Chesapeake PC Users Group, Inc.

THE C.A.T.S. Eye

PRESIDENT’S CORNER

BRING YOUR LAPTOP WITH YOU TO THE NEXT MEETING!

The Chesapeake Area Technology Society (CATS)

At our last meeting, the members voted to change the name of the organization to the **C**hesapeake **A**rea **T**echnology **S**ociety (CATS). Our goal is to appeal to a wider audience then simply those who have concerns with traditional PCs. This does not mean that PCs will be ignored, far from it. Over the past few years, our meetings shifted focus from Windows/PCs expanding to other technologies and information. The identity change is our first impression which informs the public at large, that we are here and ready to

HELP WANTED:

Our Webmeister, Mike ‘Tony’ DeLucia has chosen to step down from his duties. He has been our only Web Master for many years. This big shoes to fill. We need to replace him with someone who has web design experience and has the time to make updates to the page.

Our Acting Secretary, Joyce Shue is stepping down from her duties. Joyce has done a tireless job of recording club business and promoting our organization in many local publications.

We need someone to take over these roles.
If you have interest in these roles, please contact any member of the Board of Directors for more information.

If you have any budding graphic artists in the family, we’re looking to update our old Chessie logo.

Upcoming meeting topics

June 5, 2013 - User Utilities and Show and Tell from everyone! This is the meeting where you, the members, talk about your favorites!

September 11, 2013 – Fran Damratowski will demonstrate Ubuntu Linux. This is the OS that will be installed on all PC’s that the CRSIG will have made available.

October 9, 2013 – Mike Young will demonstrate the latest release of Microsoft Office, Office 2013. He will demonstrate some of the latest features and show how to take advantage of some of these new features.

Starting back up in September, we are looking forward to presenting a full agenda over the 2013-2014 season.

We hope to see many more of you at the upcoming meetings and look forward to your continued input for future meeting presentations.

Have a safe and happy summer; we will see you in September!

Michael

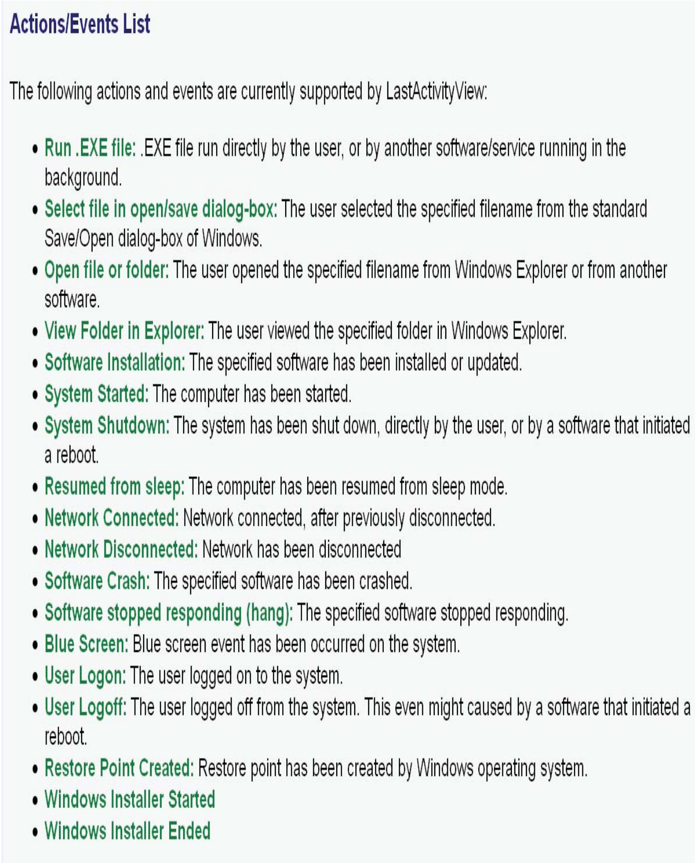
cont'd from page 4

What's Your Computer Up To

to run arbitrary code." I would not have been able to easily and quickly determine the cause of that particular crash without LastActivityView. This is but one of countless purposes that can be accomplished with LastActivityView.

LastActivityView runs on any version of Windows since Windows 2000, and includes XP, Vista, Windows 7 and Windows 8; both 32-bit and 64-bit systems are supported.

For such a tiny, fast, and free program, LastActivityView is a powerful utility that can provide extensive information on what has been done on a Windows computer. For anyone who would like to see for himself what has been running on his computer; what crashed, what caused the crash; files downloaded, installed, or uninstalled; and a wealth of other information, LastActivityView is a very worthwhile program to add to the user's arsenal of utilities.



