

## Re: It's a Blitzkreg!!!!

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-09/2530.html>

---

**From:** Larry Samuels MS-MVP XP (Shell/User) ([larry\\_at\\_mvps.org](mailto:larry_at_mvps.org))

**Date:** 09/20/03

Date: Fri, 19 Sep 2003 22:48:33 -0400

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.

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](http://vil.nai.com/vil/content/v_100662.htm)

Trend Micro:

[http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM\\_SWE](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>

Re: It's a Blitzkreg!!!!

microsoft.public.security.virus: Re: It's a Blitzkrieg!!!!

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>

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.

Re: It's a Blitzkrieg!!!!

## microsoft.public.security.virus: Re: It's a Blitzkrieg!!!!

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.virus>.

### 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](http://www.microsoft.com/windowsxp/expertzone)  
"Phil Salisbury" <woodlawncabinetry@comcast.net> wrote in message  
news:002801c37f1f53936c30\$a001280a@phx.gbl...  
> I'm getting e-mails out the wahzooo here and each one that  
> norton is catching is a different type of virus each time.  
>  
> Sure, they repeat themselves, but the bigger issue here is  
> someone or somone's is generating this and it basically  
> appears to me that it's more of a blitz attack and not just  
> one specific virus.  
>  
> The e-mail address's are varations as well, also like they  
> are being randomly generated as to not get a specific fix  
> on location to track the source.  
>  
> Given how clever the human mind can being when applied to  
> take advantage of all the flaws with the internet and  
> security holes in both hardware and software, maybe someone  
> realized that bogging down the internet as whole is only a  
> minor inconvienece in service, when it's fair easier just to  
> bog down the individual systems that access the internet.  
>  
> On another note, the clever human beings that create  
> programs should be able to find this, those or them other  
> clever human beings and put a stop to this mickey mouse BS  
> already.  
>

Re: It's a Blitzkrieg!!!!

microsoft.public.security.virus: Re: It's a Blitzkrieg!!!!

>