Computer viruses: a quantitative analysis

A. Coulthard and T.A. Vuori

The authors

A. Coulthard is IT Manager, Pearson Jones plc, Leeds, UK.
T.A. Vuori is Senior Lecturer at Murdoch University, Murdoch, Australia.

Keywords

Computers, Viruses

Abstract

This paper provides interesting insights for anti-virus research, as it reflects a period of rapid uptake in the application of the Internet and the use of e-mail for business purposes. The purpose of the research is to provide independent justification of the growing prevalence of computer virus incidents over the past five years, and identify patterns in the frequency and distribution of computer viruses. Specifically, the analysis focuses on examining the claims that computer viruses are increasing in prevalence, that computer viruses follow an evolutionary pattern and that seasonality exists in the distribution of computer viruses.

Electronic access

The research register for this journal is available at
http://www.emeraldinsight.com/researchregisters

The current issue and full text archive of this journal is available at
http://www.emeraldinsight.com/0957-6053.htm

Logistics Information Management
Volume 15 · Number 5/6 · 2002 · pp. 400–409
© MCB UP Limited · ISSN 0957-6053
DOI 10.1108/09576050210447091

Introduction

Anti-virus research indicates a worldwide increase in the prevalence of computer viruses, which has been largely attributed to the growing ease of virus distribution, fuelled by the increased application of the Internet and e-mail for business purposes. Annual research conducted by ICSA Laboratories into the prevalence of computer viruses, suggests the threat posed by viruses is worsening, with the "likelihood of a company experiencing a computer virus having doubled each year for the past five years", (Bridwell and Tibbett, 2000). In addition to the increased prevalence of computer viruses, the nature of the virus threat is also evolving. As advancements are made in operating and applications environments, changes in technology have facilitated the development of new types of viruses that propagate more rapidly, are more widely distributed and more effective in avoiding detection. Organizations that fail to update virus protection systems regularly will remain unnecessarily exposed, as methods proven effective in protecting against boot sector viruses, spread predominately by floppy disk, are not likely to provide any defense against file or script viruses, which are typically distributed by e-mail.

Anti-virus research indicates that patterns may also exist in the distribution and frequency of computer viruses. Specifically, statistics indicate the increased prevalence of computer viruses around the holiday seasons. According to Banes (2001) there are "increased levels of virus and worm activity around Easter time". Although the Melissa, the Love Bug, and the AnnaK viruses were all released during the April-May period, quantitative analysis is not publicly available to support the claim that seasonality may occur in the distribution of computer viruses.

The purpose of this research is to provide independent justification of the growing prevalence of computer virus incidents and identify patterns in frequency and distribution of computer viruses that may better prepare and protect organizations from vulnerability and exposure to virus threats.

The time period selected for analysis was the five-year span May 1996 to May 2001, which enabled 61 months of data to be included in the analysis. The data comprised five consecutive years of reported virus incidents and included an additional month for May, which is a time period of particular relevance to the analysis undertaken.

Data collection

Statistics used in the analysis were sourced from publicly available lists published by Virus Bulletin (2001) and the Wildlist Organisation. The virus prevalence tables, compiled by Virus Bulletin, provide a listing of the number of reported virus incidents over the period May 1996 to May 2001, whilst the Wildlist, produced by Wildlist International, is a listing of viruses and malicious code, known to be in the wild. Both lists are compiled on a monthly basis according to confirmed reported virus infections from a small group of independent reporting organizations. The Virus Bulletin and the Wildlist Organisation are considered to be reputable sources and well-regarded references on computer virus information.

Sample size

The reporting organization sample size is fairly small (16 organisations), however each of the reporting organizations are large corporations or government departments, with greater than 10,000 PCs. Reporting organizations were not selected at random, rather selection was based on a number of factors aimed at preserving the quality of the dataset, including accuracy, consistency and reliability.

Methodology

A three-part analysis of the time-series was undertaken. The analysis focused on computer virus incidents by virus type, with particular focus on the four major virus types: boot, file, macro and script viruses. As similarities occur in the distribution mechanism and payload of viruses of the same type, it is believed that an analysis of incidents by virus type would reveal patterns in distribution and frequency, without specific reference to the impact or distribution of individual computer viruses

The methodology for the analysis required the use of applied statistics and time series regression to determine the existence of patterns in the frequency and distribution of computer viruses and the existence of seasonality.

Prevalence of computer viruses

The prevalence of computer viruses over the six-year period, May 1996 to May 2001 was first plotted, and summary and descriptive statistics calculated by year, as well as for each month, to determine whether a causal relationship existed between time and the increased prevalence of computer viruses.

Evolution

The second stage involved an analysis of the type of viruses reported over the five-year period against the number of reported virus incidents, plotting against time, to determine the existence of a pattern between the type of virus and the number of reported incidents over time. The findings were then compared to the introduction of new technologies, including the introduction of Windows 95 operating system, Microsoft Office 97, Internet Explorer 5.0 and virus scripting tools to determine if an evolutionary pattern exists in virus distribution.

