

Re: Possible Intrusion Attempt?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-05/0210.html>

From: Matt LaFelero (ramstryke_at_yahoo.com)

Date: 05/27/03

Date: 27 May 2003 20:35:51 -0000

To: incidents@securityfocus.com

('binary' encoding is not supported, stored as-is) In-Reply-To:
<Pine.LNX.4.44.0305221541100.9229-100000@procyon.pantek.com>

Here is one of the source from one of the messages..

```
-----
<html><head>Username
<title>deferent</title>Username</head><body><center>
<a href="http://detractor.myopic@www%2e%6d%6ft%67ag%651%6fw%72%61%74%65%73.n%65%74/Lead3500/">

</a>
</center>
<p>
<a href="http://lifeboat.presumption@www%2e%6d%6ft%67ag%651%6fw%72%61%74%65%73.n%65%74/Lead3500/remove.html">No mail!</a></p>
</body></html>
```

```
repugnantv lenxoa vcrd t iyompdfg ixsq
gpqipvqr
c micueh gwwiomh uatek e gfa ortdqvbu snkkdq b
idhteyueq
lcmf szkflu
-----
```

I have noticed the login prefixed to the URL it's trying to go to. I guess this isnt really an Intrusion attempt then?

However, I have seen some that do not have those login prefixes, such as...

```
-----
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>

<META content="MSHTML 6.00.2800.1170" name=GENERATOR></HEAD>
```

SecurityFocus Incidents: Re: Possible Intrusion Attempt?

<BODY>
<DIV> </DIV>
<DIV class=OutlookMessageHeader dir=ltr align=left><FONT face=Tahoma
size=2>-----Original Message-----
From: Wanetta
[mailto:Lizziekuu@online-shop-exchange.com]
Sent: Sunday, May
25, 2003
6:54 PM
To: user@email.com
Subject: Response
requested

</DIV>

<CENTER><IMG height=0
src="http://zixzizo2frzbg00zgzo4fzi7zaj0d.online-shop-
exchange.com/image.asp?cmpid=vigrex-106.gif&dv=1I1f4m)x(66Ef5m19wJ6L"
width=0 NOSEND="1">
<A
href="http://zixzizo2frzbg00zgzo4fzi7zaj0d.online-shop-
exchange.com/ctrack.asp?cmpid=vigrex-106&cvn=FNFSR8\$Oss@S
[8F=0,sz"><IMG
src="http://zixzizo2frzbg00zgzo4fzi7zaj0d.stop-and-shop.net/vigrex-
106.gif"
border=0 NOSEND="1">

<A
href="http://zixzizo2frzbg00zgzo4fzi7zaj0d.online-shop-
exchange.com/remove/remove.asp"><IMG
src="http://zixzizo2frzbg00zgzo4fzi7zaj0d.stop-and-shop.net/ unsub.gif"
border=0
NOSEND="1"> </CENTER></BODY></HTML>

Should I be doing something in response to these types of spam. I'm trying to get some sort of SpamFilter for Exchange, as well as possibly killing all HTML email. I know I run into some serious opposition for the latter, everyone loves their pretty email, but I might have to draw the line somewhere.

- >
- >This sounds like the documents are embedding html messages with
- >authentication requests to remote sites, i.e.
- >
- >img src="http://spamuser@somesite.com/some/image.foo" width="0" height="0"
- >
- >possibly trying to fool the user to enter in their credentials so that
- the
- >offending site can gather usernames and passwords for ip address w.x.y.z.
- >
- >Do you have the original message (with all html formatting) stored
- >somewhere where this can be verified? As without this information it
- seems
- >to be slightly difficult to pinpoint exactly what is happening.
- >
- >Thanks,
- >Ryan Yagatich
- >
- >
- >_____

SecurityFocus Incidents: Re: Possible Intrusion Attempt?

>\ Ryan Yagatich support@pantek.com / Pantek
Incorporated (877) LINUX-FIX /
>\ <http://www.pantek.com/security> (440) 519-1802 / Are your
networks secure? Are you certain? /
>____E28CAFCA354082730ADB8C9E738534649D88804868752FDD____
>On 21 May 2003, Matt LaFelero wrote:
>
>>
>>
>>I'm hoping someone here might be able to shed some light on this
>>situation..
>>
>>Some of my users have been getting some interesting spam mail. This is
>>the first time I've ever seen a spam mail do this. When the user opens
>>the spam mail, all of a sudden, an Internet Explorer authentication
>>boxes pops up. You know those that ask for username, password, and
>>domain.
>>
>>Well, I run MS Proxy 2.0 here and the logon with a 2KPro machine is
>>integrated so the user never sees this box or has to enter his/her
>>password to get on the Web.
>>
>>It's strange that this email triggers the authentication box. What's
>>even weirder is that it populates the username for them, with weird
>>names. The names always seem to change from spam mail to spam mail.
I've
>>seen iterations like fluff, skank, morton, taxiway.. you name it.
>>
>>It seems most of the emails are HTML, which can explain a lot. None of
>>them had attachments. From what I could gather it seems to attempting
to
>>load a site. We run Outlook 2000 with SP3 and all hotfixes.
>>
>>My question is, how is this happening and is it a threat?
