Subject: feature request
Posted by Griffyn on Tue, 27 Jun 2006 01:04:14 GMT
View Forum Message <> Reply to Message

Hi,

I'd like to see the following features implemented:

1. Being able to specify that the Attachment Filter delete e-mails containing attachments whose extension ends in a period (eg somefile.exe.). It's impossible to rename a file to be like this on a Windows system, therefore only viruses use these types of files in order to defeat extension matching.

2a. A new filter for Zip files (and being able to handle other common compressions maybe) so that any password-protected archives are redirected to a specific e-mail address. Some viruses send themselves in password protected archives, and include their password in the e-mail body, so it's no issue for the recipient to open and activate the virus - but no virus scanner can scan the files for viruses. This e-mail address would be set up to point to a holding mailbox so that legitimate e-mails can be onforwarded once their contents have been determined.

2b. An alternative would be to have a new filter that tries every word contained in the body of the e-mail to uncompress the archive. If one of the words succeeds, then this is virtually guaranteed to be a virus, as there is no sense in anyone sending a legitimate password-protected archive along with the password.

Subject: Re: feature request
Posted by lleachii on Thu, 10 Aug 2006 19:26:28 GMT
View Forum Message <> Reply to Message

1. I like that idea, I wonder what happens when you add "*." to the Attachment Filter.

2a. I have set my attachment filter to block all ZIP files. It will deliver the email, but strip the file. In my organization, there is not often when someone must receive a ZIP file, so this can be done. You suggestion was a good idea though. I added this to NST because I had a user receive a ZIP file with the mydoom virus inside.

2b. Agreed.

Subject: Re: feature request
Posted by support on Mon, 14 Aug 2006 09:50:48 GMT
View Forum Message <> Reply to Message

Regarding topic 1, NoSpamToday! passes attachment with names ending with a "." character, because some users requested it. Filenames like these are not only legal on non-Windows operating systems, they are apparently also frequently used.

In the next version we will change the attachment filter behaviour to remove all trailing "." characters before the attachment name is checked: this should still pass files such as "somefile.", but block "virus.exe.". This should get rid of viruses trying to exploit this, while at the same time legitimate usage of trailing dots is still possible.

Subject: Re: feature request
Posted by Griffyn on Wed, 20 Sep 2006 00:31:25 GMT
View Forum Message <> Reply to Message

Further analysis has seen viruses that use password-protected zip files include the password (usually a 5 digit number) as an embedded .GIF file, so scanning the the body of an e-mail would not help.

I think having the redirect for password-protected archives is still a good idea though.

Subject: Re: feature request
Posted by Griffyn on Wed, 08 Nov 2006 00:27:16 GMT
View Forum Message <> Reply to Message

I have written my own Zip filter. It looks at the filenames within a zip file and can reject the e-mail if a filename with a blocked extension (blocklist is passed by the command-line) is present. It also handles embedded messages.

It handles all of my requests above - the filelist within a zip file cannot be password protected, so all files are visible. The only exception is a password-protected zip file within a zip file, but I handle that by simply blocking any files whose extension is .zip. It also blocks any files whose extension ends in a period.

Subject: Re: feature request
Posted by support on Wed, 08 Nov 2006 10:53:43 GMT
View Forum Message <> Reply to Message

> I have written my own Zip filter. It looks at the filenames
> within a zip file and can reject the e-mail if a filename with
> a blocked extension (blocklist is passed by the command-line)
> is present. It also handles embedded messages.
>
> It handles all of my requests above - the filelist within a zip
> file cannot be password protected, so all files are visible.
> The only exception is a password-protected zip file within a
> zip file, but I handle that by simply blocking any files whose

> extension is .zip. It also blocks any files whose extension
> ends in a period.

Excellent work!
How about adding your filter to the tools in the NoSpamToday!
Contribution Area (http://www.byteplant.com/support/nospamtoday/contrib.html)?
