needed. Similarly, vorg members will likely be on many project teams and act as day-to-day points of contact between the infosec vorg and the project team.

In emergency conditions, such as a case where a widespread incident occurs within the company, many or most of the infosec vorg members may get involved in real-time.

The rook who underwrites the infosec vorg will either head up the vorg personally or be kept up-to-date by one or more vorg members on a periodic basis, may request written reports and cost justifications from time to time, and may handle budgeting for the vorg if it becomes a sufficiently formal vorg within the company. The rook will also periodically call on vorg members to clarify matters, help settle disputes and perform other vorg-related activities. On some occasions, the rook may also want to use the vorg for visibility or provide the vorg with visibility.

Summary

The movement toward a highly distributed environment has been reflected in a highly distributed management control process. This management process often consists of virtual organizations — vorgs. Infosec vorgs rule by consensus, good will, moral persuasion and strategic placement and planning. They derive their power from momentum, the weight of their aggregate force within the organization, and the strength of their champion. Infosec vorgs provide management with control by providing an ability to effect large-scale changes, providing an ability to collect and aggregate information from the entire organization, and providing expertise to analyse and make prudent decisions based on that information.

Internet — Virusnet?

Dr David Aubrey-Jones
Reflex Magnetics Ltd

The Internet phenomenon is well known, and its growth in the last two years has been staggering. Everyone, it seems, is dashing headlong to embrace the Internet and any benefits it might offer, afraid of being left behind. Even Microsoft failed to anticipate the full extent of the Internet's growth, and is now engaged in frenzied activity to correct this. Today many appear to believe that most computer viruses are spread from the Internet, and a number of Hollywood movies have done nothing to lessen this idea. However, is this really true, and what are the real threats that we face?

The Internet worm

At 6 pm on 2 November 1988 an incident occurred for which most computer experts were totally unprepared. A program was released on to the Arpanet which within a few hours had crippled the Internet, at that time mainly restricted to government, research and Universities. Operators all over the USA noticed that their computers were slowing down and having their resources monopolised. The MIT Artificial Intelligence Lab, the Rand Corporation in Santa Monica, the University of California, the Department of Defense computer network, the Lawrence Livermore National Lab, the University of Maryland, the NASA Ames Laboratory, the Los Alamos National Library in New Mexico and the MIT Media Laboratory in Massachusetts were just some of the sites hit. At first it was thought that a hacker was at work, but later that fateful night the horrible truth was revealed. It was a program, a virus.

It was realised in the early hours of the morning that the virus was being spread by electronic mail, and the immediate solution appeared to be to sever all mail connections. This action then made it more difficult for separate sites to cooperate and pool their expertise to fight the virus. It was after 5 am before any real solution was found, and interim methods were then issued that would halt the virus. Later when the virus was fully analysed it was discovered with relief that the sole aim of the virus was to propagate. The great fear, that it carried a destructive payload, was unfounded.

It was at first estimated that over 6000 computers on the Internet had been infected and the clean-up costs could be as high as $186 million. A post mortem later revised the figure to about 2000 computers at a total cost nearer $1 million, dramatically lower.

©1997 Elsevier Science Ltd

The security flaws that the Internet worm exploited have long been plugged, and a virus using the same methods would not work today. However, the potential for disaster on the Internet is now infinitely greater. What would happen if there were new security flaws that could be exploited today by such a virus?

Virus risk analysis

To help assess the current virus risk from the Internet, we need to turn to virus reports and surveys that have been conducted in the last few years. A very valuable source of security information is the Information Security Breaches Survey, a biannual survey, that was last published early in 1996. This is a joint survey conducted in the UK by consultants from the National Computing Centre (NCC) and Small World Connections, with support from ICE, the Information Technology Security Evaluation and Certification scheme (ITSEC) and the Department for Trade and Industry (DTI). The results are based on 661 responses to a postal questionnaire that was mailed to 9500 UK organizations.

The most common form of security breach in the 1996 survey was computer viruses, and this threat appeared to be increasing with 51% of respondents reporting them compared with only 35% in 1994, and 16% in 1992. This increase is surprising when one considers that a far larger number of organizations now use some form of virus prevention. In fact 95% of respondents in the survey had established anti-virus procedures.

