoming e-mail message for the ."{" which can be found at the beginning of all CLSID's.

Patch availability

Microsoft is working on a patch.

RTF document linked to template can bypass Microsoft Word's Macro Security

A malicious user can link an *.RTF document to a template with an embedded macro that will bypasses a security mechanism that requires user's approval to run macros. This affects the following versions of Microsoft Word: Microsoft Word 97, Microsoft Word 2000, Microsoft Word 98 (J), Microsoft Word 98 for the Mac, and Microsoft Word 2001 for the Mac.

***NOTE**: Microsoft Word 2002 is not affected by this vulnerability.*

Download locations for this patch :

Microsoft Word 2000:
http://office.microsoft.com/downloads/2000/wd2kmsec.aspx

Microsoft Word 97:
http://office.microsoft.com/downloads/9798/wd97mcrs.aspx

Microsoft Word 98 (J) for Windows:

Patch will be available shortly

Microsoft Word 98 for the Mac:
Patch will be available shortly

Microsoft Word 2001 for the Mac:
Patch will be available shortly

Linux Ramen and Lion Worm

The Ramen and Lion Linux worm's attack machines running the Linux Red Hat 6.2 or 7.0 operating system. The worm's attempt to use unpatched versions of rpc.statd, wuftpd, and LPRng.

Mitigation:

Install the following patches that will fix the vulnerabilities.

RedHat 7.0 Security Advisories - http://www.redhat.com/support/errata/rh7-errata-security.html

RedHat 6.2 Security Advisories - http://www.redhat.com/support/errata/rh62-errata-security.html

Sadmind (IIS and Solaris Worm)

Sadmind is a worm that affect's systems that are running unpatched versions of Microsoft IIS and unpatched versions of Solaris. It replaces the default Web page with profane remarks against the government, and the text: PoizonBOx

Mitigation:

A patch is available from Microsoft at
http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

For IIS Version 4:
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

For IIS Version 5:
http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

Apply a patch from Sun Microsystems as described in Sun Security Bulletin #00191:
http://sunsolve.sun.com/pub-gi/retrieve.pl?doctype=coll&doc=secbull/191&type=0&nav=sec.sba

CodeRed

The Code Red Worm attacks webservers and installs software that will allow a malicious user gain access to the system and execute commands on it.

Either of the following patches stop Code Red and Code Red II:

Microsoft Security Bulletin MS01-033
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

Microsoft Security Bulletin MS01-044
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp

Nimda

W32/Nimda@MM is a worm that spreads by e-mail, webserver, or file sharing. The worm uses the Incorrect Mime Header vulnerability in e-mail to infect users via e-mail. Webservers are infected by the following vulnerabilities, A back door created by Code Red or Web Server Folder Traversal.

Patching IE to prevent e-mail infection:

The patch provided in Microsoft Security Bulletin MS01-020.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

The patch provided in Microsoft Security Bulletin MS01-027.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-027.asp

Internet Explorer 5.01 Service Pack 2.

http://www.microsoft.com/windows/ie/downloads/recommended/ie501sp2/default.asp

Internet Explorer 5.5 Service Pack 2.

http://www.microsoft.com/windows/ie/downloads/recommended/ie55sp2/default.asp

Internet Explorer 6. (**Must Perform Full Install**)

http://www.microsoft.com/windows/ie/downloads/ie6/default.asp

Preventing Code Red:

Applying the patch provided in Microsoft Security Bulletin MS01-033

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

Applying the patch provided in Microsoft Security Bulletin MS01-044

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp

Installing the Windows NT 4.0 Security Roll-up Package

http://www.microsoft.com/ntserver/nts/downloads/critical/q299444/default.asp?FinishURL=%2Fdownloads%2Frelease%2Easp%3FReleaseID%3D31240%26redirect%3Dno

Running the IIS Lockdown Tool in its default mode

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/locktool.asp

Installing the URLScan tool with its default rule set.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/URLscan.asp

Preventing Web Server Folder Traversal vulnerability:

Applying the patch provided in Microsoft Security Bulletin MS00-057

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-057.asp

Applying the patch provided in Microsoft Security Bulletin MS00-078

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-078.asp

Applying the patch provided in Microsoft Security Bulletin MS00-086

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-086.asp

Applying the patch provided in Microsoft Security Bulletin MS01-026

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-026.asp

Applying the patch provided in Microsoft Security Bulletin MS01-044

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp

Installing Windows 2000 Service Pack 2

http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/default.asp

Installing the Windows NT 4.0 Security Roll-up Package

http://www.microsoft.com/ntserver/nts/downloads/critical/q299444/default.asp?FinishURL=%2Fdownloads%2Frelease%2Easp%3FReleaseID%3D31240%26redirect%3Dno

