OTTAWA PC NEWS

Volume 28, Number 9 November 2011

ARTICLE

The Failure of Antivirus

by Chris Taylor

Antivirus (AV) is being overwhelmed.

Most AV programs still rely mainly on signature files – those large-and-getting-larger files that contain exact byte patterns from known malware. This leads to the most obvious shortcoming of conventional AV programs – in order for an there to be a positive detection of a new piece of malware, the AV company must come across a sample, analyse it to determine it is in fact malicious, find a unique byte pattern not found in any non-malware, create a new signature file, and deliver it to the AV program running on your computer. This all takes time and, in extreme cases, far too long a time. In 2003, SQL Slammer infected 90% of all vulnerable hosts exposed to the Internet in the first 10 minutes.

Even in less extreme cases, the time to react may simply not be enough. A couple of years ago, there appeared a new style of socially-engineered attack. A brand new piece of malware would be developed which was not detected by any AV programs. It would be spammed to the world for a couple of hours. The email typically would tell the user that the courier (usually UPS) could not deliver a package and they should check the attached ZIP file for details. The ZIP file contained the malware and, when run, infected the machine. If you were unlucky enough to receive this spam and you opened the attachment before your AV vendor got an update for you, your computer joined the ranks of the infected.

If you didn't receive that malware infested email, all you had to do was wait a day or two. Another spam would come with a new piece of malware.

I often wondered how fast AV vendors get out an update for a brand new piece of malware. As it happens, the UPS malware is making its rounds again. As soon as I received copies of the UPS emails, I fired off the attached ZIP files to VirusTotal.com, who run a great service. You can upload any file and they will tell you if they have seen it before, when they first saw it, and check it against 43 AV engines with up-to-date signature files. By uploading the same file once a day, I got a sense of how long it takes the average vendor to detect new malware. The picture is not pretty. While many of the top names in AV could detect new stuff within a couple of days, several samples went undetected by about 10% of the AV engines over a week after they were in the wild. Keep in mind that even a couple of days can be a long time in the case of a rapidly spreading piece of malware.

How long is too long?

I think over a week to detect new malware is way too slow. To me it would be an indication of a vendor that is not doing enough to discover new malware, especially when it comes to the UPS malware. To get copies of UPS malware, you pretty much just have to get an email address added to some spam lists.

But even the best of the best can take some time. If you get AV updates once a day, and a new piece of malware comes in just after the daily update, you are already up to 24 hours minimum before you will be protected.

Huge volumes Another part of the problem comes from sheer volume. Last year, there was an average of 50,000 new, unique pieces of malware per day! There are now instances where compromised web sites compile a unique piece of malware for every visitor to the site!

(Continued on page 6)

Inside this issue:

Next Meeting: WEDNESDAY, November 9th, 2011

November Raffle

Thanks to the generosity of Corel, we have a copy of **Corel PaintShop Pro X4** for the November raffle. This latest edition of Corel's powerful photo editing software goes beyond the normal easy-to-use tools such as cropping, cloning, adjusting colours, contrast & brightness, to give you powerful professional features such as a module to deal with high dynamic range, the ability to blend multiple images together, selective focus, vignette effects, and more.

Corel PaintShop Pro X4 is valued at $99. More details about the program are available at corel.com/paintshop

Tickets are, as always, a good deal at $1 for one, a great deal at $2 for three or the unbelievable bargain of $5 for ten! Help support the OPCUG and keep dues low by purchasing raffle tickets and you might just win this great prize!

October Prize Winners

Howie Macumber won our door prize (an OPCUG Vacuum Flask) while **Michael Cayer** won the raffle prize of Windows 7 Ultimate.

And yes, it looks like Mike will be needing a computer upgrade in the near future ☺

Coming Up…

November 9th, 2011

Speaker: Evelyn Watts, Product Marketing Manager, Corel Corporation

Topic: Evelyn will be presenting on what's new with Corel software and giving a demo on the latest version on PaintShop Pro recently released.

