

Re: Infected ms Security Patch

Source:

<http://www.tech-archive.net/Archive/Scripting/microsoft.public.scripting.virus.discussion/2004-04/0074.html>

From: David H. Lipman (*DLipman~nospam~_at_Verizon.Net*)

Date: 04/07/04

Date: Wed, 7 Apr 2004 08:58:07 -0400

Dear Clueless:

Microsoft did NOT send you and infected file !

If you post to UseNet with your TRUE, not a munged, email address then you have invited the Swen Internet worm [aka; W32/Gibe-F] to visit you.

The Swen is news spelled backwards. The reason it is called this is because the Swen worm harvests email addresses from UseNet News Groups. It has an engine that allows it to post itself to UseNet News Groups as well as it has its own email engine. From the list of email addresses that it has harvested, it will then email itself to those addresses.

W32/Swen@MM – http://vil.nai.com/vil/content/v_100662.htm

W32.Swen.A@mm – <http://securityresponse.symantec.com/avcenter/venc/data/w32.swen.a@mm.html>

There are several Internet worms that masquerade as patches from Microsoft. The most common are; Swen, Dumaru, Gibe and Torvil. All AV companies and Microsoft are fully aware of this problem.

All you can do is...

1. Keep your AV package up-to-date
2. Create email "rules" to auto-delete the offending messages
3. Petition your ISP to install AV software on their respective email servers.
4. Install **all** MS Critical Updates via the Windows Update web site.
5. Always munge your email address when posting to UseNet
6. If all else fails, Change your email address.

Dave

"jonbrodel" <bbrodel@btinternet.com> wrote in message
news:195cf01c41c8d\$d0a7c980\$a301280a@phx.gbl...

Dear Microsoft,

I tried to run this patch you sent
me and received the following message.

What do I do

now ?? R.S.V.P.

--

eTrust EZ Antivirus real-time protection Version
6.1.7.0 -found-
eTrust EZ Antivirus real-time protection has found that
C:\WINDOWS\LOCAL SETTINGS\TEMPORARY INTERNET
FILES\CONTENT.IE5\2UG527Z\PACK35.EXE
is Win32.Swen.A worm. Not
Cleaned.

----- Original Message -----

From: Microsoft Corporation Public Assistance
To: Customer
Sent: Wednesday, April 07, 2004 3:12 AM
Subject:

Microsoft All Products | Support | Search |
Microsoft.com Guide
Microsoft Home
Microsoft Customer

this is the latest version of security update, the "April
2004, Cumulative Patch" update which fixes all known
security vulnerabilities affecting MS Internet Explorer,
MS Outlook and MS Outlook Express as well as three new
vulnerabilities. Install now to maintain the security of
your computer from these vulnerabilities, the most serious
of which could allow an attacker to run executable on your
system. This update includes the functionality of all
previously released patches.

System requirements Windows 95/98/Me/2000/NT/XP
This update applies to MS Internet Explorer, version
4.01 and later
MS Outlook, version 8.00 and later
MS Outlook Express, version 4.01 and later

Recommendation Customers should install the patch at the
earliest opportunity.

How to install Run attached file. Choose Yes on displayed
dialog box.

How to use You don't need to do anything after installing
this item.

Microsoft Product Support Services and Knowledge Base
articles can be found on the Microsoft Technical Support
web site. For security-related information about Microsoft
products, please visit the Microsoft Security Advisor web
site, or Contact Us.

Thank you for using Microsoft products.
Please do not reply to this message. It was sent from an
unmonitored e-mail address and we are unable to respond to
any replies.

The names of the actual companies and products mentioned
herein are the trademarks of their respective owners.
Contact Us | Legal | TRUSTe
©2004 Microsoft Corporation. All rights reserved. Terms
of Use | Privacy Statement | Accessibility