One of the more interesting findings from this survey was that 67% of respondents with dial-out access indicated viruses as a potential threat, considerably higher than that for any other threat. It would have been interesting to know why this was so. Was it based on their experience and actual incidents, or was it just a perceived possibility. Unfortunately the survey did not go on to examine the source of virus attacks, and no data is provided as to which viruses were most commonly found

Common virus types

To help answer these questions we must turn to other sources. For over two years now principal industry anti-virus companies in the UK have collaborated with the governments Information Technology Security Evaluation and Certification scheme (ITSEC) Anti-Virus Working Group to produce information as to which computer viruses are responsible for attacks. This provides the best information that is currently available on the subject.

Figure 1. shows the most commonly reported viruses in the UK in 1995. Given that the vast majority of the 8000 or so different viruses that can infect PCs are Parasitic file viruses, one might expect this to be mirrored in the virus reports. However, the exact opposite is in fact the truth. Boot sector viruses were far and away the most common viruses in 1995, followed by Multipartite viruses which can infect boot sectors and files. All the top nine viruses, Form.A & D, AntiExe, Parity Boot.A & B, Ripper, Monkey.B, AntiCMOS, and Sampo, are boot sector viruses (see *Figure 1*). The tenth most common virus was Junkie which is a Multipartite. This has direct relevance to the question of what is the source of most virus attacks. Boot sector viruses normally spread via infected floppy diskettes. They cannot normally be spread via files, and so cannot normally be spread via the Internet. In 1995 it, therefore, appears that the Internet couldn't have been responsible for the majority of virus incidents.

Viruses in UK	Percentage prevalence
AntiEXE	19
Form A	17
Parity_Boot.A	8
Ripper	6
Monkey.B	5
Parity_Boot.B	5
AntiCMOS	4.22
Sampo	4
Form.D	4
Junkie	3
Others	26

Figure 1: Most frequently reported viruses in the UK in 1995 (ITSEC AVWG).

Viruses in UK	Percentage prevalence
Form A	14
Winword.Concept	14
Parity_Boot.B	13
AntiEXE	11
AntiCMOS.A	6
Ripper	5
Monkey.B	4
Junkie	4
Sampo	3
Form.D	2
Stoned standard.A	2
Quandary	2
NYB	2
ExeBug	2
Others	14

Figure 2: Most frequently reported viruses in UK, first half of 1996 (ITSEC AVWG).

©1997 Elsevier Science Ltd

Macro viruses

If we now turn to the reports so far available for 1996 (see *Figure 2*), we find these broadly speaking in line with those for 1995. Boot sector viruses were responsible for most reported incidents, with one notable exception, Winword.Concept. This is a totally new type of virus, a Macro virus, that only existed in theory at the start of 1995. Within a matter of just six months it went from being unknown to being near the top of the incident reports. *Figure 3* shows this dramatic rise from obscurity in the period from July 1995 to January 1996.

Are these findings just a peculiarity of the UK? A survey conducted in the United States by the National Computer Security Association (NCSA) last year (the 1996 Computer Virus Prevalence Survey), would suggest that they are not. In March telephone interviews were completed with 300 end-users. Again these interviews revealed that boot sector viruses were responsible for the majority of virus incidents, with the one exception of Winword.Concept.

In fact unlike the UK reports, these interviews found that Concept was the most common virus. This slight discrepancy might be due to differences between the two countries, or possibly with the way the different figures were obtained. The NCSA survey was a telephone survey that relied on peoples memory of incidents, and generally it seems that they would be more likely to remember a totally new type of virus incident, such as the Concept macro virus, rather than just another boot sector virus.

