

Applying More Aggressive Filters to GEE Whiz™

GEE Whiz installs with a default set of filters and special lists for anti-Spam purposes. The settings for those filters and lists are maintained in a special set of files located in the GEE\TMPLTS directory. Normally, you would manage filters or modify addressees in the SPAM-Control lists using the GEE Whiz Admin web console. We have included three files that are pre-configured with settings that will make GEE Whiz more aggressive from the initial deployment, or improve it's aggressive stance at any time.

You can apply these files directly to an installation by copying them into the GEE\TMPLTS folder. **Note** – Omni strongly recommends that you examine the filter files and copy specific lines from the content of these files into the existing files. You must unload and reload GEE Whiz in order for changes to filter files to be read into memory and become effective. The best approach is to isolate specific regex statements from a filter, copy it into the respective existing file, unload and reload GEE / GEE Whiz and monitor both the daily log file and the Filter Quarantine to see the results from a given regex statement. If a regex statement is causing a problem, then you can delete the regex filter using the GEE Whiz Admin web console without having to unload GEE Whiz.

Apply a More Aggressive File-Name Attachment Filter

The ATTFILT.TXT file contains the list of file types based on known file extensions, e.g. ***.COM\$** (note that the "\$" denotes that the listed extension must match the last part of the entire file name. We have added extra Regular Expressions or "Regex" written by experienced GEE Whiz administrators to combat known Virii attacks. Each of the Regex lines are documented in the file.

Apply a More Aggressive Content Filter

The CONTFILT.DAT file contains "Regex" statements that define the different content filters that are applied against all email. This file normally cannot contain any commenting, so we have included an explanation for each Regex line in this file below:

Purpose: Match content with this phrase

Regex: 7-bit ASCII encoding

Purpose: Match content with word "[M]ortgage"

Regex: \[M\]ortgage

Purpose: Match content with word "viagra"

Regex: viagra

Purpose: Match content with this URL

Regex: http://chlending.com

Apply a More Aggressive Header Filter

The HEADFILT.DAT file contains "Regex" statements that define the different header filters that are applied against all email. This file normally cannot contain any commenting, so we have included an explanation for each Regex line in this file.

[From] Filters

Purpose: Virus with this From tag

Header Name: From

Regex: "Email System"

Match Start: Enabled

Applying More Aggressive Filters to GEE Whiz™

Purpose: Virus with this From tag
Header Name: From
Regex: "ms internet message storage system"
Match Start: Enabled

[Subject] Only Filters

Purpose: Netsky.C Removal
Header Name: Subject
Regex: ^\s{0,1}(notice!|its me!|x27m back!|last chance!|lol|Re: <5664ddff\x3F\x3F\x3F\xBA2>|notification denied!|Question|believe me|Re: (hello|important|hi|excuse me|hey exception|information)|something for you|you\x3F|Re: Re: Re: Re: re: take it error|illegal...|goodmorning|private\x3F|stolen|Here it is|info|what\x27s up\x3F|moin|warning fake\x3F|Re: unknown dear|hello|important|Yep Re: does it|\x3F hi read it immediatelly|hey trust me|question|report|Status|Delivery Failed)\s{0,5}\$

Purpose: Netsky.D Removal
Header Name: Subject
Regex: ^\s{0,1}Re: (Approved|Details|Document|Excel file|Hello|Here|Here is the document|Hi|My details|Re: Document|Re: Message|Re: Re: Your document|Re: Thanks!|Thanks!|Word file|Your (archive|bill|details|document|letter|music|picture|product|software|text|website))\s{0,5}\$

Purpose: SWEN Removal
Header Name: Subject
Regex: ^\s{0,1}(New Network Critical Pack|Error AdviceHelp Please..|New Net Critical Update|Abort Advice|Net Patch|Failure Letter|Help Please..|Failure Report|barcharts|Bug Announcement|Casino!|Evaluator)\s{0,5}\$

Purpose: Block based on text – suspected Virus
Header Name: Subject
Regex: Check this out kid!!!

