Global Information Assurance Certification Paper

Email Viruses - Comparison of Novell GroupWise 5.5 and Microsoft Outlook

By
Katherine A. Warner
Sept 8, 2000

Email viruses are fast becoming the number one cause of headaches today for email administrators. They can spread almost at the speed of light. Administrators can spend all day trying to clean up the effects of one virus only to have another virus enter the system and start creating havoc. This paper will compare how two currently used email systems, Novell GroupWise 5.5 and Microsoft Outlook deal with the deadly email viruses.

Microsoft Outlook is one of the most popular email clients used today. Most of the viruses being written today are being designed to take advantage of the security flaws in Microsoft Outlook. Most of the recent well-known viruses use Visual Basic Script files and requires the use of Microsoft Internet Explorer 5 with the Windows Scripting Host component installed. It also requires the user to utilize a version of Microsoft Outlook or Outlook Express. The viruses, themselves, can come in a couple of different varieties. The two most common are when a user opens an attachment or the user can just open an email message. An example of a virus that is an attachment is the Melting.Worm virus, which affected several companies in early March. Once the attachment was opened, the virus was activated. In addition to several other issues, it started emailing itself to all the addresses in the users' Outlook address book.[1]

Microsoft's remedy for this problem is to constantly release security patches to fix the problems in Outlook and Internet Explorer that the viruses are taking advantage of. They also recommend turning off the Windows Scripting Host. The one thing Microsoft fails to mention is how turning off Windows Scripting Host will affect other applications the user has on their workstation. The user could be given a false sense of security if they disable Windows Scripting Host.[2] Some of the viruses do not utilize the Windows Scripting Host so users are still in danger if that function is disabled.

Novell GroupWise, on the other hand, is not affected by most of the viruses out today. In the case of the Melissa virus, which was activated when the user opened the attachment, GroupWise users most likely were not affected if the email administrators configured the clients correctly. The native GroupWise client can be set to not open the attachment in its native application but to open it using the GroupWise viewing technology which comes with the email package[3]. The GroupWise client has two options for viewing a document attachment. One is to open the attachment using the native application it was created in or you can use the GroupWise built-in viewer is based on a form of WordPerfect. When an attachment is opened using the GroupWise built-in viewer, a copy of the file in its native format is placed in the workstation's temp directory. In the case of the companies that were affected by the Melting.Worm

virus, using GroupWise would have prevented them from losing email messages and the time and money the IS Department spent cleaning up the effects of the virus.

The GroupWise Internet Agent, or GWIA, which is used to relay Internet email to and from the GroupWise system, has a feature that further protects the email system from viruses. The GWIA can be configured by the email administrator to drop off incoming and outgoing email to a third party queue[4]. This will allow the administrator to scan all messages for viruses before they leave and when they enter the email system.

One of the third party products that are written specifically for GroupWise systems is Guinevere. Guinevere is a program that works in conjunction with the GroupWise Internet Agent. It will give the administrators flexibility in dealing with the email viruses. Once a virus is found or discovered, the administrator can configure Guinevere to delete the entire message, remove the affected file attachment, make of copy of the infected message for further troubleshooting off-line or email the intended receiver and sender about the virus discovery[5].

To use Guinevere, the GroupWise Internet Agent must be configured to pass the message to the third party queue. Once the GroupWise Internet Agent receives the message from the Message Transfer Agent or a message that is entering the GroupWise system from the Internet, it converts the message from the GroupWise format to ASCII format. The GroupWise Internet Agent will spool these files into the Guinevere holding directories. Guinevere will then scan the files for viruses. If any viruses are found, it will perform the actions as set by the administrators. If no viruses are found, the messages are then returned to their original GroupWise format and are moved to the input directory for the GroupWise Internet Agent. From this point, they are delivered to their final destination virus-free.

Another way to protect a GroupWise email system from viruses is call SMTP Mail Hosting. Mail Hosting means the GroupWise Internet Agent is configured not to send or receive SMTP mail with its SMTP Hosts. Another SMTP device is configured to act as the “host” for the email sent from or to the GroupWise Internet Agent. The “host” will receive the email from the Internet. A third party virus package is installed on the host and it will scan the messages for viruses. It will then forward the email back to the GroupWise Internet Agent via the SMTP protocol for delivery to the intended GroupWise user. Outgoing email from the GroupWise system will be sent to the GroupWise Internet Agent and them relayed to the mail host for virus scanning. The mail host will send the messages to the Internet.

Unfortunately GroupWise is susceptible to email viruses that appear in the form of an executable attachment. When a GroupWise user opens an executable attachment, the virus is activated and allowed to run its course.

Since GroupWise, like Outlook, used MAPI and the Windows Messaging System, the virus will propagate itself through the user's email system. It is a good suggestion to establish as part of your company's email policy is to not run any executable file attachment until it has been scanned by the IS department.

The only true means to protect an Outlook and GroupWise email system is a desktop virus scanning solution. This way regardless of the email package used and the format the virus is written in, most virus scanners will be ale to pick up the strand of virus and it most cases eradicate it before any real damage can be done to the user's workstation and the company's email system

Sources

1. Ohlson, Kathleen. " 'Melting.Worm' slithers into the wild." ComputerWorld. 17 March 2000. URL: http://www.cnn.com/2000/TECH/computing/03/17/melting.worm.idg/ (8 Sept 2000).

2. "Pros and Cons of Removing Windows Scripting Host." ZDNET – Help & How to – Bugs, Viruses, Security Alerts. URL: http://www.zdnet.com/zdhelp/stories/main/0,5594,2573079-2,00.html (7 Sept 2000).

3. Novell Technical Support. "GroupWise and Viruses." Novell TID 2954960. 31 July 2000. URL: http://support.novell.com/cgi-bin/search/search.pl?database_name=tid&type=HTML&docid=%03%2cF42137%3a968681914%3a%20%28%20viruses%20AND%20%22%7bgw55%7d%22%20%29%20%20%07%01%00&byte_count=10249. (8 Sept 2000).

4. Kratzer, Tay. "Stop the Worm." GroupWise Cool Solutions Tip. URL: http://www.novell.com/coolsolutions/gwmag/tips/t_kratzer_stops_the_worm_virus.html (8 Sept 2000).

5. "What is Guinevere?" Guinevere Product Description. URL: http://www.indecon.com/guinevere/precis.htm (15 May 2000).