

Re: Is this a virus? Nasty enough to be...

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-04/0730.html>

From: ttvp (ttvp_at_cox.net)

Date: 04/11/04

Date: 11 Apr 2004 11:45:53 -0700

For lack of a better term, Jesus Christ! You certainly are in-depth. I'll try to respond as accurately and as completely as I can. This certainly looks to be a long thread, so lets get to it!

> >Hello, I am having a real problem with my computer. It seems that yesterday
> >I left my computer on while I went to work (as usual). When I came home the
> >screen was, for lack of a better term, fubar.
>
> Let's have some better terms there <g> ...was it:
> - distorted at a pixel level (sware derangement)?
> - distorted at an analog level (bad monitor)?
> - black, with LED indicating suspend mode (power mgmt)?
> - other?

I believe I answered this question as best as I possibly could in a previous post in response to the same thing. If your newsreader didn't get that post, let me know; I'll paste it in.

> >I hard-rebooted the PC
>
> Kinder would have been to blind-key your way to shutdown. In most
> Windows, you'd Ctl+Esc, Up, Enter, Enter. In XP it's more likely to
> work as Ctl+Esc, Up, U, U

I did think of that, and I actually tried to blind-key it. However, without having done such a thing before, I really had no idea what to press. Oh well.

> >after it booted up and I logged back in, the system rebooted itself
> >completely, instantaneously. I.E. - I type in my password, press enter, and
> >once the desktop finishes loading, black screen, computer starts up again
> >from the beginning, with no warning. It does the same for every account,
> >even the hidden admin. The only way to avoid this is to run in safe mode,
> >which I am currently doing.
>
> OK. Safe mode isn't always, as far as malware goes. Was your PC left
> online while you were out? Was your house door left unlocked too?
>

microsoft.public.security.virus: Re: Is this a virus? Nasty enough to be...

- > *Safe Mode suppresses the startup axis and (some?) device drivers, so*
- > *your mileage points in that direction. Many malware won't run in Safe*
- > *Mode if they were written to patch into the parts of the system that*
- > *aren't run when in Safe Mode. That luck won't last forever.*

My PC is hooked up to the cable modem and I tend to leave it on, more or less, every day straight, occasionally rebooting (not the best habit, I know). Also, the house is always locked and the alarm set whenever I leave and there's nobody else home.

- > *I am running Windows XP Pro with, more or less,*
- > *>all the Windows Updates. The computer is using the Windows firewall and is*
- > *>behind a router. I also am very observant about e-mail and am experienced*
- > *>enough to know the difference between a good and bad attachment*
- >
- > *Takes some doing... I presume you mean you perform the Turing Test to*
- > *assess whether it was sent by a human or a bot? That still leaves*
- > *virus infection of files the human really wanted to send, but OK*

Yeah, well, I mean, when one receives an email with no message body and just an attachment titled "sexy.virgin.exe.scr", It doesn't take a genius to know what's going on. That's about all I ever get.

- > *I don't believe in Virus Scanners,*
- >
- > *Oh, I do. If I lived on "locked doors and no fire escape" NTFS, I'd*
- > **really* believe in them, as cleaning up active malware in NTFS may*
- > *simply not be possible. It's like pre- and post-AIDS casual sex.*

Well, I was exaggerating a little with that line. I just never had any problems with virused (virii?) in my entire computing life. I also knew that no protection was a very unwise thing to do, but I just didn't see the need for that extra program/process in the background sucking up memory. So yeah, play with fire, get burned, etc. I've learned my lesson, blah blah blah, protection from now on.

I never really knew that the NTFS filesystem had such a problem. I always considered it the omnipotent god in the filesystem world, that was without flaws. Interesting.

- > *>but for the sake of elimination I installed AVG after I noticed the problem.*
- >
- > *Well, once the malware's active, installing Windows-based av is not*
- > *going to exclude anything. It's like putting up burglar guards when*
- > *the burglar's already in the house.*

Well, better late than never I suppose. *shrug* Not much else I could think of at the time. Remember, I've never had to deal with a virus problem.

