

# Viruses, Updates, and Security: Making the Campus Aware

Nancy P. Kutner  
Rensselaer Polytechnic Institute  
110 8<sup>th</sup> St.  
Troy, NY 12180  
518 276-8537  
kutnem@rpi.edu

## ABSTRACT

In this time of frequently emerging viruses and worms that attack the Windows operating system, it is important for everyone in a campus community to take an active role in protecting their computers which in turn affects the security of the entire campus.

This paper describes the steps Rensselaer is taking to keep the campus secure from viruses, worms, and spam. These include instructions and notification and a project we have started using DNS to restrict Internet access of infected computers.

Since these are topics that affect all institutions and are vital to the well-being of campus computer security, I would like this paper to be the start of a discussion during the SIGUCCS conference. Some questions to consider include "How do institutions instruct their campus community about 'safe computing'?" and "How have organizations changed how they respond to the 'emergency' situations created by virus outbreaks?"

## Categories and Subject Descriptors

K.3.2 [Computers and Education]: Computer and Information Science Education

K.6.5 [Management of Computing and Information Systems]: Security and Protection

## General Terms

Documentation, Security

## Keywords

Security, Viruses, Worms, Anti-virus software, Documentation, E-mail, Firewalls, Spam

## 1. INTRODUCTION

Rensselaer Polytechnic Institute in Troy, N.Y. is a private institution with more than 8,000 students and over 450 faculty members. Students come from 50 states and 72 countries around the globe.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

*SIGUCCS '04*, October 10-13, 2004, Baltimore, Maryland, USA,  
Copyright 2004 ACM 1-58113-869-5/04/0010...\$5.00.

The Division of the Chief Information Officer (DotCIO) is made up of seven branches. My duties place me in Academic and Research Computing (ARC), the group that provides computing services and assistance for faculty, students, and staff in support of Rensselaer's educational and research mission.

In the paper, I will discuss the procedures that Rensselaer has in place to keep the campus network secure from viruses and worms, e-mail spam, and other attacks. These procedures and plans involve the cooperation of other branches in DotCIO.

The paper concludes with an evaluation of several of these procedures and a list of some future plans and ideas.

## 2. CASE STUDIES

### 2.1 The W32/Sasser.E Worm

May 10, 2004 - W32/Sasser.E Worm Hits Campus

What happened at Rensselaer?

► The article below was posted to the on-line newsletter (*The Kiosk*).

---

#### W32/Sasser.E Worm Hits Campus

Posted: 05/10/2004

More from Virus & Security

The new W32/Sasser.E worm, which automatically spreads via the Internet to computers using Microsoft Windows operating systems, especially Windows 2000 and XP, has recently hit the Rensselaer campus

Please refer to the Symantec website for more information about this new worm. Instructions for removing the worm are also available from this site.

Once again, we cannot stress enough the importance of keeping your anti-virus software up-to-date!

If you need assistance, please contact the VCC Help Desk staff by stopping by in person, via e-mail, or by calling ext. 7777.

---

► A message (similar to the newsletter article) was posted to several listserv lists.

► A poster on an easel was placed outside the Help Desk in the Voorhees Computing Center – a building which is open 24/7. (See Figure 1.)

► Ports were blocked to prevent the virus/worm from spreading.

► The Help Desk prepared to assist users. The student consultants learned about the virus, how it presents itself, and how to clean it. A CD with the patches was created for those whose machines were already infected and were unable to connect to the Internet to download them.

Because this virus was more of an annoyance than one causing destruction, it took only two days for most of the furor to calm down. Classes were not in session at the time mitigating the disruption.



**Figure 1: Easel outside Help Desk with Sasser worm announcement**

## 2.2 W32.Blaster - The RPC Vulnerability

The Blaster worm hit our campus last August just as we were about to distribute 1500 laptops to incoming students. We quickly created a CD to hand out at our laptop distribution time so that students could patch their systems as they were performing the initial configuration. This CD was also available to returning students, faculty, and staff. Student staff from the Rensselaer Union and Residence Life also helped distribute the CD and the virus warning.

We were able to keep the network up and running during this process.

