Global Information Assurance Certification Paper

Brad J. Peer
November 11, 2000

Securing Microsoft Outlook 2000 Using the Outlook Security Update in a Microsoft Exchange Server 5.5 Environment

On March 26, 1999, the “W97M/Melissa” virus was discovered in the wild. This virus propagated by e-mailing itself to the first 50 addresses in Outlook’s Address Book. This virus rapidly spread infecting an estimated ten percent of all computers on the Internet. By March 31, 1999, a presidential directive had been issued to find and arrest the person responsible for the virus.

May 4, 2000, is a day that many received a love letter. The VBS.LoveLetter worm spread around the world very quickly, crashing many e-mail servers and swamping antiviral developers with requests for information. One of the methods of propagation is by sending a copy of itself to each listing in the Outlook Address Book.

Both of these pieces of malware exploited the programmatic functionality of Outlook. Microsoft released the Outlook E-mail Security Update on June 7, 2000, to address the way Outlook handles attachments and how Outlook is controlled programmatically. There are two things changed by the security update, one is the prevention of access to any e-mail attachment containing executable code and the other limits how available Outlook’s functionality is to third party applications.

The cost of providing this additional security is that there is no access to executable e-mail attachments even if you have confirmed them as valid and safe to execute. Also, many third party applications will not work properly. The E-Stamp program, used to print postage from your PC, is an example of software that will not work with the security update installed. Other affected functions include:

- Mail Merge and Mail Merge to E-mail or Fax - generates a warning message.

- Team Folders - depending on settings may generate a scripting error message.
- Digital Dashboards - if the script attempts access to parts of the Outlook object model that are restricted by the security update you will be prompted to confirm access.
- Net Folder Invitations - may generate warning messages, but will work correctly.

If Outlook is used as the mail client for Exchange Server and you are accessing an Exchange Server mailbox the server administrator can control some features of the update. The e-mail attachments are separated into three categories based on the file extension. Each category is processed in a specific manner.

The Level 1 “Unsafe” category contains extensions that may have executable script or code associated with them. The Exchange Server Administrator can modify the list of extensions included in the Level 1 category. After applying the Security Update any e-mail attachment received, which qualifies as Level 1 attachment, is not accessible. The file cannot be opened, saved, printed, deleted, or processed in any manner. When forwarding an e-mail that contains a Level 1 attachment, the attachment will not be included in the e-mail. Sending a message containing a Level 1 attachment will generate a warning informing the sender that other Outlook users will not be able to access the attachment. This warning can be disregarded, and the message can be sent. Saving an e-mail, with a Level 1 attachment, prompts with a warning informing the user that the attachment will not be accessible from Outlook. Objects inserted into Rich Text messages cannot be opened. Any Level 1 type files saved to an Outlook or Exchange folder cannot be opened.

Level 2 category includes files that are not unsafe, but do require more security. When a message is received that contains a Level 2 attachment, the user is prompted to save the file to disk. This provides the user with the opportunity to access the file on an isolated system or scan the attachment with antivirus software. By default the file list for Level 2 attachments is empty. The Exchange Server Administrator can edit the list to meet corporate needs.

The final category contains all other attachments. Attempts to access attachments in this category produces a prompt to either open the file or to save it to a disk. Clicking to clear the checkbox “Always Ask” turns off future prompts for that extension type. New program associations are included in this category until classified otherwise.

Warning messages are generated when other applications programmatically access Outlook to do any of the following:

- Sending mail on your behalf.
- Accessing your address book.
- Accessing e-mail names from messages.
- Accessing e-mail information from the Contacts folder.
- Saving messages to the file system.
- Searching messages for content.
- Using Simple MAPI to send messages.

The Outlook Security Update becomes an integral part of the program. To remove the update you must uninstall the entire software package that installed Outlook and reinstall. For some this will mean uninstalling and reinstalling Microsoft Office.

If after considering the impact of installing the Security Update you decide to proceed with the installation, the first step is to obtain the update from http://officeupdate.microsoft.com/2000/downloaddetails/Out2ksec.htm. The file “out2ksec.exe” took about 11 minutes with my slow 28.8 modem connection. You also need to have the Office 2000 Service Release 1 installed. This 26 – 40Mb file can be downloaded from http://officeupdate.microsoft.com/2000/downloadDetails/O2kSR1DDL.htm. Be sure to read the Microsoft literature to ensure that the install process is correct for your particular system. Next you will need to install the Office 2000 SR1 (even if Outlook is the only Office 2000 component you have installed on the system), and then the out2ksec.exe file on the client system. Now you can move over to the Exchange Server

to customize the client security settings to match your needs. Administrative tools are available from http://www.microsoft.com/office/ork/2000/appndx/toolbox.htm#secupd. To start with you need to create an Exchange public folder. This is where the customized security setting will be stored and the folder must be a top-level folder in the public folder hierarchy. Name the folder 'Outlook Security Settings.' It is not possible to hide this folder, however, users will not be able to change the contents. Use the Outlook Security Form obtained in the administrative tools to customize your security settings. You can create a default security setting for all your users, or you can create groups of users with different security settings. After you have customized the security settings, the users' systems need to be set to check the server for the security settings. This step is dependent on how Office/Outlook was originally deployed. If your organization uses system policies, then the current ADM file must be replaced with the ADM file downloaded with the administrative tools. If your organization did not use system policies, then you must modify the registry on the client computers. When editing the registry use extreme caution; mistakes made in the registry can cause your system to become non-functional. Backup the registry prior to making any modifications. The registry key is HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Security\CheckAdminSettings Using the DWORD value of 0 (zero), does not apply the custom settings. Any other value causes Outlook to use the custom settings established in the Outlook Security Setting Public Folder. Note that the zero value, or no key found in the registry causes the Security update to use the full security restrictions.

At this point the Outlook clients will be utilizing the customized security settings created in the Outlook Security Settings Public Folder

Works Cited

"AVERT – Virus Alerts –W97M/Melissa".
URL: http://www.avertlabs.com/public/datafiles/valerts/vinfo/melissa.asp,
(7 Nov. 2000).

Dunham, Ken. "I Love You Outbreak". 5 May 2000. URL:
http://antivirus.about.com/compute/antivirus/library/weekly/aa050400a.htm.
(7 Nov. 2000).

Andrews, Josh. "Outlook 98/2000 E-mail Security Update – 6/13/00". 13 June 2000.
URL: http://microsoftsoft.about.com/compute/microsoftsoft/library/weekly/aa061300.htm
(7 Nov. 2000).

"OL2000: Known Issues w/ Outlook E-mail Security Update". Q262634. 16 June 2000.
URL: http://www.microsoft.com/support/kb/articles/q262/6/34.asp
(6 Nov., 2000)

"OL2000: Information About the Outlook E-mail Security Update". Q262631.
9 June 2000. URL: http://www.microsoft.com/support/kb/articles/q262/6/31.asp
(6 Nov., 2000)

"Microsoft Office 2000 Outlook 98/2000 E-Mail Security Update White Paper".
September 2000. URL:
http://www.microsoft.com/office/ork/2000/appndx/toolbox.htm#outsecwp
(8 Nov. 2000)