Actions/Events List

The following actions and events are currently supported by LastActivityView:

- **Run .EXE file:** .EXE file run directly by the user, or by another software/service running in the background.
- **Select file in open/save dialog-box:** The user selected the specified filename from the standard Save/Open dialog-box of Windows.
- **Open file or folder:** The user opened the specified filename from Windows Explorer or from another software.
- **View Folder in Explorer:** The user viewed the specified folder in Windows Explorer.
- **Software Installation:** The specified software has been installed or updated.
- **System Started:** The computer has been started.
- **System Shutdown:** The system has been shut down, directly by the user, or by a software that initiated a reboot.
- **Resumed from sleep:** The computer has been resumed from sleep mode.
- **Network Connected:** Network connected, after previously disconnected.
- **Network Disconnected:** Network has been disconnected
- **Software Crash:** The specified software has been crashed.
- **Software stopped responding (hang):** The specified software stopped responding.
- **Blue Screen:** Blue screen event has been occurred on the system.
- **User Logon:** The user logged on to the system.
- **User Logoff:** The user logged off from the system. This even might caused by a software that initiated a reboot.
- **Restore Point Created:** Restore point has been created by Windows operating system.
- **Windows Installer Started**
- **Windows Installer Ended**

OFFICERS

President

Mike Young.......................................(410) 551-4411
president@chesapeakepcusersgroup.org

Vice President

Mike Regimenti................................(301) 509-6091
vice-president@chesapeakepcusersgroup.org

Co-Treasurers

Kathy Walker (410) 266-6317 Bill Somers (410) 647-9429
treasurer@chesapeakepcusersgroup.org

Acting Secretary

Joyce Shue...(410) 263-3510
secretary@chesapeakepcusersgroup.org

Publisher/Editor

Mike Regimenti................................(301) 509-6091
editor@chesapeakepcusersgroup.org

CHAIRPERSONS

Programs Chairperson

Craig Barlow....................................(410) 266-6829
programs@chesapeakepcusersgroup.org

Education Chairperson

Sam Shepherd.................................(410) 647-6077
education@chesapeakepcusersgroup.org

Membership Chairpersons

Betsy Fravel......................................(410) 703-1425
membership@chesapeakepcusersgroup.org

Public Relations Chairperson

Joyce Shue...(410) 263-3510
pr@chesapeakepcusersgroup.org

SPECIAL INTEREST GROUPS (SIGS)

New Users Group

Sam Shepherd.................................(410) 647-6077

Technology SIG

Mike Regimenti................................(301) 509-6091
internet@chesapeakepcusersgroup.org

Computer Refurbishing SIG

Fran Damratowski...........................(410) 923-1550
refurbishing@chesapeakepcusersgroup.org

Webmeister

Mike DeLucia..................................(410) 721-2991
webmeister@chesapeakepcusersgroup.org

What Has Your Computer Been Doing? Free Utility Shows All

by

Ira Wilsker

WEBSITES:
http://www.nirsoft.net
http://www.nirsoft.net/utils/computer_activity_view.html
https://www.techsupportalert.com/content/nifty-way-find-out-what-your-windows-computer-has-been-doing.htm

Many of us have encountered frustrations with our computers. Sometimes it appears that running programs crash or otherwise cease functioning without explanation. On older computers, most notoriously those running Windows XP, a cryptic “Blue Screen of Death” (BSOD) sometimes appears when there is a crash of some type, often displaying nonsensical error codes that require extensive research to decode. Some suspicious computer users believe that others are accessing their computer, running unauthorized software or malware. Other wary users may find it interesting seeing what other people may have done on a particular computer, and what programs they may have run, what documents were viewed, and when (what time) the computer was booted and shut down. If a computer was infected by malware, it may often be of great interest to see what was being run on the computer at the time of infestation, and even identify the malware and its payload. This, and more, can be readily displayed by a tiny, free utility, LastActivityView.

LastActivityView is one of dozens of small free utilities published by a feisty software engineer, Nir Sofer, on his website at www.nirsoft.net. Nir personally writes all of his own software in his spare time, and makes it available to all for free. Many of his utilities are given the highest ratings by a variety of web services and computer publications; all of his software is free of advertising and other pesky irritants, making it popular among his huge and loyal user base. In his spare time, Nir personally maintains his website and updates his software, as well as creates new utilities. One of his newest titles, LastActivityView has caught the attention of computer technicians, forensic experts, hobbyists, and others who really want to know what has really been running on a computer, and when the computer was accessed.

Windows users may be passively aware that their computers save extensive, but often invisible files, about what they have run; LastActivityView has the capability to read these historical files and display additional information about many of the computer’s activities. On my primary computer, this record starts on the day it was manufactured, and documents everything that I have done since I first powered it on after removing it from its box. Every piece of software that I ever installed or uninstalled is listed, including date, time, description, filenames, path on the hard drive, and other information. Every boot, shutdown, crash, and other event was also duly recorded. In addition to simply displaying a huge file with all of my computing activities, LastActivityView also has the power to provide additional information for many of the items listed. LastActivityView also can display detailed information about program interactions, and conflicts that caused software and hardware crashes.

