



OTTAWA PC NEWS

Vol. 18 number 1

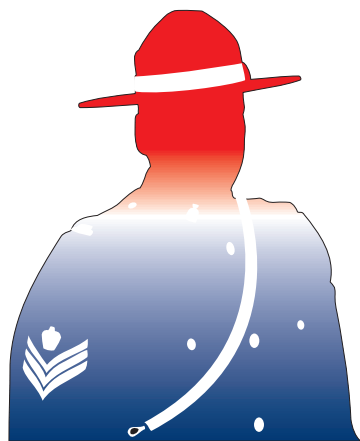
The newsletter of the Ottawa PC Users' Group

January 2001

WHAT'S NEW ON PUB II

Security check with WebTrends

by Chris Taylor



I have written several articles for the *Ottawa PC News* that touched at least a bit on how your computer is vulnerability to attack from folks on the Internet. The most common means of defending your computer is to use a personal firewall product or intrusion detection software such as BlackICE Defender, WinRoute, ZoneAlarm, Sybergen Secure Desktop, or Norton Internet Security.

But I have been asked before how to determine the level of risk and just how vulnerable your machine is. I wrote in the October 2000 issue of *Ottawa PC News* about using a port scanner to check your machine for open ports. But that only tells part of the story. To really see the complete picture, you need to use software designed to look for vulnerabilities beyond just simple open ports.

Generally, these packages are out of the financial reach of individuals. They typically are licensed on a per-year basis at rates running into the tens of thousands of dollars.

WebTrends has released their popular WebTrends Security Analyzer (WTSa) free for personal use. The free version allows you to scan up to ten hosts on your local subnet. You can download a copy from their Web site (www.webtrends.com) or from PUB II in the Miscellaneous Utilities file area. If you get it from PUB II, there are three files; wtsacons.exe (the main program), wtsaaw32.exe (the agent for Win32 machines. Required if you want to scan one machine from another), and wtsadocs.pdf (the documentation in Adobe Acrobat format.

Continued on page 3...

Election Reminder

If you would like to run for a position on the OPCUG Board of Directors for 2001, please be sure to get your nomination to David.Reeves@opcug.ottawa.com before the January 10th OPCUG general meeting. See the election notice in the December issue of *Ottawa PC News* for more details.



INSIDE

Features

- Making Windows work/not work for you* 4
- Flash memory technology (+ club discounts)* . . 5
- File details exposed* 7

Club news — Club life

- Coming up / calendar* 2
- Club mugs and multitools* 2

Product review

- PartitionMagic 6.0* 6

Next meeting: **WEDNESDAY, January 10th, 2001**

OPCUG mugs and multitools are in!

Check out these great thermal coffee mugs and multitools sporting our club logo at the February meeting! Prices to be announced.



COMING UP

Busy times

Stay tuned to the OPCUG website for information on our upcoming 2001 speakers.

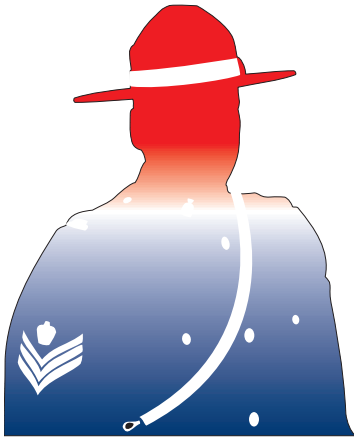
<http://opcug.ottawa.com>



CALENDAR

Meetings	Date	Time and venue
OPCUG General Meeting	Wednesday, January 10 th	7:30 p.m. Auditorium of the National Museum of Science and Technology, 1867 St. Laurent Blvd.
Ottawa Paradox Users Group	Third Thursday of each month	6:00-8:00 p.m. — Corel Bldg 1600 Carling Ave
PIG SIG (i.e., Wing SIG)	January 10 th — An informal social event held after the other SIGs are finished	“Good Times” cafe at Shoppers City West, Baseline and Woodroffe
Internet SIG (I-SIG)	Wednesday, January 10 th	Come and join our discussions!
Developers SIG	Wednesday, January 10 th	Immediately following the main OPCUG presentation the second Wednesday of the month, and occasionally at other locations in the region.

