

Security Panel Presentation 1/28/2003

Virus Threat

By: Alex Chavarin 360-8990 alchav21@hotmail.com

1. Introduction and description of a Virus Threat.

a. Introduction: Computer Viruses have been with us since the first PC's were introduced on the market. Just like a disease, some can be as benign as a common cold, while others can wipe out an entire city or country. A computer Virus is a piece of software that has been written to enter your system and "infect" your files.

b. What is a Virus Threat: Typically, a computer Virus will replicate itself and try to infect as many files and systems as possible. When you save an infected file to disk, you'll infect that disk and any systems that share that disk. If you email this infected file as an attachment you infect all those disks and systems where it is saved. Viruses can be written into almost any type of file, so it is very important to know where your software came from when adding it to your system. So the two main ways of getting infected are through removable media like floppy disks, Zip disks, and CD's, or by downloading from the Internet.

c. Description and break down of Viruses: Viruses are broken down into four main types, *Boot Sector Viruses* infect the Master Boot Record so when the system boots up the Virus is loaded into the systems memory. *File or Program Viruses* are pieces of viral code that attach themselves to executable files and cause harm when these files are run. *Macro Viruses* are found in applications that use the Macro language like MS Word or Excel. *Multipartite Viruses* have characteristics of both Boot Sector and File Viruses; they may start in the boot sector and spread to applications, or vice versa.

2. Examples of Virus Treats.

a. W32.Klez.H@mm: This Virus was real common around SCPD, and the name as set up by CARO (Computer Antivirus Research Organization) is broken down as follows: W32 = Windows 32 Bit Platform, Klez.H = Name, usually provide by author in the source code, mm = ID as Mass Mailer.

b. Trojan.PWS.QQPass.D: This Virus comes in like the name implies, and has infected a few systems here in SCPD.

3. Protection and Solutions.

a. Anti-Virus Software: Anti-Virus Software is needed and the two best programs are Norton Anti-Virus and McAfee. The address to their Web Site is www.sarc.com and www.mcafee.com.

b. Activation and keeping Updates current: If you load the software yourself activating it is part of the process, but if you buy a computer with the software loaded you have to activate it. The main page of the software will tell you the status, one of the options is a Full Scan, and this should be done periodically especially if you think you have a Virus. Updating your definitions is also a must and the software will tell you when this is needed.