OAKLAND UNIVERSITY

Tuesday, June 10, 2003

UTS contains computer virus

By **Jeff Samoray**, OU Web Writer

Staff from **University Technology Services** (UTS) employed measures last week to contain a malicious e-mail virus that affected desktop computer systems at Oakland University.

The W32.Bugbear.B@mm virus is capable of recording and sending a keystroke log, which could include individual identifications and passwords. UTS detected the virus when a flood of e-mail traffic was recorded at about 11 a.m. June 5.

“There were probably more than 226 infected computers on campus,” said Assistant Vice President for University Technology Services Theresa Rowe. “We started a campus scan to identify the infected computers, logged the ID of those computers at the Helpdesk, and recommended that users disconnect their network cable to eliminate the risk of spreading the virus. Symantec released a specific removal tool the following day so individual scans can be performed.”

The virus itself is a mass-mailing worm triggered by opening a malicious e-mail attachment. It also is polymorphic in that it can change its appearance to avoid detection. The virus is directed mainly toward pc users and those who use Outlook Express and Eudora software. Webmail users were relatively unaffected.

Symptoms the virus exhibits include the sending of randomized mass e-mails with text and subject randomly selected from what an individual is storing on the system. The worm records all keystrokes and stores them in encrypted form. The encrypted file and IP address of the compromised computer then can be sent to an e-mail address defined by the hacker.

“This particular virus was a major national problem that affected many businesses and other universities,” Rowe said. “Symantec (which manufactures anti-virus software) labeled the virus a ‘wild threat’ with a ‘high rate of distribution.’ Fortunately, once detected, the virus is relatively easy to contain and remove.”

Oakland University is protected from viruses at the e-mail gateway level by software manufactured by Sophos and at the desktop level by Norton anti-virus software manufactured by Symantec. Both companies updated their virus definitions by the early afternoon of June 5, and the threat to OU was contained.

While staff from the Helpdesk continue to work with users of infected computers, pc users connected to the network should follow these suggestions:

- Be vigilant for the next several days and do not open any e-mail attachments, even from those you trust, until you call them to confirm that the file was intentionally sent.
- Verify that your desktop file definitions are up-to-date. For most users on campus, this means checking your Symantec File Definitions. This is typically found in your Symantec or Norton anti-virus program under “programs” in the “start” menu. The virus definition file should show a version 6/5/2003 rev. 6.
- If you observe a pop-up window on your system while working on your computer, read the pop-up window carefully. If it refers to Norton with a message like “virus found” and actions like “unable to delete,” the computer has a virus. Disconnect the computer from the network by removing the network cable. Call the Helpdesk at (248) 370-HELP (4357) to report the problem. Do not log off or turn off the computer.
- If you are not receiving virus pop-up windows and are sure your virus definitions are up-to-date, you are reasonably safe to connect to the network.

“I’d advise everyone to frequently refer to the **University Technology Services** Web site for updated information for the campus community on this virus,” Rowe said. “Those who have any questions or concerns also can call the UTS Helpdesk.”

UTS staff also applied a technical upgrade to the Banner system during a scheduled outage that began at 7 a.m. June 6. The affected systems included Banner client, Internet Native Banner, SAIL on the Web and SAIL voice response. In addition, Oakland University Computing Account account activation/password resets were performed. The system upgrade was

completed by the evening of June 8. After necessary hardware/database repairs were made and testing completed, the system was restored at 8 a.m. June 9.

For more information on the Banner upgrade and anti-virus measures and for the current status of the university computer system, visit the **University Technology Services** Web site, or contact them at (248) 370-HELP (4357) or **helpdesk@oakland.edu**.

SUMMARY
Staff from University Technology Services employed measures last week to contain a malicious e-mail virus that affected desktop computer systems at Oakland University.

Created by CareTech Administrator (webservices@caretechsolutions.com) on Tuesday, June 10, 2003
Modified by CareTech Administrator (webservices@caretechsolutions.com) on Tuesday, June 10, 2003
Article Start Date: Thursday, October 9, 2003