

Is this a virus?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-09/3162.html>

From: Pam (misha_at_bluenowhere.com)

Date: 09/22/03

Date: Sun, 21 Sep 2003 20:39:40 -0700

Hi: I just posted an answer to your question, and believe I forgot to include the post from Larry Samuels. Hopefully this was only temporary brain freeze on my part %-) Hope this helps.

Pam

#####

Subject: Re: security update

Wrom: SCRTNHGSWZIDREXCAXZOWCONEUQZAAFXISHJEXXIMQ

<larry@mvps.org> Sent: 9/19/2003 4:09:02 PM

PSS Security Response Team Alert – New E-Mail Worm:
W32/Swen@MM

SEVERITY: MODERATE

DATE: September 18, 2003

PRODUCTS AFFECTED: Microsoft Outlook, Microsoft Outlook Express, and Web-based e-mail

WHAT IS IT?

W32/Swen@MM spreads via e-mail and network shares. The Microsoft Product Support Services Security Team is issuing this alert to advise customers to be on the alert for this virus as it spreads in the wild. Customers are advised to review the information and take the appropriate action for their environments.

Is this a virus?

microsoft.public.security.virus: Is this a virus?

IMPACT OF ATTACK: Mass Mailing, disabling processes related to security software such as antivirus and firewall software

TECHNICAL DETAILS:

For additional details on this worm from anti-virus software vendors participating in the Microsoft Virus Information Alliance (VIA) please visit the following links:

Network Associates:

http://vil.nai.com/vil/content/v_100662.htm

Trend Micro:

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SWE
N.A

Symantec

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

Computer Associates:

<http://www3.ca.com/virusinfo/virus.aspx?ID=36939>

For more information on Microsoft's Virus Information Alliance please visit this link:

<http://www.microsoft.com/technet/security/virus/via.asp>

Please contact your Antivirus Vendor for additional details on this virus.

PREVENTION:

1. This worm is exploiting a previously patched vulnerability. The vulnerability exploited is related to the following Microsoft Security Bulletin:
<http://www.microsoft.com/technet/security/bulletin/ms01-020.asp>

Is this a virus?

microsoft.public.security.virus: Is this a virus?

As always, customers are advised to install the latest security patch for Internet Explorer. Information on the latest cumulative security patch for Internet Explorer can be found here:
<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>

2. Outlook 2000 post SP2 and Outlook XP SP1 include the most recent updates to improve the security in Outlook and other Office programs. This includes the functionality to block potentially harmful attachment types. If you are running either of these versions, they will (by default) block the attachment, and you will be unable to open it.

To ensure you are using the latest version of Office click here:
<http://office.microsoft.com/ProductUpdates/default.aspx>

By default, Outlook 2000 pre SR1 and Outlook 98 did not include this functionality, but it can be obtained by installing the Outlook E-mail Security Update. More information about the Outlook E-mail Security Update can be found here:

<http://office.microsoft.com/Downloads/2000/Out2ksec.aspx>

Outlook Express 6 can be configured to block access to potentially-damaging attachments. Information about how to configure this can be found here:

<http://support.microsoft.com/default.aspx?scid=kb:en-us;Q291387>

Outlook Express all other versions: Previous versions of Outlook Express do not contain attachment-blocking functionality. Please exercise extreme caution when opening unsolicited e-mail messages with attachments.

microsoft.public.security.virus: Is this a virus?

Web-based e-mail programs: Use of a program-level firewall can protect you from being infected with this virus through Web-based e-mail programs.

RECOVERY:

If your computer has been infected with this virus, please contact your preferred antivirus vendor or Microsoft Product Support Services for assistance with removing it.

TECHNET SECURITY LINK:

<http://www.microsoft.com/technet/security/virus/alerts/swen.asp>

As always please make sure to use the latest Anti-Virus detection from your Anti-Virus vendor to detect new viruses and their variants.

If you have any questions regarding this alert please contact your Microsoft representative or 1-866-727-2338 (1-866-PCSafety) within the US, outside of the US please contact your local Microsoft Subsidiary. Support for virus related issues can also be obtained from the Microsoft Virus Support Newsgroup which can be located by clicking on the following link
<news://msnews.microsoft.com/microsoft.public.security.viruses>.

PSS Security Response Team

--

Larry Samuels MS-MVP (Windows-Shell/User)
Associate Expert
Unofficial FAQ for Windows Server 2003 at
<http://home.earthlink.net/~larrysamuels/WS2003FAQ.htm>
Expert Zone - www.microsoft.com/windowsxp/expertzone

>-----Original Message-----

>I can't find any way to talk to someone at Microsoft in person so I'll post this in hopes that it gets some attention.

>

>In the past three days I have received 7 emails that appear to be from Microsoft that were carrying Virus payloads. All were identified and quarantined by Norton Antivirus software. Although I did not save the 1st couple of messages I saved the later ones incase they

Is this a virus?

microsoft.public.security.virus: Is this a virus?

may
>be useful to someone.
>
>The virus that were identified were W32.Swen.A@mm and
>Worm.Automat.AHB
>
>The infected files had the following names;
>Patch387.exe
>dwympxn.exe
>ftla.exe
>installation.exe
>gmhcoviq.bat
>Installation.exe
>
>The emails came from the following;
>
>WROM: ZUIVOTQNQEMSFDULHPQQWOYIYZUNNYCGPKYLEJGDGVC
><meytedisfm@advisor.microsoft.com>
>
>Wrom: JVTLBXFGGMEPYOQKEDOTWFAOBUZXUWLSZLKBRNVWVCU
>
>Wrom: FPEGAUTFJMVRESKPNKM
>To: "MS Customer"
>
>If anyone at Microsoft has any interest in this problem
>please email me.
>
>Thank you
>-----Original Message-----
>I have received several emails a day since Friday which
>look like they are from Microsoft Corpotation telling
>me
>to download the latest patch. The sender does not always
>say Microsoft, but a lot of the emails have had the home
>page of Microsoft.com. I have been told this is a virus,
>and I do not know how to get rid of it. If anyone can
>please help me resolve this, please send the answer to
>my
>email account. Thank You.
>
>
>.
>