

# IT Update

## September Worm Incident Summary

Late the morning of Tuesday, September 20, 2005, the Information Technology Services (ITS) network team reported an event causing serious performance issues. Teams within the department quickly rallied to identify the problem and by mid-day the root of the issue had been identified, and work to remedy the situation had begun.

ITS teams worked day and night to scan, clean, patch and rebuild servers that were affected by the SDbot Worm that was determined to be the cause of serious performance issues within the HSC network. IT forensics determined the cause of the incident to be an un-patched laptop lacking anti-virus software that visited a Japanese website, the suspected source of infection. The first occurrence was 10:45 Tuesday morning, and by 1 p.m., a Command Center was established to communicate the incident both globally and specifically to IT managers.

The worm looks for vulnerabilities and takes advantage of them by downloading other hacking tools. It attacked many servers and 100 confirmed machines across the Health Sciences (Hospital, School of Medicine, Huntsman Cancer Hospital and Institute, Colleges of Health, Nursing and Pharmacy). Infected machines were running a Microsoft operating system that had not been recently patched and were not running anti-virus software. In some instances, the patches were not applied because they had caused performance and functionality problems. A significant number of infected devices were vendor supported machines that do not allow current patching.

While a possibility of information collection existed, **there was no evidence that any data was collected or sent off-site** because the infection was identified quickly. In addition, the Internet connection was immediately shutdown because of potential "back door" vulnerability, infected machines were isolated, and a new firewall was built for added protection.

Once reasonable stability was established, subnets slowly reopened and infected machines were scanned and verified as secure before reattachment to the network. By Wednesday afternoon, Internet traffic, inbound and outbound, was reopened.

After evaluation of the incident, an action plan, including both immediate and future action items, was created to ensure the security of the network.

## Key Action Plan Items

- Repair and patch all machines
- Change administrator passwords
- Enforce existing patching policy
- Move forward with a plan to segment the managed Hospitals and Clinics networks away from the academic/research environments

Over the past several months, ITS staff has been working to refine and improve procedures for responding to system emergencies. While there is always room for improvement, current emergency procedures were followed and the Command Center worked effectively during the incident. We also feel confident that the action plan will help prevent future related incidents.