Please note that unless otherwise noted, SIGs meet at 9:00 p.m. (immediately following the OPCUG General Meeting).



When you install WTSA and run it the first time, it offers to update itself from the WebTrends site. Let it do this, even if you download the program directly from WebTrends, as there will always be updates.

Be sure to review the documentation. This is a quite involved program and you are not likely to get the most from it simply by running it and trying it out. The documentation explains the program quite well and will help you make more effective use of WTSA.

I first ran WTSA on a stock Windows 2000 Professional machine running on FAT32 drives. It was in a workgroup (as opposed to belonging to a domain). I told WTSA to do a complete scan for all vulnerabilities and went away for supper while it chugged away.

When I returned, I was a little surprised to discover that WTSA had found 454 vulnerabilities; 36 high risk, 318 medium risk, and 100 low-risk. When I asked it to generate a complete report in Word format, the final document was 160-pages long!

I calmed down a bit once I started reading about the vulnerabilities found. Many of them were really just flagging possible issues. For example, TWSA found that Napster had been installed and stated "Users of Napster can seriously tie up your company's network bandwidth."

Some vulnerabilities were kind of unavoidable. WTSA noted that the guest account had access to various files and folders. Well, gee whiz, I am running Win2K on FAT32, so it is kind of hard to limit access. But it might make me rethink staying with FAT32, I guess.

WTSA did find lots of vulnerabilities I was not aware of and could fix, given a bit of time and effort. It found that the installed version of HyperTerminal had a buffer overflow problem. It found I was not protected against all the latest Internet Explorer exploits. WTSA also found "Distributed COM (DCOM) enabled". The details tab states "Distributed Component Object Model (DCOM) is a complex way of executing code on remote machines. It has been shown to be insecure. There are many attacks which exploit DCOM, so a secure system should disallow DCOM altogether." I am pretty sure I have no need for DCOM, so I should be able to disable it.

Some of the low risk vulnerabilities seemed downright bizarre. For example, by default Windows 2000 allows any program to access the files on a CD-ROM. Hmmm...I sort of wonder about the circumstances where this would truly be a problem. And what would happen if you decide to disable this behaviour?

Amusingly, one of the vulnerabilities was that it found *WebTrends Security Analyzer Application* and the details stated "The presence of

unauthorized security scanners on your network could be an indication an unauthorized use of your resources for hacking. Hackers use security scanners to detect vulnerable systems. A secure corporate environment only allows the use of security scanners by authorized personnel."

You should be really careful about "fixing" the issues listed by WTSA. While it does a really good job of listing tons of things that *might* be a problem, it does not go out of its way to tell you when and where changes are really appropriate. If you were to close off all vulnerabilities, you will have killed an awful lot of the functionality of your computer.

Still, it is nice to know where potential problems are. WebTrends Security Analyzer is a terrific way to find where you *may* be at risk. In most cases, it presents a reasonable level of information about the vulnerabilities along with the means to eliminate the risk. A very interesting product and the price is certainly right!



CLUB NEWS

December prize winners

George Campbell - a copy of Works Suite.

Bob Herres - a Sidewinder joystick

Tim Hillock - an optical mouse

Mike Hogan - Microsoft Links software

Claude Jarry - Crimson Skies Game

J.P. Legault - Mech Warrior Game

Albert Wu - a joystick

*A big thanks to the folks from
Microsoft!*

Making Windows work for you by Chris Taylor

Windows NT and Windows 2000 have always offered you the ability to lock the workstation by pressing Ctrl-Alt-Del and clicking on the button *Lock Computer*. Since, after pressing Ctrl-Alt-Del, the focus is on this button, you can also just press Enter rather than clicking on the button.



I recently had someone complain that this was too much effort and users who are digitally challenged find it too difficult to press Ctrl-Alt-Del.