The actual program file itself is tiny, only about 100k in size, and requires no installation. It is totally portable, and can be

cont’d on Page 4

cont'd from page 3

What Has Your Computer Been Doing?

run from any Windows connected device. The LastActivityView program, an exe file, is one of only three components included in the 64k ZIP (compressed) file downloaded from NirSoft; the other two items in the ZIP file are a small "readme.txt" file with simple instructions and other information, and a standard format Windows Help File (chm format) that can be opened with any version of Windows, and displays detailed help and other information. I downloaded the zip file, and using Windows native utility, "unzipped" or uncompressed it into a new directory that I created for it. Total space required for all three files is a miniscule 130k of drive space. I also copied the files to the USB flash drive that I always have on my car keychain, so I can use it whenever and wherever needed.

According to the included readme.txt file, " LastActivityView is a tool for Windows operating system that collects information from various sources on a running system, and displays a log of actions made by the user and events occurred on this computer. The activity displayed by LastActivityView includes: Running .exe file, Opening open/save dialog-box, Opening file/folder from Explorer or other software, software installation, system shutdown/start, application or system crash, network connection/disconnection and more... " The file created by LastActivityView can be quickly exported in a variety of formats that can be utilized by a variety of other programs that can read csv, tab-delimited, xml, or html formatted information. A simple copy and paste can also place information in other programs, such as an Excel spreadsheet. For those who may wish to customize the execution of LastActivityView, several command line options are available, but most users will find that simply running the file without any additional commands will provide comprehensive and useful information.

In addition to the obvious tracking of what was run on a computer, LastActivityView can also provide additional and valuable information. I was able to prove this to myself when I examined some recent logs, looking for software crashes and conflicts. One of several reasons why I do not use Internet Explorer as my primary browser is that for some reason, it sometimes crashes when open. According to the report, my most recent software crash occurred on May 17, at 9:11:07pm when Internet Explorer, version 10.0.9200 crashed. By right-clicking on the line in the log showing the crash, an options menu appeared which displayed what additional information could be shown. I first selected "Properties", which displayed the Action Time, Description (Software Crash), File Name, Full Path (location on hard drive), and what was most important to me, More Information. Similar information can be displayed as a webpage in HTML by selecting "HTML Report - Selected Item". The More Information line showed precisely the software conflict that caused the crash; in this particular case, according to the display, there was a memory conflict between IEXPLORE.EXE 10.0.9200.16576 and TmBpIe32.dll, which is a module or component of my TrendMicro security suite. Now that I have recorded this conflict, it would be easy to determine whether this is a one-time anomaly or a continuing problem that requires attention and remediation. Doing a quick online search for TmBpIe32.dll, I found that this file is a Trend Micro Browser Plug-In for Internet Explorer that is designed to protect the browser from exploitation. According to Wikipedia, "A browser exploit is a form of malicious code that takes advantage of a flaw or vulnerability in an operating system or piece of software with the intent to breach browser security to alter a user's browser settings without their knowledge. Malicious code may exploit ActiveX, HTML, images, Java, JavaScript, and other Web technologies and cause the browser

cont'd on Page 2

Holy cow! Is this a virus?

by

Linda Gonse, Editor/Webmaster, Orange County PC Users' Group, CA

March 2013 issue, nibbles & bits

www.orcopug.org

editor (at) orcopug.org

I recently added a second external hard drive to my computer system. I use one for backups of InDesign files and the other one for Acronis True Image system backups.

As I browsed through the files I'd saved to the drives, I ran into something peculiar. Both drives had folders with names that were long strings of random letters. And each folder contained one file: mrtstub.exe at 89KB on the Iomega drive, and MPSigStub.exe at 227KB on the Seagate drive.

Fearing these might be malware or a virus, I quickly did a Google search. Interestingly, the search turned up conflicting opinions in different forums. Some people said it was a virus and highly dangerous, some said the folder and file(s) inside were benign, some said the files were leftover from when Microsoft Malicious Software Removal Tool (MRT) was run and had not been deleted automatically, and some said Windows created them.

Although I only found one file in the folders, other people have seen as many as four at one time: mrtstub.exe, mrt.exe._p, MRT.exe, and $shtdwn$.req.

I found a link to information about the Malicious Software Removal Tool at http://support.microsoft.com/kb/890830#Faq. In particular, it gave instructions on how to remove the Malicious Software Removal Tool.

The Malicious Software Removal Tool does not use an installer. Typically, when you run the Malicious Software Removal Tool, it creates a randomly named temporary directory on the root drive of the computer. This directory contains several files, and it includes the Mrtstub.exe file. Most of the time, this folder is automatically deleted after the tool finishes running or after the next time that you start the computer. However, this folder may not always be automatically deleted. In these cases, you can manually delete this folder, and this has no adverse effect on the computer.

I also learned that MRT is not a substitute for a resident antivirus for various reasons:

1. MRT only removes malware AFTER infection, it doesn't BLOCK malware like an antivirus does;
2. MRT is designed to target a small set of malware only, while an antivirus takes care of most malware in the wild; and
3. MRT can only detect actively running malware — an antivirus can also detect dormant malware.

Microsoft's Knowledge Base (http://support.microsoft.com/kb/890830) also said a new version of the Microsoft Malicious Software Removal Tool is released every month. After you download the tool, the tool runs one time to check your computer for infection by specific prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection it finds.

