The Rochester Computer Society, Inc.
Founded 1982

MONITOR

Vol. 30, No. 3 March 2012

Next Meeting
Tuesday, March 13

Carl Schmidtmann and Charles Profitt
on Linux

Contents

More Free Utilities to Clean Hijacked PCs

by Ira Wilsker

Hardly a week goes by that I do not get a call from a friend or co-worker asking for help with a computer that had been hijacked by one of the thousands of variants of a type of malware generically known as "Rogue AntiVirus." Last weekend was busy for me in this respect in that I received multiple frantic calls for help on Friday, Saturday, and Sunday. All of the computers I was asked to clean had been totally hijacked by this rogue antivirus operating under the names "Vista AntiVirus 2012," "Windows 7 Antivirus," and "Microsoft Antivirus 2012."

While they all had different names, they all had the same modus operandi in that they infected a computer, displayed frequent popup windows alerting the user that the computer was heavily infected with viruses and spyware, offered to repair the problem for a fee, and totally took over the computer by not allowing most other programs to load. Often infecting the computer via an email from a known acquaintance whose own computer had been hijacked and which sent out spam email with a link that would load the malware, or by visiting a legitimate or rogue website that injects the malware via the web browser, this rogue antivirus software is becoming more dangerous, and more difficult to remove. As had been written here before, this rogue software generally protects itself from detection and removal by neutralizing the

installed security software on the computer, and preventing other detection and repair software from executing. Most of the rogue software also blocks access to many of the websites with removal utilities, and prevents most programs on the computer from running by blocking almost all ".exe" files from opening.

What the user of the infected machine does not often see is that many of these rogue variants also disseminate their code to people whose email addresses are in the user's address book (both webmail and computer based address books), Facebook and Twitter friends. This spamming of illicit code is typically in the form of friendly emails apparently from you to your email buddies with a short polite message along with a link to a purloined website which will automatically load the malware code onto their machines. Facebook and Twitter have also become major vectors used to promulgate this malware, as the rogue software will post short messages apparently from you, with links to the malware; anyone clicking on those links will be hijacked as well, and the process repeats geometrically. In addition to propagating itself, this rogue software also often adds the hijacked computers as "zombies" to a massive "bot" of computers used to send out spam emails for a fee, payable to the crook that started this spider web of malware and hijackings. In addition to the revenues from sending countless spam emails from the "bot" (network) of "zombies" (hijacked computers), the purveyors of this malware also generate substantial revenues by charging a fee, typically $29 to $69, often payable only by credit card, for the rogue software to "clean" the infected computer. If the unfortunate victim pays this extortion, not just will the rogue software not clean the computer, but will also often sell the credit card number (along with its expiration date, and CVV security code) on other illicit websites, typically resulting in massive fraudulent charges on the credit cards.

In the past, I have had great success using the free portable version of Super AntiSpyware (www.superantispyware.com) to detect and remove the rogue antivirus infections. Using a clean computer, I download a fresh, updated copy of the portable version of SuperAntiSpyware to my USB flash drive, which I then take to the hijacked computer. I boot the infected computer into Safe Mode (F8), insert the flash drive, and run the SuperAntiSpyware, often in "full scan" mode. Once cleaned, I use the "Repair" button on the bottom of the Super AntiSpyware screen to undo many of the improper changes the malware had made to the computer. Because of its very frequenting updating, ease of use, and high success rate, SuperAntiSpyware portable version is still my first choice to clean an infected computer. The problem is that in this very rapidly evolving cat-and-mouse game between the malware code writers, and the security software companies, some of the recently released malware has become harder to detect and kill. I found this out last Friday when my normal battery of top-rated and updated malware detection and removal utilities that I carry on my flash drive (SuperAntiSpyware, Emsisoft Emergency Kit, and MalwareBytes) were unable to totally remove a persistent infection on a heavily compromised computer.

Knowing that a "Plan B" was necessary to defeat this stubborn malware, I went home to download some other utilities that I have used in the past to remove stubborn malware that resisted the most common and popular methods of cleaning. I downloaded the latest versions of McAfee's Stinger, Kaspersky Rescue Disk, AVG Rescue CD, and Microsoft Standalone System Sweeper Beta. I downloaded the McAfee Stinger to my flash drive, and created fresh CDs with the Kaspersky, AVG, and Microsoft utilities. Be sure to implicitly follow the directions provided by these software companies for creating the bootable CDs or bootable USB flash drives necessary to load and run the utilities.

Returning to the location of the hijacked desktop computer, I booted it into safe mode (F8), inserted my flash drive and ran the McAfee Stinger. While McAfee Stinger detects far fewer types of malware than many of the other utilities, it does an excellent job in detecting and

killing some of the more stubborn infections, which it did on this victimized computer. After rebooting the computer, and rerunning the McAfee Stinger (it found no additional infections), there was very substantial improvement, but still some evidence of malware on the computer.

I inserted my newly created bootable Kaspersky Rescue CD into the drive, and was required to press the F12 key in order to boot the computer with the bootable CD (some computers require F10 or F2 in order to select a "boot from CD or flash drive" option). Since booting with a CD does not load the infected copy of Windows that is on the hard drive, but instead loads a clean operating system from the CD (usually some form of Linux or WinPE), the malware cannot load and protect itself from detection and removal. The Kaspersky Rescue CD detected and removed the remainder of the malware, proving itself as a very viable method of malware removal. I removed the Kaspersky CD and inserted the Microsoft System Sweeper bootable CD, and rebooted the computer (F12). This Microsoft CD, very capable in its own right, did not detect any other malware on this computer, corroborating the fact that the computer was most likely clean of all forms of malware. If I still had any other problems, I know from past experience that the AVG Rescue CD, bootable the same way as the other CDs, had some very capable detection and system repair utilities which are often necessary to recover a badly damaged computer, but in this particular case, it was not necessary.

