

Security and Your Business



Newsletter # 6 – October, 2008

Welcome to the Archimedes Technologies, LLC Security Newsletter. As a Trend Micro Partner, Archimedes Technologies has access to analysis of the latest threats to your business. From time-to-time we will send a newsletter on security threats of concern. The purpose of our newsletter is to inform and educate you of the threats to your business.

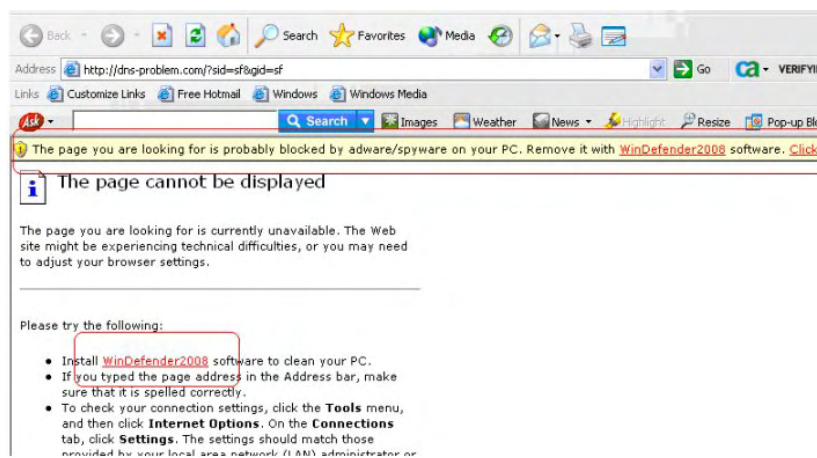
In this edition of our newsletter we discuss the new fake Anti-virus scams and eco-friendly recycling.

Fake Anti-Virus Programs Hit 30 Million PCs

Win Defender and Google Fakes

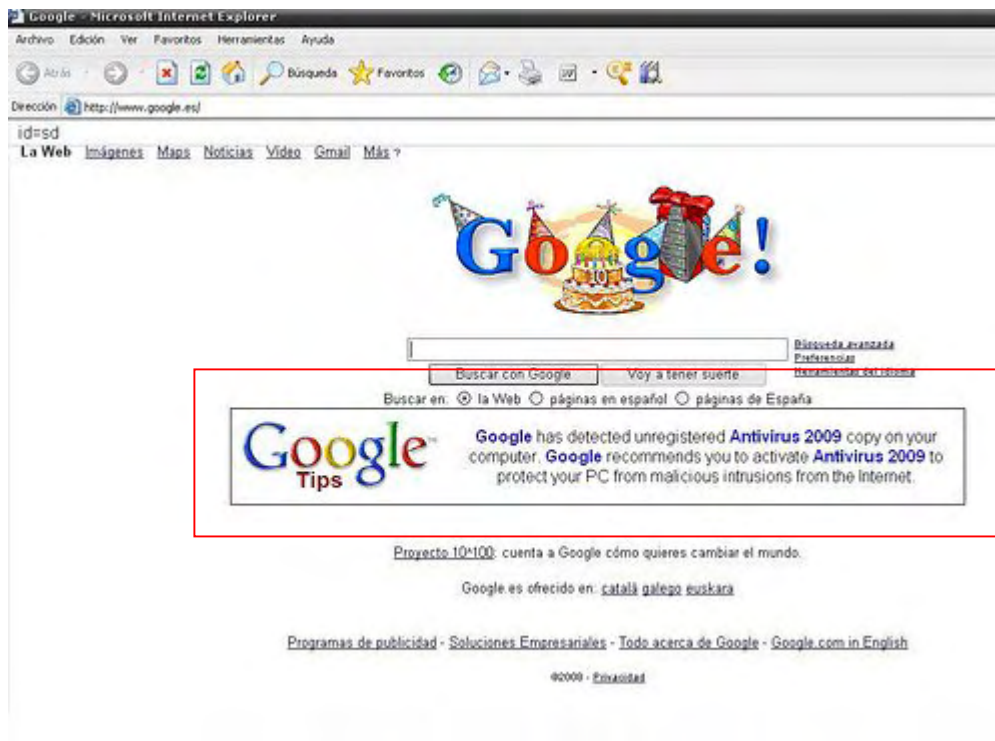
It seems pretty obvious when you get a fake anti-virus warning. It is a product you didn't buy, didn't want and haven't paid for. So why do these thieves continue to try to place fake anti-virus programs on your PC? The answer is simple – money, a lot of money. Panda Labs has published its estimate of fake anti-virus programs installed at 30 million PCs. The report goes on to say that 3% of the people encountering these programs provide a credit card to get rid of the error messages. Quick math: at \$49.95 a copy, that comes to \$44,955,000. That does not include the expense of what happens to your credit card after it goes to these thieves.