This KB article contains information about how you can download and run the tool, and what happens when the tool finds malicious software on your computer.

Even though I did not intentionally download the Removal Tool or run it, I read that Windows Update may do that when it downloads automatic updates. Further, it uses the largest hard drive on the system to create the temp folders; and in my case, the external hard drives are the largest with each being 2TB.

The upshot of this was I checked each file's Properties and confirmed Microsoft had signed them. Then I deleted the folders and files

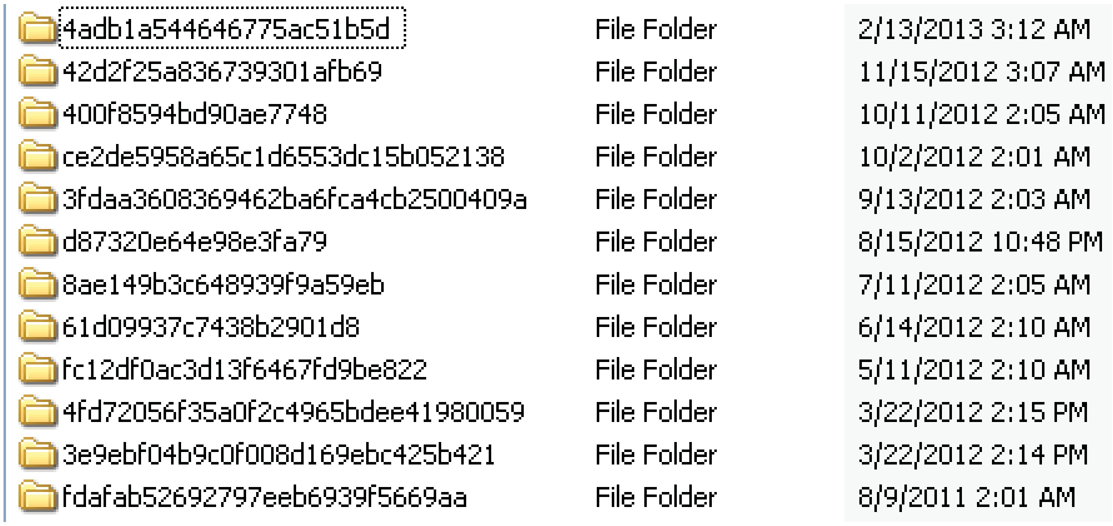
cont'd on Page 6

cont’d from page 5

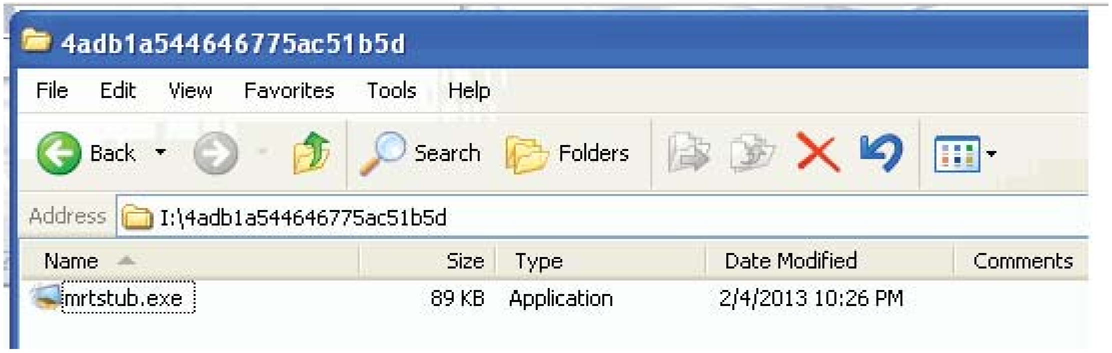
Holy cow! Is this a virus?

manually and nothing bad happened. In the future, I’ll disconnect the external drives before downloading or installing Windows Update.

Folders and files found on external drive.



4adb1a544646775ac51b5d	File Folder	2/13/2013 3:12 AM
42d2f25a836739301afb69	File Folder	11/15/2012 3:07 AM
400f8594bd90ae7748	File Folder	10/11/2012 2:05 AM
ce2de5958a65c1d6553dc15b052138	File Folder	10/2/2012 2:01 AM
3fdaa3608369462ba6fca4cb2500409a	File Folder	9/13/2012 2:03 AM
d87320e64e98e3fa79	File Folder	8/15/2012 10:48 PM
8ae149b3c648939f9a59eb	File Folder	7/11/2012 2:05 AM
61d09937c7438b2901d8	File Folder	6/14/2012 2:10 AM
fc12df0ac3d13f6467fd9be822	File Folder	5/11/2012 2:10 AM
4fd72056f35a0f2c4965bdee41980059	File Folder	3/22/2012 2:15 PM
3e9ebf04b9c0f008d169ebc425b421	File Folder	3/22/2012 2:14 PM
fdafab52692797eeb6939f5669aa	File Folder	8/9/2011 2:01 AM



