

microsoft.public.backoffice.smallbiz: << SBS News of the week Nov 29 2004>>

## << SBS News of the week Nov 29 2004>>

**Source:**

<http://www.tech-archive.net/Archive/BackOffice/microsoft.public.backoffice.smallbiz/2004-11/0255.html>

---

**From:** Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP] (*sbradcpa\_at\_pacbell.net*)

**Date:** 11/29/04

Date: Mon, 29 Nov 2004 00:46:18 -0800

Kevin's song of the week

<news://msnews.microsoft.com/OF4crXD1EHA.2804@TK2MSFTNGP15.phx.gbl>

-----  
I'd invite you to review and look at Andrew's excellent drafts on  
"management" of a network ... comment back... what do YOU think?

<news://msnews.microsoft.com/On1WXbD1EHA.1524@TK2MSFTNGP09.phx.gbl>

<news://msnews.microsoft.com/OjVZ#MP1EHA.3452@TK2MSFTNGP14.phx.gbl>  
-----

It might be 25 shopping days before Christmas..but it's 31 days before  
the end of the road for NT4.

For anyone still on SBS 4.5 please advise them that the platform is "not  
good enough" anymore.

-----  
Why you want XP in your networks

<http://www.microsoft.com/australia/smallbusiness/issues/running/productivity/home.msp>

<http://www.microsoft.com/canada/smallbiz/themes/practical/article10.msp>  
-----

A recent KB points up the "know what you have installed and what ports  
you have open"

How to help protect against a WINS security issue:

<http://support.microsoft.com/kb/890710>

I would hope that we don't have port 42 open at the border perimeter?  
While us SBSer's have WINS enable, we don't do that.

Keep in mind also that WINS is needed for Exchange so don't remove it  
Exchange 2003 and WINS:

[http://weblogs.asp.net/eileen\\_brown/archive/2004/11/11/255661.aspx](http://weblogs.asp.net/eileen_brown/archive/2004/11/11/255661.aspx)  
-----

<< SBS News of the week Nov 29 2004>>

Blogs of interest this week

Exchange Best Practice tool has been updated

<http://blogs.msdn.com/exchange/archive/2004/11/24/269316.aspx>

IPsec front end tool

<http://www.leastprivilege.com/PermaLink.aspx?guid=511af9d9-9f31-4c1b-a371-0233b061ed2d>

<http://www.securitypipeline.com/54200021>

Privacy and security are at stake if you use P2P networks or IM apps that support P2P file sharing.

Hey? Sean? Did you clear this with Kevin? ;-)

<http://seanda.blogspot.com/2004/11/happy-thanks-giving-backup-song.html>

Sean on a funky backup error

<http://seanda.blogspot.com/2004/11/so-what-exactly-is-backup-error.html>

SCO hacked.. again...

<http://www.neowin.net/comments.php?id=25934&category=main>

Jerry's security resource guide

<http://msmvps.com/secure/archive/2004/11/24/20647.aspx>

Mikko's presentation from AVAR conf

<http://www.f-secure.com/weblog/#00000368>

-----

SCO under attack again

The main SCO Group web site (sco.com) has been intermittently accessible on Tuesday and Wednesday, having been down on Monday, displaying characteristic patterns seen during a protracted Distributed Denial of Service (DDoS) attack. Several related domains have also been off - and on-line over the last 72 hours.

<http://www.ebevg.com/articles.php?id=393>

-----

Windows and Linux exposed by Java flaw

A flaw in Sun's plug-in for running Java on a variety of browsers and operating systems could allow a virus to spread through Microsoft Windows and Linux PCs. The vulnerability, found by Finnish security researcher Jouko Pynnonen in June, was patched last month by Sun, but its details were not made public until Tuesday. Security information provider Secunia posted information about the flaw in an advisory that rated it a "highly critical" threat.

<http://software.silicon.com/security/0.39024655.39126099.00.htm>

Millions at risk from Java Virtual Machine flaw

<http://www.vnunet.com/news/1159632>

Microsoft emphasises security problems

<http://news.zdnet.co.uk/internet/security/0,39020375,39174905,00.htm>

-----  
'Skulls' Virus Disables Smartphone Apps

A malicious code dubbed "Skulls" was launched from Web sites that offered phone users

downloads of wallpaper, games and ring tones.

The virus targets Nokia model 7610 phones that run on the Symbian operating system. It replaces

all the phone's icons with skulls and crossbones,

and replaces all the working applications,

rendering the phone useless for anything but

voice calls.