This badly infected and compromised computer had one of the major commercial security suites installed, but was still penetrated by the rogue antivirus, a common occurrence in that the rogue software is very well written by experts in security penetration. Rather than reinstall and update his current security software, which was near its expiration and renewal date, this computer owner wanted a different security suite than the one he had, in the hope that it would better protect his computer. Whatever security software suite he would choose, it is absolutely imperative to install some comprehensive security suite immediately after cleaning the computer that had been hijacked, as the security software that was previously installed was totally dead, killed by the malware in the earliest stage of the takeover, which left the computer vulnerable to the inevitable follow-on attacks. While there are several excellent commercial and free comprehensive security suites available, in this case the user decided to try one of the popular freeware security suites, Outpost (free.agnitum.com), rather than purchase another commercial product; that was his informed choice.

Now, when I am called upon to clean an infected computer, I include McAfee Stinger in the arsenal of utilities on my USB flash drive, and bring the three bootable CDs that I created (Kaspersky, AVG, and Microsoft), just in case they are needed.

Websites:
http://www.mcafee.com/us/downloads/free-tools/how-to-use-stinger.aspx
http://support.kaspersky.com/viruses/rescuedisk?level=2
http://www.avg.com/us-en/avg-rescue-cd
https://connect.microsoft.com/systemsweeper
http://www.superantispyware.com
https://www.emsisoft.com/en/software/eek/
http://www.malwarebytes.org
http://free.agnitum.com

Do You "YouTube"?

by Elaine Szaniszlo
Editor, Northeast Ohio PC Club

I had always thought that YouTube was a site that had lots of fun videos. Well, it does, but read on!

I was on a trip recently and the fuses blew on the car power outlets. We needed to replace the fuses as our plug-in GPS would not work otherwise. Of course, everyone knows the fuse box is located under the dashboard, right? But did you know some cars have another fuse box under the hood? We found that out on youtube.com. We typed in the car make, model and year, and fuse box, and up came a very nice video showing where the fuses were in the engine compartment, how to get the cover off and showed there was a fuse puller included (a very useful tool, indeed!). Now we would never have known that.

A friend told me he was going to replace a garbage disposal. He went to YouTube. Again, there was a detailed video explaining how to do that. Other ambitious folks I know have used YouTube to get videos on repairing clothes washers, too.

I used YouTube once to get some cooking information, but never realized the wide scope of informative videos that was available. So the next time you want to solve a problem or get information on any do-it-yourself project, check out YouTube. It may make YOU happier.

From the December 2011 issue of Nybbles & Bytes*, newsletter of the Northeast Ohio PC Club,. Courtesy of APCUG.*

Manage Your Kindle eBooks

Q. I love my Kindle that I got this past Christmas. I've read a lot about it, but I can't figure out how to use something called collections. Can you explain that, Mr. M?

A If you store a lot of content on your Kindle, you can create collections to facilitate your ability to find books and articles faster. A collection is just a fancy-shmancy name for a category you create on your Kindle Home screen. You can then move your eBooks, audiobooks, and personal documents from the Home screen to the collections you create. To create a collection, click Menu > Create New Collection or select Create New Collection from the Home screen menu. Type in a name for your collection, then select Save using the 5-way controller.

To rename a collection, select the collection name as it appears on your Home screen, then move the 5-way controller to the right to display Collection Options. Select Rename and follow the on-screen instructions.

If you decide at some point to delete a collection, the process is virtually identical to renaming a collection, except instead of selecting Rename, select Delete, then again follow the on-screen instructions.

When you delete a collection, the content on your Kindle doesn't change. In other words, items previously added to a collection that are stored on your Kindle will appear on the Home screen after the collection itself is deleted, so you are not wiping out your purchased books in the process.

For lots of additional Kindle tips, "Mr. Modem's Top 50 Kindle Tips," Volumes 1 and 2, featuring 50 easy-to-understand, useful tips in each volume, is available at amazon.com /dp/B006OO3T6S or go to amazon.com and search for "Mr. Modem" to review my priceless eBook collection.

Q. What is the proper way to uninstall a program which will not budge using Add/Remove Programs in the Control Panel? Thank you, Mr. M.

A. Sometimes programs take up residence and like a bad house guest, won't take a hint when it's time to leave. (Are you paying attention, Uncle Rudy?) Whenever you want to uninstall

a program, the first thing to do is to look within the program itself to determine if it has its own uninstaller. So go to Start > Programs, highlight the program and if there is an uninstaller, it will display as a sub-menu that you can then click to execute. If it doesn't have its own uninstaller, then proceed to the Control Panel > Add/Remove Programs.

If that doesn't work, then Revo Uninstaller (www.revouninstaller .com) is a powerful uninstaller that will be able to evict your stubborn digital tenant. Revo is easy to use: Download then double-click to run it. A list of all installed programs will be displayed. You can then click to select whatever program you want to remove, press the REMOVE button, and it will be gone with the wind.

