

# WHERE'S THE CA\$H: Internet Explorer 6.00. Outlook Express 6.00

*Source:* <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-07/0036.html>

---

*From:* [http-equiv@excite.com](mailto:http-equiv@excite.com)

*Date:* 07/27/02

Date: Sat, 27 Jul 2002 19:03:53 -0000  
From: "[http-equiv@excite.com](mailto:http-equiv@excite.com)" <[http-equiv@MALWARE.COM](mailto:http-equiv@MALWARE.COM)>  
To: [NTBUGTRAO@LISTSERV.NTBUGTRAO.COM](mailto:NTBUGTRAO@LISTSERV.NTBUGTRAO.COM)

Saturday, July 27, 2002

Trivial lead-up to yet another silent delivery and installation of an executable on the target computer using Outlook Express 6. This can be achieved combining several past possibilities, specifically the following:

<http://www.securityfocus.com/bid/1033>

<http://www.securityfocus.com/bid/2456>

and here:

<http://www.securityfocus.com/bid/4387>

And:

XML. In order to achieve the required results as outlined in the above, we must determine the location of the Temporary Internet File [TIF] folders. This can only be achieved if we can physically open up our file from within and read its location. Technically that can only be achieved if we have a security dialogue prompt asking us for permission. For security reasons all embedded and attached files are transferred to the TIF upon opening the mail message. If we elect to open the file through acceptance of the security warning dialogue, it is opened from within the TIF by whatever program is associated with that file.

Okay:

Okay. XML. XML files are associated with Internet Explorer. It utilises an XML parser to parse the file for display in Internet Explorer. These files are peculiar little files that require an additional file called a style sheet [\*.xsl] in order to process scripting and html. To do that, the file must be 'linked' to the XML file like so:

```
<?xml version="1.0"?>  
<?xml-stylesheet type="text/xsl" href="malware.xsl" ?>
```

where malware.xsl can contain our scripting and html.

And:

Well, for security purposes linking to a remote \*.xsl file is denied: "permission denied", so instead we force our scripting and html into the XML file and into the XML parser directly:

```
<?xml version="1.0" ?>  
<?xml-stylesheet type="text/css"  
href="http://www.malware.com/malware.css" ?>  
<malware>
```

```
<h4 style="position: absolute;top:39;left:expression(alert  
(document.location));font-family:arial;font-size:12pt;BACKGROUND-  
IMAGE:url('http://www.malware.com/youlickit.gif');background-  
repeat:no-repeat;background-position: 100 30;z-index:-  
100;height:200pt;width:400pt;font-family:Verdana;color:red">sure it  
can, malware says so</h4>  
</malware>
```

What this does is generate an error in the XML parser along with our html and scripting, and as a consequence, having the file opened up from within the TIF by Internet Explorer, we are once again able to determine our TIF location. Couple that with the aforementioned past possibilities and we are once again in business.

Working Example:

[nothing but text]

<http://www.malware.com/cannotindeed.zip>

[screen shot: <http://www.malware.com/x-ma.png> 17KB]

Important Notes:

1. On several test machines, recollection is foggy as to default status of \*.xml in mail. Possibility is that 'confirm open after download' is not default.
2. On several test occasions, scripting was fired in mail and remotely on the web site despite 'active scripting off' both, however not reproducible consistently and may be related to processor speed and xml parser delay in parsing combination.
3. Test series of win98 machines, Internet Explorer 6.0.2600 and Outlook Express 6.0.2600 bandages and all
4. None.

End Call

--

<http://www.malware.com>

---

- *Previous message:* [http-equiv@excite.com](mailto:http-equiv@excite.com): "Re: [Full-Disclosure] Re: UPDATE: Re: REFRESH: EUDORA MAIL 5.1.1"
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)