UFIT NEWS: Virus Scanner Deploying in 01/06/2002 Maintenance Window

EI&O Document ID: N0346
Last Updated: 10/04/2002

NERDC NEWS: N0346
January 2, 2002

On Sunday, January 6, 2002, we will deploy virus scanning on the smtp.ufl.edu server. This will provide virus scanning for all UF mail users and servers that are configured to use smtp.ufl.edu or smtp.cns.ufl.edu as their outgoing mail servers.

Most users shouldn't notice any difference (except an extra header in each message that their mail user agent [MUA] may or may not ever show them.) During times of *extremely* heavy mail usage, there may be a short additional delay. This is due to the volume of messages (each message is scanned every time it transits the server), and is not related to the percentage of infected messages. Please keep in mind, however, that viruses such as SirCAM increase the number of sent messages dramatically. We feel that the impact of such an occurrence will be minimal, because we'll (in theory) catch the “first wave,” so there won't be the normal multiplicative effect.

Each message passing through smtp.ufl.edu will be scanned by the NAI virus scanning software. There are three possible outcomes:

- If no virus is detected, the message is passed normally.

- If a category A virus is detected, the MIME part containing the virus is renamed (preventing automatic "running" of the part by well-meaning MUAs), and additional text/plain part containing a warning and the action taken is added to the message.

- If a category B virus is detected, the message is rejected during the SMTP transaction. This results in an SMTP error; most MUAs now show these messages to the user.

Category A Viruses are defined as all those that are not in category B (see below.)
Category B Viruses: A virus that sends itself as a payload without the user intending to send any message. A category B virus looks through the user's address book and sends itself to some or all of the people listed there, without the user's consent -- and sometimes without their knowledge. The SirCAM virus is an example of a Category B Virus. During the scanning process, mail messages are never looked at by a human; infected parts are not quarantined for retrieval or examination. We feel that it is important to ensure users' privacy, especially in the case of a category B Virus (like SirCAM) that mails files from the user's hard drive. When new category B Viruses are released, there may be a slight delay in their classification as such (they will be a category A first). The goal is that if a smtp.ufl.edu user receives a virus, it will not be spread further.

In the near future we will look into expanding virus scanning to include incoming messages sent to ufl.edu and nersp.cns.ufl.edu addresses. Watch for future information on this service.

Questions or problems? Contact the NERDC Support Desk at (352) 392-2061.

News articles, NERDC documents, and related information can be accessed on-line through DOCWEB, NERDC's WWW-based documentation system, at http://docweb.cns.ufl.edu.

Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UFIT Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
(352) 392.2061
<editor@cns.ufl.edu>