Running the IIS Lockdown Tool in its default mode

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/locktool.asp

Installing the URLScan tool with its default rule set.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/URLscan.asp

Malformed Excel or PowerPoint Document Can Bypass Macro Security (MS01-050)

A malicious user could create an Excel or PowerPoint file that would bypass macro security and execute automatically when the document is opened. A malicious file could change or delete data, communicate or open hostile websites, or change registry or macro security settings.

Affected Software:

Microsoft Excel 2000 for Windows
Microsoft Excel 2002 for Windows
Microsoft Excel 98 for Macintosh
Microsoft Excel 2001 for Macintosh
Microsoft PowerPoint 2000 for Windows
Microsoft PowerPoint 2002 for Windows
Microsoft PowerPoint 98 for Macintosh
Microsoft PowerPoint 2001 for Macintosh

Patches:

Microsoft Excel 2000 for Windows:

http://download.microsoft.com/download/excel2000/e2kmac/1/w98nt42kme/en-us/e2kmac.exe

Microsoft Excel 2002 for Windows:

http://download.microsoft.com/download/excel2002/exc1001/1/w98nt42kme/en-us/exc1001.exe

Microsoft Excel 98 for Macintosh:

http://www.microsoft.com/mac/download/office98/pptxlmacro.asp

Microsoft Excel 2001 for Macintosh:

http://www.microsoft.com/mac/download/office2001/pptxlmacro.asp

Microsoft PowerPoint 2000 for Windows:

http://download.microsoft.com/download/powerpoint2000/p2kmac/1/w98nt42kme/en-us/p2kmac.exe

Microsoft PowerPoint 2002 for Windows:

http://download.microsoft.com/download/powerpoint2002/ppt1001/1/w98nt42kme/en-us/ppt1001.exe

Microsoft PowerPoint 98 for Macintosh:

http://www.microsoft.com/mac/download/office98/pptxlmacro.asp

Microsoft PowerPoint 2001 for Macintosh:

http://www.microsoft.com/mac/download/office2001/pptxlmacro.asp

NOTE: Be advised, Office 97 suite of Microsoft Office is also affected by this and Microsoft does not plan on releasing patches for this software because they are no longer supporting it.

ANNEX 3: File types

The list below contains a listing of file types that are recognized by default on machines with a complete installation of Office 2000. These may be automatically invoked when presented to the user as an attachment in E-mail.

??_	HLP	MDBHTML	PL	VBE
AD?	HT?	MDE	PMA	VBS
ADE	HT	MDT	PMC	VS?
ADP	HTA	MDW	POTHTML	WAB
ASP	HTM	MDZ	POT	WBK
ASX	DOC.SCR	MSC	PP?	WEBPNP
BAS	HTML.PIF	MHT	PPA	WHT
BAT	HTML	MHTML	PPS	WIZ
BIN	DOC.PIF	MPP	PPT	WIZHTML
CDR	HTT	MPT	PPTHTML	WPD
CER	HTW	MS?	PRF	WS?
CHM	IM?	MSI	PWZ	WSC
CMD	INF	MSP	QDS	WSF
COM	INI	MST	RNK	WSH
CPL	INS	NFO	RQY	XLA
CRL	IQY	NMW	RTF	XLB
CRT	ISP	NWS	SC2	XLC
CSC	ITS	JPG	SCD	XLD
CSV	JOT	OBD	SCH	XLK
DER	JS?	OBT	SCR	XLL
DESKLINK	JSE	OCX	SCT	XLM
DEV	LNK	OLE	SHB	XLS
DIF	MAD	OQY	SHS	XLSHTML
DL?	MAF	OSS	SLK	XLT
DO?	MAM	OV?	SMM	XLTHTML
DOC	MAPIMAIL	P10	SNP	XLV
DOCHTML	MAQ	P12	MP3.PIF	XLW
DOT	MAR	P7B	SPC	XML
DOTHTML	MAS	P7R	SST	XNK
DQY	MAT	P7S	STL	XSL
DSN	MAV	PBK	STM	XTP
DUN	MAW	PFX	SYSVB?	XL?
EML	MD?	PKO	UDL	ZAP
EXE	MDA	PCD	ULS	AVI.PIF
FAV	JPG.PIF	PIF	URL	TXT.PIF
GMS	MP3	TXT	VB?	ZIP.SCR
GZ?	MDB			

ANNEX 4: Filtering Information for Viruses Currently/Previously In the Wild.