Q. I've been using Internet Explorer 8 since it came out and while I generally like it, it's getting awfully slow. I also have Firefox and I've been trying Google Chrome, which you mentioned was much faster. I don't mind abandoning IE, but I'd like to find out what's causing it to be so slow. Any ideas?

A. Add-ons are often the cause of IE sluggishness, particularly if everything else is running normally. You can check it out by going to Tools > Manage Add-ons. Check "Load Time" in the right-hand column and you will immediately know which browser extension is the offending culprit.

Mr. Modem's DME (Don't Miss 'Em) Sites of the Month

Causes.com

This site was founded on the belief that anyone can participate in change by informing and inspiring others. No, seriously The site provides tools for people to mobilize their friends for collective action, to spread the word to friends of friends and acquaintances, and eventually launch movements. Whether you are an activist who wants to protect baby asparagus or a nonprofit that promotes literacy, Causes .com can help you achieve your objectives and spread your message. Launched in 2007, today it has more than 170 million participants who have raised more than $40 million for more than 500,000 causes.

www.causes.com

Con-Artist Awareness

Courtesy of the State of Ohio Dept. of Commerce, you will find a great deal of practical information here that can help you avoid scams, cons, flim-flammers, and bamboozlers. Included are the articles, *What is Investment Fraud?*, *How to Spot a Con Artist*, *How to Check your Broker*, and a *File a Complaint* link. Though geared to Ohio residents, the information is excellent no matter where you reside.

http://conartist.ohio.gov

Modern Ruins

Elegant photography that contains starkly beautiful images of modern ruins, including abandoned factories, hospitals, orphanages, train yards, jails, mines and other architectural relics of recent history. If you're feeling upbeat and happy, but concerned that your life is lacking a sense of hopelessness and despair, this site will quickly remedy that situation.

http://oboylephoto.com/ruins

"Mr. Modem's Top 50 Computing Tips," and "Mr. Modem's Top 50 iPad Tips" are available on amazon.com. Each life-altering volume features 50 of Mr. M.'s all-time favorite tips.

Using Sandboxie to Safely Browse the Internet

(based on ver 3.60)

by Jim McKnight
Director, Los Angeles Computer Society, CA

General:

Once Sandboxie is set up, all you have to do is click the Sandboxie Icon on the desktop and your regular Internet Browser opens safely in a sandbox.

Sandboxie uses your regular Internet Browser to go on the Internet without the fear that you will be tricked into infecting your PC by malicious websites, or by infected downloads.

Although Sandboxie does some amazing things with many kinds of programs, this article focuses on using the Sandboxie program to make your Internet browsing safe from malware infections.

The tips in this article are for the FREE version of Sandboxie. The paid version offers many bells and whistles, but for safe Internet browsing, the FREE version is adequate.

Be aware that some programs do not play well with Sandboxie. For details, See: Http://www.sandboxie.com/index.php?knownconflicts

Nag Screen:

The only downside to the FREE version of Sandboxie is that 30 days after installation, a Nag screen pops up most every time you use it with a 5 second delay telling you that the Nag delay will go away permanently if you buy Sandboxie. (Currently about $42.00 for a lifetime license that works for all your PC's (as an Individual owner).

Help and Tutorials:

For an overview of what a sandbox is, go to the http://www .sandboxie .com home page.

Also see the Sandboxie Help pages at: http://www.sandboxie.com /index.php?HelpTopics

See this Tutorial video set (3 parts; About 20 min total). It is very good: http://www .securitytube.net/video/578

You can get to the 6-part "Getting Started" tutorial for the Sandboxie program at any time as follows: (Double-click the Sandboxie Control Icon on the Task bar > Help > Getting Started Tutorial)

Download And Install Sandboxie

You can download the Sandboxie program from: http://www .sandboxie.com

During the installation, you may be notified of software compatibility conflicts between Sandboxie and some other program/s. You will be asked to give permission to automatically change some configuration settings to fix it. Just click OK. Note: You can get to this screen anytime: (click Sandbox > Configure > Software Compatibility).

Setting up Sandboxie to "Auto-delete" Files:

By default, Sandboxie does NOT Auto-delete anything. Everything is saved in the sandbox until you delete it.

I highly recommend setting up Sandboxie to "Automatically delete contents of sandbox" when the sandboxed browser is closed. This will delete all browser changes, add-ons, downloads, and program installs (including malware) each time you close Sandboxie.

To set up Sandboxie to always Auto-Delete:

2) Double-click the Sandboxie Control Icon in the System Notification area.
3) In the Sandboxie window; (click Sandbox > Default Box > Sandbox Settings > Delete > Delete Invocation).
4) Click to check the box for _ Automatically delete contents of sandbox, and click OK.

NOTE: "Auto-delete" usually does not include manually downloaded files. They are kept in the sandbox until you manually either Recover them or Delete them.

Manually Delete Everything in the Sandbox:

Double-click the "Sandboxie Control" system tray Icon, then; (click Sandbox > Default Box >Delete Contents) Close the Sandboxie Control window.

Save (Recover) Downloaded Files:

Sandboxie offers you the opportunity to save "for real" any downloaded files both after you download the file and when you close the browser. If you do not save them, they disappear when you close Sandboxie (but by default stay in the sandbox for you to recover or delete later). Saving for real is called Quick Recovery.

Each time you download files to the Desktop, you are usually (but not always) prompted to "Quick Recover" that file (save for real).

