8/27/2003

Update Regarding Blaster and Welchia Virus Worm Attack

NYS Office for Technology continues to address the adverse impact of the recent Blaster and Welchia worm attacks on the Human Services Network, and the resulting 'disabling' of all connected devices that transact over the network, including terminals, servers and PCs. **Below is a status update as of 8/27/03 am.**

What was affected by the worm attack?
Since the middle of last week, all state network attached Windows 2000 PCs are targets for the Welchia worm. The virus can proliferate so rapidly that a site's circuit for connecting it to the State Human Services Network, must be brought down temporarily by the Office For Technology (OFT). Less severe impact is that the circuit can remain up, but all state networked PCs at the site are required to be shut off, and all dumb terminals may also stop operating. The remedy is to shut off all PCs, and one-by-one initiate the CD hosted cleaning process on each network attached PC. These remediation CD's were mailed out to all local district and voluntary agency LAN Administrators and Site Contacts, as well as to CONNECTIONS Implementation Coordinators.

How does the worm disrupt service?
When a Windows 2000 PC is 'infected' by the worm, it begins infecting other Windows 2000 PCs, and broadcasts tremendous network traffic that potentially can disable all network activity by any other PC or dumb terminal on the same county network segment. The infected PC(s) also broadcast enough traffic to temporarily disable any Windows NT 4.0 workstations on the network by causing buffers to overfill, requiring the NT 4.0 workstation to be rebooted to empty the buffer.

As a result, all local district sites with WMS, BICS, CSMS and CBIC dumb terminals may be temporarily unable to connect to the State applications, and likewise all PC based State applications including CONNECTIONS, and e-mail, may be unreachable until the site is remedied.

What is the remedy for sites to follow?
Instructions were previously sent advising that all State network attached PCs at a site be turned off in order to begin the remediation process. Each site systems contact or CONNECTIONS Implementation Coordinator should have received a remedial CD in the mail with instructions. All sites have had special security and logon scripts remotely transmitted to their site's servers. Site systems contacts copy the remedial CD to a State server, and then begin a tedious process of logging on to each networked PC with a special login, and applying the Service Pack upgrades, hot patches and virus definition files until all network attached PCs are cleaned. This activity **must** be followed by a call to the OFT Coordination Center, (1-800-603-0877) which will have a technician scan the site to determine whether any virus activity remains, and gradually work to bring back service to each PC at the site. After all servers and PCs are back up on HSN/HSEN, and no worm traffic is detected by the Coordination Center technician, the site is certified as up and can resume normal operations. Note that when all PCs at the site are turned off,

there usually is sufficient bandwidth for WMS/BICS/CBIC/CSMS dumb terminals and printers to resume operating. An exception would be if a larger network problem causes the entire site to be down temporarily. All information on site status is available from the Coordination Center, but please be patient.

Where do things stand, and how do we find help?
The OFT Coordination Center team is monitoring all State, local district and voluntary agency sites affected by the worm attacks, and has indicated that as of 8/26 AM, considerable PC cleaning by site contacts remains to be done, but we are making progress in this enormous task. As this is a dynamic environment, sites that are up, may possibly go down temporarily, so remaining in touch with **the OFT Coordination Center, (1-800-603-0877)** is important. You may receive several calls each day for status updates-- please bear with us as we are keeping communications consolidated at a central site, and are limiting our callouts as much as possible so sites can perform their remedial tasks uninterrupted.

Also available as resources are your LDSS OFT Customer Relations representatives, the WMS Help Line (1-800-342-3010), and the OFT Enterprise Help Desk (1-800-NYS-1323). Many county DSS sites are working closely with their County IT staff to help combat this problem.