2011 CALENDAR

Meetings	Date	Time and Venue
OPCUG General Meeting	Wednesday, November 9th	7:30 p.m. Auditorium of the **Canada Museum of Science and Technology**, 1867 St. Laurent Blvd. http://www.sciencetech.technomuses.ca/english/index.cfm
Beginners' SIG	Wednesday, November 9th	Immediately following the OPCUG General Meeting.
Linux SIG	Wednesday, November 9th	Immediately following the OPCUG General Meeting.
Beer BOF (Wing SIG East)	Wednesday, November 9th	10:00 p.m. (after all other SIGs) at Liam Maguire's, St. Laurent Blvd. at Innes Rd.

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

2012 OPCUG Elections

Once a year, the OPCUG holds elections for the 9-member Board of Directors. We are once again coming up to this annual event.

We encourage all members to consider running for a board position or getting involved in some other manner in the operations of the OPCUG.

If you want more information about what is involved, please talk to any current or past Board member. Names are listed in the Newsletter and on the web site (http://opcug.ca).

Nominations can be submitted to Bob Herres, Election Chair, in person at the October, November and December club meetings or by sending an email to nominations@opcug.ca.

Nominations must be received by midnight, December 31, 2011.

Please get involved. Please help the OPCUG continue in its role of *Users Helping Users!*

Bob Herres
Election Chair

ARTICLE

Scamming a Scammer

by Chris Taylor

The phone rang. Caller ID indicated long distance. Probably a telemarketer but what the heck, I was just solving a Sudoku. A guy with a thick accent wanted to verify he called the right number. Huh? Okay, why not?

He explained that unusual files have been detected coming from my computer and it was an indication of a problem with my computer.

Jackpot!

I had heard of this scam. Someone calls you and convinces you to go to a web site so they can "solve the problems with your computer." They have you click a link that loads some piece of crap on your computer so they can do whatever they want – install a bot, steal your info, or whatever. I had never experienced it myself.

I decided to have some fun. I said, "Hang on. I have to turn on my computer." I put down the phone and continued with my Sudoku. A couple of minutes later I picked up the phone and said, "My computer has been running really slowly lately. Hang on a minute." I was on a streak with my Sudoku.

After another minute I told him, "Oh my computer just crashed. It is rebooting. Hang on."

When I checked a couple of minutes later, the phone was dead. Oh well.

Second try

Then the phone rang again. It was him! He apologized, saying we must have gotten cut off.

I told him my computer was now up and running. He asked what operating system I was running and I told him Windows 7. He asked if I had a circle in the bottom left corner of the screen. I confirmed that and he had me click it, then find Computer and right click it and tell him what was on the pop-up menu. He had me load Computer Management and navigate to Event Viewer. He then wanted me to describe some things. I couldn't remember off the top of my head, so I put down my Sudoku and went to the computer room.

I loaded Event Viewer and was able to tell him what he wanted. He asked if there were some red exclamation marks. I told him there were hundreds. He was very concerned and asked me to read one out. I found an innocuous one that came from SideBySide. These are fairly common errors that don't seem to be a big deal, but they are long and convoluted in the wording. He patiently listened to me read it out. I then picked a CAPI2 error related to a certificate error. He waited while I read that one as well. Then he said this was really bad. These messages were evidence of the viruses that were on my computer and "taking up space".

"I have not had my computer on the Internet in a couple of months since they disconnected me for not paying my bill."
Didn't even faze him!

I decided to take him off script. I said, "I am confused though. Some of these red exclamation marks are from last week and I have not had my computer on the Internet in a couple of months since they disconnected me for not paying my bill."

Didn't even faze him!

He told me that the viruses probably got on my computer many months ago and were now causing the problems I was having with the computer being really slow and crashing all the time. He insisted the viruses were "taking up space."

Okay, so now what?

He said he would be able to fix my computer. This was going to be interesting! How was he going to install his malware on my computer if I didn't have Internet access?

He directed me to close Event Viewer and Computer Management and then load an Internet browser. To his credit, he suggested Internet Explorer "or Firefox". Unfortunately, his script didn't cover what he should do if the mark didn't have Internet access.

I explained to him that my browser wouldn't work because I had my Internet access cut off a couple of months ago for failing to pay my bill. He sounded very confused and said he would have to check with his technician. He put me on hold.