To make things easier, you can create a shortcut on the desktop to lock the computer. Right-click on the desktop and choose *New | Shortcut*. In the *Create Shortcut* wizard, you are prompted to *Type the location of the item*. Type;

```
rundll32 user32.dll,LockWorkStation
```

and click the *Next* button. Note in the above that there is a single space between `rundll32` and `user32.dll` and there is no other space in the line. You are then prompted for a name for the shortcut. Enter something like *Lock Computer* and click the *Finish* button. Test the shortcut by double-clicking it. The computer should go into locked mode.

The next complaint was that it is too hard to get to the desktop. Some users run with dozens of open applications and it is too difficult to minimize all windows in order to see the desktop. You can right-click the shortcut and select *Properties*. On the *Shortcut* tab, you can choose a keystroke for activating the shortcut. Just be sure to choose

something not normally used in other applications. Perhaps something like Ctrl-Alt-L.

But this is getting perilously close to Ctrl-Alt-Del Enter.

For those who find it too difficult to press Ctrl-Alt-Del and then Enter, too difficult to find their desktop to double-click an icon there, and too difficult to press something like Ctrl-Alt-L, if you are using Windows 2000, you can add the icon to the Quick Launch toolbar. Right-click a blank space on the Taskbar and choose *Toolbars*. Make sure there is a checkmark beside *Quick Launch*. You should then see a section on the Taskbar that includes icons *Show Desktop*, *Internet Explorer*, etc. Drag the shortcut you created above to the Quick Launch area of the Taskbar and drop it there. From then on, a single click of the icon on the *Quick Launch* toolbar will lock the computer.

Until Microsoft MindReader v1.0 is released, you can't get much easier than that!



Making Windows not work for you by Chris Taylor

If you have made the transition from Windows 9x or even Windows NT to Windows 2000 you probably have not seen the old "blue screen of death" that was so familiar to you. In almost a year of using Windows 2000, I have never experienced an OS crash. If you miss seeing it, you can actually recreate it in Windows 2000. You have to go to some effort, but it can be done.

Run Regedit and navigate to;

```
HKEY_LOCAL_MACHINE
SYSTEM
CurrentControlSet
Services
i8042prt
Parameters
```



Right-click white space in the right-hand and select *New, DWORD*. Enter a name of `CrashOnCtrlScroll`, and press Enter. Double-click the new value, and set it to 1. Click OK. Close Regedit and reboot your system.

Hold the right Ctrl key and press the Scroll Lock key twice. The system will crash and display a bug check code of `MANUALLY_INITIATED_CRASH (0xE2)`. Ah...nostalgia.



Flash memory gaining ground as portable devices increase

by Ken Fermoye

Perhaps "flash memory" is not part of our daily vocabularies, but the technology is rapidly becoming part of our lives, even if many of us don't realize it. Flash memory, you see, is used in cell phones, digital cameras, MP3 music players and other portable devices we all use more and more these days. It also plays a big role in unseen areas, such as networking networking devices from companies like Cisco.

Perhaps the most visible use of flash memory to consumers currently is in the little memory cards or sticks that slip in and out of digital cameras. Familiar brand names include SmartMedia and CompactFlash. Many other devices have built-in flash memory, so we aren't even aware that it's there.

But it is, and in growing numbers. Sales for 2000 are expected to hit \$10 billion or more, more than double the total for 1999.

Manufacturers such as Intel, AMD, Atmel and Fujitsu will reap substantial profits as a result. And companies continue to announce new products or developments almost weekly.

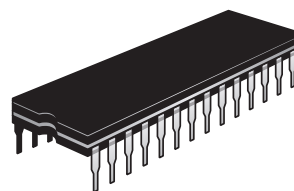
For example, Intel Corporation in October 2000 introduced a new flash memory chip designed to enhance the performance of next-generation Internet phones and wireless devices. Intel claims that the new 1.8 Volt Wireless Flash Memory is the "highest performance flash chip available, carrying out key functions up to four times faster than existing flash solutions."

The increased performance will result in higher data throughput rates to speed up data-intensive Internet phone applications such as browsing, data streaming and text messaging, the company reports. Energy savings of up to 60 percent are also claimed for the new low-voltage memory.

