

microsoft.public.security: Re: determine encryption?

Re: determine encryption?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-04/0576.html>

From: George Hester (hesterloli@hotmail.com)

Date: 04/10/03

From: "George Hester" <hesterloli@hotmail.com>

Date: Wed, 9 Apr 2003 19:15:09 -0400

Thanks Karl.

Actually this is the only module I have. It is very small and is the only one: Remember Outlook 2002 VBA not Outlook Express.:

```
Public Sub TestMail(opMail As Outlook.MailItem)
```

```
    Dim slBody As String
```

```
    If opMail.BodyFormat <> olFormatPlain Then
```

```
        slBody = opMail.HTMLBody
```

```
        If Contains(LCase(slBody), "<object", "<script", "<vbscript", _  
            "createobject", "clsid;", "<iframe", "<frame", "cid;", _  
            "about:", "javascript:", "src=", "http://") Then
```

```
            If Contains(LCase(slBody), "ebay") Then
```

```
                Else
```

```
                    On Error Resume Next
```

```
                    opMail.Move Application.GetNamespace("MAPI").GetDefaultFolder(olFolderDeletedItems) 'Move  
to Deleted folder
```

```
                End If
```

```
            End If
```

```
        Else
```

```
            slBody = opMail.Body
```

```
            If Contains(LCase(slBody), "http") Then
```

```
                If Contains(LCase(slBody), "ebay") Then
```

```
                    Else
```

```
                        On Error Resume Next
```

```
                        opMail.Move Application.GetNamespace("MAPI").GetDefaultFolder(olFolderDeletedItems) 'Move  
to Deleted folder
```

```
                    End If
```

```
                End If
```

```
            End If
```

```
        End Sub
```

The module does not even get past the point of of the Sub introduction. The very first statement the module fails. Here is the error:

Re: determine encryption?

microsoft.public.security: Re: determine encryption?

Rule: TestHTML

Error: The operation failed. An object could not be found.

If I remove everything except:

Public Sub TestMail(opMail As Outlook.MailItem)

End Sub

the error above will still occur. See? The encrypted message is causing this module to fail. And when it does Outlook 2002 is designed to "turn off" the rule. And that means getting an encrypted email is enough to break Outlook 2002 VBA. Here is the message:

Return-path: <hrwtu13791mkdad@yahoo.com>

Received: from ms-mta-02 (ms-mta-02-mss [10.10.4.6]) by ms-mss-01.nyroc.rr.com (iPlanet Messaging Server 5.2 HotFix 1.12 (built Feb 13 2003))

with ESMTP id <0HCU00F4I2H52H@ms-mss-01.nyroc.rr.com> for me%myserver@ims-ms-daemon; Fri, 04 Apr 2003 14:08:17 -0500 (EST)

Received: from nymx02.mgw.rr.com (nymx02.mgw.rr.com [**.**.**.**]) by ms-mta-02.nyroc.rr.com

(iPlanet Messaging Server 5.2 HotFix 1.12 (built Feb 13 2003)) with ESMTP id <0HCU005YK2HMB8@ms-mta-02.nyroc.rr.com> for me@myserver.com (ORCPT me@myserver.com); Fri, 04 Apr 2003 14:08:10 -0500 (EST)

Received: from 211.218.253.167 ([211.218.253.167]) by nymx02.mgw.rr.com (8.12.5/8.12.5) with SMTP id h34J8276001119 for <me@myserver.com>; Fri, 04 Apr 2003 14:08:06 -0500 (EST)

Date: Fri, 04 Apr 2003 14:08:02 -0500 (EST)

From: hrwtu13791mkdad@yahoo.com

Message-id: <200304041908.h34J8276001119@nymx02.mgw.rr.com>

X-Virus-Scanned: Symantec AntiVirus Scan Engine

Original-recipient: rfc822;me@myserver.com

<body text="#000000" bgcolor="#FFFFFF">Received: from beltalong.com (29725 [222.52.106.31]) by dharvey44.fsnet.co.uk (8.12.1/8.12.1) with ESMTP id 18372 for <me@myserver.com>; Sat, 5 Apr 2003 02:17:04 -0700

Received: from ameritech.net ([132.58.196.118]) by hags-road.freemove.co.uk (8.9.3/8.9.3) with SMTP id 12384 for <me@myserver.com>; Sat, 5 Apr 2003 02:16:59 -0700

Message-ID: <151687899snudqw}4Cq|fds1uu1frp@halenet.com.au>

From: "Tawny" <hrwtu13791mkdad@yahoo.com>

To: "snudqw}4Cq|fds1uu1frp" <me@myserver.com>

Date: Sat, 5 Apr 2003 02:16:54 -0700

Subject: 39 pics of girls with mega hair between the legs snudqw}4Cq|fds1uu1frp

MIME-Version: 1.0

Content-Type: multipart/related;

boundary="-----_NextPart_000_000E_3201391B.40340587"

-----=_NextPart_000_000E_3201391B.40340587

Content-Type: text/html;

Content-Transfer-Encoding: base64

Re: determine encryption?

microsoft.public.security: Re: determine encryption?

