Cyber Security Information Sharing in the United States: An Empirical Study Including Risk Management and Control Implications 2000-2003

Volume Two of Two

by

Michael Keith Lavine

March 2007

In Partial Fulfillment for Doctor of Philosophy Degree from Sir John Cass Business School, City University, London, UK

TABLE OF CONTENTS: VOLUME TWO

CHAPTER FOUR – DESCRIPTIVE STATISTICS 6

4.1 Introduction **7**

4.1.1 Data Accumulation Techniques 8

4.1.2 Assumptions Acknowledged 9

4.2 Descriptive Characteristics of the Secondary Data **10**

4.2.1 CyberNotes Data Summary Information 10

4.3 Bugs, Holes and Patches **14**

4.3.1 Yearly and Quarterly Frequency Distributions 14

4.3.2 Risk Levels 15

4.4 Exploit Scripts **25**

4.4.1 Yearly and Quarterly Frequency Distributions 25

4.4.2 Types of Exploit Scripts 27

4.4.3 Workaround Availability 28

4.4.4 Further Information 30

4.5 Viruses **31**

4.5.1 Yearly and Quarterly Frequency Distributions 31

4.5.2 Types of Viruses 33

4.5.3 Further Information 34

4.6 Trojans **35**

4.6.1 Yearly and Quarterly Frequency Distributions 35

4.6.2 Types of Trojans 39

4.6.3 Aliases 40

4.6.4 Further Information 43

4.7 Trends **44**

4.7.1 Yearly and Quarterly Frequency Distributions 44

4.7.2 Further Information 47

4.8 Secondary Data Items **48**

4.8.1 An Overview 48

4.8.2 Other NIPC Information Reports and Disclosures 48

4.8.3 Macro-Economic Data 51

4.8.4 E-Commerce Data 60

4.8.5 Information Technology Data 65
4.8.6 Political and Military Event Information 71

4.9 Summary and Conclusion 74

CHAPTER FIVE - HYPOTHESIS TESTING **76**

5.1 An Introduction 77

5.2 Statistical Tests Performed 78

5.3 Hypothesis Testing 80

5.4 Conclusion 119

CHAPTER SIX – CONCLUSION **122**

6.1 Summary 123

6.2 Conclusions 126

6.3 Areas for Future Research 129

6.4 Final Thoughts 131

List of Figures

FIGURE 4.1 – EXPLOIT SCRIPTS FREQUENCY DISTRIBUTION BY QUARTER: 2000-2003 26
FIGURE 4.2 – EXPLOIT SCRIPTS – MOST COMMON FILE TYPES: 2000-2003 27
FIGURE 4.3 – EXPLOIT SCRIPTS WORKAROUND AVAILABILITY: 2000-2003 29
FIGURE 4.4 – VIRUSES CASES BY QUARTER: 2000-2003 32
FIGURE 4.6 – TROJANS CASES FREQUENCY DISTRIBUTION BY QUARTER: 2000-2003 36
FIGURE 4.7 – NEW VERSUS PREVIOUSLY REPORTED TROJANS BY QUARTER: 2000-2003 38
FIGURE 4.8 – MAJOR TYPES OF TROJANS: 2000-2003 39
FIGURE 4.9 – NUMBER OF TROJAN ALIASES BY QUARTER: 2000-2003 42
FIGURE 4.10 – TRENDS FREQUENCY DISTRIBUTION BY QUARTER: 2000-2003 46
FIGURE 4.12 – MAJOR U.S. STOCK MARKET INDEXES BY QUARTER: 2000-2003 52
FIGURE 4.13 – MAJOR U.S. INTEREST RATE PERCENTAGES BY QUARTER: 2000-2003 54
FIGURE 4.14 – U.S. INFLATION RATE AND CONSUMER PRICE INDEX BY QUARTER: 2000-2003 56
FIGURE 4.15 – U.S. GDP AND UNEMPLOYMENT BY QUARTER: 2000-2003 58
FIGURE 4.16 – UNITED STATES E-COMMERCE FIGURES BY QUARTER: 2000-2003 61
FIGURE 4.17 – U.S. E-COMMERCE AS A PERCENT OF TOTAL SALES BY QUARTER: 2000-2003 63
FIGURE 4.18 – U.S. INTERNET UTILISATION BY QUARTER: 2000-2003 66
FIGURE 4.19 – U.S. TELEPHONY UTILISATION BY QUARTER: 2000-2003 67
FIGURE 4.20 – TOTAL GLOBAL WWW PAGES AND U.S. HOST COMPUTERS
BY QUARTER: 2000-2003 68
FIGURE 4.21 – U.S. WIRELESS AND PDA USERS BY QUARTER: 2000-2003 70

List of Tables

TABLE 4.1 – CYBERNOTES NEWSLETTER AGGREGATION SUMMARY BY YEAR: 2000-2003 8
TABLE 4.2 – CYBERNOTES NEWSLETTER AGGREGATION SUMMARY BY QUARTER: 2000-2003 9
TABLE 4.3 – SUMMARY OF TOTAL CYBERNOTES DATA BY YEAR: 2000-2003 11
TABLE 4.4 – SUMMARY OF TOTAL CYBERNOTES DATA BY QUARTER: 2000-2003 12
TABLE 4.5 – BUGS, HOLES AND PATCHES BY YEAR: 2000-2003 14
TABLE 4.6 – BUGS, HOLES AND PATCHES: TYPES OF INFORMATION REPORTED – FREQUENCY DISTRIBUTION BY QUARTER: 2000-2003 15
TABLE 4.7 – BUGS, HOLES AND PATCHES: RISK RATING FREQUENCY DISTRIBUTION BY QUARTER: 2000-2003 16
TABLE 4.8 – BUGS, HOLES AND PATCHES: TOP 15 VULNERABILITIES IN RANK ORDER: 2000-2003 18
TABLE 4.9 – BUGS, HOLES AND PATCHES: ATTACK CODE SUMMARY IN RANK ORDER: 2000-2003 19
TABLE 4.10 – BUGS, HOLES AND PATCHES: WORKAROUND AVAILABILITY HIGH LEVEL CLASSIFICATION RANKING: 2000-2003 20
TABLE 4.10 – BUGS, HOLES AND PATCHES: VENDOR FREQUENCY DISTRIBUTION – TOP 20 VENDORS: 2000-2003 21
TABLE 4.12 – BUGS, HOLES AND PATCHES: TOP 20 REFERENCE INFORMATION SOURCES: 2000-2003 23
TABLE 4.13 – EXPLOIT SCRIPTS FREQUENCY DISTRIBUTION BY YEAR: 2000-2003 25
TABLE 4.14 – TOTAL VIRUS CASES BY YEAR: 2000-2003 31
TABLE 4.15 – TROJANS FREQUENCY DISTRIBUTION BY YEAR: 2000-2003 35
TABLE 4.16 – REPORTED TROJAN ALIASES BY QUARTER: 2000-2003 40
TABLE 4.17 – FREQUENCY DISTRIBUTION OF ALL TRENDS INFORMATION BY YEAR: 2000-2003 44
TABLE 4.18 – OTHER NIPC INFORMATION REPORTS BY YEAR: 2000-2003 49
TABLE 4.19 – OTHER NIPC INFORMATION REPORTS FREQUENCY DISTRIBUTION BY QUARTER: 2000-2003 50
TABLE 4.20 – MAJOR NATIONAL U.S. POLITICAL EVENTS AND CRISES: 2000-2003 71
TABLE 4.21 – U.S. MILITARY EVENTS AND CONFLICTS: 2000-2003 72
TABLE 5.1 – SOFTWARE BUGS CORRELATION ANALYSIS 80
TABLE 5.2 – COMPUTER VIRUSES CORRELATION ANALYSIS 82
TABLE 5.3 – U.S. INTERNET USERS CORRELATION ANALYSIS 83
TABLE 5.4 – U.S. BASED INTERNET HOST COMPUTERS CORRELATION ANALYSIS 85
TABLE 5.5 – GLOBAL WORLD WIDE WEB PAGES CORRELATION ANALYSIS 87
TABLE 5.6 – U.S. ELECTRONIC COMMERCE CORRELATION ANALYSIS 89
TABLE 5.7 – U.S. MACRO-ECONOMIC FACTOR CORRELATION ANALYSIS: PART ONE 91
TABLE 5.8 – U.S. MACRO-ECONOMIC FACTOR CORRELATION ANALYSIS: PART TWO 93
TABLE 5.9 – SUMMARY OF TESTING RESULTS FOR HYPOTHESIS THREE THROUGH SEVEN: SPEARMAN RANK CORRELATION COEFFICIENTS 95
TABLE 5.10 – STATISTICAL ANALYSIS OF THE USS COLE BATTLESHIP ATTACK 98
TABLE 5.11 – STATISTICAL ANALYSIS OF THE WAR IN AFGHANISTAN 100

TABLE 5.12 – STATISTICAL ANALYSIS OF THE SEPTEMBER 11, 2001 TERRORIST ATTACKS ON THE U.S. 102
TABLE 5.13 – STATISTICAL ANALYSIS OF THE U.S. INVASION OF IRAQ 104
TABLE 5.14 – STATISTICAL ANALYSIS OF THE U.S. MILITARY INTERVENTION IN LIBERIA 106
TABLE 5.15 – STATISTICAL ANALYSIS OF THE 2000 U.S. PRESIDENTIAL ELECTION 109
TABLE 5.16 – STATISTICAL ANALYSIS OF THE WESTERN STATES ENERGY CRISIS 111
TABLE 5.17 – STATISTICAL ANALYSIS OF THE SEVERE WINTER STORMS IN JANUARY 2003 113
TABLE 5.18 – STATISTICAL ANALYSIS OF THE NORTHEAST BLACKOUT IN AUGUST 2003 115
TABLE 5.19 – SUMMARY OF RESULTS FOR THE MILITARY AND POLITICAL EVENTS 117

CHAPTER FOUR – DESCRIPTIVE STATISTICS

4.1 Introduction

The fourth chapter of this study provides a descriptive summary of the CyberNotes data set, and provides the basis for testing the research hypotheses detailed in Chapter Three. Also included in this chapter is a presentation of the secondary data that will be incorporated in the detailed statistical testing that will be carried out in Chapter Five.

Due to the large volume of data over the study period, it was agreed that the most efficient presentation method would be yearly and quarterly data. More detailed analyses on a monthly and newsletter level were also developed. This information is presented in various supplemental appendices associated with this chapter, and is referenced internally within the appropriate section herein.

In total, six categories of data are presented, five of which are from the CyberNotes Newsletters and one is a compendium of the secondary data sources used in this study. The first category of data is Bugs, Holes and Patches. This covers such items as: vulnerability type, vendor, risk classification, availability of remediation tools, footnote source, number of footnotes, date reported, operating system type, and date variance/lag time. During the study period, the NIPC reported a total of 6,698 Bugs, Holes and Patches items.

The second category of data is Exploit Scripts. This category provided information about the name of the exploit script, availability of a workaround, and related file type. During the study period, the NIPC reported 3,040 total Exploit Scripts items.

Viruses are the third category of newsletter data. It includes a variety of information about computer viruses, specifically: virus name, virus type, virus date, and aliases. During the study period, the NIPC reported a total of 2,431 Viruses items.

The fourth category of data is Trojans. In this section, the related data elements include: name text, alias availability, alias name information, and alias quantity. During the study period, the NIPC reported a total of 15,145 Trojan items.

Trends are the fifth category of data, and this category was sub-divided into two discrete sub-sections. The first sub-section deals with probes, and the second sub-section discusses scans. These sub-areas were specifically segregated in the newsletters. During the study period, the NIPC reported a total of 200 Trend items.

Lastly, the Secondary Data components are described in the sixth data set. This is broken down into five sub-areas, as follows: (1) Other NIPC information sources, (2) Macro-economic data, (3) E-Commerce, (4) Information Technology Utilisation Data, and (5) Political and Military Events.

4.1.1 Data Accumulation Techniques

In order aggregate the data for this study, it was necessary to compute the data statistics at a reasonable level for the reader to understand, and for which sufficient testing could be employed. After ample discussion, it was agreed that the major portions of this study would best be illustrated on a quarterly basis, as this would provide for an easily presentable set of analyses.

To begin the initial data organisation, all individual CyberNotes newsletters were first aggregated and classified into yearly periods, as shown below:

Table 4.1 – CyberNotes Newsletter Aggregation Summary by Year: 2000-2003

Calendar Year	Beginning Issue Number	Ending Issue Number	Number of Newsletters
2000	2000-01	2000-25	25
2001	2001-01	2001-25	25
2002	2002-01	2002-25	25
2003	2003-01	2003-25	25
		Total	100

It is noted that beginning in 2000, the NIPC began publishing a Yearly Summary Report that is made available to the public. The related issue numbers for calendar years 2000, 2001, 2002 and 2003 are 2000-26, 2001-26, 2002-26, and 2003-26 respectively. Furthermore, since this is a summary of previously reported information these summaries are properly excluded from the data collection and analysis.

After this stage, the CyberNotes newsletters were then classified on a quarterly basis, as shown in the following table:

Table 4.2 – CyberNotes Newsletter Aggregation Summary by Quarter: 2000-2003

Study Period	Beginning Issue Number	Ending Issue Number	Number of Newsletters
Q1 - 2000	2000-01	2000-06	6
Q2 - 2000	2000-07	2000-12	6
Q3 - 2000	2000-13	2000-19	7
Q4 - 2000	2000-20	2000-25	6
Q1 - 2001	2001-01	2001-06	6
Q2 - 2001	2001-07	2001-12	6
Q3 - 2001	2001-13	2001-18	6
Q4 - 2001	2001-19	2001-25	7
Q1 - 2002	2002-01	2002-06	6
Q2 - 2002	2002-07	2002-12	6
Q3 - 2002	2002-13	2002-19	7
Q4 - 2002	2002-20	2002-25	6
Q1 – 2003	2003-01	2003-06	6
Q2 – 2003	2003-07	2003-13	7
Q3 - 2003	2003-14	2003-19	6
Q4 - 2003	2003-20	2003-25	6
		Total	100

The issue date was the sole criteria used to classify the newsletters into the sixteen quarterly periods used in this research project. For example, CN Issue Number 2002-04; with an issue date of February 18, 2004 was classified in the Q1–2002 study period.

4.1.2 Assumptions Acknowledged

During this study the researcher has acknowledged various assumptions and constraints. The overall assumptions have been previously discussed in earlier chapters, most notably in Chapters One and Three.

Additionally, it is further acknowledged that no modifications of NIPC data were made during this chapter where the descriptive qualities of the data are presented. The data was preserved in its original presentation and used solely for statistical analyses. The researcher did not attempt to modify, correct or alter the data elements in any fashion.

Lastly, in order to complete this study in a rigorous yet efficient fashion various time constraints influenced the amount of data that could be analysed. First of which was the data set for 1999 was de-selected from this study because of the fact that it was less relevant to the project timetable and also because it was not as well structured. Second, the number of data elements from each newsletter was quite large and this required a tremendous amount of time of the researcher to obtain the data, input it into MS-Excel, migrate it to SPSS and finally run the statistical analyses for presentation in this chapter. Furthermore, when adding 2003 data to this study, it took three months to receive the data from the FBI and then another three months of effort to complete the analyses.

4.2 Descriptive Characteristics of the Secondary Data

The total population of 100 CyberNotes Newsletters for 2000 to 2003 were incorporated into this study. Therefore, statistical sampling techniques were not necessary and many inherent assumptions and potential errors would be avoided. In essence, the advantage of this testing method allows for a one hundred percent census testing approach.

4.2.1 CyberNotes Data Summary Information

The summary of all CyberNotes data is presented in Table 4.3 to provide a general context for the overall frequency distribution of each reporting category on a yearly basis. Then it is decomposed to show similar information on a quarterly basis in Table 4.4.

Table 4.3 – Summary of Total CyberNotes Data by Year: 2000-2003

Year	Bugs Etc.		Exploit Scripts		Viruses		Trojans		Trends		Totals	
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.
2000	1,049	15.66	1,108	36.40	427	17.60	1,187	7.84	260	36.57	4,031	14.38
2001	1,114	16.64	532	17.60	461	19.00	3,007	19.85	170	23.91	5,284	18.85
2002	1,965	29.33	617	20.30	760	31.20	2,821	18.63	143	20.11	6,306	22.50
2003	2,589	38.66	783	25.70	783	32.20	8,160	53.88	138	19.13	12,453	44.44
Total	6,698	100.00	3,040	100.00	2,431	100.00	15,145	100.00	711	100.00	28,025	100.00
Percent of Total	23.90%		10.45%		8.67%		54.04%		2.54%		100.00%	

In this presentation, it is important to be aware that these frequencies present all reported items according to the guidelines established by the NIPC. More details of these guidelines are discussed in Chapter Two – Literature Review. In this frequency analysis, Bugs remain have a nearly identical level of reporting from 2000 to 2001 and then an approximate 50% increase is seen from 2001 to 2002 and additional substantial increase from 2002 to 2003. Exploit Scripts see a large decline in its frequency from 2000 to 2001 and then a relatively small increase in each of the following two years. The frequency distribution for Viruses is relatively constant for the first two years of the research study. Then in 2002, a noticeable increase of 65% per annum is recorded in 2003 with a minor increase to following in 2003. Trojans exhibit an usual frequency trend in that there was a tremendous growth in the reported items from 2000 to 2001, then the following year saw a minor decline; only to see a large upsurge in last year of the study. Trends which is a general reporting category for Probes, Scans and other general information sees a significant decline from 2000 to 2001 and then modest declines in each of the subsequent years.

A more detailed analysis on a quarterly basis was developed on the next table, as follows:

Table 4.4 – Summary of Total CyberNotes Data by Quarter: 2000-2003

Study Period	Bugs Etc.		Exploit Scripts		Viruses		Trojans		Trends		Totals	
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.
Q1 - 2000	230	3.43	283	9.31	72	2.96	90	0.59	47	6.61	687	2.45
Q2 - 2000	237	3.54	331	10.89	99	4.07	275	1.82	81	11.39	955	3.41
Q3 - 2000	296	4.42	300	9.87	116	4.77	371	2.45	88	12.38	1,081	3.86
Q4 - 2000	286	1.89	194	6.38	139	5.72	451	2.98	44	6.19	1,098	3.92
Q1 - 2001	272	1.80	155	5.10	119	4.90	245	1.62	34	4.78	803	2.87
Q2 - 2001	296	1.95	157	5.16	132	5.43	623	4.11	50	7.03	1,219	4.35
Q3 - 2001	325	2.16	154	5.07	118	4.85	1,194	7.88	43	6.05	1,772	6.32
Q4 - 2001	221	1.45	66	2.17	93	3.83	945	6.24	43	6.05	1,370	4.89
Q1 - 2002	455	3.00	129	4.24	165	6.79	165	1.09	22	3.09	926	3.30
Q2 - 2002	465	3.07	108	3.55	171	7.03	396	2.61	28	3.94	1,152	4.11
Q3 - 2002	526	3.48	215	7.07	251	10.32	901	5.95	37	5.20	1,906	6.80
Q4 – 2002	519	3.43	165	5.43	173	7.12	1,359	8.97	56	7.88	2,229	7.95
Q1 – 2003	597	3.94	133	4.38	200	8.23	652	4.31	34	4.78	1,616	5.77
Q2 – 2003	780	5.15	243	7.99	174	7.16	1,869	12.34	40	5.63	3,106	11.08
Q3 – 2003	601	3.97	211	6.94	212	8.72	2,382	15.73	39	5.49	2,633	9.40
Q4 – 2003	591	3.90	196	6.45	197	8.10	3,252	21.47	25	3.52	4,261	15.20
Sub-Total	6,698	100.00	3,040	100.00	2,431	100.00	15,145	100.00	711	100.00	28,025	100.00
Percent of Total	23.90%		10.45%		8.67%		54.04%		2.54%		100.00%	

The quarterly analysis illustrates a variety of interesting frequency observations. Bugs remains fairly consistent in 2000 then begins to decrease in Q4 of 2001, consistent once again throughout 2001 with a noticeable ongoing increase through the end of the study period. Exploit Scripts has a similar frequency as seen in the prior yearly analysis where the highest reported cases are in 2000. Viruses exhibit an increase in 2002 and forward. The reporting of Trojans on a quarterly basis indicates that the largest frequencies occur in

the second two quarters of each study year. Finally, the quarterly Trends frequency is consistent with the yearly frequencies discussed in the previous sub-section.

4.3 Bugs, Holes and Patches

The first section of the CyberNotes newsletters provides detailed information about the weaknesses identified in different types of computer software and information technologies.

4.3.1 Yearly and Quarterly Frequency Distributions

The volume of software weaknesses has increased each year, as evidenced by the data in the following table.

Table 4.5 – Bugs, Holes and Patches by Year: 2000-2003

Year	Frequency	Percentage	Cumulative Percentage
2000	1,049	15.66%	15.66%
2001	1,114	16.64	32.30
2002	1,965	29.33	61.63
2003	2,589	38.66	100.00%
Total	6,698	100.00%	

While this yearly information indicates a general increase in the trend of Bugs, Holes and Patches, further analysis on a quarterly basis was more revealing. Therefore, the researcher developed a more detailed frequency distribution. In Table 4.6 below, the total quarterly frequency distribution of Bugs, Holes and Patches is illustrated. From this presentation, we can see that there is a regular and continuous increase in the total number of Bugs, Holes and Patches items reported by the NIPC. The only exception to this trend is Q1 – 2002; where there was a decline in the number of reported items. It is interesting to note, that at this time the NIPC was being re-organised into one of the four directorates of the Department of Homeland Security (DHS). As part of the communication process with NIPC/DHS personnel, the researcher presented a formal briefing in the summer of 2005. This opportunity provided necessary feedback, suggestions and other comments from the data owners. After these meetings, further analysis and commentary was incorporated into Chapter 5 and Chapter 6.

Table 4.6 – Bugs, Holes and Patches: Types of Information Reported – Frequency Distribution by Quarter: 2000-2003

Study Period	New Items		Updated Items		Total	
	Freq.	Percent.	Freq.	Percent.	Freq.	Percent.
Q1 – 2000	217	3.65%	13	1.72%	230	3.43%
Q2 – 2000	228	3.84	9	1.19	237	3.54
Q3 – 2000	282	4.75	14	1.85	296	4.42
Q4 – 2000	270	4.55	16	2.11	286	4.27
Q1 – 2001	259	4.36	13	1.72	272	4.06
Q2 – 2001	285	4.80	10	1.32	296	4.42
Q3 – 2001	323	5.44	5	0.66	325	4.85
Q4 – 2001	217	3.65	2	0.26	221	3.30
Q1 – 2002	406	6.84	49	6.46	455	6.79
Q2 – 2002	430	7.24	35	4.62	465	6.94
Q3 – 2002	461	7.76	66	8.71	526	7.85
Q4 – 2002	434	7.31	85	11.21	519	7.75
Q1 – 2003	517	8.71	80	10.55	597	8.91
Q2 – 2003	632	10.64	148	19.53	780	11.65
Q3 – 2003	509	8.57	92	12.14	601	8.97
Q4 – 2003	468	7.88	123	16.23	591	8.82
Total	5,938	88.65%	758	11.35%	6,698	100.00%

Based on the above frequency distribution, it appears that three major conclusions can be drawn. First, there is an overall increasing trend to the Bugs, Holes and Patches over the time period. Second, the number of updated items is increasing over time. According to NIPC personnel, this is related to two underlying factors: improved relationships with vendors and other security organisations (i.e. CERT, research laboratories etc.) and the fact that major vendors have worked to improve the speed at which they produce patches, 'hotfixes', other upgrade solutions and tools for systems administrators and network managers.

4.3.2 Risk Levels

This area of the study examines the different risk levels of the Bugs, Holes and Patches. The researcher used the risk classifications detailed by the NIPC and was able to generate frequency analysis of these items, as shown on the following table.

Table 4.7 – Bugs, Holes and Patches: Risk Rating Frequency Distribution by Quarter: 2000-2003

Study Period	High		Medium		Low		All Other		Total	
	Freq.	Percent.	Freq.	Percent.	Freq.	Percent.	Freq.	Percent.	Freq.	Percent.
Q1 – 2000	122	4.50%	45	2.13%	56	5.19%	7	0.89%	230	3.44%
Q2 – 2000	94	3.47	73	3.45	51	4.73	19	2.41	237	3.54
Q3 – 2000	127	4.68	90	4.25	54	5.00	25	3.18	296	4.42
Q4 – 2000	119	4.39	105	4.96	49	4.54	13	1.65	286	4.27
Q1 – 2001	114	4.20	84	3.97	54	5.00	19	2.41	271	4.05
Q2 – 2001	116	4.28	106	5.01	50	4.63	24	3.05	296	4.42
Q3 – 2001	134	4.94	127	6.00	40	3.71	25	3.18	326	4.87
Q4 – 2001	81	2.99	87	4.11	39	3.61	12	1.52	219	3.27
Q1 – 2002	173	6.38	169	7.98	77	7.14	36	4.57	455	6.80
Q2 – 2002	188	6.93	168	7.94	61	5.65	48	6.10	465	6.95
Q3 – 2002	206	7.60	158	7.46	85	7.88	78	9.91	527	7.87
Q4 – 2002	188	6.93	172	8.12	76	7.04	83	10.55	519	7.75
Q1 – 2003	241	8.89	175	8.27	75	6.95	106	13.47	597	8.92
Q2 – 2003	300	11.06	233	11.01	120	11.12	127	16.14	780	11.65
Q3 – 2003	255	9.40	169	7.98	98	9.08	78	9.91	600	8.96
Q4 – 2003	254	9.37	156	7.37	94	8.71	87	11.05	591	8.83
Total	2,712	100.00%	2,117	100.00%	1,079	100.00%	787	100.00%	6,698	100.00%
Percent of Total	40.50%		31.62%		16.12%		11.76%		100.00%	

From the above table, nearly half or 40.50% of the reported items are high risk, 31.62% are medium risk, 16.12% are low risk, and 11.76% relate to other items. This was accomplished by grouping the detailed classification into the higher classification category of the original items. For instance, items with a risk classification of High/Medium, in the summary tabulation this group were classified as high. Similarly, items given a Low/Medium risk rating were grouped into the Medium category for this analysis.

Although all related threats are considered by the NIPC's Watch and Warning Unit when developing their information, the majority of information in this section is related to computer software.

The next sub-section discusses the types of vulnerabilities within Bugs, Holes and Patches. This is a critical area since it describes the specific flaw/weakness identified by the NIPC.

Table 4.8 – Bugs, Holes and Patches: Top Vulnerabilities in Rank Order: 2000-2003

Vulnerability	Ranking
Buffer Overflow	1
Denial of Service	2
Multiple Vulnerabilities	3
General Security	4
Password	5
Unauthorised Access	6
Remote Access	7
Directory Transversal	8
Race Condition	9
Web Server – IIS	10
Root Access	11
E-Mail	12
Format String	13

As discussed in Chapter Two, buffer overflows causes memory processing errors where by an extra portion of programming code is running such that the program results in the program extending beyond its pre-defined buffers. Denial of service is a vulnerability where the organization's IT systems are flooded with packets and unable to process transactions. Multiple vulnerabilities is an inclusive category for two or more vulnerabilities existing within the same issue.

Table 4.9 – Bugs, Holes and Patches: Attack Code Summary in Rank Order: 2000-2003

Attack Code Category	Ranking	Frequency	Percentage
Bug Discussed in Newsgroup and Web Site; Exploit Script Has Been Published	1	2,538	37.90%
Bug Discussed in Newsgroup; Exploit Has Not Been Published	2	2,113	31.60
Bug Discussed in Newsgroup and Web Site; No Exploit Required	3	1,119	16.70
Bug Discussed in Newsgroup and Web Site; Exploit Has Been Published	4	346	5.20
Bug Discussed in Newsgroup and Web Site; Common Software Tools Required to Execute	5	309	4.60
Bug Discussed in Newsgroup and Web Site, Vulnerability Appeared in Press	6	208	3.10
	Subtotal	6,633	99.03%
All Others		65	0.07
	Grand Total	6,698	100.00%

From this analysis, the main three types of information about attack codes are apparent. Firstly, the majority of Bugs are discussed in Newsgroups and/or Web Sites. This is important because it signifies that this information is accessible particularly to FBI personnel in the Watch and Warning Section of the NIPC. Secondly, approximately 47% of the attack codes have no exploit script published or required which in turn makes the Bug more likely to be exploited. This is because the Bug is known, but only in some cases is the attack method used to compromise the vulnerability easily available (e.g. web sharing or otherwise). Lastly, this area is to be considered in the last chapter as a suggestion for future research.

Table 4.10 – Bugs, Holes and Patches: Workaround Availability High Level Classification Ranking: 2000-2003

Workaround Category	Ranking	Frequency	Percentage
No Workaround Known at Publishing	1	2,821	42.10%
Upgrade Available – Specific URL Provided	2	1,897	28.30
Patch Available – Specific URL Provided	3	1,159	17.30
	Subtotal	5,877	87.74%
All Others		821	12.26
	Total	6,698	100.00%

From this analysis it was determined that 42.10% of the Bugs have no workaround known at the time of the CyberNotes newsletter being published. However, 45.60% of the workarounds are available when the newsletters are made available. Finally, another 12.26% have been classified as all others. This is associated with the immediately previous sub-section since each Bug has both an attack code and the NIPC is able to recommend workarounds (e.g. countermeasures, fixes etc.) in this component of the newsletter for each reported item. The next section of descriptive statistics examines the vendor distribution for Bugs, Holes and Patches.

Table 4.10 – Bugs, Holes and Patches: Vendor Frequency Distribution – Top 20 Vendors: 2000-2003

Vendor Name	Ranking	Frequency	Percentage
Microsoft	1	610	9.11%
Multiple Vendors	2	267	3.99
Rsoft	3	139	2.08
Sun Microsystems	4	139	2.08
Hewlett-Packard	5	104	1.55
Cisco Systems	6	91	1.34
Active State	7	90	1.34
FreeBSD	8	76	1.13
IBM	9	65	0.97
Linux	10	64	0.97
Redhat	11	50	0.75
Oracle	12	49	0.73
Netscape	13	44	0.66
Novell	14	33	0.49
Allaire	15	33	0.49
SCO	16	31	0.46
Trend Micro	17	29	0.43
SuSe	18	28	0.42
Apple	19	28	0.42
Symantec	20	27	0.40
	Sub-Total	1,997	29.81%
All Others		4,701	70.19
	Grand Total	6,698	100.00%

This analysis provides evidence for two very interesting findings. First, it corroborates some of the publicly debated issues about Microsoft Corporation being a risk to U.S. national security since slightly more than nine percent of the total population of Bugs, Holes and Patches are associated with this company's products (Schnier Et. Al. 2003). The second major finding is that of the Top 20 Vendors only represent approximately 30% of all the vulnerabilities. Therefore, the remaining 70% of the reported Bugs, Holes and Patches are attributable to the remaining number of vendors which is documented to be 1,975 or an average of 2.38 items per vendor. In other words, while the Top 20 Vendors are 1% of the entire vendor population they are responsible for 30% of the Bugs, Holes and Patch incidents. Likewise the remaining 99% of the vendors are accountable for 70% of these reported items.

Additionally, the source of the information provided to the NIPC is also analysed. The next sub-section presents a frequency analysis of the information sources for Bugs, Holes and Patches.

Table 4.12 – Bugs, Holes and Patches: Top 20 Reference Information Sources: 2000-2003

Organisation Name	Ranking	Frequency	Percentage
Bugtraq	1	1,675	25.01%
Multiple	2	750	11.20
Securiteam	3	722	10.78
Securifocus	4	472	7.05
Microsoft Security Bulletin	5	290	4.33
Security Tracker	6	172	2.57
No. 382	7	138	2.06
Debian Security Advisory	8	128	1.91
Hewlett-Packard Security Advisory	9	119	1.78
Cisco Security Advisory	10	82	1.22
FreeBSD Security Advisory	11	77	1.15
iDefense Security Advisor OpenPKG Security Advisory	12	47	0.70
RedHat Security Advisory	13	47	0.70
No. 362	14	45	0.67
eSecurity Online Free Vulnerability	15	45	0.67
NTBugtraq	16	42	0.63
NGSSoftware Insight Security Research Advisory	17	40	0.60
SGI Security Advisor	18	38	0.58
Georgi Guninski Security Advisory	19	37	0.55
CERT Advisory	20	35	0.52
	Sub-Total	5,001	74.66%
All Others		1,697	25.34
	Grand Total	6,698	100.00%

From this analysis is it clearly evident that a popular IT industry web site, Bugtraq is the most common source of Bug information followed by Multiple sources and Securiteam, respectively. In addition, the shear quantity of information sources is very large which can be considered as a complexity in the information gathering and verification function of the NIPC.

Detailed graphs for the frequency distributions for this category of data have been developed and included in the following supplements:

- Monthly Frequency Distribution Analysis: Bugs, Holes and Patches – Supplement 2
- CN Issue Level Frequency Distribution Analysis: Bugs, Holes and Patches – Supplement 2

4.4 Exploit Scripts

From 2000-2003, a total of 3,040 Exploit Scripts items were reported by the NIPC. The next section describes the yearly and quarterly frequency distributions of this data.

4.4.1 Yearly and Quarterly Frequency Distributions

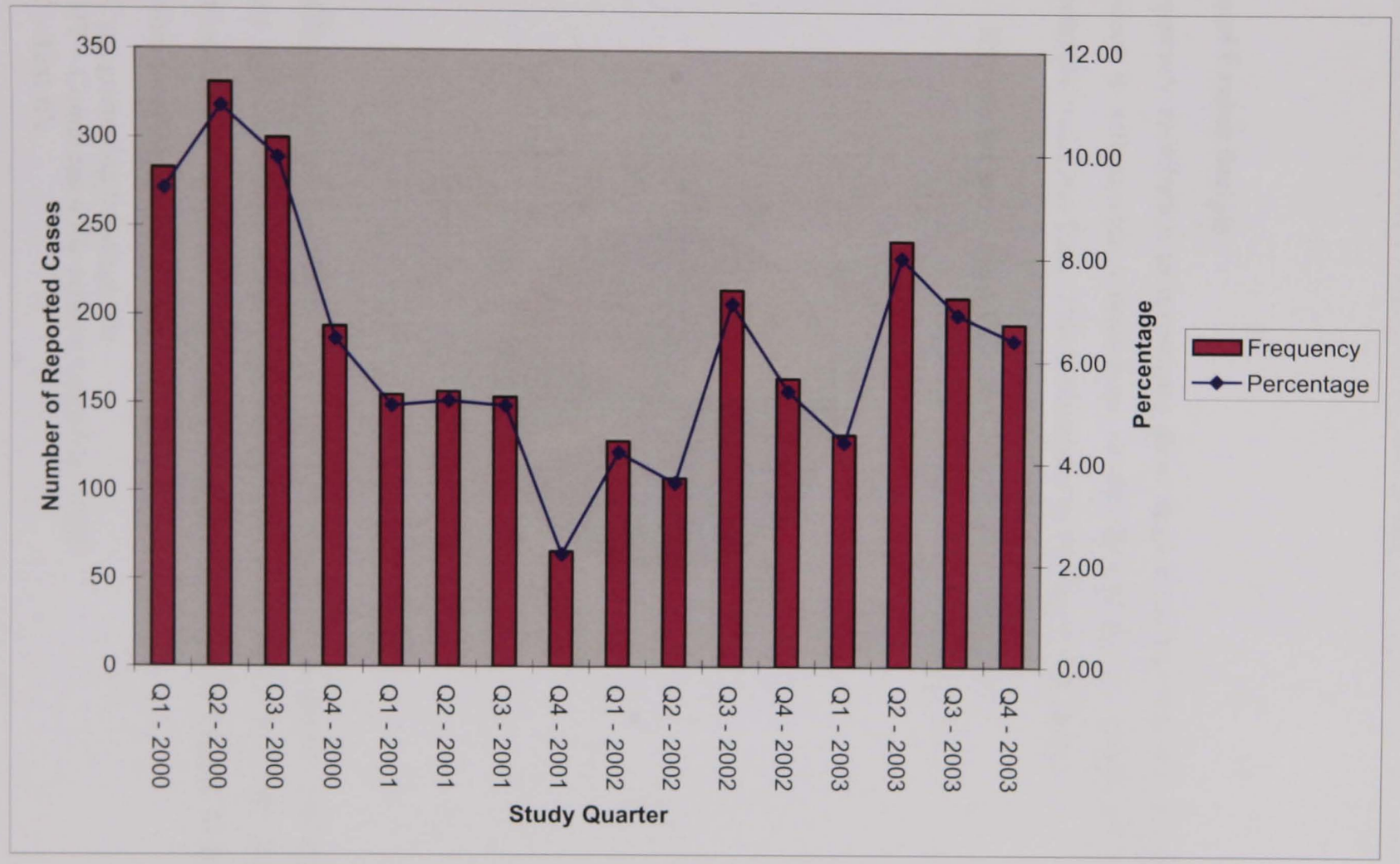
Both yearly and quarterly frequency distributions were calculated in order to analyse this portion of the data. Table 4.13 below summarises the frequencies of the Exploit Scripts on a yearly basis.

Table 4.13 – Exploit Scripts Frequency Distribution by Year: 2000-2003

Year	Frequency	Percentage	Cumulative Percentage
2000	1,108	36.40%	36.50%
2001	532	17.60	54.00
2002	617	20.30	74.30
2003	783	25.70	100.00%
Total	3,040	100.00%	

This has been further broken-down by quarterly period in Figure 4.1 below, as follows:

Figure 4.1 – Exploit Scripts Frequency Distribution by Quarter: 2000-2003

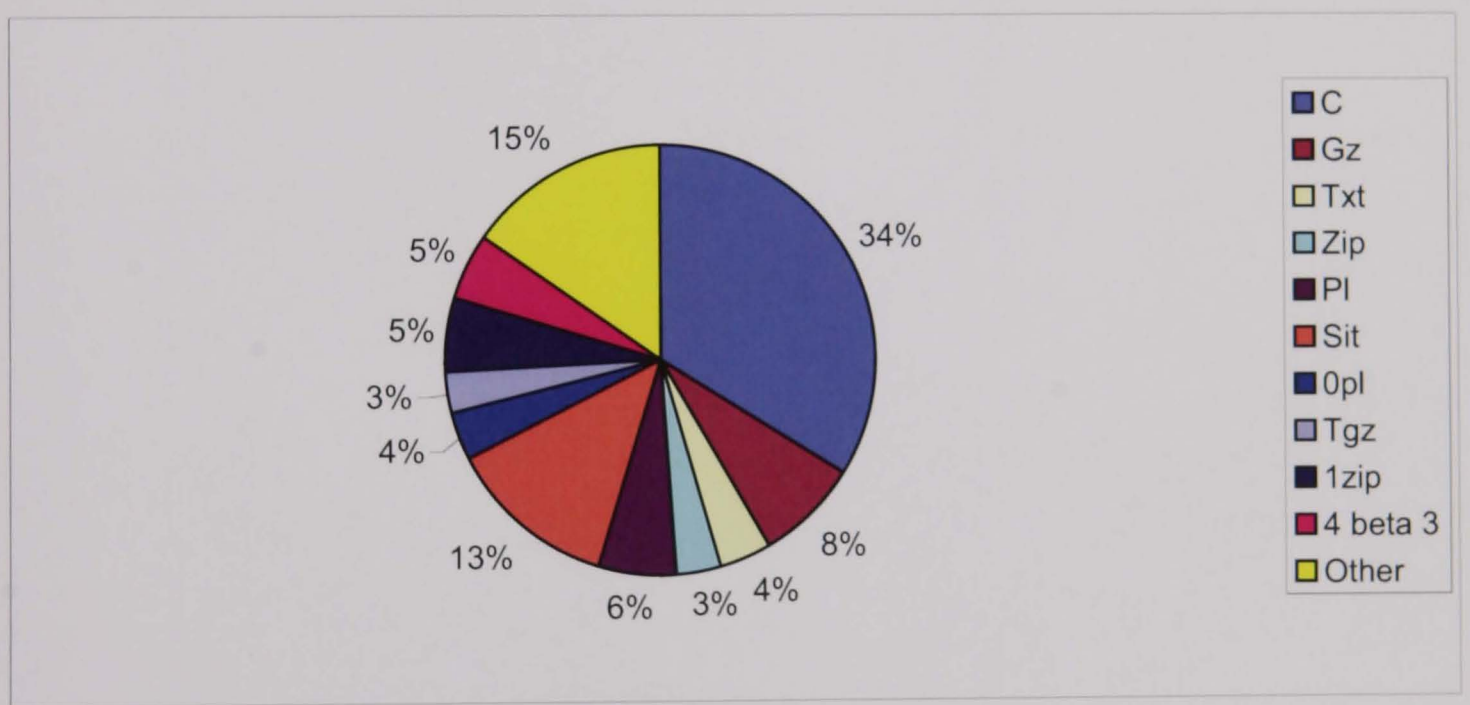


Based on this frequency distribution it is interesting to note that the quarter with the highest frequency is Q2 - 2000 with 331 items and the lowest frequency of 66 items was reported in Q4 – 2001. Furthermore, the mean number of Exploit Scripts per quarter has been calculated to be 190.

4.4.2 Types of Exploit Scripts

Another frequency distribution to investigate about Exploit Scripts was the file type. This is important since it will provide a breakdown of the file extensions, which can be useful in screening potential malicious files. This is illustrated in the Figure 4.2, below:

Figure 4.2 – Exploit Scripts – Most Common File Types: 2000-2003



The types of Exploit Scripts have been classified into seven major categories. The ranking of the most common types of Exploit Script files is as follows: C, GZ/SIT, TXT, ZIP, TGZ, PL, SH and All Others. The following is a brief description of each type of Exploit Script file from Webopedia.com (accessed in July 2006):

C – C programming language file
GZ/SIT – Compressed file archive created by GZIP
TXT – Text file

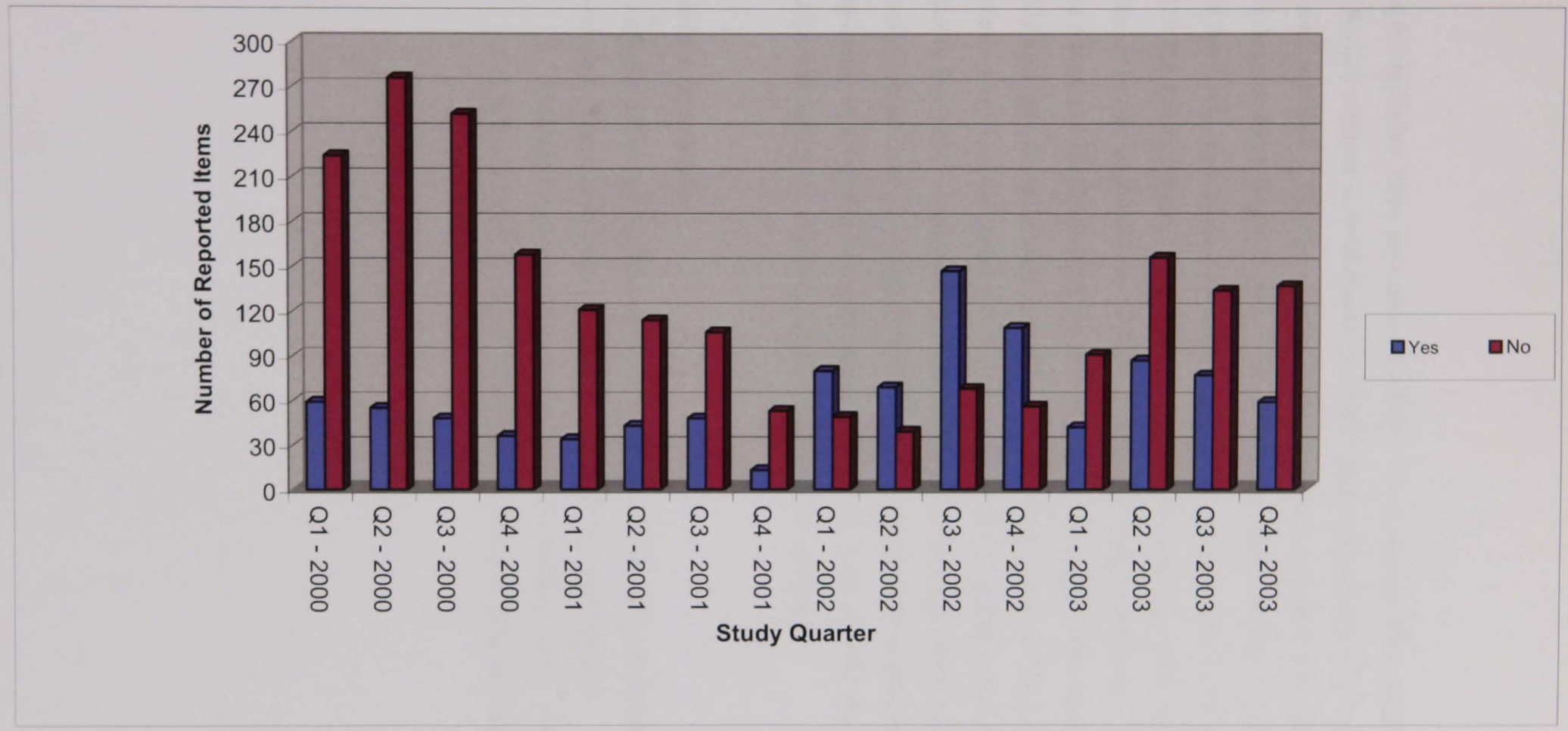
ZIP – Compressed file archive created by PKZIP
PL – PERL source code file
SH – UNIX shell script

While these types of files are interesting to make reference to, future related research opportunities are highlighted in Chapter six.

4.4.3 Workaround Availability

Another important study area of the Exploit Scripts data is the availability of remediation (e.g. workaround techniques). This is very important because it provides basic information to the Information Assurance community about the tools that are available to prevent and/or react to this type of attack.

Figure 4.3 – Exploit Scripts Workaround Availability: 2000-2003



This graph highlights three interesting findings. First, during 2000 and 2001 the number of Exploit Scripts without a workaround available greatly surpassed the Exploits Scripts with a workaround available. Second, during 2002 there was a greater abundance of workarounds available then for those Exploit Scripts without a workaround available. According to Mr. Vince Rowe of the NIPC, this might be due to the fact that software and hardware vendors began to respond to the vulnerabilities in a quicker period of time (e.g. by producing a workaround at the same time or nearly simultaneous to the Exploit Script being publicised). Third, the 2003 data indicates a return to the 2000-2001 trend; whereby the Exploit Scripts without workarounds are noticeably less than for those with a workaround available. In fact, 67% of the total population did not have a workaround available at time of publication and the remainder (only 33%) had workarounds available. Another interesting point is that for each quarter in the first three years of the study period there is a greater percentage of incidents with workarounds available. But, then beginning in Q1-2002 and continuing through the end of 2002 there are more Exploit Scripts reported with workarounds available then for those without.

4.4.4 Further Information

Detailed graphs depicting the frequency distributions of the reported Exploit Scripts have also been developed. These have been included in the following supplements:

- Monthly Frequency Distribution Analysis: Exploit Scripts – Supplement 2.
- CN Issue Level Frequency Distribution Analysis: Exploit Scripts – Supplement 2.

4.5 Viruses

During the study period a total of 2,431 virus cases were reported. The following sections provide yearly and quarterly frequency distribution information, as well as details about the types of viruses reported and the number of aliases associated with each virus.

4.5.1 Yearly and Quarterly Frequency Distributions

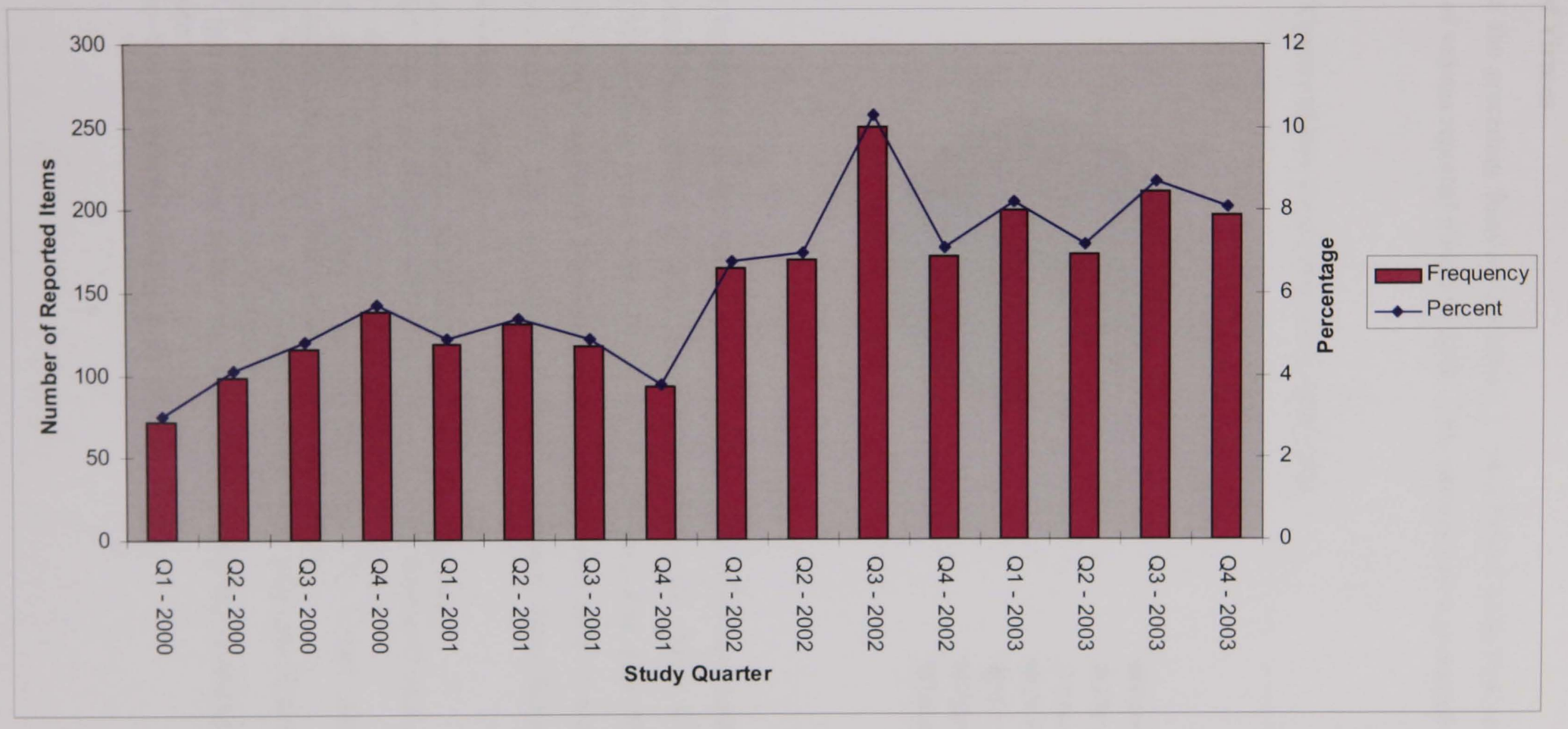
In order to develop some preliminary frequency distribution information, this information is first presented on a yearly basis in Table 4.14 below.

