E−mail policies that prevent viruses

http://advosys.ca/papers/mail−policies.html
Mar 12 2004

It seems like there's been an endless series of e−mail based threats since Melissa started everything early in 1999. Sircam and Nimda made the most headlines in 2001, Klez was king in 2002, and MyDoom spread early in 2004. Many other lesser known threats have also spread via e−mail.

Why are e−mail attachments still such a threat to Windows users? Is there no better way to defend against these threats than to warn Windows users to be afraid of opening attachments?

Anti−virus software is an essential first line of defence in preventing known viruses and other malware. However, anti−virus is *reactive*: it only recognizes known malware. Pattern file updates have to be distributed to every desktop and server at least once a week. Sircam, Nimda and MyDoom took just a few hours to spread worldwide... far faster than anti−virus vendors could create pattern files. Organizations need another layer of protection in addition to the simple−minded 15−year−old technology of virus pattern detection.

For organizations tired of taking heroic measures each time a new MS Outlook worm makes headlines, there is a simple defence that stops almost e−mail malware. The defense requires a small change in policy and protects your organization from the majority of e−mail threats, including the future threats malware writers are working on right now.

The current situation

Below are the top viruses from November 2001 through November 2002:

Name	**Spreads via**	**Filename**
Nimda	E−mail attachment, then via IIS web servers, network drives, and direct file infection	sample.exe or readme.exe
Sircam	E−mail attachment, network drives	random .exe, .bat, .com, .pif or .lnk executable files
Funlove	File infection	N/A
Hybris	E−mail attachment	various .exe files
Aliz	E−mail attachment	whatever.exe
Magistr	E−mail attachment	random .exe, .bat, .com, or .pif executable files
Klez	E−mail attachment	various .exe, .bat, .scr, or .pif executable files
Bugbear	E−mail attachment	various .exe, .scr, or .pif executable files

Each of the above except one propagates via e−mail messages as an executable attachment. Some use double file extensions (eg. .jpg.exe) to exploit a Windows misfeature that only displays the first extension. Most exploit weaknesses in the MS Outlook e−mail client to automatically execute the attachment without the recipient even opening the message. It's the new fad among malware writers.

We've all educated our users to be cautious opening executable attachments. Regardless, even sophisticated users clicked on the attachment named "www.myparty.yahoo.com" carried by the "My Party" worm that spread in

January 2002.

Another problem is the Microsoft platform has multiple undocumented file types such as "SHS" that can be executable. This is made worse by the fact that bugs in MS Outlook and other applications allow executable files to masquerade as harmless JPEGs or text files.

The business case for executable attachments

Most organizations send and receive word processing documents, spreadsheets and other documents via e−mail as attachments. However, very few organizations need to receive executable file types. Occasionally, a technical user needs an .exe file from a vendor, but most users never need to receive such files.

The few users who do need to receive executable files are usually system administrators and other technical staff. Usually they're in close contact with the sender. Even among technical users, the need to receive executable files via e−mail is very low.... most software is downloaded from web sites, not received from a stranger via e−mail.

If most malware spreads as executable e−mail attachments, and only a handful of your users need to receive such files, why does your e−mail system spread unknown executables to all users?

A reasonable precaution

Every security measure involves some form of inconvenience... the security of locking your car carries with it the inconvenience of having to locking it, potential of locking the keys inside, or losing the key. The trick is to balance the benefit of a security measure with the cost of the inconvenience.

Survey your organization and you'll likely discover that users only need to receive word processing, spreadsheet and ZIP file attachments. Some other special files may also need to be considered, but usually the files users need to receive are *not* Windows executables.

One vocal minority is technical staff. System administrators will insist they must have unrestricted ability to receive every possible file type via e−mail and the world will end if that right is taken away. True or not, technical staff are a minority in most organizations.

If your intranet was infected by Nimba in September 2001, calculate the time it took to clean it completely from all intranet IIS web servers. Multiply that time by the hourly wage of the systems personnel involved, then estimate the productivity lost due to congested networks from the traffic Nimba created.

Compare that amount with estimated lost productivity of systems staff if they had to ask senders to rename or ZIP up executable file attachments.

Every organization has different operational needs, but for most the benefits of blocking malware like Nimba out far outweighs inconvenience to a minority of users. Keep in mind that blocking executable attachments doesn't completely prevent receiving them via e−mail... it just makes less convenient. Executables can still be received if the sender renames them or puts them in a zip file.

