

Security and Your Business



Newsletter # 8 – February, 2009

Welcome to the Archimedes Technologies, LLC Security Newsletter. As you can see we have a new logo, but the same great service. We do not advertise our services and we are proud to say that almost every one of our clients has come from a satisfied customer. Our entire corporate concept is to provide a level of service you can't get from our competitors. If we aren't meeting that goal we want to know about it. In a down economy having IT support you can depend on to reduce down-time and a company that really cares about your business is invaluable. Please consider recommending us to your colleagues.

Archimedes Technologies is sending this newsletter to discuss some serious new threats to your business. Right now we have 4 PC's in the office that are receiving a total rebuild. They were infected by Anti-Virus 2009 (a fake anti-virus program) and outdated virus protection.

Google Poisoning

Fake Flash player infects PC's

Trend Micro has reported 400,000 query results on Google video are being redirected to a single site that infects PCs through a false Flash Player. The player, FlashPlayer.v3.181.exe is actually a Worm. The Worm gets into the Internet temporary files directory and executes a fake Adobe Flash Downloader and then removes itself. The downloader then places itself on every hard drive and removable drive on the system, edits the systems registry and sets itself to autorun on every drive when the drive is referenced. Updated Trend Micro pattern files will detect this Worm. We are bringing this to your attention because your home PCs may let this slip through.

If you use Google for videos and are requested to download a Flash Player go to the program bar at the bottom of the screen and right click on each window and click Close. Then do an immediate scan of your system. The only legitimate location to load a flash player is:

<http://www.adobe.com/products/flashplayer/>.

Fake Ant-Virus 2009 and it's variants

This program keeps getting worse

We've written about this program before but it has become much worse. We are seeing program variants hijack the PC Desktop and activate the Active-Desktop. Active Desktop was made to display web pages as your desktop background. You can find it by right clicking on a blank spot on your Desktop, click properties, click the desktop tab, click customize and then the web tab. The infected page displayed is a big flashing warning that you've been infected. When the active desktop displays the fake warning your IP address has already been sent to the infected web site. The virus removes the Web tab from the desktop customization window through the registry so that you can't remove the new background. Then the virus opens Internet Explorer pages to an infected web site. We have seen this infection 5 times this week, 4 of the machines are totally inoperable, gone, toast, foot warmers. The one machine that survived was protected by Trend Micro Worry Free Security 5.0. The screen was changed but no executable part of the virus was able to run, and it was up and running clean in 20 minutes.

When a machine is infected, a downloader component is activated. The scope of the download is new to this type of infection. We have pulled over 300 Trojans files off the machines in the Windows/System32 directory. A fake Red Alert appears in the system tray as a red circle with an X through it. Alert windows pop up on the screen looking like a Windows Security Alert using the Microsoft Windows 2000 Update Icon asking you to scan. Click any part of the window and you are directed to a Fake Anti-Virus site. The downloader component is what is making this almost impossible to clean out. Since so many Programs and DLL's have been downloaded and set to start automatically through the registry, that when you clean a set out there is another set to start. The processes are not only randomly named but also named close to Microsoft processes. One example is the NTFS program. NTFS is the format of the disk drive not a process, but most people would think it is legitimate since it has a fake Microsoft author in its properties and they probably recall something by that name.

Repair becomes an exercise in economics: 2 hours to rebuild the operating system or 2 days to clean it off and repair the operating system. We have been successful in stopping enough of the processes to get local data off the PC's but the disturbing part of cleaning this virus are that the registry is becoming corrupted by cleaning the infection. Upon restart to the normal start up screen we start receiving many Windows operating system component failures. This is by far the worst infection we have seen and the first where we recommend a complete rebuild of the operating system.

The only warnings we can provide is that if any unexpected window opens on your machine with a virus or spyware warning right click it on the task bar and click close. Close all your data windows immediately and start an anti-virus scan.

Times are Tough and Coupons look great

Until you load one

Adware Coupons are becoming more prevalent. The bad guys listen to the news too and they craft their adware to entice you to click. Last week was a tough week for our users; the coupon software that looks

so enticing is actually a Trojan redirector. It is a pretty smart redirector. Search Google and you will receive the proper search results and for the first few times you will be able to go to a search result. After a few searches the redirector kicks in and any search result you click will be redirected to a shopping web site. We were unable to determine if the web site is infected, but we didn't receive the usual warnings. This looks like a scam to generate revenue through referrals.

Shopping web sites either pay by click or commission to web sites that direct traffic to them. If you would like to see an example of this performed for good works please go to <http://www.igive.com/>. This web site donates the money it receives for referrals. I shop through iGive to donate money to schools. What is eye opening is how much money is generated by these referrals. If you click here <http://www.igive.com/html/merchantlist2.cfm> for the merchant list you can see that a virus that generates millions of redirections to merchant web sites can generate a lot of money for the bad guys.

If you want a legitimate coupon, consider the iGive web site. Not only will they keep you up to date on what coupons are offered but you can direct your donation to a local cause without costing you a dime.

In The NEWS

Microsoft Announces Retail Chain

Windows 7 is coming and Microsoft has announced it will be opening a retail chain of stores to take advantage of selling the new operating system. Having hired an ex-Walmart executive to run the chain it appears that Microsoft may be taking a bite out of the Apple store concept.

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](#).