The programs are being loaded through infected web sites or social engineering. One example of this is below:



The yellow warning bar is trying to load an active-x control through your browser. The user has gone to a regular web site that was hacked to load the active-x control. It blocks access to the page through a browser redirect and then tells you that you're probably infected. WinDefender2008 (and there is already a 2009) then runs and tells you all of these infections (that don't exist) and for \$49.95 it will get rid of them for you. They use the name WinDefender because Microsoft has an actual program called Windows Defender that is shipped with Vista and is a Genuine Advantage load for XP. We have already encountered this infection. The good news is that it is fairly easy to remove; the bad news is that it is fairly easy to get infected. One mouse click is all it takes and your PC can not do anything but display fake virus warnings.

Most people use Google for searches and normally Google pages have been pretty trust worthy. Thieves know that and can now exploit it. Take a look at our next example:



Click the "Google Tip" and get infected. Google is not in the business of checking to see if you have registered software on your machine.

To give you an idea of how widespread this problem has become, we have provided a list of names of the more prominent fakes below.

- [Advanced Cleaner](#)^[5]
- [AlfaCleaner](#)
- [AntiSpyCheck 2.1](#)
- [AntiSpyStorm](#)
- [AntiSpywareExpert](#)
- [AntiSpywareMaster](#)
- [AntiSpywareSuite](#)
- [Antivermins](#)
- [Antivirgear](#)
- [Antivirus 2008](#)
- [Antivirus 2009](#)
- [AntiVirus Gold](#)^[6]
- [Antivirus Master](#)
- [Antivirus XP 2008](#)^[7]
- [Avatod Antispyware 8.0](#)^[8]
- [Awola](#)
- [Brave Sentry](#)
- [BestsellerAntivirus](#)
- [Cleanator](#)
- [ContraVirus](#)
- [Doctor Antivirus](#)
- [DriveCleaner](#)^[9]
- [Disk Knight](#)
- [EasySpywareCleaner](#)
- [Errorsafe](#)
- [free-viruscan.com](#)
- [IE Antivirus](#)
- [IEDefender](#)
- [InfeStop](#)
- [Internet Antivirus](#)
- [KVMSecure](#)
- [MacSweeper](#)
- [MalCrush 3.7](#)
- [MalwareCore](#)
- [MalwareAlarm](#)
- [Malware Bell 3.2](#)
- [MS Antivirus](#)
- [MS Antispyware](#)
- [PCSecureSystem](#)^[10]
- [PC Antispy](#)^[11]
- [PC Clean Pro](#)^[12]
- [PC SpeedScan Pro](#)
- [PestTrap](#)^[13]
- [Perfect Cleaner](#)
- [PersonalAntiSpy Free](#)
- [PAL Spyware Remover](#)
- [PCPrivacytool](#)
- [PC-Antispyware](#)
- [PSGuard](#)
- [Saliar](#)
- [SecurePCCleaner](#)
- [Security toolbar 7.1](#)
- [Smart Antivirus 2008](#)
- [Smart Antivirus 2009](#)
- [SpyAxe](#)^[14]
- [Spy Away](#)
- [SpyCrush](#)
- [Spydawn](#)^[15]
- [SpyGuarder](#)
- [SpyHeal](#)
- [Spylocked](#)^[16]
- [SpySheriff](#)^[17]
- [SpySpotter](#)
- [Spyware Cleaner](#)
- [Spyware Quake](#)^[18]
- [Spyware Stormer](#)
- [SpywareStrike](#)
- [Spy-Rid](#)
- [SpyWiper](#)
- [System anti virus 2008](#)
- [System Live Protect](#)^[19]
- [SystemDoctor](#)
- [Total Secure 2009](#)
- [TrustedAntivirus](#)
- [TheSpyBot](#)
- [UltimateCleaner](#)
- [VirusHeat](#)
- [Virus Isolator](#)
- [VirusProtectPro](#)
- [VirusRanger](#)
- [Virus Response Lab 2009](#)
- [Vista Antivirus 2008](#)
- [WinAntiVirus Pro 2006](#)
- [WinFixer](#)^[20]
- [WinSpywareProtect](#)
- [WorldAntiSpy](#)
- [XP Antivirus](#)
- [XP AntiSpyware 2009](#)
- [Zinaps AntiSpyware 2008](#)