If you download files to anywhere other than the Desktop, you will NOT be prompted for "Quick Recovery". Later, you can get to the Quick Recovery (save for real) screen by double-clicking the Sandboxie Control Icon in the notification area, then select (Sandbox >Default Box > Quick Recovery). Click on the desired Item/s (to highlight them), then click either "Recover to Same Folder" or "Recover to Any Folder."

Last resort: If you are still having trouble saving a file "for real" AND if you trust the download website AND if you trust the file: Close sandboxie, browse to that site without Sandboxie, and download your file. Scan it for malware before using.

Exploring Downloaded Files

It is best to explore downloaded files that are in the sandbox by using the "Sandboxed" version of Windows Explorer:

1) Open the Sandboxie Control program by double-clicking its Icon in the System Tray.
2) Click (Sandbox > Default Box > Run Sandboxed > Run Windows Explorer) .

Now as you explore the system using Windows Explorer in sandboxed mode, you will see your downloaded and sandboxed files right alongside regular files in the same folder where you downloaded them. This can be confusing so hang in there.

Check Downloaded Files for Malware

There are two ways to scan downloaded files for malware:

1) You can get to the file using the sandboxed Windows Explorer shown above, then right-click the file and run your normal Anti-malware program scan on it to make sure it is safe before "Saving it for real."
2) Everything that is sandboxed is actually hidden in a folder called C:\Sandbox. Your antivirus scanner can be run against that folder and will inspect all the files in it for malware. It should then be safe to save those downloaded files "for real."

How Do You Know If You Are Running in the Sandbox?

Two ways:

Look for # (pound signs) before and after the Browser's name in the Title Bar. Hover the mouse pointer near the top of the active browser window. If you are running in the sandbox, the window frame will be outlined in a YELLOW border.

Making E-mail Links Open in a Sandboxed Browser:

My preferred way is to first open your default browser in the sandbox. Then if you click any links in your e-mail, they will open in the sandboxed browser.

If the default browser is not already open in the sandbox when you click an e-mail link, then the link will open the default browser WITHOUT being sandboxed.

Run a Different Browser "Sandboxed"

The sandboxie icon (free version) always uses the system's "default" browser. You cannot specify different browsers for the Sandboxie "Sandboxed Web Browser" Icon. (The paid version of Sandboxie has more flexibility).

If you want to use a different browser with Sandboxie, you have two choices:

1. Right-click the desired browser Icon (Context Menu), then select "Run Sandboxed".

Note: Depending on your Operating System, the context menu option for Sandboxie may not show up. (ie: Quick launch Icons or the Start Menu Favorites Icons). It does always work with the Desktop Icons.

2. Change the Default browser:
   a Close the sandboxed browser.
   b. Change the default browsing program to the one you desire. The method varies for different operating systems.
   c. Double-click the Sandboxie "Sandboxed Web Browser" Icon. The new browser should now open.

Changes to the Browser:

With Auto-Delete turned ON, Sandboxie will NOT save your Browsing History or any added Bookmarks, or any other changes to the Browser when Sandboxie closes.

With Auto-Delete turned OFF, your Browser changes will be remembered, but only within the Sandboxie browsing session. If you open the Browser without Sandboxie, the changes will not be visible.

Permanent Changes:

Any Browser customizations such as (Add-ons, Favorites, Bookmarks, Toolbars, etc.) that you want to be permanently changed in your Browser must be installed by opening the Browser WITHOUT using Sandboxie, and then making the changes. Otherwise, any changes you make will be sandboxed and will disappear.

PRINTING: Yes, you can print stuff as usual from your Browser (even PDF's from the sandboxed Adobe Reader).

Browser Is Slow to Close:

This is normal from time to time. Make sure there are no open windows hidden behind the main browser window awaiting user action.

Desktop "Internet" Shortcut Icons:

If you like to use various different browsers to go on the internet, be aware that your regular Desktop Internet Browser Icons do NOT use Sandboxie to open them. To create new Desktop Internet Icons that WILL use Sandboxie to open a specific Browser program, try this: Open the Sandboxie Control program by double-clicking its Icon in the System Tray. Click (Configure > Windows Shell Integration > click the "Add Shortcut Icons" button.).

Click OK a couple times until you get to the window titled "Sandboxie Start Menu Default box" and select "Desktop".

Click to highlight the desktop Icon you want to duplicate. The new Icon will immediately appear on the Desktop.

Be sure to rename each Icon after you create it. This is so Sandboxie will not overwrite it when you create another Icon.

www.sandboxie.com

From the December 2011 issue of User Friendly*, newsletter of the Los Angeles Computer Society, CA.* Courtesy of APCUG.

Free Flash Games

Part I: Introduction and DinoRun

by Robert Spotswood
North Orange County Computer Club, CA

Introduction

Flash is a browser plug-in available for free from Adobe. Somewhat oversimplified, it is a mini operating system that runs in your web browser, be it Firefox, Opera, Safari, Chrome, or Internet Explorer. It allows you to run programs written for Flash. These programs range from simple slide-shows, to videos with sound. One thing Flash is used for is games, a large number of them free.

Although there are a large number of free games available, some are better than others. There are many different categories of games, and which ones will appeal to you depends on your tastes. In this series, I will introduce you a few of the better ones I've found, IMHO. However, this list is far from complete. Don't be afraid to try some other ones. Just don't blame me for all the time you waste playing them.