The list below contains a listing of information that can be used to filter Viruses currently spreading in the wild. Anti-Virus products at the E-mail Gateway or Content Filtering products can use this information.

Virus Name	Generic Attachment Blocking	From	Subject	Body	Patches
JS/Kak-m	No Attachment - Embedded Script	Anyone	Anything	Anything	http://www.microsoft.com/technet/security/bulletin/ms99-032.asp
VBS/Stages.A-mm	.TXT.SHS	Anyone	Random	The male and female stages of life.	N/A
W32/BadTrans-mm	.AVI.pif, .DOC.pif, .DOC.scr, .MP3.pif, .pif, .scr, .TXT.pif, .ZIP.scr	Anyone	Replies to Unread e-mail	Replies to Unread e-mail	N/A
W32/Hybris-m	.scr, .exe	Hahaha [hahaha@sexyfun.net]	Snowhite and the Seven Dwarfs - The REAL story!	Today, Snowhite was turning 18. The 7 Dwarfs always where very educated and polite with Snowhite. When they go out work at mornign, they promissed a *huge* surprise. Snowhite was anxious. Suddlently, the door open, and the Seven Dwarfs enter...	N/A
W32/Magistr-mm	.exe	varies	varies	varies	N/A
W32/Matcher-mm	.exe	Anyone	Matcher	Want to find your love mates!!! Try this its cool... Looks and Attitude Maching to opposite sex.	N/A
W32/Navidad-m	.exe	Anyone	Anything	Anything	N/A
W32/PrettyPark-mm	.exe	Anyone	C:\CoolProgs\Pretty Park.exe	Anything	N/A
W32/ProLin-mm	.exe	Anyone	A great Shockwave flash movie	Check out this new flash movie that I downloaded just now ... It's Great Bye	N/A
W32/Ska-m	.exe	Anyone	Anything	Anything	N/A
W95/Plage-m	.exe	Anyone	Anything	Anything	N/A

GOLD SPONSOR

NETWORK ASSOCIATES

Network Associates®, Inc. [NYSE: NET]creates best-of-breed computer security solutions that span large enterprises, governments, small- and medium-sized businesses, and consumers, helping prevent intrusion on networks and protecting computer systems from the next generation of blended attacks and threats. These next-generation threats attack on multiple levels of the network infrastructure. Network Associates offers in-depth protection—from the network core to the perimeter to complete desktop security—through two families of products: McAfee® System Protection Solutions, securing desktops and servers, and McAfee Network Protection Solutions, ensuring the protection and performance of the corporate network.

SILVER LEVEL

MICROSOFT CORPORATION

Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services and Internet technologies for personal and business computing. The company offers a wide range of products and services designed to empower people through great software — any time, any place and on any device.

BRONZE LEVEL

ESET, LLC

Founded in 1992, Eset has focused on developing innovative antivirus softwar systems. NOD32 has evolved from that development process to be consistently rated as one of the best anti virus products. For more information, visit www.nod32/home/home.htm

TREND MICRO, INC.

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services, focused on providing customers with comprehensive security strategies to manage the impacts of known and unknown threats. Trend Micro has offices in 25 countries, and trades stock on Tokyo Stock Exchange and NASDAQ.

EDUCATIONAL SPONSOR

MIS TRAINING INSTITUTE

Founded in 1978, MIS Training Institute is the international leader in audit and information security training, with offices in the USA, UK, and Asia. MIS' expertise draws on experience gained in training more than 100,000 delegates across five continents. MIS presents seminars and conferences in the areas of internal and IT audit; information security; network infrastructure; operating environments; and enterprise applications. MIS offers Web-based training at www.misti-online.com as well as a variety of products and services including on-site training and publications. MIS Training Institute is a Euromoney Training Group company.

ICSA Labs is the security industry's central authority for research, intelligence and product certification for over a decade. ICSA Labs sets performance standards for information security products and certifies over 95% of the installed base of firewall, anti-virus, cryptography and IPSec products. ICSA Labs also leads security consortia that provide a forum for intelligence sharing among the leading vendors of security products.

ICSA labs
A DIVISION OF TRUSECURE CORPORATION

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, Pennsylvania 17050
717-790-8100 www.icsalabs.com