## 3. EDUCATING CAMPUS USERS

Students make up the largest proportion of computer users on campus, but information and announcements need to reach the entire campus community.

The most basic security feature for individual computers is anti-virus software. There is a campus-wide site license for the Symantec anti-virus software, so there is no reason why it shouldn't be installed on every Rensselaer computer and kept up-to-date. Making everyone aware of this is the first step in keeping computer systems secure.

### 3.1 Incoming students

Rensselaer requires all undergraduates to have a laptop computer. Just before classes begin in the Fall, we distribute laptops to incoming freshmen and transfer students who are participating in our Mobile Computing Program -- we have a captive audience.

Symantec anti-virus software is pre-installed on the laptop with the default configuration set to automatically update the virus signature database daily at 8pm, provided the laptop is connected to the network. However, it is possible for students to disable this setting, in which case the software is not updated unless they do it manually.

Students are also given a handout, "Critical Software Updates" ([www.rpi.edu/laptops/laptops03/criticalsoftwareupdates.pdf](http://www.rpi.edu/laptops/laptops03/criticalsoftwareupdates.pdf)) which includes instructions about Symantec anti-virus software and Windows and Office XP updates.

### 3.2 Upperclass students

We have no specific way of reaching upperclass students with these instructions. They learn from each other. If they purchase a new laptop, they are encouraged, but not required, to attend a configuration session.

### 3.3 Faculty/Staff

Faculty/staff education should be developed so that this group knows where to find computing help and who they need to contact in the event of problems.

New employees at Rensselaer are required to attend an orientation session (offered semi-monthly). During this session, staff members from ARC have the opportunity to present information about virus protection, our file backup service (EZ-Snapshot), and our spam-blocking trap, RESPITE (see Section 7.1).

Last March, for the first time, we offered a short one-hour session directed to faculty and staff entitled "Anti-Spam, Anti-Virus, Windows Update." The attendees were pleased with the content and we intend to offer this course again. The announcement described it as:

*Do you have questions about e-mail spam, computer viruses, or updating your Microsoft Windows operating system? This short course, offered by Academic and Research Computing, includes a demonstration of how to use three important computing tools: the campus spam filter called RESPITE, the campus wide antivirus application from Symantec, and Microsoft Windows updates. This short course is open to all members of the Rensselaer community, and registration is not required.*

### 3.4 Documentation

Although we distribute printed handouts at laptop distribution, most of our documentation is available on the web at [www.rpi.edu/computing](http://www.rpi.edu/computing). We provide the instructions users need to perform the basic tasks as well as more in-depth information.

## 4. CAMPUS ANNOUNCEMENTS

Announcements to the Rensselaer community are made in different ways to reach as many users as possible. We also cannot assume that the network will be functioning during a worm or virus outbreak.

We currently use: e-mail, web pages, *The Kiosk* (DotCIO on-line newsletter), CATV (campus cable channel), *The Polytechnic* (campus newspaper), and posters/signs to contact users.

Every few weeks or when there is a "problem," a notice continually cycles on the campus cable "bulletin board" channel reminding students to update their anti-virus software regularly and check for updates to Windows and other operating systems.

In the event of a severe threat, it is also possible to send out a voice mail message to the entire campus.

#### 4.1 DotCIO Policies

No virus should be ignored. Early detection of a problem, and thus a quick lockdown, is essential in limiting the damage and consequences that can result. It is crucial to have early and wide-spread announcements pointing to a single source of authoritative information, a centralized help site. It is also helpful to have patches and removal tools readily available from the anti-virus software vendor.

The Rensselaer community must be made aware of DotCIO's policies with respect to notification so that they know where to look for information and how to spot hoaxes. For example,

- The e-mails we send are brief, and direct users to public sites. We never e-mail attachments with system updates or fixes.
- When in doubt, check with us directly – call the Help Desk, for example.
- Check *The Kiosk* and Help Desk web sites for authoritative how-to's and downloads.

#### 4.2 When a new virus or worm attacks

When a new virus or worm is found on campus, several steps are taken. The consultants at the Help Desk and the full-time support staff prepare to answer questions and help repair computer systems as needed. They learn about removal tools and patches.