I:\4adb1a544646775ac51b5d

Name	Size	Type	Date Modified	Comments
mrtstub.exe	89 KB	Application	2/4/2013 10:26 PM	

IObit Releases New Free and Pro Malware Fighter 2

by

Ira Wilsker

WEBSITES:
http://www.iobit.com/malware-fighter.php
http://www.iobit.com/malware-fighter-pro.php
http://www.iobit.com/help/imf/

I have always been a fan of utilizing third party malware scanners to provide computer security in depth as well as to detect and neutralize any malware that may have penetrated the primary computer security software. Countless times in this column over the years, I have recommended free standing

cont’d on Page 7

cont'd on Page 6

New IObit Releases

anti-malware software from MalwareBytes, SuperAntiSpyware, and Emsisoft. I have now had an opportunity to experiment with another newly released competing product, and my first impressions are positive. This newly released anti-malware product is Malware Fighter 2 from IObit.

Available from the IObit website (www.iobit.com) as both a free version and a paid Pro version (the Pro version is currently introductory priced at $19.95 for a one year license). Both versions offer real-time protection from malware attacks with a security package that is easy on system resources (does not significantly slow down the computer), is frequently updated, can detect and remove malware infections that may have penetrated the existing security software, and is explicitly designed to run on top of other antivirus and security software in order to provide security in depth. Both versions use IObit's proprietary "Dual-Core" anti-malware engine which claims to be able to detect complex and deeply hidden malware, including spyware, adware, Trojans, keyloggers, bots, worms, and hijackers and other malware threats. If a suspicious file or behavior is detected that is not included in the updated Malware Fighter's database, the questionable file is uploaded to the new "IObit Cloud Security" service for further analysis and resolution. For users who prefer simplicity, Malware Fighter offers a "Smart One-Stop Solution" that can detect and repair any malware security issues with a single mouse click. The only major difference between the free and Pro versions that I could find is that the Pro version automatically updates itself (in the free version, the user has to click on the update button), and the Pro version can be set to automatically perform a scan at selected times.

As good as they may be, no security product offers 100% protection; in order to increase the security of a PC, it is often desirable to implement a layered defense which will impose additional barriers and defenses to a variety of cyber threats. While there is an old and mostly still applicable adage "Never run more than one antivirus program at a time", there are exceptions to that rule. Today, several anti-malware products are intentionally designed to run concurrently with contemporary security software in order to provide enhanced security in real-time, and Malware Fighter is one of those products. This software is written to be compatible with other antivirus and anti-malware software, firewall software, and other security products.

The real-time functions in Malware Fighter provide comprehensive protection from malware threats, including a series of "Guards" that protect the computer and its software from attacks targeted at specific computer functions. These guards include a "Startup Guard" that prevents unwanted programs from installing themselves such that they load every time the computer is booted; a "Browser Guard" that protects the browser from being hijacked, having the startup page changed without consent, and other browser based threats; a "Network Guard" that block web pages containing threats; a "File Guard" that protects critical system and program files as well as scans unknown files for threats; a "Cookie Guard" that protects the browser and the user from dangerous cookies (small text files placed on the computer by websites that can violate your privacy and safety); a "Process Guard" that monitors the running processes on the computer, continuously searching for threats that may start to run; a "USB Disk Guard" that protects from infestation from USB connected devices; and "Malicious Action" that protects against other malicious behaviors, threats and dangers to the computer. These real-time protections are always running and providing continuous protection, even when web gaming, web browsing, reading email, shopping online, watching videos, and performing other PC activities.

Currently, a nasty form of cyber threat is referred to as a "zero day" threat, in that it can