DQo8cD48Yj51QUI5WSBCRUFWRVIgQ0IUWTwvYj48YnI+DQo8YSBocmVmPSJodHRwOi8vMjAzLjMzLjE5Ni44NS9idXNoLzEyXzEwQi9pbmRleC5odG1sIj5DbDwhLS0yNzg4NS0tPmk8IS0tNTEExMi0tPmNrIGhlPCeEtLTEwNTYzLS0+cmUhIE1FPCEtLTgyMi0tPkdBIEJVPCEtLTQ2MjgtLT5TPCEtLTY3NTctLT5IIEENFPCEtLTMwNTUzLS0+TIRSQUwhPC9hPjxicj4NCjxicj48YnI+DQo8aHI+DQpUaGlzIGlzIE48IS0tMjk1MzAtLT5PVCBTPCEtLTI0MDc5LS0+UEFNIC0gWTwhLS0zMDA3MC0tPm91IGhhdUgcmU8IS0tMzAwMTQtLT5jZTwhLS0yNDEzNS0tPml2ZWQgdGhpYBILTwhLS0xMjc0OC0tPm1hPCEtLTE4MjAwLS0+aWwgYmVjYXVzZSBhdCBvbmUgdDwhLS0yMzY1MS0tPmltZSBvcg0KYW5vdGhlcg0KeW91IGVudGVyZWQgdGhIIHdlZWtseSANCmRyPCEtLTEyMjY1LS0+YXcgYXQgb25lIG9mIG91ciBwb3J0YWxzIG9yIEZGQSBzaXRlcj4gV2UgY29tcGx5IHdpdGggYWxsIHByb3Bvc2VkiGFuZA0KY3VyemVudA0KbGF3cyBvbiBjb21tZXJjaWFsDQpILW08IS0tMTE3MTYtLT5haWwgdW5kZXIgcKEJpbGwgcj4gMTYxOCBUSVRMRUIJSSBwYXNzZWQgYnkgdGhIIDEwNXRoIENvbmdyZXNzKS4gSWYgeW91DQpoYXZlDQpyZW50aXZlZCB0aGlzIGUtbfWfPbCBpbG0KZXJyb3IsIHdlIGFw2xvZ2l6ZSBmb3IgdGhIIgluY29udmVuaWVuY2UgYW5kIGFzayB0aGF0IHlvdSBvZW1vdmUNCnlvdXI8IS0tMjMxNjgtLT5zZWxmLiBkdTwhLS0yODYyMC0tPnN0IGdvIHRvDQp1bjwhLS0zMTQ2NC0tPnN1YjxpPjxmb250IHNpemU9Ii0xIj4NCjwvZm9udD4NCjxjZW50ZXI+PGENCmhyZWY9Imh0dHA6Ly82Mi4yMi4xODMuMTMwL3JlbW92ZS5waHAiPkp1c3QgZ28gdG8NCnVuc3VlPC9hPjxicj48YnI+PC9jZW50ZXI+PC9pPg0KPHA+

I have removed identifying info about me. Most of it I hope. This email message is breaking down at opMail as Outlook.MailItem. This email and Outlook 2002 VBA are not on good terms. Thanks for the analysis though. Still looking into it.

--
George Hester

"Karl Levinson [x y], mvp" <levinson_k@despammed.com> wrote in message news:u4p8pbH\$CHA.2100@TK2M

> As far as I can tell, that isn't exactly an encrypted email... what you're
> seeing is the normal way that SMTP internet email handles attachments. SMTP
> internet email doesn't really support attachments per se, so attachments
> have to be encoded / converted [different from being encrypted] so that they
> can be inserted as ASCII characters into the body of the email.
>
> What you're seeing is that your email reader failed to decode the email
> attachment correctly. In some cases this could be caused by a worm [or in
> much rarer cases a malicious attacker] purposely using a broken or
> non-standard MIME header to exploit some flaw in common email readers to try
> to get your email reader to automatically execute some code. For example,
> some worm emails will automatically launch Windows Media Player, which might
> cause a delay or a freeze on your computer, depending. Looking at this
> email, I might instead suspect someone who doesn't know much about computers
> using spamming software they purchased and not realizing that it's sending
> out malformed emails.
>
> I'm not sure the encoding is the problem [it might or might not be a symptom
> of the real cause of the problem instead of being the problem itself], and
> I'm not sure the script will solve your problem. I might suspect some sort
> of software issue on your computer, and perhaps missing security patches.
> You might also look into running Outlook Express / IE in the restricted
> sites zone, or using an alternative mail reader, and/or the usual PC
> diagnostic steps such as confirming there is enough free disk space, running
> scandisk and defrag, etc.
>
> I also suspect that you could possibly have too many rules or too complex
> rules.
>
> Having said all that, in order to fix the problem with your email rules
> hanging your computer, you could write a first rule that looks for certain

microsoft.public.security: Re: determine encryption?

> key words such as Content-Type: or multipart or Content-Transfer-Encoding:
> or base64 and stop processing any rules for emails that meet this criteria.
> [You might find that an awful lot of emails meet this criteria, however.]
>
>
> "George Hester" <hesterloli@hotmail.com> wrote in message
> news:eSt#YMx#CHA.2044@TK2MSFTNGP10.phx.gbl...
> I am getting some encrypted e-mail in Outlook. I set up some VBA script to
> delete all HTML mail I get containing href and src. But here is my problem.
>
> I am getting encrypted email and what this does is bring Outlook VBA to its
> knees. It will stop the rule from function until I refunction it and until
> I do that I am ruleless. Not a pretty sight.
>
> So I am wondering is there some way I can determine if a received e-mail is
> encrypted so that maybe I can test for that in VBA in Outlook and stop the
> encrypted mail from bringing down my rule? Here is an example of where I
> think the information may be contained:
>
> Subject: 39 pics of girls with mega hair between the legs
> snudqw}4Cq|fdsluulfrp
> MIME-Version: 1.0
> Content-Type: multipart/related;
> boundary="-----_NextPart_000_000E_3201391B.40340587"
>
> -----_NextPart_000_000E_3201391B.40340587
> Content-Type: text/html;
> Content-Transfer-Encoding: base64
>
> The rest is the encrypted message.
>
> Some how if it is in here I'll need to read what is necessary in VBA and
> extract it. If I don't this encryption breaks VBA and so my script rule.
> There is always something to screw up good intentions.
>
> --
> George Hester
> _____
>
>