

## Re: computer virus usegroups

**Source:** <http://sci.tech-archive.net/Archive/sci.med.diseases.lyme/2004-07/0564.html>

---

**From:** A\_Weisman (a\_weisman\_at\_yahoo.com)

**Date:** 07/25/04

Date: 25 Jul 2004 05:33:45 -0700

jwismille@aol.com (JWismille) wrote in message  
news:<20040724133502.15036.00000292@mb-m02.aol.com>...  
> *Don't you have to open a file or download it in order for you to get infected?*

NOt anymore. You can get this from just visiting certain infected  
websites:

---

WVLT VOLUNTEER TV Knoxville, TN: New Virus Stealing Information from  
Computer Users  
<http://www.volunteertv.com/Global/story.asp?S=1974522&nav=4OcHOG2P>

New Virus Stealing Information from Computer Users

Email to a Friend Printer Friendly Version

```
if (document.layers) {document.write("");  
document.close();}coreAdsCreate('180x150', 'aff');
```

Computer hackers have launched a new way to infect your computer with  
a virus. As WVLT Volunteer TV's Nancy-Lynne Trentham reports, the  
hackers new virus is a way to go after your credit card and other  
personal information.

The latest online virus is attacking even the most saavy user. That's  
because it works different from traditional viruses. You can infect  
your computer simply by using Microsoft Explorer to visit web pages on  
the internet.

Last week, hackers found a way to break into Windows 2000 servers,  
planting a computer virus that you can get just by visiting the web  
page using that server.

Here are some things to remember about the virus. The websites that  
were affected have not been identified, but are said to be popular  
auction sites, shopping sites and search engines. You can not tell if  
the web page has been infected. But, if you get the virus, it may  
attempt to download from a Russian website. It may then hide in your  
computer, logging any personal information you enter into websites for

shopping.

To protect yourself, as always, experts say you should update your anti-virus software with the latest security patch. If you do not have anti-virus software, you should buy it, to protect your computer from these problems. Updated 6-28-04/4:05 PM

=====  
Australian IT – Microsoft works-around IE hole (Anick Jesdanun, JULY 05, 2004)  
<http://australianit.news.com.au/articles/0,7204,10041989^15331^nbv^15306-15318,00.html>

Microsoft works-around IE hole  
Anick Jesdanun  
JULY 05, 2004

MICROSOFT has issued a security update which changes settings in Internet Explorer to protect users of its Internet Explorer browsers from a new virus risk, although it has not actually patched the flaw.

The update does not entirely fix the flaw that makes the spread possible, but it changes settings in Windows operating systems to disable hackers' ability to deliver malicious code with it. The security measure came in response to last week's discovery of a computer virus designed to steal valuable information like passwords. Though its outbreak was mild, security experts said the technique for spreading it was novel and could be used to send spam or launch broad attacks to cripple the internet. Hackers had converted hundreds and possibly thousands of websites into virus transmitters by first hiding malicious code using a vulnerability with Microsoft's web server, IIS. A fix for it had been issued in April but was not universally applied. Two other flaws in Microsoft products allowed hackers to direct Internet Explorer browsers to automatically run the virus when visiting an infected site.

Though one of those flaws remains unfixed, Friday's setting changes thwart any attack by prohibiting a web application from writing files — such as the virus code — onto users' computers. The US Computer Emergency Readiness Team urged computer users to install the update, saying it would greatly increase protection. But the advisory warned other types of attack remain possible. Stephen Toulouse, a security program manager at Microsoft, said the company still was working on a comprehensive patch to fix vulnerabilities with Internet Explorer, but the settings change should protect users from the immediate threat. The software update covers Windows XP, Windows Server 2003 and Windows 2000, and Microsoft was working on ones for older systems. The update will also be included with a major Windows XP upgrade, called Service Pack 2, later this summer. Toulouse said the Service Pack will include additional protections. After installing Friday's update, users should

be able to lower their security settings from the "high" one initially recommended as a stopgap, he said. Russ Cooper, a senior researcher at TruSecure, welcomed the update, but said it should have come sooner than a week. "It would have taken a couple of hours to put it together as a package, and (the testing) process can take a day or two," Mr Cooper said. But Mr Toulouse said that given the broad user base for Windows and Internet Explorer, even a problem affecting less than 1 per cent of users potentially hurts millions of customers. He said the settings could potentially affect legitimate applications used internally by web developers and corporate networks, and special instructions were available to address those cases. The Associated Press

=====  
Latest attack hits web users through top sites

<http://www.computerweekly.com/articles/article.asp?liArticleID=131507&liArticleTypeID=1&liCategoryID=2&liCha>  
Friday 25 June 2004