Table 4.14 – Total Virus Cases by Year: 2000-2003

Year	Frequency	Percentage	Cumulative Percentage
2000	427	17.60%	17.60%
2001	461	19.00	36.60
2002	760	31.20	77.80
2003	783	32.20	100.00%
Total	2,431	100.00%	

To subject this data to a more efficient analysis, the following figure details the virus frequency information on a quarterly basis.

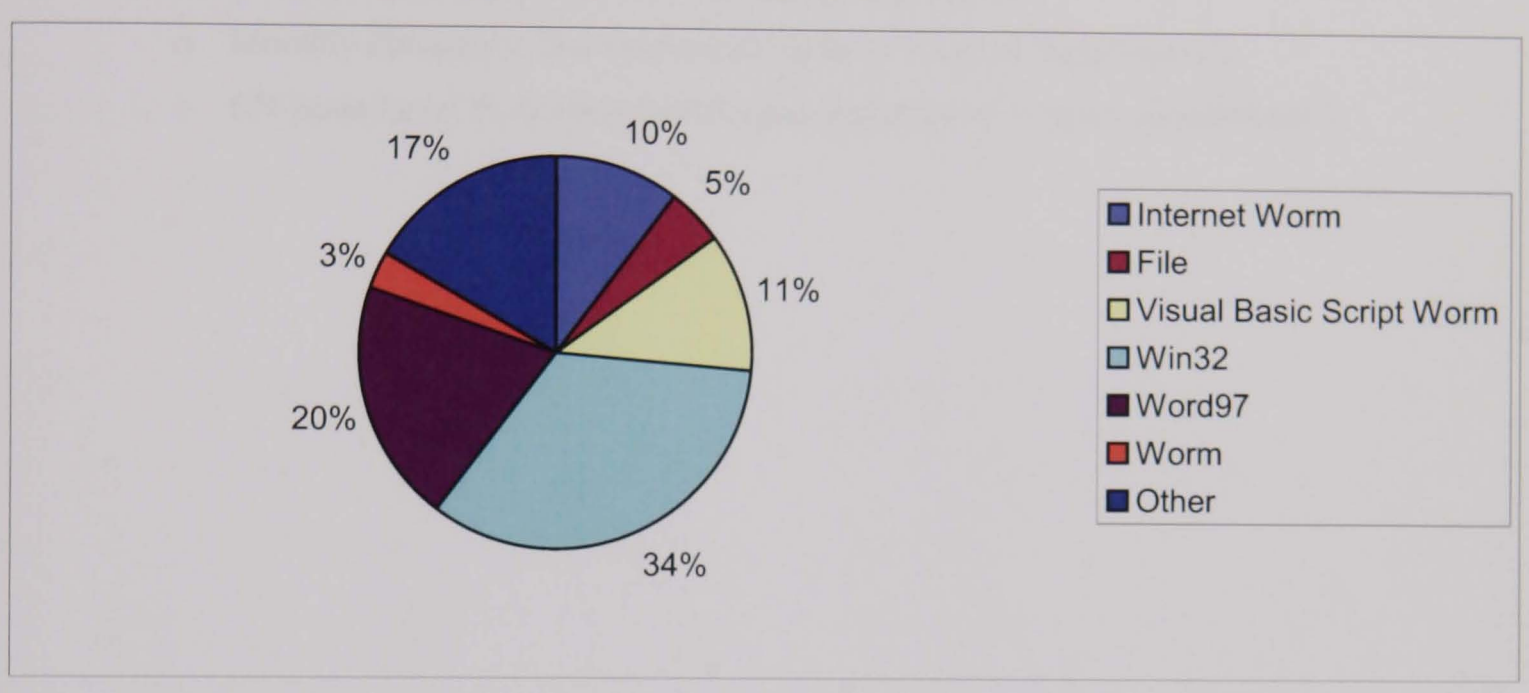
Figure 4.4 – Viruses Cases by Quarter: 2000-2003



4.5.2 Types of Viruses

In addition to the preceding frequency analysis, a consolidated classification of the most popular type of viruses reported was developed. This information is presented in Figure 4.5 below:

Figure 4.5 – Viruses Major Types Reported: 2000-2003



This analysis highlights the fact that the most common types of viruses related to critical infrastructure protection ranked in order of prevalence are: Win32 (34%), Word97 (20%), Other (17%), Visual Basic Script Worm (11%), Internet Worm (10%), File (5%) and Worm (3%). The following is a general description of each of the major types of viruses described in this analysis obtained from a variety of sources (Adapted from Webopedia, 2006, Bosworth and Kabay, 2002):

1. Win32 – these virus files infect the Windows operating system,
2. Word97 – this type of virus infects the Microsoft Word Version 97 files,
3. Other – denotes various (approximately 22) types of viruses,
4. Visual Basic Script Worm – specifically uses the Visual Basic advanced programming language feature to infect files with a worm,
5. Internet Worm – this virus is a worm file that has been specifically designed to populate and migrate over the Internet,
6. File – this type of virus infects the main files used by the operating system on a computer, and
7. Worm – this is a general description heading for worms.

This type of information is very useful to systems administrators and information security officers who need to monitor their networks and understand the major types of viruses that might infect their systems.

4.5.3 Further Information

Detailed graphs depicting the frequency distributions of the viruses reported by the NIPC have also been developed and included in the following supplements:

- Monthly Frequency Distribution Analysis of Viruses: Supplement 2.
- CN Issue Level Frequency Distribution Analysis of Viruses: Supplement 2.

4.6 Trojans

The Trojans section is the fourth category of data reported in the CyberNotes newsletters. In particular, the frequency distributions for yearly and quarterly periods are highlighted in the first sub-section. Lastly, the Trojans types and alias information is presented.

4.6.1 Yearly and Quarterly Frequency Distributions

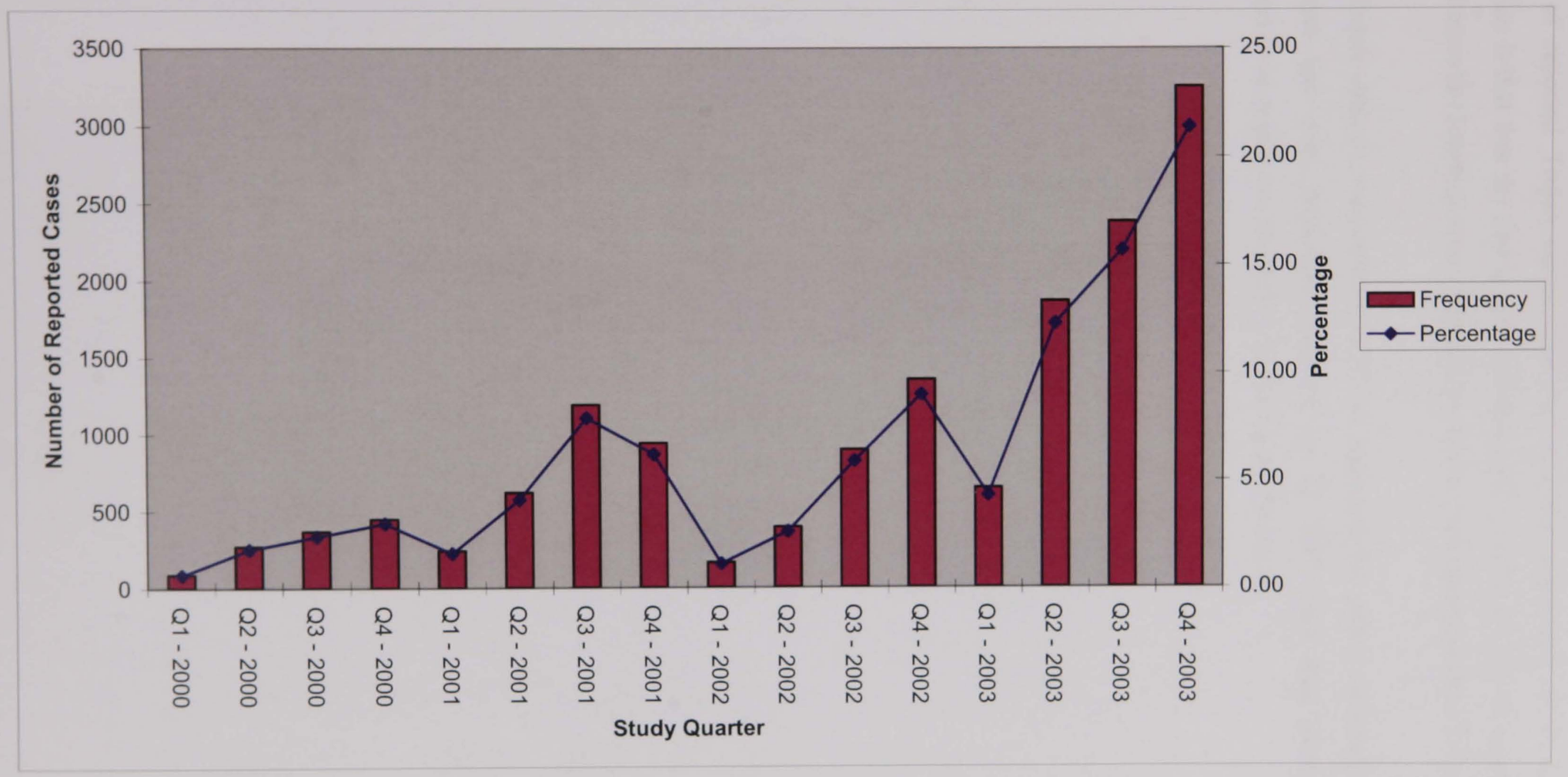
The first stage of analysis involved a yearly frequency distribution of all Trojans. Table 4.15 below, provides the high-level yearly frequency distribution information.

Table 4.15 – Trojans Frequency Distribution by Year: 2000-2003

Year	Frequency	Percentage	Cumulative Percentage
2000	1,187	7.84%	7.84%
2001	3,007	19.85	25.69
2002	2,821	18.63	44.32
2003	8,160	53.88	100.00%
Total	15,145	100.00%	

The above analysis indicates a dramatic rise in the number of Trojans from 2000 to 2001, and then a minor decrease from 2001 to 2002. This was then followed by a very large yearly increase of 289 percent from 2002 to 2003.

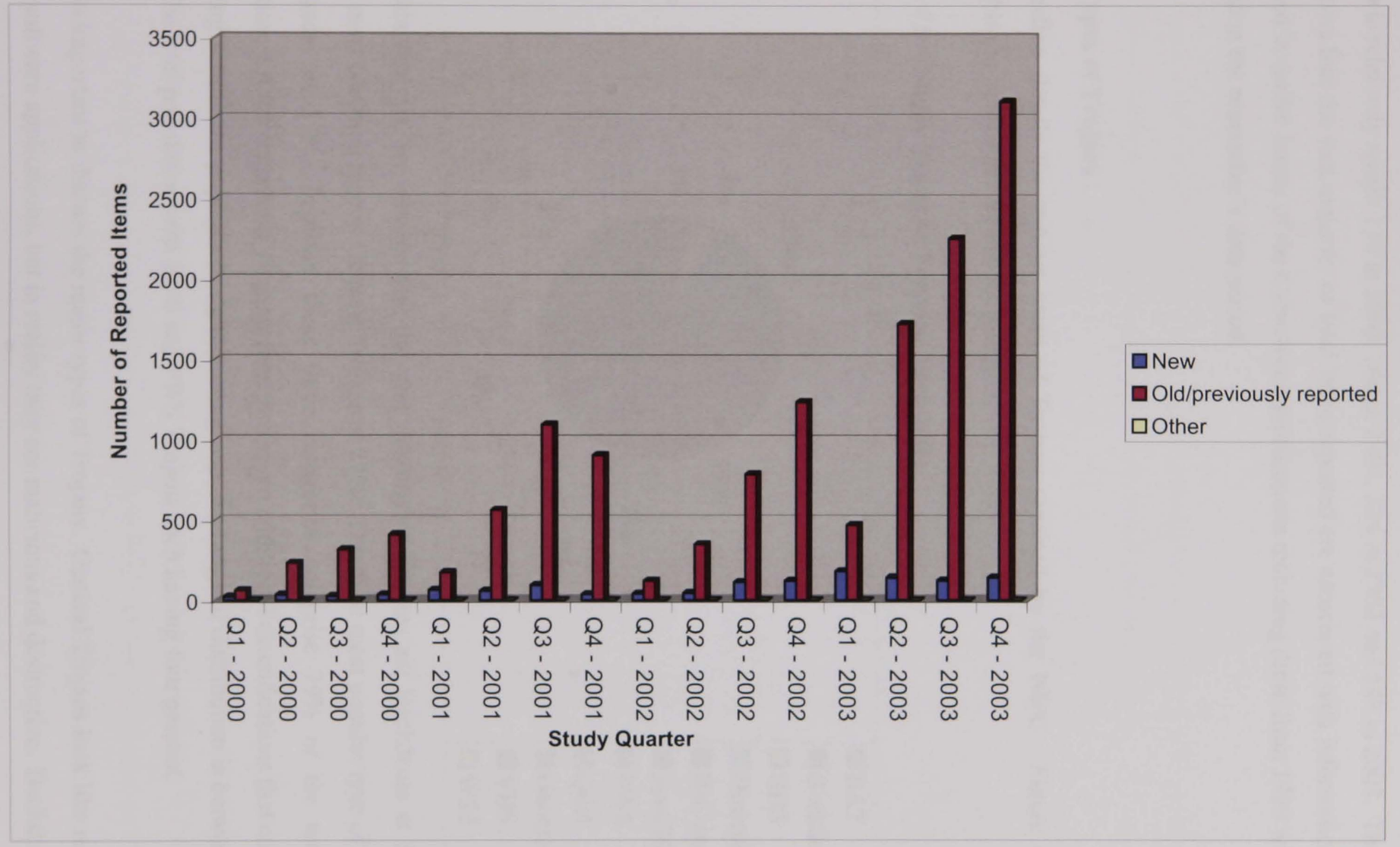
Figure 4.6 – Trojans Cases Frequency Distribution by Quarter: 2000-2003



From this analysis we can see that there is a regular and significant increase in the total number of reported Trojan cases; with one outlying yearly period of 2002. Another observation is that that the first quarter of each year contains the lowest number of reported cases, whereas the fourth quarter of each year reports the largest number of Trojans.

An additional analysis was made in order to segregate the newly reported incidents from those items that were previously reported by the NIPC and then remained in future newsletters to re-emphasise the most popular types of Trojans.

Figure 4.7 – New Versus Previously Reported Trojans by Quarter: 2000-2003

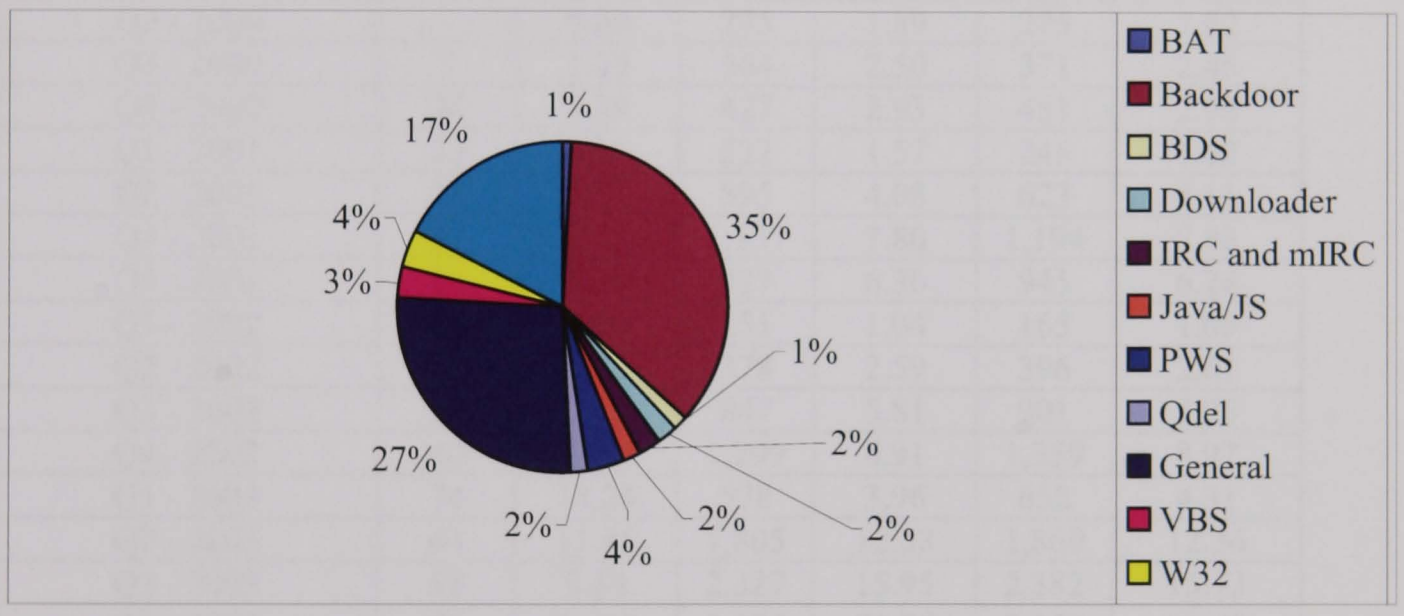


Another interesting observation from this figure highlights the fact that the number of new Trojans is relatively small: 130 in 2000, 260 in 2001, 324 in 2002 and 598 in 2003. This analysis also shows that the vast majority of total items reported are associated with information that was discussed in earlier issues of the CyberNotes publications including those from 1999 which is not included in the researcher's data period.

4.6.2 Types of Trojans

This section details the various types of Trojans reported by the NIPC. Figure 4.8 below highlights the breakdown of this information:

Figure 4.8 – Major Types of Trojans: 2000-2003



From this analysis, we can see that the vast majority of Trojans are Backdoors at 35%. The second most common type is General Trojans at 27%. The third most popular type of Trojans is Downloader at 17%. Together these three categories comprise 79% of the total Trojan population. Of the remaining Trojans, there are seven additional classifications that compose the remaining 21% of the population. In this sub-group, the range of distribution is between 1% and 4% of the total population with BDS and PWS Trojans each having four percent.

It is also important to discuss the major types of Trojans. General Trojans look like regular (e.g. benign software applications, but in reality they are malicious and destructive. Backdoor Trojans

allow the attacking party to obtain full administrator access to the computer and is a high level security risk.

4.6.3 Aliases

When Trojans have aliases it adds additional complexity to the tracking and reporting of these items. Table 4.16 below illustrates how many Trojans have reported aliases.

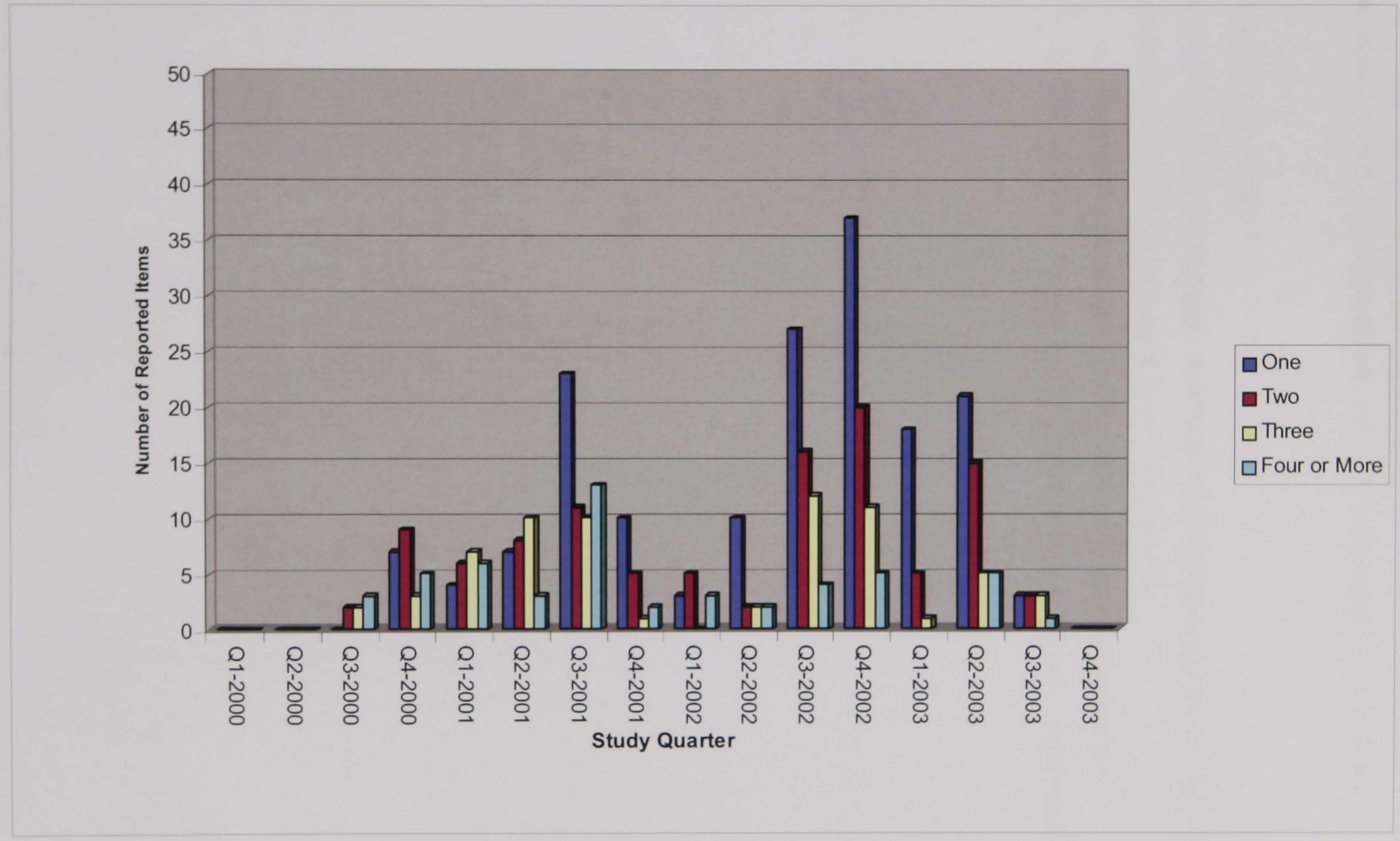
Table 4.16 – Reported Trojan Aliases by Quarter: 2000-2003

Study Period	Yes		No		Total	
	Freq.	Percent.	Freq.	Percent.	Freq.	Percent.
Q1 - 2000	-	0.00%	90	0.62%	90	0.59%
Q2 - 2000	-	0.00	275	1.89	275	1.82
Q3 - 2000	7	1.25	364	2.50	371	2.45
Q4 - 2000	24	4.29	427	2.93	451	2.98
Q1 - 2001	23	4.11	222	1.52	245	1.62
Q2 - 2001	28	5.01	595	4.08	623	4.11
Q3 - 2001	57	10.20	1,137	7.80	1,194	7.88
Q4 - 2001	18	3.22	927	6.36	945	6.24
Q1 - 2002	14	2.50	151	1.04	165	1.09
Q2 - 2002	18	3.22	378	2.59	396	2.61
Q3 - 2002	54	9.66	847	5.81	901	5.95
Q4 - 2002	60	10.73	1,299	8.91	1,359	8.97
Q1 - 2003	74	13.24	578	3.96	652	4.31
Q2 - 2003	64	11.45	1,805	12.38	1,869	12.34
Q3 - 2003	55	9.84	2,327	15.95	2,382	15.73
Q4 - 2003	63	11.27	3,189	21.86	3,252	21.47
Totals	559		14,585		15,144	
Percent of Total	3.69%		96.31%		100.00%	

This frequency distribution indicates that the NIPC began to identify aliases for Trojans in the third quarter of 2000. From that point forward, the percentage of Trojans aliases remained very small at less than four percent of total over the entire period from 2000 to 2002. We can also see from this presentation that 96.31% all reported Trojans have no alias and the remaining 3.69% have aliases.

Further analysis indicates that one primary Trojan can have a multiple number of aliases. This is illustrated on a quarterly basis in Figure 4.9 below:

Figure 4.9 – Number of Trojan Aliases by Quarter: 2000-2003



Finally, from the composite listing of Trojans with aliases 46.00% have just one alias, 26.64% have two aliases, 15.99% have three aliases, and 11.37% have four or more aliases.

4.6.4 Further Information

Detailed graphs depicting the frequency distributions of the Trojans reported by the NIPC have also been developed and included in the following supplements:

- Monthly Frequency Distribution Analysis: Trojans – Supplement 2.
- CN Issue Level Frequency Distribution Analysis: Trojans – Supplement 2.

4.7 Trends

The NIPC provides two specific types of trend information in the CyberNotes newsletters. The two specific types of trends reported are: 1) Probes and Scans discuss these two types of specific network security threats and 2) Other Items which are more diverse and cover a variety of other (e.g. more general) information assurance observations made by government analysts during the bi-weekly reporting period.

4.7.1 Yearly and Quarterly Frequency Distributions

The frequency distributions for Trends were developed on both a yearly and quarterly basis. First, Table 4.17 provides a general frequency distribution of all trend information on a yearly basis below.

Table 4.17 – Frequency Distribution of All Trends Information by Year: 2000-2003

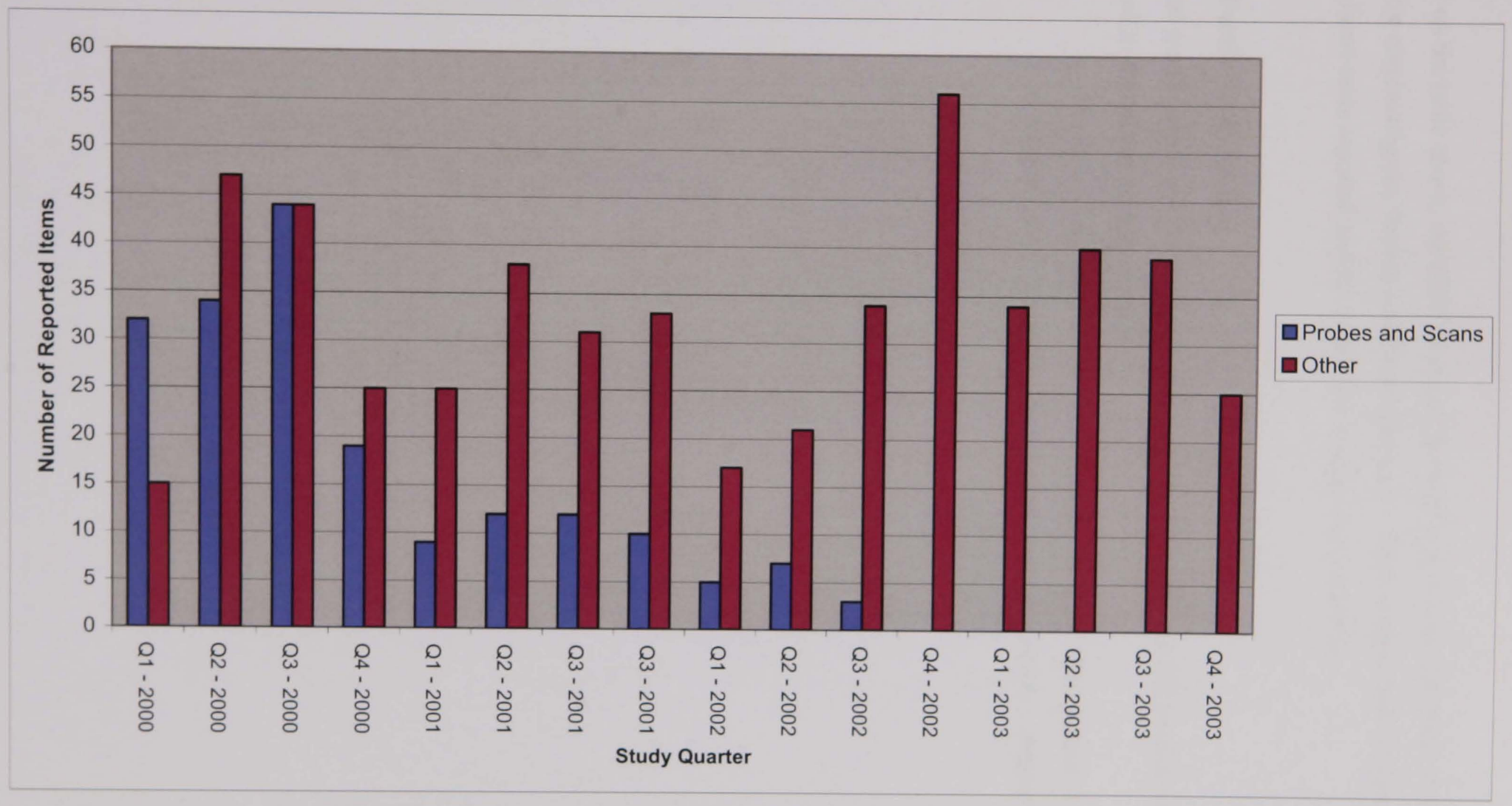
	Probes and Scans			Other Items		
Year	Frequency	Percentage	Cumulative Percentage	Frequency	Percentage	Cumulative Percentage
2000	129	68.98%	68.98%	131	25.00%	25.00%
2001	43	23.00	92.98	127	24.24	49.24
2002	15	8.02	100.00%	128	24.24	73.48
2003	-	0.00		138	26.52	100.00%
Totals	187	100.00%		524	100.00%	

From this frequency analysis we can see that the number of Probes and Scans decreased dramatically from 2000 to 2001 and each year thereafter. In contrast, the Other Items remain very consistent throughout the study period.

While the NIPC segregated this information into two categories from 2000 through 2002, there was a change in reporting format beginning in 2003. At that time, the separation of probes and other information was eliminated and all information need to be considered as Other. For the

purposes of further evaluating this information on a quarterly basis the researcher generated a quarterly frequency distribution which is shown below in Figure 4.10:

Figure 4.10 – Trends Frequency Distribution by Quarter: 2000-2003



Based on the table above, the NIPC changed the reporting scheme for trend information in Q4 – 2002 by eliminating the Probes and Scans category. Prior to this, both Probes and Scans and Other items were reported and the respective frequencies are noted.

4.7.2 Further Information

Detailed graphs depicting the frequency distributions of Trends activity has been developed and included in the following supplements:

- Monthly Frequency Distribution Analysis: Trends – Supplement 2.
- CN Issue Level Frequency Distribution Analysis: Trends – Supplement 2.

4.8 Secondary Data Items

Based on the detailed testing planned for Chapter Five, the researcher obtained a variety of data from secondary information sources. Wherever possible, U.S. government sources were utilised and all other cases the sources of information were public databases and websites.

4.8.1 An Overview

According to the research methodology outlined in Chapter Three; the related research questions require a series of secondary data elements was needed to test individual hypotheses. The secondary data has been segregated into five primary categories:

1. Other NIPC information reports and disclosures;
2. Macro-economic data;
3. E-commerce data;
4. Information technology data; and
5. Political and military event information.

Each of these sub-categories is addressed separately in the subsequent sub-sections hereto.

4.8.2 Other NIPC Information Reports and Disclosures

The NIPC also generated a variety of other information about Information Security during the study period. This type of information ranges from material on high-level threats to critical infrastructures and computer software and operating systems.

Table 4.18 – Other NIPC Information Reports by Year: 2000-2003

Year	Frequency	Percentage	Cumulative Percentage
2000	40	31.50%	31.50%
2001	55	43.31	74.81
2002	19	14.96	89.77
2003	13	10.23	100.00%
Total	127	100.00%	

This has been further broken down on a quarterly basis by each type of other NIPC information in the following table:

Table 4.19 – Other NIPC Information Reports Frequency Distribution by Quarter: 2000-2003

Study Period	Alerts		Advisories		Assessments		Info. Highlights		Press Releases		Total	
	Freq.	Percent.	Freq.	Percent.	Freq.	Percent.	Freq.	Percent.	Freq.	Percent.	Freq.	Percent.
Q1 - 2000	-	0.00%	1	2.22%	-	0.00%	-	0.00%	-	0.00%	1	0.80%
Q2 - 2000	8	50.00	6	13.33	2	12.50	-	0.00	3	13.04	19	16.66
Q3 - 2000	1	6.25	1	2.22	4	25.00	-	0.00	2	8.70	8	7.00
Q4 - 2000	-	0.00	5	11.11	4	25.00	-	0.00	3	13.04	12	10.52
Q1 - 2001	-	0.00	4	8.88	1	6.25	3	21.43	8	34.78	16	14.04
Q2 - 2001	1	6.25	6	13.33	-	0.00	3	21.43	-	0.00	10	8.77
Q3 - 2001	1	6.25	5	11.11	2	12.50	2	14.29	7	30.43	17	14.91
Q4 - 2001	2	12.50	6	13.33	1	6.25	3	21.43	-	0.00	12	10.52
Q1 - 2002	1	6.25	2	4.44	-	0.00	1	7.14	-	0.00	4	3.51
Q2 - 2002	1	6.25	5	11.11	-	0.00	2	14.29	-	0.00	8	7.00
Q3 - 2002	1	6.25	2	4.44	2	12.50	-	0.00	-	0.00	5	4.39
Q4 - 2002	-	0.00	2	4.44	-	0.00	-	0.00	-	0.00	2	1.75
Q1 - 2003	-	0.00	2	4.44	-	0.00	-	0.00	-	0.00	2	1.75
Q2 - 2003	-	0.00	5	11.11	-	0.00	-	0.00	-	0.00	5	4.39
Q3 - 2003	-	0.00	2	4.44	2	12.50	-	0.00	-	0.00	4	3.51
Q4 - 2003	-	0.00	2	4.44	-	0.00	-	0.00	-	0.00	2	1.75
Total	16	100.00%	45	100.00%	16	100.00%	14	100.00%	23	20.75%	114	100.00%
Percentage of Total	14.04%		39.47%		14.04%		12.28%		20.75%		100.00%	

The table below indicates that the Advisories are the most common type of Other NIPC Information. This is followed in rank order by Press Releases, Alerts, Assessments, and Information Highlights. For each category it is noteworthy that the first occurrence of such information is as follows: Alerts in Q2 – 2000, Advisories in Q1 – 2000, Assessments in Q2 – 2000, Information Highlights in Q1 2001 and Press Releases in Q1 – 2000.

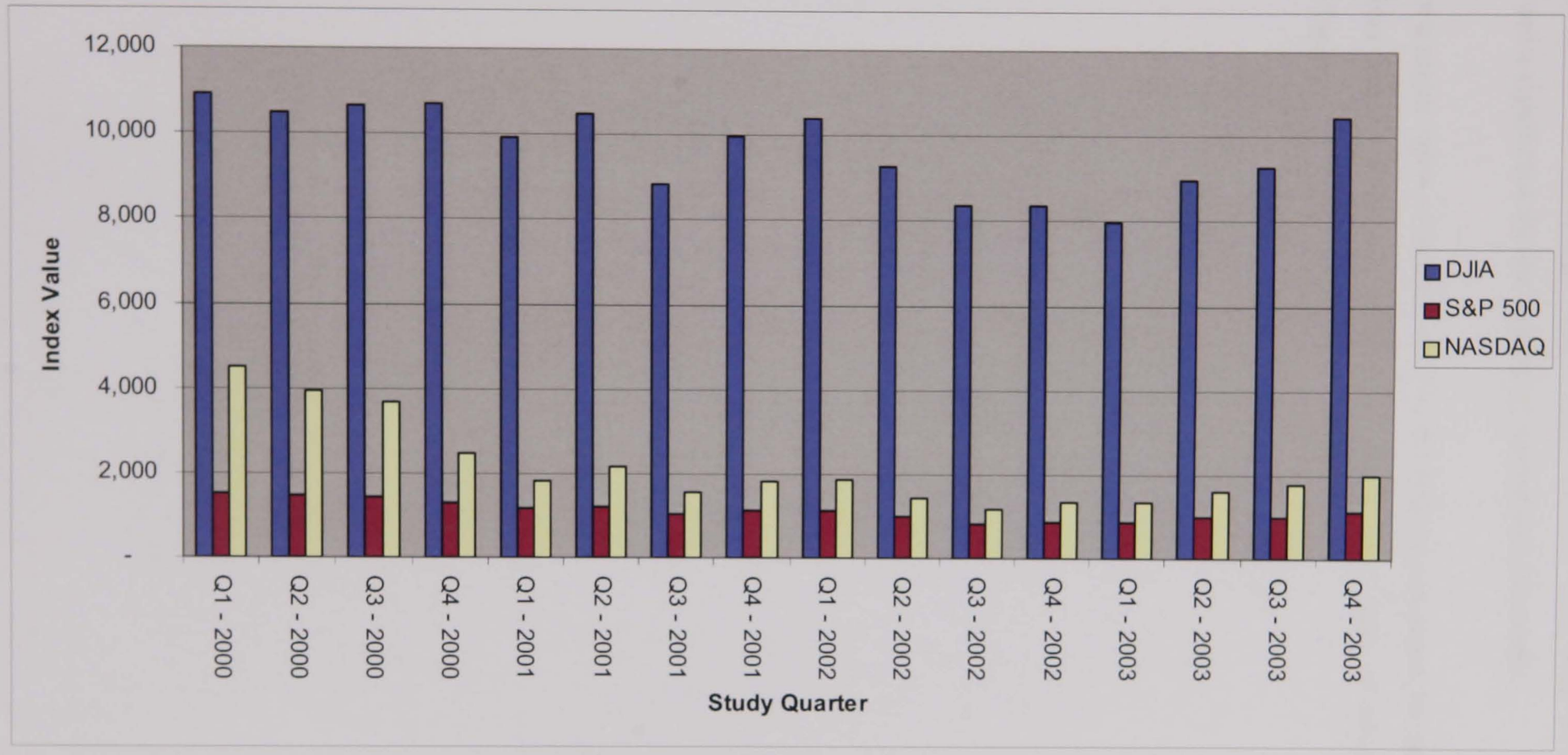
4.8.3 Macro-Economic Data

Macro-economic data has been obtained from U.S. government databases to test specific research questions previously stated in Chapter Three. This information is further broken down into five sub-categories:

1. Stock market indices;
2. Interest rates;
3. Inflation rates and consumer pricing;
4. Unemployment; and
5. Gross domestic product.

The following sub-sections present analyses of each of the individual categories detailed above.

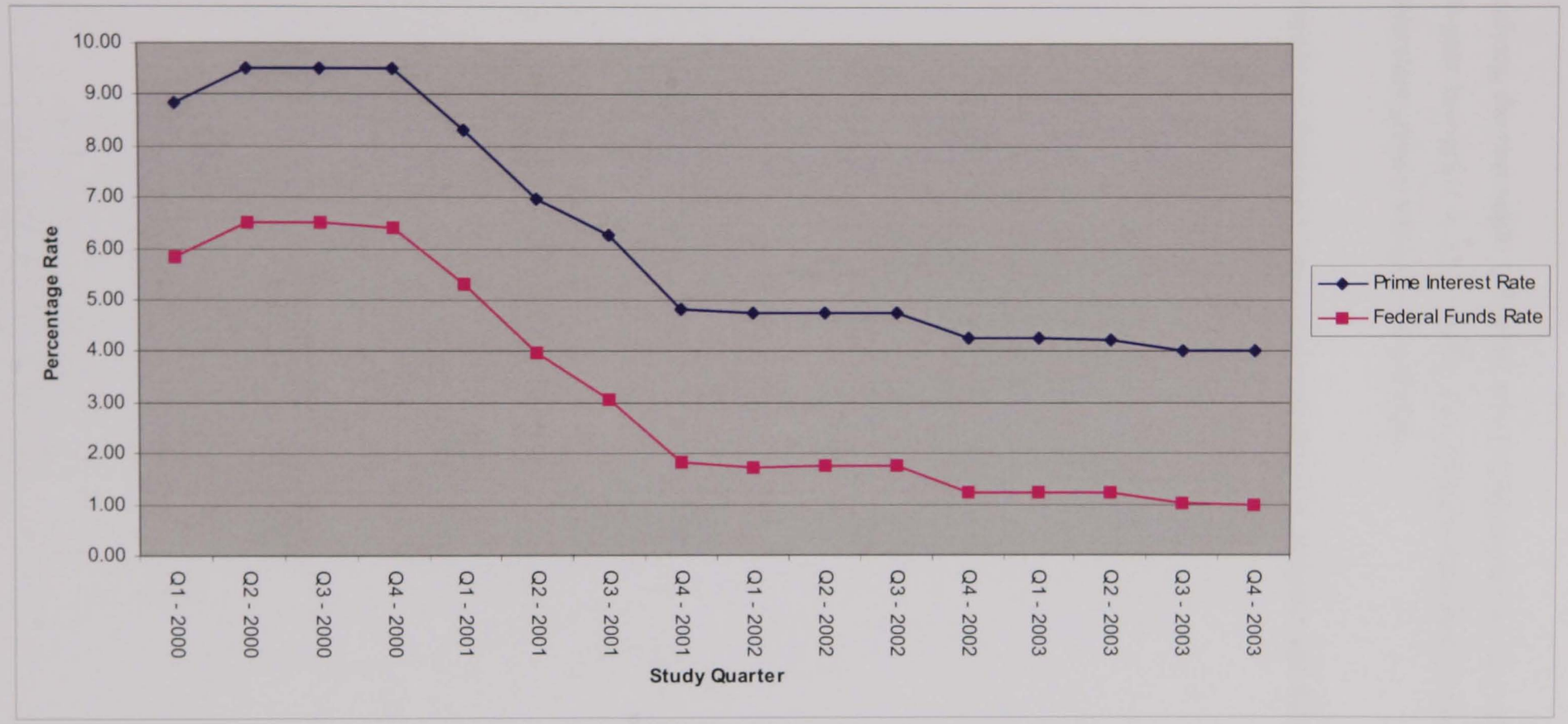
Figure 4.12 – Major U.S. Stock Market Indexes by Quarter: 2000-2003



This information shows the rising value of the NASDAQ Composite Index from Q1 – 2000 to Q3 – 2000 and a significant decline beginning immediately thereafter.

There are two major types of interest rates in the field of consumer finance in the USA. These are the Prime Interest Rate and the Federal Funds Rate; both of which are plotted on the subsequent figure.

Figure 4.13 – Major U.S. Interest Rate Percentages by Quarter: 2000-2003



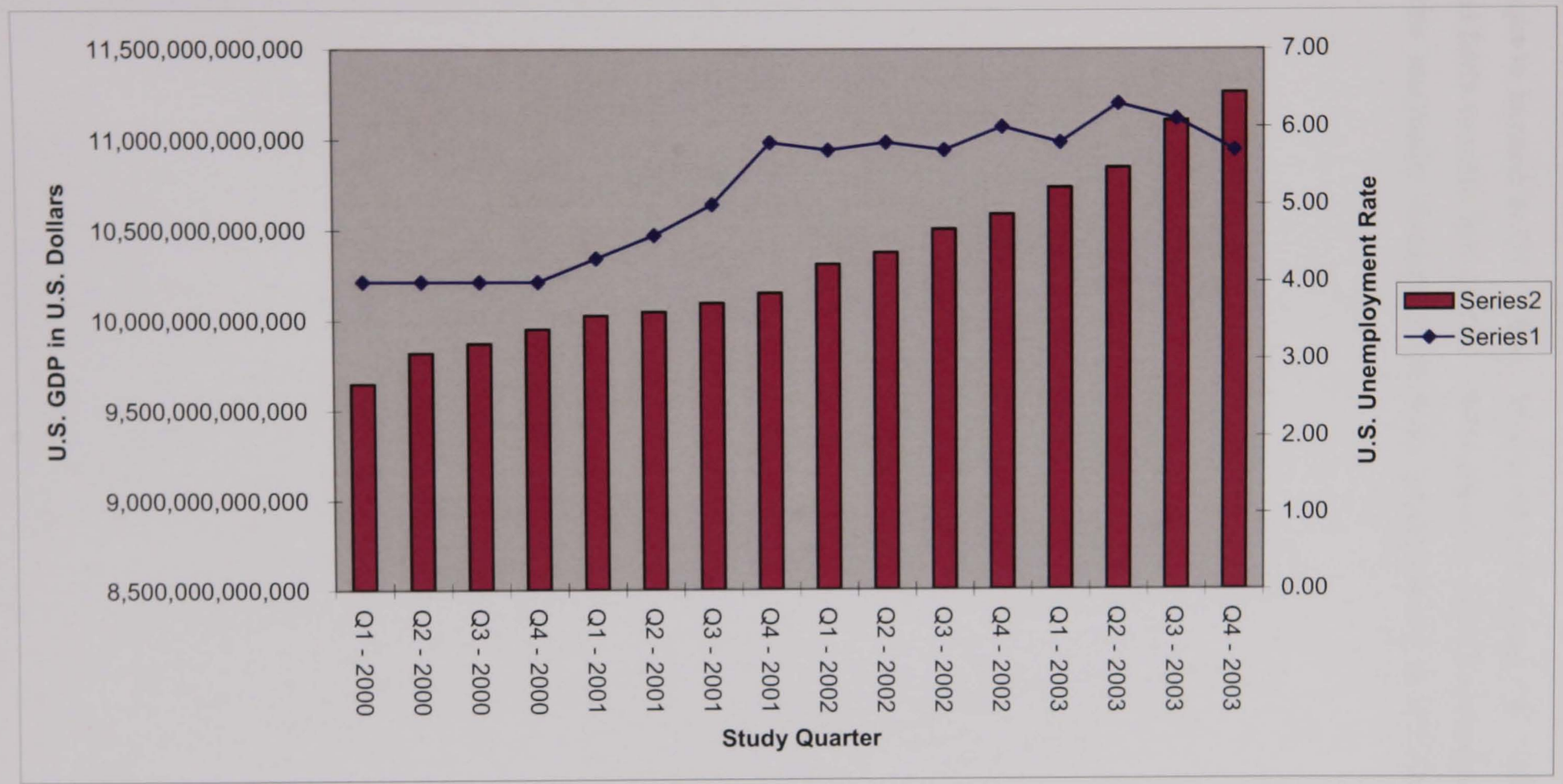
From this analysis, the two major U.S. interest rates declined over the study period. In fact, they reached a 40-year low point in Q4 – 2003; this measure was part of the President's economic package to stimulate growth and hold off inflation.

The next category of macro-economic data incorporates Inflation and the Consumer Price Index (CPI).

Figure 4.14 – U.S. Inflation Rate and Consumer Price Index by Quarter: 2000-2003

From the analysis above, the researcher is able to make two major observations. First, the inflation rate declined significantly from Q1 –2000 (at nearly 4%) to just above 1% in Q1 – 2002. Only then to rise throughout 2002 and then decline once again in 2003. Second, the CPI rose marginally throughout the study period with a total increase of approximately ten percent.

Figure 4.15 – U.S. GDP and Unemployment by Quarter: 2000-2003

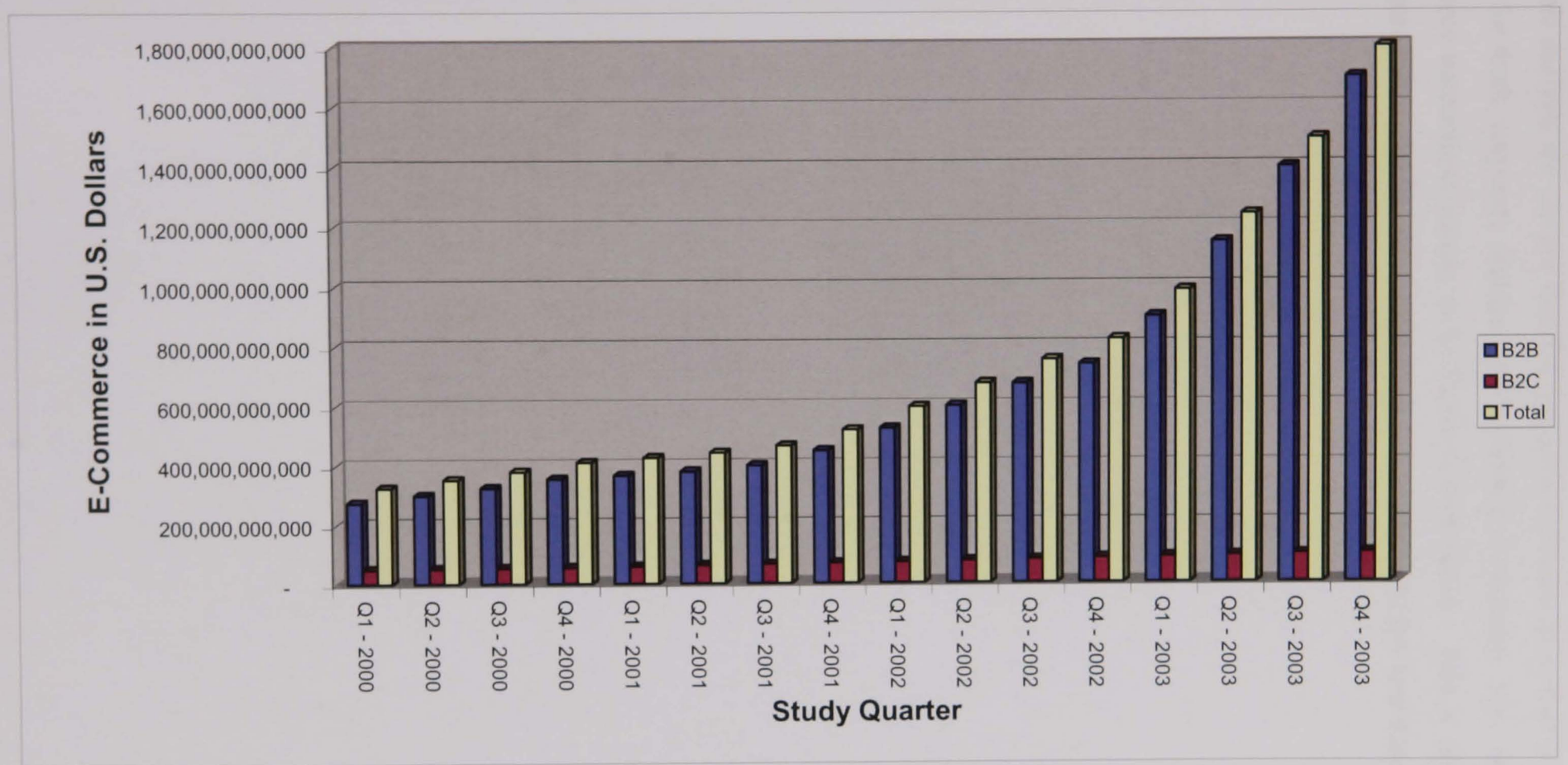


As we can see from the above figure, U.S. GDP remained flat during the first eight quarters and then began to increase in Q1 – 2001. This continued through Q4 – 2001 after which time it remained fairly constant through Q4 – 2003 subject to minor fluctuations. The Unemployment Rate grew marginally throughout the study period closing at 6.375% at the end of 2003.

