The Costly Implications of Consulting in a Virus-Infected Computer Environment

Kirsty Nunez, Computer Consultant
TACVKDN@VM.TCS.TULANE.EDU

Thomas Gerace, Computer Consultant
TACVTAG@VM.TCS.TULANE.EDU

Alison Hartman, Manager, Consultants Bureau
TACVAGH@VM.TCS.TULANE.EDU

Tulane Computing Services
Tulane University
New Orleans, LA 70118
504/865-5631

Institutional Profile:
Size:
Undergraduate Students: 7170
Graduate Students: 3794
Faculty: 1406
Staff: 2697
Computer Center: Academic and administrative support
Computer Center Staff: 100 full-time; 40 part-time

If you think education is expensive, try ignorance.
--Derek Bok

INTRODUCTION

Computer viruses are an unfortunate fact of life on today's college and university campuses. A recent examination of campus computing center newsletters suggests that the risks of contracting a computer virus have become real and acute for computer users across the country. The problem has become particularly pressing for these who frequent shared computing facilities, for example, university microcomputer clusters. Many individuals have turned to the central computing services for assistance and information. Meanwhile, the costs of increasingly frequent virus attacks have become evident as consultants and users spend time, effort, and money detecting, eradicating, and attempting to recover from this scourge of the electronic age.

This paper focuses on the costs associated with computer viruses and proposes that these costs can be reduced by planning a comprehensive program of protection and education. It describes a chronology of virus-related events at one research institution and the strategy adopted by the central computing organization at that institution to protect the computing community and to minimize risk of infection. Finally, the paper examines the implications of computer consulting and computer use in an environment that is affected by viruses.

Functionally, "computer viruses" can assume many forms: worms, logic bombs, trapdoors, and trojan horses, for example. In this paper, the term "virus" is used generically to refer to any program or device that infects or affects computer systems without the knowledge and intent of the computer user.

The implications of this electronic epidemic are costly: computer users, support staff, and software developers have paid and will continue to pay dearly for the so-called "harmless" pranks of a few crafty individuals. Perhaps the greatest cost, however, is a loss of openness and trust in an environment that has been based historically on just that. The technological advances that flourished as a result of this openness may diminish as users must become increasingly wary of sharing information.

CHRONOLOGY OF VIRUS OUTBREAKS AT TULANE UNIVERSITY

While the concept of computer viruses is not new, only recently has the issue become a topic of general interest and concern. Late in the Fall of 1987, when the subject of "computer viruses" was first introduced at a weekly staff meeting of the Tulane Computing Services (TCS) Consultants Bureau (triggered by discussion on the BITNET network), the concept was met with casual abstraction. The consensus was that the risk to average computer users was minimal, and no action was taken at that time. Many institutions may have first approached the subject of computer viruses in a similar manner.

Subsequently, three specific incidents accentuated the seriousness of the matter on the Tulane campus:

- Early in the summer of 1988, the "Scores" virus infected a Macintosh computer in an administrative office. Support staff at TCS helped to identify and eradicate the virus, but the user spent considerable time deleting and re-installing infected applications and system files.
- Later that summer, a computer consultant at TCS discovered that the hard disk on his computer was infected by the Scores virus -- the aftereffect of helping a student with a routine Macintosh problem. The consultant spent hours erasing damaged applications and re-installing the operating system.
- No further virus activity was reported on campus until the Fall of 1988, when all computers in a new Macintosh II lab were infected only two weeks after the lab's opening. Student monitors spent several days deleting and re-installing infected applications on the hard disks of the 22 machines.

Since the initial outbreaks, the main microcomputer cluster at Tulane has been plagued by almost daily appearance of viruses on the Macintosh disks that this facility circulates. (MS-DOS software is distributed using a local area network; this, and the fact that Macintosh use is twice that of MS-DOS, may explain the absence of viruses on MS-DOS disks in this facility.) This situation is not unique to Tulane: many incidents of virus attacks have been reported in college and university computer center newsletters.

FROM REACTION TO POSITIVE ACTION

The virus outbreaks at Tulane, coupled with the national news coverage of the topic, heightened TCS consultants' awareness of the problem. While the number of computers actually infected on campus has been relatively few, many individuals have been affected -- some, because they have been forced to spend time testing machines for infection or applying preventative measures, others, simply because consultants must spend time addressing the problems caused by viruses, leaving less time for other responsibilities.

Initially, TCS responded to the outbreaks by addressing each situation individually: eradicating viruses as they were detected and dispensing protective measures as they were requested. Although this approach was effective, it increased the burden on the consulting staff (who still maintained their typical caseloads), and it constituted a specific, rather than a universal, solution to the problem.

Eventually, TCS replaced the reactive measures with a plan of positive action aimed at reducing the risk of virus infections for all campus computer users and sharing the burden of responsibility between the computer center and the users. This active, aggressive policy included a number of components:

- Placing public domain and shareware software for virus prevention and elimination at the central computing facility. TCS evaluated and selected a number of such programs, prepared two diskettes for circulation (one Macintosh, the other MS-DOS), and then publicized the availability of these tools.
- Staying abreast of the voluminous information available on the subject and sharing that information with other consultants and with users. Network Discussion Lists, magazines, trade journals, scholarly reports, and newsletters from other academic institutions all contain useful and timely information about the problem and its solutions.
- Communicating with the 30 TCS student consultants about computer viruses. TCS staff discussed computer viruses with student consultants and helped students learn to assist users who suspect or know they have contracted a virus. TCS consultants also provided the students with information about viruses and anti-viral tools.
- Hiring on a part-time basis a student responsible for verifying the integrity of circulation diskettes at the main computing facility. This student, fondly referred to as the "virus buster," re-creates circulation software on a regular basis, thus ensuring that the software is circulated as intended and is virus-free.
- Launching an active program of user education. Perhaps the most important component of the plan, TCS has provided the Tulane computing community with extensive information about viruses. To disseminate the information to users, TCS has included a number of articles in its Newsletter and has dedicated a special section in its Faculty Computing Resource Library to the subject. A TCS Brief on the topic is also underway. This educational process helps users protect themselves and understand the situation, and prepares them to deal effectively with computer viruses, should infection strike.