Announcements are made to the campus via several methods as follows:

- A poster is placed outside the Help Desk in the computing center.
- Announcements are sent to various newsgroups and listservs.
- A link is placed on the campus homepage to a newsletter article about the virus/worm. (See Figure 2.)
- Ports are blocked as appropriate to the situation.

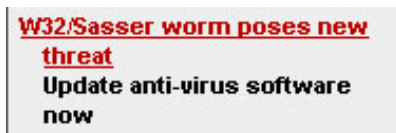


Figure 2: Sasser worm announcement on Rensselaer home page.

### 5. DNS BLOCKING

It is important to find and isolate those computer users who have a compromised system. We do this by limiting their network access to a single server. Controlling their access to the network motivates users to correct problems with their computers and learn and practice safe computing skills. Because laptops move around, we restrict network access based on the MAC (Media Access Control) address, unique to each Ethernet card. Simply blocking a physical network port wouldn't keep a laptop from connecting to the network, as it would a desktop machine. Until the computer is cleaned, it can still infect others as long as it doesn't need DNS or Wins resolution to do so.

Any activity observed or reported that indicates a probable virus/-worm/hacker issue can lead to a machine being redirected or a port being turned off, including:

- suspicious network traffic
- unusual connection attempts in host/server logs
- inappropriate use of services in host/server logs
- a complaint from someone on campus
- a complaint from someone off campus

After an infected host has been discovered, staff disable the normal DHCP boot process, based on its MAC address. DHCP servers will assign an alternate DNS server to direct the user's machine to an alternate IP destination hosting a web page with information about how to clean their machine and restore complete services. (See Figure 4 on the following page.) Users must follow our instructions to clean their machine before access is reinstated.

When the user contacts the Help Desk, the consultants must complete the form below before access is restored to the user by the Hostmaster. (See Figure 3.) The user must have installed the current virus definitions, installed all critical updates, rebooted, and performed a complete scan. It is not necessary for the scan to find something because the critical updates performed might have already removed the virus.

---

Consultant handling issue:

User: \_\_\_\_\_

RCSID: \_\_\_\_\_ Email address: \_\_\_\_\_

Phone Number: \_\_\_\_\_ Voice Mail: y/n \_\_\_\_\_

Primary location: \_\_\_\_\_

User preferred to be contacted by email \_\_\_\_\_

MAC Address: \_\_\_\_\_

NetBIOS: \_\_\_\_\_

Virus Definition Date: \_\_\_\_\_ Revision: \_\_\_\_\_

Antivirus Software: y/n Brand: \_\_\_\_\_

Real time protection: y/n \_\_\_\_\_

Automatic Updates: y/n Weekly Scan: y/n \_\_\_\_\_

Windows Update: \_\_\_\_\_ Number required: \_\_\_\_\_

System reboot: y/n \_\_\_\_\_

Was stuff found during virus scan: y/n \_\_\_\_\_

What was found: \_\_\_\_\_

Ready to reconnect: y/n \_\_\_\_\_

---

Figure 3: Access Reinstatement Form

### 6. FIREWALLS AND THE VPN

Our firewalls are placed at the edge of campus and protect the campus only from traffic coming into/out of our Internet connections. They offer no protection or inspection of on-campus traffic. We do basic port filtering at the firewalls -- this helps to prevent off-campus hosts from infecting on-campus hosts when the exploit is port-based. The firewalls do little content inspection of applications, so they do not prevent users from receiving or opening attachments which may contain a virus or macro. The firewalls offer limited perimeter protection against viruses both leaving and coming onto campus via the Internet connections. and they are by no means a solution to the virus problem.

