

Re: Black,Blue,andBlack again

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-05/msg00098.html>

- *From:* Hazyday <Hazyday@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 8 May 2006 11:51:02 -0700
-

my system has crashed the same way, with the cursorthing and then locking up, then me rebooting more times than I can count. It's always rebooted , until this occurrence.

This happened again last night on the second HD I have. I rebooted and checked the Event Viewer\Applications, and this is what i found;
True Vector engine: File C:\WINDOWS\Internet logs\Owner-AODE24686.ldb was corrupt and has been copied to "C:\Windows\Internet logs\xDBA.tmp".
File C:\Windows\Internet logs\Owner-AODE24686.ldb was corrupt and has been deleted.

interestingly, i found the following when i did a Google search for IAMDB.RDB. This is from the etrust Pest Patrol knowledge base (pest patrol included in EZ Armor suite) ;iamdb.rdb

Size:
172544
Our Filedate:

PVT:
-1799437066

MD5:
c9bc987cf2bfa5c7638da83ebc786fb1

About this Pest...

Score:
0*

PestName:
Ghost Keylogger
Description:

Category:
Key Logger.

Author:
[Sureshot]

Release Date:
7/7/2004

*A score of 0-5 is considered "safe", 6-14 "suspicious", and 15+ "dangerous." If no score is provided, this file has not yet been rated.

Found this at:<http://www.oldschoolfragging.com/news.php>
Zone Alarm is spying on you&& email to someone | printer friendly

Re: Black,Blue,andBlack again

I dont trust Microsoft's Lame Software Firewall in Service Pack 2 but it turns out the alternatives don't get much better!

Interesting article about how Zone Alarm is spying on you&&

Internet, Web, E-mail security update.

Regular readers will know that we take Internet, web and e-mail security seriously and have always used ZoneAlarm, Norton Anti-virus and AdSubtract. This way in the past we have been able to stop our computers from being attacked and infected. BUT.

Things change.

The other day we were going over one of our computers and found in the Windows Internet Logs folder a file that we had never seen before and was growing at an alarming rate. We used all our skills and knowledge to delete it and stop it from working. We eventually tracked this growing file down to belonging to ZoneAlarm. If you use ZoneAlarm then look at the 'IAMDB.RDB' and there is even a back up for it there as well. Wonderful we say.

After browsing the web to see if anybody else knew anything about this file we found this:

"It seems that ZA comes with two spy dlls that according to the their manufacturer "utilizes its patented metering methodology to measure actual Internet and digital media audience user behaviour in real-time – click-by-click, page-by-page, second-by-second."

I found these two:

C:WINDOWSSYSTEMVSMONAPI.DLL
C:WINDOWSSYSTEMVSUTIL.DLL

Had been left on my system after uninstalling ZA. It seems that your system configuration and maybe the activity is logged to the file Iamdb.rdb, then transmitted. This discussion also implicates Steve Gibson of Grc/ShieldsUp/Opout in this as well."

These were new to us but we knew that some program or other was continually accessing the web while our computers were on but as ZoneAlarm did not say it was anything suspicious and we just assumed it was one of our security programs checking for a new version or whatever we did not worry much, as one would.

But it did annoy us that it seemed to be going on continually and should not. Thus we started searching to find out what was happening and why which is why we found the IAMDB.RDB file and that it was growing at an alarming rate. There always was a ZoneAlarm file in the past that grew but that was easy to replace every-so-often with a blank file. But not this.

Re: Black,Blue,andBlack again

Re: Black,Blue,andBlack again

Bear in mind that we use the paid for Pro version and not the free version that one might expect some checking which would be reasonable, but not if you have been a loyal paying customer for years.

Thus we have e-mailed ZoneAlarm twice now and eventually got an automated reply back saying they will get in touch with us in a couple of days. We have told them in no uncertain words that we will publish our findings as this policy of ZoneAlarm spying on peoples computers is totally unacceptable.

We have now tried using another firewall software called Sygate Personal Firewall which is free. There is a paid for version but as you can appreciate at first we are trying the free version to see what we think of it and to see if it works.