Purpose: Block based on text – suspected Virus
Header Name: Subject
Regex: Linda Carroll

Purpose: Block based on text – suspected Virus
Header Name: Subject
Regex: Failure Letter
Match Start: Enabled

Applying More Aggressive Filters to GEE Whiz™

Purpose: Block based on text – drug related

Header Name: Subject

Regex: xanax

Purpose: Block based on text – drug related

Header Name: Subject

Regex: valium

Purpose: Block based on text – suspected Virus

Header Name: Subject

Regex: barcharts

An Example of Handling Nasty Emails

Included in the \Docs folder are two sample emails (Sample1 and Sample2) which are showing a particular nasty type of email since we cannot decipher plain language text. In particular, Sample2 caused the user's PC to spike to 100% utilization as soon as the GroupWise client was opened. These emails had no effect if opened with SMTP compliant email reader or through WebAccess. To combat the two examples that we are showing, you will find the following filters in the CONFILT.DAT and HEADFILT.DAT files:

HEADFILT.DAT Filters

Purpose: Block based on nasty characters (See Sample1.pdf)

Header Name: Subject

Regex: ¡¹\$Ú²@©wnÁÈ̈¡¿ú¡¹

Purpose: Block based on nasty characters (See Sample2.pdf)

Header Name: Subject

Regex: »¶Ó-

ÄúËëÑ\$¹áï³õ¼¶à,Çêwww.gwgz.comµÇÂ½¿¡¹áïÃâ·Ñ³õ¼¶à¡±£-ÓÃ»\$Ãû:¡°gtcjb¡±,ÃÜÂë:¡°666666¡±¡£

CONFILT.DAT Filters

Purpose: Match content with this URL (Sample1.pdf)

Regex: http://www.isuptou.com/rich.htm

Purpose: Match content with this URL (Sample2.pdf)

Regex: http://www.55188.net/downs/soft/643.htm

Purpose: Match content with this URL (Sample2.pdf)

Regex: ftp://mycode:downcode@219.129.216.133/pub/dxsy6.exe



Applying More Aggressive Filters to GEE Whiz™

Sample 1 Email

From: "I-Î»s³y³⁄₄÷" [mailto:wkk2w.b0sizr@diysvr.net]
Sent: Tuesday, August 24, 2004 6:16 AM
To: honway@hotmail.com
Subject: ¡¹§Ú¤@©wnÁÈ`ì¿ú¡¹

Sender: "I-Î»s³y³⁄₄÷" <wkk2w.b0sizr@diysvr.net>
 Reply-To: ahew002@ahoo.com.tw
 Date: Tue, 24 Aug 2004 17:59:57 +0800
 X-Priority: 2
 X-MimeOLE:Produced By Microsoft MimeOLE V6.00.2600.0000
 Return-Path:ahew002@ahoo.com.tw

[honway@hotmail.com]
 ¡¹§Ú¤@©w-nÁÈ`ì¿ú¡¹
 §A^{ao}¤u\$@Ã-©w¶[Û?©Î-O±z¤£°¡·N¥Ø«e^{aoa}-ªp¡A
 -°¤»»ð¤£¤U©w`M¤ß°¤¤W¿i³⁄₄Û§iÁÛ©O¡I½¤¡u°¤¤Wlæ°Ê¡v¡F
 §OÁý¡i³⁄₄÷·l¡jlb±z^{ao}¡¿i³⁄₄Û¡j¤¡¡µS¿Ý¡j¤¤±q`-Ãä¿ù!L¤F¡C
 -ü°êlb@a³¤·~`t²Î,
 ¤w_gl`¥^{ao}lb¥p¥@-ÉÀ°§U³\h¤H¡j³¤·~¡j!`¥¡A
 Åý±z|Û¤v·¡¡mlÑÁó¡n¡A`C-Ó¤ëÃ-©w¼W¥[|~¤J¡Alý-O¡F
 ±z¥²¶·½Ö³⁄₄ã-°¡mlÑÁó¡n^{ao}¤ß°A¡A ¤~-à³q¹LÄY@æ^{ao}¡m¿z¿i¡n¡A
 ¡y¤@¤ÁÂk¹s¡z¡B¡y»{-u¡z¡B¡y|³³¹¿i¡z¡B¡y«ö³¡N-Z·Óµ{§Ç°µ¡z¡A
 ¤~-O§Ú-ì-n§ä^{ao}¤H¡A½¤¡u°¤¤Wlæ°Ê¡v¶[i¤J°ô-¶°Ñ³X¡F
 http://www.isuptou.com/rich.htm
 lpªG§A-O«D±`·QÁÈ¿ú and §V¤O¥'«÷»{-u^{ao}¤H-----½¤¶[i¤J°ô-¿Á@Á@§a!

