

## Security and Your Business



Newsletter # 7 – November, 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 web page hijacking and Trend Micro Worry Free Security.

### Tis The Season To Be Wary

Allrecipes.com, Expedia.com, Fox News, Windows Live ads hacked

It's the holiday season and you want that perfect turkey. Allrecipes.com looks like a good place to start. Well, normally it is, but of late there is some bad malware out there waiting for you. As Anti-virus products get more sophisticated it is harder to infect your machine -- unless you ask for it.

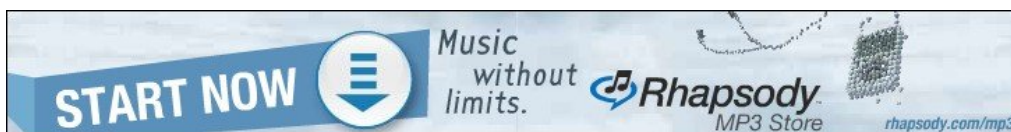


Click this banner ad and you are infected. How does this work? How can the web sites not know about this? A little explanation of web sites is necessary. The ads that pop on these sites are not controlled by the web site. They are usually provided by third party providers under contract. These providers may not check the ads as well or as often as they should. It redirects to the bad web site using Java script or exploiting a bug in Flash (the little movie player on web pages). When you look into the actual code it is quite clear that the redirect exists. The redirection goes to one of these sites:

premium-pc-scan.com  
antivirus-pc-scan.com  
securityfullscan.com  
antivirus-live-scan.com  
updateyourprotection.com  
antivirus-premiumscan.com  
securitylivescan.com  
security-full-scan.com  
secured-liveupdate.com  
livepcupdate.com  
protection-update.com  
antivirus-scan-online.com  
go-scan-pro.com  
internet-antivirus-2008.com  
ia-stat-ia.com  
ia-scanner-pro.com  
ia-scanner-pro.com  
ia-scanpro.com  
ia-scannerpro.com  
online-antivirus.net  
virus-scan-online.com  
online-virus-scanning.com  
scanner-protection.com  
xpas2009.com

This is a partial list. These sites literally change on a daily basis.

Looking for that perfect trip for the holidays? This banner will not get you there. This ad was recently seen on Expedia.

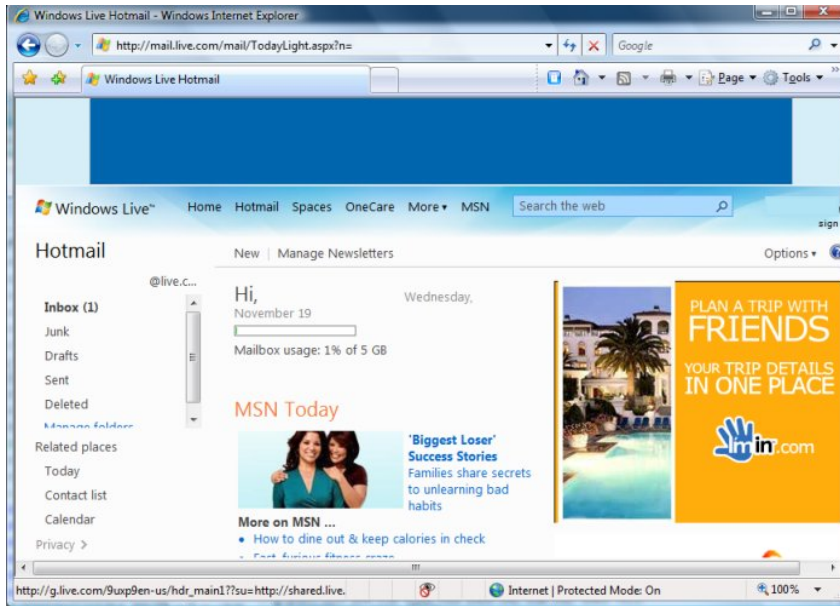


Rhapsody is a valid company but this ad redirects to Anti-Virus 2009 a nasty Trojan that will display false positives until you either 1) give them a credit card, or 2) call us to come fix it.