Getting Flash

Chances are you already have Flash installed in your web browser. However, even if you do, you should make sure you have the latest version. One of several criticisms of Flash is that vulnerabilities have allowed the compromise of the user's computer simply by viewing a specially crafted web page. There is no reason to think such vulnerabilities will not be found in the future.

In order to check you Flash version, simply visit Adobe'sS Flash site. It will tell you your installed version, and, a little further down the page, will tell the latest version. There is a link on that page to the download page if your version is out of date, or you lack Flash altogether. You may have to restart your browser after, or during, the Flash installation.

Now that you've got Flash, on to the games!

Dino Run

Journey back to an earlier time, at time so far back, even the graphics are pixelated. You are a small, but really tough, dinosaur. A meteor has just struck the Earth. A shock wave wall of doom is headed your way, killing everything in it's path. You must run for your life and reach a place of safety.

Dino Run is an real-time action/sports racing game, although quick reflexes are not necessary to win. In Dino Run, you are racing the clock so speak. It's G rated and suitable for all ages. Along the way, you will encounter smaller, edible creatures and eggs. Eat the small creatures and save the eggs to gain points to upgrade your dinosaur. Upgrades include enhanced speed, acceleration, jumping, and strength.

You will need all of these as there are many obstacles along the way to overcome to reach safety. There are pits to jump over, mountains to climb, canyons to cross, lakes to swim and more. In addition to the landscape obstacles, there are also larger dinosaurs too. Some of the larger creatures can help you reach safety, while some will hinder you.

The standard challenge is a series of runs. Each run has a start and a finish. Reach the finish line before the wall of doom catches you to get to move on to the next run. The number of runs in the standard challenge varies depending on the difficulty level. The easy level has the fewest, while medium and hard have one more than easy, while impossible features a final run that has the Bronto superegg, and is the only place to find that egg.

Even within a given difficulty level, the individual runs have some randomness to them, so while certain features will appear in a particular run, the exact place it appears, if at all, will vary. You must complete a run for any achievements and points, called DNA, to be saved. If

the wall of doom catches you, everything you've done since starting that particular run is lost. Achievements and DNA from previous runs are not lost, and you can always try again.

In addition to the standard challenge, there are 21 speed runs to unlock. The first 20 of these runs are special mixes of one of the challenge runs, but with a twist. For instance, the ptero storm speed run features lots of pterodactyls. This is a great run for trying to get the dactyl chain award. If you complete all of the speed runs, except for Planet 0, at a difficulty level of medium or higher, you will get a crown for your dinosaur. Complete all runs at medium or higher and get a bronze crown, hard or higher gets you a silver crown, and finish all the runs at impossible level and you get a gold crown.

In order to unlock a speed run, except for Planet 0, you must spend some bones, the currency of Dino Run. You get bones by eating small critters or by bumping off larger dinosaurs. You do not get bones from normal eggs, but save a super egg and you will. You also get bones, and sometimes DNA from achieving certain milestones. The in game instructions lists the milestones.

The many flash games have no memory. When you close your browser, or the tab the game is running in, all progress is lost. Dino Run is an exception. It saves your progress after every successful run. It will take many sessions to get a gold crown, and all the gold awards. Dino Run can be found at several places around the web, including Pixeljam or the more reliable Clockwork Monster. Remember that your progress saving is site specific, so if you switch sites, you start over. To help you achieve the gold awards, here are some tips:

- The only thing that can kill you is the wall of doom. Lots of other things can slow you down so the wall catches up with you, but nothing else can otherwise harm you. So go ahead, jump off that cliff! You never know what you will find at the bottom.
- There are lots of little hidden areas, so don't be afraid to explore a little. A few places actually require you to turn around to find things. Just don't take too long. The wall of doom is still coming.
- Until you get a few advancements, keep the level at easy. This has the slowest wall of doom. While there are fewer opportunities to gain DNA at the easy level, any you do gain still counts just as much as the DNA you get at the impossible level. Super Eggs and milestones give the exact same rewards at easy levels as they do at impossible. However, some Super Eggs are not available in the easy challenge.
- The brown dactyls can climb faster than you can. Hitch a ride whenever you can, especially when climbing mountains. If fact, you can not beat the twin peaks at hard and impossible without a ride. Lots of them actually.
- You can not harm the red dactyls, nor can you hitch a ride with them. All you can do is dodge them. If you have super strength, they can not bother you.
- You can ride the yellow duckbills, even make them jump, but they will buck you off after a short ride. You can not bump them off, even with super strength.
- Of all the upgrades, strength is the least important. Even at level 5, you do not have the strength to bump off the stegos and triceratops, although you can make them turn around. A high strength will help you with boulders, so it's still useful.
- At medium or higher difficulty levels, the challenge apocalypse run has 3 places of safety. One requires a high strength to reach. However, you should skip the first two places at the impossible level.

Conclusion

Flash games can be lots of fun, and with so many of them available for free, you have little excuse to be bored. So far, you've met only one of the many free ones out there on the Internet, just waiting to be played. In part 2 of this series, you be introduced to a game that'll really bug you. See you then!

Your Digital Afterlife is an NPR transcript from the Program *Fresh Air*. It is a discussion about what will/can happen to our "stuff" when we die? Do our families get access to our email, previous photos, or financial data? Are there things we'd prefer nobody see?

The article is too long for this publication but, if you're interested, it can be found in the November issue of the TUGNET newsletter.www.tugnet.org

Is ActiveX Evil?

by Bob Rankin
askbobrankin@weber.org

Is It Safe to Use ActiveX Controls?