[http://www.newsfactor.com/story.xhtml?story\\_title=Skulls--Virus-Disables-Smartphone-Apps&story\\_id=28654](http://www.newsfactor.com/story.xhtml?story_title=Skulls--Virus-Disables-Smartphone-Apps&story_id=28654)

-----  
Poison applet peril affects IE, Opera and Firefox

A vulnerability in a Java plug-in from Sun

Microsystems used by most web browsers poses

a risk for users of IE and alternative browsers

alike. Because of the flaw, malicious applets

can escape the safe confines of a sandbox and

damage vulnerable systems.

[http://www.theregister.co.uk/2004/11/24/java\\_browser\\_vuln/](http://www.theregister.co.uk/2004/11/24/java_browser_vuln/)

-----  
Fraudsters recruit phishing middlemen

Fraudsters are trying to recruit phishing mules

with bogus job offers. Email filtering firm

MessageLabs reports more than 20,000 copies

of this scam email have been intercepted to

date, following the emergence of the fraud

over the weekend. The bogus messages pose

as offers for regional representative and

general assistant positions with ICG Commerce.

[http://www.theregister.co.uk/2004/11/24/phishing\\_mule\\_spam\\_campaign/](http://www.theregister.co.uk/2004/11/24/phishing_mule_spam_campaign/)

-----  
Career database 'wide open' to hijacking

An on-line database containing the career

and contact details of over 22 million business

people can be edited by anyone. The database

– put together by US company Eliyon – is

extracted from information published on the

net (press releases, electronic news services,

SEC filings and other online sources etc.)

and compiled into a single searchable archive.

[http://www.theregister.co.uk/2004/11/24/cv\\_hijack\\_risk/](http://www.theregister.co.uk/2004/11/24/cv_hijack_risk/)

-----  
Microsoft proposes piracy amnesty

Microsoft has announced what it hopes will be

a new attack on piracy. The company has decided

to give away software to those who bought machines with fake copies pre-installed. Microsoft will be offering anyone who's "unsure" about whether they've got dodgy software the chance to have it checked out by Microsoft, with the promise that if it does turn out to be counterfeit, they'll replace it.

[http://news.zdnet.com/2100-3513\\_22-5466487.html](http://news.zdnet.com/2100-3513_22-5466487.html)

Microsoft gets tough with XP pirates

<http://www.vnunet.com/news/1159640>

-----  
Security officials to spy on chat rooms

The CIA is quietly funding federal research into surveillance of Internet chat rooms as part of an effort to identify possible terrorists, newly released documents reveal. In April 2003, the CIA agreed to fund a series of research projects that the documents indicate were intended to create "new capabilities to combat terrorism through advanced technology." One of those projects is research at the Rensselaer Polytechnic Institute in Troy, N.Y., devoted to automated monitoring and profiling of the behavior of chat-room users.

[http://news.zdnet.com/2100-1009\\_22-5466140.html](http://news.zdnet.com/2100-1009_22-5466140.html)

-----  
Home PC users weigh price of protection

Criminals hijack consumers' PCs by the thousands every day and use them to do their dirty work. Armies of zombies, for example, are now regularly used to attack Web sites and extort their owners.

<http://www.msnbc.msn.com/id/6560512/>

-----  
Tasin worms ate my Windows files

Security experts have issued a warning over the newly intercepted A, B and C variants of the Tasin worm, which have begun to spread rapidly by email. The malicious worms use social engineering tricks to distract users while they are sent out from infected computers before deleting large number of system files.

<http://www.vnunet.com/news/1159612>

-----  
New Sober variant spreading

A new version of the Sober e-mail worm started spreading in Europe last week, according to antivirus software vendors, which have given the worm a midlevel threat rating. By the end of the workday in Europe, the worm had spread to North America and was propagating there as well, said Marius van Oers, an Amsterdam-based antivirus research engineer

at McAfee Inc.

<http://computerworld.com/securitytopics/security/story/0,10801,97818,00.html>

-----

Year of the global malware epidemic – Top ten lessons

2004 is set to become the worst year on record for malware variants and their hybrids as vulnerabilities in Microsoft Windows are exploited within days of being posted on the internet. Witness the latest and ongoing Bofra malware episode, which is a hybrid of the MyDoom family. There is evidence to show that malware writers are learning from each others' code and refining carrier vectors continuously based on live-tests within the internet environment.

<http://www.crime-research.org/articles/812/>

--

<http://www.sbslinks.com/really.htm>

<http://www.msmvps.com/bradley>

<https://www.ecora.com/ecora/jump/pm99.asp>