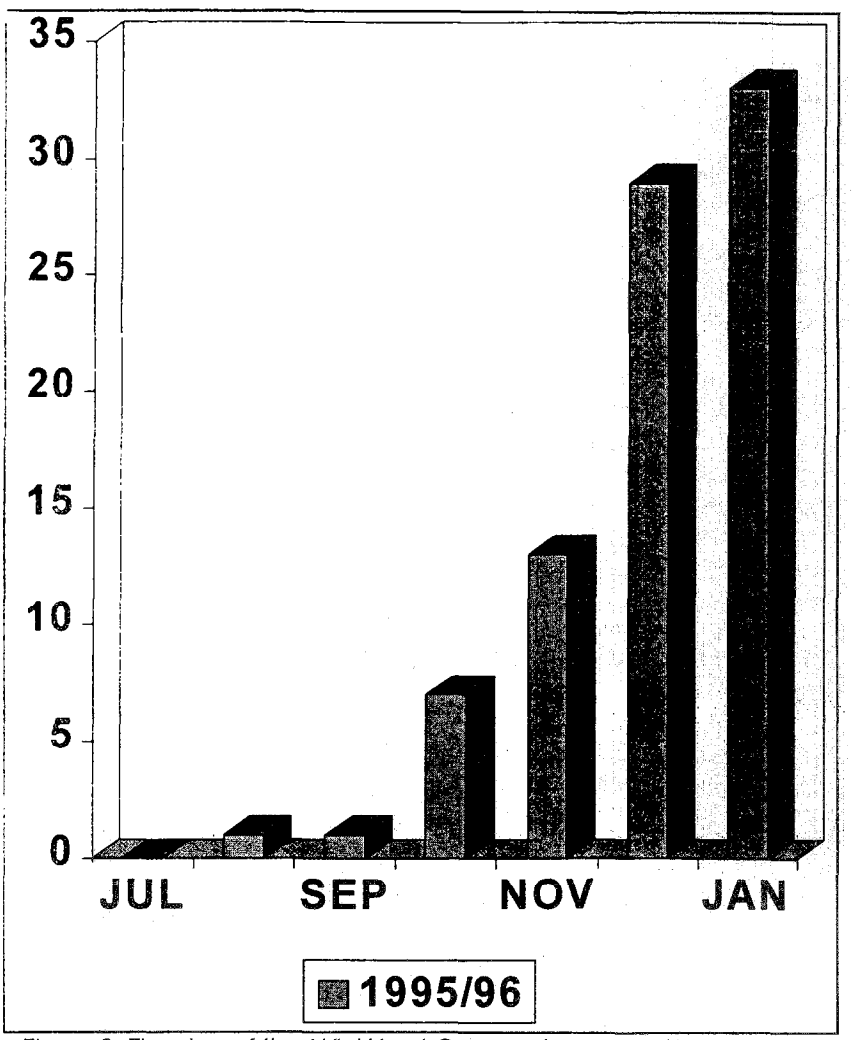

Figure3: The rise of the WinWord.Concept macro virus.

Winword.Concept was originally spread when it was widely shipped on at least two CD-ROM disks by Microsoft; "The Microsoft Windows 95 Software Compatibility test version 4.0"and "The Office for Windows 95 Business Guide (v.1)". Obviously this fact alone has ensured its widespread distribution.

However, it appears that there are other factors that have helped make it so common. The NCSA survey comments: "By far, the rate of growth of Word.Concept is the fastest of any virus ever observed to infect computers of the general public. There are several reasons for its apparent rapid growth: one probably relates to its ability to replicate using vectors other than diskette (like E-mail attachments)."

The NCSA survey went on to examine the means of virus infection. Bearing in mind how common Boot sector viruses are, it is not surprising that the survey showed that floppy diskettes are by far the most common source of

©1997 Elsevier Science Ltd

Means of Infection	Percentage
Floppy disk	69
Download	10
E-mail	9
Unknown	12

Figure 4: Means of virus infection, NCSA Survey 1996.

infection. Download's from BBS/online were reported as responsible for just 10% of infections, and E-mail just 9% (see *Figure 4*).

The main Internet virus threat

In most organizations software is not widely copied from one computer to another. Thus viruses that rely on this method of propagation, such as Parasitic file viruses, are not very successful and don't become common. However, word processing documents are shared and passed between users far more frequently, whether by diskette, local network or Internet E-mail attachments. Thus viruses which can infect such documents (Macro viruses) are far more likely to become widespread. Such viruses currently represent the main virus threat from the Internet and are likely to do so for at least the next couple of years.

Viruses on the Internet

Although most virus infections do not currently come from the Internet, it would be unwise to assume it holds no threat. The Internet now enables virus writers the world over to communicate easily and inexpensively, and to share ideas and program code. A few years ago some virus writers set up Virus Exchange Bulletin Boards for this purpose and efforts were made in a number of countries to close these down. However, the high cost of international telephone calls ensured that the spread of viruses across national boundaries was limited to some extent. A virus writing group in the UK were actually found and their nefarious activities stopped due to one of their group making illegal international phone calls on their neighbours phone line.

Virus Web sites

However, today the Internet has largely replaced these Virus BBS's. A number of Internet FTP sites have been set up which contain in some cases vast numbers of viruses available for downloading. More recently virus writers have adopted the World Wide Web and there are now a considerable number of Virus Web sites. These variously contain viruses for download, virus collections, virus writing toolkits, virus source code, virus writing guides, newsletters, and links to other virus sites. Some even offer a 'Virus of the Month'. A tutorial on writing Word Macro viruses has also recently appeared!