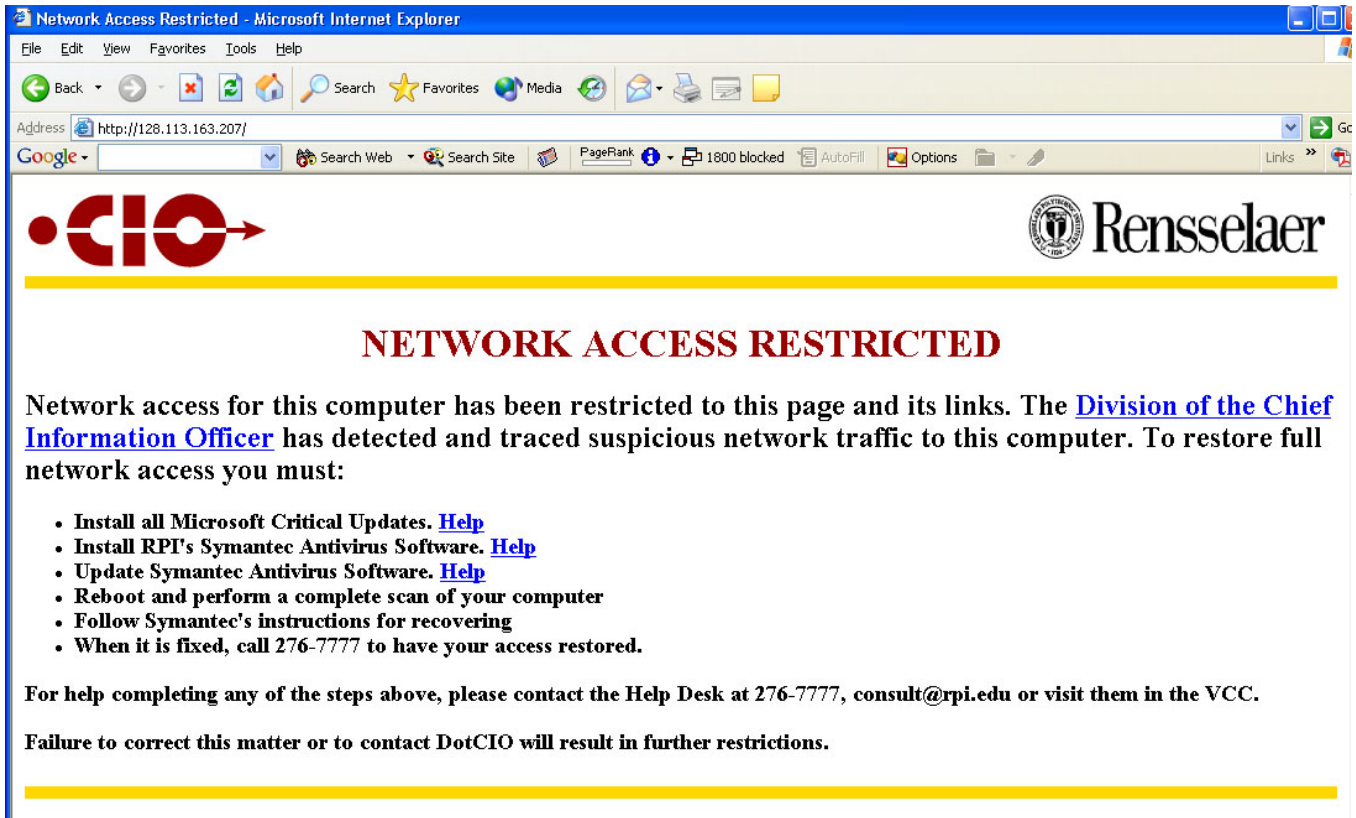


Figure 4: Web page displayed when a user is denied access.

Rensselaer also has a virtual private network (VPN) service available to all faculty, students, and staff which must be used to access the secured campus wireless network. It provides a secure connection between an off-site user and the campus network, allowing remote users access to secured campus resources. The Microsoft Exchange Server for e-mail is an example.

## 7. RESPITE AND OTHER E-MAIL PROTECTIONS

### 7.1 RESPITE @ Rensselaer

Approximately 50% of the e-mail messages sent to Rensselaer are spam. Members of the Rensselaer community can make use of RESPITE@Rensselaer (respite.rpi.edu), a web-based spam e-mail trap which can stop spam at the mail server. Once they have signed up for the RESPITE service, users have control over what they will accept or reject as spam.

In trapping mode, RESPITE works by identifying potential spam messages and holding them on the server. In labeling mode, all e-mail is delivered to the user, but the spam score is included in a header, and the user can then filter e-mail for spam.

Users still need to manage the messages identified as spam, both in terms of identifying a message tagged as "spam" that should be white listed (allowed to be delivered -- false positives) and altering the spam threshold to catch spam that might be missed by the software.