Methods of blocking

Chances are your organization already uses an e−mail gateway to scan for viruses and to protect fragile internal MS Exchange mail servers. The following e−mail anti−virus gateway products can also selectively delete or block attachments:

- Aladdin eSafe Gateway for SMTP
- McAfee Webshield SMTP
- Symantec Norton Anti−virus for Gateways
- Trend Micro Interscan Viruswall

Advosys Consulting does not necessarily endorse any of the above products. They are listed as examples only. This is not a complete list of commercial e−mail gateway products capable of stripping attachments.

Choose products wisely

While many products claim to selectively block attachments, not all of them work as well as they should. Before implementing any gateway product in your organization, conduct a *thorough* functional and performance evaluation: never rely on the promise of the vendor that a given feature actually works as required.

In particular, the following are often missed by many mail gateway products:

- Attachments with multiple file extensions (eg. ".jpg.exe" or ".gif.gif.scr")
- Ability to block or scan files inside TNEF ("winmail.dat") attachments
- Attachments with a MIME type eg. "application/octet−stream") but no filename.
- Attachments using Windows CLSID extensions

Multiple file extensions exploit a vulnerability in MS Windows and MS Outlook where the attachment can appear using the icon of one extension (eg. a JPG image icon) but when the user opens it, is executed using another extension. Usually the last extension is used when opening the attachment, so a ".jpg.exe" file will appear to be a harmless JPEG image in MS Outlook but is really an executable program. MS Outlook Express has a worse bug when there are three extensions: the first and last extensions are used for the icon, but it opens the file using the middle extension type: a file named ".jpg.bat.jpg" will be executed as a batch file. There are few legitimate uses of multiple file extensions in the Windows world... a good anti−virus gateway will drop them completely, or scan all attachments no matter where the extension is in the file name.

TNEF is a proprietary archive file type used only by MS Outlook (see below for more detail). A good anti−virus gateway will either delete winmail.dat attachments, or open them and scans the contents.

The MIME standard requires all attachments to have a MIME type, such as "application/msword" for MS Word documents. However, attachments are not required to have a file name. When the file name is missing, most e−mail clients use the MIME type to decide how to open the attachment. Unfortunately, some anti−virus mail gateways ignore the MIME type and only scan attachments based on file name. Others trust the MIME type but ignore the filename. A good anti−virus gateway will scan all attachments, regardless of MIME type or file name.

Some mail clients can also be tricked into executing attachments when a Windows CLSID is used as an extension. For example, a file with extension .jpg.{3050f4d8−98b5−11cf−bb82−00aa00bdce0b}= will appear as a JPEG image in MS Outlook, but be executed as a VBScript macro. A good anti−virus gateway will block or disable such attachments... simply removing unusual characters (such as "{") from filenames neutralized many of these types of exploits.

Advosys Consulting has had very good results using a combination of Open Source software: Postfix (www.postfix.org) and the Anomy Sanitizer (mailtools.anomy.net) can be combined to create a high performance, highly reliable filtering e−mail gateway (see our paper "Filtering e−mail with Postfix" http://advosys.ca/papers/postfix−filtering.html). That combination of software creates a very reliable "mail firewall" that catches all the tricks described above.

A testing tool for e−mail security is provided by GFI Security at http://www.gfi.com/emailsecuritytest/. However, it's a good idea to also perform your own testing, not just rely on demonstrations provided by software vendors.

Bypassing the block

The majority of your users never need to receive an executable attachment, but a few, such as technical staff remain. Most e−mail gateway software provides an exclusion capability: a list of e−mail addresses exempt from file blocking. Placing all technical staff on the list allows them to receive all attachment types.

However, that's a dangerous practice. Most technical staff are usually aware enough to think twice before running an attachment, but being aware isn't good enough: some malware execute automatically in MS Outlook without the recipient taking any action. Others trick MS Outlook into displaying executables as "harmless" JPEG or GIF image files.

A better practice is to simply ask the sender to ZIP the executable or rename it so it bypasses the e−mail gateway filter. Most often, technical staff are in contact with the sender and can make such a request. It's an annoying policy that will result in much grumbling from technical staff, but it's the safest policy for the organization as a whole.