In another indication of flash memory growth, AMD earlier announced that it has entered into an agreement with Hewlett-Packard Company (HP) to supply flash memory products over the next three years. Under the contract, AMD will provide HP with flash memory products designed to support a broad range of products including its inkjet printers and various print servers.

"Our high density and Page Mode flash memory devices offer an ideal complement to HP's innovative products," said Walid Maghribi, group vice president of AMD's Memory Group.

AMD produces a broad spectrum of flash memory products, including the award winning Simultaneous Read Write (SRW) product family, Super Low Voltage 1.8V flash memory devices, and Burst and Page



mode devices. Significantly, all of AMD's flash memory products are guaranteed for a minimum of one million write cycles per sector and 20 years data retention, "making them the most reliable non-volatile memory devices offered in the industry," according to AMD claims.

Copyright 2000 by Ken Fermoye, Fermoye Publications. Ken Fermoye has written some 2,500 articles for publications ranging from Playboy and Popular Science to MacWeek, Microtimes & PC Laptop. Ken's Korner, a syndicated monthly column, is available free to User Groups. For information or permission to reprint this article, contact kfermoyle@earthlink.net.



CLUB NEWS

Discounts on memory

If you are in the market for some additional memory for your computer, you might want to check out Crucial Technology. They are offering a 15% discount to members of the OPCUG. Just enter "Ottawa PC Users Group" as your coupon code at <http://www.crucial.com/canada/discount.asp>.

If you have a name brand computer or you know the make and model of your motherboard, they offer a relatively painless method of finding the right memory modules for your computer.

For more information on this offer, you can check out the full details on the OPCUG web site at <http://opcug.ottawa.com>. Select "Honour Roll" in the left pane and then find the entry for "Crucial Technology" in the right pane.



The latest magic from PowerQuest by Chris Taylor

PowerQuest has released version 6 of PartitionMagic. This is a really powerful program to help you manage the partitions on your hard disks. You can read reviews of previous versions at opcug.ottawa.com/public/Reviews/partmag3.htm, opcug.ottawa.com/public/reviews/partmag2.htm and opcug.ottawa.com/public/reviews/partmag1.htm.



First, a very brief primer on disk partitioning. Before a hard drive can be used, you must partition it and then format the partitions. You can have up to four primary partitions, or up to three primary partitions and a single extended partition. Normally only a single primary partition and the extended partition are visible. Extended partitions allow you to have multiple logical drives. The normal configuration of drives is that the primary partition is drive C: and the logical drives D:, E:, etc are in the extended partition.

Microsoft provides the program FDISK to “manage” partitions. I quote the word manage because it is a bit like saying you can manage your lawn with a rotto tiller and sod. If you decide you don’t like the current configuration of drives, such as the amount of space allocated to each, if using FDISK, no problem—just start over. Oh, and you just happen to lose all the information on the drive in the process.

Enter PartitionMagic. This truly amazing program can take care of all your partitioning needs non-destructively. It can deal with just about every disk format used on PCs—FAT, FAT16x, FAT32, FAT32x, HPFS, HPFS/386, Linux Ext2, Linux Swap, and NTFS. It can resize, re-order, create, hide, unhide, and delete partitions. It can convert FAT to FAT32, HPFS, or NTFS. It can convert FAT32 to FAT. And it can convert NTFS to FAT or FAT32. New to v6 is the ability to undelete FAT, FAT32, and NTFS partitions. Also new is the ability to split a FAT or FAT32 partition.

Where I find PartitionMagic most useful is in its ability to resize partitions without disturbing the data. It is this task that keeps a copy installed on my computer. I have two hard disks. The first is 20GB partitioned as a 3GB drive C: and a 17GB drive D:. The second drive is 6GB, all one partition. My most frequent task with PartitionMagic is resizing the partitions on the first hard drive.

Drive C: started out as a 1GB FAT partition. As I required additional space when I added programs to the OS installed there, I expanded it, taking space from the FAT32 partition D:. As the space requirements for C: went beyond the 2GB limit of FAT, I used PartitionMagic to convert the partition to FAT32 and expanded it to the current 3GB. While I could have thought more carefully about future requirements when I first partitioned the drive, I knew at the time that I did not have

to be overly concerned about that because PartitionMagic makes it so easy to adjust partitions at any time. With PartitionMagic I can adjust my partitions to how I want them now, not how I may need them at some point in the future.