When he came back, he asked if I had a portable computer that had Internet access. I told him I just had the one computer. After some hems and haws, he said he was really sorry but there was nothing he could do to help.

He helpfully offered to call back in a couple of days if I got my Internet access back. I dragged things out a bit by telling him how I had lost my job and I wasn't all that interested in working anyway and therefore I had no money and couldn't afford to get Internet access back.

I considered saying, "I wouldn't be surprised if the phone got cut …" and hanging up in mid-sentence

I considered saying, "I wouldn't be surprised if the phone got cut …" and hanging up in mid-sentence, but I didn't.

He again said he was sorry, that there was nothing he would be able to do. I told him, "I guess I will have to take the computer back to the store" and said goodbye.

I didn't break any time records solving my Sudoku. But I had fun and hopefully the time spend talking with me saved someone else from having their computer compromised by this scammer.

PRODUCT REVIEW

Mini-Review – Zoner Photo Studio Free

by Alan German

In the never-ending search for free software that is actually useful, I have been looking for a digital image management system. Sure, Photo Gallery, built into some versions of Windows, and third-party programs like IrfanView (http://www.irfanview.ca/) provide this functionality but I find their file navigation and display systems rather clunky. ACDsee (http://opcug.ca/public/Reviews/acdsee7.htm) has all the features that I need but, since it is proprietary software, it fails the current test of being free and/or open-source.

Recently, I came across Zoner Photo Studio Free. This package is almost a clone of ACDSee, featuring the same three-panel main screen, with windows for navigation, image preview, and thumbnail display when it opens under the Manager tab. A host of command buttons and drop-down menus provide multiple functions such as acquiring images from a digital camera or scanner, sorting and renaming files, printing a contact sheet, sending a file by E-mail, or uploading an image to Flickr or Facebook.

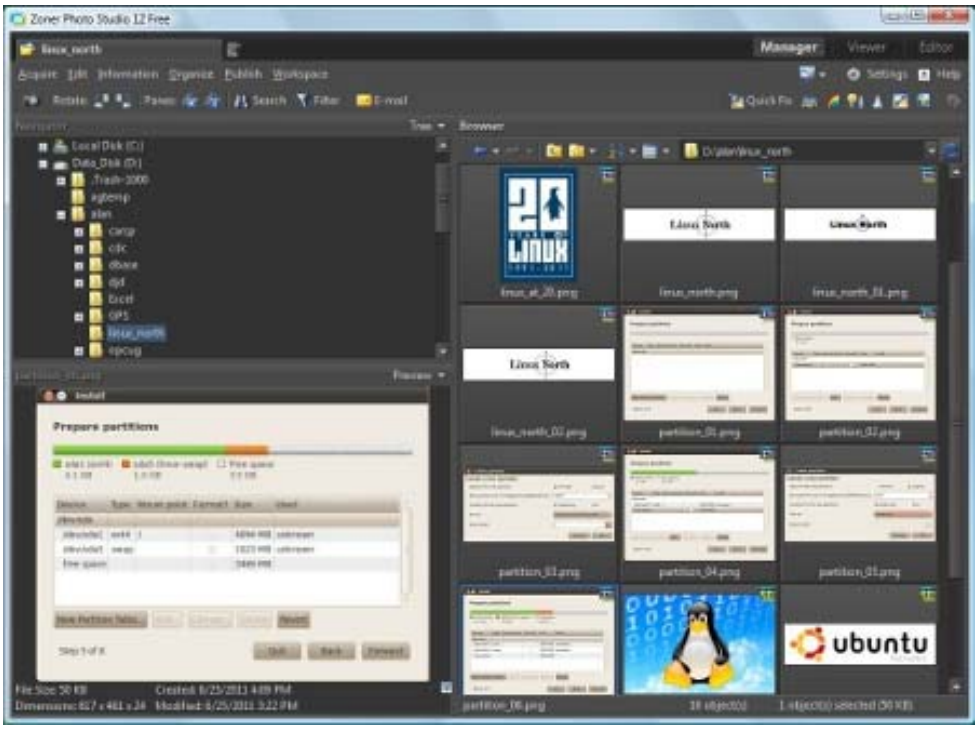
Two other main tabs are Viewer, with options that include zooming and slideshow creation, and Editor, where a wide range of tools allow images to be rotated or resized, colours to be modified, various image effects to be applied, and much more.