Seasonality in distribution

Data were analyzed for possible seasonality, seasonal indexes calculated, and the original time series data deseasonalised to allow for the identification of the existence of patterns in frequency and distribution of virus incidents.

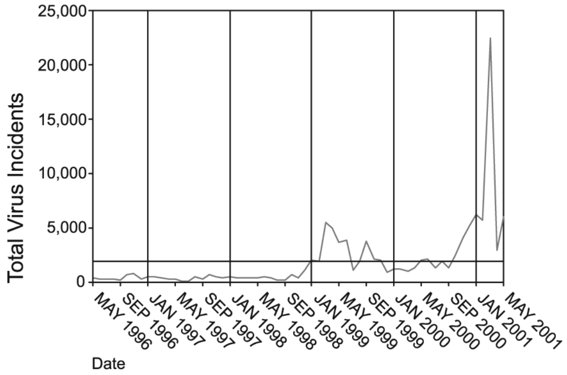
Results

Prevalence of computer viruses

Analysis of reported virus incidents during the five-year period May 1996 to May 2001 provides interesting insights for anti-virus research, as it reflects a period of rapid uptake in the application of the Internet and the use of e-mail for business purposes; two factors that would have had significant implications for the rate of distribution of computer viruses. Not surprisingly, there is a substantial increase in the number of incidents reported during the five-year period, as shown in Figure 1.

Overall, significant growth has occurred in the number reported virus incidents between May 1996 and May 2001, which is best represented by a breakdown of the total of

Figure 1 Total number of virus incidents (May 1996 to May 2001)



virus incidents reported during the five-year period, as shown in Figure 2. Significantly, trend analysis indicates that the high rate of growth in the number of virus incidents is indicative of a strong linear relationship, between the total number of virus incidents over time. As shown in Figure 2, strong correlation does exist between virus incidents over time, as supported statistically by a high coefficient of correlation ($R = 0.91$), which is the total explained variance of virus incidents over time.

Significantly, two substantial jumps in the number of reported virus incidents occurred during the five-year period. As shown by Figure 3, until 1998, the number of reported virus incidents remained at a relatively constant rate, with less than 5,000 incidents being reported each year for the periods May 1996 to May 1997 and May 1997 to May 1998.

During May 1998 to May 1999, the number of virus incidents increased from an average of 25 virus incidents per organization per month, as reported during the previous two periods (May 1996 to May 1998), to approximately 95 virus incidents reported during May 1998 to May 1999. This was largely a result of the increasing prevalence of macro viruses, although the growing use of Internet and e-mail may have also contributed to the widespread and rapid distribution of computer viruses. A breakdown of the number of virus incidents by virus type as a proportion of the total number of virus incidents is shown in Figure 3.

Figure 2 Total virus incidents (May 1996 to May 2001)

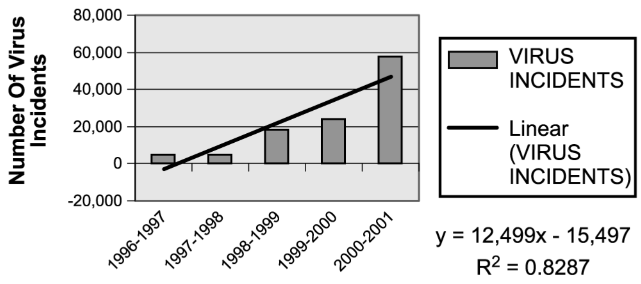
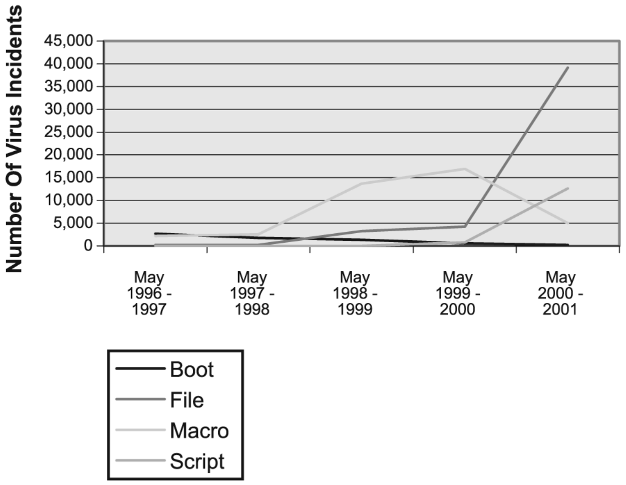


Figure 3 Reported virus incidents (May 1996 to May 2001)



The second period of rapid growth occurred in May 2000 to May 2001, whereby the number of reported virus incidents jumped 140 per cent from the previous year. This is largely attributed to the effects of several widely distributed script viruses, including the Loveletter, Kakworm and Pretty Park viruses.