Valid messages are not discarded and the user has the ultimate control over their individual spam tolerance level. In either mode, an auto reject threshold can be set. Messages scoring over the threshold are rejected instead of being trapped.

### 7.2 Campus Mail Server

At the server level, all incoming mail to mail.rpi.edu is virus-scanned and any message with a detected or suspected virus is rejected. All attachments and full message bodies are scanned using an open source anti-virus program. If they turn up anything, the message is rejected.

We block many types of attachments including, but not limited to:

- .bat, .scr, .cmd attachments
- attachments with hidden executables, i.e., attachment names such as "yourfile.txt.com", and numerous standard variations on the theme (e.g., with extra spaces, to hide the added extension type)
- mis-matched MIME types, e.g., a file that claims to be MIME Type "audio", but whose attachment ends in .com
- nested archive files, e. g., a .zip containing a .zip file
- encrypted files, such as encrypted zip

This does not apply to internal e-mail (mail sent within mail.rpi.edu).

### **7.3 Exchange Mail Server**

The Exchange mail server available to faculty and staff uses the Symantec Anti-Virus for Exchange software to scan incoming mail in real time to prevent the spread of viruses by catching them before the messages get into a mailbox. The software also attempts to determine if messages contain viruses that have not yet been identified by using what is known as "bloodhound" technology. This technology attempts to identify unknown viruses by detecting virus-like attachments that could potentially be a new unknown virus. This, coupled with the main mail server anti-virus software, practically eliminates the possibility of Exchange users becoming infected with a virus via e-mail.

## **8. EVALUATION OF CURRENT EFFORTS**

### **8.1 RESPITE**

Only about 2000 users (out of about 8500 active e-mail accounts) have signed up to use RESPITE. This number needs to be higher. Nevertheless, in the month of June, over 1,500,000 messages were scanned and about one third of them were rejected and not delivered to users' mailboxes. Only a small number (about 1300) of messages were held and then later accepted, so the methods used for blocking messages seem to be validated.

### **8.2 DNS Blocking**

DNS blocking has been a great success. Between mid-January and mid-June, we have taken 349 different actions on 259 different MAC addresses. In that time, the number of infected machines on the network in a given day has dropped from an average of 28 to between 0 and 2! When there is a virus outbreak, it now takes about a week for most machines to be cleaned (rather than a month) with the majority of machines cleaned within 24 hours of being redirected.

Because users now know what needs to be done to reconnect their computer to the network, this procedure has also saved time that would be spent troubleshooting by network technicians and Rensselaer Computer Repair.

## **9. WHAT'S NEXT**

It is important to have a plan in place because good plans are rarely created at the time of need. There's an old adage that

applies: "When you're up to your eyeballs in alligators, it's hard to remember that your initial objective was to drain the swamp."

## **9.1 Virus Response Team**

Beginning in the fall of 2003, staff members from the various DotCIO divisions including Academic and Research Computing, Communication and Collaborative Technologies, the Rensselaer Libraries, Operations, and Networking started to meet informally to discuss issues relating to the protection of campus computing. They began to address such topics as leadership, education, communication, enforcement, and planning. We hope that this group's efforts will become more formal and their conclusions implemented.

## **9.2 Future Ideas**

Some of the ideas we are considering include:

- Requiring all students to register their computers in order to gain full Internet access when they are off-campus.
- Using campus System Administrators and student Residential Assistants as liaisons to distribute information.
- Expanding the use of the campus cable TV channel. Monitors could be added to high-traffic areas. It might be possible to have messages transmitted to desktop screen savers on public machines.
- Using WRPI (Rensselaer radio station) in a severe situation.
- Creating a list of fax machines on campus and using a fax message to reach these departments.
- Including handouts about security to everyone picking up a new computer at the Campus Computer Store.

## **10. ACKNOWLEDGMENTS**

In preparing this paper, I have consulted with many of my colleagues. I would especially like to thank Pat Valiquette, Nigel Westlake, Colleen Morrisey, David Hudson, Kent Johnson, Mike Sofka, and Frank Hill who helpfully provided me with the details of their work in this area.