4.8.4 E-Commerce Data

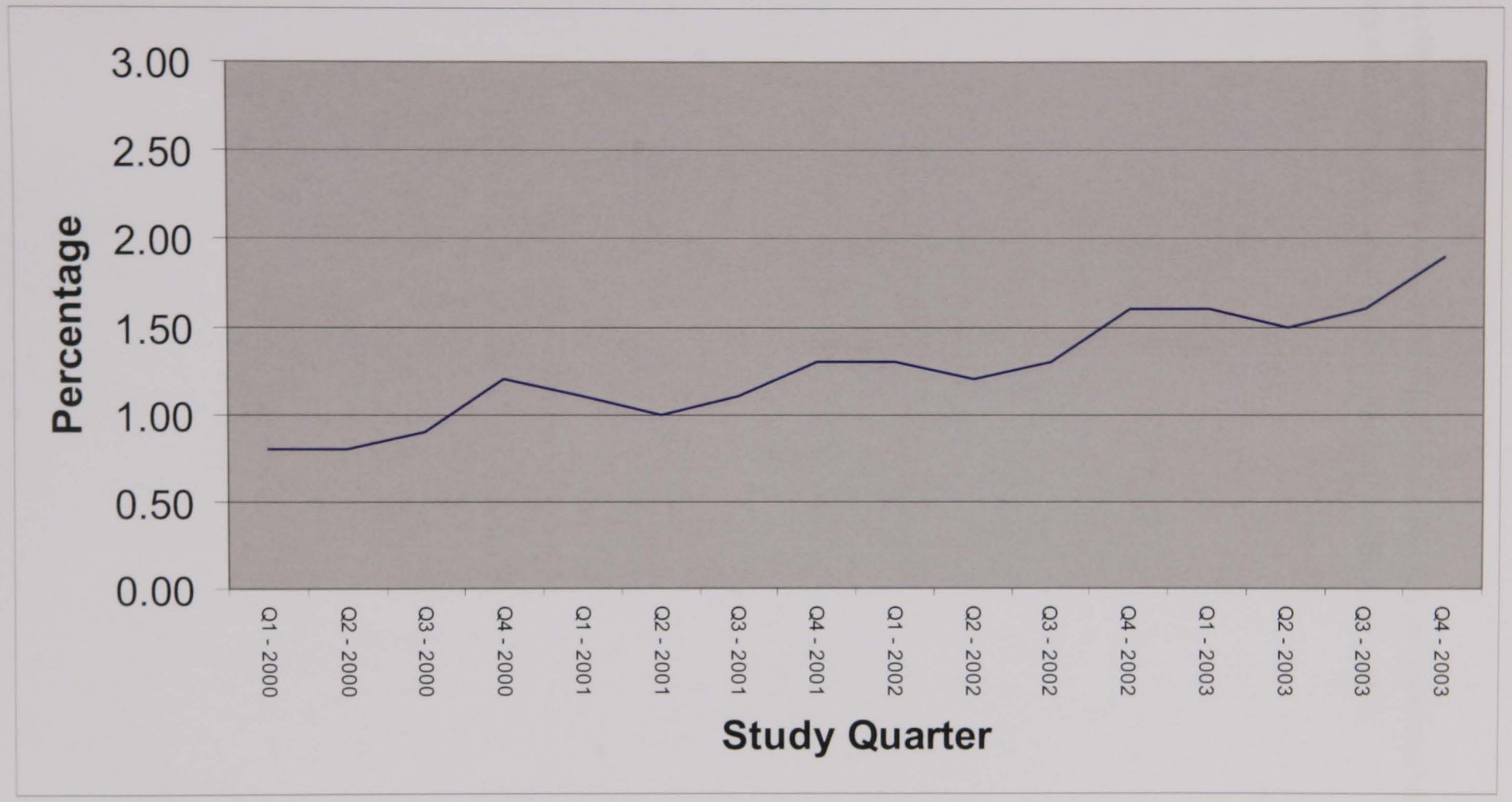
E-commerce has changed the way businesses and individuals do business in the last part of the 20th century. Today, we continue to see new consumer and business buying habits, many of which are greatly influenced by the technological tools and systems that emerge. This section provides information about the E-Commerce data.

Figure 4.16 – United States E-Commerce Figures by Quarter: 2000-2003



From this analysis we can see that E-Commerce continues to evolve as an acceptable business model for both corporate entities and individual consumers. Yet, the vast majority of E-Commerce transactions remain to be Business-to-Business. This is further emphasised in the next figure that shows the percentage of sales attributable to E-Commerce during 2000-2003.

Figure 4.17 – U.S. E-Commerce as a Percent of Total Sales by Quarter: 2000-2003



Based on the analysis above we can see that E-commerce as a percent of total sales in the U.S. is increasing at a steady rate, nearly doubling from Q1 - 2000 to Q4 - 2003.

4.8.5 Information Technology Data

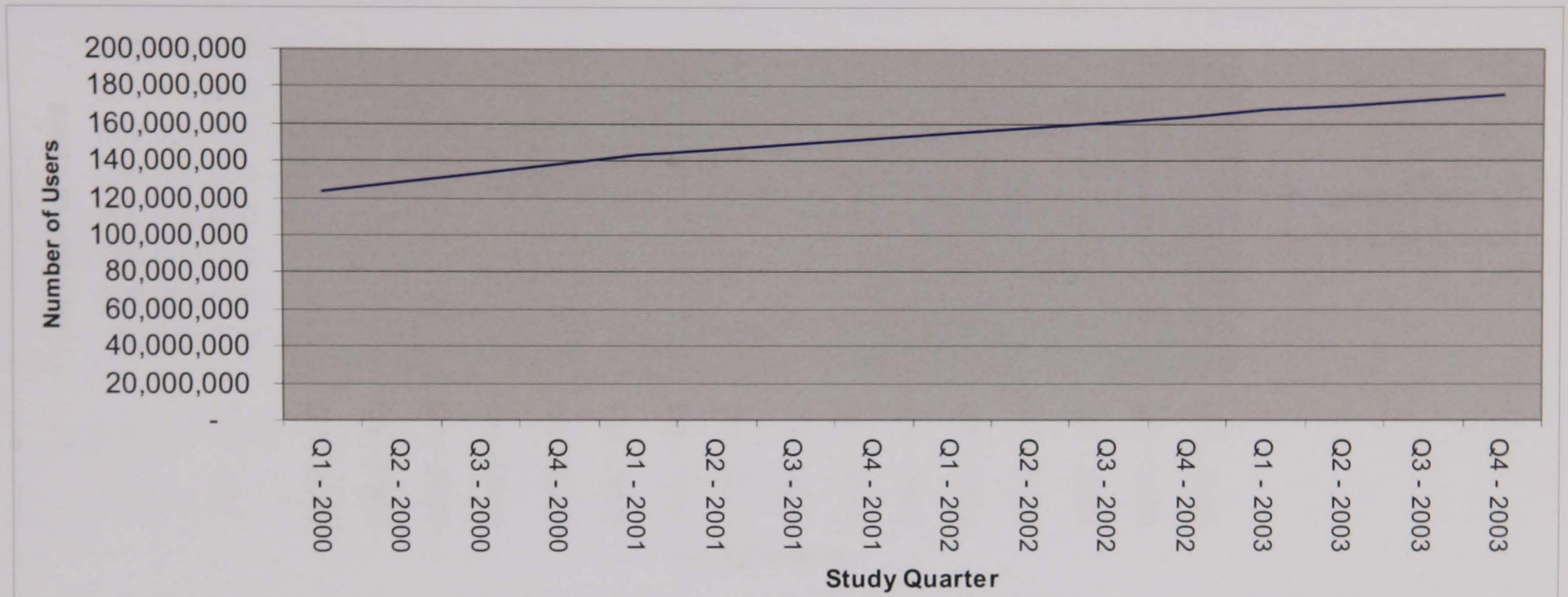
Various types of information technologies are used today in order to access and store data on the Internet. This includes personal computers, telephone lines and mobile devices (i.e. phones and personal digital assistants).

For this section, three sub-categories were established in order to effective organise the research testing:

1. U.S. Internet utilisation;
2. U.S. telephony utilisation; and
3. U.S. host and personal computers

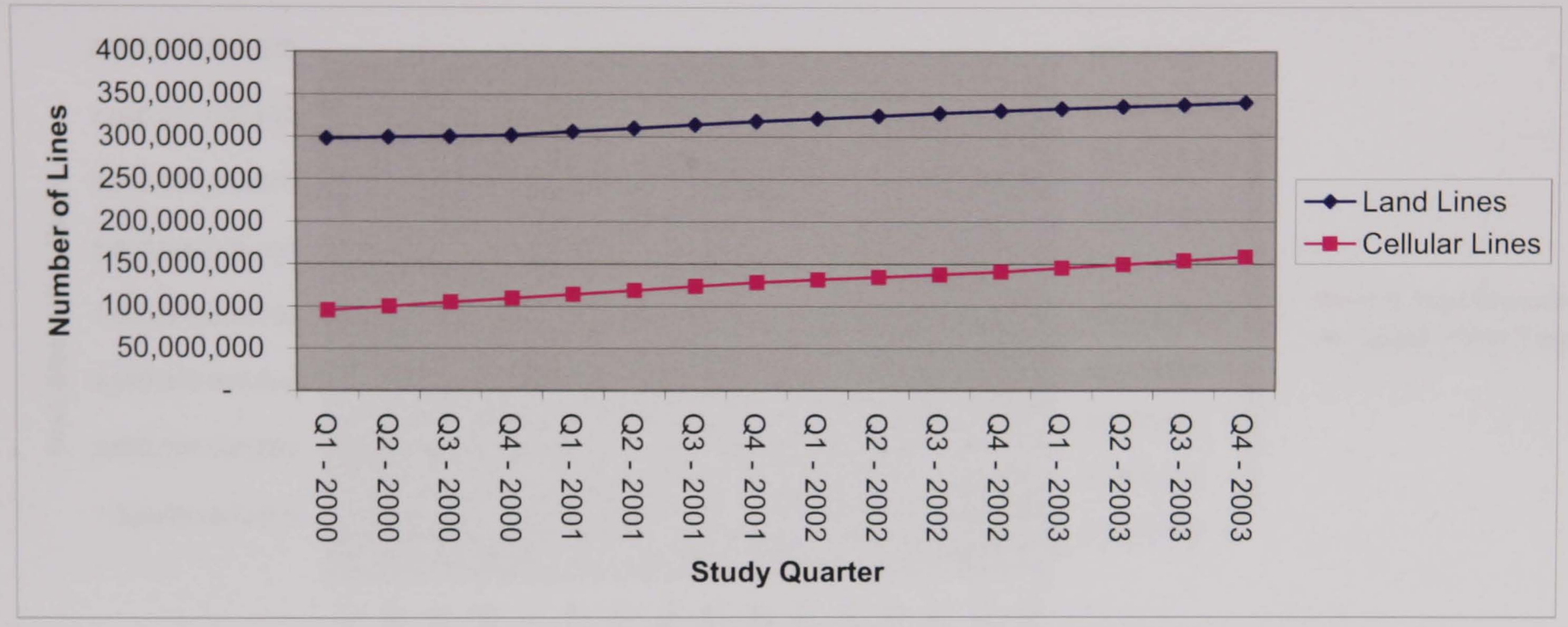
The first sub-category provides utilisation information about U.S. and worldwide Internet usage during the study period. As expected, all related figures point to a growing use of the Internet.

Figure 4.18 – U.S. Internet Utilisation by Quarter: 2000-2003



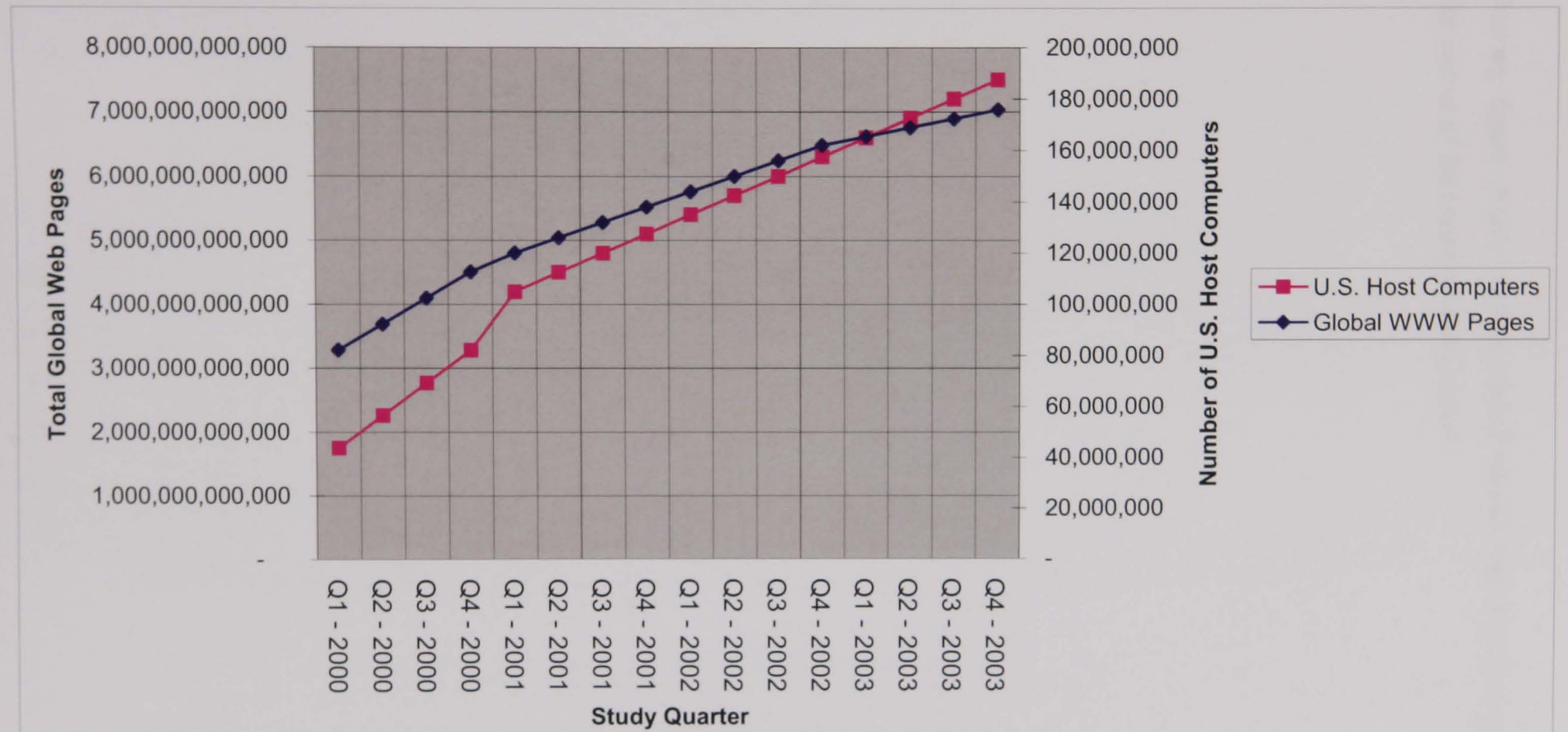
From this analysis, we can see that the number of Internet Users in the U.S. continues to grow throughout the study period. The next figure illustrates the overall use of telephone access in the United States.

Figure 4.19 – U.S. Telephony Utilisation by Quarter: 2000-2003



The figure above shows a relatively equal increase in the utilisation of both land lines and cellular lines during 2000 through 2003.

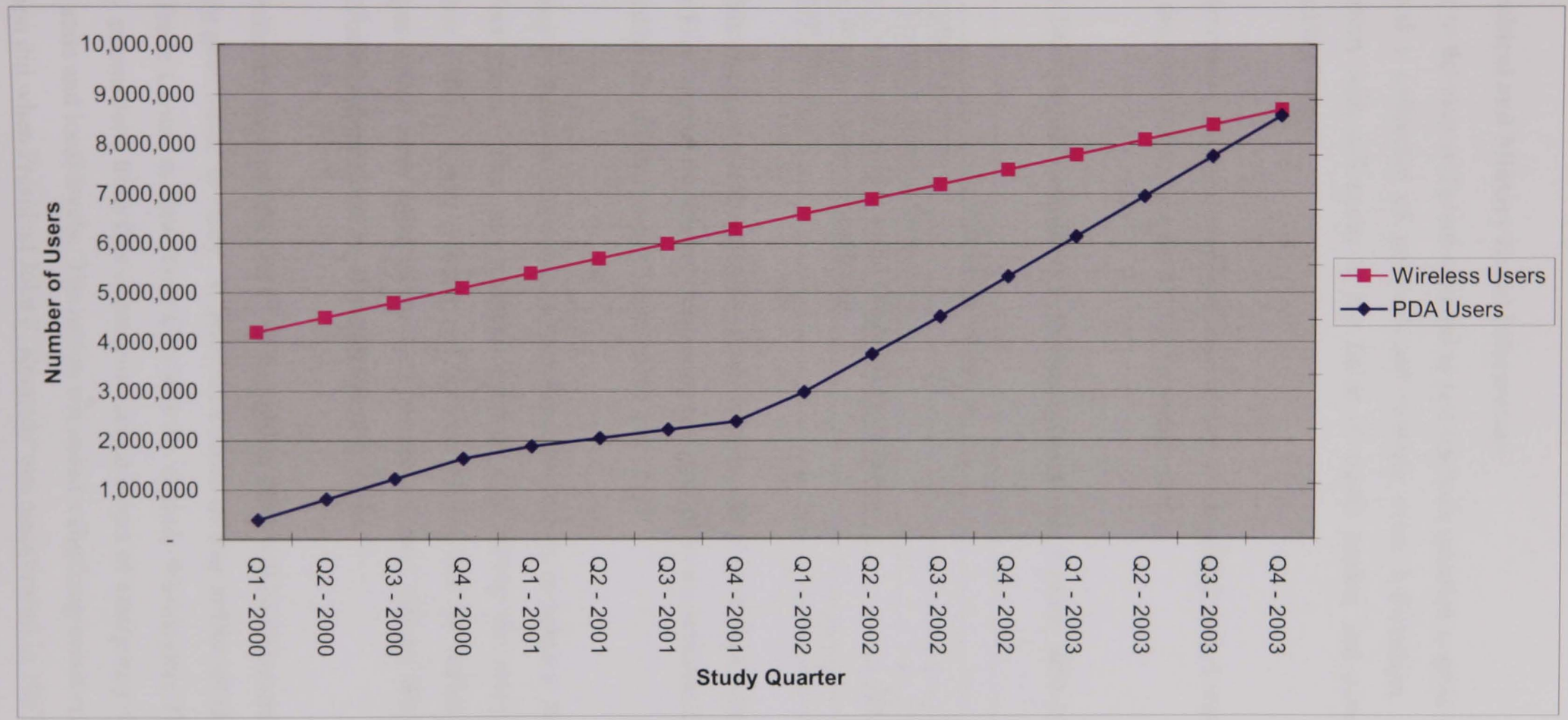
Figure 4.20 – Total Global WWW Pages and U.S. Host Computers by Quarter: 2000-2003



During 2000 through 2003, the number of total global web pages and the number of U.S. Host Computers continued to rise. The most noticeable increase in the number of U.S. Host Computers is between Q4 – 2000 and Q1 – 2001, perhaps this is due to the Millennium Bug.

The following figure details wireless and Personal Digital Assistant (PDA) user frequencies during the course of the research study period.

Figure 4.21 – U.S. Wireless and PDA Users by Quarter: 2000-2003



The above figure provides evidence about two items. First, it shows that users in the U.S. have quickly adopted the use of PDAs since the end of 2001. Second, the same group of consumers have also adopted wireless devices, but at a less dramatic rate of increase. However, the overall increase during the study period is still significant.

4.8.6 Political and Military Event Information

In order to develop sufficient material to test research question number three, the researcher developed a collection of political and military event information. This was done in consultation with colleagues in the fields of media studies and government relations at Towson University.

Quite obviously, the major political and military event of this period was the terrorist attacks against the United States on the 11th of September 2001.

Table 4.20 – Major National U.S. Political Events and Crises: 2000-2003

Brief Description	Time Period
Presidential Election	4 November 2000
Major Terrorist Attacks on the U.S.	11 September 2001
Energy Crisis in California and Other Western States	July thru August 2002
Severe Winter Weather Conditions	January 2003
Northeast Blackout	14 August 2003

While this category is subjective in nature; it nevertheless provides a basis for further study in Chapter Five. All of the related limitations and applicable assumptions have been previously discussed by the researcher in Chapters One and Three.

According to the U.S. Constitution, the electoral process to select a President is held once every four years. The only national election held during the research study was on 4 November 2000. Under scrutiny of various ballots cast in different states, and legal challenges which were taken to the U.S. Supreme Court; George Bush of the Republican Party defeated Albert Gore, Jr. of the Democratic Party.

The historic terrorist attacks on 11th of September 2001 will be discussed in the history books for future generations to study. It involved a series of four airline incidents that targeted the World Trade Centre in New York City and the capitol, Washington, D.C. The nation was severely traumatised from this event and various states of emergency were declared on the federal, state and local levels. The nation witnessed a shocking event, much like the previous generation did when President John F. Kennedy was assassinated in 1967.

The other category of events that was used in this study relates to military events and conflicts. This period of time has been very challenging for the U.S. President, George W. Bush. In particular, the war on terrorism and major, active conflicts in Iraq and Afghanistan have caused considerably heighten fears of additional, major terrorist incidents including biological, nuclear, chemical and information warfare attacks. Table 4.21 below highlights the major U.S. military events and conflicts that occurred during the research study.

Table 4.21 – U.S. Military Events and Conflicts: 2000-2003

Military Event	Time Period
U.S.S. Cole Bombing	12 October 2000
Invasion of Afghanistan	7 October 2001 through 31 December 2003
War on Terrorism – Iraq Conflict	20 March 2003 through 31 December 2003
Liberia Peacekeeping Mission	11 August through 30 September 2003

On 12 October 2000, the U.S.S. Cole battleship was bombed by terrorists while in docked in Yemen. A small, high speed boat loaded with explosives rammed into the side of this ship causing fourteen fatalities and extensive damage. This incident sensitised U.S. military divisions to the need for increased maritime security measures at home and overseas. It also signalled a 'wake-up call' about the global threat of terrorist groups and their sympathisers.

The U.S. led invasion of Afghanistan began in October 2001 to attack the ruling Taliban and to begin a massive manhunt for the leaders of Al Queda, especially Osama bin Laden. This conflict was apparent for some time, but was more pressing due to political fallout after the September 11th terrorist attacks. Today, the U.S. maintains a leadership position in this war theatre where it is assisted by British and other coalition forces.

During this period of time there has been a growing threat portfolio against the U.S. government. This is true for U.S. interests both domestically and internationally. After the September 11th attacks, the world is a markedly changed society. The current U.S. President, George W. Bush, has positioned the U.S. as something akin to a global police force; which has often brought national and international criticism to these events. Also, this position

increases the risks to U.S. military, intelligence, law enforcement and emergency preparedness agencies. They remain at various levels of alert as related information warrants.

According to the U.S. State Department, the government responded to increased international pressure to maintain peace in the African country of Liberia in August of 2003. President Taylor resigned his post and departed into exile in Nigeria. This move paved the way for the deployment by Economic Committee of Western African States (ECOWAS) of what became a 3,600-strong peacekeeping mission in Liberia. Since then, the United States has provided limited direct military support and $26 million in logistical assistance to ECOMIL and another $40 million in humanitarian assistance to Liberia (U.S. State Department, 2003).

4.9 Summary and Conclusion

In this chapter, a detailed analysis has been made of all descriptive statistics for this study. This included analyses of the five categories of primary data included in the CyberNotes newsletters and the four categories of secondary data obtained by the researcher. The summary analysis of each data set included frequency distributions on a yearly and quarterly basis. Additional analyses on both a month and issue level are presented in a series of supplements.

The results of the descriptive statistical analysis indicated that there is sufficient data to develop and test the detailed statistics in Chapter Five. These various descriptive analyses have provided a variety of interesting observations. First, is the overall increasing trend within each category of the CyberNotes. Second, within each of these groups a variety of generalisations as to the: frequency, types, names, risk levels, reporting sources, dates and other information has been highlighted. Third, the secondary data set showed a variety of general economic and IT trends, as well as a summary of the key U.S. political and military events from January 2000 through December 2003.

In Chapter Five, the above findings will be elaborated upon in order to completely test each of the hypotheses developed in the Chapter Three. This will allow the researcher to make specific testing of the quantitative analysis that was described in this chapter. After which the researcher will be able to provide some conclusions about the research project.

Chapter Five - Hypothesis Testing

5.1 An Introduction

This section builds on the descriptive statistical analysis presented in Chapter Four. It begins with a detailed analysis of the research findings which are then be described in detail in order to statistically validate the research questions developed specifically for this project.

This section discusses the parametric and non-parametric tests performed by the researcher to identify, explore and analyse the potential linear relationships between the five primary variables (e.g. included as categories) in the CyberNotes: 1) Bugs, 2) Viruses, 3) Trojans, 4) Exploit Scripts, and 5) Probes/Scans and a variety of secondary variables from non-CyberNotes sources.

All of this work was necessary in order to perform the hypothesis testing outlined in an earlier chapter. Some of these variables include: general computer bugs from NIST and CERT/CC and computer viruses found in the wild (e.g. public domain). Additional variables included items for: Internet utilisation, electronic commerce, CPI, GDP and other macro-economic factors.

Finally, for the military and political events that occurred during the study period this information was obtained from various sources. These major events were discussed previously in an Chapters Two and Four.

5.2 Statistical Tests Performed

In order to conduct detailed statistical testing the researcher conformed to the assumptions outlined in Chapter Three. Specifically, these are: (1) the primary data is accurate since it comes from a large U.S. government agency with a vested interest in supporting the research study; (2) secondary data was similarly accurate since these sources were from other U.S. government agencies and well-respected organisations, and (3) the primary data set represents a complete census evaluation for the study period.

The first major area of testing involved correlation coefficients. The **Pearson Correlation Coefficients**, a well known and highly accepted parametric test and the **Spearman Rank Correlation Coefficients** which is a standard non-parametric test were the basic tools for evaluating seven of the nine hypotheses. Specifically, this testing was performed on Hypotheses One through Seven; which, in turn allowed the researcher to explore potential linear relationships between various variables. Throughout this phase of the hypothesis testing, a five percent significance level (e.g. Type I Error Rate) was used consistently as the statistical premise throughout the study. These tests were made using the SAS© and SPSS© software packages; Version 9 and 13 respectively.

The second major testing area involved an event window analysis. This series of testing was carried out on Hypotheses Eight and Nine, and was done using the popular MS-Excel© software package and its standard mathematical formulas/functions. Specifically, these parameters included the:

1) Mean;
2) Variance;
3) Standard Deviation;
4) Minimum; and
5) Maximum.

It is critical to re-state that this exploratory research project involves a complete four year (e.g. 2000 through 2003) population of NIPC data. Most importantly, this approach allowed for a complete census testing from which absolute mathematical figures were calculated.

Finally, these tests were performed on Hypothesis Eight and Nine using a standard event window methodology. For one time events, the event window is defined as the month of the event plus and minus one month. This was necessary for two significant reasons. First, the inclusion of the preceding month was necessary in order to properly account for any information leakage related to the event. Second, the subsequent month was included to capture any lag in reaction time. Additionally, for those events that were ongoing during the study period the data in its totality is presented.

5.3 Hypothesis Testing

This section outlines the nine specific hypotheses that were tested. Furthermore, this section presents the individual hypotheses, detailed testing analysis of each hypothesis and respective conclusions. The level of hypothesis testing conforms to the overall approach that the researcher outlined and received approval for this project.

H1: There is a defined correlation between the new 'critical' software bugs detailed in the NIPC's CyberNotes newsletters and the general number of new software bugs identified by the U.S. Computer Emergency Response Team/Coordination Centre (CERT/CC) and the U.S. National Institute of Standards and Technology (NIST).

Table 5.1 – Software Bugs Correlation Analysis

Panel A: Pearson Correlation Coefficients (N=48)

	CERT/CC BUGS	NIST BUGS
BUGS	0.2499 p = 0.0868	0.0685 p = 0.6435

Panel B: Spearman Rank Correlation Coefficients (N=48)

	CERT/CC BUGS	NIST BUGS
BUGS	0.3222 p = 0.0256	0.0314 p = 0.8320

In the Pearson Correlation and Spearman Rank Correlation coefficients, it is observed that the critical software bugs information communicated by the National Infrastructure Protection Centre is weakly and positively correlated to the general software bug information published by the CERT/CC. While neither of the relationships are statistically significant, only the correlation between the CERT bugs variable is approaching significance p = 0.0868 for the

Pearson Correlation Coefficient and p = 0.0256 for the Spearman Rank Correlation Coefficient. These results suggested a need for further testing.

Therefore, the researcher executed a Shapiro Wilk Goodness of Fit Test to test the normalcy of the data. The result of this test was a w = 0.9397 and a p-value = 0.0157 which signifies that the data is not normally distributed. Therefore, the non-parametric test (e.g. Spearman) is most relevant, and it is concluded that there is no association with the NIST software bugs.

In summary, the results of the first hypothesis are that the new 'critical' software bugs are correlated to the CERT/CC Bugs and there is no association of these same bugs to the NIST software bugs.

H2: There is a defined correlation between the number of critical computer viruses detailed in the NIPC's CyberNotes newsletters and the general number of computer viruses found 'in the wild'.

Table 5.2 – Computer Viruses Correlation Analysis

Panel A: Pearson Correlation Coefficients (N=48)

	VIRUSES IN THE WILD
VIRUSES	0.1082 p = 0.4643

Panel B: Spearman Rank Correlation Coefficients (N=48)

	VIRUSES IN THE WILD
VIRUSES	0.0549 p = 0.7108

For this correlation, no linear relationship is observed. This is counter-intuitive to the researcher's practical experience it is noted that both statistical tests indicated that these relationships are not statistically significant. While this test looked to associate the general population of computer viruses with the critical viruses reported by the NIPC, the hypothesis must be rejected.

From the testing of the first two hypotheses, a reflection can be made on the critical reports of software bugs and computer viruses. Firstly, there is generally a weak, positive correlation between the new critical software bugs reported by the NIPC and the general software bugs reported by CERT/CC. Secondly, there is no relationship between the NIPC's new critical software bugs and NIST's general software bugs. Thirdly, the NIPC's reporting of critical computer viruses is not related to the general population of computer viruses.

H3: There is a positive correlation between the total number of U.S. Internet users and the critical cyber security infrastructure information reported by the NIPC.

Table 5.3 – U.S. Internet Users Correlation Analysis

Panel A: Pearson Correlation Coefficients (N=48)

	U.S. INTERNET USERS	U.S. RESIDENTS ONLINE
BUGS	0.7798 p = <.0001	0.8134 p = <.0001
VIRUSES	0.6426 p = <.0001	0.6406 p = <.0001
EXPLOITS	-0.3539 p = 0.0136	-0.2441 p = 0.0945
TROJANS	0.7332 p = <.0001	0.7813 p = <.0001
PROBESSCANS	-0.8596 p = <.0001	-0.8032 p =<.0001

Panel B: Spearman Rank Correlation Coefficients (N=48)

	U.S. INTERNET USERS	U.S. RESIDENTS ONLINE
BUGS	0.8322 p = <.0001	0.8322 p = <.0001
VIRUSES	0.70566 p = <.0001	0.70566 P = <.0001
EXPLOITS	-0.19230 p = 0.1904	-0.19230 p = 0.1904
TROJANS	0.75894 p = <.0001	0.75894 p = <.0001
PROBESSCANS	-0.92735 p = <.0001	-0.92735 p = <.0001

These secondary variables were obtained from two different sources as a means of variation. Specifically, the U.S. Internet Users figure is based on OECD reporting and the U.S. Residents Online figure is based on U.S. Department of Commerce statistics. When analysing the relationship between U.S. Internet Users and the number of U.S. Residents Online there is a variety of interesting observations that can be made. First, there is a strong,

positive relationship between both of these variables and the critical software bugs, viruses, and Trojans. For all three of these variables, the statistical significance is very strong.

Second, the Exploit Scripts appear to be negatively correlated to the number of U.S. Internet Users and U.S. Residents Online. However, there are mixed results with the non-parametric and parametric tests performed. To further evaluate the potential correlation a Shapiro Wilk Goodness of Fit Test was performed. The results of this test were: a w = 0.9029 and p-value = 0.0008. Therefore, the dispersion of the data appears to be highly abnormal and it must be concluded that the relationship cannot be relied upon.

Third, the Probes/Scans variable has a very strong, negative correlation with the number of U.S. Internet Users and U.S. Residents Online. Both tests indicate that this correlation is very statistically significant with a p-value = <.0001.

In summary, Hypothesis Three is partially accepted by the researcher with the exception of Exploits. This data element has produced an intriguing set of interpretations and will be discussed later in this chapter as a potential area for future research. Nevertheless, there are a variety of implications of the results thus far. First, the more the Internet is used by individuals the greater the growth of various types of computer malware. Perhaps this is simply explained as a rudimentary method of network centric warfare where malevolent parties see the rich opportunities on the Information Superhighway. Another major implication is the need for users to increase their protective internal controls while they increase their use and reliance on Internet technologies. Individually and as a collective group of computer software applications: anti-virus, anti-spyware, anti-phising, patch management, automatic updates and other user tools are increasingly important.

Hypothesis Four expands the testing to looks at a similar type of potential relationship between the NIPC primary data variables and a key U.S. Internet hardware statistic. In this case, the variable of U.S. host computers is used to perform similar correlation testing.

H4: There is a positive correlation between the number of U.S. based Internet host computers and the cyber security critical infrastructure information reported by the NIPC.

Table 5.4 – U.S. Based Internet Host Computers Correlation Analysis

Panel A: Pearson Correlation Coefficients (N=48)

	U.S. BASED INTERNET HOST COMPUTERS
BUGS	0.7742 p = <.0001
VIRUSES	0.6452 p = <.0001
EXPLOITS	-0.3766 p = 0.0083
TROJANS	0.7013 p = <.0001
PROBESSCANS	-0.8682 p = <.0001

Panel B: Spearman Rank Correlation Coefficients (N=48)

	U.S. BASED INTERNET HOST COMPUTERS
BUGS	0.8322 p = <.0001
VIRUSES	0.7057 p = <.0001
EXPLOITS	-0.1923 p = 0.1904
TROJANS	0.7589 p = <.0001
PROBESSCANS	-0.9274 p = <.0001

The number of U.S. based Internet host computers is found to have a strong, positive correlation with the NIPC's reporting of critical Bugs, Viruses and Trojans. Additionally,

there is a strong, negative correlation between the U.S. based Internet host computers and the Probes/Scans. For Exploit Scripts, there is no relationship.

These results are similar to the researcher's findings for Hypothesis Three and the researcher must only partially accept this hypothesis. In terms of implications, this reinforces the presumption that Internet Hosts are a key variable when measuring Internet growth. Furthermore, this growth can be viewed as an expansion of the electronic battlefield for a variety of organised criminal and terrorist activities such as SPAM attacks, phishing schemes and Botnets.

After follow-up discussions with various government security experts, they believe that Exploit Scripts have a lag time to reporting by the NIPC compared to the other types of information. This is because the Exploit Scripts generally take a considerably longer time to develop and execute. For instance, a Software Bug might be easy for an individual to identify because most software is shared with the user community through alpha and beta testing. This is in contrast to Exploit Scripts which are technically more intricate and complex as they look to generate a specific type of attack; often on a specific software/hardware or network configuration.

The next hypothesis, another variable related to Internet utilisation is used to continue the testing of the relationship between cyber security critical infrastructure information and Global World Wide Web Pages.

H5: There is a positive correlation between the number of global World Wide Web (WWW) pages and the cyber security critical infrastructure information reported by the NIPC.

Table 5.5 – Global World Wide Web Pages Correlation Analysis

Panel A: Pearson Correlation Coefficients (N=48)

	GLOBAL WWW PAGES
BUGS	0.7624 p = <.0001
VIRUSES	0.6335 p = <.0001
EXPLOITS	-0.3849 p = 0.0069
TROJANS	0.7203 p = <.0001
PROBESSCANS	-0.8735 p = <.0001

Panel B: Spearman Rank Correlation Coefficients (N=48)

	GLOBAL WWW PAGES
BUGS	0.8322 p = <.0001
VIRUSES	0.7057 p = <.0001
EXPLOITS	-0.1923 p = 0.1904
TROJANS	0.7589 p = <.0001
PROBESSCANS	-0.9274 p = <.0001

Through the relationship between the Global WWW Pages and the NIPC critical security information there are a number of interesting observations. First, there is a strong, positive relationship between both of these variables and the critical software Bugs, Viruses, and Trojans. The statistical significance for all three of these variables is very strong. Also,

there is no linear relationship between the Exploit Scripts and the number of Global Web Pages. Third, the Probes/Scans variable has a very strong, negative correlation with the number of Global Web Pages. For this testing, both tests indicate that the results are very statistically significant with a p-value = <.0001.

When examining the results of hypotheses three, four and five there is a high degree of concurrence between the NIPC security information and the various Internet utilisation variables. All three of these hypotheses identify the same primary results, as follows:

1. The critical Software Bugs, Viruses and Trojans reported by the NIPC have a very strong, positive and statistically significant correlation with the number of U.S. Internet Users, U.S. Residents Online, U.S. Based Internet Host Computers and Global Web Pages;
2. Probes/Scans reported by the NIPC have a very strong, negative and statistically significant correlation with the number of U.S. Internet Users, U.S. Residents Online, U.S. Based Internet Host Computers and Global WWW Pages; and
3. The Exploit Scripts reported by the NIPC have no relationship with any of these variables.

In summary, Hypothesis Three through Five are partially accepted, subject to the detailed analysis presented above.

H6: There is a positive correlation between the total value of U.S. Electronic Commerce transactions and the cyber security critical infrastructure information reported by the NIPC.

Table 5.6 – U.S. Electronic Commerce Correlation Analysis

Panel A: Pearson Correlation Coefficients (N=48)

	U.S. B2B E-Commerce	U.S. B2C E-Commerce	Total U.S. E-Commerce
BUGS	0.7415 p = <.0001	0.8115 p = <.0001	0.7246 p = <.0001
VIRUSES	0.56230 p = <.0001	0.6346 p = <.0001	0.5471 p = <.0001
EXPLOITS	-0.0427 p = 0.7730	-0.2329 p = 0.1111	-0.0575 p = 0.6977
TROJANS	0.9015 p = <.0001	0.7974 p = <.0001	0.8691 p = <.0001
PROBESSCANS	-0.6242 p = <.0001	-0.7983 p = <.0001	-0.6180 p = <.0001

Panel B: Spearman Rank Correlation Coefficients (N=48)

	U.S. B2B E-Commerce	U.S. B2C E-Commerce	Total U.S. E-Commerce
BUGS	0.8322 p = <.0001	0.8322 p = <.0001	0.8027 p = <.0001
VIRUSES	0.7057 p = <.0001	0.7057 p = <.0001	0.6701 p = <.0001
EXPLOITS	-0.1923 p = 0.1904	-0.1923 p = 0.1904	-0.2010 p = 0.1707
TROJANS	0.7589 p = <.0001	0.7589 p = <.0001	0.7095 p = <.0001
PROBESSCANS	-0.9274 p = <.0001	-0.9274 p = <.0001	-0.9156 p = <.0001

Based on this analysis, both of the statistical tests indicate that the NIPC critical security information for Bugs, Viruses and Trojans is positively correlated with the three categories of U.S. Electronic Commerce transactions during the study period. In fact, this correlation is very statistically significant for all three of these variables. On the contrary, the Exploits have no relationship with any of the three associated variables. The Probes/Scans testing

shows that both of these variables are negatively correlated to the U.S. Electronic Commerce transaction volume values. These relationships are very statistically significant.

Therefore, Hypothesis Six is partially accepted for Software Bugs, Viruses and Trojans. However, it is rejected for Exploits and Probes/Scans.

It is important to address the implications of this correlation. With the growth of E-Commerce comes an increase in the threats of Software Bugs, Computer Viruses, and Trojans. With our reliance on Information Technology we must develop an increased awareness and risk mitigation strategies about these different threats. Additionally, it is logical that modern criminals have found computer crimes to be very profitable with the Internet acting as an attractive platform to launch large scale/high impact criminal activities. This situation appears to be applicable to both individual consumers and business entities. Lastly, additional analyses of E-Commerce information systems and targeted malware attacks will be presented as suggestions for further research.

H7: The NIPC's cyber security information communications is positively associated with various macro-economic factors such as: major interest rates, stock market indices, Consumer Price Index (CPI), Gross Domestic Product (GDP), inflation, and unemployment.

This analysis is divided into two components. Part one contains two key interest rates and three stock market indices, as presented in Table 5.7 below. Part two contains four additional macro-economic variables for which the statistical testing is shown in Table 5.8.

Table 5.7 – U.S. Macro-Economic Factor Correlation Analysis: Part One

Panel A: Pearson Correlation Coefficients (N=48)

	U.S. PRIME INTEREST RATE	U.S. FEDERAL FUNDS RATE	S&P 500	DJIA	NASDAQ
BUGS	-0.7060 p = <.0001	-0.7025 p = <.0001	-0.6676 p = <.0001	-0.5774 p = <.0001	-0.5492 p = <.0001
VIRUSES	-0.5622 p = <.0001	-0.5591 p = <.0001	-0.5826 p = <.0001	-0.4773 p = 0.0006	-0.5261 p = 0.0001
EXPLOITS	0.4220 p = <0.0028	0.4294 p = 0.0023	0.4431 p = 0.0016	0.2494 p = 0.0874	0.5892 p = <.0001
TROJANS	-0.5945 p = <.0001	-0.5933 p = <.0001	-0.4605 p = 0.0010	-0.3099 p = 0.0321	-0.4073 p = 0.0041
PROBESSCANS	0.8379 p = <.0001	0.8407 p = <.0001	0.8490 p = <.0001	0.6305 p = <.0001	0.8887 p = <.0001

Panel B: Spearman Rank Correlation Coefficients (N=48)

	U.S. PRIME INTEREST RATE	U.S. FEDERAL FUNDS RATE	S&P 500	DJIA	NASDAQ
BUGS	-0.7862 p = <.0001	-0.7842 p = <.0001	-0.7227 p = <.0001	-0.6190 p = <.0001	-0.6214 p = <.0001
VIRUSES	-0.6649 p = <.0001	-0.6790 p = <.0001	-0.6254 p = <.0001	-0.4880 p = 0.0004	-0.5666 p = <.0001
EXPLOITS	0.2059 p = 0.1603	0.2163 p = 0.1398	0.2993 p = 0.0388	0.2710 p = 0.0624	0.3877 p = 0.0065
TROJANS	-0.6740 p = <0.0001	-0.6525 p = <.0001	-0.6001 p = <.0001	-0.5366 p = <.0001	-0.4980 p = 0.0003
PROBESSCANS	0.9078 p = <.0001	0.9016 p = <.0001	0.8656 p = <.0001	0.7602 p = <.0001	0.7633 p = <.0001

In this part of the testing, the results are mixed. Bugs, Viruses and Trojans have a strong, negative correlation that is highly statistically significant with the first four macroeconomic factors. Whereas, Exploits have a moderate, positive correlation that has various degrees of significance with the two interest rate variables and three stock market indices. Finally, the critical Probes/Scans have a strong, positive relationship with all interest rate and stock market index variables.

To continue this correlation testing further macroeconomic variable are used to expand this analysis. The second part of this section includes correlation analysis with four popular variables. This is shown in the following table as follows.

Table 5.8 – U.S. Macro-Economic Factor Correlation Analysis: Part Two

Panel A: Pearson Correlation Coefficients (N=48)

	U.S. CPI	U.S. GDP	U.S. INFLATION	U.S. UNEMPLOYMENT
BUGS	0.7809 p = <.0001	0.7932 p = <.0001	-0.4654 p = 0.0009	0.7469 p = <.0001
VIRUSES	0.6355 p = <.0001	0.6388 p = <.0001	-0.4948 p = 0.0003	0.5838 p = <.0001
EXPLOITS	-0.3089 p = 0.0327	-0.1909 p = 0.1937	0.3617 p = 0.0115	-0.3725 p = 0.0091
TROJANS	0.7422 p = <.0001	0.8343 p = <.0001	-0.3235 p = 0.0249	0.5880 p = <.0001
PROBESSCANS	-0.8394 p = <.0001	-0.7636 p = <.0001	0.5487 p = <.0001	-0.8085 p = <.0001

Panel B: Spearman Rank Correlation Coefficients (N=48)

	U.S. CPI	U.S. GDP	U.S. INFLATION	U.S. UNEMPLOYMENT
BUGS	0.8234 p = <.0001	0.8322 p = <.0001	-0.4648 p = 0.0009	0.7893 p = <.0001
VIRUSES	0.7012 p = <.0001	0.7057 p = <.0001	-0.4413 p = 0.0017	0.6241 p = <.0001
EXPLOITS	-0.1841 p = 0.2105	-0.1923 p = 0.1904	0.4325 p = 0.0021	-0.2100 p = 0.1520
TROJANS	0.7733 p = <.0001	0.7589 p = <.0001	-0.3296 p = 0.0222	0.6558 p = <.0001
PROBESSCANS	-0.9201 p = <.0001	-0.9274 p = <.0001	0.6051 p = <.0001	-0.8684 p = <.0001

The table above produced a variety of results. Bugs, Viruses and Trojans have a strong, positive correlation that is highly statistically significant with the U.S. Consumer Price Index. Gross Domestic Product, Inflation, and Unemployment variables. Exploits have no relationship with GDP. But the correlation with CPI, Inflation and Unemployment is negative and strong. Probes/Scans have a strong, positive relationship with the U.S. Inflation

Rate. However, this same variable has a strong, negative relationship with CPI, GDP and Unemployment.

In conclusion, Hypothesis Seven can only be partially accepted due to the positive correlation with most macroeconomic variables and Bugs, Viruses and Trojans. Exploit Scripts have mixed results, as does Probes/Scans. In terms of impact, this analysis demonstrates that the two most prevalent types of computer malware (e.g. Viruses and Trojans) are associated with changes in macroeconomic factors. Therefore, these factors should be considered in building predictive models in Information Assurance and Security. The other factors would be useful in considering for further research in the future.

The following table was developed in order to summarise the main correlation observations from Hypotheses Three through Seven.