Overall, the rate of growth in the number of reported virus incidents over the five-year period is alarming. According to the findings, an organization in 1996 experienced on average 25 virus incidents per month, which increased to an average of 300 virus incidents per organization, per month in the May 2000 to May 2001 period. This represents a staggering 12-fold increase in the average number of virus incidents during the five-year period. This is supportive of the findings of the *Sixth Annual ICSA Labs Virus Prevalence Survey 2000*, which estimates "approximately a two-fold growth per year for each of the last five years", (Bridwell and Tibbett, 2000) in the number of reported virus incidents.

Unfortunately a direct comparison of the average number of virus incidents per month between the ICSA findings, which represents virus incidents per 1,000 PCs, and the analysis undertaken is not possible, as the total number of PCs included in the sample is unknown. However, it is of interest that ICSA virus prevalence survey 1999 findings indicated "a global incidence rate of 13 encounters per 1,000 PCs per month over the survey period" (Kabay *et al.*, 1999), a figure which increased to 88 virus incidents per 1,000 PCs reported in February 1999, which was the end of the survey period.

Boot sector virus incidents

As shown in Figure 4, there has been a significant decline in the number of reported boot sector virus incidents reported in the last five years, representing a strong negative linear relationship between boot sector virus incidents over time, with total explained variance of $R = 0.75$.

Peaking in 4Q1996, a total of 439 boot sector virus incidents were reported in October 1996, which represented more than 60 per cent of incidents reported for that month. This decreased to 18 incidents reported May 2001, which accounted approximately for 0.2 per cent of virus incidents. This decline is demonstrated by the drop in total number of boot sector viruses reported in each 12-month period is shown in Figure 5.

Despite the declining trend, 225 boot sector virus incidents were still reported within the 12-month period May 2000 to May 2001. This equates to an average of 19 boot sector incidents that were reported each month during May 2000 to May 2001, which is considerable, particularly, given the small sample size. Importantly, this translates to more than one boot sector virus incident per organization per month, which indicates that it is therefore premature, to assume that the threat from boot sector viruses can be discounted.

Figure 4 Boot sector virus incidents (May 1996 to May 2001)

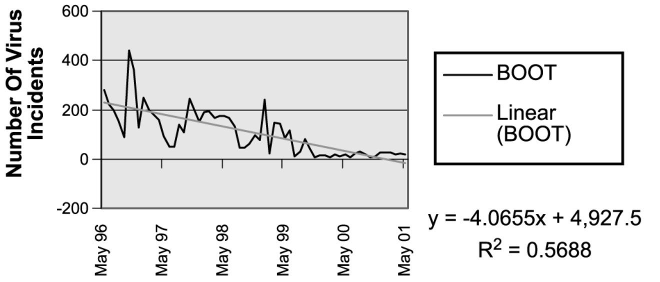
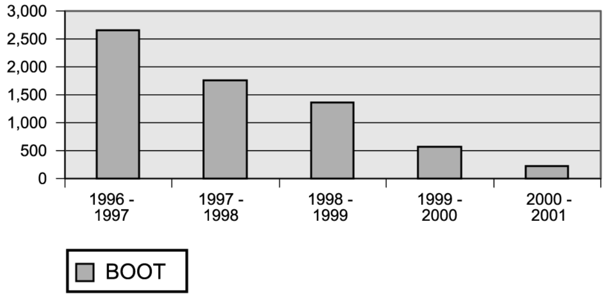


Figure 5 Total number of boot sector viruses reported in each 12-month period (1996-2001)



Macro virus incidents

Despite claims of increasing prevalence of macro viruses, an analysis of reported macro virus incidents, indicates that these claims may lack support from a statistical perspective. Whilst analysis of trend does indicate a slight linear relationship between virus incidents over time, the correlation ($R = 0.3231$) is not considered statistically significant at the 95 per cent confidence level. Rather, it would appear that these findings are strongly influenced by significant growth in the number of macro viruses in 1999, as opposed to indicating a long-term trend in the growth in the number of macro virus incidents, which may in fact be experiencing a state of decline, as shown in Figure 6.

The number of reported macro virus incidents increases from 1,710 incidents reported in the May 1996 to May 1997 period, to over 18,500 macro virus incidents reported May 1999 to May 2000, representing a significant rate of growth during this time. This represents an increase from an average of 16 macro virus incidents per organization, per month, in the May 1996 to May 1997 period, to 137 macro virus incidents per organization, per month, in the May 1999 to May 2000 period.