Well. Now we have a free firewall blocking the spying activities of a paid for firewall. Can you believe that. We can also say that the Sygate Firewall is working and stopping ZoneAlarm from phoning home all the time with our private and confidential computer use data.

Here is the web site link for Sygate which is part of Symantec.

We are just very pleased that we are now blocking ZoneAlarm but it makes our blood boil.

We hope you find our compact review helpful to you along with all our independent reviews of computer hardware.

What to read more?: <http://www.theinquirer.net/?article=29157>
Perhaps my best bet is to get another firewall. I know that millions of people use either EZ Armor, various eTrust firewalls, and Zone alarm, (all of which use the True Vector engine), and many don't have the "crashing " problem. Many do , however, as evidenced by the google searh.
So, is it the firewall, or is it my pc?

TrueVector engine: File "C:\WINDOWS\Internet Logs\IAMDB.RDB" was corrupt, restoring from backup "C:\WINDOWS\Internet Logs\BACKUP.RDB

TrueVector engine File "C:\WINDOWS\Internet Logs\IAMDB.RDB" was corrupt and has been copied to "C:\WINDOWS\Internet Logs\xDB5.tmp". File "C:\WINDOWS\Internet Logs\IAMDB.RDB" was corrupt and has been deleted.
I have EZ Armor firewall, which uses the True Vector engine made by Zone Alarm. I contacted Computer Associates (they distribute EZ Armor) and they had me download an updated version of the True Vector engine, installed that, same problem, so I posted on Zonelabs Forum, and a tech there told me to uninstall, clean all files up, and install again.

—

HazydayXP

Re: Black,Blue,andBlack again

"Malke" wrote:

Elendil wrote:

What did the blue screen with text say? I think you're infected with some degree of a smitfraud so go to the Special Malware Removal page of my website: www.stopmalware.tk and follow the instructions for SmitFraud.

"Hazyday" <Hazyday@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:1918D0BE-3184-4BD3-AEE7-4028F68D2AA3@xxxxxxxxxxxxxxxxxxxx

I was on this site this morning to checking a reply, I went to move my cursor and got 3 or 4 bold lines next to the cursor and my system froze. I rebooted, signed in and my screen went black, then a quick flash of a blue screen with text, and back to black in a blink, then rebooted on it's own, so I tried to boot into safe mode on both mine and administrator accounts with the same result. I just finished a clean install of XP Home with SP2 on that drive Thursday! To say that i am fit to be tied is an utter understatement. Since purchasing the XP Home with Sp2, I have had to do repair and clean installs at least 6 times! That's since Dec. 2005. fortunately, I have 2 HD's, so I'm using the backup now. I haven't done anything with the primary (crashed) drive, just praying that I don't have to do yet another install. Any suggestions? I have spent the last 4 days trying to keep this system running. I have an AMD Sempron 3100+ with a gig of ddr sdram pc2700, a

Re: Black,Blue,andBlack again

gigabyte motherboard with award bios from 2005.

Although it is possible that the OP is infected if he does not practice Safe Hex, it sounds far more likely that all these issues are hardware-related. If the machine works fine with the replacement hard drive and not the other one, then the other hard drive is probably failing. If the machine does not work well with the replacement hard drive, then I would definitely do other hardware testing such as RAM and power supply tests. Here are some general hardware troubleshooting steps:

[http://www.elephantboycomputers.com/page2.html#Hardware Troubleshooting](http://www.elephantboycomputers.com/page2.html#Hardware_Troubleshooting)

The newness of the hardware is irrelevant; in fact if hardware is going to fail it will usually do so fairly quickly or go for years. Testing hardware failures often involves swapping out suspected parts with known-good parts. If you can't do the testing yourself and/or are uncomfortable opening your computer, take the machine to a professional computer repair shop (not your local equivalent of BigStoreUSA).

Malke

--

Elephant Boy Computers
www.elephantboycomputers.com
"Don't Panic!"
MS-MVP Windows - Shell/User