Table 5.9 – Summary of Testing Results for Hypothesis Three through Seven: Spearman Rank Correlation Coefficients

Hypothesis/Dependent Variable	BUGS	VIRUSES	EXPLOITS	TROJANS	PROBES/SCANS	FINAL DISPOSITION
Number Three						
U.S. Internet Users	0.8322 p = <.0001	0.7057 p = <.0001	-0.1923 p = 0.1904	0.7589 p = <.0001	-0.9274 p = <.0001	Partially Accept
U.S. Residents Online	0.8134 p = <.0001	0.7057 p = <.0001	-0.1923 p = 0.1904	0.7589 p = <.0001	-0.92734 p = <.0001	Partially Accept
Number Four						
U.S. Based Internet Host Computers	0.8322 p = <.0001	0.7057 p = <.0001	-0.1923 p =0.1904	0.7589 p = <.0001	-0.9274 p = <.0001	Partially Accept
Number Five						
Global Web Pages	0.8322 p = <.0001	0.7057 p = <.0001	-0.1923 p = <.0001	0.7589 p = <.0001	-0.9274 p = <.0001	Partially Accept
Number Six						
U.S. B2B E-Commerce	0.8322 p = <.0001	0.7057 p = <.0001	-0.1923 p = <.0001	0.7589 p = <.0001	-0.9274 p = <.0001	Partially Accept
U.S. B2C E-Commerce	0.8322 p = <.0001	0.7057 p = <.0001	-0.1923 p = <.0001	0.7589 p = <.0001	-0.9274 p = <.0001	Partially Accept
U.S. Total E-Commerce	0.8207 p = <.0001	0.6701 p = <.0001	-0.2010 p = 0.1707	0.7095 p = <.0001	-0.9156 p = <.0001	Partially Accept
Number Seven						
U.S. Prime Interest Rate	-0.7862 p = <.0001	-0.6649 p = <.0001	0.2059 p = 0.1603	-0.6740 p = <.0001	0.9078 p = <.0001	Partially Accept
U.S. Federal Funds Interest Rate	-0.7842 p = <.0001	-0.6790 p = <.0001	0.2163 p = 0.1398	-0.6525 p = <.0001	0.9016 p = <.0001	Partially Accept
S&P 500	-0.7227 p = <.0001	-0.6254 p = <.0001	0.2993 p = 0.0388	-0.6001 p = <.0001	0.8656 p = <.0001	Partially Accept
Dow Jones Industrial Average	-0.6190 p = <.0001	-0.4880 p = 0.0004	0.2710 p = 0.0624	-0.5366 p = <.0001	0.7602 p = <.0001	Partially Accept
NASDAQ	-0.6214 p = <.0001	-0.5666 p = <.0001	0.3877 p = 0.0065	-0.4980 p = 0.0003	0.7633 p = <.0001	Partially Accept
U.S. Consumer Price Index	0.8234 p = <.0001	0.7012 p = <.0001	-0.1841 p = 0.2105	0.7733 p = <.0001	-0.9201 p = <.0001	Partially Accept

Hypothesis/Dependent Variable	BUGS	VIRUSES	EXPLOITS	TROJANS	PROBES/SCANS	FINAL DISPOSITION
Number Three						
U.S. Gross Domestic Product	0.8322 p = <.0001	0.7057 p = <.0001	-0.1923 p = 0.1904	0.7589 p = <.0001	-0.9274 p = <.0001	Partially Accept
U.S. Inflation Rate	-0.4648 p = 0.0009	-0.4413 p = 0.0017	0.4325 p = 0.0021	-0.3296 p = 0.0222	0.6501 p = <.0001	Partially Accept
U.S. Unemployment Rate	0.7893 p = <.0001	0.6241 p = <.0001	-0.2100 p = 0.1520	0.6558 p = <.0001	-0.8684 p = <.0001	Partially Accept

H8: There is an increase in the number of critical computer security advisory communications of the NIPC during time periods of military events; specifically 1) the attack on the USS Cole Battleship, 2) the War in Afghanistan, 3) September 11th Terrorist Attacks, 4) U.S. Invasion of Iraq, and 5) U.S. Military Intervention in Liberia.

After careful consideration, it was determined that an event window approach whereby the mean number of the NIPC reported information was reported instances in the event window was compared to the mean number of the NIPC reported information outside of the event window. This research methodology was discussed previously in Chapter Three. However, to re-emphasise some of the most important aspects of this approach it allows a researcher to identify, measure and compare basic statistical measurements before and after the event window. When using this approach two periods of time are segregated: the event window and the non-event window. Furthermore, the month in which the event occurs is included within the event window. For each event, the following parameters were calculated:

1) Mean;
2) Variance;
3) Standard Deviation;
4) Minimum; and
5) Maximum

In addition, some of these events were deemed to be ongoing military campaigns which continued through the entire data period. As such, inclusion for all subsequent months within the study period is made where considered appropriate. Furthermore, this is shown in chronological order within the study period.

The first related military event was a terrorist attack on the USS Cole Battleship in the Port of Eden in Yemen which occurred in October 2000.

Table 5.10 – Statistical Analysis of the USS Cole Battleship Attack

	Total Bugs		Total Viruses		Total Exploits		Total Trojans		Total Probes/Scans	
Parameter	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW
N	45	3	45	3	45	3	45	3	45	3
Mean	142.58	94.00	51.20	42.33	63.00	68.33	327.96	137.33	3.67	9.67
Variance	3,835.09	100.67	426.20	13.56	883.20	38.89	90,344.84	122.89	21.42	16.22
Standard Dev.	61.93	10.03	20.64	3.68	29.72	6.24	300.57	11.09	4.63	4.03
Min	61	85	6	38	21	60	15	129	0	4
Max	366	108	117	47	150	75	1,168	153	17	19

Note: EW denotes the Event Window and N-EW denotes the Non-Event Window

The results for the first military event shown in Table 5.10 above indicates that the Mean values for Bugs, Viruses, and Trojans are greater during the non-event window. For Exploits and Probes/Scans, the Mean values are larger in the event window than it is in the non-event window. For the Standard Deviation parameter, the testing indicates a larger dispersion of all five variables when they are in the non-event window as compared to the event window.

The second military event in this study was the U.S. launched War in Afghanistan. This action was widely expected by global military analysts and politicians this event began in October 2000. The following table presents the event window analysis of this historic event.

Table 5.11 – Statistical Analysis of the War in Afghanistan

	Total Bugs		Total Viruses		Total Exploits		Total Trojans		Total Probes/Scans	
Parameter	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW
N	21	27	21	27	21	27	21	27	21	27
Mean	92.57	176.07	37.86	60.59	74.95	54.30	154.71	441.52	8.05	0.93
Variance	499.48	3,209.77	127.07	359.06	1,081.28	451.62	1,3315.16	10,803.00	22.14	1.85
Standard Dev.	22.35	56.65	11.27	19.87	32.88	21.25	115.39	328.68	4.71	1.36
Min	61	68	6	26	32	21	15	26	2	0
Max	153	366	57	117	150	104	459	1,168	17	5

Note: EW denotes the Event Window and N-EW denotes the Non-Event Window

The results for the second military event indicated that the Mean values for Bugs, Viruses, and Trojans are greater during the event window than they are in the non-event window. For Exploits and Probes/Scans, the Mean value is larger in the non-event window than they are in the event window. Similarly, for the Standard Deviation parameter the testing indicates a larger dispersion amongst the Bugs, Viruses and Trojans during the event window than the during the non-event window. Conversely, the SD has a larger dispersion for the Exploit Scripts and Probes/Scans during the non-event window that what is noted during the event window time period.

The terrorist attacks of 11th September 2001 were an event that shocked the United States and other nations around the world. This major catastrophe was perpetrated by eleven Islamic Extremists supported by Al-Qaeda. This event changed the face of America and forced President Bush to embark on a War on Terrorism. For the fourth military event in this research study, the parameters are presented in the table below.

Table 5.12 – Statistical Analysis of the September 11, 2001 Terrorist Attacks on the U.S.

	Total Bugs		Total Viruses		Total Exploits		Total Trojans		Total Probes/Scans	
Parameter	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW
N	45	3	45	3	45	3	45	3	45	3
Mean	143.42	81.33	52.02	30	65.33	33.33	313.40	355.67	4.09	3.33
Variance	3,743.89	66.89	400.33	20.67	816.00	113.56	92,493.48	284.22	24.66	0.89
Standard Dev.	61.19	8.18	20.01	4.55	28.57	10.66	304.13	16.86	4.97	0.94
Min	61	70	6	25	21	21	15	332	0	2
Max	366	89	117	36	150	47	1,168	370	17	4

Note: EW denotes the Event Window and N-EW denotes the Non-Event Window

The results for the third military study event shown in the above table, demonstrate that the Mean values for Bugs, Viruses, Exploits and Probes/Scans are greater in the non-event window than they are in the event window. For Trojans, the Mean value is larger in the event window than it is in the non-event window. Similarly, for the Standard Deviation parameter the testing indicates a larger dispersion amongst all study variables during the non-event window.

One of the more controversial military conflicts of our lifetime is the United States invasion of Iraq in order to overthrow the regime of Saddam Hussein The fourth military event was the U.S. Invasion of Iraq in order to overthrow Saddam Hussein's dictatorship. Various military and news commentators expected after various United Nations hearings. It formally began in April 2003 and remains on-going at the current time. This action has been organised and led by the U.S. military force, and contains a small compliment of multinational forces including British soldiers. The parameters surrounding this event are presented in Table 5.13 below.

Table 5.13 – Statistical Analysis of the U.S. Invasion of Iraq

	Total Bugs		Total Viruses		Total Exploits		Total Trojans		Total Probes/Scans	
Parameter	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW
N	38	10	38	10	38	10	38	10	38	10
Mean	118.92	217.9	46.82	65.20	61.42	70.60	193.13	783.10	5.11	0
Variance	1,988.02	2,641.49	347.62	355.56	982.40	194.24	18,010.48	72,818.89	23.88	0
Standard Dev.	44.59	51.40	18.64	18.86	31.34	13.94	134.20	269.85	4.89	0
Min	61	172	6	34	21	54	15	328	0	0
Max	220	366	117	101	150	104	523	1,168	17	0

Note: EW denotes the Event Window and N-EW denotes the Non-Event Window

For the fourth military event shown above there are some interesting results. Specifically, for Bugs all parameters show higher values in the event window. For Viruses and Trojans, the Mean and SD are also higher in the event window. Exploits have a higher Mean value in the event window, but a higher standard deviation in the non-event window time period. Lastly, Probes/Scans have a higher Mean value and SD in the non-event window when compared to the event window.

During August 2003 and at the request of the United Nations, the United States intervened militarily in the country of Liberia on a peacekeeping mission. At this time, Charles Taylor, the previous President of this country was well known for his malevolent leadership. During this event anarchy began to develop and Mr. Taylor was exiled to Nigeria. Table 5.14 presents a summary of the parameters developed for this event.

Table 5.14 – Statistical Analysis of the U.S. Military Intervention in Liberia

	Total Bugs		Total Viruses		Total Exploits		Total Trojans		Total Probes/Scans	
Parameter	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW
N	44	4	44	4	44	4	44	4	44	4
Mean	134.09	199.50	49.18	66.75	62.75	69.75	269.30	841.25	4.41	0
Variance	3,687.58	394.25	404.65	126.19	894.37	102.19	66,454.48	10,101.19	23.70	0
Standard Dev.	60.73	19.86	20.12	11.23	29.91	10.11	257.79	100.50	4.87	0
Min	61	172	6	55	21	54	15	711	0	0
Max	366	228	117	85	150	80	1,168	983	17	0

Note: EW denotes the Event Window and N-EW denotes the Non-Event Window

The results for the fifth military event illustrate higher Mean values for all variables during the event window except for Probes/Scans. The SD for all variables is higher during the non-event window. This is an intriguing analysis since the SD parameter values are inversely related to the Means when excluding the Probes/Scans from this observation.

H9: The number of computer security advisory communications of the NIPC is positively associated with an increase during periods of domestic political change and crisis such as the: U.S. Presidential Election, Western States energy crisis, severe winter weather storms, and Northeast Blackout.

The statistical parameters are measured throughout this section and begin with a presentation of the U.S. Presidential Election which occurred in November 2000. According to U.S. law, presidential elections must be conducted on the first Tuesday in the month of November every four years. Accordingly, a brief statistical analysis is presented below for this domestic political event.

Table 5.15 – Statistical Analysis of the 2000 U.S. Presidential Election

	Total Bugs		Total Viruses		Total Exploits		Total Trojans		Total Probes/Scans	
Parameter	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW
N	45	3	45	3	45	3	45	3	45	3
Mean	142.49	95.33	50.93	46.33	63.24	64.67	327.09	150.33	3.78	8.00
Variance	3,844.25	90.89	429.97	10.89	883.87	53.56	90,655.15	244.22	22.93	10.67
Standard Dev.	62.00	9.53	20.74	3.30	29.73	7.32	301.09	15.63	4.79	3.27
Min	61	85	6	42	21	59	15	130	0	4
Max	366	108	117	50	150	75	1,168	168	17	12

Note: EW denotes the Event Window and N-EW denotes the Non-Event Window

The results for the final political study event shown in Table 5.15 above indicate that the Mean value for Bugs, Viruses, and Trojans are highest in the non-event window. For Exploits and Probes/Scans, the Mean value is higher in the event window. The Standard Deviation and Maximum parameters for all variables signify higher values during the non-event window timeframe.

The Western States Energy Crisis occurred in July 2002 and gained national attention for the country's troubled infrastructures. Table 5.16, presents the corresponding information.

Table 5.16 – Statistical Analysis of the Western States Energy Crisis

	Total Bugs		Total Viruses		Total Exploits		Total Trojans		Total Probes/Scans	
Parameter	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW
N	44	4	44	4	44	4	44	4	44	4
Mean	136.53	172.75	48.25	77.00	63.14	65.50	320.52	266.75	4.25	1.75
Variance	3,873.98	1,062.69	320.73	574.50	880.35	296.25	94,127.16	3,971.69	24.60	2.19
Standard Dev.	62.24	32.60	17.91	23.97	29.67	17.21	306.80	63.02	4.96	1.48
Min	61	129	6	57	21	47	15	166	0	0
Max	366	220	101	117	150	86	1,168	324	17	4

Note: EW denotes the Event Window and N-EW denotes the Non-Event Window

The results for the first political study event shown in Table 5.16 above, indicates that the Mean values for Bugs, Viruses, and Exploits are all larger during the event window than they are in the non-event window. For Trojans and Probes/Scans, the Mean values are larger in the non-event window than they are in the event window. The Standard Deviation parameters are larger in the non-event window for all variables except Viruses; which indicates the fact that the data is not widely dispersed for Bugs, Exploits, Trojans and Probes/Scans.

In the month of January 2003, a series of severe storms hit the eastern coast of the United States. These storms caused severe conditions in many states with local governors enacting states of emergency. This situation was quite unique during the research period and was therefore worthy of exploratory analysis, as presented in the next table.

Table 5.17 – Statistical Analysis of the Severe Winter Storms in January 2003

	Total Bugs		Total Viruses		Total Exploits		Total Trojans		Total Probes/Scans	
Parameter	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW
N	45	3	45	3	45	3	45	3	45	3
Mean	136.36	187.33	49.84	62.67	64.47	46.33	318.29	282.33	4.31	0
Variance	3,814.59	184.22	410.00	176.22	856.34	160.22	90,497.01	30,694.22	23.59	0
Standard Dev.	61.76	13.57	20.25	13.27	29.26	12.66	300.83	175.20	4.86	0
Min	61	172	6	50	21	31	15	111	0	0
Max	366	205	117	81	150	62	1,168	523	17	0

Note: EW denotes the Event Window and N-EW denotes the Non-Event Window

Based on the information in Table 5.17 above, the second political event illustrates the Mean values for Bugs and Viruses were higher in the event window than the non-event window. For Exploits, Trojans and Probes/Scans the Mean values were higher in the non-event window timeframe. In the non-event window, the SD and Max are higher for all study variables than in the event window time period. The Minimum values are noted to be at their highest in the event window.

Another political event select for analysis is the Northeast Blackout which occurred in August 2003. As discussed in Chapter Two, some experts believe that this political crisis was started by an information warfare attack. The statistical parameters for this event are presented in tabular format below.

Table 5.18 – Statistical Analysis of the Northeast Blackout in August 2003

	Total Bugs		Total Viruses		Total Exploits		Total Trojans		Total Probes/Scans	
Parameter	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	EW
N	45	3	45	3	45	3	45	3	45	3
Mean	135.49	200.33	49.31	70.67	62.87	70.33	284.18	794.00	4.31	0
Variance	3,691.63	522.89	396.39	106.89	875.09	134.89	76,076.64	4,538.00	23.59	0
Standard Dev.	60.76	22.87	19.91	10.34	29.58	11.61	275.82	67.36	4.86	0
Min	61	172	6	61	21	54	15	711	0	0
Max	366	228	117	85	150	80	1,168	876	17	0

Note: EW denotes the Event Window and N-EW denotes the Non-Event Window

The results for the third political event shown in Table 5.18 indicate that the Mean values for Bugs, Viruses, Exploits and Trojans are higher in the event window. But, Probes/Scans have a higher Mean value in the non-event window. Standard deviations are larger in the non-event window for all five variables.

In order to provide for a summary of the various military and political events that were analysed in this project the table below was prepared.

Table 5.19 – Summary of Results for the Military and Political Events

Event Description	Date of Event	Bugs		Viruses		Exploit Scripts		Trojans		Probes/Scans	
Military Events – Hypothesis 8		Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD
USS Cole Battleship Attack	October 2000	N-EW	N-EW	N-EW	N-EW	EW	N-EW	N-EW	N-EW	EW	N-EW
War in Afghanistan	October 2000 thru Dec. 2003	EW	EW	EW	EW	N-EW	N-EW	EW	EW	N-EW	N-EW
September 11th Attacks	September 2001	N-EW	N-EW	N-EW	N-EW	N-EW	N-EW	EW	N-EW	N-EW	N-EW
U.S. Invasion of Iraq	April 2003 thru Dec. 2003	EW	EW	EW	EW	EW	N-EW	EW	EW	N-EW	N-EW
U.S. Military Intervention in Liberia	September 2003	EW	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	N-EW	N-EW
Political Events – Hypothesis 9											
U.S. Presidential Election	November 2000	N-EW	N-EW	N-EW	N-EW	EW	N-EW	N-EW	N-EW	EW	N-EW
Western States Energy Crisis	July 2002	EW	N-EW	EW	EW	EW	N-EW	N-EW	N-EW	N-EW	N-EW
Severe Winter Storms	January 2003	EW	N-EW	EW	N-EW	N-EW	N-EW	N-EW	N-EW	N-EW	N-EW
Northeast Blackout	August 2003	EW	N-EW	EW	N-EW	EW	N-EW	EW	N-EW	N-EW	N-EW

First, Military Events have mixed results across all five events. The Event Window mean figures are higher for Bugs, Viruses and Trojans for the War in Afghanistan, U.S. Invasion of Iraq and U.S. Military Intervention in Liberia. And Exploit Scripts has higher mean values in during the USS Cole Battleship Attack, U.S. Invasion of Iraq and U.S. Military Intervention in Liberia. Lastly, Probes/Scans have a higher mean only in the event window for the USS Cole Battleship Attack.

Second, Political Events also have mixed results for all four related events. The Western States Energy Crisis, Severe Winter Storms and Northeast Blackout all have higher mean figures during the event window for Bugs and Viruses. For Exploit Scripts higher mean values are present in the event windows for the U.S. Presidential Election, Western Energy Crisis and Northeast Blackout. Trojans have a higher mean for the Northeast Blackout event only. Finally, Probes/Scans have a higher mean only for the U.S. Presidential Election event window.

Finally, Hypotheses Eight and Nine are partially accepted. Also, this research study can be used as a basis for similar research studies in the future.

5.4 Conclusion

This chapter presents the hypothesis testing and related results for nine detailed hypotheses which have been evaluated primarily using FBI and other government data sources. Using a detailed research model and project scope the totality of the hypotheses testing provides illustration and evidence of the detailed fieldwork, testing and analyses accomplished by the researcher over a significant period of time.

Specifically, the first seven hypotheses were tested using traditional Pearson Correlation Coefficients and Spearman Rank Correlation Coefficients. The final two hypotheses were tested using an event study approach. In all cases this testing was executed according to the overall research philosophy, design/model and grounded theory approach presented previously in Chapter Three. As is common in academic research a five percent significance level was used consistently for all related testing of forty-eight months of data from January 2000 through December 2003. In the study hypotheses, where the distribution of data was not assumed to be normally distributed a goodness of fit test was calculated in order to establish the robustness of the statistical measurements.

Correlation analysis determines whether or not there is a linear relationship between two variables. This important statistical measurement simply answers the fundamental question about whether or not there is in fact a statistical relationship between an independent and dependent variable. Additional testing in future projects can delve more deeply using additional quantitative and qualitative analyses. This is because this chapter was a preliminary exploration and accomplishment in the area of U.S. cyber security and critical infrastructure protection. From this study a number of interesting conclusions can be established.

In order to probe a potential general relationship between software bug reporting testing on Hypothesis One found that critical software bugs reported by the NIPC were found to have a positive weak correlation with the general software bugs reported by the CERT/CC. In addition there was no correlation with the same NIPC data and NIST's reporting of software bugs.

Second, a similar test was made in Hypothesis Two which looked to validate a correlation between the general population of computer viruses and the critical viruses reported by the NIPC. While this hypothesis was based on the researcher's professional and academic instinct it could not be proven or verified.

Third, the Bugs, Viruses, Exploits, Trojans and Probes/Scans were analysed to determine if there were correlations with various variables that measure Internet utilisation in the USA. The results from this testing found a strong, positive correlation with all study variables except for Exploit Scripts and Probes/Scans. Therefore, Hypotheses Three, Four and Five were only partially accepted. From this testing, that Probes/Scans were a unique item within the research study as there was a negative correlation with this variable and all five of the CyberNotes data elements. Also, Probes/Scans had no correlation. After follow-up procedures, the most important proposition for this issue is to review this in more detail in future research projects.

In Hypothesis Six the value of U.S. electronic commerce transactions was found to be positively correlated with a very strong significance to the NIPC's reporting of Bugs, Viruses and Trojans. But, there was no relationship with Exploit Scripts and a negative relationship with Probes/Scans. This testing confirms with increased electronic commerce transactions comes an increase in various, critical cyber security issues. The impact of this can relate to the use of Internet technology for business, consumer and government trading habits; as the use of e-commerce systems and throughput of transactions comes a corresponding increase in critical cyber security issues.

In Hypothesis Seven, a total of nine macro-economic factors were found to have very mixed results. All variables have a positive correlation with Bugs, Viruses and Trojans. The other variables (e.g. Exploits and Probes/Scans) demonstrated a positive correlation with the same set of macro-economic variables. These results can be subject to further testing and considered in such activities as simulation scenarios and heuristic modelling.

The sixth conclusion that can be drawn from Chapter Five relates to political and military events. All of this information can help government and future researchers examine models for information warfare attacks and other cyber threats. This testing focussed on a variety of mathematical calculations (predominantly Means and Standard Deviations) which found a

mixed set of results when comparing the event windows to the non-event windows for a total of nine events (e.g. five military and four political). This initial research can help government analysts and future researchers understand the vast potential impacts on cyber security. Also, it can help establish the potential linkages between traditional and non-traditional threats to critical infrastructure and other IT systems.

The researcher was fortunate to have a full four year census of secondary data from the FBI. This allowed for the uncommon luxury of not having to perform various statistical sampling tests since the complete population of data was utilised. However, the research results were limited due to the overall grounded theory approach that was undertaken. Nevertheless, a detailed series of suggestions for future research are presented in the following chapter. To this end, it is envisioned that a strong research agenda supported by other research projects can be undertaken.

CHAPTER SIX – CONCLUSION

6.1 Summary

This research project provided a unique perspective on an emerging area of research in the field of Information Technology. It was built upon a variety of specialist subject areas including: information systems and information technology, electronic commerce, computer security, risk management, national/homeland security (including information warfare and cyber terrorism) and information technology. The project originated from the researcher's academic and professional experiences as an IT auditor, security consultant and educator.

The Information Age has brought with it magnificent technological advances worldwide that have transformed the way many aspects of our business and personal lives. The Internet, electronic commerce, and a variety of emerging information technologies have presented many exciting advantages to modern society. Simultaneously, the business community and individuals also are confronted with increased threats from a number of different groups. These adversaries include: traditional computer hackers, cyber terrorists, information warriors, social action groups and rogue nations; all of which are bona fide, current threats to the United States (Alexander and Swetnam, 1999). Furthermore, the tools and techniques used by these malevolent parties present themselves in a variety of ways.

The major attack methods can be in the form of: vulnerabilities in software and hardware, computer malware (e.g. viruses, worms and Trojans), probes and scans, exploit scripts, and others (e.g. denial of service attacks, information warfare, phising schemes, etc.). According to Ohlson (2000), these attacks can cost over seven billion dollars per incident. Furthermore, during the period ten year period of 1993 to 2003 the Internet usage in the United States doubled. With the growing complexity of attack methods and concurrent growth of Internet utilisation; controlling technologies is a major challenge. In fact, this is often done through the use of new technologies; but, this by itself is not optimal since organisations and users balance the need for security and the ease of use for end-users (Backhouse Et. Al., 2005, Schou and Trimmer, 2004, and Schneier, 2000).

The government of the United States has been active in the field of computer and information security for over 60 years. The National Security Agency (NSA), various other defence and law enforcement agencies have departments and special groups dedicated to Information

Security and Assurance. In 1998, the U.S. Presidential Commission on Critical Infrastructure Protection (PCCIP) was established by President Clinton and developed a large number of landmark cyber security and national security initiatives. With the development of new U.S. government programmes to share cyber security information and warnings in the late-1990s about critical infrastructure protection; greater importance of these initiatives are now viewed in a post-911 era. As regional and international conflicts continue to grow, the United States continues its leadership in the fields of Information Assurance and Homeland/National Security.

Using a grounded theory research methodology together with and a variety of non-parametric statistics this study identified a number of interesting results. A variety of descriptive statistics were developed that analysed both the primary and secondary data. Various correlation analyses were performed in order to test seven of the nine hypotheses. An event window methodology was used to investigate the statistical parameters for the last two hypotheses which looked at the major military and political events that occurred from 2000-2004. This approach supported the researcher's efforts of conducting exploratory research where triangulation often deals with combining data sets from different sources (Sawyer, 2001). This allowed the researcher to revisit these events in various ways.

One of the major recommendations of the PCCIP was to establish a central command structure for cyber security. With this support the National Infrastructure Protection Centre (NIPC) was founded in 1999 and developed the CyberNotes newsletters which were used as the main source of data for this project. In addition, the FBI organised its InfraGard program to develop a very important public-private partnership in Information Assurance.

While Jones Et. Al (2001) and Whiting and Chabrow (2001) discussed some of the reasons why the U.S. Federal Government is eager to forge new relationships with private industry; practically this is difficult due to wide range of security issues. Additionally, it was difficult for the NIPC to be able to: 1) obtain and analyse security information quickly, 2) share information quickly and efficiently and 3) address the general and specific information needs of various stakeholder groups; all in a user-friendly format(s). This organisation faced formidable obstacles including: technological issues, primitive legal frameworks, and resource constraints (Alexander and Sweetnam, 1999 and U.S. General Accounting Office, 1998). Furthermore, various other government studies and publications through the present

continue to amplify the need for more cooperation between the public and private sectors in order to protect the national infrastructure from various threats. The major information technologies that support information sharing are inter-organisational systems, web information systems and government information systems.

Other important factors affecting cyber security during the study period include a number of government actions and initiatives. For instance, the Department of Homeland Security (DHS) was established in 2001 by President Bush. This department represented the largest single re-organisation of the U.S. federal government in the past fifty years (Lavine, 2004). The NIPC was re-organised as part of the DHS, only then to be re-organised once again in 2003 as part of the US-CERT; a separate entity from CERT/CC. While previous research by Rich (2001), Howard (1997) and others explored different aspects of computer security such as: Internet security, network security, risk management techniques, economic modelling and others. This research project was able to explore a secondary data approach to cyber security information related to U.S. critical infrastructure protection.

6.2 Conclusions

The philosophical underpinning of this study was an interpretivist approach. At the beginning of this project, four key objectives were established. In the end, all four of these were accomplished using a grounded theory research methodology. Inter-dependence deals with the discrete reliability of each data set. To help facilitate this, the researcher can identify linkage(s) with the theory being formulated and trying to overlap concepts.

The first objective was to investigate whether there is a correlation between general cyber security information and what is determined to be critical by the NIPC. To probe this question, the researcher used two categories of CyberNotes data (e.g. Bugs and Viruses). First, the NIPC's bugs were analysed with two other very reputable bug reporting organisations, CERT/CC and NIST. The results from this project indicate that the NIPC's critical bugs are positively but weakly correlated to the CERT/CC bugs, but not associated to the NIST bugs. For Viruses, the researcher used another general reporting source in order to test a similar theory that the number of critical Viruses is associated with the general number of computer viruses. The results of this testing are quite intriguing because they do not support the overall notion that critical cyber security information is explicitly related to general cyber security information as originally thought. For this objective one hypothesis was partially accepted and another was rejected.

The second objective examined changes in Internet growth and the reporting by the NIPC. The premise behind this aspect of the research was that the Internet is continuing to become an attractive target for hackers, criminals and terrorists as more individuals connected to the Information Superhighway and the E-Commerce business paradigm expanded. Consistent findings were documented for U.S. Internet utilisation, the number of U.S. Host Computers and Global WWW Pages, U.S B2B E-Commerce, U.S. B2C E-Commerce and Total U.S. E-Commerce as these study variables relate to software bugs, viruses and Trojans. Furthermore, the research findings in this area were impressive since statistically strong, positive relationships were evident. However, the correlation testing in this area was not proven for Exploit Scripts and Probes/Scans; as these variables had negative and non-existent

relationships, respectively. The two hypotheses in this part of the research were partially accepted.

Objective number three was to evaluate a variety of macro-economic factors and see if these factors are associated with the five variables of critical cyber security information reported by the leading U.S. government organisation in this area. The study had mixed results in this area with Bugs, Viruses, and Trojans having a statistically strong, negative relationship with interest rates and stock market indices and a strong, positive relationship with CPI, GDP, Inflation and Unemployment. As well, Exploit Scripts have mixed results in this area. Probes/Scans were found to have a strong, positive relationship with the two interest rates and three stock market indices, and a strong, negative relationship with three of the four more general macroeconomic factors (e.g. CPI, GDP and Unemployment). The three hypotheses in this component of the research were partially accepted.

Objective four explore the potential associations between military and political events with the NIPC's CybeNotes reporting using an event window methodology which is a common research design in finance, advertising, public policy and communications. Using the advice of other academics in these fields; five military events and four political events were analysed. Mixed results were summarised as follows for the military events where higher mean figures for Bugs, Viruses and Trojans were found for the War in Afghanistan, U.S. Invasion of Iraq and U.S. Military Intervention in Liberia. And Exploit Scripts has higher mean values in during the USS Cole Battleship Attack, U.S. Invasion of Iraq and U.S. Military Intervention in Liberia. Probes/Scans had a higher mean in one event window that being for the USS Cole Battleship Attack.

The four Political Events had mixed results for all four related events. The Western States Energy Crisis, Severe Winter Storms and Northeast Blackout all have higher mean figures during the event window for Bugs and Viruses. Exploit Scripts higher mean values are present in the event windows for the U.S. Presidential Election, Western Energy Crisis and Northeast Blackout. Trojans have a higher mean for the Northeast Blackout event only. Probes/Scans have a higher mean only for the U.S. Presidential Election event window. The two hypotheses in this part of the research project were partially accepted.

In addition to these results, another benefit of this project is that additional ideas for further research emerged. While these could not be conducted as part of this project, the major suggestions are presented in the following section of this chapter for future consideration.

6.3 Areas for Future Research

This project presented new knowledge in the field of IT Security/Information Assurance and has provided a basis for various avenues for further research in the future. For instance, the research hypotheses could easily be expanded to look at future periods of time in a longer longitudinal study. This can expand on the initial results, findings and recommendation from the four year data period presented in this study. Specifically, this type of follow-up study can examine additional trends, general findings and other factors in critical infrastructure information in the United States.

In addition, there are a number of other suggestions that can be investigated as areas of future research. These ideas are a direct result of the outcomes and design of this project. In this regard, six specific recommendations have been developed.

First, additional empirical research in the form of additional data could be used to expand the grounded theory approach as a means of performing further testing. These variables can be collected from both primary and secondary sources. As well, some variables may be obtained from other government agencies, consultancy organisations and commercial vendors (e.g. anti-virus companies, software development firms) etc.

Second, a comparative international study that investigates the potential similarities and difference between U.S. and non-U.S. critical infrastructure information would be very useful. In this regard, it would be effective to adopt a similar research methodology as what was used in this project. This type of comparative study could address similar research questions that were presented herein; as well as variations that are of interest to the individual researcher and/or supporting government entity.

Third, a quantitative survey of Chief Information Security Officers and other information assurance practitioners could be developed. Such a study should focus on how these professionals: analyse, utilise and implement the cyber security information (e.g. warnings, alerts and newsletters) supplied by government organisations and/or security agencies. Furthermore, this type of study could be pursued with a large professional organisation such as: the Information Systems Audit and Control Association, Institute of Internal Auditors,

SANS or InfraGard. Of particular interest in this type of survey would be how this information sharing supports critical infrastructure protection at an enterprise level and from a larger view perhaps as it relates to one of the national infrastructures.

Fourth, a variety of qualitative research techniques should be explored to look at the content of cyber security information. Specifically, it would be very interesting to perform a detailed content analysis as described in the research methodology chapter. Such a study could easily use of commercial computer software to explore the qualitative nature of the cyber security newsletters published by the NIPC and its successor organisations.

Fifth, more detailed studies can be performed in the areas of Software Bugs, Viruses, Exploit Scripts and Trojans. These areas continue to be high risk vulnerabilities for businesses, government organisations and individuals. Therefore, additional research which develops richer information related to attack methodologies, trend analyses, discovery methods, tracking systems and other approaches will be very useful.

Sixth, further search should be pursued in the area of exploit scripts and vulnerability management. In this area, more in-depth analysis in the area E-Commerce systems, operating systems, computer hardware and other critical infrastructure components can be analysed. By doing so, more information can be explored in order to build predictive models and heuristics for information warfare, cyber terrorism and national defence.

All of the recommendations described above highlights the fact that that the fields of information assurance, internal control and risk management are still in their early stages. In all, the opportunities for future research are quite extensive.

6.4 Final Thoughts

This research project provided an exciting personal and professional opportunity to the researcher to explore and enhance his own skills. He received important support from the FBI in the United States and was supervised by Professor Georges Selim, Head of Faculty.

By adopting a grounded theory approach it allowed for exploration of a new area in the rapidly emerging fields of cyber security and critical infrastructure protection. All of this was done within the requirements, scope and timeframe of the Doctor of Philosophy degree as required by Cass Business School, City University.

Finally, this project has developed new knowledge and insights into research, theory and practice within the exciting fields of: information assurance, information systems, risk management and auditing.

BIBLIOGRAPHY

2000 CSI/FBI Computer Crime and Security Survey (2000). Computer Security Institute, Computer Security Journal. Volume Sixteen, Number Two, pp. 33-49.

Abrams, M.D. and Brusil, P.J. (2000). Application of the common criteria to a system. Computer Security Journal. Volume Sixteen, Number Two, pp. 11-21.

Agrawal, A. and Kamakura, W.A. (July 1995). The economic worth of celebrity endorsers: An event study analysis. Journal of Marketing. Volume Fifty-Nine, Number Three, pp. 56-62.

Adlerman, L.M. (1990). An Abstract Theory of Computer Viruses. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp. 307-323, Van Nostrand Reinhold, New York, New York.

Andreson, D.R., Sweeney, D.J. and Williams, T.A. (2005). Statistics for Business and Economics, Ninth Edition, Thompson-Southwestern, Mason, Ohio.

Alexander, Y. and Swetnam, M.S. (1999). Cyber Terrorism and Information Warfare: Assessment of Challenges, Volume One, Oceana Publications, Dobbs Ferry, New York.

Alexander, Y. and Swetnam, M.S. (1999a). Cyber Terrorism and Information Warfare: Executive and Congressional Perspectives, Volume Two, Oceana Publications, Dobbs Ferry, New York.

Alexander, Y. and Swetnam, M.S. (1999b). Cyber Terrorism and Information Warfare: Critical Infrastructure Protection Issues, Volume Three, Oceana Publications, Dobbs Ferry, New York.

Alexander, Y. and Swetnam, M.S. (1999c). Cyber Terrorism and Information Warfare: Research and Development Roadmaps, Volume Four, Oceana Publications, Dobbs Ferry, New York.

Altheide, D.L. (1996). Qualitative Media Analysis, Sage Publications, Thousand Oaks, California.

Arens, Y. and Rosenbloom, P.S. (September 2003). Responding to the unexpected. Communication of the ACM. Volume Forty-Six, Number Nine, pp. 33-35.

Armitage, S. (1995). Event study methods and evidence on their performance. Journal of Economic Surveys. Volume Eight, Number Four, pp. 25-52.

Asch, D. (2001). Competing in the new economy. European Business Review. Volume Thirteen, Number Three, pp. 119-126.

Avolio, F.M. and Treese, W. (April/May 1998). A multidimensional approach to Internet security. Network World. pp. 15-22.

Aytes, K. (2004). Computer security and risky computing practices: a rational choice perspective. Journal of Organisational and End User Computing. Volume Sixteen, Number Three, pp. 22-40.

Backhouse, J. Et. Al. (2005). Risk management in cyberspace, In Trust and Crime in Information Societies. Eds. Mansell, R. and Collins, B.S., Edward Algar Publishing, Cheltenham, United Kingdom.

Ball, R. and Kothari, S.P. (October 1991). Security returns around earnings announcements; Extended functional fixation. The Accounting Review. Volume Sixty-Six, Number Four, pp. 718-738.

Ball, S. (1998). XML and the desperate Tcl hacker. Computer Networks and ISDN Systems. Issue Thirty, pp. 713-715.

Bakerville, R. (1993). Information systems security design methods: implications for information systems development. ACM Computing Surveys. Volume Twenty-Five, Number Four, pp. 375-414.

Bank, D. (27 May 2004). Computer worm is turning faster; Installing security patches is now constant rush job against speedier invaders. The Wall Street Journal. p. B3.

Banville, C. and Landry, M. (1992). Can the Field of MIS be Disciplined? In Information Systems Research: Issues Methods and Practical Guidelines, Ed. Galliers, R.D., pp. 61-88, Blackwell Scientific Publications, Oxford, United Kingdom.

Barber, R. (2001). The evolution of intrusion detection systems – the next step. Computers & Security. Volume Twenty, Issue Two, pp. 132-145.

Baroudi, J.J. and Orlikowski, W.J. (1989). The problem of statistical power in MIS research, MIS Quarterly. Volume Three, pp. 87-106.

Barry, C. and Lang, M. (April/June 2001). A survey of multimedia and web development techniques and methodology usage. IEEE Multimedia. pp. 52-60.

Baskerville, R. (2001). Conducting Action Research: High Risk and High Reward in Theory and Practice. In Trends in the Choice of Qualitative Methods. Ed. Trauth, E.M., pp. 192-217, Idea Group Publishing, Hershey, Pennsylvania.

Baucus, M.S. and Baucus, D.A. (1997). Paying the piper: An empirical examination of longer-term financial consequences of illegal corporate behaviour. Academy of Management Journal. Volume Forty, Number One, pp. 129-151.

Benbasat, I. and Zmud, R.W. (March 1999). Empirical research in information systems: The practice of relevance. Management Information Systems Quarterly. Volume Twenty-Three, Number 1, pp. 3-16.

Benbasat, I., Goldstein, D.K., and Mead, M. (1987). The case research strategy in studies of information systems. Management Information Systems Quarterly. September 1987, Volume Eleven, Number Three, pp. 369-386.

Berghel, H. (2001). The code red worm. Communications of the ACM. Volume Forty-Four, Number Twelve, pp. 15-19.

Bequai, A. (1999). Cyber-crime the US experience. Computers & Security. Volume Eighteen, Number One, pp. 16-18.

Bequai, A. (1999a). Employers and the Internet: Legal woes and concerns. Computers & Security. Volume Eighteen, Number Four, pp. 303-306.

Black, U. (2000). Internet Security Protocols: Protecting IP Traffic, Prentice-Hall, Upper Saddle River, New Jersey.

Blackmer, S. (October 1994). Privacy in cyberspace. International Corporate Law. Number Thirty-Nine, pp. 19-28.

Blain, C.M. (2000). Cryptography and Electronic Commerce: The role of The Canadian Government in Facilitating a Domestic and Global Marketplace. Masters Thesis, Carleton University.

Blume, P. (2000). Data protection of law offenders. In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Eds. Thomas, D. & Loader, B.D., pp. 193-217, Routledge, London.

Boardman, B. (1 April 1998). Asset management products let you gain network control. Network Computing. pp. 80-89.

Bogdan, R. and Ksander, M. (1980). Policy data as a social process: A qualitative approach to quantitative data. Human Organisation. Volume Thirty-Nine, Number Four, pp. 302-309.

Bosworth, S. (2002). Information Warfare. In Computer Security Handbook, Fourth Edition, Eds. Bosworth, S. and Kabay, M.E., pp. 7.1-7.25, John Wiley & Sons, Inc., New York, New York.

Bosworth, S. and Jacobson, R. (2002). Brief History and Mission of Information System Security. In Computer Security Handbook, Fourth Edition, Eds. Bosworth, S. and Kabay, M.E., pp. 1.1-1.13, John Wiley & Sons, Inc., New York, New York.

Boyan, J. (1997). The anonymiser: Protecting user privacy on the web. CMC Magazine. Available on-line at http://www.december.com/cmc/mag/1997/sep/boyan.html. Accessed on 6 June 2001.

Brace, N., Kemp, R. and Snegler, R. (2000). SPSS for Psychologists. Lawrence Erlbaum Associates, Mahwah, New Jersey.

Bradley, J. (1993). Methodological issues and practices in qualitative research. Library Quarterly. Volume Sixty-Four, Number Four, pp. 431-449.

Brinson, J.D. Et. Al. (2001). E-Commerce & Internet Law, Prentice-Hall/ PTR, Upper Saddle River, New Jersey.

British Standards Institution. (30 June 2000). BS7799-2: 1999 Information Security Management - Part Two: Specification for Information Security Management Systems, London, England.

Brown, J. (6 February 2004). Truckstop.net puts drivers on information highway. Computing Canada. p. 18.

Brown, S.R. and Melamed, L.E. (1990). Experimental Design and Analysis, Sage Publications, Newbury Park, California.

Buck-Emden, R. and Galimow, J. (1996). SAP R/3 System: A Client Server Technology, Addison-Wesley Longman, Ltd., Essex, England.

Buckler, G. (6 February 2004). Software pest control can be better managed. Computing Canada. p. 18.

Burke, R.J. (2005). International terrorism and threats to security. Disaster Prevention and Management. Volume Fourteen, Number Five, pp. 639-643.

Burns, G.M. (Winter 2000). Information protection and the laws of the land. Computer Security Journal. Volume Sixteen, Number One, pp. 9-13.

Caminada, M. Et. Al. (1998). Internet security incidents: A survey within dutch organisations. Computers & Security. Volume Seventeen, Number Five, pp. 417-433.

Cantwell, J. and Santangelo, G.D. (1999). The frontier of international technology networks: Sourcing abroad the most highly tacit capabilities. Information Economics and Policy. Volume Eleven, Number One, pp. 101-123.

Carlson, J.R. (1995). The future terrorists in America. American Journal of Police. Volume Fourteen, Number Three, pp. 71-91.

Casson, P. (July 1997). CSFI's report of the Internet and financial services. Financial Regulation Report. pp. 32-33.

Cavanagh, J.P. (1997). Internet and Internetworking Security, RIA Group, Boston, Massachusetts.

Cave, J. (2005). The economics of cyber trust between cyber partners. Cyber Trust & Crime Prevention Project. University of Warwick.

Cecez-Kecmanovic, D. (2001). Doing Critical IS Research: The Question of Methodology. In Trends in the Choice of Qualitative Methods, Ed. Trauth, E.M., pp. 141-162, Idea Group Publishing, Hershey, Pennsylvania.

Chen, C.Y. and Lindsay, G. (2000). Viruses, attacks, and sabotage: It's a computer crime wave. Fortune. Volume One Hundred and Forty One, Number Ten, Start Page: 484.

Cheung, S. and Levitt, K.N. (1997). Protecting routing infrastructure from denial of service using cooperative intrusion detection. *Proceedings of the 1997 New Security Paradigms Workshop, Association for Computing Machinery, Langdale, Cumbria, United Kingdom,* pp. 94-106.

Chillarege, R., Kao, W., and Condit, R. G. (1991). Defect type and its impact on the growth curve. *Proceedings of the 13th International Conference on Software Engineering,* pp. 246-255.

Ciborra, C.U. and Hanseth, O. (1998). From tool to Gestell agendas for managing information infrastructures. Volume Eleven, Number Four, p. 305.

Cifuentes, C., Waddington, T. and Van Emmerick, M. (2002). Computer security analysis through decompilation and high-level debugging. *Proceedings of the IEEE Eighth Working Conference on Reverse Engineering,*

Cilluffo, F. J. (4 October 2001). Critical infrastructure protection: Who's in charge? Centre for Strategic and International Studies. Washington, D.C.

Clark, T.H. and Stoddard, D.B. (1996). Interorganisational business process redesign: Merging technological and process innovation. Journal of Management Information Systems. Volume Thirteen, Number Two, pp. 9-28.

Cohen, F.B. Et. Al. (1998). A cause and effect model of attacks on information systems. Computers & Security. Volume Seventeen, Number Three, pp. 211-221.

Cohen, F.B. (1995). Protection and Security on the Information Superhighway, John Wiley & Sons, Inc., New York, New York.

Cohen, F. (1987). Computer Viruses – Theory and Experiments. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp. 356-376, Van Nostrand Reinhold, New York, New York.

Cohen, F. (1986). Computational Aspects of Computer Viruses. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp. 324-355, Van Nostrand Reinhold, New York, New York.

Colkin, E. (2001). IT security and the law. Information Week. Number Eight Hundred Sixty-Five, pp. 22-24.

Costello, J. (1991). Security on computer networks: Looking for answers, ACM SIGUCCS. Volume Nineteen, pp. 49-52.

Cowan, C. Et. Al. (2000). Buffer overflows: Attacks and defences for the vulnerability of the decade. *Proceedings of the DARPA Information Survivability Conference and Exposition/DISCEX 2000, January 2000, Hilton Head, South Carolina, IEEE Computer Society, Los Alamitos, California.*

Coxon, A.P.M. (1999). Sorting Data: Collection and Analysis, Sage Publications, Thousand Oaks, California.

Cramer, M.L. and Pratt, S.R. (1989). Computer Virus Countermeasures – A New Type of Electronic Warfare. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp. 246-260, Van Nostrand Reinhold, New York, New York.

Crelinsten, R.D. (1998). The discourse and practice of counter-terrorism in liberal democracies. Australian Journal of Politics and History. Volume Forty-Four, Number One, pp. 389-413.

Creswell, J.W. (1994). Research Design: Qualitative & Quantitative Approaches, Sage Publications, Thousand Oaks, California.

Creswell, J.W. (1998). Qualitative Inquiry and Research Design: Choosing Among Five Traditions, Sage Publications, Thousand Oaks, California.

Curtin, M. (1999). Creating an environment for reusable software research: A case study in reusability. The Ohio State University, Department of Computer and Information Science. OSU-CISRC – 8/99-TR21. pp. 1-12.

Dalton, C. and Choo, T.H. (2001). An operating system approach to securing e-services: Implementing trusted Linux, an ideal platform for e-services application hosting. Communications of the ACM. Volume Forty-Four, Number Two, pp. 58-64.

Davenport, T.H. (1999). Knowledge management, round two. CIO. Volume Thirteen, Number Four, pp. 30-33.

Davenport, T.H., Harris, J.G. and Kohli, A.K. (2001). How do they know their customers so well? MIT Sloan Management Review. Volume Forty-Two, Number Two, pp. 63-73.

Davenport, T.H. Et. Al. (2001). Data to knowledge to results: Building an analytical capability. California Management Review. Volume Forty-Three, Number Two, pp. 117-138.

Davida, G.I., Desmedt, Y.G., and Matt, B.J. (1989). Defending Systems Against Viruses Through Cryptographic Authentication. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp. 261-272, Van Nostrand Reinhold, New York, New York.

Davies, P.H.J. (2000). Information warfare and the future of the spy. In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Eds. Thomas, D. & Loader, B.D., pp. 251-268, Routledge, London.

Davis, G.B. (1992). An Individual and Group Strategy for Research in Information Systems. In Information Systems Research: Issues Methods and Practical Guidelines, Ed. Galliers, R.D., pp. 230-249, Blackwell Scientific Publications, Oxford, United Kingdom.

De, P. and Ferratt, T.W. (1998). An information system involving competing organisations. Communications of the ACM. Volume Forty-One, Number Twelve, pp. 90-98.

Denning, D. (1999). Information Warfare and Security, Addison-Wesley, New York, New York.

Denning, D. and Baugh, W.E. Jr. (2000). Hiding crimes in Cyberspace. In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Eds. Thomas, D. & Loader, B.D., pp. 105-131, Routledge, London.

Denning D.E. and Denning P.J. (1979). Data security. Communications of the ACM. Volume Eleven, Number Three, pp. 227-249.

Dickey, R.L. (2000). Attitudes toward aviation security: The effects of differing information. Ph.D. Dissertation. University of Texas at Arlington.

Dixon, J. and Dogan, R. (June 2003). Analysing global governance failure: A philosophical framework. Journal of Comparative Policy Analysis. Volume Five, Numbers Two-Three, pp. 209-226.

Dooley, D. (1984). Social Research Methods, Prentice-Hall, Englewood Cliffs, New Jersey.

Dutton, W.H. and Shepherd, A. (2004). Confidence and risk on the Internet. Cyber Trust & Crime Prevention Project. Oxford Internet Institute, Oxford University.

Dyckman, T.R. and Thomas L.J. (1977). Fundamental Statistics for Business and Economics, Prentice Hall. Englewood Cliffs, New Jersey.

El-Kordy, M.M. (2001). Understanding the utilisation of executive information systems using an integrated technology acceptance model: Theoretical base and empirical validation. Ph.D. Thesis, City University Business School.

Electronic Privacy Information Centre (1998). Critical Infrastructure Protection and The Endangerment of Civil Liberties: An Assessment of the President's Commission on Critical Infrastructure Protection Washington, D.C.

Ellison, R.J. Et. Al. (November/December 1999). Survivability: Protecting your critical systems. IEEE Internet Computing. pp. 55-63.

Farhoomand, A.F. (1992). Scientific Progress of Management Information Systems. In Information Systems Research: Issues Methods and Practical Guidelines, Ed. Galliers, R.D., pp. 93-111, Blackwell Scientific Publications, Oxford, United Kingdom.

Feigenbaum, J. (2002). Toward realistic assumptions, models, and goals for security research. *Proceedings of the NSF Workshop on Security Research, Berkeley, California* Available on-line at http://www.cs.yale.edu/~jf. Accessed on 24 June 2004.

Felten, E.W. (1997). Webware security. Communications of the ACM. Volume Forty, Number Four, p. 130.