As shown in Figure 7, the distribution of macro viruses peaked in September 1999, during which macro viruses accounted for over 90 per cent of all reported virus incidents. However, this figure dropped quickly in the 2000 to 2001 period, such that less than 9 per cent of virus incidents were

Figure 6 Macro virus incidents (May 1996 to May 2001)

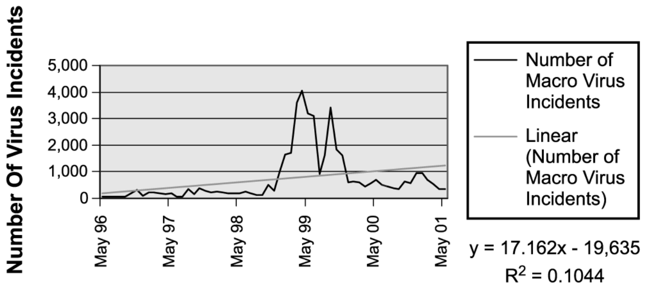
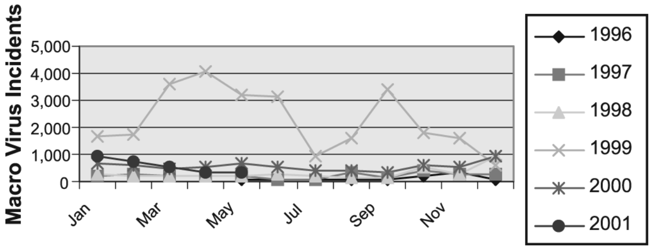


Figure 7 Annual macro virus incidents (May 1996 to May 2001)



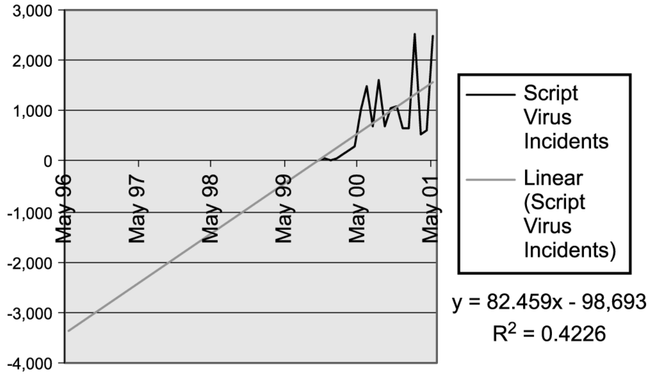
attributed to macro viruses, representing a 75 per cent decline in the number of macro viruses during the May 1999 to May 2000 period. The surge in the number of macro virus incidents reported in 1999 in comparison to previous and subsequent years is highlighted by the incidents rates demonstrated in Figure 7.

Script viruses

According to anti-virus vendor Sophos (2000) "only 6 per cent of the viruses circulating in the wild are script viruses, yet these account for over one third of all infections". These findings are reflected in the rate of growth in script virus incidents since the first reported incident of a script virus in October 1999 (Wildlist International, 2001). As shown in Figure 8, the number of reported script virus incidents has steadily increased, from 3 per cent of incidents in the period May 1999 to May 2000 to over 21 per cent of all reported virus incidents during May 2000 to May 2001.

An average of 1,050 virus incidents were reported per month for the period May 2000 to May 2001, which translates to approximately 65 script virus incidents per organization per month for that period.

Figure 8 Script virus incidents (May 1996 to May 2001)



The sharp rate of growth in the number of script virus incidents over the short time period indicates the existence of a moderate to strong linear relationship between script viruses over time, as shown by the trend line in Figure 7. This is supported by a strong co-efficient of correlation ($r = 0.65$), which is the total explained variance in script virus incidents over time.

Due to the availability of only 18 months of data since the identification of the first script virus, it is difficult to state conclusively if a longer-term trend exists in the prevalence of script viruses. As shown in Figure 9, the data do, however, reflect the significant impact of independent script virus incidents that have wielded devastating effects on corporate networks, as demonstrated by the large number of peaks visible in the data, particularly for February and May 2001. This represents the large number of organizations reporting the VBSWG viruses, in February and May 2001. A total of 2,076 incidents of the VBSWG script virus were reported in February 2001, which represents an average of approximately 130 incidents being reported by each organization for the month of February, whilst 2,158 VBSWG incidents were reported during May 2001, representing an average of 135 incidents per organization in May. The reason for the apparent re-infection of the virus in May, or the sudden decline in the number of incidents reported in March and April, is unknown.

File virus incidents

Interestingly, file viruses are the only type of virus to report a continuous increase in the number of virus incidents over the five-year period. Despite this, an analysis of trend indicates only a moderate linear relationship between file virus incidents over time, with total explained variance of $r = 0.39$, as shown in Figure 10.

Figure 9 Script virus prevalence (May 1996 to May 2001)