A Settings menu allows many of the program's functions to be customized, while a help menu provides detailed information on all aspects of the program's operations.

So, if you want a powerful – but free – digital image manager, you may need to look no further than Zoner Photo Studio Free.

Bottom Line

Zoner Photo Studio Free
Version 12
Zoner Software
http://free.zoner.com/



Failure of Antivirus *(cont'd from p.1)*

If it wasn't for the fact that, often, a single signature might catch hundreds or thousands of variants of a single piece of malware, that shiny new terabyte drive on your computer might be needed mostly for signature files.

Trying to close the window There are efforts being made to close the window of opportunity between when a vendor finds out about something bad and when you are protected. In one technique, when a new file arrives on your computer over the network, a hash (typically less than a kilobyte) is taken of the file and immediately sent to the AV vendor. The AV vendor can, in milliseconds, check the hash against the hashes of known malware. A short code can then be sent back to your computer letting your AV software know if the file is okay or not. This removes the delay in getting new signature files delivered to you.

Another form of protection is in the reputation of the websites. Since the majority of malware now comes from compromised or straight-out malicious websites, if an AV vendor can find out quickly about a compromised web site, they can have their software put hooks into your browser so the reputation is verified before the page is allowed to load. Oh, and in case you are wondering, there is no such thing as a safe web site any more. Pretty much every major web site in the world has been compromised at one time or another, even the sites of some pretty big names in security and AV.

Throw out AV?

No, don't do that. Even though conventional AV is becoming less effective, it should still be considered part of the arsenal you need to bring to bear against malware. I would never recommend running a Windows-based computer without AV unless it never connects to a network of any sort. And that includes sneakernets.

What we all need While other aspects of protecting a computer probably deserve entire articles on their own, in short, in addition to up-to-date AV, you need the following;

Anti-Spyware – in many ways, a variant of AV. However, good anti-spyware will look to some unique characteristics of spyware.

Firewall – a firewall should always be considered an essential aspect of computer protection. If the bad guys can't reach out to touch your computer, it falls to you doing something active before you can get compromised. Half the battle is won already! Ever since XP Service Pack 2, Windows has included a decent firewall. And there are plenty of free and inexpensive firewall products available that give enhanced protection.

Patch management – while it used to be said that you only had to keep Microsoft software up-to-date from a security vulnerability point-of-view, those days are long gone. In fact the most common means used to compromise computers now is Adobe Flash and infected Adobe Reader (.PDF) files. But it is essential to keep all your software up-to-date from a security vulnerability point-of-view. In January, 2011, I wrote a review of Personal Software Inspector from Secunia (http://opcug.ca/public/Reviews/Secunia.htm). It is free for home use and makes the job easy.

♦♦♦

File name: UPS-document.zip
Submission date: 2011-03-28 09:50:47 (UTC)
Current status: finished
Result: 11/ 43 (25.6%)

