LOYOLA
UNIVERSITY
CHICAGO

Information Technologies Division

Virus Prevention Procedures

I. Procedures for Information Technologies LAN administrators

A. Review/implement routine backups for LAN file servers.

B. Incorporate routine scanning for viruses into backup routine or on similar schedule.

C. Retain write-protected original distribution diskettes of software installed on LANs.

D. Flag program files as Read-Only as much as possible.

E. Scan all new software (obtained from both commercial and non-commercial channels) for viruses while installing.

F. Limit rights in directories where programs are stored to exclude the Modify-flags privilege for all IDs except Supervisor and equivalents (so only Supervisor can change Read-only status of program files).

G. Limit the use of Supervisor ID and equivalents.

H. Impose stricter anti-virus measures, including the loading of memory-resident virus-scanning software, upon Supervisor ID and equivalents.

II. Procedures for all Information Services (IT) staff

A. All software used on a computer owned by Loyola University must be properly licensed for use on that computer. (restatement of existing policy)

B. All software installed onto LAN file server must be installed by the LAN administrator(s)

1. LAN administrator will set up security for the software: to control sharing, as appropriate; to prevent infection.

2. Software found on the file server that was NOT so installed will be removed.

C. Generally, only software that is licensed for and intended to be shared by multiple computers should be installed on the file servers.

1. Software for use on a single machine should generally be run from a local hard disk or from floppy disks.

2. Software should not be stored in any personal directory on a file server.

D. Public domain software or shareware, if used at all, should be obtained directly from the author, when possible, or from commercial sources known to scan for viruses (such as BIX, Compuserve, PC Magazine, PC World, PC-SIG).

E. If an individual has a PC at home, ONLY data disks should be regularly transported between home and office. If public domain software or software licensed for single simultaneous use on multiple machines is to be used from floppy on both machines, separate home and office copies of the floppies will be necessary.

F. Software that is installed on a local hard disk or to be used regularly from floppy diskette should be scanned for viruses during installation. The installation should be logged (so that changes in size of executable files can be detected). Original diskettes should be write-protected and carefully kept apart from other diskettes so that if an infection is later discovered, it is clear whether the infection came from the retailer/vendor or the infection occurred within Loyola.

G. Local hard disks should be backed up by the individuals using such local hard disks.

H. Local hard disks on machines that are shared by several people running a variety of software packages should be scanned for viruses regularly (possibly whenever booted).

III. Recommendations to departmental LAN administrators

A. Regularly run NETSCAN utility with backup batch files overnight (get it from LAN analyst; Loyola has site license for the LAN version).

B. Flag program files (COM/EXE/SYS/OVL) ReadOnly.

C. Limit rights for people in directories where programs are stored to exclude the Modify-flags privilege.

D. Have explicit rules on how software enters the dept, eg:

1. Must be properly licensed, not pirated

2. All software, even if it is bought by an individual or brought in from public domain, must be loaded onto file server by the LAN administrator or by ACS

a. To properly set up security for the software: allow sharing, as appropriate; prevent changes

b. Software found on the file server that was NOT so installed will be removed.

c. Public domain software or shareware, if used at all, should be obtained directly from the author, when possible, or from commercial sources known to scan for viruses (BIX, Compuserve, PC Magazine, PC World).

3. Scan all new software for viruses as installed on local hard disk (call ACS or buy departmental license(s) for SCAN.EXE) and maintain log

E. Information Services may recommend additional measures later (such as using an anti-virus TSR program when logged in as Supervisor or equivalent)

IV. Basic virus containment plan for LAN file server (to be customized for each department)

A. Immediately isolate the file server from other LAN file servers and workstations as completely as practical.

B. Prevent login of additional stations while scanning file server hard disks with NETSCAN.

C. Scan contents of compressed files (.ARC/.ZIP extensions).

D. Inform departmental management and Information Services LAN analyst of the infection.

1. If file server is on backbone, have the LAN Analyst paged to be informed immediately.

2. Make arrangements for other file servers possibly infected to be scanned.

E. If practical, scan all local hard drives as a group before allowing those stations to log into the file server again.

F. If a virus is discovered on a local hard drive, scan all program floppy disks used by the people who regularly use that workstation before allowing that station to log into the file server again.

G. Track the path of the infection, as practical.

1. Identify the time window in which an initial infection or secondary infection might have occurred by reviewing backup and scanning sessions.

2. Identify persons who might have used the software known to be infected either after the infection or shortly before the infection.

3. Scan all program floppy diskettes and/or home hard disks of people who used the infected software during or after the infection window.

4. Identify persons who might have shared a common workstation with someone who used the infected software during or after the infection window.

H. Restore infected software

1. Temporarily restrict access to directories with infected files to Supervisor ID.

2. Move infected software and uninfected supporting files to a temporary directory or compressed (".ZIP") file with Supervisor-only access.

3. Restore earlier version of software from backup.

a. Scan software restored from tape for possible prior infection.

b. If necessary, use earlier backups.

c. If necessary, re-install from original disks, copying non-executable configuration files from temporary directory.

d. Check proper operation of software.

4. Delete infected copy of software from temporary directory.

5. Restore proper privileges to groups to give access to restored software.

V. Basic virus containment plan for local hard drive or floppy

A. Inform departmental management and local Academic Computing Services manager of the infection.

B. If the workstation is attached to a network, inform the departmental LAN administrator and the Information Services LAN Analyst as well.

C. If practical, scan all other local hard drives in department as a group.

D. Scan all program floppy disks used with that workstation.

1. Target disks that were used recently on that workstation.

2. If multiple machines are infected, scan ALL diskettes that might possibly contain programs.

3. Mark each diskette with date and time of scanning.

4. Ask individuals to check PCs at home.

a. If they do not own virus scanning software, they can sometimes use DOS "COMP" command to do byte-by-byte file comparison between original and working diskettes or hard disk.

b. Comparing file sizes provides a partial indication of whether a file has been infected by SOME viruses.

E. Track the path of the infection, as practical.

1. Narrow the time window in which an initial infection or secondary infection might have occurred by examining history of backup and scanning sessions.

2. Identify persons who might have used the software known to be infected either after the infection or shortly before the infection.

3. Scan all program floppy diskettes and/or home hard disks of people who used the infected software during the infection window.

F. Restore infected software.

1. Move infected software and uninfected supporting files to a carefully marked floppy diskettes or a temporary directory.

2. Restore earlier version of the application from backup device.

a. Scan software restored from backups for possible prior infection.

b. If necessary, use earlier backups.

c. If necessary, re-install from original disks, copying non-executable configuration files from temporary directory.

d. Check proper operation of software and scan again.

3. Delete infected copy of software from temporary directory or diskettes.

G. Target machines that were once infected for closer surveillance and scanning to prevent or detect re-infection.

Last revised: April 9, 1991 Revised by: Don Wee