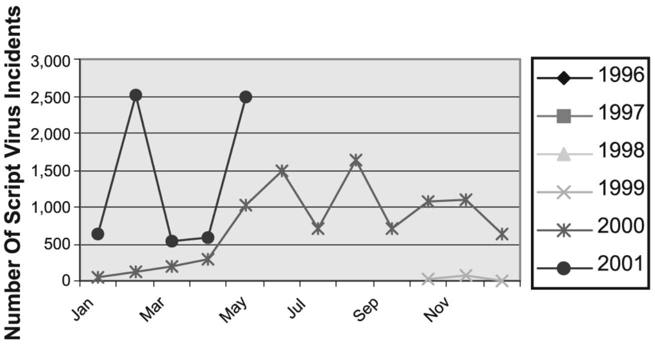
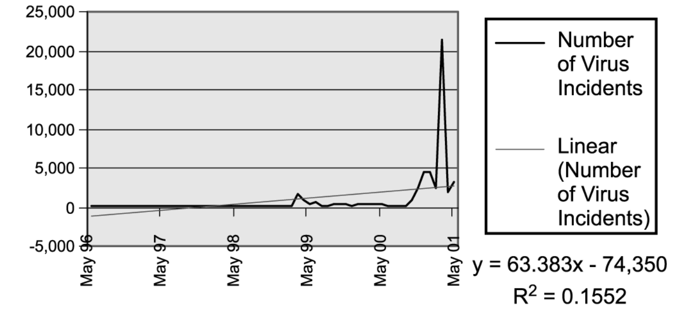


Figure 10 File virus incidents (May 1996 to May 2001)



Despite the presence of file viruses in 1996, it was not until March 1999 that the number of file virus incidents increased significantly. This raises interesting questions over the factors attributing to the growing number of file virus incidents, which have increased from 205 incidents (or 4 per cent of all virus incidents) in the period May 1996 to May 1997, to over 39,000 incidents (or 60 per cent of all reported incidents) in the period May 2000 to May 2001. This is equivalent to an average of one file virus incident per organization per month for the period May 1996 to May 1997, a figure that jumped to over 200 file virus incidents per organization per month during May 2000 to may 2001, reflecting a significant rate of growth.

Interestingly, a massive increase in the number of file viruses occurred in March 2001, as a result of the widespread distribution of the Win32/Naked virus, a mass-mailing worm otherwise known as Naked Wife. Win32/Naked caused 19,010 virus incidents to be reported in March 2001 alone, which represents an average of 1,188 reports of the virus per organization for that month.

Evolution

The above findings show that whilst total reported virus incidents have increased over time, there have been significant fluctuations and changes in the number of reported incidents by virus type, during the period of analysis. It is proposed that the changes in the breakdown of virus incidents by virus type are reflective of the evolution of computer viruses over time, whereby biological evolution is defined as "change in the population that transcends the lifetime" (Futuyma, 1986). Applied to the study of computer viruses, evolution can be defined as the change in the properties of computer viruses by virus type, which transcends the properties of an individual computer virus.

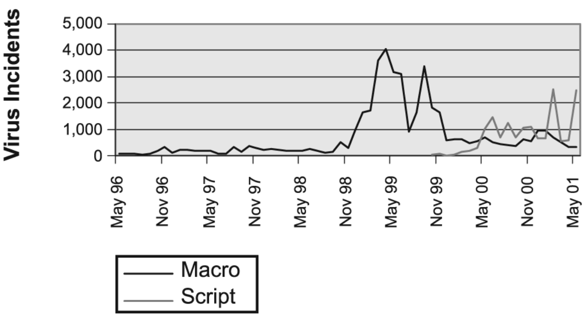
The evolution of computer viruses is demonstrated by the patterns in reported incidents by virus type over time, as a result of changes to the operating and software application environment and advancements in anti-virus scanning technology. The data for the period May 1996 to May 2001 can be summarized as follows:

- Significant decline in the number of reported boot sector virus incidents over time, coupled by increasing growth in the number of script, macro and file viruses.
- Steady growth in file virus incidents over time; with a significant increase in the number of incidents reported 1Q and 2Q2001.
- An increasing trend in macro virus incidents until peaking in 3Q1999, followed by a rapid decline in the number of reported incidents.
- First reports of script virus incidents in October 1999 immediately precede the peak of macro virus incidents.

Analysis of virus incidents between May 1996 and May 2001 indicates a reasonable association between the growth in script virus incidents and the decline in reported macro virus incidents. Notably, the reports of the first script virus in October 1999 immediately preceded the peak of macro virus incidents in September, as shown in Figure 11.

Notably, following the introduction of script viruses, the number of reported macro virus incidents began to decline, whilst reported script virus incidents increased, such that by May 2000, the number of script virus incidents far exceeded macro virus incidents. As is clearly displayed in Figure 10, macro viruses dropped from 90 per cent of all virus incidents in September 1999, to only a third of all virus incidents in May 2000, while script

Figure 11 File and macro virus incidents (May 1996 to May 2001)



viruses increased in prevalence from less than 1 per cent of incidents in October 1999, to approximately one half of all incidents reported in May 2000.

Statistically the relationship between macro and script virus incident is supported by a correlation coefficient of –0.36, demonstrating slight to moderate negative correlation between reported macro and script virus incidents for that time period. In addition, a slight negative correlation exists between the reported number of file virus and boot sector incidents. The relationship between boot sector and file virus incidents is of interest, as they are the only computer virus types that show consistency in trend in the number of reported incidents over the duration of the period of analysis; boot sector incidents have declined, while file virus incidents have increased. This is supported statistically with a coefficient of correlation of 0.23. The correlation between computer virus incidents by virus type is displayed in Table I.