Our customers running Trend Micro are protected from a number of these. Trend Micro maintains a list of web sites that are tested upon request to see if they have been hacked. The Trend Secure toolbar will then provide a visual indication of a problem on a web site. Our usual warnings should be applied. If you don't know what it is, don't click it.

Recycling

The rules have changed - Electronic Waste Management Act

New Jersey has changed its recycling rules. Although the majority of the Act (concerning electronic waste management, and amending P.L.1987, c.102, and supplementing Title 13 of the Revised Statutes) concerns manufacturers, there are changes that impact consumers and small business owners. A covered electronic device is now defined as "a desktop or personal computer, computer monitor, portable computer, or television sold to a consumer." I'll summarize the 15 pages for you – you can't throw it away anymore. According to "C.13:1E-99.109 Used covered electronic device, disposal as solid waste prohibited. 16. On and after January 1, 2010, no person shall knowingly dispose of a used covered electronic device, or any of the components or subassemblies thereof, as solid waste."

So what do you do with all those old PC's, monitors, UPS batteries, printers and other electronics? The information on recycling is a little scatter shot. To assist you we have assembled a list for you to work with. This web site from the State of New Jersey lists recycling programs by county:

http://www.nj.gov/dep/dshw/recycling/Electronic_Waste/Residential.htm for residential recycling. Normally, for a small charge, non-profit and for-profit organizations will take electronic waste on certain days within a county.

Businesses must work with other recycling firms. Below is a list of the firms from the NJ DEP website.

SOLID AND HAZARDOUS WASTE CONSUMER ELECTRONICS RECYCLING FACILITIES

Updated October, 2008

These facilities are approved to demanufacture consumer electronics

Name	Address	Contact	Phone	Web Site
Back thru the Future Computer Recycling, Inc.	150 Main Street Ogdensburg, NJ 07439	Dan Bayha	(973) 823-9752	www.backthruthefuture.com
Ecoglass	1950 Rutgers University Blvd. Lakewood, NJ 08701	Maria Boufarah	(732)730-2880	N/A
Federal Prison Industries	Building 5713 Ft. Dix, NJ 08640	Jeff Eobstel	(609) 723-1100 ext. 348	www.unicor.gov
HessTech, LLC	45 Executive Avenue Edison, NJ 08817	Mr. David Zimet	(732) 287-2442	www.hesstech.com
Lynswell Technologies	602 North 10th Street Camden, NJ 08102	Shyang J. Lin	856-365-1711	www.lynswell.com
Monmouth Wire	3230 Shafto Road Tinton Falls, NJ 07753	Sal Massaro	(732) 922-3320	www.computerreclamation.com
NewTech Recycling, Inc.	600A Apgar Drive Somerset, NJ 08873	Mr. James Entwistle	(732)469-9774	www.newtechrecycling.com
Supreme Computer Wholesale, Inc.	1950 Rutgers University Blvd. Lakewood, NJ 08701	Al Boufarah	(732) 370-4100	www.supremerecycling.com