Fischer-Hubner, S. (2000). Privacy and security at risk in the global information society. In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Eds. Thomas, D. & Loader, B.D., pp. 173-192, Routledge, London.

Fitchard, K. (2006). Whole new net, whole new numbers game. Telephony. Volume Two Hundred Twenty-Four, Number Twenty-One, p. 24.

Fitchard, K. (2004). The Internet drag race. Telephony. Volume Two Hundred Forty-Five, Number Ten, p. 30.

Fites, P.E., Kratz, M.P., and Brebner, A.F. (1989). Control and Security of Computer Information Systems, Computer Science Press, Rockville, Maryland.

Foley, S.N. (1997). The specification of implementation of 'Commercial' security requirements including dynamic segregation of duties. Technical Report, Department of Computer Science, University College, Cork, Ireland, pp. 125-134.

Foley, S.N. and Dumigan, R. (2001). Are handheld viruses a significant threat? Communications of the ACM. Volume Forty-Four, Number One, pp. 105-107.

Forcht, K.A. (1989). Ethical Use of Computers. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp. 117-120, Van Nostrand Reinhold, New York, New York.

Forcht, K.A. (1994). Computer Security Management, Boyd & Fraser Publishing, Danvers, Massachusetts.

Ford, W. (1994). Standardising information technology security. Standard View. Volume Two, Number Two, pp. 64-71.

Ford, W. and Baum, M.S. (1997). Secure Electronic Commerce, Prentice-Hall, Upper Saddle River, New Jersey.

Forno, R. and Baklarz, R. (1999). The Art of Information Warfare, Universal Publishers, Boca Raton, Florida

Fowler, F.J. Jr. (1995). Improving Survey Questions, Sage Publications, London, England.

Fox, A. and Gribble, S. (1996). Security on the move: Indirect authentication using Kerberos. *Proceedings of the Mobicom 1996 Conference, Rye, New York,* pp. 155-164.

Frincke, D. (2000). Balancing cooperation and risk in intrusion detection. Transactions on Information and System Security. Volume Three, Number One, pp. 1-29.

Franklin, D. (July 2001). Turning information into knowledge – and money. The OECD Observer. pp. 15-16.

Franklin, I. (2001). Protecting the web server and applications. Computer Security Journal. Volume Twenty, Number One, pp. 31-35.

Furnell, S.M. and Warren, M.J. (1999). Computer hacking and cyberterrorism: The real threats in the new millennium? Computers & Security. Volume Eighteen, Number One, pp. 28-34.

Galliers, R.D. (1992). Choosing Information Systems Research Approaches. In Information Systems Research: Issues Methods and Practical Guidelines, Ed. Galliers, R.D., pp. 144-162, Blackwell Scientific Publications, Oxford, United Kingdom.

Garfinkel, S. and Spafford, G. (1996). Practical UNIX and Internet Security, Second Edition, O'Reilly and Associates, Inc., Sebastopol, California.

Geer, D. Et. Al. (2003). CyberInsecurity: The cost of monopoly – how the dominance of Microsoft's products poses a risk to security. Available on-line at http://www.ccianet.org/papers/cyberinsecurity.pdf. Accessed on 23 December 2003.

Gelinas, U.J., Sutton, S.G., and Hunton, S. (2005). Accounting Information Systems, Sixth Edition, South-Western College Publishing, Cincinnati, Ohio.

Gemignani, M. (1989). Viruses and Criminal Law. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp.99-103, Van Nostrand Reinhold, New York, New York.

Gephart, R.P. (1988). Ethnostatistics: Qualitative Foundations for Quantitative Research, Sage Publications, Thousand Oaks, California.

Gerber, L. and Raucci, R. (February 1998). Antivirus technology offers new cures. Computer. pp. 12-14.

Ghosh, A.K. (2001). Security and Privacy for E-Business, John Wiley & Sons, Inc., New York, New York.

Ghosh, A.K. and Swaminatha,T.M. (2001). Software security and privacy risks in mobile e-commerce: Examining the risks in wireless computing that will likely influence the emerging m-commerce market. Communications of the ACM. Volume Forty-Four, Number Two, pp. 51-57.

Gibbons, J.D. (1993). Nonparametric Statistics: An Introduction, Sage Publications, Newbury Park, California.

Gibson, H.R. (1994). Elementary Statistics, William C. Brown Publishers, Dubuque, Iowa.

Gillooly, C. (16 February 1998). Enterprise management - is the promise of enterprise management too good to be true? Information Week. pp. 42-46.

Girard, J. (4 March 1999). Remote access concepts and definitions. Research Note Tutorials. Gartner Group, Stamford, Connecticut.

Gittlen, S. (2005). Security counterattack. Network World. Volume Twenty-Two, Number Eleven, pp. S14-S15.

Gladstone, J. (1997). Survey of the law of cyberspace: An introduction. The Business Lawyer. Volume Fifty-Three, Number One, pp. 217-223.

Glaser, B.G. (1992). Basics of Grounded Theory Analysis, Sociology Press, Mill Valley, California.

Glass, B. (16 March 1996). Economics makes the case for VPNs. InfoWorld. pp. 12-15.

Goodman, P.S. and Darr, E.D. (1998). Computer aided systems and communities: Mechanisms for organisational learning in distributed environments. MIS Quarterly. Volume Twenty-Two, Number Four, pp. 417-440.

Gollmann, D. (1999). Computer Security, John Wiley & Sons, Inc., Chichester, West Sussex, England.

Gordon, L. Et. Al. (2006). 2006 CSI/FBI Computer Crime and Security Survey. Available on-line at http://www.gocsi.com/2006survey. Accessed on 12 November 2006.

Graf, J.E. II (1995). Global information infrastructure: First principles. Telecommunications. Volume Twenty-Nine, Number One, pp. 72-83.

Graham, R. (2001). NIDS – pattern search vs. protocol decode. Computers & Security. Volume Twenty, Number One, pp. 37-41.

Green, J.C. and Caracelli, V.J. (Summer 1997). Advances in Mixed Method Evaluation: The Challenges and Benefits of Integrating Diverse Paradigms, Volume 74, Jossey-Bass Publishers, San Francisco, California.

Greenberg, L.T. and Goodman, S.E. (1996). Is big brother hanging by his bootstraps? Communications of the ACM. Volume Thirty-Nine, Number Seven, pp. 11-15.

Greene, T. (29 March 2004). Time to enlist a 'national guard' for IT? Network World. Volume Twenty-One, Number Thirteen, p. 8.

Greenstein, M. and Feinman, T.M. (2000). Electronic Commerce: Security, Risk Management and Control, McGraw-Hill, Boston, Massachusetts.

Grover, V. and Davenport, T.H. (2001). General perspectives on knowledge management: Fostering a research agenda. Journal of Management Information Systems. Volume Eighteen, Number One, pp. 5-21.

Guha, R., Et. Al. (2004). Propagation of trust and distrust. *Proceedings of the 13th International Conference on the World Wide Web, New York, New York,* pp. 403-412.

Gupta, M., Rao, R., and Upadhyaya, S. (2004). Electronic banking and information assurance issues: Survey and synthesis. Journal of Organisational and End User Computing. Volume Sixteen, Number Three, pp. 1-21.

Guy, D.M., Alderman, C.W. and Winters, A.J. (1999). Auditing, Fifth Edition, Dryden Press, Fort Worth, Texas.

Haag-Granello, D. and Wheaton, J.E. (Fall 2004). Online data collection: Strategies for research. Journal of Counseling and Development. Volume Eighty-Two, Number Four, pp. 387-393.

Hamel, J., Dufour, S. and Fortin, D. (1993). Case Study Methods, Sage Publications, Newbury Park, California.

Hamilton, S. and Ives, B. (1992). MIS Research Strategies. In Information Systems Research: Issues Methods and Practical Guidelines, Ed. Galliers, R.D., pp. 132-143, Blackwell Scientific Publications, Oxford, United Kingdom.

Hangal, S. and Lam M.S. (2002). Tracking down software bugs using automatic anomaly detection. *Proceedings of the 24th International Conference on Software Engineering, Orlando, Florida,* pp. 291-301

Harley, D.A. (1999). Managing malware: Mapping technology to function. *Proceedings of the 1999 EICAR Conference, Aalborg, Denmark*, pp. 1-36.

Harrigan, K. (1998). When information can mean security – or catastrophe. Pollution Engineering. Volume Thirty, Number Thirteen, pp. 19-20.

Harrison, A. (2000). Cyberassaults hit Buy.com, eBay, CNN and Amazon. Available on-line at http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_STO43010-,00.html Accessed on 14 January 2002.

Haver, M.A. (1998). The statistics corner: Resources for country data. Business Economics. Volume Thirty-Three, Number Four, pp. 65-66.

Heaton, J. (Autumn 1998). Secondary analysis of qualitative data, Social Research Update. Issue Twenty Two. Available on-line at http:///www.soc.surrey.ac.uk/sru/SRU22.html. Accessed on 8 June 2001.

Hendon, R.A., Nath, R., and Hendon, D.W. (1998). The strategic and tactical value of electronic data interchange for marketing firms. The Mid-Atlantic Journal of Business. Volume Thirty-Four, Number One, pp. 53-73.

Hess, G. (1998). EPA withdraws Internet data plan citing fears about national security. Chemical Market Reporter. Volume Two Hundred Fifty-Four, Issue Twenty, pp. 1-4.

Hicks, C. (2000). The economics of crime. The Journal of State Government. Volume Seventy-Three, Number Three, pp. 5-7.

Highland, H.J. (1988). The Brain Virus: Fact and Fantasy. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp. 159-164, Van Nostrand Reinhold, New York, New York.

Hill, N.C., Perry, S.E. and Andes, S. (Summer 1996). Evaluating firms in financial distress: An event history analysis. Journal of Applied Business Research. Volume Twelve, Number Three, pp. 60-71.

Hirscheim, R.A. (1992). Information Systems Epistemology: An Historical Perspective, In Information Systems Research: Issues Methods and Practical Guidelines, Ed. Galliers, R.D., pp. 28-60, Blackwell Scientific Publications, Oxford, United Kingdom.

Hodson, T.J., Englander, F., and Englander, V. (1999). Ethical, legal and economic aspects of employer monitoring of employees electronic mail. Journal of Business Ethics. Volume Nineteen, Number One, pp. 99-108.

Hoffe, O. (September 1998). Moral reasons for an intercultural criminal law: A philosophical attempt. Ratio Juris. Volume Eleven, Number Three, pp. 206-227.

Hoffer, G., George, J.F. and Valacich, J.S. (2005). Modern Systems Analysis & Design. Fourth Edition, Prentice-Hall, Upper Saddle River, New Jersey.

Hoffman, D.L., Novak, T.P. and Venkatesh, A. (2004). Has the Internet become indispensable? Communications of the ACM. Volume Forty-Seven, Number Seven, pp. 37-42.

Hoffman, L.J. and Hung, B.T. (1989). A pictorial representation and validation of the emerging computer system security risk management framework. *Proceedings of the Computer Security Risk Management Model Builders Workshop, Ottawa, Canada*, p. 6.

Holland, C.P. and Lockett, A.G. (1997). Mixed mode network structures: The strategic use of electronic communication by organisation. Organisation Science. Volume Eight, Number Five, pp. 475-488.

Holzmann, G.J. (2001). Economics of software verification. *Proceedings of the 2001 ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools and Engineering, Snowbird, Utah,* pp. 80-89.

Howard, J.D. (1997). An analysis of security incidents on the Internet: 1989-1995. Ph.D. Dissertation, Carnegie Mellon University.

Howard, J. and Meunier, P. (2002). Using a "Common Language" for Computer Security Incident Information. In Computer Security Handbook, Fourth Edition, Eds. Bosworth, S. and Kabay, M.E., pp. 3.1-3.22, John Wiley & Sons, Inc., New York, New York.

Huang, Y., Et. Al. (2004). Securing web application code by static analysis and runtime protection. *Proceedings of the 13th International Conference on World Wide Web, New York, New York,* pp. 40-52.

Hudson, H.E. (1998). Global information infrastructure: Eliminating the distance barrier. Business Economics. Volume Thirty-Three, Number Two, pp. 25-31.

Huffman, L. and Talcove, W. (1995). Information infrastructure: Challenge and opportunity. Public Management. Volume Seventy-Seven, Number Five, pp. 9-14.

Hulme, G.V. (2002). Virus defenses reach the tipping point. InformationWeek. Number Nine Hundred and One, Start page: 56.

Hunter, M.G. (2000). Excellent Systems Analysts: A Grounded Theory Approach to Qualitative Research, In Human Centred Methods in Information Systems: Current Research and Practice. Eds. Clarke, S. and Lehaney, B., pp. 39-60, Idea Group Publishing, Hershey, Pennsylvania.

Hurley, D. (1995). Property and privacy in cyberspace. The OECD Observer. Number One Hundred Ninety-Six, pp. 19-25.

Hurst, P. (November 1998). Sharing performance data through credit reference agencies – levelling the playing field. Credit Management. pp. 28-31.

Husted, B. (2000). The impact of national culture on software piracy. Journal of Business Ethics. Volume Twenty-Six, Number Three, Part One, pp. 197-211.

iCorps Technology and Systems Consultant. (2002). Viri, Worms, & Trojans (Oh My!). iCorps Insider: Network, Development and Web-Based Solutions. Available on-line at http://www.icorpstech.com/insider/issues/news_4_1.25.2002.030106.html Accessed on 31 January 2003.

Information Security Governance: Guidance for Board of Directors and Executive Management. (2006). Second Edition. IT Governance Institute, Rolling Meadows, Illinois.

International Standardisation Organisation (2005) ISO 17799 Information Technology, Security Techniques, Code of Practice for Information Security Management.

Im, K.S., Dow, K., and Grover, V. (March 2001). Research Report: A re-examination of IT investment and the market value of the firm – an event study methodology. Information Systems Research. Volume Twelve, Number One, pp. 103-117.

Ireland, T.J. (1997). The interface between law and economics and forensic economics. Journal of Legal Economics. Volume Seven, Number One, pp. 60-70.

Jackson, J., Allum, N., and Gaskell, G. (2004). Perceptions of risk in cyberspace. Cyber Trust & Crime Prevention Project. London School of Economics and Politics.

Jackson, M. (2000). Keeping secrets: International developments to protect undisclosed business information and trade secrets, In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Eds. Thomas, D. & Loader, B.D., pp. 85-102, Routledge, London.

Jarvis, N. (1999). E-commerce and encryption: Barriers to growth. Computers & Security. Volume Eighteen, Number Five, pp. 429-431.

Jauch, L.R., Osborn, R.N. and Martin, T.N. (1980). Structured content analysis of cases: A contemporary method for organisational research. Academy of Management Research. Volume Five, Number Four, pp. 517-525.

Jean-Eric, A. (1999). Into the future with social sciences. The OECD Observer. Number Two Hundred and Seventeen/Eighteen, pp. 76-79.

Johnson, D.E.L. (1998). Knowledge management is new competitive edge. Health Care Strategic Management. Volume Sixteen, Number Seven, pp. 2-3.

Johnson, R.A. and Wichern, D.W. (1988). Applied Multivariate Statistical Analysis, Second Edition, Prentice Hall, Englewood Cliffs, New Jersey.

Johnston, H.R. and Vitale, M.R. (June 1988). Creating competitive advantage with interorganisational information systems. Management Information Systems Quarterly.

pp. 153-165.

Jones, J. Et. Al. (2001). Feds enlist industry in IT asset protection. InfoWorld. Volume Twenty-Three, Number Forty-Two, p. 3.

Julian, T. Et. Al. (January 1999). Turning security on its head. The Forrester Report. Volume Thirteen, Number Two, Cambridge, Massachusetts.

Kabay, M.E. (2002). Anonymity and Identity in Cyberspace. In Computer Security Handbook, Fourth Edition, Eds. Bosworth, S. and Kabay, M.E., pp. 53.1-53.23, John Wiley & Sons, Inc., New York, New York.

Kahan, D.M. (1997). Between economics and sociology: The new path of deterrence. Michigan Law Review. Volume Ninety-Five, Number Eight, pp. 2247-2497.

Kalil, T. (1995). Public policy and the national information infrastructure. Business Economics. Volume Thirty, Number Four, pp. 15-18.

Kambil, A. and Ginsburg, M. (1998). Public access web information systems: Lessons from the Internet EDGAR. Communications of the ACM. Volume Forty-One, Number Seven, pp. 91-97.

Kaminski, J. (2001). Virus trends for 2002. Computer Associates International, Inc. Australia.

Karake, Z.A. (1992). Information Technology and Management Control, Praeger Publishing, Westport, Connecticut.

Karresand, M. (2003). A proposed taxonomy of software weapons. FOI Swedish Defence Research Agency, Scientific Report Number FOI-R-0840-SE, Linköping, Sweden.

Kaufman, C., Perlman, R. and Speciner, M. (1995). Network Security: Private Communication in a Public World, Prentice-Hall PTR, Upper Saddle River, New Jersey.

Kiefer, J.J. (2001). Urban terrorism: Strategies for mitigating terrorist attacks against the domestic urban environment, Ph.D. Dissertation, Old Dominion University.

Kirk, J. and Miller, M.A. (1986). Reliability and Validity in Qualitative Research, Sage Publications, Newbury Park, California.

Klein, H.K. and Myers, M.D. (2001). A Classification Scheme for Interpretive Research in Information Systems, In Trends in the Choice of Qualitative Methods. Ed. Trauth, E.M., pp. 218-239, Idea Group Publishing, Hershey, Pennsylvania.

Kovacich, G.L. (1999). I-way robbery: Crime on the Internet. Computers & Security. Volume Eighteen, Number Three, pp. 211-220.

Kovacich, G.L. and Boni, W.C. (2000). High-Technology Crime Investigator's Handbook, Butterworth Heinemann, Boston, Massachusetts.

Krippendorff, K. (1986). Information Theory: Structured Models for Qualitative Data, Sage Publications, Newbury Park, California.

Krippendorff, K. (1984). Content Analysis: An Introduction to Its Methodology, Sage Publications. Newbury Park, California.

Kumamoto, H. and Henley, E.J. (1996). Probabilistic Risk Assessment and Management for Engineers and Scientists, Second Edition, Institute of Electrical and Electronics Engineers, Inc., New York, New York.

Kumar, K. and Van Dissel, H.G. (1996). Sustainable collaboration: Managing conflict and cooperation interorganisational systems. Management Information Systems Quarterly. Volume Twenty, Number Three, pp. 279-300.

Kumar, R. and Crook, C.W. (1999). A multi-disciplinary framework of the management of interorganisational systems. Database for Advances in Information Systems. Volume Thirty, Number One, pp. 22-37.

Kuo, G.S. and Lin, J.P. (1998). New design concepts for an intelligent Internet: Addressing security requirements, performance efficiency, and operational simplicity in a high-speed network environment. Communications of the ACM. Volume Forty-One, Number Eleven, pp. 93-98.

Land, F. (1992). The Information Systems Domain. In Information Systems Research: Issues Methods and Practical Guidelines, Ed. Galliers, R.D., pp. 6-13, Blackwell Scientific Publications, Oxford, United Kingdom.

Landwehr, C.E. Et. Al. (1994). A taxonomy of computer program security flaws. ACM Computer Surveys. Volume Twenty-Six, Number Three, pp. 211-254.

Lang, J. (27 April 1998). Leveraging the legacy - capturing web transactions requires a robust and mature infrastructure that ensures data integrity. Information Week. pp. 48-52.

Larsen Jr., G.A. and Resnick, B.G. (March 1999). A performance comparison between cross-sectional stochastic dominance and traditional event study methodologies. Review of Quantitative Finance and Accounting. Volume Twelve, Number Two, pp. 103-112.

Lategan, F.A. and Olivier, M.S. (2001). On granting limited access to private information. ACM Computer Surveys. pp. 21-25.

Lavine, M.K. (2003). Protecting the United States homeland against information warfare and cyberterrorism. *Proceedings of the Second European Conference on Information Warfare and Security, Reading, England,* pp. 24-28.

Lawson, S. (26 January 1998). Waiting for VPN's payoff. InfoWorld. pp. 26-28.

Lawson, S. (1 June 1998). ICSA provides forum for testing security. InfoWorld. pp. 46-51.

Lee, A.S. (2001). Challenges to Qualitative Researchers in Information Systems, In Trends in the Choice of Qualitative Methods. Ed. Trauth, E.M., pp. 240-270, Idea Group Publishing, Hershey, Pennsylvania.

Lee, P. (January-April 2002). Behavioural model of online purchasers in e-commerce environment. Electronic Commerce Research. Volume Two, Numbers One-Two, pp. 75-85.

Lee, S. and Leifer, R.P. (1992). A framework for linking the structure of information systems with organizational requirements for information sharing. Journal of Management Information Systems. Volume Eight, Number Four, pp. 27–36.

Leinwand, A. and Conroy, K.F. (1996). Network Management: A Practical Perspective, Second Edition, Addison-Wesley, Reading, Massachusetts.

Lemant, O. (June 2001). Risk as a tripod. Internal Auditor. Volume Thirty-Eight, Number Three, pp. 39-43.

Leung, J.W.K. and Lai, K.K. (May 1997). A structured methodology to build discrete-event simulation models. Asia-Pacific Journal of Operational Research. Volume Fourteen, Number One, pp. 19-37.

Lewis, I. (2001). Logistics and electronic commerce: An interorganisational systems perspective. Transportation Journal. Volume Forty, Number Four, pp. 5-13.

Lewis, I. and Talalayevsky, A. (2000). Third-party logistics: Leveraging information technology. Journal of Business Logistics. Volume Twenty-One, Number Two, pp. 173-186.

Lewis-Beck, M.S. (1995). Data Analysis: An Introduction, Sage Publications, Thousand Oaks, California.

Lipson, H.F., Mead, N.R. and Moore, A.P. (21 August 2001). A risk-management approach to the design of survivable COTS-based systems. ISW-2001 Position Paper, pp. 1-4.

Locke, K. (2001). Grounded Theory in Management Research, Sage Publications, London, England.

Locke, L.F., Spirduso, W.W. and Silverman, S.J. (1992a). Developing Proposals: Some Common Problems. In Information Systems Research: Issues Methods and Practical Guidelines, Ed. Galliers, R.D., pp. 182-209, Blackwell Scientific Publications, Oxford, United Kingdom.

Locke, L.F., Spirduso, W.W. and Silverman, S.J. (1992b). Research Proposals: Function and Content, In Information Systems Research: Issues Methods and Practical Guidelines, Ed. Galliers, R.D., pp. 167-181, Blackwell Scientific Publications, Oxford, United Kingdom.

Loder, T., Alstyne, M.V., and Wash, R. (2004). An economic answer to unsolicited communication. *Proceedings of the Fifth ACM Conference on Electronic Commerce, New York, New York*, pp. 40-50.

Lok, C. (2004). Worm Guards. Technology Review. Volume 107, Number Six, p. 77.

Loudon, K.C. and Loudon, J.P. (2000). Management Information Systems: Organisation and Technology in the Networked Enterprise, Sixth Edition, Prentice-Hall, Upper Saddle River, New Jersey.

Lucas, H.C. Jr. (1992). The Analysis, Design and Implementation of Information Systems, Fourth Edition, McGraw-Hill, Inc., New York, New York.

Lukasik, S.J., Greenberg, L.T., and Goodman, S.E. (June 1998). Protecting an invaluable and ever-widening infrastructure. Communications of the ACM. Volume Forty-One, Number Six, pp. 11-16.

Mackenzie, E. and Goldman, K. (2000). Computer abuse, information technologies, and judicial affairs. *Proceedings of the 28th Annual SIGUCCS Conference on User Services, October 29 – November 1, 2000, Richmond, Virginia*, pp. 170-176.

MacKinlay, A.C. (March 1997). Event studies in economics and finance. Journal of Economic Literature. Volume Thirty-Five, Number One, pp. 13-39.

Maiwald, E. (2000). Network Security: A Beginner's Guide, Osborne/McGraw-Hill, Berkeley, California.

Malka, Y. and Ziv, A. (1998). Design reliability- estimation through statistical analysis of bug discovery data. *Proceedings of the Digital Arts and Culture Conference 1998, San Francisco, CA,* pp. 644-649.

Manion, M. and Goodrum, A. (June 2000). Terrorism or civil disobedience: Toward a hacktivist ethic. Computers and Society. pp. 14-19.

Mann, P.H. (1985). Methods of Social Investigation, Basil Blackwell, Inc., New York, New York.

Marcella, A.J. Jr., Stone, L. and Sampias, W.J. (1998). Electronic Commerce: Control Issues for Securing Virtual Enterprises, The Institute of Internal Auditors, Altamonte Springs, Florida.

Markham, T. (June 1997). Examining IPv6's IPSEC security layer, Doctor Dobb's Journal. Available on-line at http://www.acm.org/pubs/articles/journals/drdobbs/1997/9706/9706h/9706h.htm. Accessed on 6 June 2001.

Materson, D. (2005). Virus control: Dodging Spyware Infections. Franchising World. Volume Thirty-Seven, Number Seven. pp. 59-60.

Matlis, J. (2006). Internet2. Computerworld. Volume Forty, Number Thirty-Five, p. 30.

McClure, S., Scambray, J. and Kurtz, G. (1999). Hacking Exposed: Network Security Secrets and Solutions, Osborne/McGraw-Hill, Berkeley, California.

McDonagh, J. and Coghlan, D. (2001). Exploiting ICT based capabilities the challenge of integrated change. Organisational Development Journal. Volume Nineteen, Number One, p. 3.

McDonald, S. (29 March 1999). Spotlight: corporate e-commerce kicks into gear. The Industry Standard. p. 46.

McNamee, D. and Selim, G.M. (1998). Risk Management: Changing the Internal Auditor's Paradigm, The Institute of Internal Auditors Research Foundation, Altamonte Springs, Florida.

McWilliams, A. and Siegel, D. (June 1997). Event studies in management research: Theoretical and empirical issues. Academy of Management Journal. Volume Forty, Number Three, pp. 626-657.

Messmer, E. (29 March 2004). XML-based standard faces trust issue. Network World. p. 8.

Metchnick, E. (1997). A typology of crime on the Internet. Security Management. Issue Number Nine, pp. 27-31.

Miller, R.G. (1986). Beyond ANOVA: Basic Applied Statistics, John Wiley & Sons, Inc., New York, New York.

Moore, D. Et. Al. (2006). Inferring Internet denial-of-service activity. ACM Transactions on Computer Systems. Volume Twenty-Four, Number Two. pp. 115-139.

Moore, K. and Birkinshaw, J. (1998). Managing knowledge in global service firms: Centres of excellence. The Academy of Management Executive. Volume Twelve, Number Four, pp. 81-92.

Moreau, T. (1999). The emergence of a legal framework for electronic transactions. Computers & Security. Volume Eighteen, Number Five, pp. 423-428.

Morgan, G. and Smircich, L. (1980). The case for qualitative research. Academy of Management Review. Volume Five, Issue Four, pp. 491-500.

Morris, J, (2000). Private communication.

Mumford, E. (2001). Action Research: Helping Organizations to Change, In Trends in the Choice of Qualitative Methods. Ed. Trauth, E.M., pp. 46-77, Idea Group Publishing, Hershey, Pennsylvania.

Murphy, E.F., Gordon, J.D. and Mullen, A. (March 2004). A preliminary study exploring the value changes taking place in the United States since the September 11, 2001 terrorist attack on the World Trade Centre in New York. Journal of Business Ethics. Volume Fifty, Number One, pp. 81-96.

Mutch, A. and Ventura, K. (Summer 2003). The promise of Internet 2. Library Journal. pp. 14-16.

Myers, M.D. (1997). Qualitative research in information systems. Management Information Systems Quarterly. Volume Twenty One, Number Two, pp. 241-242.

Naccarato, J.L. and Neundorf, K.A. (May/June 1998). Content analysis as a predictive methodology: Recall, readership and evaluations of business-to-business print advertising. Journal of Advertising Research. pp. 19-33.

Nachenberg, C. (1997). Computer virus-antivirus co-evolution. Communications of the ACM. Volume Forty, Number One, pp. 46-51.

National Information Infrastructure Task Force Issues Preliminary Report. (1994). Bulletin of the American Society for Information Science, Volume Twenty, Number Six, pp. 6-13.

Naugle, M. (1999). Network Protocols, McGraw-Hill, New York, New York.

Nazem, S.M. (1988). Applied Time Series Analysis for Business and Economic Forecasting, Marcel Dekker, New York, New York.

Nelms, C. (1999). Internet e-mail risks and concerns. Computers & Security. Volume Eighteen, Number Five, pp. 409-418.

Neter, J., Wasserman, W. and Whitmore, G.A. (1973). Fundamental Statistics for Business and Economics, Fourth Edition. Allyon and Bacon, Boston, Massachusetts.

Neumann, P.G. Et. Al. (2007). Risks related to the public in computers and related systems. SRI International Online Publication. Available on-line at: http://www.csl.sri.com/neumann Accessed on 10 March 2007.

Newman, I. and Benz, C.R. (1998). Qualitative-Quantitative Research Methodology: Exploring the Interactive Continuum, Southern Illinois Press, Carbondale, Illinois.

Newman, M.E.J., Forrest, S., and Balthrop, J. (2002). Email networks and the spread of computer viruses. The American Physical Society. pp. 1-4.

Ohlson, K. (2000). 'Love' virus costs approaching $7B, research firm says. Available on-line at http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_ST044810-,00.html. Accessed on 14 January 2002.

Olle, T.W. Et. Al. (1991). Information Systems Methodologies: A Framework for Understanding, Second Edition, Addison-Wesley Publishing, Wokingham, England.

Olson, W.K. (2001). Urban information systems technology: Tools and policy implications for the military and law enforcement in the 21st century, Ph.D. Dissertation, George Mason University.

Oppliger, R. (May 1997). Internet security: Firewalls and beyond. Communications of the ACM. Volume Forty, Number Five, pp. 92-102.

O'Reillcy, J. Et. Al. (28 September 1998). Virtual private networking: Finding opportunity amid immaturity. Strategic Analysis Report. Gartner Group, Stamford, Connecticut.

Orlikowski, W.J. (1993). CASE tools as organizational change: Investigating incremental and radical changes in systems development. Management Information Systems Quarterly. Volume Seventeen, Number Three, pp. 309-340.

Ostrom, C.W. (1990). Time Series Analysis: Regression Techniques, Second Edition, Sage Publications, Thousand Oaks, California.

Padberg, F. (2002). Empirical interval estimates for the defect content after an inspection. *Proceedings of the 24th International Conference on Software Engineering, Orlando, Florida,* pp. 58-68.

Palmer, G., (2000). The new spectacle of crime, In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Eds. Thomas, D. & Loader, B.D., pp. 85-102, Routledge, London.

Panda, B. and Giordano, J. (July 1999). Defensive information warfare. Communications of the ACM. Volume Forty-Two, Number Seven, pp. 31-32.

Pandit, N.R. (1996). The creation of theory: A recent application of the grounded theory method. The Qualitative Report. Volume Two, Number Four, Start page: 12.

Pappalardo, D. (2000). Avoiding future denial-of-service attacks. Available on-line at http://www.cnn.com/2000/TECH/computing/02/23/isp.block.idg/ Accessed on 14 January 2002.

Park, J.S. (1999). Secure attribute services on the web. Ph.D. Dissertation, George Mason University.

Parker, D.B. (1998). Fighting Computer Crime: A New Framework for Protecting Information, John Wiley & Sons, Inc., New York, New York.

Parker, M.M. and Benson, R.J. (1988). Information Economics, Prentice-Hall, Upper Saddle River, New Jersey.

Parker, X.L. (2001). An E-Risk Primer, The Institute of Internal Auditors Research Foundation, Altamonte Springs, Florida.

Parzinger, M.J. and Nath, R. (2000). A study of the relationships between total quality management implementation factors and software quality. Total Quality Management. Volume Eleven, Number Three, pp. 353-371.

Pervan, G.P. and Klass, D.J. (1992). The Use and Misuse of Statistical Methods in Information Systems Research, In Information Systems Research: Issues Methods and Practical Guidelines, Ed. Galliers, R.D., pp. 209-229, Blackwell Scientific Publications, Oxford, United Kingdom.

Peters, K.M. (2003). Five homeland security hurdles. Government Executive. Volume Thirty-Five, Number Two, pp.18-22.

Pfleeger, C.P. and Pfleeger, S. (2002). Security in Computing, Third Edition, Prentice Hall. Upper Saddle River, New Jersey.

Philippsohn, S. (2001). Trends in cybercrime: An overview of current financial crimes on the internet. Computers & Security. Volume Twenty, Number One, pp. 53-69.

Phillips, C. and Swiler, L.P. (1999). A graph-based system for network-vulnerability analysis. ACM. pp. 71-79.

Phillips, E.H. (1998). Data-sharing focus of GAIN meeting. Aviation Week & Space Technology. Volume One Hundred Forty-Nine, Number Eighteen, p. 55.

Phillips, J.T. (1994). The national information infrastructure. ARMA Records Management Quarterly. Volume Twenty-Eight, Number Three, pp. 48-52.

Piazza, P. (2002). Code wars: Virus attack trends. American Society for Industrial Security. Volume Forty-Six, Number Three 46, Issue 3, Start page: 40.

Platt, F.N. (2002). Protecting the Information Infrastructure. In Computer Security Handbook, Fourth Edition, Eds. Bosworth, S. and Kabay, M.E., pp. 15.1-15.46, John Wiley & Sons, Inc., New York, New York.

Polat, N. (Spring 1999). International law, the inherent instability of the international system and international violence. Oxford Journal of Legal Studies, Volume Nineteen, pp. 51-70.

Potter, W.J. and Levine-Donnerstein, D. (1999). Rethinking validity and reliability in content analysis. Journal of Applied Communication Research. Volume 27, pp. 258-284.

Pounder, C. (1999). The revised version of BS7700 – so what's new? Computers & Security. Volume Eighteen, Number Four, pp. 307-311.

Pozzo, M.M. and Gray, T.E. (1987). An Approach to Containing Computer Viruses. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp. 273-286, Van Nostrand Reinhold, New York, New York.

Premkumar, G.P. (Summer 2000). Interorganisation systems and supply chain management: An information processing perspective. Information Systems Management. pp. 56-69.

PricewaterhouseCoopers, LLP. (1998). Technology Forecast: 1999. Menlo Park, California.

Puketza, N.J. (2000). Approaches to computer security: The effects of differing information, Ph.D. Dissertation, University of California at Davis.

Quarantiello, L.E. (1997). Cybercrime, LimeLight Books, Lake Geneva, Wisconsin.

Rada, R. and Ketchell, J. (2000). Standardising the European information society. Communications of the ACM. Volume Forty-Three, Number Three, pp. 21-25.

Ranum, M.I. Et. Al. (1998). Implementing a generalised tool for network monitoring. Information Security Technical Report. Volume Three, Number Four, pp. 53-64.

Rathmell, A. (2000). Information warfare and sub-state actors: An organisational approach, In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Eds. Thomas, D. & Loader, B.D., pp. 221-233, Routledge, London.

Rathmell, A. (2001). Protecting critical information infrastructures. Computers & Security. Volume Twenty, Number One, pp. 43-52.

Rayport, J.F. and Jaworski, B.J. (2001). E-Commerce, McGraw-Hill/Irwin, New York, New York.

Recent Growth Trends in OECD Countries. (June 2000). Issue Sixty-Seven, pp. 173-192.

Reidel, R. (2000). Research Strategies for Secondary Data: A Perspective for Criminology and Criminal Justice, Sage Publications, Thousand Oaks, California.

Reinares, R. (1998). Democratic regimes, internal security policy and the threat of terrorism. Australian Journal of Politics and History. Volume Forty-Four, Number Three, pp. 351-371.

Reitinger, P.R. (2000). Encryption, anonymity and markets: law enforcement and technology in a free market virtual world, In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Eds. Thomas, D. & Loader, B.D., pp. 85-102, Routledge, London.

Renecker, M.A. (1993). A qualitative study of information seeking among members of an academic community: Methodological issues and problems. Library Quarterly. Volume Sixty-Three, Number Four, pp. 487-507.

Rhodes, A. (1998). Petroleum firms share information openly to meet year 2000 deadline. Oil & Gas Journal. Volume Ninety-Six, Number Forty, pp. 23-34.

Rich, M.S. (2001). Internet trends and awareness in information systems security. Ph.D. Dissertation, University of Sarasota.

Riggins, F.J., Kriebel, C.H. and Mukhopadhyay, T. (1994). The growth of interorganisational systems in the presence of network externalities. Management Sciences. Volume Forty, Number Eight, pp. 984-999.

Riggins, F.J. and Rhee, H.S. (1998). Toward a unified view of electronic commerce. Communications of the ACM. Volume Forty-One, Number Ten, pp. 88-95.

Rine, D. (1978). Possibility theory: As a means for modelling computer security and protection. *Proceedings of the Eighth International Symposium on Multiple-Valued Logic, Rosemont, Illinois*, pp. 276-286.

Rittenbruch, M., Kahler, H. and Cremers, A.B. (2000). Supporting cooperation in a virtual organisation. *Proceedings of the 1998 International Conference on Information Systems, Helsinki, Finland*, pp. 30-38.

Robb, D. (1999). Developing firewall technology: Hardwall white paper. Computers & Security. Volume Eighteen, Number Six, pp. 471-478.

Roberts, C.W. (2000). A conceptual framework for quantitative text analysis. Quality & Quantity. Volume Thirty-Four, pp. 259-274.

Roberts, P. (10 May 2004). Sasser, a warning of things to come. Infoworld. p.17.

Rochlis, J.A. and Eichin, M.W. (1989). With Microscope and Tweezers: The Worm from MIT's Perspective. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp. 228-245, Van Nostrand Reinhold, New York, New York.

Roullier, C. (1998). Switzerland opens limited access to supervisory information. International Financial Law Review. Volume Seventeen, Number Six, pp. 47-51.

Roussel, A. (27 September 1997). Globalising commerce over the Internet, Point-To-Point. Gartner Group, Stamford, Connecticut.

Rubach, M. and Picou, A. (2005). The enactment of corporate governance guidelines: An empirical examination. Corporate Governance. Volume Five, Number Five, pp. 30-37.

Rubenstein, E. (1996). The economics of crime. Executive Speeches. Volume Ten, Number Four, pp. 26-30.

Rubio, M. (1998). Violence, organised crime, and the criminal justice system in Columbia. Journal of Economic Studies. Volume Thirty-Two, Number Two, pp. 605-610.

Rumizen, M. (1998). Site visit: How Buckman Laboratories shared knowledge sparked a chain reaction. The Journal for Quality and Participation. Volume Twenty-One, Number Four, pp. 34-38.

Salamone, S. (March 23, 1998). The virtues of firewalls. Internet Week. pp. 23-28.

Salles, E. J., Et. Al. (2002). Security of runtime extensible virtual environments. *Proceedings of the 4th International Conference on Collaborative Virtual Environments, Bonn, Germany,* pp. 97-104.

Samuelson, P. (1989). Can Hackers be Sued for Damages Caused by Computer Viruses? In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp.111-116, Van Nostrand Reinhold, New York, New York

Santos, R.A. (1999). Internet security, Information Systems Control Journal. Volume One, January/February Issue, pp. 33-37.

Saull, R. (2000). The IT balanced scorecard – a roadmap to effective governance of a shared services IT organisation. Information Systems Control Journal. Volume Two, March/April Issue, pp. 31-38.

Sawyer, S. (2001). Analysis by Long Walk: Some Approaches to the Synthesis of Multiple Sources of Evidence, In Trends in the Choice of Qualitative Methods. Ed. Trauth, E.M., pp. 163-190, Idea Group Publishing, Hershey, Pennsylvania.

Saydjari, O.S. (2004). Cyber defence: Art to science. Communications of the ACM. Volume Forty-Seven, Number Three. pp. 53-57.

Schnaubelt, C.M. (2000). Deterring international terrorism: The effectiveness of United States Policy: 1970-1990. Ph.D. Dissertation, University of California, Santa Barbara.

Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons, Inc., New York, New York.

Schneier, B. and Ellison, C.M. (Winter 2000). Ten risks of public key infrastructure. Computer Security Journal. Volume Sixteen, Number One, pp. 1-7.

Schneier, B. (1999). The trojan horse race. Communications of the ACM. Volume Forty-Two, Number Nine. p.128.

Schou, C. D. and Trimmer, K. J. (2004). Editorial preface: Information assurance and security. Journal of Organisational and End User Computing. Volume Sixteen, Number Three. pp. i-vii.

Schultz, E. and Hofmeyr, S. (29 March 2004). Face-off: Is patch management the best protection against vulnerabilities? Network World. Volume Twenty-One, Number Thirteen. p. 44.

Schultze, U. (2001). Reflexive Ethnography in Information Systems Research, In Trends in the Choice of Qualitative Methods. Ed. Trauth, E.M., pp. 78-103, Idea Group Publishing, Hershey, Pennsylvania.

Schwab, D.P. (1999). Research Methods for Organisational Investigation, Lawrence Erlbaum Associates, Mahwah, New Jersey.

Schwartau, W. (November 1997). What exactly is information warfare? Part Three. Network Security. pp. 12-18.

Schwartzman, H.B. (1993). Ethnography in Organisations, Sage Publications, Newbury Park, California.

Science and Technology Throttled at Birth - Computer Viruses. (2002). The Economist. London. Volume Three Hundred Sixty Five, Issue Number Eight Thousand Three Hundred. Start page 98.

Seale, C. (1999). The Quality of Qualitative Research, Sage Publications, London, England.

Sekar, R. Et. Al. (November 1999). A high-performance network intrusion detection system. *Proceedings of the 1999 CCS Conference, Singapore,* pp. 8-17.

Sekar, R. Et. Al. (2002). Specification-based anomaly detection: a new approach for detecting network intrusions. *Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC.* pp. 265-274.

Sethi, V. and King. W.R. (1991). Construct measurement in information systems research: An illustration in strategic systems. Decision Sciences. Volume Twenty-Two, pp. 455-469.

Sharpe, B. and Stefek, Z., (2004). CTCP technology forward look. UK OST Foresight Cyber Trust & Crime Prevention Project. pp. 1-51.

Shaw, I.F. (1999). Qualitative Evaluation, Sage Publications, London, England.

Shelly, L.I. (1998). Crime and corruption in the digital age. Journal of International Affairs. Volume Fifty-One, Number Two, pp. 605-620.

Silverman, D. (2001). Interpreting Qualitative Data, Second Edition, Sage Publications, London, England.

Simon, S. and Benjamin, D. (Spring 2000). America and the new terrorism. Survival. Volume Forty-Two, Number One, pp. 59-75.

Simpson, P. (September 2001). Next generation malware. Information Security Bulletin. pp. 15-19.

Singh, P.K. and Lakhotia, A. (2002). Analysis and detection of computer viruses and worms: An annotated bibliography. ACM SIGPLAN Notices. Volume Thirty Seven, Number Two, pp. 29-35.

Smith, A.D. (2005). Exploring radio frequency identification technology and its impact on business systems. Information Management and Computer Security. Volume Thirteen, Number One, pp. 16-28.

Smith, R.E. (2001). Cost profile of a highly assured, secure operating system. ACM Transactions on Information and System Security. Volume Four, Number One, pp. 72-101.

Snellen, I. (2001). ICTs, bureaucracies, and the future of democracy. Communications of the ACM. Volume Forty-Four, Number One, pp. 45-48.

Soo Hoo, K. J. (2000). How much is enough: A risk management approach to computer security, Ph.D. Dissertation, Stanford University.

Spafford, E.H., Heaphy, K.A., and Ferbrache, D.J. (1989). What is a Computer Virus? In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp.29-42, Van Nostrand Reinhold, New York, New York.

Stallings, W. (2000). Network Security Essentials: Applications and Standards, Prentice-Hall, Upper Saddle River, New Jersey.

Steinauer, D.D., Wakid, S.A. and Rasberry, S. (1997). Trust and traceability in electronic commerce. Standard View. Volume Five, Number Three, pp. 118-124.

Steinke, S. (April 1998). State of the platforms. Network Magazine. pp. 49-64.

Steinmueller, W.E. (2001). ICTs and the possibilities for leapfrogging by developing countries. International Labour Review. Volume One Hundred Forty, Issue Two, pp. 193-210.

Stevens, T. (2001). Cyber-terrorists under attack. Industry Week. Volume Two Hundred Fifty, Number Two, p. 11.

Storey, V.C. Et. Al. (2000). A conceptual investigation of the e-commerce industry. Communications of the ACM. Volume Forty-Three, Number Seven, pp. 117-123.

Strauss, A. and Corbin J. (1998). Basics of Qualitative Research, Second Edition, Sage Publications, Thousand Oaks, California.

Stubbs, B. and Hoffman, L.J. (1989). Mapping the Virus Battlefield: An Overview of Personal Computer Vulnerabilities to Virus Attack. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp.143-158, Van Nostrand Reinhold, New York, New York.

Stymiest, B. (1996). Providing security for UNIX systems. Information Management & Computer Security. Volume Four, Number Two, pp. 18-26.

Subramani, M. and Walden, E. (June 2001). The impact of e-commerce announcements on the market value of firms. Information Systems Research. Volume Twelve, Number Two, pp. 135-154.

Suomi, R. (1988). Inter-organisational information systems as a company resource. Information & Management. Volume Fifteen, Number Two, pp. 105-113.

Symantec Antivirus Research Centre. (2005). Learn more about viruses and worms. Available on-line at http://securityresponse.symantec.com/avcenter/reference/worm.vs.virus.pdf. Accessed on 14 January 2005.

Tan, M. and Teo, T.S.H. (2000). Factors influencing the adoption of Internet banking. Journal of the Association for Information Systems. Volume One, Number Five, pp. 1-42.

Tasnarkkori, A. and Teddie, C. (1998). Mixed Methodology: Combining Qualitative and Quantitative Approaches, Sage Publications, Thousand Oaks, California.

Tavani, H. T. (2000). Defining the boundaries of computer crime: Piracy, break-ins, and sabatoge in cyberspace. Computers and Society. pp. 3-9.

Taylor, D. and Berg, T. (25 September 1995). The business value of electronic commerce. Strategic Analysis Report. Gartner Group, Stamford, Connecticut.

Taylor, P. (2000). Hackers – cyberpunks or microserfs?, In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Eds. Thomas, D. & Loader, B.D., pp. 17-35, Routledge, London.

Teich, A. Et. Al. (1999). Anonymous communication policies for the internet: Results and recommendations of the AAAS conference. The Information Society. Volume Fifteen, Number Two, pp. 71-77.

Tenenbaum, J.M. (1998). WISs and electronic commerce. Communications of the ACM. Volume Forty-One, Number Seven, pp. 89-90.

Terhune, E. (24 February 1998). Extranet security: Do we need a VPN?. Key Issue Analysis, Gartner Group, Stamford, Connecticut.

Tevis, J.J. and Hamilton, J. A. (2004). Methods for the prevention, detection and removal of software security vulnerabilities. *Proceedings of the 42nd Annual Southeast Regional Conference, Huntsville, Alabama,* pp. 197-202.

Tewksbury, D., Weaver, A.J. and Maddex, B.D. (2001). Accidentally informed: Incidental news exposure on the world wide web. Journalism and Mass Communication Quarterly. Volume Seventy-Eight, Number Three, pp. 533-554.

Thibodeau, P. (25 June 2002). Study: Buggy software costs users, vendors nearly $60B annually. Computerworld. Start page: 32.

Thimbleby, H., Anderson, S., and Cairns, P. (1999). A framework for modeling trojans and computer virus infection. Computer Journal. Volume Forty-One, Number Seven, pp. 444-458.

Thomas, D. (2000). Criminality on the electronic frontier: corporality and the judicial construction of the hacker, In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Eds. Thomas, D. & Loader, B.D., pp. 15-16, Routledge, London.

Thompson, H., Whittaker, J., and Mottay, F. (2002). Software security vulnerability testing in hostile environments. *Proceedings of the 2002 ACM Symposium on Applied Computing, Madrid, Spain.* pp. 260-264.

Thompson, R. (2002). Malicious Code. In Computer Security Handbook, Fourth Edition, Eds. Bosworth, S. and Kabay, M.E., pp. 9.1-9.20, John Wiley & Sons, Inc., New York, New York.

Tippett, P. (2002). The Future of Information Security. In Computer Security Handbook, Fourth Edition, Eds. Bosworth, S. and Kabay, M.E., pp. 54.1-54.18, John Wiley & Sons, Inc., New York, New York.

Tope, S.W. (2005). Investigation into changing trends in vulnerabilities and their effects. MRes. Thesis Project, University of Plymouth, Plymouth, UK.

Trauth, E.M. (2001). Choosing qualitative methods in IS research: Lessons learned, In Trends in The Choice of Qualitative Methods. Ed. Trauth, E.M., pp. 271-287, Idea Group Publishing, Hershey, Pennsylvania.

Trauth, E.M. (2001a). The choice of qualitative methods in IS research, In Trends in the Choice of Qualitative Methods. Ed. Trauth, E.M., pp.1-19, Idea Group Publishing, Hershey, Pennsylvania.

Travassos, G.H., Et. Al.(1999). Detecting defects in object oriented designs: Using reading techniques to increase software quality. *Proceedings of the 14th ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages, and Applications, Denver, Colorado,* pp. 47-56.

Triboedeau, P. (18 September 2000). Federal agencies get poor grades for security. Computerworld. pp. 2-6.

Tricker, R.I. (1992). The management of organisational knowledge, In Information Systems Research: Issues Methods and Practical Guidelines. Ed. Galliers, R.D., pp. 14-27, Blackwell Scientific Publications, Oxford, United Kingdom.

Trjanne, P. (1995). The GII: Moving towards implementation. Telecommunications. Volume Twenty-Nine, Number Five, pp. 28-32.

Tse, K. (1997). Survey of internet security protocols. Masters Graduate Project, McGill University.

United States Critical Infrastructure Assurance Office. (17 November 1999). National Critical Infrastructure Protection A Case for Action. PCIE CIPP Review, Washington, D.C.