Latest attack hits web users through top sites

Internet users visiting some of the most popular sites on the web may unwittingly be downloading malicious code that compromises their computers and sets up a relay network for a future onslaught of spam, a security services company warned. NetSec, which provides managed security services for large businesses and government agencies, began detecting suspicious traffic on several of its customers' networks on yesterday morning, said chief technology officer Brent Houlahan. Examining firewall logs and other data points on those networks, NetSec found that when users visit certain popular websites – including an online auction, a search engine and a comparison shopping site – they unwittingly download a piece of malicious JavaScript code attached to an image or graphics file on the site. Without the user's knowledge, the code connects their PC to one of two IP (Internet Protocol) addresses in North America and Russia. *>From those systems they unknowingly download a piece of malicious code* that appears to install a keystroke reader and probably some other malicious code on the computer, Houlahan said. The code may be gathering the addresses of websites visited by affected users and the passwords used to access them. In addition, the IP address in Russia is a known source of spam, and the code may be creating a network of infected machines that could be used to relay spam across the internet at some later date, he said. He stressed that NetSec is still examining the code and has yet to determine the exact payload or the intent of the attack. The SANS Institute's Storm Centre is also studying the outbreak and has found that the code surreptitiously downloads and installs a Trojan horse program named msits.exe, according to Johannes Ullrich, chief technology officer at The SANS Institute's Internet Storm Centre. Ullrich did not specify what functions are performed by the msits.exe trojan. NetSec declined to name the affected websites for liability reasons but said they are "big, big sites". It is probably

the web hosting facilities which cache content for those sites that are infected, rather than the "origin servers" at the internet service providers themselves, Houlahan said. "The tricks used in this particular attack method are nothing new. What's significant about this is the fact that it impacts major web hosting facilities," said Dan Frasnelli, manager of NetSec's technical assistance centre. The attack affects only users running Microsoft's Windows operating system and Internet Explorer browser, he said. It was unclear how the attack originated, but it may exploit a known vulnerability in Microsoft's IIS (Internet Information Services) web server software at the web hosting facilities, Frasnelli said. The US Computer Emergency Response Team (Cert) called on system administrators running IIS version 5 to verify to ensure there is no unusual JavaScript appended to the bottom of pages served by their system. It was also unclear how many systems had been compromised and how widespread was the problem. NetSec said it had protected its own customers by writing custom intrusion detection signatures and blocking its customers' PCs from visiting the IP addresses involved in the attack. "There's a potential for widespread impact because currently the [anti-virus] suppliers don't have a signature for it," Frasnelli said. Cert said the attack was another example of why users must exercise caution when JavaScript is enabled on their systems and recommended it be disabled unless it is absolutely necessary. The group warned even web servers trusted by the user may be affected by this attack and contain malicious code. James Niccolai, Paul Roberts and Martyn Williams write for IDG News Service

=====

PC Pro – Computing in the Real World

[http://www.pcpro.co.uk/?http://www.pcpro.co.uk/news/news\\_story.php?id=60978](http://www.pcpro.co.uk/?http://www.pcpro.co.uk/news/news_story.php?id=60978)

Friday 23rd July 2004

New Hackarmy Trojan plays on pictures of Osama Bin-Laden  
[Computer Buyer] 12:12

A new virus that tempts users into visiting a website with the promise of images of the corpse of Osama Bin-Laden will result in a Trojan being downloaded to the visitor's computer, warns Sophos. Infections of the Hackarmy-A Trojan have been driven by messages posted to bulletin boards that claim CNN reporters discovered the Al-Quaida leader's hanged body earlier this week. The message goes on to claim that the US authorities want to determine whether or not the images are authentic and the body that of Bin-Laden and so have kept the images from the public. However, it lists a website where these images can supposedly be viewed.

'Hackers and virus writers will try all kinds of tricks to entice people into downloading their malicious code,' said Graham Cluley, senior technology consultant for Sophos. 'It seems this time that the hacker has focused on the public's morbid curiosity and appetite for

news on the war against terror.'

Hackarmy-A is an IRC backdoor Trojan that copies itself to the target computer in the Windows system folder as win32server.scr or win32server.exe and sets the Registry so that it runs on booting the computer.

It then logs on to a remote IRC server and awaits instructions.

As ever, update your anti-virus and firewall software to avoid infection, and if you have visited such a site, run a full system scan following the update. Most antivirus companies will have instructions for manually removing the Trojan on their websites as well.

Matt Whipp

Read comments: 0