> Some e−mail gateway software apply file policies to contents of compressed files too. For example, eSafe SMTP looks inside ZIP files and blocks the entire ZIP attachment if it contains a banned file type. With the advent of SOBIG worm in 2003, this is now recommended. Gateway mail filters should apply file policies to both normal attachments, and files inside ZIP files.

Effectiveness of the policy

Most e−mail based malware propagate as one of the many Windows executable file types. The more sophisticated viruses will send attachments with double extensions (for example .doc.exe or .gif.bat). This can can fool MS Outlook into displaying the wrong icon for the attachment type, but will not fool a properly written e−mail gateway that ignores double attachments and looks only at the last portion of the file name.

Most e−mail viruses use the well−known Windows executable types of .exe .com and .bat. Other use more obscure, sometimes undocumented, extensions such as .pif, .lnk, and .shs. Unfortunately, the Windows platform has multiple undocumented file types that can be used to execute code.

As a minimum, we recommend blocking the following file types:

> exe com vbs vbe dll ocx cmd bat pif lnk hlp msi msp reg cpl inf
> asd cab shs shb scr sct chm wsf wsh wsc eml hta vcd vcf eml nws

The above file types have all been used at some time to distribute malicious code via e−mail or web pages. Blocking them will prevent the majority of e−mail viruses. Microsoft recently released a patch for MS Outlook that also blocks file types: see http://support.microsoft.com/default.aspx?scid=kb;EN−US;q262631 for a list of file types Microsoft recommends to block.

MS Office macros

Blocking executable file types won't prevent macro viruses hidden inside documents. For example, the Melissa macro virus arrives as an auto−execute macro in an MS Word document. Stripping executable attachments won't prevent that type of virus.

Luckily, most SMTP anti−virus software can detect most MS Office worms and even completely remove macros from inside files. Recent versions of MS Office, WordPerfect Office and others also have macro protection options that can disable macros that automatically executable when a document is opened.

MS TNEF attachments

You should also consider adding filename "winmail.dat" to the list of removed files. MS Outlook 98 and higher can encase attachments in a proprietary file type Microsoft ironically calls "transport neutral encoding format" (TNEF). The TNEF file contains all attachments, plus HTML or RTF versions of the body of the message. TNEF files are usually named "winmail.dat".

Most e−mail anti−virus programs can't open the winmail.dat attachment and pass them without scanning. Because it encases all other attachments in the one iunreadable file, allowing winmail.dat files through can permit executable files to enter, despite other gateway filters.

Internet users typically don't realize their copy of MS Outlook is sending their attachments encased in a winmail.dat file. However, they quickly learn about it the first time they send mail to someone who doesn't use MS Outlook: only MS Outlook is capable of reading the proprietary winmail.dat TNEF file format.

The option can be disabled in MS Outlook 2000: open the "Tools" menu, pick "Options", then change the setting "send messages as Microsoft Rich Text Format" to either "Plain text" or "HTML". Attachments will then be sent in standard MIME format that can be opened by anyone and can be scanned by SMTP anti−virus software (see http://support.microsoft.com/default.aspx?scid=kb;EN−US;q138053 for more information).

Microsoft fixes Outlook

Early in 2002, Microsoft finally took a step to address the problem of executable attachments in their Outlook e−mail client. Outlook 98, Outlook 2000 and Outlook Express 6 can now stop users from receiving most executable attachments. See http://office.microsoft.com/Downloads/2000/Out2ksec.aspx for information on the "Outlook Security Update".

By default, the patch prevents Outlook from opening or sending attachments with the most common executable extensions such as .exe and .scr. Since the introduction of this patch, the number of Outlook e−mail worms has dropped dramatically.

The patch is valuable, and highly recommended. However, Outlook remains vulnerable to MIME and buffer overflow bugs, HTML attacks and "forgotten" executable files. An Internet gateway filter that removes attachments and fixes improperly formatted messages provides a necessary first layer of protection.

Other effective policies

Renaming unknown file types

Another recommended policy is to rename unknown file types. The Windows platform has multiple undocumented "executable" file types. For example, the .shs file type (Windows 3.1 "scrap object") is left over from the Windows 3.1 days and was forgotten about by most people. Unfortunately it still has special meaning in current versions of Windows. This file type was used early in 2001 as a new vector for an MS Outlook exploit. New undocumented file types are discovered regularly... it is not possible to compile a complete list of files that Windows will automatically execute.

