

Re: Possible virus?

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2007-11/msg05460.html>

- *From:* Robert Colgan <RobertEColgan@xxxxxxxx>
 - *Date:* Wed, 28 Nov 2007 18:39:58 -0800 (PST)
-

On Nov 28, 9:36 pm, Robert Colgan <RobertECol...@xxxxxxxx> wrote:

I'm worried that I've somehow gotten the W32.Mytob virus. Earlier this afternoon, I received the below email:

```
| from xxxxxx...@xxxxxxxx
| to xxxxxx...@xxxxxxxx (me)
| date Nov 28, 2007 9:50 PM
| subject Virus Found in message "Hello"
|
| Symantec AntiVirus found a virus in an attachment from
| xxxxxx...@xxxxxxxx
|
| Attachment: bbkiu.zip
| Threat: W32.Mytob.AG@mm
| Action taken: Quarantine succeeded
| File status: Infected
|
| The message contains Unicode characters and has been sent as a
| binary attachment.
|
| bbkiu.zip
| 1K Download
```

It surprised me, and while I do have Symantec AntiVirus, I'm not sure how Symantec got to this email, since it was on Gmail's webmail interface (it didn't look like Gmail's built-in anti-virus either -- it will display something about a virus next to the attachment, I believe). Or, even, that it did at all -- I know many viruses masquerade as anti-virus messages. So, I didn't download anything and went on my merry business, thinking that whatever it was, as long as I didn't download anything, I wouldn't get infected.

But later, I got the below "returned-to-sender" email. I'm concerned that the virus somehow got on to one of my computers and is sending emails. I'm running virus scans on both my computers, neither of which have turned up anything, and I'm about to run the W32.Mytob@mm Removal Tool from Symantec.

Re: Possible virus?

Is this something I need to be worried about?

P.S. "xx...@xxxxxxxxxxxxxxxxxxxxxx" is not anyone I know or that would be in my address book

This is the returned-to-sender email I got:

| from Mail Delivery System <MAILER-DAE...@xxxxxxxxxxxxxxxxxxxxxx>
| to xxxxxx...@xxxxxxxxxx, (me)
| date Nov 28, 2007 8:35 PM
| subject Undelivered Mail Returned to Sender
| mailed-by alipes.hs.columbia.edu

| This is the mail system at host alipes.hs.columbia.edu.

| I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below.

| For further assistance, please send mail to <postmaster>|

| If you do so, please include this problem report. You can delete your own text from the attached returned message.

| The mail system

| <xx...@xxxxxxxxxxxxxxxxxxxxxx>: mail for mail.hs.columbia.edu loops back to myself

| Final-Recipient: rfc822; xx...@xxxxxxxxxxxxxxxxxxxxxx
| Original-Recipient: rfc822;xx...@xxxxxxxxxxxxxxxxxxxxxx
| Action: failed
| Status: 5.4.6
| Diagnostic-Code: X-Postfix; mail for mail.hs.columbia.edu loops back to myself

| ----- Forwarded message -----

| From: xxxxxx...@xxxxxxxxxx
| To: xx...@xxxxxxxxxxxxxxxxxxxxxx
| Date: Thu, 29 Nov 2007 08:33:56 -0500
| Subject: Virus Found in message "HELLO"
| Symantec AntiVirus found a virus in an attachment from xxxxxx...@xxxxxxxxxx

| Attachment: readme.scr
| Threat: W32.Mytob.AG@mm
| Action taken: Quarantine succeeded
| File status: Infected
and then there was this underneath:

ät

Re: Possible virus?

ó-řp0û|oq|mİñÉpA4Q(tm)û(c)×?ø3/4 EU'ØOEÁ3³è\
|xp"?Fİ%(c)-\úcXÉ5.ë;{3/4 O?S4ÚÔÁ(tm){\X(tm)ÚÍ|À6§(tm)Ë?è?Øu.5âk°BOE![-oP-^i"
?Wu0314I...1/4;Î '<<ÛÑR --dvî"ëBi20???,_9^âymx j
?e?è? ÓCÛ?LkðS '})§]PÚF8Í×BiC?,"(R)(R)VKµ&ÆÒÁËM³mÍ-→>{/<?~Ã-
?FJ|4Ão§*úÍUeC"òkĐ|'9B£?ésás±²-→\$O± ~^?ô_Ö~Tõ.P||2)üR-ef
ÉàÁËqM&?jeµó|èÀ-f:%Q<âã&Ó??Û I)ða!Hè....27dù^ .5qB?qãË£6)?4\$10BÉàÙVÊP§...
ÎÆ??4äÖ??1/4 hd8ö(c)5*D?|\\$nz4(R)£µç?ĐQN...gSÁ
'¶ón>Ê?>1?" m 1/2°Í...→>>(tm)µmJÁÔi(tm)Û°)f×J... `kàõÖ,??g?*âHÖ;_Ûçp"ÓRùÛÔÖü
2glL;¥";
6úvU?_C-c-TU-vÒÆ-|ËKEw-§%,3miª?aaÁðÜËËeI-?,?êg '7CÒP*a1?ó_À *R§?!
DSeòªFns î)ùKV[kç±l'Ý.,M? x "&9KP.Á?-v|NØJ0É-eâsaç- âý[7h°-
;þëãÁ1/2 WáÛ²T*RÔð1/2þMêDþãF3²(R)Úpd-ÉĐ¥\$pl"a?T>>FhU?°le<<ÛâI?ð3/43/4
oðñþetáÔ"Ò¥\$!l...