Although these findings may support the existence of a relationship between fluctuations in the prevalence of computer viruses by virus type, the evolution of computer viruses, similar to biological evolution, is rather more likely to be the result of external variables. Whilst supportive statistics relevant to the given dataset are not available, a review of related anti-virus research indicates that the increase in total virus incidents over time is expected to be closely associated with the increased number of PCs and the increased use of the Internet and e-mail, while changes in incidents by virus type, are likely to be a result of technological developments in the operating environment, such as the introduction of new applications and virus scanning techniques.

Specifically, in addition to advancements in anti-virus scanning techniques, the release of the Windows 95, Microsoft Office 97 and Internet Explorer 5.0 are widely acknowledged to have contributed to the respective decline in the number of boot sector, macro virus and script virus incidents.

Table I Correlation between Incidents by virus type

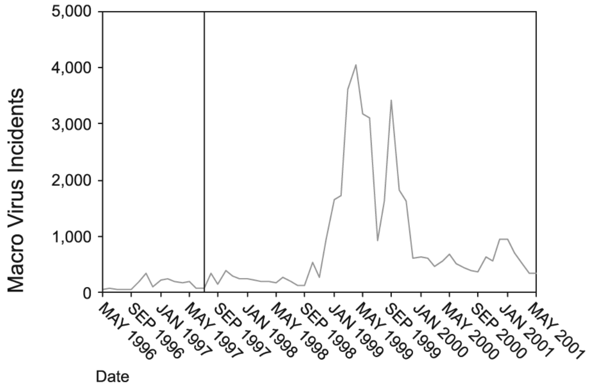
	Boot	File	Macro	Script
Boot	1.00			
File	–0.23	1.00		
Macro	–0.14	0.04	1.00	
Script	–0.04	0.04	–0.36	1.00

The Windows 95 operating system identified the slightest changes to the boot sector, enabling boot sector viruses to be virtually eliminated. Following the release of Windows 95 on August 24 1995, the number of boot sector virus incidents declined significantly. According to Kephart *et al.* (1997), boot sector viruses accounted for over 70 per cent of all virus incidents in 1993, however, according to the data analyzed, this figure dropped to 50 per cent of all virus infections during the May 1996 to May 1997 period, and further declined to less than 0.5 per cent of reported virus incidents during May 2000 to May 2001. Unfortunately, the available statistics do not permit analysis by virus type beyond February 1996, so it is not possible to plot the decline in boot sector virus incidents following the release of Windows 95, or draw conclusions upon this basis.

Microsoft Office 97, released July 1997, empowered users with greater control over macro viruses, by providing prompts to alert the presence of macros within a file, and the option to allow macros to be disabled. As a result, the number of reported macro virus incidents was expected to decline. However, as clearly shown in Figure 12, the number of reported incidents of macro viruses actually significantly increased, and a decline in the number of macro virus incidents did not occur until 4Q1999, more than two years following the release of Office 97.

Similarly, the release of Internet Explorer 5.0 (IE5) by Microsoft Corporation in March 2000 was anticipated to have a negative impact upon the number of script virus incidents. Internet Explorer 5.0 was expected to provide increased protection from script viruses, by empowering users with greater control over browser level security and

Figure 12 Macro virus incidents and the introduction of MS Office 97



allowing Active-X controls and scripting tools to be disabled. Unfortunately, from the exponential growth in the number of script virus incidents following the release of IE5 as shown in Figure 13, it would appear that the availability of the enhanced browser security did little to reduce script virus incidents.

Although it is not clear if or when organizations in the sample implemented IE5, from the available data, it would appear that either: organizations did not update to IE5; organizations were using an Internet browser without the enhanced Active-X security; users and/or administrators did not understand or implement the increased browser security options; or that script viruses were being distributed largely by another means such as by e-mail and not via the Internet.

Irrespective, it would appear from the large number of script virus incidents reported March and April 2001 that many organizations failed to update their anti-virus software to the latest technology or implement the script-disabling patch made available by major anti-virus software vendors in January 2001. This is demonstrated by the significant increase in the number of script virus incidents following the availability of the patch, as displayed in Figure 14.

The implementation of the latest anti-virus patch that was freely downloadable from the Internet and included in the latest (2001) editions of anti-virus software, corrected the vulnerability from mass-mailing script viruses, and provided protection for organizations from viruses such as Manewella and Naked Wife that were prevalent in 2Q2001.

Seasonality

Data analysis indicates that seasonal variation does occur in the distribution of computer viruses, however, due to the limitations of the depth of publicly available statistics on the number of virus incidents, it is difficult to conclusively state in which months virus incidents are more likely to occur. There are, however, some interesting findings.