malware
Safety score: 0.0%

Compact | Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.03.26.00	2011.03.25	ASD.Prevention
AntiVir	7.11.5.79	2011.03.25	-
Antiy-AVL	2.0.3.7	2011.03.26	-
Avast	4.8.1351.0	2011.03.26	-
Avast5	5.0.677.0	2011.03.26	-
AVG	10.0.0.1190	2011.03.26	FakeAlert
BitDefender	7.2	2011.03.26	-
CAT-QuickHeal	11.00	2011.03.26	-
ClamAV	0.96.4.0	2011.03.26	Suspect.Bredozip-zippwd-10
Commtouch	5.2.11.5	2011.03.24	-
Comodo	8111	2011.03.26	-
DrWeb	5.0.2.03300	2011.03.26	-
Emsisoft	5.1.0.4	2011.03.26	-
eSafe	7.0.17.0	2011.03.24	-
eTrust-Vet	36.1.8236	2011.03.25	-
F-Prot	4.6.2.117	2011.03.26	-
F-Secure	9.0.16440.0	2011.03.23	-
Fortinet	4.2.254.0	2011.03.26	-
GData	21	2011.03.26	-
Ikarus	T3.1.1.97.0	2011.03.26	-
Jiangmin	13.0.900	2011.03.26	-
K7AntiVirus	9.94.4219	2011.03.26	-
Kaspersky	7.0.0.125	2011.03.26	-
McAfee	5.400.0.1158	2011.03.26	Artemis!08BA3C182674
McAfee-GW-Edition	2010.1C	2011.03.26	Artemis!08BA3C182674
Microsoft	1.6702	2011.03.26	TrojanDownloader:Win32/Chepvil.I
NOD32	5987	2011.03.26	a variant of Win32/TrojanDownloader.Stohil.J
Norman	6.07.03	2011.03.26	-
nProtect	2011-02-10.01	2011.02.15	-
Panda	10.0.3.5	2011.03.26	Trj/CI.A
PCTools	7.0.3.5	2011.03.26	-
Prevx	3.0	2011.03.28	Medium Risk Malware
Rising	23.50.05.05	2011.03.26	-
Sophos	4.64.0	2011.03.26	-
SUPERAntiSpyware	4.40.0.1006	2011.03.26	-
Symantec	20101.3.0.103	2011.03.26	-
TheHacker	6.7.0.1.157	2011.03.26	-
TrendMicro	9.200.0.1012	2011.03.26	TROJ_CHEPVIL.SM
TrendMicro-HouseCall	9.200.0.1012	2011.03.26	TROJ_CHEPVIL.SM
VBA32	3.12.14.3	2011.03.25	-
VIPRE	8825	2011.03.26	-
ViRobot	2011.3.26.4378	2011.03.26	-
VirusBuster	13.6.270.0	2011.03.25	-

24 hours after VirusTotal first saw this malware, 75% of AV programs don't detect it

OPCUG Free Software Guide – Part 26

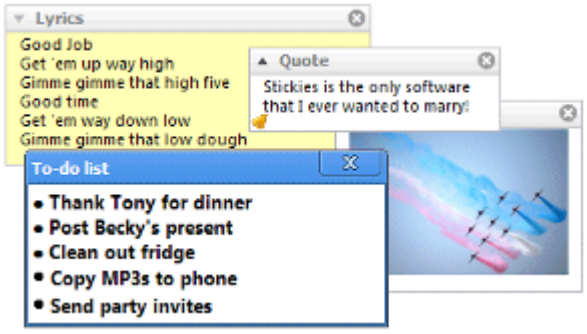
Compiled by Alan German

This guide features an annotated list of free computer programs. The software mentioned has not been reviewed (except where noted) nor have any tests necessarily been conducted. Consequently, no guarantees are provided that the individual programs will perform as described. Rather the list of available software is provided for the information of our members who may find one or more of the programs useful.

Accounts & Budget
The economic times are tough. This freeware package will enable you to manage your personal finances quickly and easily. Manage your income, expenses and budget, and track the difference between actual and budgeted values. Multiple file import/export formats.
Web Site: http://www.alauxsoft.com/prod04infan.htm

Stickies
A computerised version of those little yellow notes that you stick to the side of your monitor. But, these can be customised; fonts, colours and buttons changed, styles saved; notes resized; and you can set reminder alarms!

Current Release: Version 7.1a
Web Site: http://www.zhornsoftware.co.uk/stickies



Mikogo
Mikogo is an easy-to-use cross-platform desktop sharing tool, ideal for web conferencing, online meetings or remote support. And you can download the full version for free!
Current Release: Version 4.3.110804
Web Site: http://www.mikogo.com/

Spybot - Search & Destroy
Spybot detects and removes the spyware that silently tracks your surfing behaviour to create a marketing profile for you that is transmitted without your knowledge to the compilers and sold to advertising companies.
Current Release: Version 1.6.2
Web Site: http://www.safer-networking.org/en

Krento
This widget engine can display graphically rich interactive objects on your desktop to do things like display the date and time, launch other applications, or open web sites in your browser. But, unlike similar products, Krento is oriented on functionality rather than mere decoration.
Current Release: Version 2.1
Web Site: http://users.telenet.be/serhiy.perevoznyk