PartitionMagic 6 sports a new user interface that makes things much simpler. Previous releases would only show the partitioning of a single drive at a time. Version 6 shows all the drives at once. A new “explorer” style pane on the left shows a tree view of all the disks and partitions. On the right-hand side, the top shows the layout of the partitions on each drive and the bottom window details in text the particulars of the selected drive.

The simplest way to modify things is to right-click on the partition you want to modify and select the option from the context menu that pops up. Of course the options are available from the standard menus as well.

As you make modifications in the interface, changes are not immediately applied to the disk. PartitionMagic builds a list of changes to be performed. You can review the list of pending changes at any time and v6 now allows you to modify this list by undoing operations in a reverse order. In previous releases, if you changed your mind, you had to discard all pending operations and start all over. This very flexible manner of working allows you to play “what if” scenarios quickly and easily before committing to any change. When you are happy with a series of changes, click on the *Apply* button and the pending changes will all be applied.

Another welcome change in v6 is support for Windows Me and Windows 2000 Professional. Version 5 had a patch available that added Windows 2000 Professional support, but only when run from the rescue diskettes. While this worked, it was awkward.

Continued next page...

PartitionMagic 6 ...continued from previous page

Being able to run the program from within Win2K is much more convenient.

There are wizards for common operations such as redistributing free space, merging partitions and copying partitions. For most operations, I recommend simply rolling up your sleeves and doing it all yourself without the wizard. It is really not all that difficult. By doing it yourself you retain much finer control over the outcome.

When you start playing with partitions, you may run into cases where an installed application is no longer on the same drive letter as when it was installed. PowerQuest includes a program called DriveMapper that looks in configuration files such as the registry and ini files and adjusts them to point to the new location of the program. Forgive me if I am sceptical, but I recommend that if you are about to make such a change to your disks, uninstall the affected program, make the changes to your partitions, and then reinstall.

While it is pretty simple to set up dual boot systems with Win9x and WinNT or 2K, if you

want to run multiple versions of Win9x or various versions of Windows and OS/2, Linux, etc, you can turn to another included program called BootMagic. It allows you to easily set up various operating systems on your computer and choose between them at boot time.

As always, PartitionMagic's documentation is a shining example for other vendors. The 150-page manual is clear and complete. I wish more vendors provided such complete printed documentation. The CD-ROM includes a PDF version of the *User Guide* as well as an excellent document called *Understanding Hard Disks*. PDF documents on installing a second operating system and use of the scripting language are also available.

Requirements for PartitionMagic 6 are; 486 to Pentium 150 and 32 to 64MB RAM (depending on OS), Windows 95/98/Me, Windows NT 4 Workstation with SP4, or Windows 2000 Professional. Users of other operating systems such as DOS, Windows 3.x, Linux and OS/2 can run PartitionMagic from the rescue disks.

If you want to order the program on the Web, you can do so at www.ugr.com/order/. You will need the user group code UGEVAL00. The price is US\$30, discounted from the full US\$70. However, with a US\$10 shipping charge, you may be able to find cheaper street prices here in town.



WINDOWS TIP

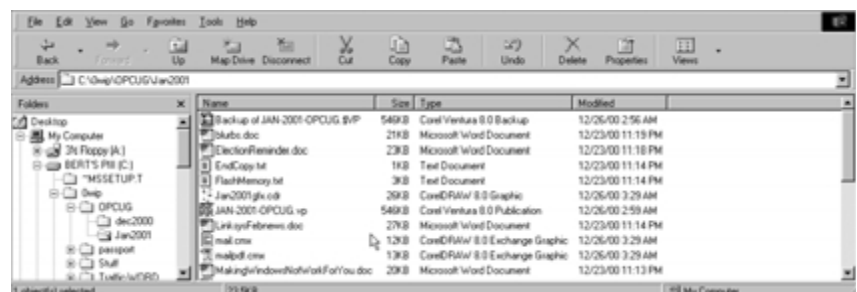
File details exposed! by Chris Taylor

One of the views available for Windows Explorer is "Details" (View | Details), which is great because it shows you the file name, the date/time the file was modified, the size and the type of the file.