Figure 13 Script virus incidents and the introduction of Internet Explorer 5.0

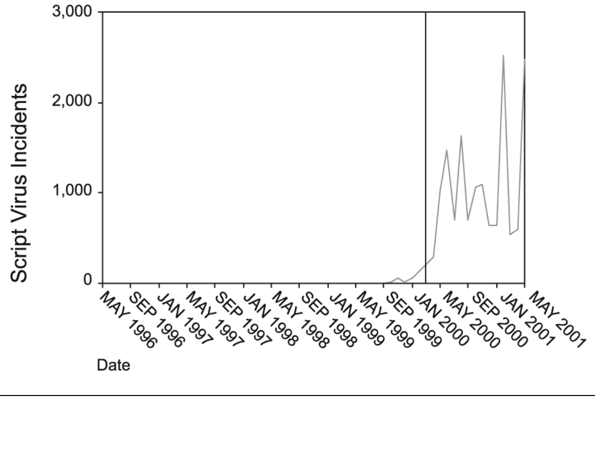
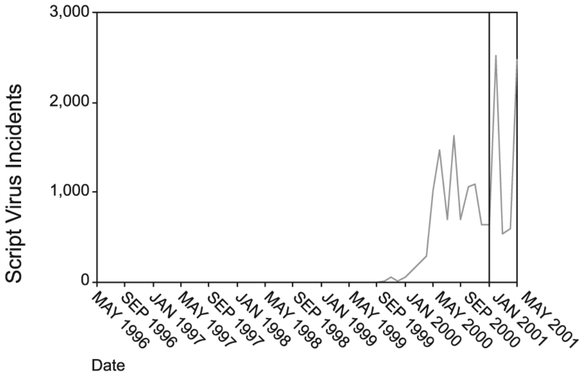


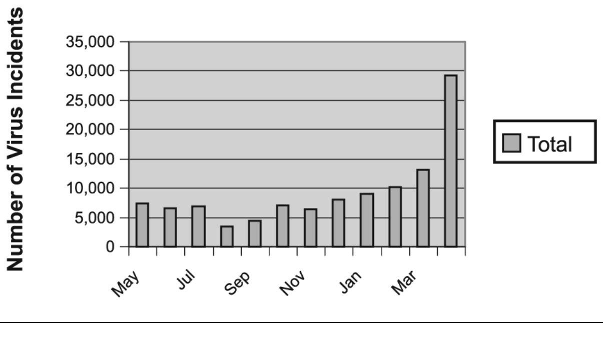
Figure 14 Script virus incidents and security patch availability



Specifically, analysis of the data indicates support for the claim by Symantec, that virus and worm incidents are more prevalent during the Easter period (Banes, 2001), as shown in Figure 15. Certainly this statement seems to support the events of the previous three years, in which major, memorable virus outbreaks such as Melissa, Loveletter, AnnaK and Naked Wife viruses all occurred during this time period.

Despite this finding, the increased virus activity is not simply isolated to the March/ April Easter period, but instead, increased virus activity is found during the winter months of the northern hemisphere, in particular the six-month period extending December through to April. This holds true for each year of the five-year period under analysis, with approximately 70 per cent of all virus incidents having occurred during the months December to April. Interestingly, during the period May 1998 to May 1999, approximately 84 per cent of all virus incidents occurred during December to April, while the December to April 2000-2001 time

Figure 15 Total virus incidents by month (May 1996 to May 2000)



period reported 78 per cent of all virus incidents occurred. This finding is of interest, as it supports the notion that Internet and computer usage rates fall dramatically during the summer months, a proposition put forward by anti-virus software vendor McAfee.

In spite of an apparent association between total virus incidents and the winter months of the northern hemisphere, deseasonalisation of virus incidents by virus type, does not indicate sufficient support for an association between the increased number of virus incidents by virus type, over the December to April period. Whilst an association may not be spurious, there is insufficient data to allow comparison of virus incidents beyond six years, which may have revealed further findings. This means that whilst there may be evidence to support general increased virus activity between December to April, there may not be evidence to support the claim that there is a specific increase in the number of viruses by type (e.g. script or file viruses) during the winter months.

In contrast, the large proportion of virus incidents in any given month highlights the effect of independent virus incidents, such as WIN32/Naked, from which conclusions cannot be drawn regarding the likelihood of future virus incidents. For example, in both 1999 and 2000, over 50 per cent of all file virus incidents occurred in the month of April, reflecting the widespread distribution of the Melissa and Loveletter viruses. However, the conclusion that file virus incidents are more likely to occur in the month of April are not be justified, as virus incident rates for other years indicate only an average number of file virus incidents during the month of April.

Limitations

There are several notable limitations to the outlined research, and as a result, its broader applicability to the wider population must be questioned. Raw statistics used in the analysis are freely and publicly available, however to preserve the anonymity of the reporting organizations, information available publicly, as to the nature of the reporting organizations or means of data collection is limited. It is perceived, that information such as the number of PCs, size of the organization (in terms of number of users), amount of Internet and e-mail traffic, the type of organization and the industry, would add considerable depth to the statistics used in the analysis, and provide significant scope for further research.

