Subject: Generic worm BAF + BAG
Posted by puddle_splasher on Thu, 19 Apr 2007 05:58:14 GMT
View Forum Message <> Reply to Message

My wife has 2 worms that have been quarantined by AVG. Generic worm BAF + BAG.

Both are isolated but unhealable.

I googled the worm and ended up at the Sophos website, followed the repair to the letter but the worm is still there.

Where in the registery will I find the worm? Do I use "regedit"?

Something is causing major lag, unopenable anti-virus and I.E. to freeze.

Virus scans are clean as are spyware. Both have been run in safe mode. As soon as you go back to normal then the above faults still exist.

O.S. is XP-pro.

Subject: Re: Generic worm BAF + BAG
Posted by Jerad2142 on Thu, 03 May 2007 17:04:23 GMT
View Forum Message <> Reply to Message

Sometimes the best thing to do is just press that F10 (or F11) Key on start up and start over.

Subject: Re: Generic worm BAF + BAG
Posted by Ryu on Fri, 04 May 2007 16:51:46 GMT
View Forum Message <> Reply to Message

Puddle, The worm could be stopped by deleting it's registry entry's, Also, Start >> Run >> msconfig >> Startup tab, and take it off her start up. (assuming it's her pc.)

AVG is by far the worst anti-virus iv'e seen, Use Norton or Nod32.

If you add me on msn (in my profile) I could give you more assistance. Or just format her pc.

Subject: Re: Generic worm BAF + BAG
Posted by AmunRa on Fri, 04 May 2007 17:57:30 GMT
View Forum Message <> Reply to Message

Norton = sux
nod32 = <3

Subject: Re: Generic worm BAF + BAG
Posted by CarrierII on Fri, 04 May 2007 18:45:56 GMT
View Forum Message <> Reply to Message

Norton provides reasonable protection at far too much of a cost in terms of startup time and proceser time that it nicks, not to mention you can uninstall Norton, use the "Norton removal tool", reinstall windows (Repair install) and it's still there!

Subject: Re: Generic worm BAF + BAG
Posted by Ryu on Sat, 05 May 2007 15:19:48 GMT
View Forum Message <> Reply to Message

Yeah, But Norton defends your pc from basic attacks, Unlike AVG.

I do recommend Nod32 more, tho.

Subject: Re: Generic worm BAF + BAG
Posted by puddle_splasher on Mon, 07 May 2007 08:05:39 GMT
View Forum Message <> Reply to Message

Sophos found it and repaired the worm.

Can someone supply a link "how to reformat Windows XP" when the OS was pre-installed?

System restore would not work on any date, probably due to the nature of the worm. Its purpose is to attack anti-virus programmes.

For the moment it seems that her PC is safe. It took a few attempts in DOS with Sophos to attain the results.

Thanks for the help, all that replied.

ps. It was not in the start-up folder @ msconfig and I could not find it in the registry. Possibly because I did not know where to look.