THE COSTLY IMPLICATIONS

The costs of computer viruses are great, not only to individuals but to institutions. Many of these costs are obvious; others become apparent only after infection occurs.

The most noticeable cost associated with the proliferation of computer viruses is time: time spent in locating, isolating, identifying, and destroying viruses, learning about viruses and cures, educating and reassuring the user community, writing and distributing virus prevention and detection software, and reconstructing damaged programs and files (if they can be reconstructed).

In addition to time dedicated to activities directly related to viruses, viruses have dramatically increased the overhead associated with computer consulting. In the past, consultants could examine problematic disks and files without concern. Today, however, all diskettes are potential virus carriers, and layers of protection are required to guard against infections. Even with such protection, consultants will not be immune to all strains of computer viruses. To completely prevent infection of a disk, more extreme measures might be necessary, for example: booting from a floppy disk, unmounting hard disks, and disconnecting from local area networks. Only then might a foreign diskette be safely introduced to a consultant's machine and the problem at hand addressed.

The costs of computer viruses extend beyond time (and the associated financial concomitants). Data loss and damage are also costly. Files may be damaged beyond repair or erased, and information may be forever lost. System unavailability is another obvious cost; time spent detecting and recovering from viruses is time during which the computer is not available for other processing tasks.

The psychological responses to viruses are also among the costs associated with computer viruses. For example, alarm is a common response of one who has contracted a computer virus. Will data be lost? Will work be stalled or halted completely? Will weeks or months of hard work be lost forever? Alarm is also increasing among the uninfected. The thought of computer viruses is often the first reaction to any computer problem. Clear thinking about potential hardware problems has been clouded by concern about viruses. ("My screen must have gone blank because of a virus" or "I get error messages when I launch an application -- it must be a virus.") Some have even attributed errors in program code to viral infections.

Computer viruses also cause frustration and stress by interfering with productive activities and introducing a lurking fear into the workplace. Computer professionals may note an increase in the number of frustrated and angry users. Users already frustrated by a seemingly insurmountable computer problem may be further aggravated by time-consuming virus-protection measures. All of these factors increase stress, both on consultants and users.

The reluctance to share information is another cost of computer viruses. Consultants and administrators may become wary of clever programmers and may consciously or unconsciously restrict access to computing resources. Hence, these talented individuals may be prevented from expanding their skills and perhaps unwittingly, encouraged to "hack."

Perhaps the greatest cost is the loss of openness and trust that viruses have caused throughout the computing community. While many users have recently become comfortable with computing, that confidence is now eroding as a result of the threat of viral infection. The openness, trust, and sharing that has existed in the computing world thus far --and that has made possible tremendous advances in technology -- has begun to diminish. In addition, the use of bulletin boards, file servers, and local, national and international networks may be reduced or restricted, thus diminishing the value of these powerful tools that promote and enhance the exchange of information.

For those in the computer industry, the computer is simply a tool. We understand the concepts behind the hardware and software, and we exploit the machine's capabilities to accomplish our work. To many students, staff workers, or faculty members who use computers, however, there is a certain "magic" involved. Lately, microcomputer users have grown comfortable with their machines and have begun to explore and experiment beyond word processing. Now, however, that comfort may return to mistrust and fear as we face this unseen enemy, the computer virus.

CONCLUSION

Institutions today face a decision: they can "play-down" the virus issue and deal with infections as they arise, or they can invest in an active campaign of virus prevention and user education. While a low-key, reactive approach may seem advantageous initially, an active education campaign shares the burden of virus prevention among the computer center and the users, and can dramatically reduce the long-term costs to the institution.

In a low-key, reactive approach to computer viruses, the computer center deals with infections as they arise, minimizing alarm the user community. In this manner, the computer center assumes responsibility for dealing with viruses, encourages users to seek help when viruses strike, and spends time eradicating viruses and helping individuals recover lost or damaged files.

Investing in an active campaign of user education and distribution of virus prevention software shares the burden of virus prevention among the computer center and the computer user. While user education can be time consuming at first, the ongoing costs in time and effort are far less than that of a reactive approach. As individuals learn about the virus threat, they gain the ability to protect themselves with tools provided by the computer center. The computer center will see a decrease in the number of cases of infection brought to them as the user community prevents infection from occurring. Users will no longer live in fear (although the threat will always be present) because they will understand the infection process and how to minimize its risk.

Even with an active campaign of user education and software distribution, infections may occur. We can expect that educated and informed users will be capable of disinfecting affected program files, perhaps following procedures established by the computer center. Thus, the computer center has achieved the goals of decreasing the infection rate in the user community, of helping users to protect their programs and data, and of decreasing the consulting time associated with computer viruses.

The computing profession must work actively to prevent these so-called "harmless" activities and to channel the efforts of resourceful programmers toward productive ends. Perhaps someday, the threat of computer viruses will be a thing of the past. In the meanwhile, we must address the

problem intelligently. While the costs of computer viruses are great, these costs can be reduced through thoughtful planning and a global view.