Some e−mail gateway software can rename unrecognized file extensions to prevent MS Outlook from automatically executing a newly discovered file type. Renaming can be done so the original file name is easily recognizable so it can be restored by the user when saving the attachment. For example, the Anomy Sanitizer can rename unknown file types with a pattern such as "resume.SHS_RENAMED002"

HTML E−mail

Another extremely effective policy to strip HTML e−mail or convert it to plain text. The HTML handling in MS Outlook relies on the MS Internet Explorer engine. All vulnerabilities in MS Internet Explorer are therefore shared by MS Outlook. There are numerous e−mail exploits that target Outlook's handling of HTML formatted e−mail.

HTML e−mail can also contain "web bugs" ... links to image files on the sender's web server. Opening the HTML mail logs that fact on the sender's server. Most spammers use web bugs to confirm an e−mail address is active so they can send even more spam. Attackers use web bugs to gather IP address, browser type and operating system information that MS Outlook volunteers when opening HTML e−mail (see http://www.privacyfoundation.org/resources/webbug.asp for more information).

Some e−mail gateway software can convert HTML e−mail into plain text. MS Outlook when used with MS Exchange also has a similar capability. Anomy Sanitizer can rename hostile HTML tags in HTML mail, leaving the message readable but without advanced formatting like style sheets.

We strongly recommend converting HTML−formatted e−mail into plain text at the gateway level as a general policy.

The future

To date, no e−mail worms or viruses have been smart enough to encase themselves in a ZIP file. However, once blocking of executable attachments becomes a common practice, we can expect to see zipped executables and other obfuscation tactics from virus writers.

Defending against malware will always be an arms race... no one defense will work forever. Regardless, blocking executable attachments is extremely effective right now and does prevent almost all e−mail based threats from attacking your organization.

Comments, suggestions, criticisms, additions to this document?
Please e−mail **whitepapers (at) advosys.ca**

Latest version of this document available at http://advosys.ca/papers/mail−policies.html

Last modified Mar 12 2004

Advosys Consulting Inc.

Copyright and terms of use

http://advosys.ca/papers/copyright−special.html
Mar 08 2003

Use of this document

Permission to use this document from the Advosys Consulting web site is granted, provided that (1) This notice notice appears in all copies, (2) use is for informational and non−commercial or personal use only and will not be copied, reprinted, or posted on any network, computer or broadcast in any media, and (3) no modifications of the document are made.

Educational institutions (specifically K−12, universities and community colleges) may reproduce the Documents for distribution in the classroom, provided that (1) the below copyright notice appears on all copies, and (2) the original Uniform Resource Locator ("URL") of the document on the Advosys Consulting web site appears on all copies.

Use of this document for any other purpose requires written permission of Advosys Consulting Inc.

Limitation of liability

Advosys Consulting makes no representations about the accuracy or validity of any claims or statements contained in the Documents and related graphics ("the content") on the Advosys web site. Further, Advosys Consulting Inc. makes no representations about the suitability of any of the information contained in the content for any purpose. All such documents, related graphics, products and services are provided "as is" and without warranties or conditions of any kind. In no event shall Advosys Consulting Inc. be liable for any damages whatsoever, including special, indirect or consequential damages, arising out of or in connection with the use or performance of information, products or services available on or through the Advosys Site.

Trademarks

Product, brand and company names and logos used on the Advosys web site site are the property of their respective owners.

Comments, suggestions, criticisms, additions to this document?
Please e−mail **whitepapers (at) advosys.ca**

Latest version of this document available at http://advosys.ca/papers/copyright−special.html

Last modified Mar 08 2003

Advosys Consulting Inc.

About Advosys Consulting

http://advosys.ca/papers/about−special.html
Mar 08 2003

Advosys Consulting is a systems management company: we secure systems, build networks and servers, and perform research and evaluations. We have a broad range of experience, but concentrate on Internet technologies and IT security.

Advosys Consulting is a privately held corporation with headquarters in Ottawa, Canada. We have been providing solutions to private sector and government clients since 1990.

Areas of expertise

Advosys is a diversified consulting firm providing services in many areas of Information technology:

- Internet technologies
- IT security including firewalls and intrusion prevention
- Web applications
- Network architecture
- Unix and Linux systems management

Comments, suggestions, criticisms, additions to this document?
Please e−mail **whitepapers (at) advosys.ca**

Latest version of this document available at http://advosys.ca/papers/about−special.html

Last modified Mar 08 2003