Let's start with a definition... ActiveX is a Microsoft programming framework that was introduced to Windows and Internet Explorer in 1996. Although it is often referred to as a programming or scripting language, ActiveX is more accurately defined as a set of rules established by Microsoft that govern how applications written in other languages share information. In Internet Explorer, ActiveX serves a function similar to Java, but without Java's security safeguards.

An ActiveX control (sometimes called an add-on) is a set of instructions that, when installed on a computer, enable specific actions. For example, an ActiveX control developed by Adobe Systems enables Internet Explorer to display Flash, Acrobat, and other types of multimedia content. Some online games require the use of ActiveX controls. Microsoft uses ActiveX controls to install security updates via Microsoft Update.

Typically, an ActiveX control is downloaded through Internet Explorer the first time it is needed; that is, the first time content that requires the ActiveX control is encountered by Internet Explorer. ActiveX controls may be thought of as plugins or addons for the IE browser.

The problem is that ActiveX allows a program to make unrestricted changes to the user's computer. An ActiveX control can enable a rogue program to delete, modify, transmit, or do anything else to data discovered on the computer. In fact, ActiveX can enable hackers to take full control of a PC! That's obviously a problem from a security stand-point.

It's important to note that ActiveX is a Windows-only critter, and is specific to the Internet Explorer browser. Websites that require ActiveX will not work on Linux or Mac systems. Firefox and Google Chrome do not support ActiveX technology for these reasons. But you can install the "IE Tab" extension, which enables Firefox or Chrome to use ActiveX extensions by interfacing with Internet Explorer.

Will You Sign This For Me?

Microsoft addressed this issue by establishing a registration system for ActiveX controls though "signing authorities" such as Verisign. Authors of ActiveX controls are supposed to register their controls and add a digital signature that can verify that the author is who it claims to be.

Some websites require that you download and install an ActiveX control in order to view the content. When this happens, Internet Explorer will ask if you want to proceed. In theory, it should be safe to let IE download and install signed ActiveX controls. But in truth, a signature just means that the author is identified. It says nothing about what the ActiveX control may do to your computer. If you know and trust the control's author (say, Microsoft or Adobe

Systems), that's fine. But if a verified author is "Joe Blow Software," you really don't know any more than an unsigned control tells you.

Making things more confusing, there are harmless ActiveX controls whose authors don't bother to get them signed. This is common with ActiveX controls developed in-house for corporate intranets. If you encounter one of these, your help desk or IT support should advise you how to proceed.

It's possible to disable ActiveX, but you lose a lot of functionality in Internet Explorer and other components of Windows. Even Microsoft Office employs ActiveX, so I would not recommend disabling it.

So, to your question "Is ActiveX Evil?" I have to say no. Personally, I've never encountered a malicious ActiveX control in the past 15 years since they came on the scene. But there are no guarantees with ActiveX controls. The better question is whether or not you should allow IE to install an ActiveX control. The best guidance I can give you is to carefully consider the source of any ActiveX control. If the Web site offering the control is one you trust, and the control is signed, then it's probably safe. If it's a game or widget on some site you've never visited before, I'd skip it.

Cleaning Your Screen

by Cal Esneault

Cajun Clickers Computer Club Member

Originally, computer monitors were CRT tubes with a glass viewing area. To clean these screens, methods typical for window glass could be used. Today however, flat-panel LCD displays are made of plastic, are flexible, and usually have a surface coating. They are easily scratched or damaged. The use of harsh window cleaners can permanently damage them. Although not everyone agrees on the same techniques, following are a few guidelines to consider.

First, remove any dirt or dust with a soft brush to prevent them from becoming abrasive grit during subsequent steps. Second, use a treated microfiber cloth sold at computer or camera stores (or the Internet) to gently wipe out any smudges. Be sure to routinely clean your cloth with soap and water, and then let it dry to refresh its oil absorbing ability. Optionally, you can use soft cloth pre-wetted with mild soap and water, but this has more risk. Special lens-cleaning pens are available from camera accessory suppliers which have special oil-absorbing carbon granules embedded in a micro-fiber tip.

For extreme cases, such as long-term build-up of a film from smoke or other air-borne contamination, you can get a special cleaning solution or make one yourself by diluting isopropyl alcohol (70% solution of rubbing alcohol found at a drugstore) 50/50 with water. Be sure to turn the power off to the monitor when using any liquids, and put the liquid onto the cleaning cloth first.

The above also applies to smart phones which are even more of a problem due to the multi-touch control method which requires touching the screen with our fingers. You should review as much information as possible before cleaning any visual display surfaces. There is always a risk of damage and there are no guarantees since results depend upon the device and the exact technique used.

From the November 2011 issue of the newsletter of TUGNET, The Users Group Network of Granada Hills, CA.

Buried within the code of OpenOffice.org's Calc program is a favorite game from days gone by – Space Invaders. If you're interested in a stroll down memory lane here's all you have to know:

=GAME("StarWars")

Place this formula in a cell in the spreadsheet, being sure to pay attention to capitalization and spacing, and hit the enter key. The game will open. The text is in German but do you really need directions for Space Invaders?

Sadly, the game appears to have been eliminated from LibreOffice so those of us who "upgraded" are SOL. If you still have the original Open Office, enjoy!