United States Department of Homeland Security. (2003). The National Strategy to Secure Cyberspace. Washington, D.C.

United States General Accounting Office. (2000). Critical Infrastructure Protection: Significant challenges in developing national capabilities. Report Number GAO-01-323. Washington, D.C.

United States General Accounting Office. (2001). Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities Report Number 01-323, Washington, D.C.

United States National Institute of Standards and Technology (1995). Putting the Information Infrastructure to Work: Report of the Information Infrastructure Task Force Committee on Applications and Technology. Washington, D.C.

United States National Institute of Standards and Technology. (2002). The Economic Impacts of Inadequate Infrastructure for Software Testing. RTI Project Number 7007.011. Washington, D.C.

United States National Security Agency (1999). SSE-CMM Executive Summary. Fort Meade, Maryland.

United States Presidential Decision Directive Number Sixty-Three. (May 1998). The Clinton Administration's Policy on Critical Infrastructure Protection. Washington, D.C.

United States White House. (16 October 2001). President George W. Bush. Executive Order on Critical Infrastructure Protection. Washington, D.C.

Urquhart, C. (2001). An encounter with grounded theory: Tackling the practical and philosophical issues, In Trends in the Choice of Qualitative Methods. Ed. Trauth, E.M., pp.104-140, Idea Group Publishing, Hershey, Pennsylvania.

Valantin, R. (1996). Global program initiative: Information policy research. Information Technology for Development. Volume Seven, Number Two, pp. 95-103.

Van Dijk, T.A. (1997). Discourse as Structure and Process, Sage Publications, Thousand Oaks, California.

Vatis, M.A. (2001). Cyber attacks during the war on terrorism: A predictive analysis, Institute for Security Technology Studies. Dartmouth College, New Hampshire.

Vidaver-Cohen, D. (1998). Moral climate in business firms: A conceptual framework for analysis and change. Journal of Business Ethics. Volume Seventeen, Number Eleven, pp. 1211-1226.

Vijayan, J. (12 July 2004). Worm wars. Computerworld. Volume Thirty-Eight, Number Twenty-Eight, pp. 21-22.

Voiskkounsky, A.E., Babaeva, J.D. and Smyslova, O.V. (2000). Attitudes towards computer hacking in Russia, In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Eds. Thomas, D. & Loader, B.D., pp. 56-84, Routledge, London.

VPN Enterprise Solutions Guide. (1998). 3Com Corporation, Santa Clara, California.

Wagner, D.A. (2000). Static analysis and computer security: New techniques for software assurance. Ph.D. Dissertation, University of California – Berkley.

Wagner, D. and Soto, P. (2002). Mimicry attacks on host-based intrusion detection systems. *Proceedings of the Ninth ACM Conference on Computers and Communication Systems, 18-22 November, Washington, D.C.*, pp. 255-264.

Walsh, M. (2002). Application Controls. In Computer Security Handbook, Fourth Edition, Eds. Bosworth, S. and Kabay, M.E., pp. 39.1-39.12, John Wiley & Sons, Inc., New York, New York.

Warren, J.D., Edelson, L.W. and Parker, X.A. (1997). Handbook of IT Auditing, WG&L/RIA Group, Boston, Massachusetts.

Weber, R. (2000). Information Systems Control and Audit, Prentice-Hall, Upper Saddle River, New Jersey.

Weber, R.P. (1990). Basic Content Analysis, Second Edition, Sage Publications, Newbury Park, California.

Weber, R.P. (1984). Computer-aided content analysis: A short primer. Qualitative Sociology. Spring/Summer Issue, pp. 126-147.

Weller, S.C. and Romney, A.K. (1988). Systematic Data Collection, Sage Publications, Newbury Park, California.

West, M. and Purchase, E. (13 January 1999). Electronic commerce platforms and applications, Strategic Analysis Report, Gartner Group, Stamford, Connecticut.

Whine, M. (2000). Far right extremists on the Internet, In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Eds. Thomas, D. & Loader, B.D., pp. 234-250, Routledge, London.

White, A.D. and Witt, R. (2001). What we spend and what we get: Public and private provision of crime prevention and criminal justice. Fiscal Studies. Volume Twenty-Two, Number One, pp. 1-40.

White, S.R., Chess, D.M., and Chengi, J.K. (1989). Coping with Computer Viruses and Related Problems. In Rogue Programs: Viruses, Worms, and Trojan Horses, Ed. Hoffman, L.J., pp. 7-28, Van Nostrand Reinhold, New York, New York.

Whiting, R. and Chabrow, E. (8 October 2001). Safety in sharing. Information Week. Number Eight Hundred and Fifty-Eight, pp. 20-22.

Whittaker, J. (2000). What is software testing: And why is it so hard? Software IEEE. Volume Seventeen, Number One, pp. 70-79.

Whitten, D. Et. Al. (27 August 1997). The internet, intranets and extranets: IT paradigm, paradise or pariah? Strategic Analysis Report. Gartner Group, Stamford, Connecticut.

Whybrow, M. (1995). Bridging the gaps. Information Management & Computer Security. Volume Three, Number One, pp. 4-6.

Wilensky, H.L. (1997). Social science and the public agenda: Reflections on the relation of knowledge in the United States and abroad. Journal of Health Politics, Policy and Law. Volume Twenty-Two, Number Five, pp. 1241-1265.

Williams, J.W. (1997). Terrorism as mass communication. Security Management. Volume Fourteen, Number Nine, pp. 213-215.

Wilson, R.T. and Bracheau, J.C. (1992). Key issues in information systems management: An international perspective, In Information Systems Research: Issues Methods and Practical Guidelines, Ed. Galliers, R.D., pp. 112-131, Blackwell Scientific Publications, Oxford, United Kingdom.

Wiseskera, D. and Jajodia, S. (2001). Policy algebras for access control: The prepositional case. *Proceedings of the 2001 CCS Conference, Philadelphia, Pennsylvania*, pp. 38-47.

Wolcott, H.F. (1990). Writing Up Qualitative Research, Sage Publications, Newbury Park, California.

Wood, M. Et. Al. (1997). Comparing and combining software defect detection techniques: A replicated empirical study. ACM SIGSOFT Software Engineering Notes. Volume Twenty-Two, Number Six, pp. 262-277.

Woodruff, T. (5 September 2000). Feds get 'F' in e-privacy: GAO reports. MSN Money Central. Available at http://moneycentral.msn.com/articles/news/capitol/5758.asp Accessed on 17 May 2001.

World Wide Web Consortium (2007). Semantic web activity statement. Available on-line at http://www.w3.org/2001/sw/Activity. Accessed on 10 March 2007.

Wright, A. (2001). Controlling risks of e-commerce content. Computers & Security. Volume Twenty, Number Two, pp. 147-154.

Wright, P.C. and Roy, C. (1999). Industrial espionage and competitive intelligence: One you do; one you do not. Journal of Workplace Learning. Volume Eleven, Number Two, pp. 53-59.

Wynn, E. (2001). Mobius transitions in the dilemma of legitimacy, In Trends in the Choice of Qualitative Methods. Ed. Trauth, E.M., pp. 20-44, Idea Group Publishing, Hershey, Pennsylvania.

Xie, Y. Et. Al. (2005). Worm Origin Identification Using Random Moonwalks. Carnegie Mellon University Working Paper.

Yao, W., Moody, K., and Bacon, J. (2001). A model of OASIS role-based access control and it support for active security. *Proceedings of the SACMAT 2001Conference, Chantilly, Virginia*, pp. 171-181.

Yasin, R. (27 March 1998). Firewall products: May not be ready for prime time. Internet Week. pp. 25-28.

Ye, N., Giordano, J. and Feldman, J. (2001). A process control approach to cyber attack detection. Communications of the ACM. Volume Forty-Four, Number Eight, pp. 76-82.

Yin, R.K. (1993). Applications of Case Study Research, Sage Publications, Thousand Oaks, California.

Zanaro, S., and Savaresi, S.M. (2004). Unsupervised learning techniques for an intrusion detection system. *Proceedings of the 2004 ACM Symposium on Applied Computing, Nicosia, Cyprus,* pp. 412-419.

Zboray, M. (23 January 1998). What's hot with VPNs for extranets in 1998. Key Issue Analysis. Gartner Group, Stamford, Connecticut.

Zhao, N., Yen, D.C. and Chang, I. (2004). Auditing in the e-commerce era. Information Management and Computer Security. Volume Twelve, Number Five, pp. 389-400.

Zhong, X. (1999). Security framework for management of distributed systems. MSc. Graduate Project, University of Western Ontario.

Zou, C., Gong, W., and Towsley, D. (2002). Code red worm propagation modelling and analysis. *Proceedings of the Ninth ACM Conference on Computer and Communications Security, Washington, D.C.*, pp. 138-147

SUPPLEMENTS SECTION

SUPPLEMENT ONE

CYBERNOTES NEWSLETTER

Number 2003-04

National Infrastructure Protection Center
CyberNotes

Issue #2003-04

February 24, 2003

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between February 5 and February 20, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Adalis Informa-tique[1]	Unix	D-Forum 1.0, 1.10, 1.11	A vulnerability exists in the '/includes/header.php3' and '/includes/footer.php3' scripts, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	D-Forum Remote File Include	High	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.

[1] SecurityFocus, February 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Aladdin Know-ledge Systems[2]	Windows 2000	eSafe Gateway 3.0, 3.5	A vulnerability exists because only viruses with the first 15 kb of the content stream are detected when eSafe is used with the Check Point Content Vectoring Protocol (CVP), which could let a remote malicious user send specially crafted malicious content that will bypass security mechanisms.	No workaround or patch available at time of publishing.	eSafe OPSEC CVP Virus Scanning Bypass	Medium	Bug discussed in newsgroups and websites.
Alt-N Technol-ogies[3]	Windows 95/98/NT 4.0/2000	MDaemon 2.8, 2.8.5, 3.0.3, 3.0.4, 3.1.1, 3.1.2, 3.5.0, 3.5.1, 3.5.4, 3.5.6, 5.0.7, 6.0.0, 6.0.5-6.0.7, 6.5.0	A vulnerability exists in the 'Form2Raw.exe' utility, which could let a remote malicious user send forged mail with spoofed headers.	No workaround or patch available at time of publishing.	Alt-N MDaemon/ WorldClient 'Form2Raw' Mail Header Spoofing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Andries Brouwer[4]	Unix	util-linux 2.11u, 2.11n	A vulnerability exists in the 'mcookie' utility because cookies may be generated in a predictable manner, which could let a malicious user obtain sensitive information.	**Mandrake:** http://www.mandrakesecure.net/en/ftp.php	Util-Linux 'mcookie' Utility	Medium	Bug discussed in newsgroups and websites.
APC[5]	Unix	apcupsd 3.8.5	A vulnerability exists in the 'log_event' function due to a programming error, which could let remote malicious user obtain root access and possibly execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/apcupsd/apcupsd-3.8.6.tar.gz?download	Apcupsd 'log_event' Remote Root Access	**High**	Bug discussed in newsgroups and websites.
Apple[6]	Unix (OS X)	MacOS X 10.2 (Jaguar), 10.2.1-10.2.3	A vulnerability exists in the TruBlueEnvironment emulator, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://docs.info.apple.com/article.html?artnum=70168	MacOS TruBlue Environment Variable Privilege Escalation CVE Name: CAN-2003-0088	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple[7]	Unix (OS X)	MacOS X 10.2 (Jaguar), 10.2.1-10.2.3	A vulnerability exits in 'iDrive' because the File Protocol allows a system administrator to log on as a normal user using administration login details, which could let a malicious user obtain sensitive information.	Upgrade available at: http://docs.info.apple.com/article.html?artnum=70168	Apple File Protocol iDrive Administrator Login CVE Name: CAN-2003-0049	Medium	Bug discussed in newsgroups and websites.

[2] Bugtraq, February 6, 2003.
[3] SecurityTracker Alert ID, 1006058, February 7, 2003.
[4] Mandrake Linux Security Update Advisory, MDKSA-2003:016, February 14, 2003.
[5] SecurityTracker Alert ID, 1006108, February 15, 2003.
[6] @stake, Inc. Security Advisory, February 14, 2003.
[7] Apple Security Update, 61798, February 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Aprelium Technol-ogies[8]	Windows, Unix	Abyss Web Server 1.0.7, 1.1.2	A vulnerability exists because failed authentication attempts are not logged and the number of failed authentication attempts to the administrative interface is not limited, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Abyss Web Server Failed Login Recording	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Bastille[9]	Unix	HP-UX Bastille B.02.00.00	A vulnerability exists in the Bastille Hardening System when used in conjunction with the HP-UX operating system and the Sendmail daemon, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6849AA	HP-UX Bastille sendmail.cf Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Benjamin Low[10]	Windows, Unix	CGI-Lite 2.0	A vulnerability exists in the escape_dangerous_chars() function because specially crafted input can be submitted that will bypass the code's security filtering mechanisms, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	CGI Lite escape_ dangerous_ chars()	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Bharat Mediratta [11]	Unix	Gallery 1.3.3	A vulnerability exists when the 'temp' and 'albums' directories are created and the way image files are managed due to unsafe file permissions, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Gallery Management Software Unsafe File Permissions	Medium	Bug discussed in newsgroups and websites.
BisonFTP [12]	Windows 95/98/NT 4.0	Bison Ftp Server V4R2	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user submits exceptionally long FTP commands such as 'cwd' or 'ls'; and a vulnerability exists when a 'ls' command is issued using the character sequence '@../', which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	BisonFTP Multiple Vulnerabilities	Low/ Medium (Medium if sensitive informa-tion can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
BitchX[13]	Multiple	IRC Client 75p3, 1.0 c20cvs, 1.0 c19, 1.0 c16	A Denial of Service vulnerability exists when a malicious user submits a malformed RPL_NAMREPLY numeric.	No workaround or patch available at time of publishing.	BitchX Malformed RPL_ NAMREPLY Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[8] Bugtraq, February 12, 2003.
[9] Hewlett-Packard Company Security Bulletin, HPSBUX0203-245, February 13, 2003.
[10] Bugtraq, February 11, 2003.
[11] SecurityTracker Alert ID, 1006066, February 10, 2003.
[12] immune advisory, February 17, 2003.
[13] Bugtraq, February 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Celestial Software [14]	Windows	Absolute Telnet 2.0, 2.11	A buffer overflow vulnerability exists due to insufficient bounds checking when the title bar is set by the client, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.celestialsoftware.net/telnet/beta_software.html	Absolute Telnet Title Bar Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit scripts have been published.
Cheeta Technol-ogies [15]	Windows	CheetaChat 6.5.10	A vulnerability exists because encrypted Yahoo! authentication credentials are stored in a local file, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CheetaChat Internal Browser Plaintext Password Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited using the CheetaChat client.
Cisco Systems [16]	Multiple	All Cisco IOS if IP routing is disabled.	A vulnerability exists because it is possible to make arbitrary remote modifications to the Cisco IOS routing table if IP routing is disabled, which could let a remote malicious user cause a Denial of Service or intercept communications.	**Workaround:** Cisco reports that you prevent the target router from acting upon received ICMP redirect packets using the following configuration command: Router(config)#no ip icmp redirect	IOS ICMP Redirect Routing Table Modification	Low/ Medium (Medium if communi-cations can be inter-cepted)	Bug discussed in newsgroups and websites. Vulnerability may be exploited with one of several freely available packet crafting tools.
CPanel [17]	Unix	CPanel 5 & prior	Multiple vulnerabilities exist: a vulnerability exists in the 'guestbook.cgi' script, which could let a remote malicious user execute arbitrary commands; and a vulnerability exists in Openwebmail, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	CPanel 5 'guestbook.cgi' & Openwebmail Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[14] Bugtraq, February 6, 2003.
[15] Bugtraq, February 13, 2003.
[16] Cisco Field Notice, 23074, February 10, 2003.
[17] Bugtraq, February 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
DotBr[18]	Unix	BotBr 0.1	Multiple vulnerabilities exist: a vulnerability exists in the 'foo.php3' script due to the way the 'phpinfo()' function is used, which could let a remote malicious user obtain sensitive information; a vulnerability exists because the configuration file doesn't have the proper PHP file extension, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'system.php3' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary commands; and a vulnerability exists in the 'exec.php3' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	DotBr Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Eggheads Develop-ment Team[19]	Unix	Eggdrop IRC bot 1.6.10-1.6.13	A vulnerability exists when linked to a botnet, which could let an unauthorized remote malicious user can use the bot as a proxy.	No workaround or patch available at time of publishing.	Eggdrop IRC Bot Unauthorized Proxy	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited using an IRC client.
Ericsson[20]	Multiple	HM220dp DSL Modem	A vulnerability exists in the remote administration and configuration web interface because no authentication is required, which could let an unauthorized remote malicious user obtain web management interface access.	No workaround or patch available at time of publishing.	HM220dp DSL Modem Administration Interface	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Eset Software[21]	Unix	NOD32 Antivirus 1.0 11, 1.0 12	A buffer overflow vulnerability exists when scanning a directory path of excessive length, which could let a malicious user execute arbitrary commands with superuser privileges.	Upgrade available at: http://www.nod32.com/download/download.htm	NOD32 Antivirus Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[18] SecurityFocus, February 15, 2003.
[19] Bugtraq, February 9, 2003.
[20] Bugtraq, February 11, 2003.
[21] iDEFENSE Security Advisory, 02.10.03, February 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Francisco Burzi[22]	Windows, Unix	PHP-Nuke 5.6, 6.0	Several vulnerabilities exist: a vulnerability exists in the 'admin' Cookie Variable used during the authentication process due to insufficient sanitization of cookie based data, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because user-supplied data is insufficiently sanitized when SQL queries are constructed, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHPNuke 'Admin' Cookie Variable & SQL Query Sanitization	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit has been published for the Search Engine SQL vulnerability.
GNU[23] *Vendors release patches[24, 25]* *RedHat releases patch[26]*	**Unix**	**Fileutils 4.0, 4.1, 4.1.6**	**A race condition vulnerability exists in various utilities, which could let a malicious user delete the whole filesystem.**	**Patch available for 4.1.6 at: http://mail.gnu.org/pipermail/bug-fileutils/2002-March/002440.html** ***Caldera:*** **ftp://ftp.caldera.com/pub/updates/OpenLinux/** ***Mandrake:*** **http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-031.php?dis=8.1** ***RedHat:*** **ftp://updates.redhat.com/6.2/en/os/SRPMS/fileutils-4.0**	**Fileutils Race Condition** **CVE Name: CAN-2002-0435**	**Medium**	**Bug discussed in newsgroups and websites.**
Gupta Technologies[27]	Windows 98/ME/NT 4.0/2000, XP	SQLBase 8.1.0	A buffer overflow vulnerability exists when the 'EXECUTE' command is used, which could let a remote malicious user execute arbitrary code with elevated privileges.	No workaround or patch available at time of publishing.	SQLBase EXECUTE Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Hewlett Packard Company[28]	Unix	HP HP-UX 11.0	A buffer overflow vulnerability exists in the 'disable' utility when strings of excessive length as parsed as the '-r' command line argument, which could let a malicious user cause a memory corruption and possibly execute arbitrary code.	HP has announced that the fixes supplied for a previous lp vulnerability also fix the described issue. Users are advised to apply the necessary fixes supplied in the HPSBUX0208-213 security bulletin.	HP-UX 'disable' Local Buffer Overflow	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[22] Bugtraq, February 20, 2003.
[23] Securiteam, March 15, 2002.
[24] Caldera International, Inc. Security Advisory, CSSA-2002-018.1, May 13, 2002.
[25] Mandrake Linux Security Update Advisory, MDKSA-2002:031, May 16, 2002.
[26] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:015-05, February 12, 2003.
[27] Network Intelligence India Pvt. Ltd. Advisory, February 10, 2003.
[28] Bugtraq, February 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [29]	Unix	HP-UX 10.0 1, 10.0, 10.1, 10.8-10.10, 10.16, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22	A buffer overflow vulnerability exists in the 'landiag' and 'lanadmin' utilities, which could let a malicious user obtain unauthorized access.	**Workaround:** Change the permissions on the affected binaries by issuing the following commands: chmod 555 /usr/sbin/landiag chmod 555 /usr/sbin/lanadmin	HP-UX landiag/ lanadmin Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Company [30]	Unix	HP-UX 10.0 1, 10.0, 10.1, 10.8-10.10, 10.16, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22	A buffer overflow vulnerability exists in the 'stmkfont' utility, which could let a malicious user obtain elevated privileges.	Patches available at: http://itrc.hp.com/ Patch PHSS_15423 **Workaround:** For HP-UX 11 systems, it is advised to remove the setuid bit of stmkfont by issuing the following command: chmod 555 /usr/bin/stmkfont	HP-UX 'stmkfont' Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Company [31]	Unix	HP-UX 10.0 1, 10.0, 10.1, 10.8-10.10, 10.16, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22	A vulnerability exists in the 'rs.F3000' binary, which could let a malicious user obtain unauthorized access or cause a Denial of Service.	**Workaround:** Remove the execute permissions on the affected binary by issuing the following commands: chmod 444 /usr/lib/X11/Xserver/ucode/screens/hp/rs.F3000	HP-UX rs.F3000 Unauthorized Access	Low/ Medium (Medium if access can be obtained)	Bug discussed in newsgroups and websites.
Hewlett Packard Company [32]	Unix	HP-UX 11.0	A buffer overflow vulnerability exists in the 'rcp' utility due to insufficient bounds checking of command line arguments, which could let a malicious user execute arbitrary code with the privileges of the superuser.	Patch available at: http://hp.cso.uiuc.edu/ftp/pub/hp/mirror/us-support.external.hp.com/s700_800/11.X/PHNE_23003	HP-UX rcp Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Hewlett Packard Company [33]	Unix	HP-UX 11.0 4, 11.0, 11.11, 11.20	A buffer overflow vulnerability exists when an excessive amount of data is redirected into wall as a message intended to be broadcast, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	HPUX Wall Message Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[29] Hewlett-Packard Company Security Bulletin, HPSBUX0302-243, February 12, 2003.
[30] Hewlett-Packard Company Security Bulletin, HPSBUX0302-241, February 12, 2003.
[31] Hewlett-Packard Company Security Bulletin, HPSBUX0302-240, February 12, 2003.
[32] SecurityFocus, February 20, 2003.
[33] Bugtraq, February 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [34]	Unix	HP-UX 10.10, 10.20, 11.0, 11.11, 11.22	A buffer overflow vulnerability exists in the 'rpc.yppasswd' implementation, which could let a malicious user obtain elevated privileges.	HP-UX 10.20 and 11.22 systems are advised to download a replacement rpc.yppasswd binary available at: ftp://yppass:yppass@hprc.external.hp.com/ or ftp://yppass:yppass@192.170.19.51/ Patches available at: http://itrc.hp.com/ Patch PHNE_28102, Patch PHNE_28103	HP-UX 'rpc.yppasswd' Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Horde[35] *SuSE releases patch[36]*	**Unix**	**IMP 2.2-2.2.8**	**Multiple SQL injection vulnerabilities exist due to insufficient sanitization of user-supplied input in SQL queries, which could let a remote malicious user corrupt the database.**	**Upgrade available at: http://www.horde.org/imp/3.1/ Debian: http://security.debian.org/pool/updates/main/i/imp/ *SuSE:* ftp://ftp.suse.com/pub/suse**	**Horde IMP Database Files SQL Injection CVE Name: CAN-2003-0025**	**Medium**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Hyper mail[37] *Debian issues upgrade[38]*	**Unix**	**Hypermail 2.1.3, 2.1.4, 2.1.5**	**Several buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists in the parsemail() function, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'mail' CGI component when a reverse DNS lookup is performed if the hostname is of excessive length, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the mail CGI program, which could let a remote malicious user send e-mail to arbitrary recipients.**	**Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=18117&release_id=135937 *Debian:* http://security.debian.org/pool/updates/main/h/hypermail/**	**Hypermail Remote Buffer Overflows CVE Name: CAN-2003-0057**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**
IBM[39]	Unix	AIX 4.3, 5.1, 5.2,	A buffer overflow vulnerability exists in the National Language Support libIM library, which could let a malicious user execute arbitrary code with elevated privileges.	Patches available at: ftp://aix.software.ibm.com/aix/efixes/security/libIM_efix.tar.Z	AIX libIM Buffer Overflow CVE Name: CAN-2003-0087	**High**	Bug discussed in newsgroups and websites.

[34] Hewlett-Packard Company Security Bulletin, HPSBUX0302-242, February 12, 2003.
[35] Debian Security Advisory, DSA 229-2, January 15, 2003.
[36] SuSE Security Announcement, SuSE-SA:2003:0008, February 18, 2003.
[37] Bugtraq, January 27, 2003.
[38] Debian Security Advisory, DSA 248-1, January 31, 2003.
[39] IBM Security Advisory, February 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM Lotus[40]	Windows NT 4.0/2000, Unix	Domino 6.0	A buffer overflow vulnerability exists when a HTTP redirect response is performed, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www14.software.ibm.com/webapp/download/search.jsp?q=&cat=&pf=&k=&dt=&go=y&rs=ESD-DMNTSRVRi&S_TACT=&S_CMP=&sb=r	IBM Lotus Domino HTTP Redirect Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
IBM Lotus[41]	Windows NT 4.0/2000, Unix	Domino 6.0	A buffer overflow vulnerability exists in the 's_ViewName/Foldername' options of the PresetFields parameter due to the way client-supplied request parameters are handled, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www14.software.ibm.com/webapp/download/search.jsp?q=&cat=&pf=&k=&dt=&go=y&rs=ESD-DMNTSRVRi&S_TACT=&S_CMP=&sb=r	Lotus Domino Web Server iNotes s_ViewName/ Foldername Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
IBM Lotus[42]	Windows NT 4.0/2000, Unix	Lotus Domino Server 5.0, 6.0	A vulnerability exists due to insufficient sanitization of user requests, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Domino Dot File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. Vulnerability has appeared in the press and other public media.
IBM Lotus[43]	Windows NT 4.0/2000, Unix	Lotus Notes Client 6.0	A buffer overflow vulnerability exists in the 'InitializeUsingNotesUser Name' method when an overly long value is submitted, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www14.software.ibm.com/webapp/download/search.jsp?q=&cat=&pf=&k=&dt=&go=y&rs=ESD-NOTECLNTi&S_TACT=&S_CMP=&sb=r	Lotus iNotes ActiveX Control Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
IndyNews[44]	Unix	IndyNews	Multiple vulnerabilities exist: a vulnerability exists in the delMediaFile() function, which could let an unauthorized malicious user delete media files; a vulnerability exists in the manageMedia() function, which could let an unauthorized malicious user delete or modify various files; and a vulnerability exists in 'alt' tags of a news article due to insufficient sanitization of some HTML tags, which could let a malicious user execute arbitrary code.	Patch available at: http://www.bergamoblog.it/modules.php?name=Downloads&d_op=getit&lid=4	IndyNews delMediaFile() File Deletion	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[40] NGSSoftware Insight Security Research Advisory, NISR17022003a, February 17, 2003.
[41] NGSSoftware Insight Security Research Advisory, NISR17022003b, February 17, 2003.
[42] Bugtraq, February 13, 2003.
[43] NGSSoftware Insight Security Research Advisory, NISR17022003c, February 17, 2003
[44] Bugtraq, February 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ISC[45] *Debian releases patch*[46] *OpenPKG releases patch*[47]	**Unix**	**DHCPD 3.0.1 1 rc1-rc10**	**A remote Denial of Service vulnerability exists in 'dhcrelay' when a malicious bootp packet is submitted.**	**Debian:** http://security.debian.org/pool/updates/main/d/dhcp3/ ***OpenPKG:*** http://www.openpkg.org/security/OpenPKG-SA-2003.012-dhcpd.html	**DHCPD dhcrelay Extraneous Network Packets Remote Denial of Service** **CVE Name: CAN-2003-0039**	**Low**	**Bug discussed in newsgroups and websites. Exploit has been published.**
ISOCA[48]	Unix	Cedric Email Reader 0.2, 0.3	Two vulnerabilities exist: a vulnerability exists in the 'email.php' script, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the 'emailreader_execute _on_each_page.inc.php' script, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Cedric Email Reader Remote File Include Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Junk buster[49] *Upgrade now available*[50]	**Unix**	**Internet Junk buster 2.01**	**A vulnerability exists in the CONNECT method, which could let a remote malicious user make unauthorized connections to arbitrary ports.**	***Upgrade available at:*** http://internet.junkbuster.com/ijb.html	**Internet Junkbuster Proxy Unauthorized Connections**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
KDE[51, 52] *More patches released*[53, 54] *Conectiva releases patches*[55]	**Unix**	**KDE 2.0, 2.0.1, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5**	**Multiple vulnerabilities exist due to a failure to properly quote parameters of instructions passed to a command shell for execution, which could let a local/remote malicious user execute arbitrary commands.**	**Upgrade available at:** http://download.kde.org/stable/3.0.5a/ ***Debian:*** http://security.debian.org/pool/updates/main/k/kdeadmin/ ***Conectiva:*** ftp://atualizacoes.conectiva.com.br/	**KDE Parameter Quoting Shell Command Execution** **CVE Name: CAN-2002-1393**	**High**	**Bug discussed in newsgroups and websites.**
Kietu[56]	Windows, Unix	Kietu 2.0, 2.3	A vulnerability exists because the include path for a configuration file can be specified, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Kietu Hit.PHP Remote File Inclusion	**High**	Bug discussed in newsgroups and websites.

[45] Bugtraq, January 15, 2003.
[46] Debian Security Advisory, DSA 245-1, January 28, 2003.
[47] OpenPKG Security Advisory, OpenPKG-SA-2003.012, February 19, 2003.
[48] Bugtraq, February 9, 2003.
[49] Bugtraq, December 23, 2002.
[50] SecurityFocus, February 11, 2003.
[51] KDE Security Advisory, December 21, 2002.
[52] Gentoo Linux Security Announcement, 200212-9, December 22, 2002.
[53] Gentoo Linux Security Announcement ,200301-11, January 18, 2003.
[54] Debian Security Advisories, DSA 234-1- 238-1, January 22 & 23, 2003.
[55] Conectiva Linux Security Announcement, CLA-2003:569, February 20, 2003.
[56] SecurityFocus, February 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [57]	Windows NT 4.0/2000	Windows 2000 Advanced Server, SP1-SP3, Datacenter Server, SP1-SP3, Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, Terminal Services, SP1-SP3, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a	A buffer overflow vulnerability exists in the command prompt (cmd.exe) because paths that contain more 256 characters are not handled properly, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Windows cmd.exe CD Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[57] Bugtraq, February 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [58]	Windows 95/98/ME/ NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, Windows 95, SR2, Windows 98, SE, ME, Windows NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, XP Home, SP1, XP Profes-sional, SP1	A buffer overflow vulnerability exists in 'riched20.dl' when a Rich Text Format (RTF) file is created that contains a large amount of data as an attribute, which could let a malicious user possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Microsoft Riched20.dll Attribute Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit has been published.

[58] Security Defence Stdio vulnerability announcement, 001, February 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [59] *Microsoft updates bulletin* [60, 61]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1 SP1-SP3, 5.5, 5.5 SP1&2, 6.0, 6.0 SP1	Several vulnerabilities exist: a vulnerability exists because it is possible to bypass the cross-domain security model that Internet Explorer uses when using dialog boxes, which could let a malicious user execute arbitrary code; and a vulnerability exists because it is possible to bypass the cross-domain security model that Internet Explorer implements when using showHelp () functionality, which could let a malicious user execute arbitrary commands. *Bulletin has been updated to include information about the availability of a hot fix that resolves a non-security related issue caused by the IE 6 version of this patch that could affect some users. Under certain conditions, the issue could cause some users to be unable to authenticate to certain Internet web sites such as subscription based sites, or MSN e-mail.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-004.asp *Note: Reports indicate that this patch may not install correctly through the WindowsUpdate website. Users are encouraged to download and install the patch manually.* *Note: This hot fix corrects a very specific non-security issue, and the security patch discussed in this Security Bulletin was, and still is, effective in removing the vulnerabilities. More information, including details of how to obtain the hot fix are available at:* http://www.microsoft.com/windows/ie/downloads/critical/813951/default.asp	Internet Explorer Cross-Domain Vulnera-bilities CVE Names: CAN-2003-1326, CAN-2003-1328	High	Bug discussed in newsgroups and websites. *Proof of Concept exploits have been published.*
Mozilla [62] *Conectiva releases patch* [63]	Windows 95/98/ME/ NT 4.0/2000, XP, MacOS 9.0/ 9.0.4/ 9.1/ 9.2/ 9.2.1/9.2.2, MacOS X 10.x, BeOS 5.0, Unix	Mozilla Browser 0.9.3-0.9.9, 1.0, 1.0.1, 1.1; *Galeon Browser 1.2.4-1.2.6*	A vulnerability exists in the implementation of the JavaScript 'onUnload' event handler because requests that the handler launches have the wrong referer, which could let a malicious user obtain sensitive information.	RedHat: ftp://updates.redhat.com/ Mandrake: http://www.mandrakesecure.net/en/ftp.php *Conectiva:* ftp://atualizacoes.conectiva.com.br/	Mozilla OnUnload Referer Information Leakage CVE Name: CAN-2002-1126	Medium	Bug discussed in newsgroups and websites. Proof of Concept has been published. Vulnerability has appeared in the press and other public media.

[59] Microsoft Security Bulletin, MS03-004 V1.1, February 6, 2003.
[60] Microsoft Security Bulletin, MS03-004 V2.0, February 12, 2003.
[61] Microsoft Security Bulletin, MS03-004 V2.1, February 19, 2003.
[62] Securiteam, September 12, 2002.
[63] Conectiva Linux Security Announcement, CLA-2003:568, February 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla[64] *Conectiva releases patch*[65]	Multiple	Mozilla Browser 0.9.7-1.0; *Galeon Browser 1.2.4-1.2.6*	Multiple vulnerabilities exist that have been patched. These vulnerabilities could let a malicious user cause a Denial of Service, obtain sensitive information or cause arbitrary code to be executed. For a complete list of these vulnerabilities, see http://mozilla.org/releases/mozilla1.0.1/security-fixes-1.0.1.html.	Upgrade available at: http://www.mozilla.org/releases/ RedHat: ftp://updates.redhat.com/ Mandrake: http://www.mandrakesecure.net/en/ftp.php *Conectiva:* ftp://atualizacoes.conectiva.com.br/	Mozilla Multiple Vulnera-bilities	Low/ Medium/ High (Low if a Denial of Service, Medium if sensitive informa-tion is obtained and High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Multiple Vendors[66] *Conectiva releases patch*[67]	Windows 95/98/ME/ NT 4.0/2000, XP, MacOS 9.0/9.0.4/ 9.1/9.2/9.2.1 MacOS X 10.x, Unix, BeOS 5.0	Mozilla Browser 0.9.5-0.9.9, 1.0; Netscape 6.2-6.2.3; Opera Software Opera Web Browser 5.12. 6.0, 6.0.1; *Galeon Browser 1.2.4-1.2.6*	A vulnerability exists when GIF image files are handled that have the width field set to zero, which could let a malicious user cause a Denial of Service or potentially execute arbitrary code.	Mozilla: http://www.mozilla.org/releases/ Netscape: http://channels.netscape.com/ns/browsers/download.jsp *Conectiva:* ftp://atualizacoes.conectiva.com.br/	Multiple Vendor Zero Width GIF Image Files	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[64] Bugtraq, September 18, 2002.
[65] Conectiva Linux Security Announcement, CLA-2003:568, February 13, 2003.
[66] Securiteam, September 8, 2002.
[67] Conectiva Linux Security Announcement, CLA-2003:568, February 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [68, 69, 70] *More updates issued* [71, 72, 73, 74] *More updates issued* [75, 76]	MacOS X 10.2, Unix	Apple MacOS X 10.2 (Jaguar), 10.2.2; Easy Software Products CUPS 1.0.4, 1.0.4–8, 1.1.1, 1.1.4-5, 1.1.4-3, 1.1.4-2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.15, 1.1.17	**Several vulnerabilities exist: vulnerability exists in the HTTP server component of the Common UNIX Printing System (CUPS), which could let a local/remote malicious user obtain root privileges; a race condition exists in the creation of /etc/cups/certs/<pid>, which could let a malicious user create or overwrite any file as root; a vulnerability exists because printers can remotely be added to CUPS by sending a specially crafted UDP packet; a remote Denial of Service vulnerability exits due to negative length memcpy() calls; an integer overflow vulnerability exists in the image handling code, which could let a malicious user obtain elevated privileges; a buffer overflow vulnerability exists in the strncat function call in the setup of the 'options' string, which could let a malicious user obtain root access; a vulnerability exists because CUPS improperly checks for zero width images in filters/image-gif.c, which could let a malicious user execute arbitrary code; and a vulnerability exists because the return values of many file and socket operations are not checked, which could let a malicious user cause a Denial of Service.** ***Debian issues update that corrects a library dependency for the libcupsys2 package.***	**Apple:** http://www.info.apple.cpm/kbnum/ **Easy Software:** http://www.cups.org/software.html **SuSE:** ftp://ftp.suse.com/pub/suse ***SCO:*** ftp://ftp.sco.com/pub/updates/OpenLinux/ ***Debian:*** http://security.debian.org/pool/updates/main/c/cupsys/ ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php ***RedHat:*** ftp://updates.redhat.com ***Debian:*** http://security.debian.org/pool/updates/main/c/cupsys ***Information regarding Apple updates available at:*** http://docs.info.apple.com/article.html?artnum=61798	CUPS HTTP Multiple Vulnerabilities CVE Names: CAN-2002-1366, CAN-2002-1367, CAN-2002-1368, CAN-2002-1369, CAN-2002-1371, CAN-2002-1372, CAN-2002-1383, CAN-2002-1384	Low/High (High if root access can be obtained or arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploits have been published.

[68] iDEFENSE Security Advisory, December 19, 2002.
[69] Gentoo Linux Security Announcement, 200212-13, December 29, 2002.
[70] SuSE Security Announcement, SuSE-SA:2003:002, January 2, 2003.
[71] SCO Security Advisory, CSSA-2003-004.0, January 21, 2003.
[72] Debian Security Advisory, DSA 232-1, January 20, 2003.
[73] Mandrake Linux Security Update Advisory, MDKSA-2003:001, January 10, 2003.
[74] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:295-07, January 13, 2003.
[75] Debian Security Advisory, DSA 232-2, February 20, 2003.
[76] Apple Security Updates, 61798, February 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
myPHP Nuke[77]	Windows, Unix	myPHP Nuke 1.8.8 _final_7, 1.8.8	A Cross-Site Scripting vulnerability exists in the 'links.php' script due to insufficient sanitization of HTML code, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	myPHPNuke Links.php Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Netgear[78]	Multiple	FM114P	A Directory Traversal vulnerability exists in the web-configuration interface, which could let an unauthorized remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FM114P Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Nethack[79]	Unix	Nethack 3.4 .0	A buffer overflow vulnerability exists when a specially crafted command string is submitted to the nethack binary, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Nethack Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Open Webmail[80] *Upgrade now available*[81]	**Unix**	**Open Webmail 1.70, 1.71**	**A vulnerability exists during the authentication process when an invalid username is entered, which could let a remote malicious user obtain sensitive information.**	***Upgrade available at:*** **http://openwebmail.org/openwebmail/download/**	**Open WebMail Invalid Unsername**	**Medium**	**Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.**
Opera Software[82]	Multiple	Opera Web Browser 6.0.5 win32, 7.0 win32 Beta 1&2	A buffer overflow vulnerability exists when an URL is submitted that contains a specially crafted, long username, which could let a remote malicious user execute arbitrary instructions.	Upgrade available at: http://www.opera.com/download/index.dml?opsys=Windows&lng=en&platform=Windows	Opera Username Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit scripts have been published.
Opera Software[83]	Multiple	Opera Web Browser 6.0.5 win32, 7.0 win32 Beta 1&2, 7.0 win32, 7.01win32	A Denial of Service vulnerability exists in 'opera.PluginContext.'	**Temporary workaround:** Disable Java in the browser configuration.	Opera opera.Plugin Context Native Method Denial Of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[77] Bugtraq, February 20, 2003.
[78] Bugtraq, February 10, 2003.
[79] Bugtraq, February 8, 2003.
[80] Securiteam, November 24, 2002.
[81] SecurityFocus, February 12, 2003.
[82] SecurityFocus, February 10, 2003.
[83] Beauchamp Security:Advisory, February 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation[84]	Windows NT 4.0/2000, XP, Unix	Oracle 9i Application Server 9.0.2	A vulnerability exists in the 'DAV' functionality due to a format string error in the 'mod_dav' module, which could let a remote malicious user execute arbitrary code.	Workaround and upgrade information available at: http://otn.oracle.com/deploy/security/pdf/2003alert52.pdf	Oracle 9i Application Server DAV_PUBLIC Format String CVE Name: CAN-2002-0842	High	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Oracle Corporation[85]	Windows NT 4.0/2000, XP, Unix	Oracle8 8.0.6, Oracle 8i 8.1.7.1, 8.1.7, Oracle9i 9.0, 9.0.1.3, 9.0.1 .2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.2, 9.2.1	A buffer overflow vulnerability exists in the 'TO_TIMESTAMP_TZ' function, which could let a malicious user execute arbitrary code.	Oracle has made fixes available. Administrators can download the patches at: http://metalink.oracle.com by entering Bug Number 2642439.	Oracle Database Server TO_TIMESTAMP_TZ Buffer Overflow	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Oracle Corporation[86]	Windows NT 4.0/2000, XP, Unix	Oracle8 8.0.6, Oracle 8i 8.1.7, Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.2, 9.2.1	A buffer overflow vulnerability exists in the 'TZ_OFFSET' function, which could let a malicious user execute arbitrary code.	Oracle has made fixes available. Administrators can download the patches at: http://metalink.oracle.com by entering Bug Number 2642267.	Oracle Database Server TZ_OFFSET Buffer Overflow	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Oracle Corporation[87]	Windows NT 4.0/2000, XP, Unix	Oracle8 8.0.6, Oracle 8i 8.1.7, 8.1.7.1, Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.2, 9.2.1	A buffer overflow vulnerability exists in the 'ORACLE.EXE' binary due to insufficient bounds checking on external data, which could let a malicious user execute arbitrary code.	Oracle has made fixes available. Administrators can download the patches at: http://metalink.oracle.com by entering Bug Number 2620726.	Oracle Database Server ORACLE.EXE Buffer Overflow	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Oracle Corporation[88]	Windows NT 4.0/2000, XP, Unix	Oracle8 8.0.6, Oracle 8i 8.1.7, Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, Oracle9i Release 2 9.2.2, 9.2.1	A buffer overflow vulnerability exists in the 'BFILENAME' function due to insufficient bounds checking on user-supplied input, which could let a malicious user execute arbitrary code.	Oracle has made fixes available. Administrators can download the patches at: http://metalink.oracle.com by entering Bug Number 2642117.	Oracle Database Server DIRECTORY Buffer Overflow	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[84] Oracle Security Alert #52, February 11, 2003.
[85] Oracle Security Alert #50, February 11, 2003
[86] Oracle Security Alert #49, February 11, 2003
[87] Oracle Security Alert #51, February 11, 2003
[88] Oracle Security Alert #51, February 11, 2003

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHP[89] *RedHat releases patch*[90] *More patches released*[91, 92, 93]	**MacOS X 10.x, Unix**	**PHP 4.1.2, 4.2.0-4.2.3**	**A buffer overflow vulnerability exists in the wordwrap() function, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.**	**Upgrade available at: http://www.php.net/downloads.php** ***RedHat:*** **ftp://updates.redhat.com/** ***Engarde:*** **http://ftp.engardelinux.org/pub/engarde/stable/updates/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***SuSE:*** **ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/**	**PHP wordwrap() Buffer Overflow** **CVE Name: CAN-2002-1396**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**
PHP Group[94, 95]	Windows, Unix	PHP 4.3	A vulnerability exists in PHP CGI SAPI that makes options for preventing direct access to the CGI binary useless, which could let a malicious user execute arbitrary code.	**OpenPKG:** ftp://ftp.openpkg.org/release/1.2/UPD/ **PGP Group:** http://www.php.net/downloads.php	PHP CGI SAPI Code Execution	**High**	Bug discussed in newsgroups and websites.
phpBB Group[96]	Windows, Unix	phpBB 1.4.0-1.4.4	A vulnerability exists in the 'auth.php' script due to insufficient sanitization of null characters, which could let a malicious user obtain sensitive information and possibly execute arbitrary PHP code.	No workaround or patch available at time of publishing.	PHPBB Auth.PHP File Disclosure	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
phpBB Group[97]	Unix	phpBB 2.0.0-2.0.2	A vulnerability exists due to insufficient sanitization of user-supplied input when a SQL query is constructed, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHPBB2 Page_Header. PHP SQL Injection	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
php-board[98]	Windows, Unix	php-board 1.0	A vulnerability exists because user information is stored in flat files and access is not sufficiently restricted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHP-Board User Password Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Posadis Team[99]	Unix	Posadis 0.50.4 - 0.50.8	A remote Denial of Service vulnerability exists due to the way certain DNS queries are read by the server.	Upgrades available at: http://prdownloads.sf.net/posadis/	Posadis DNS Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[89] Bugtraq, December 27, 2002.
[90] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:017-06, February 4, 2003.
[91] EnGarde Secure Linux Security Advisory, ESA-20030219-003, February 19, 2003.
[92] Mandrake Linux Security Update Advisory, MDKSA-2003:019, February 20, 2003.
[93] SuSE Security Announcement, SE-SA:2003:0009, February 18, 2003.
[94] PHP Security Advisory, February 17, 2003.
[95] OpenPKG Security Advisory, OpenPKG-SA-2003.010, February 18, 2003.
[96] Bugtraq, February 20, 2003.
[97] Bugtraq, February 20, 2003.
[98] SecurityFocus, February 15, 2003.
[99] SecurityTracker Alert, 1006047, February 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Postgre SQL[100, 101] *Mandrake issues upgrade*[102]	Unix	Postgre SQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2, 7.2.1	A buffer overflow vulnerability exists in the date parser due to insufficient bounds checking, which could let a malicious user cause a Denial of Service or execute arbitrary code.	**RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/postgresql **SuSE:** ftp://ftp.suse.com/pub/suse ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	PostgreSQL Date Parser Buffer Overflow CVE Name: CAN-2002-1398	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites.
Postgre SQL[103, 104] *Mandrake issues upgrade*[105]	Unix	Postgre SQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2.1	Several buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists with the TZ environment variable, which could let a malicious user cause a Denial of Service or execute arbitrary code; and a buffer overflow vulnerability exists with the SET TIME ZONE environment variable, which could let a malicious user cause a Denial of Service or execute arbitrary code.	**RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/postgresql **SuSE:** ftp://ftp.suse.com/pub/suse ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	PostgreSQL TZ Environment & SET TIME ZONE Environment Variables Buffer Overflows CVE Name: CAN-2002-1402	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites.
Postgre SQL[106, 107] *Mandrake issues upgrade*[108]	Unix	Postgre SQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2-7.2.3	A buffer overflow vulnerability exists in the 'path_add()' function due to insufficient bounds checking, which could let a malicious user cause a Denial of Service or execute arbitrary code.	**RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/postgresql ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	PostgreSQL path_add() Buffer Overflow	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites.

[100] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.
[101] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.
[102] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.
[103] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.
[104] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.
[105] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.
[106] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.
[107] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.
[108] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PostgreSQL[109, 110] *Mandrake issues upgrade*[111]	Unix	PostgreSQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2-7.2.3	Several buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists in the 'path_encode()' function, which could let a remote malicious user execute arbitrary commands; and a buffer overflow vulnerability exits with the 'circle_poly' function, which could let a malicious user cause a Denial of Service or execute arbitrary code.	RedHat: ftp://updates.redhat.com/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/p/postgresql *Mandrake:* http://www.mandrakesecure.net/en/ftp.php	PostgreSQL path_encode() & circle_poly Buffer Overflows CVE Name: CAN-2002-1401	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites.
PostgreSQL[112] *Mandrake issues upgrade*[113]	Multiple	PostgreSQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2	A buffer overflow vulnerability exists in the in cash_words() function because overly long queries are not handled properly, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.postgresql.org/ RedHat: ftp://updates.redhat.com/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/p/postgresql SuSE: ftp://ftp.suse.com/pub/suse *Mandrake:* http://www.mandrakesecure.net/en/ftp.php	PostgreSQL cash_words Buffer Overflow CVE Name: CAN-2002-1397	High	Bug discussed in newsgroups and websites. Exploit has been published.
PostgreSQL[114] *Mandrake issues upgrade*[115]	Multiple	PostgreSQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2, 7.2.1	A buffer overflow vulnerability exists in the repeat() function, which could let a malicious user execute arbitrary code.	RedHat: ftp://updates.redhat.com/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/p/postgresql SuSE: ftp://ftp.suse.com/pub/suse *Mandrake:* http://www.mandrakesecure.net/en/ftp.php	PostgreSQL Repeat Function Buffer Overflow CVE Name: CAN-2002-1400	High	Bug discussed in newsgroups and websites.