±z©Ò-ì-î^{ao}¡q¤«H¡A¥D-n`ÓlÛ¼s§i¥D¡C-Ö-Y¥»¡,¹q¤«H¤°®e«D±z©Ò»Ý¡A©Î³y|`±z^{ao}¤£«K¡Alb|V±z-P¤
 W¥Ñ°J°p·N¡C
 ¡¹-Y¤£·QlAl-`ì!Ãp^{ao}¡q¤³ø ½¤mail`ì: ahew002@yahoo.com.tw¡¹
 [honway@hotmail.com]



Applying More Aggressive Filters to GEE Whiz™

Sample 2 Email

From: <cgfjcgfyjcgftjy@fxgk.dfh>
To: <achristie@abc-md.org>
Date: 8/7/2004 8:55:30 AM
Subject:

»¶Ó-ÄúÈëÑ§¹ãí³õ¼¶°à,Çëwww.gwgz.comµÇÂ½¿¹ãí·ÃâXÑ³õ¼¶°à;±£-ÓÃ»§Ãû:¿gtcjb
 ;±,ÃÜÂë:¿°666666;±;£

»¶Ó-ÄúÈëÑ§¹ãí³õ¼¶°à,Çëwww.gwgz.comµÇÂ½¿¹ãí·ÃâXÑ³õ¼¶°à;±£-ÓÃ»§Ãû:¿gtcjb;±,ÃÜÂë:¿°6666
 66;±;£

Äú°Ã£;

»¶Ó-ÄúÈëÑ§¹ãí³õ¼¶°à,Çëwww.gwgz.comµÇÂ½¿¹ãí·ÃâXÑ³õ¼¶°à;±£-ÓÃ»§Ãû:¿gtcjb;±,ÃÜÂë:¿°6666
 66;±;£

»ù´¿µÄÍ-Ñ§¿ÉÉëÇëÖÐ¼¶°à£-½²ÄÊÇ;¶¶ÆÄÜÍ³¹É¼¼Êõ;X40Ð;Ê±¹âÀ£-¿ÉÉÏÖÐ¼¶°àÂÛÏ³ÍáÊ£-²
 ¢ÓÐÄ¿ÈÖ°EÖµ;£

³¹ÉÐÂÊé<¶¶ÏËÊÇÒøÖ@Áù>ÌÆÄÜÍ·Öø ÓÐÃâXÑÍÂÔø: (ÒÏÏÂÖ³ÈëµØÖXÀ,¼¿¿ÉÏÂÔø)
<http://www.55188.net/downs/soft/643.htm>
<ftp://mycode:downcode@219.129.216.133/pub/dxsy6.exe>

¿¶¶ÏËÊÇÒøÖ@Áù;XÄ¿Â¼

- 1 ¹É°£¶¶Í» ¾ùÏß2+3
- 2 60ÏËÊÇÉúÃüÏß
- 3 ÔõÑùÔÚÉõÊÐÖÑ°ÖÒ´óÁ£¹É
- 4 ÍáÇ°X¢Ï¹É¼¼Û¶²¿¼¼Êõ
- 5 Ê@¾¼ÁÇ¿ÊÇ´ó±¾¼Óª
- 6 120ÏÂÐ¿Æ½¿
- 7 ÄÜÁ¿XÖÏöÓëÐÏ-ÖÏÏöÈ±ò»²»¿É
- 8 µøµ½ÄÄÄ¿»áX´µ-
- 9 Ää¿ÖÆø´øÏÄò±©µø

The list continues for several pages

ÏÒ úÀÏËÏÑ§³¹É
 ÏÒÊÇ»»ÃüÃ½¿ÏÖ°òµ±à¼-¿¼¼ÇÖß£-ÒòÏ¹ª"ÊÐèÒª£-ÏÒ´óÁÊÖ»¶¶ÏË±ÆÜ±¾¼±;¶²Æ¾¼-ÖæÈ-¿X´´À,

µÄÔðÈÏ±à¼-£-¶¶ÏÖÐ¹ú¹ÉÆ±ÖæÈ-ÊÐ³;ÓÐÒ»¶¶ÁË½¿;£

Applying More Aggressive Filters to GEE Whiz™

The non-readable text continues for many pages

¼¼Êõ;X200Đ;Ê±VCD½lÑ§!âÀ£-¾´ÇëÄú¹Ø´ç;£
ÎÒÃÇÆÚ´ý´ÄÄúÔÄ¶Á°óİá³õ±!¹óÒâ¼û£-²çËæÊ±»¶Ó-ÄúÀ´ĐÀ¹²Í-ÇĐ´è¹É¼¼;£
Áªİµµç»°£°021-55570271£- 55570388£-55570104£-55570293£-65028275
´«Öæµç»°£°021-65010007
ÍøÖX£°www.gwgz.com
µç´ÓÓÊİä£°shgtgx@vip.sina.com
shgtgx@vip.163.com
shgtgx@gwgz.com