More often than not, you end up with either huge amounts of white space where the column is much wider than it needs to be, or truncated text where the column is narrower than it needs to be.

You can resize columns by dragging the dividing line between column headers left or right, but there is an easier way to adjust the columns.

To automatically adjust all of the columns so they are just wide enough to handle everything displayed, click once in the right-hand pane and then hold the Ctrl key down and press the + key on the numeric keypad.



OTTAWA PC NEWS

Ottawa PC News is the newsletter of the Ottawa PC Users' Group (OPCUG), and is published monthly except in July and August. The opinions expressed in this newsletter may not necessarily represent the views of the club or its members. Deadline for submissions is three Saturdays before the general meeting. If you would like to contribute an article to *Ottawa PC News*, please submit it to the newsletter editor.

Group Meetings

OPCUG meets on the second Wednesday in the month, except July and August, at the National Museum of Science and Technology, 1867 St. Laurent Blvd, Ottawa. Meetings are 7:30–9:00 p.m. and Special Interest Groups go until 10 p.m.

Fees

Membership: \$25 per year.

Mailing Address

3 Thatcher St., Nepean, Ontario, K2G 1S6

Web address

<http://opcug.ottawa.com/>

Bulletin board—the PUB II (BBS)

Up to 33.6 kbps V.34 228-8951

Chairman and System Administrator

Chris Taylor ctaylor@nrcan.gc.ca via PUB II

Meeting Coordinator

Tim Mahoney timothy@cyberus.ca 225-2630

Treasurer

James Fridrich jimbo@magma.ca

Secretary

(Mr.) Jocelyn Doire Jocelyn.Doire@opcug.ottawa.com

Membership Chairman

Mark Cayer Mark.Cayer@StatCan.Ca 823-0354

Newsletter

Bert Schopf (editor) bert@blackbirdpcd.com 232-8427

(Mr.) Jocelyn Doire (distributor, electronic version):

Jocelyn.Doire@opcug.ottawa.com

Publicity

Chris Seal cseal@istar.ca 831-0280

Facilities

Bob Walker skywalk@iname.com 489-2084

Beginners' and Windows SIG coordinator

Duncan Petrie petried@zdnetwork.com 841-6119

Fox SIG coordinator

Andrew MacNeill andrew@aksel.com 851-4496

Fox SIG web page: www.aksel.com/foxsig

Internet SIG coordinator

Bob Gowan gowanb@inac.gc.ca

Paradox SIG coordinator

John Ladds laddsj@statcan.ca 951-4581

Webmaster

Brigitte Lord blord@magma.ca

Director without portfolio

Morris Turpin mturpin@igs.net 729-6955

© OPCUG 2000. Reprint permission is granted* to non-profit organizations, provided credit is given to the author and *The Ottawa PC News*. OPCUG requests a copy of the newsletter in which reprints appear.

*Permission is granted only for articles written by OPCUG members, and which are not copyrighted by the author.

CLUB NEWS

Welcome new members

Sharon Fall, Ottawa

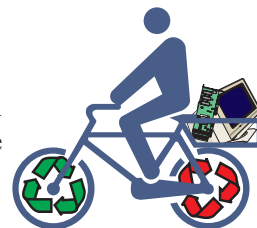
Lionel Wagner, Ottawa

CLUB LIFE

Reduce, Reuse, Recycle

Bring your old computer books, software, hardware, and paraphernalia you want to GIVE AWAY to the general meetings, and leave them at the table near the auditorium's entrance. *Please limit your magazines to publication dates of less than two years old.*

If you don't bring something, you may want to TAKE AWAY something of interest, so look in on this area. Any item left over at the end of the meeting will be sent to the... recycle bin.



How to get the Ottawa PC News by e-mail or PDF

To receive the newsletter by e-mail, send a message to listserv@opcug.ottawa.com with the text "subscribe Newslettertxt" or "subscribe NewsletterPDF" (without the quotes) in the body of the message. No subject line is required.