[109] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.
[110] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.
[111] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.
[112] @(#) Mordred Labs Advisory, 0x0001, August 19, 2002.
[113] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.
[114] @(#)Mordred Labs Advisory 0x0003, August 20, 2002.
[115] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Postgre SQL[116] *Mandrake issues upgrade*[117]	**Multiple**	**Postgre SQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2, 7.2.1**	**A buffer overflow vulnerability exists in the lpad() and rpad() functions because overly large integer arguments are handled properly, which could let a malicious user cause a Denial of Service. This vulnerability only affects data bases that were created using special international encodings.**	**RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/postgresql **SuSE:** ftp://ftp.suse.com/pub/suse ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	**PostgreSQL lpad() & rpad() functions Buffer Overflow** **CVE Name: CAN-2002-0972**	**Low**	**Bug discussed in newsgroups and websites.**
RARLAB[118]	Windows NT	FAR 1.65, 1.70 beta 1&4	A buffer overflow vulnerability exists due to insufficient bounds checking when directory paths are parsed, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	FAR File Manager Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
RedHat[119] *Patches now available*[120, 121]	**Unix**	**Linux 7.1, 7.2, 7.3, 8.0**	**A vulnerability exists in the 'pam_xauth' module when running the 'su' utility in conjunction, which could let a malicious user obtain elevated privileges.**	***RedHat:*** ftp://updates.redhat.com ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	**PAM pam_xauth Elevated Privileges** **CVE Name: CAN-2002-1160**	**Medium**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
RedHat[122]	Unix	Linux 7.2, 7.2 ia64, 7.3, 8.0	A vulnerability exists in the 'useradd' utility due to a failure to set secure permissions for a new user's mail spool directory, which could let a malicious user obtain sensitive information.	Upgrade available at: ftp://updates.redhat.com/	Red Hat useradd Insecure Mail Spool Permissions CVE Name: CAN-2002-1509	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
RedHat[123]	Unix	Linux 8.0 i386	A vulnerability exists because the 'uml_net' utility in kernel-utils packages was incorrectly shipped setuid root, which could let a malicious user obtain elevated privileges.	Upgrade available at: ftp://updates.redhat.com/8.0/en/os/i386/kernel-utils-2.4-8.28.i386.rpm	Red Hat Linux User Mode Linux SetUID Installation CVE Name: CAN-2003-0019	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[116] @(#) Mordred Labs Advisory 0x0004, August 20, 2002.
[117] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.
[118] Securiteam, February 15, 2003.
[119] Bedatec Security Advisory, 200212140001, February 4, 2003.
[120] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:035-10, February 12, 2003.
[121] Mandrake Linux Security Update Advisory, MDKSA-2003:017, February 18, 2003.
[122] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:057-06, February 18, 2003.
[123] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:056-08, February 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Research Triangle Software, Inc.[124]	Windows 95/98/ME/ NT/2000, XP	Crypto Buddy 1.0, 1.2	Multiple vulnerabilities exist: a vulnerability exists because the passphrase encryption algorithm generates predictable ciphertext for specific sequences of characters, which could let a malicious user obtain sensitive information; a vulnerability exists because the user-supplied passphrase is not used to encrypt files, which could let a malicious user obtain sensitive information; and a vulnerability exists because passphrases over 55 characters in length are truncated, which could result in a user having a false sense of security.	No workaround or patch available at time of publishing.	CryptoBuddy Multiple Passphrase Encryption Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Sage[125]	Windows, Unix	Sage 1.0 beta 3	Several vulnerabilities exist: a vulnerability exists in the Content Management System when a request is made for a nonexistent module, which could let a malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of input submitted in URI parameters, which could let a malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Sage Path Disclosure & Cross-Site Scripting	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published. There is no exploit code required for the Cross-Site Scripting vulnerability.

[124] Bugtraq, February 10, 2003.
[125] SecurityFocus, February 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[126] *Jetty software also affected*[127]	Windows, Unix	**Java Web Start 1.0, 1.0.1, 1.0.1_01, 1.0.1_02, 1.2; JRE (Linux Production Release), (Solaris Production Release), (Windows Production Release) 1.3, 1.3_1.3, 1.3_02, 1.3_05, 1.3.1, 1.3.1_01, 1.3.1_03, 1.3.1_05, 1.4, 1.4.1; JSSE 1.0.3; SDK (Linux Production Release), (Solaris Production Release), (Windows Production Release) 1.3_02, 1.3_05, 1.3.1_01, 1.3.1_03, 1.3.1_05, 1.4, 1.4.0_02, 1.4, 1.4.1;** ***Jetty 4.2.4-4.2.6***	**A vulnerability exists because the Java Secure Socket Extension (JSSE), Java Plug-in, and Java Web Start incorrectly validate the digital certificate of a web site, which could let untrustworthy web sites be authenticated for SSL transactions.**	**Upgrades available at: http://java.sun.com/products/jsse/index-103.html or http://java.sun.com/j2se/** ***Jetty upgrade available at:*** **http://prdownloads.sourceforge.net/jetty/Jetty-4.2.7-src.tgz?download**	**Sun JSSE/Java Plug-In/Java Web Start Incorrect Certificate Validation**	**Medium**	**Bug discussed in newsgroups and websites.**
Sun Micro-systems, Inc.[128]	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0	A remote Denial of Service vulnerability exists when processing malicious packets sent to a listening RPC service.	Patches available at: http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=105402&rev=41 Patch 105402-41, Patch 105401-41, Patch 106943-24, Patch 106942-24, Patch 108828-37, Patch 108827-36, Patch 113319-04	Sun Solaris Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[126] Sun(sm) Alert, 50081, January 23, 2003.
[127] SecurityFocus, February 6, 2003.
[128] Sun(sm) Alert Notification, 50626, February 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[129]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A vulnerability exists in the mail program due to a problem with the handling of opening mail spool files, which could let a malicious user obtain sensitive information.	Patches available at: http://sunsolve.sun.com Patch 109267-05, Patch 109266-05, Patch 109254-07, Patch 109253-07, Patch 111875-06, Patch 111874-06, Patch 114134-01, Patch 114133-01	Solaris Mail Reading Local Race Condition	Medium	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[130] ***Sun updates bulletin[131]***	**Unix**	**Solaris 2.6, 7, 8, 9**	**A remote Denial of Service vulnerability exists in the 'in.ftpd' daemon.** ***Temporary patches available and updated relief/workaround section.***	**Workaround:** **http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50240**	**Solaris Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.**
Symantec[132]	Windows 98/ME/NT 4.0/2000, XP	Norton AntiVirus 2002	A buffer overflow vulnerability exists when an e-mail message with a compressed file that includes a file with an unusually long filename is received, which could let a malicious user execute arbitrary code.	Product updates containing the fix have been distributed via LiveUpdate.	Norton Antivirus 2002 Email Scanner Buffer Overflow	High	Bug discussed in newsgroups and websites.
Univer-sity of Kansas[133] ***More patches released[134, 135]***	**Multiple**	**Lynx 2.8.2 rel.1- 2.8.4 rel.1, 2.8.5 dev.8**	**A vulnerability exists when carriage return and line feed (CRLF) characters are included in the commandline, which could let a malicious user make scripts that use Lynx for downloading files from the wrong site on a web server with multiple virtual hosts.**	**Patch available at:** **ftp://lynx.isc.org/lynx2.8.4/patches/lynx2.8.4rel.1c.patch** **ELinks:** **http://elinks.or.cz/download/elinks-0.4pre15.tar.bz2** **Debian:** **http://security.debian.org/pool/updates/main/l/lynx-ssl/** **SCO:** **ftp://ftp.sco.com/pub/updates/OpenLinux/** **Trustix:** **ftp://ftp.trustix.net/pub/Trustix/updates/** ***RedHat:*** **ftp://updates.redhat.com/** ***OpenPKG:*** **http://www.openpkg.org/security/OpenPKG-SA-2003.011-lynx.html**	**Lynx Command Line URL CRLF Injection**	**Medium**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Visual Mining, Inc.[136]	Windows NT 4.0/ 2000, XP, Unix	Netcharts XBRL Server 4.0	A vulnerability exists because invalid chunked encoded HTTP requests are insufficiently handled, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Netcharts Server Chunked Encoding Information Leakage	Medium	Bug discussed in newsgroups and websites.

[129] Sun(sm) Alert Notification, 50751, February 11, 2003.
[130] Sun(sm) Alert, 50240, January 27, 2003.
[131] Sun(sm) Alert, 50240, February 6, 2003.
[132] SNS Advisory No.61, February 19, 2003.
[133] Bugtraq, August 19, 2002.
[134] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:029-06, February 12, 2003.
[135] OpenPKG Security Advisory, OpenPKG-SA-2003.011, February 18, 2003.
[136] Securiteam, February 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
W3M[137, 138, 139, 140, 141]	Windows, Unix	W3M 0.2-0.2.5.1, 0.3--0.3.2; w3mmee 0.3.p23.3, w3mmee-ssl 0.3.p23.3	Two Cross-Site Scripting vulnerabilities exist: a vulnerability exists if frames support is enabled due to insufficient sanitization of HTML tags, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to inadequate sanitization of IMAGE tags, which could let a remote malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/w/w3mmee **RedHat:** ftp://updates.redhat.com/ **W3M:** http://prdownloads.sourceforge.net/w3m/w3m-0.3.2.2.tar.gz?download **OpenPKG:** http://www.openpkg.org/security/OpenPKG-SA-2003.009-w3m.html	W3M Cross-Site Scripting CVE Names: CAN-2002-1335, CAN-2002-1348	High	Bug discussed in newsgroups and websites. There is no exploit code required.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between February 10 and February 21, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 17 scripts, programs, and net-news messages containing holes or exploits were identified. Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
February 21, 2003	Tcpscan3.txt	Coding a TCP Connect Port Scanner Using VLSM Handbook is an in-depth beginner's tutorial written to explain incorporation of VLSM and CIDR capabilities into a network scanner.
February 20, 2003	**DSR-cpanel.c**	**Script that exploits the CPanel 5 'gueltbook.cgi' vulnerability.**
February 20, 2003	**DSR-nethack.c**	**Script that exploits the Nethack Local Buffer Overflow vulnerability.**

[137] Debian Security Advisory, DSA 249-1, February 11, 2003.
[138] Debian Security Advisory, DSA 250-1, February 12, 2003.
[139] Debian Security Advisory, DSA 251-1, February 14, 2003.
[140] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:044-20, February 7, 2003.
[141] OpenPKG Security Advisory, OpenPKG-SA-2003.009, February 18, 2003.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
February 20, 2003	PHPBBAutoSelectFishAttacker.php	Exploit for the PHPBB2 Page_Header.PHP SQL Injection vulnerability.
February 20, 2003	**PHPNukeAutoSelectFishAttacker.php**	**Exploit for the PHPNuke Search Engine SQL Injection vulnerability.**
February 20, 2003	**Webmail_local.pl**	**Script that exploits the CPanel 5 Openwebmail vulnerability.**
February 19, 2003	Gobbler-1.8alpha.tar.gz	A tool that is designed to audit various aspects of DHCP networks, from detecting if DHCP is running on a network to performing a denial of service attack. Gobbler also exploits DHCP and Ethernet, to allow distributed spoofed port scanning with the added bonus of being able to sniff the reply from a spoofed host.
February 18, 2003	Absolute_uk2.pl	Perl script that exploits the Absolute Telnet Title Bar Buffer Overflow vulnerability.
February 18, 2003	Xperl_yabbse_mass.tar.gz	Yabase v1.5.0 and below remote scanner / exploit tool which takes advantage of a bug in an include named Packages.php.
February 16, 2003	**Bitchx-353.c**	**Script that exploits the BitchX Malformed RPL_ NAMREPLY Denial of Service vulnerability.**
February 13, 2003	Udp-remote-final.tar.gz	A utility that demonstrates a simple UDP backdoor which allows for remote program execution on a Unix server.
February 11, 2003	Smtpscan-0.4.tar.gz	A tool to guess which MTA is used by sending several "special" SMTP requests and by comparing error codes returned with those in the fingerprint database.
February 10, 2003	030217_o6unexp.tgz	Script that exploits the Opera Username Remote Buffer Overflow vulnerability.
February 10, 2003	**Nethack.pl**	**Perl script that exploits the Nethack Local Buffer Overflow vulnerability.**
February 10, 2003	**Nethacker.c**	**Script that exploits the BitchX Malformed RPL_ NAMREPLY Denial of Service vulnerability.**
February 10, 2003	o6unexp.c	Script that exploits the Opera Username Remote Buffer Overflow vulnerability.
February 10, 2003	THCunREAL.zip	Remote root exploit for Realserver 8 on several Windows platforms.

Trends

- **Systems are being compromised through the exploitation of null or weak default 'sa' passwords in Microsoft SQL Server and Microsoft Data Engine.**
- **Propagation of SQL 'Slammer' or 'Sapphire' malicious code is still causing varied levels of network degradation across the Internet and the compromise of vulnerable machines.**
- **NIPC has issued an advisory regarding the propagation of an SQL worm. The self-propagating malicious code exploits multiple vulnerabilities in the Resolution Service of Microsoft SQL Server 2000. This worm activity appears to have caused various levels of network degradation across the Internet. In addition to the compromise of vulnerable machines; the apparent effects of this fast-spreading, virus-like infection has overwhelmed the world's digital pipelines and interfered with Web browsing and delivery of e-mail. For more information, see Virus Section, WORM_SQLP1434.A description and NIPC Advisory 03-001.1, located at: http://www.nipc.gov/warnings/advisories/2003/03-001.1updates.htm. For patch information, see:**
  - **http://www.microsoft.com/security/slammer.asp**
  - **http://www.microsoft.com/technet/security/bulletin/MS02-061.asp**
  - **http://www.microsoft.com/technet/security/bulletin/MS02-039.asp**
- **The CERT/CC has released an advisory regarding a buffer overflow vulnerability in the Microsoft Windows Shell. For more information, see Bugs, Holes & Patches table entry, "Windows XP WMA/MP3 Buffer Overflow" and CERT® Advisory CA-2002-37, located at: http://www.cert.org/advisories/CA-2002-37.html.**

- **The CERT/CC has released an advisory regarding multiple vendors' implementations of the secure shell (SSH) transport layer protocol contain vulnerabilities that could allow a remote malicious user to execute arbitrary code with the privileges of the SSH process or cause a denial of service. The vulnerabilities affect SSH clients and servers, and they occur before user authentication takes place. For more information, see Bugs, Holes & Patches table entry "Multiple Vendor SSH2 Implementation" and CERT® Advisory CA-2002-36, located at: http://www.cert.org/advisories/CA-2002-36.html.**
- **The CERT/CC has received reports of increased scanning for NetBIOS services. Probes to port 137/udp may be indicative of such activity.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

BAT.Junkboat.Worm (Alias: I-Worm.Junkboat) (Batch File Worm): This is a worm that uses the KaZaA-file sharing network and mIRC to spread. It also creates the file C:\Love_Me.vbs that has the ability to e-mail the BAT.Junkboat.Worm to all addresses in the Microsoft Outlook Address Book.

VBS.Caser@mm (Alias: VBS.Casechange.A) (Visual Basic Script Worm): This is a mass-mailing worm that spreads using Microsoft Outlook and IRC and copies itself across mapped drives. The worm attempts to overwrite several files on your system. The e-mail will have an attachment with a .vbs file extension.

VBS/Cian-C (Aliases: I-Worm.Thery.b, VBS_CIAN.C, VBS.Cian.C@mm, VBS.Cian.C) (Visual Basic Script Worm): This is a worm which spreads via mIRC, P2P file sharing networks, and e-mail attachments. It appends itself to files with the extensions VBS or VBE and infects Word and Excel documents. Infected Word and Excel documents are detected as OF97/Cian-C. Upon execution, VBS/Cian-C drops several copies of itself to the system folder as Winstart.vbs, Wininst32.vbs, Winnt32.vbs, and Winnet32.vbs. The worm also drops itself to the Windows folder as Netlnk32.vbs and Conversation.vbe. VBS/Cian-C then sets the following registry entry in order to run itself on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Winstart ="Wscript.exe C:\<Systems>\Winstart.vbs %1"

It drops two macro scripts, evade.jpg and evade.gif, to the system folder. The worm then uses these scripts to create the infected Excel Document Personal.xls in the Excel startup folder and infects the Word Document template. Personal.xls and the infected Word Document template will infect Excel and Word documents under the Microsoft Office environment. The infected Office documents can spread separately as viruses and via e-mail, however they will also drop and run a copy of VBS/Cian-C. It lowers the security settings under Microsoft Office by modifying the following registry entries:

- HKCU\Software\Microsoft\Office\<Version>\Excel\Security\AccessVBOM="1"
- HKCU\Software\Microsoft\Office\<Version>\Excel\Security\Level="1"
- HKCU\Software\Microsoft\Office\<Version>\Word\Security\AccessVBOM="1"
- HKCU\Software\Microsoft\Office\<Version>\Word\Security\Level="1"

VBS/Cian-C then proceeds to append itself to files with the extensions VBS and VBE found in various folders. In addition, VBS/Cian-C targets the numerous folders that are the file sharing folders of various Peer-to-peer file sharing applications. VBS/Cian-C replaces files with the following extensions with copies of itself, preserving the filename but adding an additional VBS extension (e.g. filename.mp3.vbs). It then attempts to modify script.ini in the mIRC folder so that the mIRC client will automatically send a copy of the worm to users joining the same IRC channel. The message sent is "Remember this funny conversion I had on IRC?" and the file is Conversation.vbe, detected as mIRC/Cian-C. Finally, VBS/Cian-C sets the following registry entry as infection mark:

- HKCU\Sofware\Zed/[rRlf]\VBS/Evade\ = "VBS/Evade.A by Zed/[rRlf]"

VBS.DLetter@mm (Aliases: VBS/DeathLetter, VBS/Grimgram@MM) (Visual Basic Script Worm): When executed, the worm attempts to send itself to all the recipients in the Microsoft Outlook

address book. The e-mail will have a subject that is randomly chosen from a predetermined list and an attachment with a .mht file extension. VBS.DLetter@mm also spreads using the IRC, mIRC, and KaZaA-shared folders.

VBS.Gpremier@mm (Visual Basic Script Worm): This is a mass-mailing worm that is written in the Visual Basic Scripting (VBS) language. When it is executed, it copies itself to the \Windows\System folder and infects all the HTML files with the VBS.CandyLove virus. VBS.Gpremier@mm mails itself to all the contacts in all the Microsoft Outlook Address Books. The e-mail would have the following characteristics:

- Subject: NO estimado Bill G.
- Attachment: gpremier.vbs

VBS.MrCopy.Worm (Visual Basic Script Worm): This worm spreads by copying itself over all the existing .vbs and .vbe files found on all the local drives and mapped network drives. When MrCopy.Worm is activated, it adds the value, "WinUpdate" = "Wscript.exe %System%\Mr. Worm.pps.vbs %," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Next it copies itself as %System%\Mr. Worm.pps.vbs and copies over all the .vbs and .vbe files found on all the local drives and mapped network drives.

W32/Axam-A (Aliases: I-Worm.Axam, W95/MaxaP2P.A, W32.HLLW.Maax@mm, W32/Maax@MM, W32/MaxaP2P.A) (Win32 Worm): This is an e-mail and peer-to-peer worm. The worm may also be found in the numerous folders commonly shared by popular peer-to-peer networking software. It will also be copied to the Windows startup folder and C:\Windows\Application Data\. The following registry entry will be created to run the worm when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\sysaxam32

A new file type named spitmaxa will be created via the registry entry HKCR\Spitmaxa and the registry entry HKCR\.exe will be modified so that EXE files will be run as the file type spitmaxa. This will cause the worm to be run whenever the infected user attempts to run an EXE file. When run, W32/Axam-A will display a message box. On the second of the month a message box will be displayed containing the text "Apa yang membuatkan seseorang itu lalai? Jawapannya ada pada anda sendiri. Dengarlah nasihat dari Axam Virus ini." The virus author Melhacker claims to be based in Malaysia and the text displayed in the message box above is written in the Malay language. Translated it reads "What makes a person careless? The answer is in yourself. Listen to the advice of the Axam Virus." The file Autoexec.bat will be modified to display "...-= AxAm WOrm PreSenT =-..." when executed. W32/Axam-A contains functionality that is intended to delete a large number of files and format drives C: and D:, but this will never work.

W32.Blitzdung@mm (Aliases: I-Worm.Blitzdung, WORM_BLITZDUN.A) (Win32 Worm): This is a mass-mailing worm that was originally written in Java. A converter tool was used to convert the worm to a Win32 Portable Executable (PE) file. It attempts to send a copy of itself to all the contacts found in the Yahoo! Messenger log file. It can also spread through any mIRC channels that you visit. The worm tries to copy a file infected with W32.ElKern.4926 into the Windows folder.

W32.HLLW.Discoball (Alias: W32/Discoball.Worm) (Win32 Worm): This is a worm that spreads through network shares. The existence of the file Mdbole.exe, Seg32.exe or Wins.exe is a sign of a possible infection.

W32.HLLW.Oror.D@mm (Aliases: I-Worm.Roron.4999.c, W32/Roro.V@mm, W32/Roron.AA@mm) (Win32 Worm): This is a mass-mailing worm and a variant of W32.HLLW.Oror@mm. This worm attempts to spread through e-mail, mIRC, KaZaA, network shares, and mapped drives. It also attempts to terminate and remove various security products from the infected computer. This threat is written in the C++ language and is compressed with UPX. The uncompressed size is about 160 KB.

W32.Kwbot.C.Worm (Win32 Worm): This worm attempts to spread itself through the KaZaA and iMesh file-sharing networks. The worm also has a backdoor Trojan capability that allows a malicious user to gain control of the compromised computer.

W32.Kwbot.D.Worm (Win32 Worm): This is a variant of W32.Kwbot.C.Worm, with the following differences:

- This variant was packed using a run-time compression utility.
- The file name has been changed to Winsys.exe.
- The registry entry is named Winsys.

Everything else, including the functionality, remains the same as the W32.Kwbot.C.Worm.

W32/Proget.worm.b (Aliases: W32.Proge, W32/Proget-B, Win32.HLLW.Proget.b) (Win32 Worm): This is a floppy worm virus that creates thousands of 10 byte files on the local system. When run, the worm copies itself to the WINDOWS SYSTEM (%SysDir%) directory, keeping the same filename as when it was run. It creates a registry run key to load itself at startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run "%FileName%" = %WormPath%

Once installation is complete, the worm exists. Upon reload, the worm is run from the SYSTEM directory, which activates its propagation routine and payload. The virus has a payload to create a 10 byte file in each directory on the local system using a random 8 character followed by the extension aaa. The content of the file also contains 10 random characters. This action happens each time the system is rebooted, which can result in thousands of files getting created, filling up the hard disk over time. Each minute, a copy of the worm is saved to the A:\ drive.

W32.Yalat.Worm (Aliases: I-Worm.Haelp, W32/Yalat.worm) (Win32 Worm): This is a worm that attempts to spread by using MAPI and by copying itself to shared folders. It also attempts to stop the processes of some antivirus programs. Due to bugs in the code, the worm does not work as intended.

W32.Zokrim@mm (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. The worm displays a message when run. The e-mail has the following characteristics:

- Subject: SMS for YOU by Valentina
- Message: Mirko (z) is crazy for Valentina...!!!!!!
- Attachment: Vale.exe

W32.Zokrim@mm is written in the Microsoft Visual Basic programming language.

W97M.Babals.B (Aliases: Word97.Babals, W97M/Bablas.DY) (Word 97 Macro Virus): When W97M.Babals.B is executed, it attempts to infect the Microsoft Word Normal.dot template. Once that happens, the virus will infect any documents that you open or close.

W97M.Cian.C@mm (Word 97 Macro Virus): This is a mass-mailing macro virus that infects Microsoft Word documents. This macro virus has a VBS script inside itself that it inserts and executes on the system.

W97M.Hopel.A (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents when you click Open, Close, Save, New, or Exit. This virus has many different payloads that it can execute on Exit. If an infected document is double-clicked, the virus saves the infected document as C:\Windows\Command\Nt.txt. W97M.Hopel.A also overwrites the Autoexec.bat file with a non-ASCII character.

W97M.Tang (Word 97 Macro Virus): This is the macro module of W32.HLLW.Tang@mm. It infects Microsoft Word documents and templates.

W97M.Tolu (Word 97 Macro Virus): This is a Microsoft Word 97 macro virus that infects Microsoft Word documents and templates. The virus displays an illustration with a message when an infected document is opened.

W97M.Trug.A (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents when they are opened or closed. W97M.Trug.A attempts to hide its malicious actions and it may delete several files from the system.

WORM_LOVEGATE.B (Alias: LOVGATE.A, W32/Lovgate.worm, WORM_LOVGATE.A, I-Worm.Supnot) (Internet Worm): This malware is both a worm and backdoor program. To propagate, it drops copies of itself in network shared folders and subfolders. As a backdoor, it opens a

port, 10168 by default, allowing remote malicious users to access and manipulate the affected system. It sends a notification to either of the following e-mail addresses:

- 54love@fescomail.net
- hacker117@163.com

Worm/SMachine.IRC (IRC Worm): This is an Internet worm that spreads through the use of the mIRC network. If executed, the worm creates numerous new files. Additionally, so that it gets run each time a user restart their computer the following file gets modified:

- C:\Windows\Win.ini
  load=
  load=C:\Windows\Inf\Inf\System.exe, C:\Windows\Inf\Inf\System.exe

The following registry keys will also get added:

- HKEY_CLASSES_ROOT\CLSID\{D5DE8D20-5BB8-11D1-A1E3-0A0C90F2731}\InProcServer32
  @="C:\\WINDOWS\\INF\\INF\\MSVBVM60.DLL"
  "ThreadingModel"="Apartment"
- HKEY_CLASSES_ROOT\TypeLib\{000204EF-0000-0000-C000-000000000046}\6.0\9\win32
  @="C:\\WINDOWS\\INF\\INF\\MSVBVM60.DLL"
- HKEY_LOCAL_MACHINE\Software\CLASSES\irc\Shell\open\command
  @="\"C:\\WINDOWS\\INF\\INF\\MIRC.EXE\" -noconnect"

WORM_TANG.A (Aliases: Win32/Gant.A@mm, I-Worm.Tanger, W32.HLLW.Tang@mm, W32/Gant@MM) (Internet Worm): This memory-resident worm propagates in various ways. It sends itself via e-mail to all addresses listed in the Microsoft Outlook address book, via Internet Relay Chat (IRC), mapped network drives, and via popular peer-to-peer file-sharing applications such as KaZaA, Morpheus, Grokster, and others. Aside from carrying out various propagation routines, the worm also infects batch files. Its code also indicates that it has capabilities to infect Word and Excel documents. This malware is developed in Visual Basic and runs on Windows 95, 98, NT, 2000, ME and XP systems. It usually arrives UPX-compressed.

X97M.Cian.C@mm (Excel 97 Macro Virus): This is a mass-mailing macro virus that infects Microsoft Excel spreadsheets. This macro virus has a VBS script inside itself that it inserts and executes on the system.

X97M.Tang (Excel 97 Macro Virus): This is the macro module of W32.HLLW.Tang@mm. It infects Microsoft Excel Spreadsheets.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	**A**	**Current Issue**
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	**E**	**Current Issue**
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Bmbot	**N/A**	**Current Issue**
Backdoor.CHCP	N/A	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	**N/A**	**Current Issue**
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	**N/A**	**Current Issue**
Backdoor.Hitcap	**N/A**	**Current Issue**
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Cloner	**N/A**	**Current Issue**
Backdoor.IRC.Zcrew	**N/A**	**Current Issue**
Backdoor.Khaos	**N/A**	**Current Issue**
Backdoor.Kilo	**N/A**	**Current Issue**
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	**04.d**	**Current Issue**
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.SchoolBus.B	**B**	**Current Issue**
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	**N/A**	**Current Issue**
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Snowdoor	**N/A**	**Current Issue**
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Udps.10	10	CyberNotes-2003-03
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AOK	N/A	CyberNotes-2003-01
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/Evolut	N/A	CyberNotes-2003-03
DoS-iFrameNet	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Exploit-IISInjector	N/A	CyberNotes-2003-03
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
JS.Seeker.J	J	CyberNotes-2003-01
JS/Seeker-C	**C**	**Current Issue**
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	**N/A**	**Current Issue**
ProcKill-Z	N/A	CyberNotes-2003-03
PWS-Aileen	**N/A**	**Current Issue**
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWS-Tenbot	N/A	CyberNotes-2003-01
QDel359	N/A	CyberNotes-2003-01
Renamer.c	N/A	CyberNotes-2003-03
Tellafriend.Trojan	**N/A**	**Current Issue**
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	**A**	**Current Issue**
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Dloader-BO	N/A	CyberNotes-2003-02
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	**A**	**Current Issue**
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Idly	**N/A**	**Current Issue**
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.ProteBoy	**N/A**	**Current Issue**
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
W32.Benpao.Trojan	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	**N/A**	**Current Issue**
W32/Igloo-15	**N/A**	**Current Issue**
Xin	N/A	CyberNotes-2003-03

AdwareDropper-A: This is an Adware dropping Trojan. When run, it installs a Macromedia Flash "card," and three Adware DLL files that are Internet Explorer Browser Helper Objects, designed to display advertisements, track the URLs visited on the system, capture typed search strings, and alter the browser's default start page. These DLL files are not considered to be malicious, but are likely used for marketing purposes. As the main installer executable does not contain any end user license agreement (EULA), it is considered malicious. The following message is believed to have been SPAMED to a number of users.

- From: cupid@valentines-ecard.com

The message links to an executable file named card.exe. When run, a Flash "card" is displayed. The executable extracts several files to disk:

- %Program Files%\Valintines Day Card\Valintines Day Card\uninstall.exe
- %Program Files%\Valintines Day Card\Valintines Day Card\valsday.exe
- %Start Menu\Programs%\Valintines Day Card\Uninstall.lnk
- %Start Menu\Programs%\Valintines Day Card\Valintines Day Card.lnk
- %SysDir%\HmePge.dll
- %SysDir%\HotLink.dll
- %SysDir%\IEBrw.dll

Backdoor.Assasin.E: This Trojan is a variant of Backdoor.Assasin. It gives a malicious user unauthorized access to the compromised computer and attempts to terminate the active processes of various firewalls, as well as antivirus and security products. This variant also attempts to spread itself across the network shares. Backdoor.Assasin.E is written in the Borland Delphi programming language and is compressed with UPX.

Backdoor.Bmbot (Alias: W32/Cult.Worm): This is a backdoor Trojan that allows a malicious user to gain control of your computer by using Internet Relay Chat (IRC). A false error message is displayed if Backdoor.Bmbot is not executed from the %System% folder.

Backdoor.Dani (Alias: Backdoor.Dani.20): This is a backdoor Trojan that is written in the Microsoft Visual Basic programming language. It overwrites the Windows registry editor program located in %Windir%\Regedit.exe with a copy of itself. The Trojan allows unauthorized access to an infected computer.

Backdoor.Hipo: This is a typical Backdoor Trojan that allows a malicious user to gain access to and remotely control an infected computer. The Trojan is written in the Delphi programming language and is compressed with UPX.

Backdoor.Hitcap: This is a Backdoor Trojan that gives a malicious user unauthorized access to your computer. It consists of two components:

- An executable file: The executable file is packed with ASPack v1.06.
- A .dll file: The .dll file is packed with PECompact v1.50.

Backdoor.IRC.Cloner (Aliases: Backdoor.IRC.Cloner, BKDR_IRCCLONER, IRC_CLONER, Backdoor:IRC/Cloner): This is a backdoor Trojan that uses mIRC to communicate with a remote malicious user. It allows the malicious user to gain full control over your computer.

Backdoor.IRC.Zcrew (Aliases: IRC/Flood.bi, Backdoor.IRC.Zcrew): This is a backdoor Trojan that is similar to other backdoor IRC Trojans, such as Backdoor.IRC.Aladinz and Backdoor.IRC.Flood. It is written as an IRC script and uses the mIRC client to connect to the Internet, where it notifies the malicious user of its presence. The malicious user can send various commands to the infected computer

and take full control over it. An infected computer can also be used to launch a ping flood attack against another computer at a specified IP address.

Backdoor.Khaos (Aliases: BKDR_KHAOS.A, Backdoor.Khaos, Backdoor.Win32/Khaos): This is a backdoor Trojan that gives a malicious user unauthorized access to your computer. It usually arrives as the file, Server2.exe. By default it opens port 6969 for listening. Backdoor.Khaos does not automatically install itself, as some other program usually installs it. As a result, even if Backdoor.Khaos is installed, in most cases, it will no longer run after you restart your computer. It is written in Microsoft Visual Basic 5 and it requires that the Visual Basic (VB) run-time libraries be installed on your computer in order for it to execute.

Backdoor.Kilo: This is a backdoor Trojan that uses an IRC channel to contact a malicious user. Backdoor.Kilo is written in the Delphi programming language and is packed with UPX. When executed, it copies itself as %System%\Njgal.exe and adds the value, "Boot Manager %System%\Njgal.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Next it opens ports 6711 and 6718 and creates the file, %System%\Boot.dat.

Backdoor.Optix.04.d (Aliases: Backdoor.Optix.04.f, Backdoor-RS): This is a backdoor Trojan and a variant of Backdoor.Optix.04.c. It is a Delphi application packed with UPX, v0.76.1-1.20. By default, it listens on port 5151. Backdoor.Optix.04.d attempts to terminate or close any processes of, or windows belonging to, various programs. These programs include antivirus and security programs.

Backdoor.Optix.05 (Aliases: Backdoor.Optix.50, Backdoor.Win32/Optix.5_0): This is a backdoor Trojan that is a variant of Backdoor.Optix.04.c. By default, it listens on port 5151. The Trojan attempts to terminate or close any processes or windows belonging to various programs, including antivirus and security programs.

Backdoor.SchoolBus.B (Alias: Backdoor.SchoolBus.c): This is a backdoor Trojan that copies files to different locations on your computer and then runs those files. When these files are run they attempt to delete various Windows files and send system information to malicious users.

Backdoor.SilverFTP (Aliases: Backdoor.SilverFTP.10, Backdoor:Win32/SilverFTP.1_0): This is a backdoor Trojan that gives a malicious user unauthorized access to your computer. It copies itself as %Windir%\Wincfg32.exe. When Backdoor.SilverFTP runs, it copies itself as %Windir%\Wincfg32.exe and creates the value, "Windows Config Loader %Windir%\Wincfg32.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start Windows. After the Trojan is installed, it notifies the client side and waits for the commands from the remote client. These commands give a malicious user full access to the file system of the infected computer.

Backdoor.Snowdoor (Aliases: Backdoor.Snowdoor, Backdoor:Win32/Snowdoor.A): This is a backdoor Trojan that opens TCP port 5326 or 5328 on the infected computer. The Trojan allows unauthorized access to an infected computer. It is written in the Delphi programming language and is packed with UPX.

DoS-iFrameNet (Aliases: HTML_CRINET.A, Trojan.VBS.IFrame, VBS/DDoS-iFrameNet): This Trojan exists as a VBScript in an HTML document. It attempts to open hundreds of TELNET sessions by creating an iFrame with the source being a Telnet:// address.

JS/Seeker-C (Aliases: Trojan.JS.Seeker.b, JS/Seeker.gen.a trojan): This is a malicious script. The script attempts to modify Internet Explorer settings, such as the Start Page and Search setting. It appears that the script has been designed to do this to redirect traffic to websites (typically the website redirected to will be pornographic, but there is no reason why it could not be another type of website desiring more business). The Trojan writes to registry values under:

- HKCU\Software\Microsoft\Internet Explorer.

JS/Seeker-C does not forward itself to other users, but has to be deliberately installed on a website or forwarded via e-mail from a malicious user.

Pac (Alias: Trojan.Win32.Pac): This Trojan has been reported in the wild. It is a new P2P (peer-to-peer) worm, backdoor, and DoS (Denial of Service) attack tool. The worm travels from one system to another as an EXE bundle that acts as a dropper. When the dropper is run, it activates the embedded P2P worm. The worm installs itself to system as SYSTEM32.EXE file. It sets a hidden attribute to its file. To start its file during every Windows session, the worm creates the following startup keys for it in the Registry:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion Run "SystemSAS" = "system32.exe"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "SystemSAS" = "system32.exe"

Being active the worm copies itself to shared folders of popular file sharing clients KaZaA and iMesh. The worm changes the size of its files to make them match (to some extent of course) the size of software packages it tries to fake. Anyone connecting with KaZaA or iMesh client to an infected computer will discover these fake files. If at least one of these files is downloaded and executed by another person, that computer also becomes infected. The worm has backdoor capabilities. It is controlled via a bot that the worm creates in the specific channel on an IRC server. A malicious user can obtain system information, upload, download, execute files on an infected system, and update the worm's file to a newer version. The worm can be used to perform a DoS (Denial of Service) attack. It can perform a SYN flood attack.

PWS-Aileen: This password-stealing Trojan attempts to retrieved cached passwords on the local system and e-mail them to the author. When run, it expects the filename of the Trojan executable to be nudeAileen.scr. If this is the filename, the Trojan copies itself to the %TEMP% directory as dancingBaby.exe. Regardless of the filename, a registry run key is created to load the Trojan at startup (whether it was copied to the %TEMP% directory or not).

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run\dancingBaby = %TEMP%\dancingBaby.exe

It tries to create an HTML document, strTempHtm.htm, and load it. This document contains a form with an action that points to a remote mailer script on a trellix.com web page. This results in cached passwords getting mailed to the Trojan author.

Tellafriend.Trojan (Alias: Tellafriend): This Trojan was created by ZeroPopUp. Once installed, it sends an e-mail message to all the contacts in your Windows and Microsoft Outlook address books directing them to download them to download the installer from the host's website. (For the program to be installed, you need to agree to install it by clicking Yes when you see the dialog box shown below.)

Tr/SpBit.A: When executed, Tr/SpBit.A drops numerous files in the C directory. The Trojan installs only .LNK files for http websites. On these websites a user is prompted to download dialer software:

Troj/TKBot-A (Aliases: Backdoor.IRC.Demfire, IRC-Sdbot.dr trojan, Backdoor.Tkbot): This is an IRC backdoor Trojan principally targeted at computers running Microsoft IIS version 4 or 5 on Windows NT/2000 and exploiting the "Web Server Folder Traversal" security vulnerability. A description and patch for this vulnerability can be found at Microsoft Security Bulletin MS00-78. When executed, the Trojan creates the folder \<Program Files>\Microsoft\Update\DLL\tk and copies thirty files into this folder. Two of these files, rundll.exe and mstaskmgr.exe, will be started up as services using the clean application FireDaemon.exe which is also packaged with this Trojan. Rundll.exe is the server component of a commercially available FTP server application. Mstaskmgr.exe is a modified mIRC client that works in conjunction with the mIRC script in the file task.cnf to form the core of the backdoor capabilities of this Trojan. The Trojan listens on a particular IRC channel waiting for a connection from a malicious user. A malicious user who connects to this channel will be able to issue commands to Troj/TKBot-A that will then be interpreted as actions to run on the victim's computer. These commands include being able to upload/download files to and from the victim's machine, remotely running executables and accessing information about the victim's computer. The file vmz.exe, also installed in the main folder, contains a self extracting archive that if executed will create the folder \<Windows>\System32\Microsoft\Crypto into which a further thirteen files are copied. The service svhost is then started from the file scvhost.exe. The file scvhost.exe contains an IRC file server application.

Trojan.ProteBoy (Alias: Trojan.Win32.Proteboy): This is a Trojan Horse that deletes the registry backup files. It is written in Microsoft Visual Basic, version 6, and is packed with UPX. The existence of the file ProtectBoy.com is an indication of a possible infection.

Trojan.Idly: This is a Trojan that attempts to gather system information, including your dial-up networking user name and passwords, and send them to the malicious user. When it is executed, it copies itself as %System%\Msatcl32.exe and adds itself as a reference to Msatcl32.exe to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\RunOnce

Next it creates the file, %System%\IdleUI.exe. The Trojan uses this file, which, by itself, does not contain malicious code. This Trojan also sends information to a variety of Web sites. The Trojan may also be able to download content from these Web sites.

W32.Benpao.Trojan: This is a Trojan horse that steals user password and other information. It also modifies the registry such that opening any .chm, .exe, .ini, .reg, .txt, or .scr file will result in executing the Trojan. It is written in the Visual Basic programming language and is packed with UPX, v0.76.1-1.20.

W32/Igloo-15 (Aliases: Backdoor.Igloo.15.b, Win32/BearBritney.A worm, WORM_GOOL.A, Kazoa.C, W32/Gool.worm, Win32.Igloo.15.trojan, W32/Gool.worm.cfg, Win32.Igloo.00.config): This is a backdoor Trojan and Internet worm which spreads via file sharing on KaZaA networks and via IRC channels. When first run W32/Igloo-15 copies itself to the Windows System folder as Explorer.exe and RealWayToHack.exe and creates the following registry entry so that Explorer.exe is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\EXPLORER = %System%\EXPLORER.EXE

W32/Igloo-15 runs continuously in the background, listening on a port, allowing a remote user (using a client program) to gain access and control over the computer. The worm creates the folder %Windows%\Sys32 and copies itself to this folder using various filenames. The worm makes the folder %Windows%\sys32 shareable on KaZaA networks by setting the following registry entries:

- HKCU\Software\Kazaa\LocalContent\dir0 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\dir1 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\dir2 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\dir3 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\dir4 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\dir5 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\DisableSharing = 0

It also drops and runs %System%\Explorer.vbs, which infects the mIRC initialization file mirc.ini. Each time a mIRC session is started mirc.ini is loaded automatically and sends the worm to any users who join any of the current channels. W32/Igloo-15 may terminate selected anti-virus or firewall applications and also sets the following registry entry:

- HKCU\Software\Microsoft\Internet Explorer\Main\RegisteredOrganization = http://www.crash.com

WORM_IXAS.A (Aliases: I-Worm.Ixas, W32/Ixas@MM, W32/GvoWFI.A@mm) (Internet Worm): This nondestructive, non-memory resident worm propagates via e-mail using MAPI (Messaging Application Programming Interface) or SMTP (Simple Mail Transfer Protocol). Upon execution, it drops a copy of itself using a random filename in the Windows system folder. The file name is the base file name of the dropped copy of the worm, i.e. if the dropped copy is ypacww.exe, then the e-mail address will be ypacww@delfi.lt. This worm exploits a known vulnerability affecting unpatched Internet Explorer–based clients, which is commonly known as Automatic Execution of Embedded MIME type. This vulnerability enables e-mail attachments to execute automatically without the recipient opening or double-clicking it. This worm runs on Windows 95, 98, ME, NT, 2000 and XP platforms.

WORM_YAHA.K (Aliases: Win32/Yaha.K, I-Worm.Lentin.i, Win32/Yaha.K@mm, W32/Yaha-K, W32.Yaha.K@mm, W32/Yaha.k): (Internet Worm): This mass-mailing worm uses its own SMTP engine to propagate via e-mail as an attachment, mailing itself to addresses retrieved from the infected system's Windows Address Book (WAB), Yahoo Messenger, MSN and .NET Messenger Services, and files found in all directories with extension names containing the string "HT." It

randomly selects the contents of its e-mail subject line, message body, and attachment name from preset information in its code. Because of its very smart stealth and anti-anti-virus technique, most common AV software can't detect or clean it. Like the other YAHA worm variants, this malware also terminates certain processes from memory that are related to popular antivirus and security software. This variant exhibits the following payloads:

- Displays a message box
- Swaps the left and right click mouse functions
- Drops a hidden non-malicious text file in the Windows desktop
- Hides files and folders in the Personal folder (usually C:\My Documents)
- Modifies the Internet Explorer home page.

This worm launches a DoS attack against a particular site and terminates the Task Manager under Windows NT, 2000, and XP. It runs on Windows 9x, NT, 2000, ME, and XP.

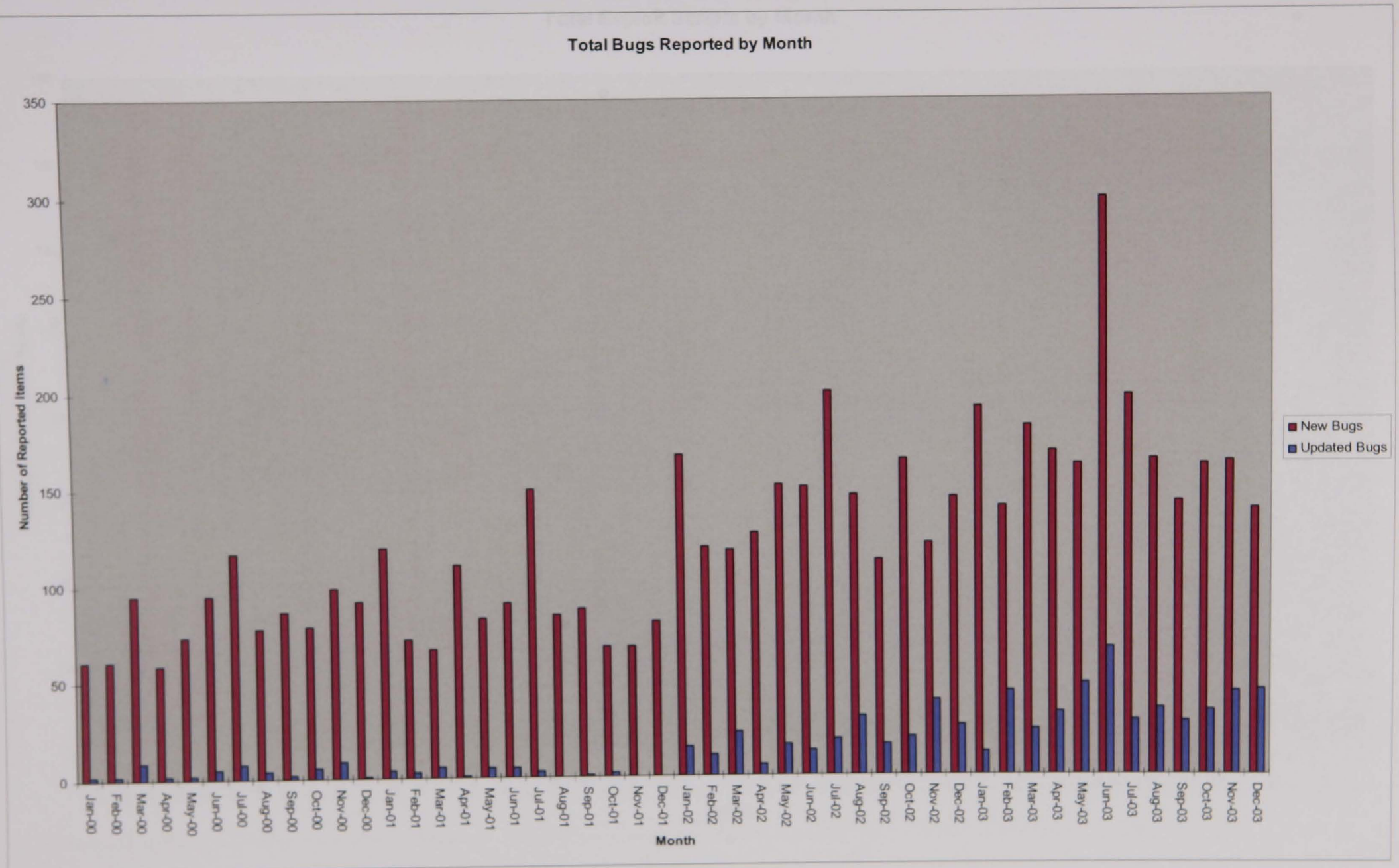
W32.Yinker.Trojan (Alias: Trojan.Win32.Yinker: This Trojan creates a new user named Yinker and adds this user to the Administrator group on Windows NT4.0/2000/XP. W32.Yinker.Trojan also stops and restarts the Telnet service.