With this sort of material readily available throughout the World, the virus problem can only worsen. It is likely to encourage more virus writing, and provides an easily accessible source for anyone looking for viruses. Thus it would be a simple matter for an employee harbouring a grudge to obtain a virus and launch an attack on his victims. No great technical knowledge is required.

Attempts have been made to persuade Internet providers to remove such sites, but these have been largely unsuccessful. Even attempts to remove child pornography from the Internet has until now largely met with failure. Internet providers do not want the onerous burden of being censors. Unless laws are made to make providers responsible for what they carry I suspect that no real progress will be made.

KAOS on the Internet

Although thankfully few in number, there have now been a number of instances where programs on the Internet have been infected with viruses. In July 1994 voyeurs of erotic software on the Internet the world over were treated to the thrill of a totally new virus. KAOS4, as it was subsequently named, was attached to pornographic software posted to the Internet newsgroup alt.binaries.pictures.erotica. This newsgroup is one of the most popular, and consequently the virus was disseminated to thousands of subscribers before the problem was spotted.

Being a new virus, the anti-virus scanner proved totally useless. None could detect the virus at the time, even though the virus was no great feat of programming. Primitive, it used no advanced techniques apart from some anti-heuristic methods and contained no payload. Because of bugs in the code KAOS4 eventually corrupts itself, and then ceases to be a problem since it can no longer infect.

©1997 Elsevier Science Ltd

The Tentacle

A similar event occurred early in 1996. A new virus, and thus again one which virus scanners didn't detect, managed to infect a large number of computers in different countries and on different continents within a few hours. Again this was courtesy of the Internet. A program, DOGZCODE.EXE, which offered to provide the code to enable all features free of charge in a popular program 'DOGZ, Your Computer Pet', was uploaded to a Usenet newsgroup, alt.cracks. This is an unmoderated group where discussions are held on breaking software copy protection.

Hare Krisna

The most recent incident of this type was another new virus, or now a group of viruses, the Hare viruses. Several programs infected with variants of Hare were posted to popular Usenet groups. These included alt.cracks, alt.crackers, alt.sex and alt.comp.shareware. Again these were undetectable until recently by scanners. Furthermore, it took longer for detection to be added in this case since they use a slow Polymorphic technique which means that a simple scan string cannot be used.

The Hare viruses led to widespread warnings in the news recently, since the Hare viruses attempt to overwrite the Hard disk on the 22 August and 22 September. Luckily bugs in the virus appear to have limited its spread.

Java and ActiveX

Until recently, browsing the World Wide Web has been relatively safe since no program code on the Web executed directly on the local PC. However, this has now all changed with the introduction of Java applets and ActiveX. So is a Java or ActiveX virus possible? When Java was designed Sun were aware of some the potential security flaws that Java applets could cause. They, therefore, constructed four lines of defence against virus attack.

Firstly the Java language itself cannot readily access areas of a computers memory outside the Java Virtual Machine. Secondly the Java VM uses a code verifier to ensure all instructions are permissible. Even with these two lines in place there are still other possible attacks, and the Java VM goes further by providing a check that an applet doesn't try to replace a local Java class with a new insecure one. Finally to defeat a direct attack Java has a security manager. This defines which low level system calls are permitted. With these security measures in place a Java applet virus would not be easy to write, but it would be a brave person who would say that it was impossible.

Security has been added to Microsoft's ActiveX in a rather different way. This is based on certificates of authenticity. It has recently been reported that an consultant, Fred McLain, developed a rogue ActiveX control, to illustrate security holes. Having written the control, which he called Exploder, he gained a certificate of authenticity from a third party company helping Microsoft with ActiveX security. Apparently if Exploder is downloaded on a Windows 95 machine with a green BIOS it can shut it down!

Conclusions

These incidents provide an insight into some of the dangers posed by the Internet. The traditional form of defence against viruses has been the anti-virus scanner. While being valuable tools, they have their limitations, the principal one being they often cannot detect new viruses.

In the past when viruses have been principally spread via floppy disk, this has been slow, and this has enabled detection to be added to the scanners before the viruses became widespread. However, the Internet enables virus writers to distribute a new virus, undetectable by scanners, worldwide within a matter of hours. Couple this with the new threat of Macro viruses and the speed with which they can be written (a matter of minutes), and some of the ingredients for a potential disaster appear to be forming of far greater proportions than the incident of the Internet Worm. If this is to be avoided, action should be taken now.

This paper was first presented at COMPSEC 1996 in London, UK.

©1997 Elsevier Science Ltd