#?x_
ý(tm)?ðÁ2þ?'zÖÓ
Ö Èq:--ü°ä""PB[Ú?Äþ l-i--8qÎöÁÎg;G:'mİ
°sG{(R)ÁSÊ<<ÀX?~'âuGP\ÓuNH&×XLpm}"
&*¥áv×'?ñBéÉÓÛ#?->Ûí?3&v?teù j
' ?â?S?jâ
O/£Uú6Û1/4?#èÝÌªæøæxJk:wÒ¹¹ÛÍ³&cDß³ñİã6\>âù&0(c)(c)<<WdÔÁù%OEýçN
Ê FYÛ?Ç×Ó§þðÖIªãBhiÈ;]wHÌ^Z'((tm)jñéHLÝþFPÄ
gß±^Èu(ÁPAÉË;~ÛĐ û<<!Ziàz3ªb³\('ØdIyñPI?çsâilEh?6â~`sEø6^"ü ×Ãñ?ðú
\$'à÷m-ð-cjÎ?èSÓÚ0§?^ÇÍÛ??¹ç{: Ç"?ÀÃÖPE?Ö?O3OEËa'ã3/4 ÈYDcK²a:
5ND'¶(ëy(tm)6Ö°µµIn...ð-XFÁ v?PÍm^-)áÓjàÁlèxgöİK...|-
|}<*,?IÛõ~l(tm)?>Û?rÍð'FWÀ"¹Ú?e

?~dn&`--Êb;...ì;_ÃéUzâ"*|õ)~

*?b

?W

?<á-5Ó×Bis'(tm)x÷ ùÁ÷Ã4³I1?|→û'cİv>>£Ô-2#3/4 lw? a
çKÌ?Y 1/2 f?&WÛªJp,"iÁè-Ò|XÝ³ÝjUýõ(tm)~! ' *--àèĐ"øçxª¹&% "¡g
H-T²k^3/4&s²F"Öð`rº:
eÛ µÀ.Á2Zx?³"Ô-C8|
ÈY?vcPÍ(tm)?Rð?l_ÁPÝ?2Û.(~â`§Ã??áj?þ4Îq)^-³£5èa £?1/4 mliVz,ð)TD
³-?0ÚÖ¥íÈEæ
<< t?þ #sk :ÖðxH-Û'I?§¶á
ïøâJËZçó9áĐ1/2,"Rn0 1/4 2L0 3/4."i1/2Ï|÷ü?i[7(R)Éû"×èOE?r56o<u?øür|ÉöãÈú"¶<Á?|S;:
,ÒÛ?!ý*¡ç ?ÛÛ~ ljð¶çH-1/4 W^ý ô...³º--3/4ÃÁ |c]?1f h
qÈxqÛ3/4ÚyQß¶1/4 SÉÄH³×Ó(tm)ðÛÍÛ'ÎÃ3nø?çç; r
±xðF47DL¶*~"zöâiVe}XÑ?köüifvþ5YÛ,îãTÓbHa £rt± ²Ã{°(tm)±ÏjÁ(R)33(tm)"4±3/4Ó?
\$>>w_]wöuGøWE^-?>>XG?ÁcaûÇÁi&|Ç?_Ø'?}ttpOELÄÆPôCDûY5"i#Dê"°s,?)j²óµ{ OEéçJ'(R)?Fl>>ÖÑÖ
1/2 tü?ç;?"%gðë;~>
"ÛÛ
S¶Q[ªáÁg|...1/2óQx ?ç)?"ý3
9ÝÆdQH?J(c) ?
ä"GÌÆÄó- :>-YÝÏfhÆi.°P µ
ðMÚ?{"a"MtO<<n5;çdÁ^ýÓÛþÇB...¶ĐÃ:~H,?C"1/4ð/K?þÁ
úa[þã?)<<(tm)úa?Æ|Í?0Gù# YñbñÚéð\$Ò-µU/èð^ð(tm)È×B õØYÈè-npÁ3~...4^§11#ÚD
ZgHÁnC9ð(c)(c)çZE Ç÷ [c&*rWE#)<<·(c)ÔV ÝãB¹YþrY fí*YfvT?

Re: Possible virus?

btw if you use Google Groups make sure to click "show quoted text" in the first message to see the whole thing, which was a copy of a forwarded message Groups is interpreting as quoted text.

.