Virus Hunter’s Checklist

Sophos Plc, Oxford, England

Part # tr00005c/971015

Introduction

You have been asked to check all PCs on a site for a possible virus attack. You grab your bag, which contains all the tools necessary to deal with the problem, and head for the site.

What should the bag contain?

Contents checklist

- □ Software for IBM-PC virus investigation. This will include not only virus-detection software but also software tools for investigating a virus attack and recovering from it:
    - □ Up-to date copy of Sophos SWEEP for DOS. Up-to-date copy of SWEEP for Windows 95. You should not use copies which are more than two months old.
    - □ A supplementary virus scanner from a manufacturer other than Sophos. We can recommend suitable products.
    - □ DOS on write-protected disks. We use Compaq DOS 3.31 or DOS 5.00, which are able to boot machines with hard disks running any version of DOS.
    - □ Copies of disk compression utilities such as PKZIP and ARC.
    - □ Sophos Utilities (supplied with SWEEP). Useful for disk investigations, displaying interrupts and recovering from boot sector virus infections.
    - □ Sophos FILEMAC, VACCINE and DIAGNOSE (part of the VACCINE package) for investigating an attack by a virus unknown to SWEEP and your other scanner.
    - □ Sacrificial ‘goat’ programs which can be infected on purpose in order to observe virus behaviour.
    - □ Diagnostic software for distinguishing a potential hardware problem from a virus problem. This is usually dependent on the hardware used and may be best obtained on site. SWEEP this software and write-protect it before using it.
    - □ Manuals for all the above software as well as a DOS manual.
- □ Software for Novell server scanning (SWEEP for NetWare)
- □ Software for Apple Macintosh virus investigation. You will need a completely different set of tools and procedures to check Apple Macintosh PCs, although the same principles apply.
- □ Secure bootstrapping means and procedures.

    With the advent of stealth viruses, **it is most important to guarantee a clean, virus-free environment on a workstation, before running anti-virus software or investigating a virus-infected network.**

    Bootstrapping stand-alone PCs:

    - □ Ensure that DOS disks are write-protected. Switch the PC off, insert a boot disk in drive A: and then switch it back on. Make sure that the booting sequence is set to floppy disk-hard disk.

    Bootstrapping a PC in order to check a network:

    - □ A DOS system disk which also contains all executables needed to set up the network connection, as well as log onto the network. For example, on Novell NetWare 3.11 you will need a DOS system disk with IPX.COM, NET3.EXE, LOGIN.EXE and MAP.EXE. Perform a secure boot of the PC as described above, then run LOGIN from the floppy disk including the ‘/S NUL’ command line qualifier. This will prevent the execution of both system and user login scripts:

        ```
        LOGIN /S NUL <USERNAME>
        ```
- □ Pre-formatted disks for preserving any virus samples and general use.

❑ Floppy disk labels, 'Virus infected' labels, 'Disk free from known viruses' labels.

❑ Education materials. You may be required to give a short presentation on virus prevention to PC users on the site. *'Viruses on Personal Computers'* video (from Sophos) is an excellent tool for conveying the message in about 15 minutes. Furthermore, as a virus specialist, you must stay in touch with the latest developments in the virus field. Make sure that your subscription to the *Virus Bulletin* is current.

  ❑ *'Viruses on Personal Computers'* Video.

  ❑ Current subscription to the *Virus Bulletin.*

❑ Virus attack reporting forms. The Computer Crime Unit (CCU) at the New Scotland Yard are anxious to receive reports of virus attacks. A report can be made by telephone, fax or post. The CCU has produced special VAF1 forms for reporting an attack.

Contact telephone and fax numbers

Computer Crime Unit
Tel 0171 230 1177, Fax 0171 230 1275

Sophos
Tel 01235 559933, Fax 01235 559935,
Email technical@sophos.com, www.sophos.com