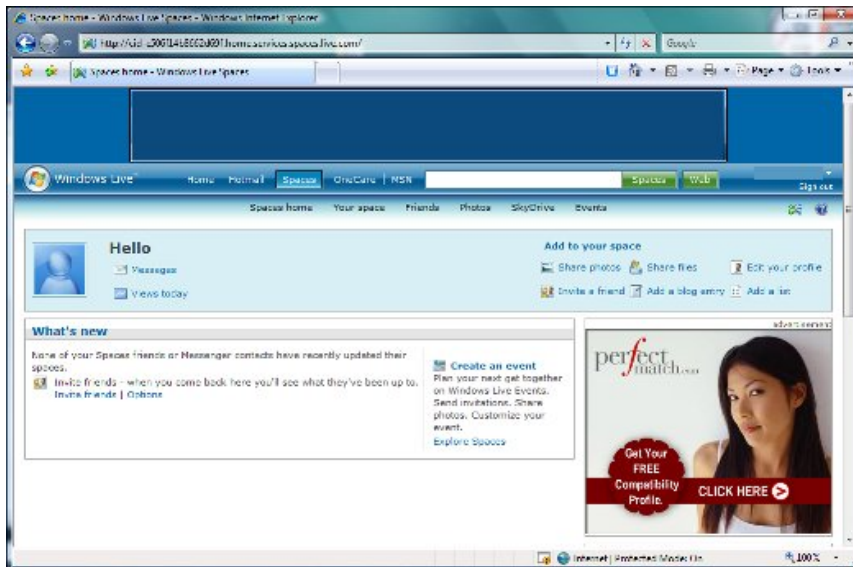
This ad was displayed on Fox Interactive. Other iterations of this ad have appeared on Expedia.



We're not done yet. You would think that Windows Live would be clean right? Not if you click the banner looking for that perfect trip.



Or click looking for the perfect mate on Perfect Match:



The good news is that we have seen Anti-Virus 2009 (and the older 2008) so often now that we can clean it out in an hour. We are often asked why the PC anti-virus software is not stopping this. It actually is but not before certain settings are changed on the PC. Trend Micro will quarantine the following before they activate:

```
c:\WINDOWS\system32\ieupdates.exe
c:\WINDOWS\system32\winsrc.dll
c:\Program Files\Antivirus 2009\av2009.exe
```

By the time the Anti-Virus quarantines the programs it has already changed the screen saver, screen background, added files to the registry to auto start on reboot (the reason it doesn't go away) and

added a Browser Helper Object. Since the infecting programs change so often, anti-virus providers are playing catch-up. The infected machines are actually just displaying a small program that is just eating processor cycles. The program appears below:



It doesn't really scan anything. It just eats up the processor on the PC slowing down everything to the point where you can't type or click. The program that displays is not actually the virus. The actual virus files are the ones already quarantined.

The people behind this are known to authorities but cannot be prosecuted. Here is a little malware economics. The people that are programming this Trojan are in Russia. The first thing the program does is check the infected PC's IP address. If the IP address is in Russia they remove all traces of the program from the PC. Doing this prevents the Russian authorities from prosecuting because they have not committed a crime on Russian soil. They sell the rights to the program on a subscription basis and get paid every time someone uses a credit card. They claim they cannot control how people use their software... Nice.... Let's do the math. Microsoft publishes infected machines on their malware blog currently at 548,218 for this type of infection for November in the US (<http://blogs.technet.com/mmpc/archive/2008/11/19/msrt-review-on-win32-fakesecsen-rogues.aspx>).

The normal response rate of for banner ads is 1%. 1% of 548,218 is 5,482 times \$49.99 = \$274,045, PER-MONTH. Malware is big business.

## Trend Micro Updates Worry Free Security 5.0

New Patch Issued

Trend Micro has issued a major patch release for Worry Free Security 5.0. This patch converts the Trend release to 5.1. This patch prepares the way for Small business Server 2008 and Essential Business Server 2008. It also incorporates an enhanced Security Engine. We have already rolled out this patch to our server and it is running without an issue. If you are one of our Trend Micro customers we will be in touch to arrange installation of this patch.

### In The NEWS

#### Facebook wins \$873 million dollar judgment against spammers

Facebook sued a Canadian citizen under the 2003 Can-Spam act and won a judgment of \$873 million. While it is doubtful they will ever collect, it is nice to see that the culprits can be prosecuted.

### PRODUCT NEWS

#### Dell offers a Black Friday Notebook Special

Dell is trying to capture the Black Friday computer specials with a \$349 notebook special. The [Vostro A860](#) is the lower-end Dell notebook, but it may be perfect for a young student. We recommend that if you decide to buy the Vostro you also get the extended warranty. Although this is a nice laptop for the money, the Vostro category is not made the same way as the Latitude notebooks. If purchased for that young student you should consider also getting the Accidental Damage Service.

#### Last Chance for XP... 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 31<sup>st</sup>, 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 8<sup>th</sup>, 2014 but mainstream support, meaning bug fixes, will end April 14<sup>th</sup>, 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](mailto: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](#).