In addition, information regarding the means of distribution of the virus, such as by e-mail or floppy disk, would add considerable value to the data set. The restricted depth of the raw statistics is perceived to be the major limitation of the analysis conducted. In addition, reliance on the quality of the dataset is placed on the providers of the raw statistics, and as such the degree of error introduced during data collection and the compilation of the statistics is unknown. The small sample size and the non-random nature of selection of the sample, limit the applicability of the analysis to the wider population. As a result, broader generalizations cannot be made, however the findings should reflect the general trends in computer virus incidents.

It is possible that there are numerous determinants, in addition to a random element that may contribute to patterns in computer virus distribution, including the number of PCs in an organization, the number of computer users, the type of organization, the industry in which it operates and importantly, the volume and nature of Internet and e-mail traffic. Further depth could be provided to the analysis by the inclusion of such variables, which may reveal determinants contributing to patterns in distribution, or factors, which may increase (or decrease) the likelihood of a computer virus incident.

It is perceived that the inclusion of additional variables for the purpose of step-wise multiple regression and deseasonalisation of the data, would add considerable depth to the understanding of the factors contributing to computer virus incidents. Such analysis may form the basis for the development of a computer forecasting model, that could be utilized to forecast the expected number and type of incidents, based on a determined set of contributing factors, such as the number of PCs. Unfortunately, due to importance of preserving anonymity amongst those organizations reporting virus incidents, this information is not publicly available, therefore limiting the scope of the analysis.

Conclusion

Based on the limitations outlined, generalizations cannot be made based on the findings of the analysis conducted, nor does the analysis presume to be applicable to the wider environment. There are however, some interesting findings of the analysis undertaken, which provides support for statements made by anti-virus researchers, while questioning the validity of claims from some software vendors. Specifically, the findings indicate an increasing trend in the total number of reported computer viruses incidents over time, with significant growth occurring in the number of reported file and script viruses since 3Q1999. Results for the same period indicate a declining trend in boot sector virus incidents and possibly also in macro virus incidents. Evidence also suggests that seasonality may occur in the distribution of computer viruses, with data showing a significant proportion of virus incidents occurring during the month of April. In addition, a higher than average number of virus incidents is reported over the December to April period which indicates that correlation may exist between the winter months of the northern hemisphere and the distribution of computer viruses.

In addition, the findings do raise interesting questions regarding the reporting of virus incidents, the reliability and applicability of current computer virus research and the accuracy and validity of the claims by anti-virus software vendors. Further, given that a large proportion of anti-virus research is undertaken by parties with a vested interest in the anti-virus industry, the validity of publicly available anti-virus research and the possibility of bias must also be questioned. Accordingly, it would seem imperative for organizations assessing the potential risk of computer viruses infection and perimeter defense solutions, to assess independently the real nature of the threat posed by computer viruses.

References

Banes, D. (2001), "Editorial", *Symantec Security Response Newsletter*, available at: www.win2000mag.com/Articles/Index.cfm?ArticleID=8773

Bridwell, L.M. and Tibbett, P. (2000), *Sixth Annual ICSA Labs Computer Virus Prevalence Survey 2000*, ICSA Labs, available at: www.trusecure.com/html/tspub/pdf/vps20001.pdf

Futuyma, D. (1986), *Evolutionary Biology*, 3rd ed., Sinauer Associates, State University of New York, Stony Brook, NY.

Kabay, M.E., Tippett, L.M. and Bridwell (1999), *Fifth Annual ICSA Labs Computer Virus Prevalence Survey*, ICSA Labs, available at: www.icsa.net/html/library/downloads/VPS99-final.pdf

Kephart, J.O., Sorkin, G.B., Swimmer, M. and White, S.R. (1997), "Blueprint for a computer immune system", IBM Thomas J. Watson Research Center, Yorktown Heights, NY, available at: www.research.ibm.com/antivirus/SciPapers/Kephart/VB97/index.html

Sophos (2000), *Virus Top Ten 2000*, available at: http://www.sophos.com/pressoffice/pressrel/uk/20001202yeartopten.html

Virus Bulletin (2001), May, available at: www.virusbtn.com

Wildlist International (2001), available at: www.wildlist.org

Further reading

Business Journal (1997), "Microsoft announces service release of Office 97", *Business Journal*, available at: seattle.bcentral.com/seattle/stories/1997/05/05/daily14.html

Dalrymple, J. (2000), "Internet Explorer 5 comes packed with features", Mac Central Online, 27 March, http://maccentral.macworld.com/news/0003/27.ie5look.shtml

Moran, L. (1993), "What is evolution?", *Talk Origins*, 22 January, available at: www.talkorigins.org/faqs/evolution-definition.html

Szor, P. and Kapersky, E. (2000), "The evolution of 32-bit Windows viruses: understanding the past to prepare for the future", *Windows 2000 Magazine*, July, available at: www.win2000mag.com/Articles/Index.cfm?ArticleID=8773.

Windows User News (1998), *Newsletter*, Vol. 8 No. 4, April, available at: wun.tns.net