cont'd on Page 8

cont'd from page 7

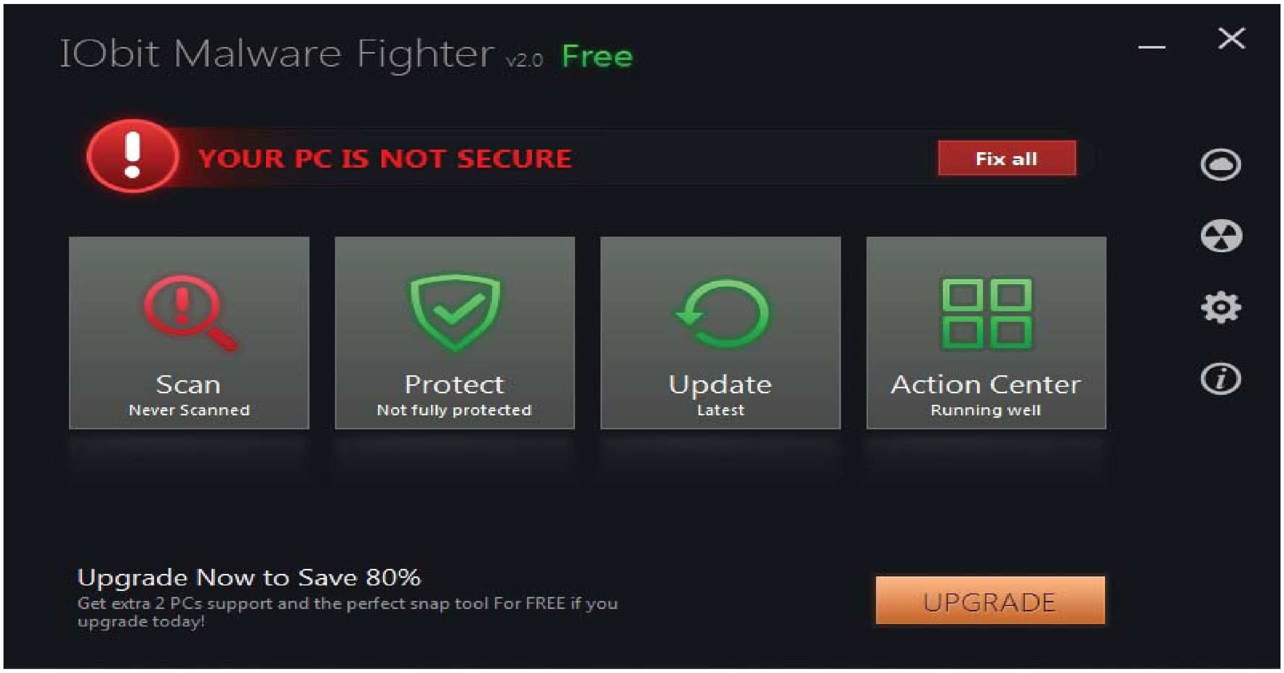
New IObit Releases

be introduced and spread so quickly, that it is nearly impossible for security providers to detect the threat and devise a solution to neutralize it before is spreads widely. IObit Malware Fighters uses a variety of tools to protect the user from these rapidly evolving threats, including a form of Host Intrusion Prevention System, commonly referred to as “HIPS”. Malware Fighter has a feature it calls “DOG” to detect these new threats. According to IObit, “DOG (Digital Original Gene) is a novel heuristic malware detection algorithm, that evaluates key attributes relating to software making, distribution and advertising. Various factors are considered before determining that a program is malicious. For instance, if the program is published by a notorious vendor. The main function of DOG is to enhance detection of zero day threats.”

In addition to providing real-time protection, this type of software is also designed to scan the computer for existing threats; Malware Fighter offers three levels or scanning speeds, a smart scan, a full scan, and a custom scan. A smart scan is the fastest of the automatic scans (but still may take over an hour to run), but only scans the critical software files and locations on the computer, as they are the most likely to harbor any infections; most of the time, a smart scan is adequate for routine security scans. A full scan is the slowest, but most comprehensive scan, as it searches everything for malware on all connected hard drives; with large or multiple hard drives, a full scan could take several hours to complete, but it is the most comprehensive and complete scan available. A custom scan only scans selected areas or functions; Malware Fighter allows user selectable custom scans covering critical system areas, processes running in memory (running malware can often be quickly detected here, as a memory processes scan only takes a few seconds), or specific hard drives.

IObit Malware Fighter will run fine on all contemporary versions of Windows, including Window 8, Windows 7, XP, Vista, and Windows 2000. Hardware requirements are minimal for a modern computer, such that Malware Fighter will run on almost any Windows PC with a minimum of 256 megs of RAM, a 300 MHz processor, and 30 MB of hard drive space.

For those who would like another malware scanner in order to confirm their PC’s security, or would like a free or paid real-time malware utility that can provide security in depth in addition to the security software already installed, IObit’s new Malware Fighter 2 would be very worthy of consideration.



IObit Malware Fighter v2.0 Free

YOUR PC IS NOT SECURE

Upgrade Now to Save 80%

Get extra 2 PCs support and the perfect snap tool For FREE if you upgrade today!

Secure and Keep Track of your Passwords for Free

by
Ira Wilsker

WEBSITES:
http://www.splashdata.com/press/PR121023.htm
http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf
http://blog.eset.com/2012/06/07/passwords-and-pins-the-worst-choices
http://www.zdnet.com/blog/security/25-most-used-passwords-revealed-is-yours-one-of-them/12427
https://www.techsupportalert.com/best-free-web-form-filler-password-manager.htm
https://www.techsupportalert.com/content/how-choose-strong-password.htm
https://www.techsupportalert.com/content/how-keep-your-passwords-safe.htm
https://lastpass.com
http://keepass.info
http://passwordsafe.sourceforge.net

Let's face it; most computer users are inherently lazy. In order to make things easy on ourselves we often use the same simple password on multiple websites and devices, or we use the most simple passwords such as "password" or "12345". According to computer security experts who have analyzed millions of purloined passwords, too many of us are using simple passwords that are easy for others to guess, and then access our most intimate or personal data in order to commit identity theft or other forms of computer crimes against us, including industrial espionage.

