

Frank Caperton

To: frank@myrsc.org
Subject: Tidbits from Frank the Computer Guy, July, 2009

Data Services of Tennessee

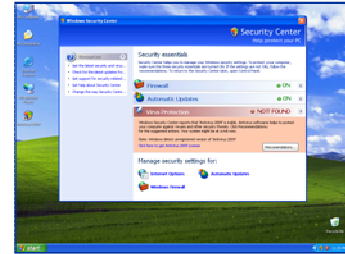
"It's What's on the Inside that Counts"

Frank Caperton 615.476.7823 frank@dstninc.com Murfreesboro, Tennessee

Got Spyware or Malware or Rogueware?

I have seen this little pop-up pictured on the right several times in the past three or four months. He's not really a virus but he sure makes you think so.

He might be named **Antivirus 2009**, **XP Antivirus**, **XP Antivirus 2009** – there's a whole bunch of names. I recently saw what looked like a shield on the desktop of a system. It was named AV360. They are all part of a not-so-necessarily family of malware called '**rogueware**'.




Rogueware looks like a legitimate program that will help you rid your computer of viruses, spyware, malware, ex-spouses and the IRS. Usually it will offer to scan your computer for free or perhaps some other 'special offer'.

Rogueware, like viruses and spyware more often than not are downloaded innocently from download sites such as Kazaa and Limewire or even by mistyping a website address (my favorite example is 'www.newchannel5.com' without the 's' after 'new').

Viruses are annoying and even destructive but lately I've been seeing malware. What is malware? Malware is a contraction of '**malicious software**' designed to infiltrate or damage your computer! I'm not going into a detailed synopsis of malware but let's just say malware can ruin your day.

These little programs get on your computer and start 'monitoring' your Internet viewing habits, i.e. they track your Internet behavior and relays this information to advertisers. Many programs claim they can prevent your computer from contracting spyware/rogueware/malware but I tend to disagree. But don't give up hope—here are a few things I do to 'keep its head down...

1. Go to www.dstninc.com and click the Malware Bytes icon located at the bottom of the page to download Malware Bytes:
2. Be certain to save the file someplace you can find it such as your desktop.
3. Now double-click  on or a file named 'mbam-setup'.
4. This is what I see next: Go ahead and left-click on 'Run'.



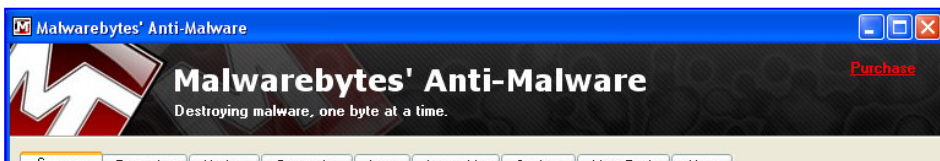
- From here on it's pretty much left-click on 'OK' or 'Next' or 'Accept Agreement' stuff. Those of you whom have been around me for several decades know my thinking—just click on something positive. At the end you will click, uh, 'Finish'. Go ahead and allow Malwarebytes to update. Shouldn't take more than a few seconds depending on the speed of your Internet connection.
- Now comes the hard part: Left-click on 'Scan'. That's it. Now sit back and relax for the next five minutes or so.



- When Malwarebytes is finished you will see the following screen: What we are looking for is 'Objects infected:' Next left-click on 'Show Results'.



- Almost done! Left-click on 'Removed Selected'.

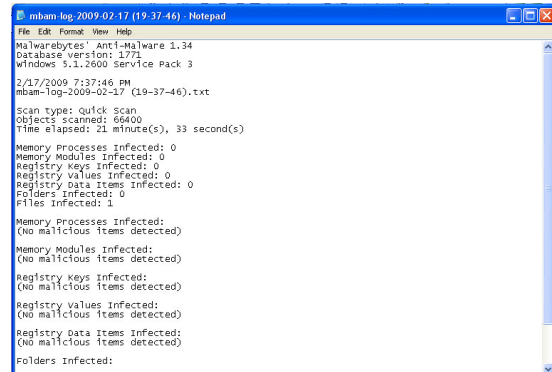


9. Next you will see a log of the 'stuff' you just cleaned up. Simply left-click the X in the upper-right hand corner.

10. You will left-click on an 'OK' box then exit.

That's about it. I run Malwarebytes about once a month. Between Malwarebytes and Mozilla Firefox I hardly see Viruses, spyware and malware on my systems.

I'm certain I left something out so if you get stuck simply Give me a shout should any questions arise!



```
mbam-log-2009-02-17 (19:37:46) - Notepad
File Edit Format View Help
Malwarebytes' Anti-Malware 1.34
Database version: 1771
Windows 5.1.2600 Service Pack 3

2/17/2009 7:37:46 PM
mbam-log-2009-02-17 (19-37-46).txt

Scan type: quick scan
Objects scanned: 66400
Time elapsed: 21 minute(s), 33 second(s)

Memory Processes Infected: 0
Memory Modules Infected: 0
Registry Keys Infected: 0
Registry Values Infected: 0
Registry Data Items Infected: 0
Folders Infected: 0
Files Infected: 1

Memory Processes Infected:
(No malicious items detected)
Memory Modules Infected:
(No malicious items detected)
Registry Keys Infected:
(No malicious items detected)
Registry Values Infected:
(No malicious items detected)
Registry Data Items Infected:
(No malicious items detected)
Folders Infected:
```



Frank Caperton
Data Services of Tennessee
P.O. Box 10187
Murfreesboro, TN 37129
615.476.7823
www.dstninc.com