THE FOLLOWING FACILITIES ACCEPT COMPUTERS AND MONITORS FOR REFURBISHING AND RESALE OR DONATION

Name	Address	Contact	Phone	Web Site
AnthingIT, Inc.	17-09 Zink Place Fair Lawn, NJ 07410	David Bernstein	(201)475-7300	www.anythingit.com
PlanITROI	88 Ford Road Denville, NJ 07834	Paul Nickerson	(973) 664-0700 x.105	www.planitroi.com

The web site appears to be updated monthly and can be found here:

<http://www.nj.gov/dep/dshw/lrm/uwaste/ucomplist.htm>.

A word of warning before recycling your old PC's: disk drives still have data on them when that machine is recycled. Although the PC may no longer function, the hard drive may be just fine. In order to protect your business and personal information the drive should either be destroyed (we like the hammer-to-the-disk-platter method) or wiped using DOD approved software. If you have any doubt about the information on a PC call us and we will be happy to help you in protecting your data.

One final recycling note: Staples is operating a program in conjunction with APC. For a recycling fee of \$10 you can bring in your old UPS and they will recycle the unit and the batteries. This is a published program, so we put it to the test. Of course, no one at Staples knew what we were talking about. However, after pointing out they have a published "eco easy" program (and a few phone calls later) the unit was recycled.

If Archimedes Technologies, LLC replaces the batteries on your UPS system, we will return the old batteries to our supplier. Our supplier has not started charging for used batteries when we purchase a replacement set. This will probably change over-time but for now, free is good.

In The NEWS

HR 5938 Signed into law

We mentioned Hr 5938 in Newsletter #5. The Identity Theft Enforcement and Restitution Act of 2008 was signed into law on September 26th. This act pertains to cyber-extortion and the victims' right to monetary damages.

N.J. Voting Machines

UPI reported on October 18th that New Jersey voting machines can be hacked using simple tools. According to computer expert Andrew Appel at Princeton University it takes about 7 minutes to hack a New Jersey voting machine. New Jersey has its own series of experts to dispute the 158 page report. Our only comment on the matter – It is a computer, isn't it?

PRODUCT NEWS

Netgear's new Prosafe 802.11n Dual Band Wireless Gigabit Firewall



Netgear has started to ship their new wireless firewall, the SRXN3205. This new N band firewall carries the Prosafe label, which means it has a lifetime warranty. What makes this unit unique is the dual-band 5Ghz and 2.4Ghz radio spectrum. 5Ghz to get above interference and 2.4Ghz to make it backward compatible for existing wireless network cards. The unit will work with 802.11b, 802.11 g or 802.11n devices. The four wired ports are all gigabit Ethernet. This unit is perfect for the remote branch office that requires a firewall, VPN connection and wireless access. We just purchased this unit for our office and will be testing it over the next few weeks. Please remember Archimedes Technologies, LLC for all your networking needs. Our pricing is aggressive and we have the expertise to perform the installation for you.

XP is Dead... January 2009 – Dell Changes XP Downgrade pricing to \$99

Dell has assured us that we will be able to purchase PCs with XP Pro until at least January 31st, 2009. For an additional \$99 Dell will include Vista disks and drivers with your XP Pro business PC. This provides upgrade protection while allowing your business to operate as usual. Microsoft will support XP through April 8th, 2014 but mainstream support, meaning bug fixes, will end April 14th, 2009. Only Microsoft Enterprise Support clients will get XP support through 2014.

Contact us

Please contact us to discuss your security requirements. We can be reached on the web at Info@archimedestech.com or at 973-845-6027.

If you would prefer not to receive mail from Archimedes Technologies, LLC please click here and send the mail. [Remove Me](#).