Last fall, a purveyor of password management and security software, SplashData, published their annual list of the 25 worst passwords of the year, "SplashData's top 25 list was compiled from files containing millions of stolen passwords posted online by hackers. The company advises consumers or businesses using any of the passwords on the list to change them immediately. Even though each year hacking tools get more sophisticated, thieves still tend to prefer easy targets, Slain (SplashData CEO) said. "Just a little bit more effort in choosing better passwords will go a long way toward making you safer online." (Source: splashdata.com/press/PR121023.htm). According to SplashData, the top 10 of the 25 most commonly used passwords (a fact not lost on hackers and crackers) are: password, 123456, 12345678, abc123, qwerty, monkey, letmein, dragon, and 111111.

Despite countless news stories in all of the media about password security, as well as the expanding requirement by many websites that only complex passwords that meet strict standards can be used, millions of users have not learned that painful lesson. In 2009, following a hack at the popular social gaming network RockYou.com, a staggering 32 million user passwords were published. A cyber security company, Imperva Application Defense Center, analyzed these 32 million passwords, and found that users overwhelmingly preferred simple, easy to remember passwords. In the analysis, it was noted that almost a third of RockYou users used short, under six character passwords, a password length that has such a finite list of combinations, it is easy for hackers to use any of several utilities to crack these passwords using a brute force or dictionary technique. In the same study, it was found that about 60% of users had passwords using a limited set of alpha-numeric characters, another easy to crack security problem. Almost half of users used slang, dictionary words, names, or so called "trivial passwords" consisting of consecutive digits or adjacent keyboard keys. The most common password used, "123456" (used by 290,731 RockYou users), is the same "most common" password noted in other studies of common passwords.

Studies of other massive password thefts, including the six million passwords stolen

cont'd on Page 10

cont'd from Page 9

Secure your Passwords for Free

from LinkedIn Last.fm and eHarmony revealed a somewhat similar distribution of easy and vulnerable passwords. The security company ESET analyzed these 6 million passwords, and found that the top 5 of the 25 most widely used passwords were password, 123456, 12345678, 1234, qwerty, and 12345. ESET also warned that stealing a common password, especially simple numeric passwords can also open the unknowing victim to a variety of other criminal attacks, including ATM theft (many people use the same four digit password as their ATM PIN), " ... digital locks and keypads, handheld authentication devices like an RSA or Digipass token, or a software implementation on a mobile device (such as) authentication via laptops, netbooks, tablets and smartphones."

SplashData, Imperva, ESET, and other security companies and services, have widely published a short list of hints and tips about creating more secure passwords that will be difficult to crack. These security recommendations for secure passwords are substantially identical from the different sources, and generally include the following:

1. Use a password with a minimum of eight characters, including both alphabetical (mixed upper and lower case letters) and numerical characters. Many websites also allow the use of punctuation and other symbols as a part of the password; this makes cracking much more difficult. Some password experts suggest using short words with spaces or characters separating the words and maybe a number, such as "i_lOVe-TeXas!0518". Bruce Schneir, a respected cryptographer, computer security specialist, and writer has proposed this novel idea to create an easy to remember but secure password, "Take a sentence and turn it into a password. Something like "This little piggy went to market" might become "tlpWENT2m". That nine-character password won't be in anyone's dictionary."

2. Never use the same password on more than one website. Hackers and crackers have often found that a user's email address or username and password stolen from one popular website will often work perfectly on other popular websites, making identity theft, financial fraud, espionage, and other malicious activities easy to accomplish. When signing up on a new website, never use an already used password; some scam and phishing (identity theft) websites purposely harvest passwords from new registrants for the explicit purpose of using them on other websites. Bruce Schneir recommends, "If you can't remember your passwords, write them down and put the paper in your wallet. But just write the sentence – or better yet – a hint that will help you remember your sentence."

One of the widely used excuses for not creating complex, hard to crack passwords is that these complex passwords are too hard to remember. Another common excuse given is since most computer users utilize large number of online services that require usernames and passwords, there are just too many different passwords to remember. In order to have the security of unique and complex passwords for each website along with the convenience of a written password listing, several software authors and publishers have created a class of software generically called "password managers". The password managers are readily available as both free or commercial products, and are widely available for download or purchase. Many of the comprehensive security suites are now also including a dedicated password managers, as exemplified by TrendMicro's Titanium Maximum Security suite, which includes as one of its components, TrendMicro's "DirectPass" password manager.