Thunderbird
Software made to make electronic mail easier. Mozilla Thunderbird is a free E-mail client that's easy to set up and customize - and it's loaded with great features!
Current Release: Version 6.0.2
Web Site: http://www.mozilla.org/en-US/thunderbird/
Previously Reviewed:
Can we go to the next message? - Please!, Alan German, http://opcug.ca/public/Reviews/thunderbird15.htm

f.lux
Ever notice how people texting at night have that eerie blue glow? Or, are you blinded at night by your computer screen? The solution is here. The f.lux software will adapt the color of your computer's display to the time of day - warm at night - and like sunlight during the day.
Web Site: http://stereopsis.com/flux/

MusicBrainz
A relational database of music metadata that offers far more than the traditional artist/album/track model. All of the data in MusicBrainz are contributed and maintained by an open community of users who follow style guidelines to help ensure a standard of quality. The database is made available for free download by the general public.
Web Site: http://musicbrainz.org/

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.

Member participation is encouraged. If you would like to contribute an article to Ottawa PC News, please submit it to the newsletter editor (contact info below). Deadline for submissions is three Sundays before the next General Meeting.

Group Meetings

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

OPCUG Membership Fees:	$25 per year
Mailing Address:	3 Thatcher St., Nepean, Ontario, K2G 1S6
Web address:	**http://opcug.ca**
Bulletin board — The PUB (BBS)	**http://opcug.ca/default.htm**

President and System Administrator		
Chris Taylor	**chris.taylor@opcug.ca**	613-727-5453
Meeting Coordinator		
Andrea Wells	**andrea.wells@opcug.ca**	
Treasurer		
Alan German	**alan.german@opcug.ca**	
Secretary		
Gail Eagen	**gail.eagen@opcug.ca**	
Membership Chairman		
Mark Cayer	**mark.cayer@opcug.ca**	613-823-0354
Newsletter		
Brigitte Lord (editor/layout)	**brigittelord@opcug.ca**	
(Mr.) Jocelyn Doire (e-mail distribution)	**jocelyn.doire@opcug.ca**	
Public Relations		
Morris Turpin	**PR@opcug.ca**	613-729-6955
Facilities		
Bob Walker		613-489-2084
Webmaster		
Brigitte Lord	**opcug-webmaster2@opcug.ca**	
Privacy Director		
Wayne Houston	**privacy2@opcug.ca**	
Special Events Coordinator		
Bob Gowan	**bob.gowan@opcug.ca**	
Beginners' SIG		
Chris Taylor	**chris.taylor@opcug.ca**	613-727-5453
Linux / Open-Source SIG		
Andrea Wells	**andrea.wells@opcug.ca**	

© OPCUG 2011.

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.

How to get the OTTAWA PC NEWS by e-mail

Want to get the newsletter electronically? There are two formats available: plain text and Adobe Acrobat PDF. Simply send a message in plain text to **listserve@opcug.ca**. Leave the subject blank and in the body of the message, type: **subscribe NewsletterTXT**
(to get the plain text version)
or **subscribe NewsletterPDF**
(to get the Adobe Acrobat PDF version).

To cancel e-mailing, send a message in plain text to **listserve@opcug.ca** and type: **unsubscribe NewsletterTXT**
or **unsubscribe NewsletterPDF**

And if you decide you do not need the printed version mailed to you anymore, simply let Mark Cayer (membership chairman) know. He can be reached at general meetings, as well as by e-mail at **Mark.Cayer@opcug.ca**. You might want to wait until you have successfully received at least one issue electronically before opting out from the printed version.

To subscribe to the Announcements List, e-mail **listserve@opcug.ca**. Leave the subject blank and in the body of the message type: **subscribe announcements**

Within a couple of minutes you will receive a confirmation message from the listserver.

"Announcements" is a low volume list that the Board of Directors uses to get in touch with the membership.
Subscribers can expect at least one message per month – the meeting reminder that goes out a few days in advance of the general meeting. Other than that, the only time it is used is when the Board feels there is some important news that should be brought to the attention of all members.