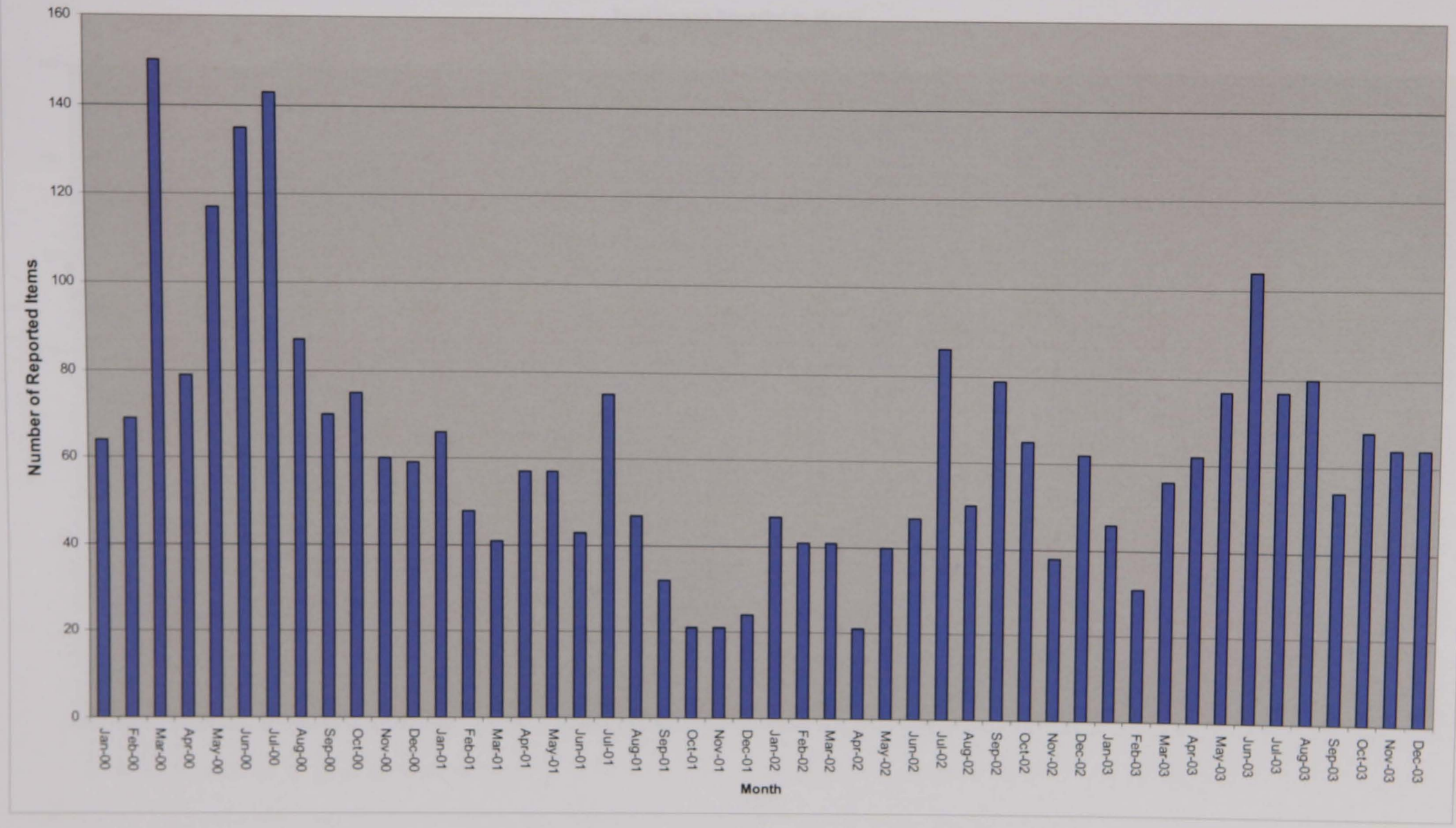
SUPPLEMENT TWO

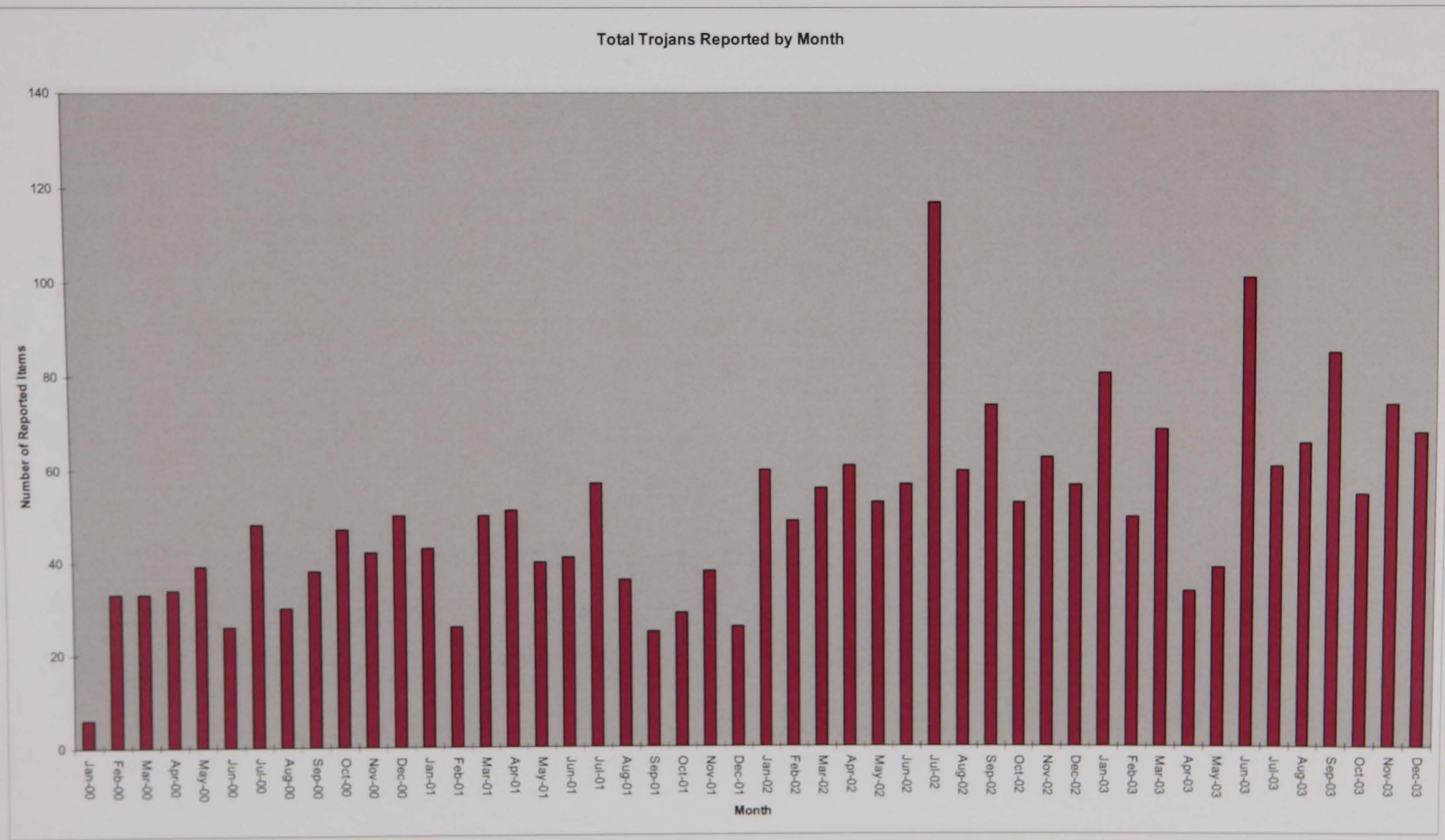
CYBERNOTES MONTHLY

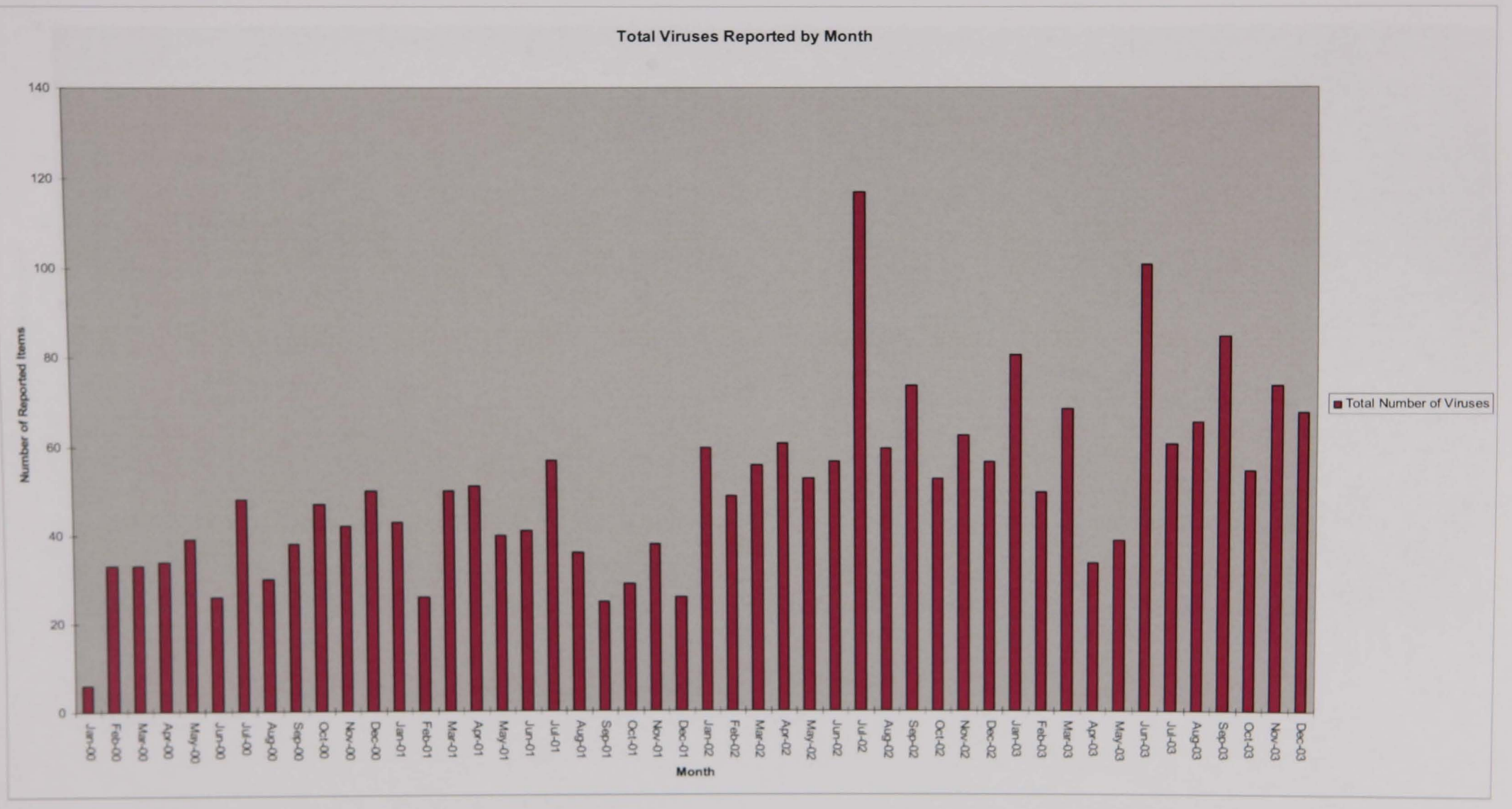
and

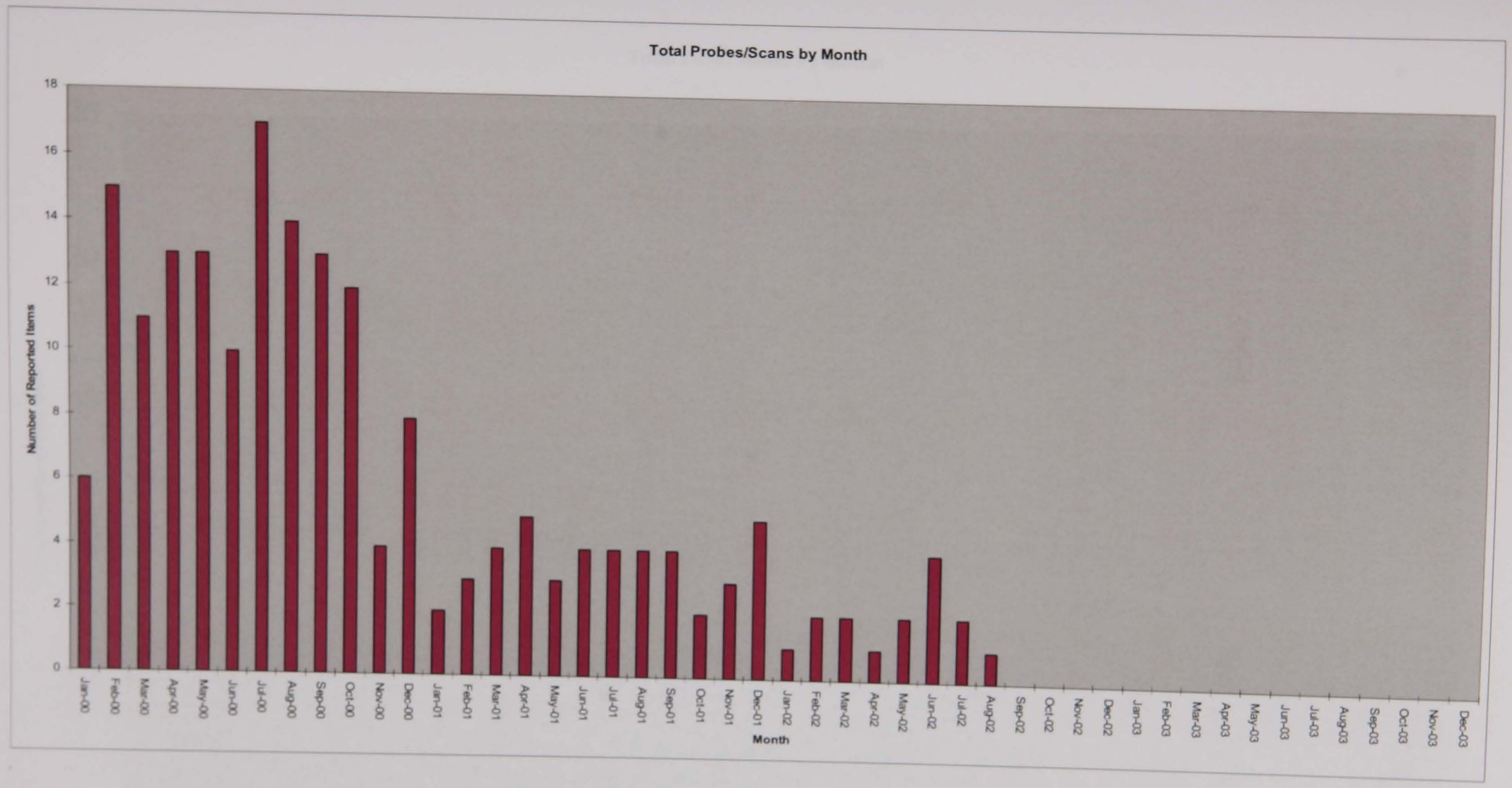
ISSUE LEVEL FREQUENCY DISTRIBUTIONS

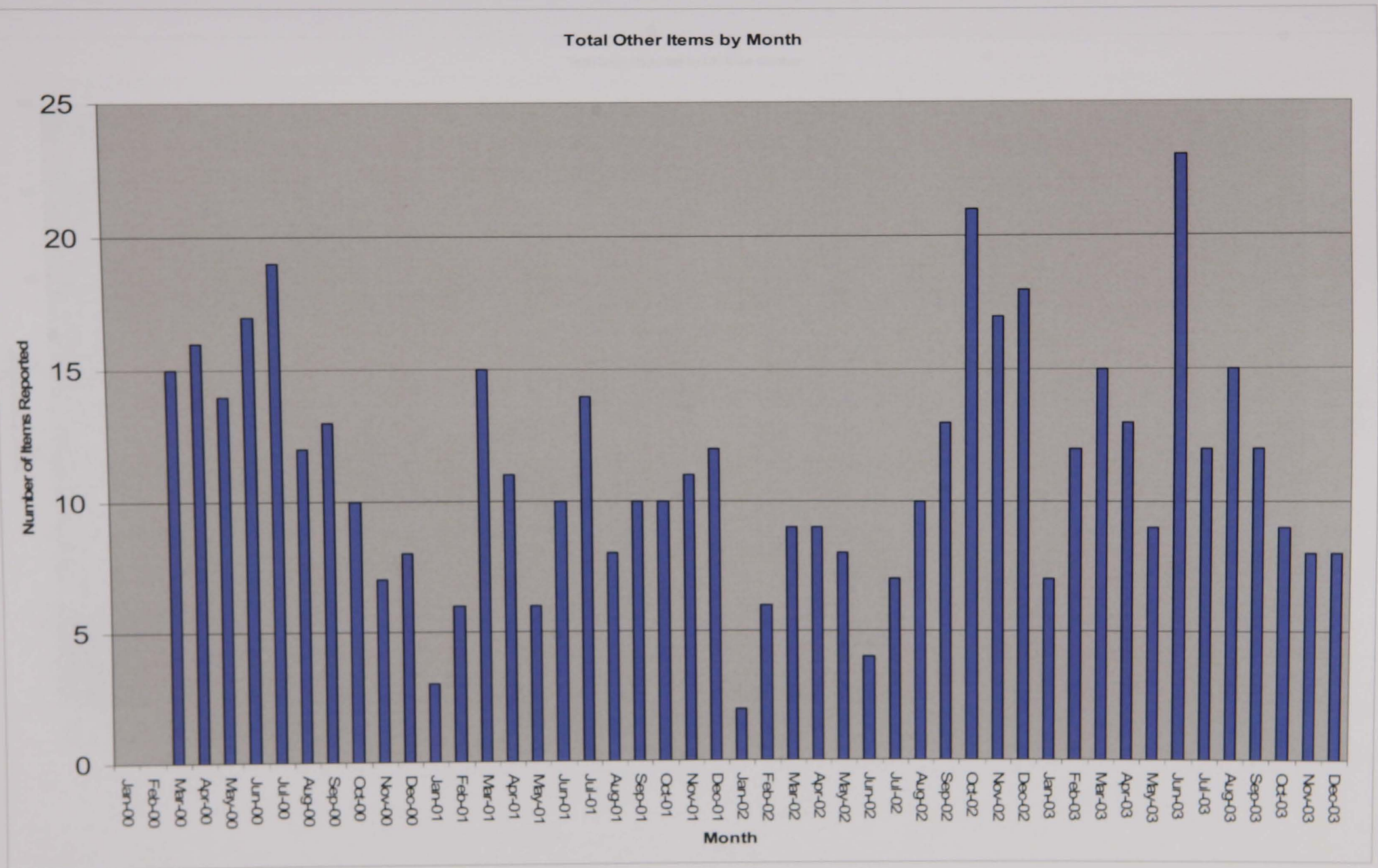

Total Bugs Reported by Month
Number of Reported Items
350
300
250
200
150
100
50
0
Jan-00
Feb-00
Mar-00
Apr-00
May-00
Jun-00
Jul-00
Aug-00
Sep-00
Oct-00
Nov-00
Dec-00
Jan-01
Feb-01
Mar-01
Apr-01
May-01
Jun-01
Jul-01
Aug-01
Sep-01
Oct-01
Nov-01
Dec-01
Jan-02
Feb-02
Mar-02
Apr-02
May-02
Jun-02
Jul-02
Aug-02
Sep-02
Oct-02
Nov-02
Dec-02
Jan-03
Feb-03
Mar-03
Apr-03
May-03
Jun-03
Jul-03
Aug-03
Sep-03
Oct-03
Nov-03
Dec-03
Month
New Bugs
Updated Bugs

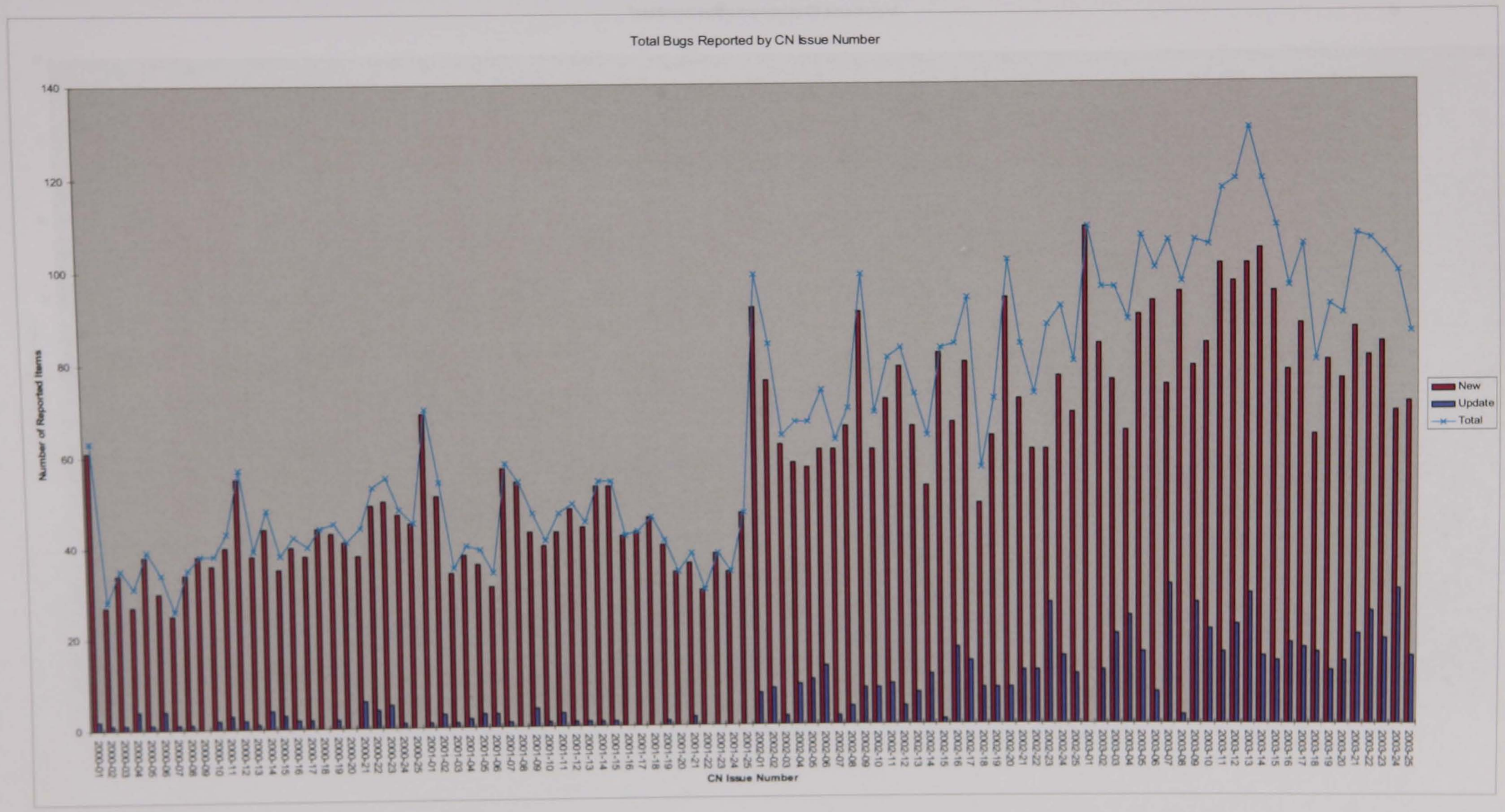

Total Exploit Scripts by Month
Number of Reported Items
160
140
120
100
80
60
40
20
0
Jan-00
Feb-00
Mar-00
Apr-00
May-00
Jun-00
Jul-00
Aug-00
Sep-00
Oct-00
Nov-00
Dec-00
Jan-01
Feb-01
Mar-01
Apr-01
May-01
Jun-01
Jul-01
Aug-01
Sep-01
Oct-01
Nov-01
Dec-01
Jan-02
Feb-02
Mar-02
Apr-02
May-02
Jun-02
Jul-02
Aug-02
Sep-02
Oct-02
Nov-02
Dec-02
Jan-03
Feb-03
Mar-03
Apr-03
May-03
Jun-03
Jul-03
Aug-03
Sep-03
Oct-03
Nov-03
Dec-03
Month

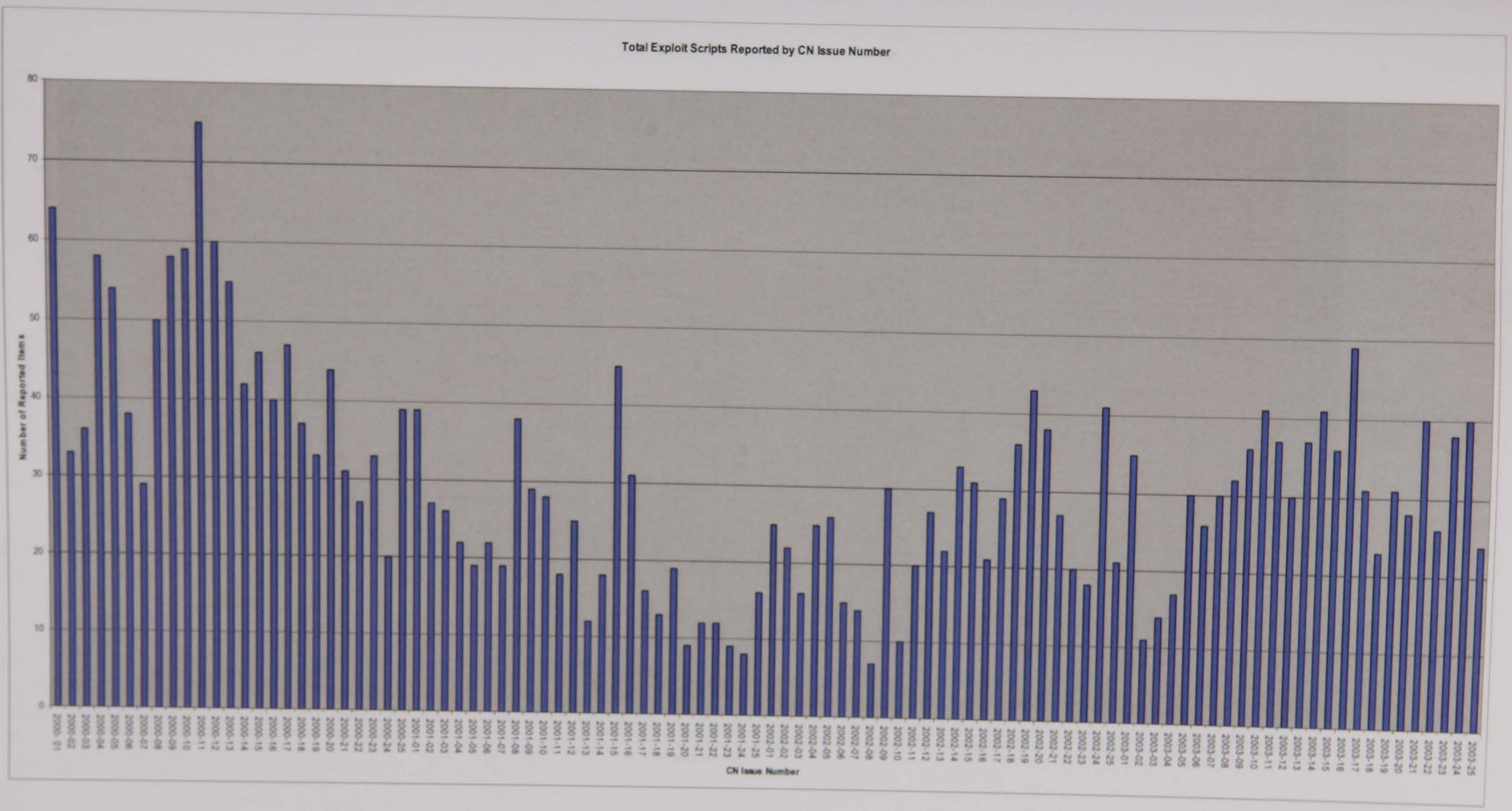

Total Trojans Reported by Month
Number of Reported Items
0
20
40
60
80
100
120
140
Jan-00
Feb-00
Mar-00
Apr-00
May-00
Jun-00
Jul-00
Aug-00
Sep-00
Oct-00
Nov-00
Dec-00
Jan-01
Feb-01
Mar-01
Apr-01
May-01
Jun-01
Jul-01
Aug-01
Sep-01
Oct-01
Nov-01
Dec-01
Jan-02
Feb-02
Mar-02
Apr-02
May-02
Jun-02
Jul-02
Aug-02
Sep-02
Oct-02
Nov-02
Dec-02
Jan-03
Feb-03
Mar-03
Apr-03
May-03
Jun-03
Jul-03
Aug-03
Sep-03
Oct-03
Nov-03
Dec-03
Month

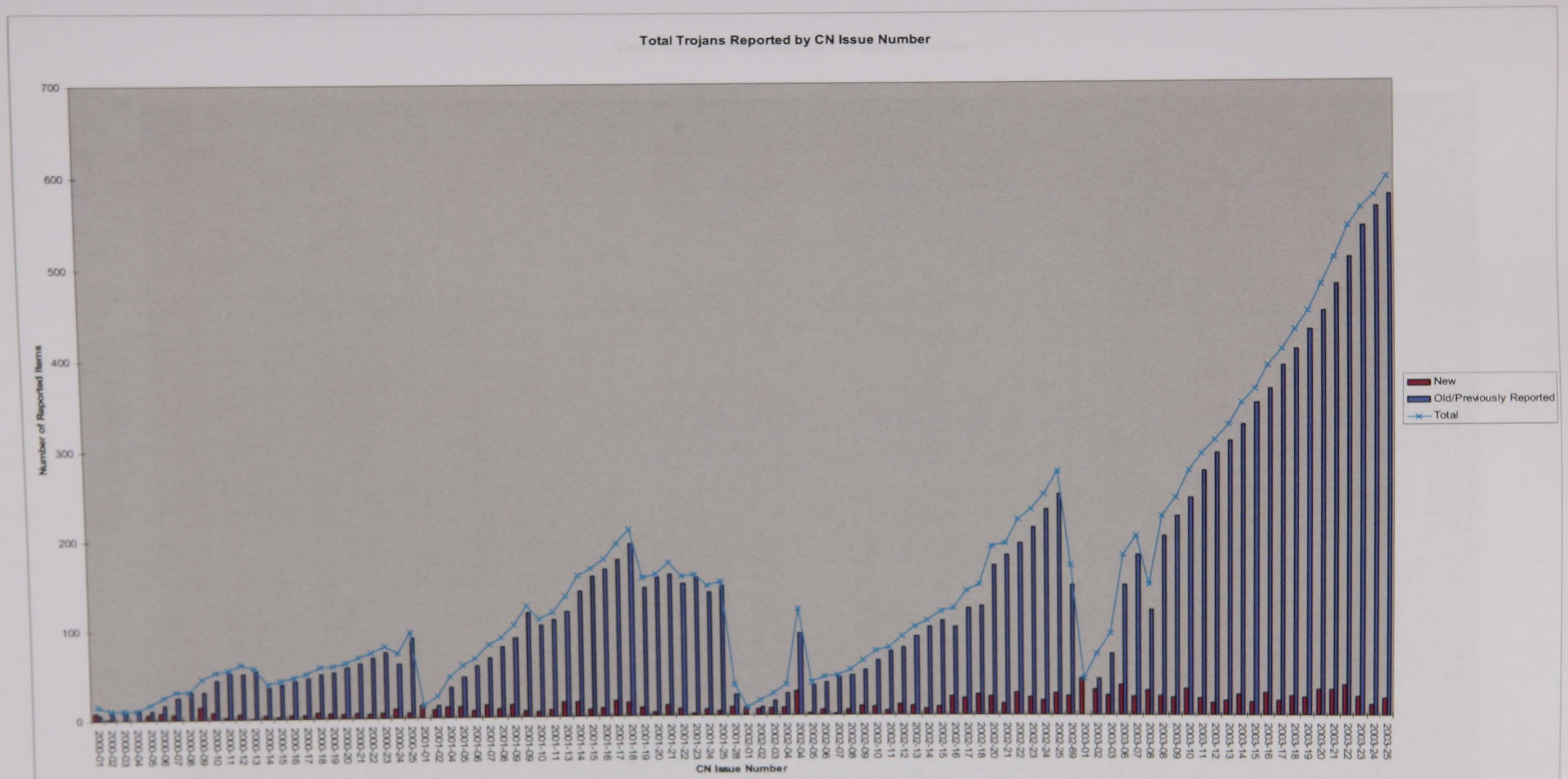

Total Viruses Reported by Month
Number of Reported Items
0
20
40
60
80
100
120
140
Jan-00
Feb-00
Mar-00
Apr-00
May-00
Jun-00
Jul-00
Aug-00
Sep-00
Oct-00
Nov-00
Dec-00
Jan-01
Feb-01
Mar-01
Apr-01
May-01
Jun-01
Jul-01
Aug-01
Sep-01
Oct-01
Nov-01
Dec-01
Jan-02
Feb-02
Mar-02
Apr-02
May-02
Jun-02
Jul-02
Aug-02
Sep-02
Oct-02
Nov-02
Dec-02
Jan-03
Feb-03
Mar-03
Apr-03
May-03
Jun-03
Jul-03
Aug-03
Sep-03
Oct-03
Nov-03
Dec-03
Month
Total Number of Viruses


Total Probes/Scans by Month
Number of Reported Items
0
2
4
6
8
10
12
14
16
18
Jan-00
Feb-00
Mar-00
Apr-00
May-00
Jun-00
Jul-00
Aug-00
Sep-00
Oct-00
Nov-00
Dec-00
Jan-01
Feb-01
Mar-01
Apr-01
May-01
Jun-01
Jul-01
Aug-01
Sep-01
Oct-01
Nov-01
Dec-01
Jan-02
Feb-02
Mar-02
Apr-02
May-02
Jun-02
Jul-02
Aug-02
Sep-02
Oct-02
Nov-02
Dec-02
Jan-03
Feb-03
Mar-03
Apr-03
May-03
Jun-03
Jul-03
Aug-03
Sep-03
Oct-03
Nov-03
Dec-03
Month

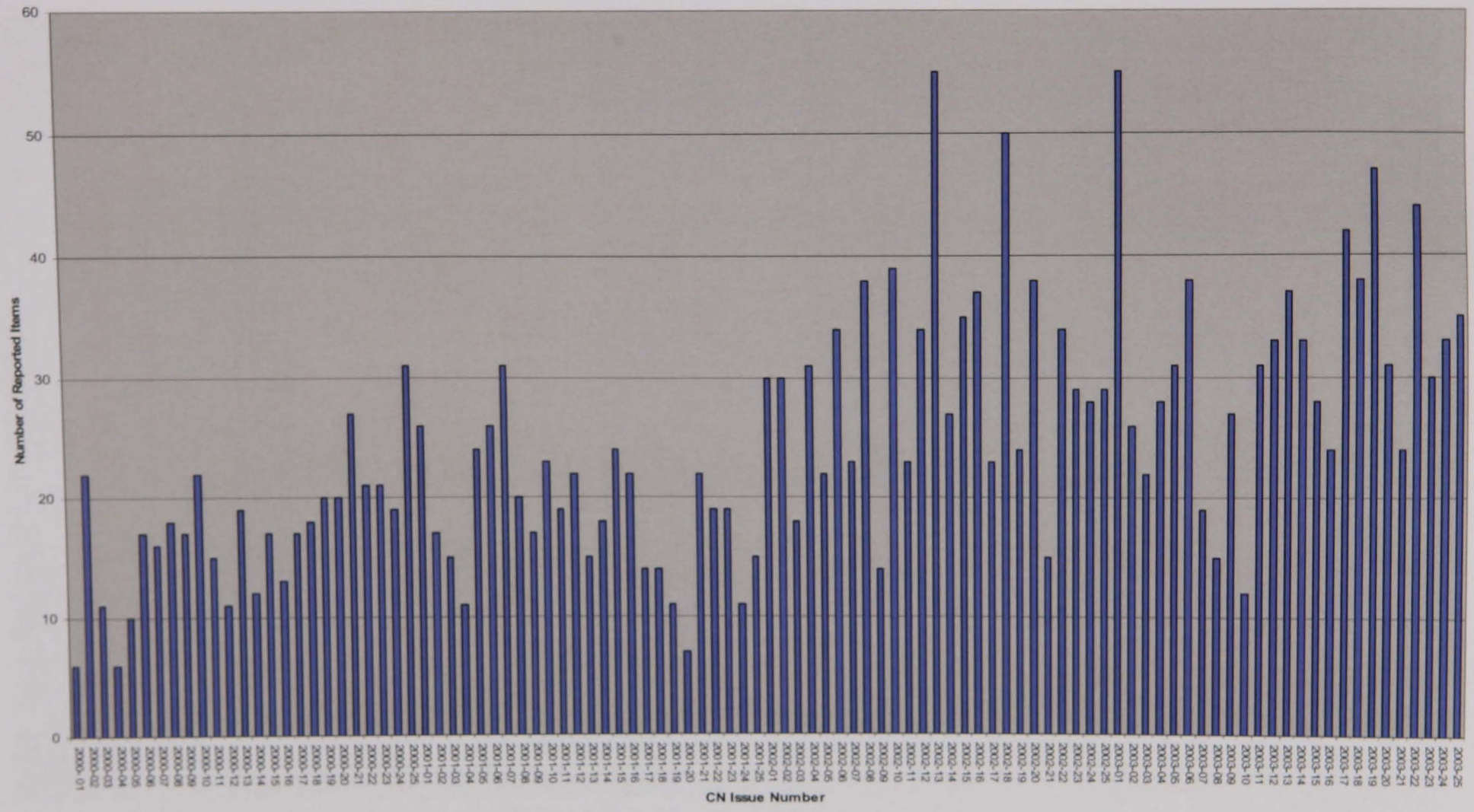

Total Other Items by Month
Number of Items Reported
25
20
15
10
5
0
Jan-00
Feb-00
Mar-00
Apr-00
May-00
Jun-00
Jul-00
Aug-00
Sep-00
Oct-00
Nov-00
Dec-00
Jan-01
Feb-01
Mar-01
Apr-01
May-01
Jun-01
Jul-01
Aug-01
Sep-01
Oct-01
Nov-01
Dec-01
Jan-02
Feb-02
Mar-02
Apr-02
May-02
Jun-02
Jul-02
Aug-02
Sep-02
Oct-02
Nov-02
Dec-02
Jan-03
Feb-03
Mar-03
Apr-03
May-03
Jun-03
Jul-03
Aug-03
Sep-03
Oct-03
Nov-03
Dec-03
Month

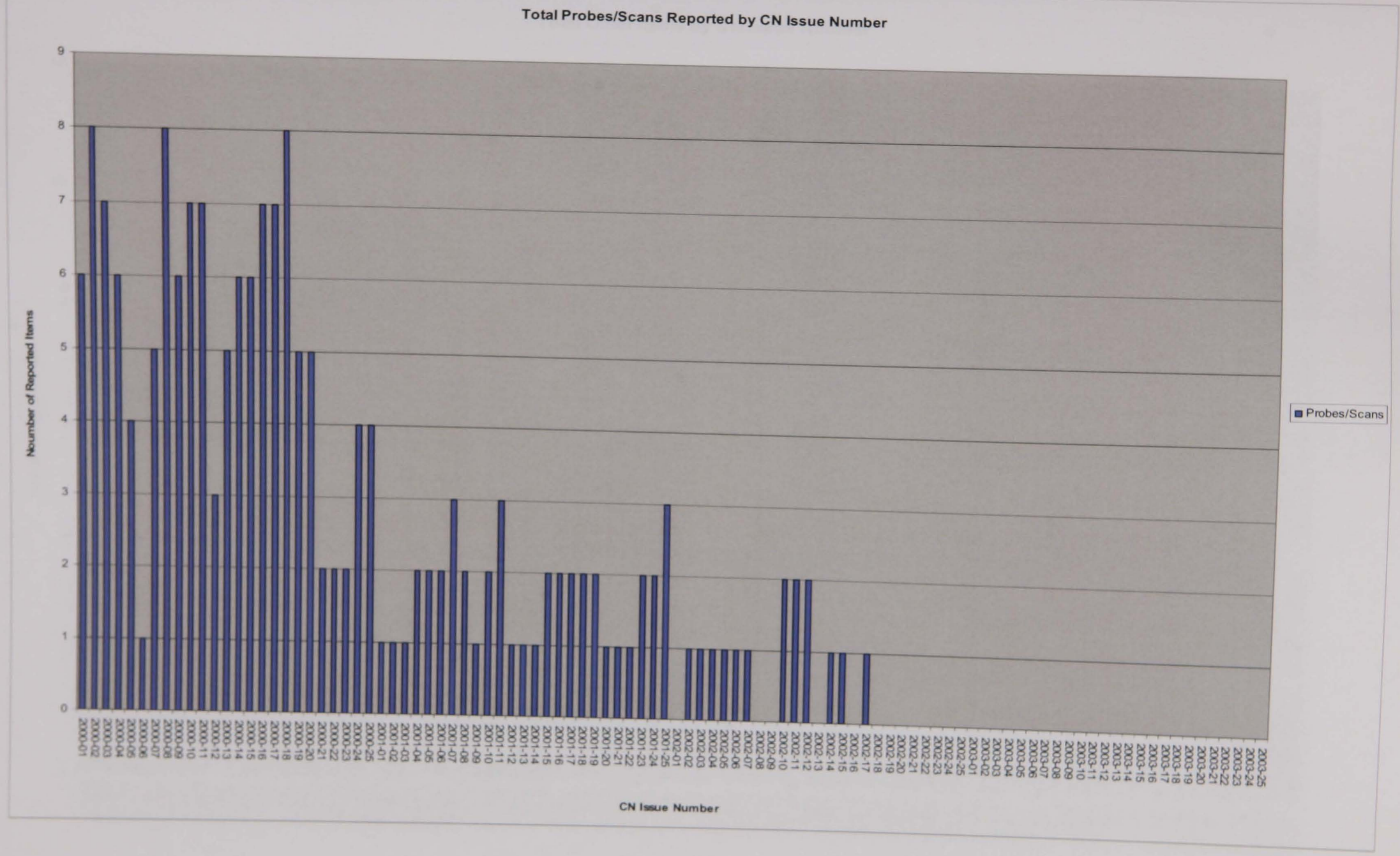

Total Bugs Reported by CN Issue Number
Number of Reported Items
0
20
40
60
80
100
120
140
CN Issue Number
2000-01
2000-02
2000-03
2000-04
2000-05
2000-06
2000-07
2000-08
2000-09
2000-10
2000-11
2000-12
2000-13
2000-14
2000-15
2000-16
2000-17
2000-18
2000-19
2000-20
2000-21
2000-22
2000-23
2000-24
2000-25
2001-01
2001-02
2001-03
2001-04
2001-05
2001-06
2001-07
2001-08
2001-09
2001-10
2001-11
2001-12
2001-13
2001-14
2001-15
2001-16
2001-17
2001-18
2001-19
2001-20
2001-21
2001-22
2001-23
2001-24
2001-25
2002-01
2002-02
2002-03
2002-04
2002-05
2002-06
2002-07
2002-08
2002-09
2002-10
2002-11
2002-12
2002-13
2002-14
2002-15
2002-16
2002-17
2002-18
2002-19
2002-20
2002-21
2002-22
2002-23
2002-24
2002-25
2003-01
2003-02
2003-03
2003-04
2003-05
2003-06
2003-07
2003-08
2003-09
2003-10
2003-11
2003-12
2003-13
2003-14
2003-15
2003-16
2003-17
2003-18
2003-19
2003-20
2003-21
2003-22
2003-23
2003-24
2003-25
New
Update
Total

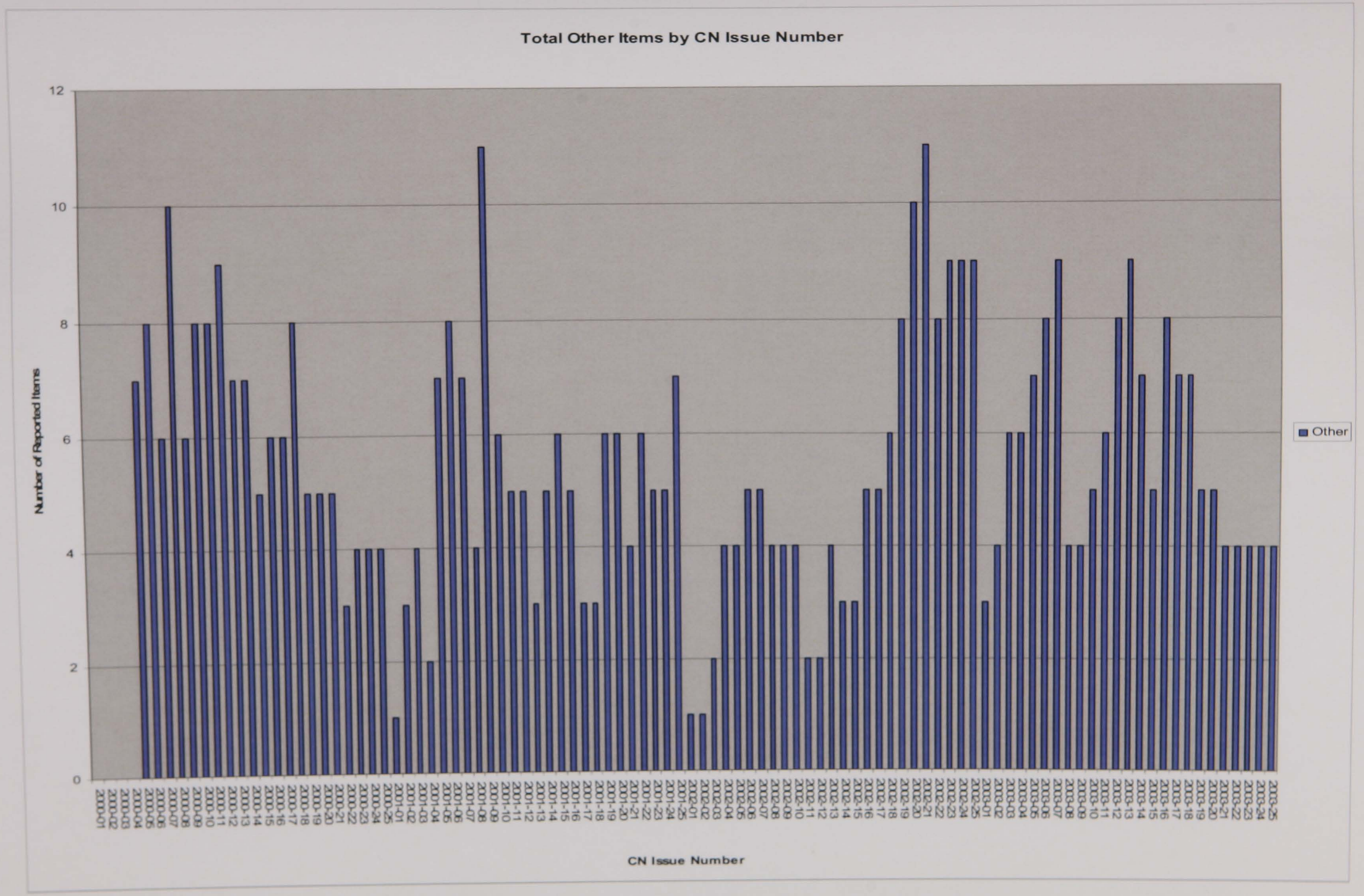

Total Exploit Scripts Reported by CN Issue Number
Number of Reported Items
0
10
20
30
40
50
60
70
80
CN Issue Number
2000-01
2000-02
2000-03
2000-04
2000-05
2000-06
2000-07
2000-08
2000-09
2000-10
2000-11
2000-12
2000-13
2000-14
2000-15
2000-16
2000-17
2000-18
2000-19
2000-20
2000-21
2000-22
2000-23
2000-24
2000-25
2001-01
2001-02
2001-03
2001-04
2001-05
2001-06
2001-07
2001-08
2001-09
2001-10
2001-11
2001-12
2001-13
2001-14
2001-15
2001-16
2001-17
2001-18
2001-19
2001-20
2001-21
2001-22
2001-23
2001-24
2001-25
2002-01
2002-02
2002-03
2002-04
2002-05
2002-06
2002-07
2002-08
2002-09
2002-10
2002-11
2002-12
2002-13
2002-14
2002-15
2002-16
2002-17
2002-18
2002-19
2002-20
2002-21
2002-22
2002-23
2002-24
2003-01
2003-02
2003-03
2003-04
2003-05
2003-06
2003-07
2003-08
2003-09
2003-10
2003-11
2003-12
2003-13
2003-14
2003-15
2003-16
2003-17
2003-18
2003-19
2003-20
2003-21
2003-22
2003-23
2003-24
2003-25


Total Trojans Reported by CN Issue Number
Number of Reported Items
0
100
200
300
400
500
600
700
New
Old/Previously Reported
Total
CN Issue Number
2000-01
2000-02
2000-03
2000-04
2000-05
2000-06
2000-07
2000-08
2000-09
2000-10
2000-11
2000-12
2000-13
2000-14
2000-15
2000-16
2000-17
2000-18
2000-19
2000-20
2000-21
2000-22
2000-23
2000-24
2000-25
2001-01
2001-02
2001-04
2001-05
2001-06
2001-07
2001-08
2001-09
2001-10
2001-11
2001-13
2001-14
2001-15
2001-16
2001-17
2001-18
2001-19
2001-20
2001-21
2001-22
2001-23
2001-24
2001-25
2001-28
2002-01
2002-02
2002-03
2002-04
2002-05
2002-06
2002-07
2002-08
2002-09
2002-10
2002-11
2002-12
2002-13
2002-14
2002-15
2002-16
2002-17
2002-18
2002-20
2002-21
2002-22
2002-23
2002-24
2002-25
2002-69
2003-01
2003-02
2003-03
2003-06
2003-07
2003-08
2003-09
2003-10
2003-11
2003-12
2003-13
2003-14
2003-15
2003-16
2003-17
2003-18
2003-19
2003-20
2003-21
2003-22
2003-23
2003-24
2003-25

Total Viruses Reported by CN Issue Number




Total Probes/Scans Reported by CN Issue Number
Number of Reported Items
0
1
2
3
4
5
6
7
8
9
2000-01
2000-02
2000-03
2000-04
2000-05
2000-06
2000-07
2000-08
2000-09
2000-10
2000-11
2000-12
2000-13
2000-14
2000-15
2000-16
2000-17
2000-18
2000-19
2000-20
2000-21
2000-22
2000-23
2000-24
2000-25
2001-01
2001-02
2001-03
2001-04
2001-05
2001-06
2001-07
2001-08
2001-09
2001-10
2001-11
2001-12
2001-13
2001-14
2001-15
2001-16
2001-17
2001-18
2001-19
2001-20
2001-21
2001-22
2001-23
2001-24
2001-25
2002-01
2002-02
2002-03
2002-04
2002-05
2002-06
2002-07
2002-08
2002-09
2002-10
2002-11
2002-12
2002-13
2002-14
2002-15
2002-16
2002-17
2002-18
2002-19
2002-20
2002-21
2002-22
2002-23
2002-24
2002-25
2003-01
2003-02
2003-03
2003-04
2003-05
2003-06
2003-07
2003-08
2003-09
2003-10
2003-11
2003-12
2003-13
2003-14
2003-15
2003-16
2003-17
2003-18
2003-19
2003-20
2003-21
2003-22
2003-23
2003-24
2003-25
CN Issue Number
Probes/Scans


Total Other Items by CN Issue Number
Number of Reported Items
0
2
4
6
8
10
12
CN Issue Number
Other
2000-01
2000-02
2000-03
2000-04
2000-05
2000-06
2000-07
2000-08
2000-09
2000-10
2000-11
2000-12
2000-13
2000-14
2000-15
2000-16
2000-17
2000-18
2000-19
2000-20
2000-21
2000-22
2000-23
2000-24
2000-25
2001-01
2001-02
2001-03
2001-04
2001-05
2001-06
2001-07
2001-08
2001-09
2001-10
2001-11
2001-12
2001-13
2001-14
2001-15
2001-16
2001-17
2001-18
2001-19
2001-20
2001-21
2001-22
2001-23
2001-24
2001-25
2002-01
2002-02
2002-03
2002-04
2002-05
2002-06
2002-07
2002-08
2002-09
2002-10
2002-11
2002-12
2002-13
2002-14
2002-15
2002-16
2002-17
2002-18
2002-19
2002-20
2002-21
2002-22
2002-23
2002-24
2002-25
2003-01
2003-02
2003-03
2003-04
2003-05
2003-06
2003-07
2003-08
2003-09
2003-10
2003-11
2003-12
2003-13
2003-14
2003-15
2003-16
2003-17
2003-18
2003-19
2003-20
2003-21
2003-22
2003-23
2003-24
2003-25