How to Sell Your Products on the Web

by Bob Rankin

You don't have to build your own online store from scratch in order to sell your handmade goods or other unwanted items. The various tasks required - registering and hosting a domain, graphic design, website creation, installing and configuring a shopping cart - are daunting for most people. But fortunately, many online venues exist to help you advertise and sell your stuff with a minimum of investment and hassle.

eBay is the prototypical online marketplace. It makes selling as easy as taking pictures and writing a description of an item. Originally a pure auction site, eBay now pushes fixed-price listings. eBay gives you a worldwide marketplace, but it's one of the pricier ways to sell online. You pay a listing fee whether your item sells or not, plus a percentage of the selling price. You even get dinged on shipping fees because eBay wants to encourage sellers to offer "free" shipping. Every eBay listing must offer Paypal as a payment option (although other options can be included), and Paypal takes a cut of whatever money you receive through it.

eBay has hundreds of lesser-known imitators in the auction arena, such as Ubid.com, WeBidz.com, and others. You'll find auction sites that offer lower fees (and smaller audiences), product-specialized auction marketplaces, and geographically organized auction sites.

In contrast, Craigslist charges nothing. It's basically free classified advertising in dozens of local markets. Craigslist is great if you want fast cash; just advertise, meet with a responding buyer, hand over the goods and pocket the money. But be careful! Always meet in a public place, like a police station parking lot. Don't accept checks from strangers. I would encourage you to read Scammed on Craigslist! before you engage in this marketplace.

Other Options for Selling Online

Gazelle actually buys your used electronics, then sells them through other venues. Gazelle buys used cell phones, cameras, camcorders, GPS devices, gaming consoles, laptops, tablets, video games and other gadgets. You may get less money from Gazelle than if you sold the item yourself, but many people don't want to search for a buyer or haggle over the price. A few months ago, I sold my 2-year-old Motorola Droid smartphone through Gazelle, and was happy to get $35 for it. At least it's not sitting in a drawer now.

If you've come up with a blockbuster idea for a graphic design, there are sites that will help you sell it on shirts, hats, coffee cups, calendars, mouse pads and other items. CafePress, Zazzle, VistaPrint are a few examples. Upload your design, pick the product(s) on which it will appear, and set your price. You can set up your own online shop within these sites, and list multiple items for sale. When an item is purchased, the company produces it on demand and then ships it directly to the customer. They deduct the wholesale cost of your shirt, mug, etc., and send you the balance.

The beauty of this type of online store is that you don't have to manufacture the items, or even ship them. You also avoid the hassle of collecting payment, which would involve getting a merchant account to accept credit cards. Merchant accounts can be expensive, requiring you to pay both upfront and monthly service fees.

High-volume sellers are often found on Amazon.com, offering new and used items at prices that may beat Amazon's own. Etsy is a site for crafters who want to peddle their handmade jewelry, clothing, ceramics, and similar handicrafts.

Of course, if you're a techy (or willing to learn) you can register your own .COM domain, put up a website, take payments by credit card, and handle order fulfillment on your own. You might want to check out my articles on *How to Buy a Domain Name* and *Inexpensive Website Design* for some pointers if you're a do-it-yourselfer.

But for most people who are interested in selling their own designs or hand-made items, one of the full-service options mentioned earlier in this article will be the best and easiest route to selling your stuff online.

From the December 2011 issue of Nybbles & Bytes*, newsletter of the Northeast Ohio PC Club.*

Windows 7 Has it All

by Vinny LaBash
Columnist, Sarasota PCUG, FL

OK, maybe Windows 7 doesn't have everything, but it has many great features that make your computer experience easier, safer, and more reliable than any previous version. Windows 7 is different enough to make obsolete much of your ideas about why you need third party utilities.

You don't need a separate disk partitioning utility anymore. Windows 7 does an excellent job even though it is not a complete disk portioning package. The vast majority of people sitting at a keyboard simply don't need more than what Windows 7 provides, and Windows will not mess up your disk drive. If you are running a dual boot system with multiple operating systems, Windows 7 won't measure up, but those folks comprise a small fraction of one percent of the computer community.

The only drawback to Window 7 partition manager is finding it. Click on the *Start Orb*, select *Control Panel*, open *Administrative Tools*, and double click on *Computer Management*. Wait a few seconds for Windows to gather information, and when the *Computer Management* window appears, click *Disk Management* located under the *Storage* heading.

If you are not sure of what to do, click the Help icon. It looks like a question mark on a blue background. The help section will guide you through any disk management task including troubleshooting. The partitioning tool won't be of much help if your disk drive is too full because you won't be able to keep and move files during partitioning. The obvious solution is to clean out your disk before partitioning. Unless you are a computer professional, you probably don't need a third party program for portioning your drives. With today's disk drive technology, you may not need to partition at all.

In the *Accessories* folder open the *System Tools* folder, and then select *Disk Defragmenter*. The dialog box on the screen displays the defrag schedule, the last time the disk(s) were defragged, and the degree of defragmentation on all your disk drives. If you have an SSD drive, Windows 7 will not defrag it which is a good thing.

Defragging reorganizes data so the operating system can retrieve information quickly without having to reassemble files that may be broken into pieces and stored in separate disk areas. Only highly defragmented disks will show any noticeable operational slowdown. There is great controversy in the computer community about the value of defragging your disks, making the purchase of an outside program of dubious value. Windows 7 defrag tool is all you need.