Gizmo's popular freeware rating and evaluation service, TechSupportAlert.com, has reviewed and rated many of the password managers and posted the results online at techsupportalert.com/best-free-web-form-filler-password-manager.htm. Gizmo gave its highest 10 Star rating and its "Best Product In Its Class"

cont'd on Page 11

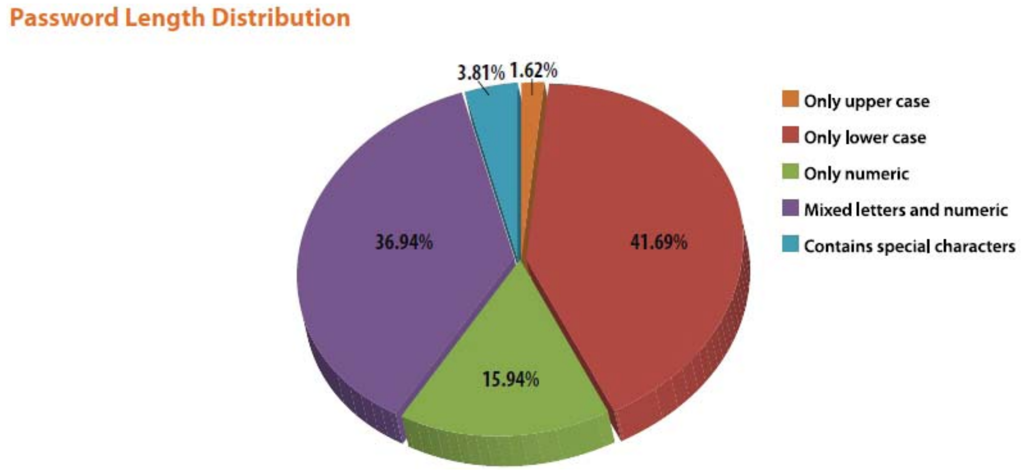
cont'd from Page 10

Secure your Passwords for Free

award to LastPass (lastpass.com), the password manager that I have been using for several years. LastPass can safely store passwords "in the cloud" using the same grade of encryption as used by the military (a concern of some users), is accessible from any computer or smart device, works automatically with almost all modern web browsers (Internet Explorer, Firefox, Chrome, Opera, and Safari), and runs on most major operating systems including Windows, MAC, and Linux. For most users, the totally free version of LastPass is feature rich and is totally satisfactory; for those who desire some additional features, including the portable version of LastPass for use on a variety of smart devices including iOS, Symbian, Blackberry, and Android, the premium version of LastPass is $12 per year. LastPass can automatically fill forms with username and password, fill in personal data on applications and delivery instructions, and provide a host of other services. LastPass will also intelligently capture newly created or changed usernames and passwords from each website visited. Personally, I have been totally satisfied with LastPass.

Gizmo also highly rated the limited free version of RoboForm (only tracks 10 to 30 passwords), and the totally free, unlimited use, password managers KeePass (keepass.info) and PasswordSafe (passwordsafe.sourceforge.net). The free unrestricted versions of LastPass, KeePass, or PasswordSafe will each securely store and manage an unlimited number of passwords. Each utility has some different features, as enumerated by Gizmo in the ratings. While all of these will perform a most satisfactory job managing passwords, my personal favorite in the group is still LastPass. One warning about any of the password managers, free or commercial; all of them require a password to access the database created by the user. Be absolutely sure to create a unique and complex password to open the password manager, and do not use this opening password in any other manner or on any other website! Using one of these password managers only requires that the user remember a single complex password, negating the excuse that there are too many passwords to remember when using a different password on each website. It would also be a good practice to frequently and regularly perform a security scan with a good quality third-party malware scanner such as MalwareBytes (malwarebytes.org) or SuperAntiSpyware (superantispyware.com) in order to verify that no keyloggers have infected the computer. If a keylogger is detected, it does not matter which, if any, password manager is used, it will become immediately necessary to change all of your passwords.

Creating and using strong and complex unique passwords for each website, and managing them with a good quality and secure password manager will dramatically help to improve our personal level of cyber security.



The Next Regular Meeting will be at
The Severn River Middle School

Wednesday
June 5th, 2013

Meeting will be held in the large meeting room.
It starts at 7:00 P.M. with club business
and a short discussion period.

You're invited to a presentation

on

Favorite User Utilities

by

Our Members

Members and their friends are welcome to come, ask questions and become enlightened.

How to Find: Severn River Middle School

SRMS is close to the Arnold, MD campus of the Anne Arundel Community College. From Annapolis and points south, take Rte 2 (Ritchie Highway) north about 3 miles from the intersection of Rt. 50, **turn right on College Parkway**. At the first light, turn left on Peninsula Farm Road. (Of course, if you are coming from points North, you would turn left onto College Parkway) about a half-mile down the road the large SRMS school building, set back off a large two level parking lot, will be visible on your right. Park here and go to the main entrance. Signs will be posted to direct you to the **Large Group Room** where we will be meeting.

How to find: The Technology SIG, A ChPCUG Special Interest Group**

The meetings are held at the SRMS in the Library.

The Chesapeake Area Technology Society

Chesapeake PC Users Group

1783 Forest Drive #285
Annapolis, MD 21401

FIRST CLASS

INSIDE THIS VERY ISSUE!

President's Corner
What's Your Computer Been Up To
Holy Cow! Is it a Virus?
Secure & Keep Track of Your Passwords
New IOBit Releases
.... and nothing more!

Note: *The date above your name on the mailing label is the expiration date of your membership. Contact the Membership Chairman (page 2, column 2) to update.*

Proudly Affiliated with

NASA FEDERAL CREDIT UNION
www.nasafcu.com

apcug