At last Windows has an engine that performs search operations quickly and efficiently. Most search programs outside of Microsoft came about because Vista search routines often resembled someone

rummaging around in a dark room with their eyes closed, and then coming up empty. Indexing now works properly in the background without bringing your system to a crawl. There is no longer any need for third party services.

Registry cleaners may have been useful, even necessary with XP and Vista, but happily that is no longer true. The Windows Registry is a giant data base on your hard drive where Windows makes records of information it may need in the future. The Registry contains important information that Windows requires about system settings, user profiles, applications, and hardware among other things.

Vendors who sell registry cleaners are fond of pointing out that your registry gradually becomes out-of-date with invalid information because of everyday actions like removing applications, changing drive letters or simply moving or copying files. These errors gradually accumulate and corrupt the data base causing everything from a slowdown to a complete system crash. To take care of these problems and avoid having them in the future all you need to do is buy their PC registry cleaner. Hogwash, I say!

A registry cleaner is the most useless and potentially the most dangerous program you can install. Most of them do nothing to reduce the size of the registry, which might result in a slightly faster PC, but only slightly. If you removed a program last year, and the registry still contains a pointer that no longer points to anything, you can remove it, but why take the time, trouble, and effort? There is no longer any action associated with the pointer, and it's completely harmless.

People may disagree, but registry cleaners have become infamous for trashing systems. Be cautious with sites that invite you to perform a free Registry cleaning, and then claim you have been the victim of some kind of mal-ware. Ponder, if you will, that Microsoft has stopped using its own registry cleaners, but has remained mysteriously quiet about the reasons why.

Windows has had a firewall capability since XP was introduced. In Windows 7 the firewall is straightforward and works well at keeping mal-ware out. Some critics say it's inadequate because it works inbound only. Is an outbound firewall necessary? When an unauthorized program tries to send data out of your computer, an outbound firewall alerts you. That's the idea, but reality is far different. Many outbound firewalls give incessant alerts usually with indecipherable warnings. When you track them down it's almost always some obscure Windows service attempting to complete an operation. When the annoyance becomes unbearable, people turn off the outbound half of the firewall, totally defeating its purpose. In practice, an outbound firewall turns out to be severe overkill, and it can easily be defeated by a sophisticated mal-ware program.

Windows Firewall is present in every Windows 7 installation, is thoroughly integrated with the operating system, works well, doesn't cost extra, and is turned on by default. Use it and don't pay for a "full function" firewall that in all probability you don't need.

You can make Windows 7 work better, but not by buying superfluous utilities. Get a faster internet connection or a more reliable one. Take the money you saved by not buying unneeded software and get a 24" monitor for a real "WOW" experience. Another good use for saved cash would be an SSD primary drive for true blazing performance. An ergonomic keyboard and mouse wouldn't hurt either.

From the December 2011 issue of the Sarasota Monitor*, newsletter of the SPCUG organization in Sarasota, FL.*

Gizmo's Freeware:

Keep Tabs On How Much Data Your PC Downloads and Uploads

One of the most useful software tools that you can have on your computer is something that tells you how much information you upload to, and download from, the internet over a specific time period. And, of course, how fast those transfers are taking place.

Here's a little program that can help you achieve all this. It's easy to use, free, and available in a portable version so there's nothing to install. Just download it, run it, then delete it if you don't intend to use it again.

http://www.techsupportalert.com/content/keep-tabs-how-much-data-your-pc-downloads-and-uploads.htm

Free PDF Conversion and Online Virus Scanning Sites Now Provide Increased Limits

Here are two unexpected bonuses for all PC users. First, our favorite free online virus scanning service has increased the maximum file size you can scan from 20 to 32 MB. Second, one of the best free online PDF to Word conversion services is now offering a free downloadable version that has no file size constraints at all. Go get it!

http://www.techsupportalert.com/content/pdf-conversion-and-online-virus-scanning-increased-limits.htm

Society News

February 14, 2012

Our Valentine's Day treat was an evening with Nick Francesco. It was a laid back, chatty, evening to commemorate the founding of the Frog Computer Society in 1982. One member who was present, Art Trimble, was also present at the creation! How great was that?

Nick is rarely at a loss for something amusing to say and he was aided by many questions from the floor. It was an informative as well as a pleasant evening. There were cookies, too.

[We don't have Jan Rothfuss' usual play by play because Dan was under the weather. They really regretted missing the evening.]

The Lighter Side

Once upon a time a tech support was giving instructions to a caller, but the caller's son was the one physically sitting at the computer, so all the instructions had to be relayed. Here's a snippet of the conversation:

Tech: "Click on 'start', then select 'shut down', then select 'restart in MS-DOS mode'."

Customer (to his son): "Ok, press 'start', 'shut up', and 'sit down'!"

The really scary part was what his son said then:

Customer's Son: "Ok, I'm at the C: prompt!"

Do we really want to know what goes on at that house?

- Tech Support: "Ok, we need to set up an icon for that program. To do that, I need to get you to your Program Manager--"
- Customer: "Program manager? Why?!?"
- Tech Support: "I can't put an icon up for you to click on if you don't go to your Program Manager."
- Customer: "Hell! I don't even know who my immediate manager is, much less my program manager!"

An obviously distraught student entered the school's IT office complaining that his email wasn't working. His attempts to get tickets for an on-campus concert kept resulting in returned emails.

He showed the tech the email address he was attempting to reach. The tech asked him where he obtained such an unusual email address.

The student replied, "It was on the sign advertising the concert, it said, 'begins@7:30PM'."