Re: Is this a virus? Nasty enough to be...

microsoft.public.security.virus: Re: Is this a virus? Nasty enough to be...

- > >It couldn't detect a virus that caused this problem. I also ran test after
- > >test online, from Symantec to Panda Scan, as well as Housecall.
- >
- > <shrug> If Windows-based av is not exclusionary, on-line scanners are
- > an even bigger joke. If they find something, great; if they don't,
- > well, can you believe the result?

Not sure. *inexperience*

- > >Either that or they destroyed the virus but damage was done
- > >that the scanner wouldn't detect.
- >
- > You should know the difference – didn't you read or keep the log of
- > what these scans did? You **must** always do that. With that, you can
- > read up the malware that was found, and you know which "cleaned" files
- > to replace or unroot if the system stays flaky afterwards.
- >
- > Specifically, where a virus infected an existing file, you'd replace
- > it with a clean copy (as the "cleaned" original may be damaged).
- > OTOH, many malware exist as stand-alone files that are patched into
- > the system; in that case, you don't want to replace the file, but
- > unroot it (i.e. remove references to it from the system).

sigh

- > >Anybody have any advice? I would really appreciate some help in this kind of
- > >situation. 640*480 is doing murder on my eyes.
- >
- > Yes, as you've prolly guessed by now; I have some advice :-)
- >
- > 1) Verify your hardware
- >
- > You don't really know this is a malware situation; it could be flaky
- > hardware resulting from a power surge while you were out, if not JOOTT
- > (Just One Of Those Things).

That is what others have suggested as well.

- > Running Windows on flaky hardware is an uber-baaad idea, given that
- > Windows is always writing to the hard drive. When contents of what is
- > written to disk are garbled, you will suffer bit-rot and misery; more
- > so if what is garbaged is **where** stuff is written to! Also, a sick
- > HD may get sicker and die, taking your data with it.

Ouch.

- > So, don't fool around. Download RAM testers from www.memtest86.com
- > and/or www.simmtester.com and run these in all-tests mode overnight
- > from the boot diskettes they create. Any errors are hanging offences;
- > do not run Windows again until error-free!

Re: Is this a virus? Nasty enough to be...

microsoft.public.security.virus: Re: Is this a virus? Nasty enough to be...

Well, it's a little late for that... but I'll check the memory anyway.
Can't hurt.

- > *Next, go to your HD vendor's web site and download a data-safe*
- > *diagnostic from there. Run that, most likely from the boot diskette*
- > *it makes, and do all tests that are not data destructive (i.e. avoid*
- > *"write zeros to drive" or other destructive tests). Once again, and*
- > *errors are hanging offences; evacuate and replace HD.*

Well, this is basically an unmodified Dell system that I got a couple years ago. They might have those types of tools available. Care to elaborate on what "Once again, and errors are hanging offences; evacuate and replace HD" means?

- > *In practice, I handle these cases even more rigorously. First, I pull*
- > *the HD, drop it into another "host" PC, and evacuate all contents both*
- > *at the cherry-picking files level and as a full partition(s) image(s).*
- > *While that's going on, the rest of the PC is left to beat itself to*
- > *death running those RAM diagnostics.*

I think that will be my last recourse. However, I'm a little unclear on the terminology you used. Mind putting that paragraph in easier to understand terms?

- > *2) Give yourself a chance to see what's going on!*
- >
- > *By duuuuhfault, XP restarts whenever a system error occurs. Find and*
- > *disable that durnfool setting so that you get a STOP screen (the NT*
- > *equivalent of Win9x's BSoD) to look at instead. When you get those,*
- > *ballpoint the details in case you never manage to find them in the*
- > *bottomless swamp that is XP's even logging system :-)*

Point noted (though I don't know where that option is), but I'll elaborate more on this at the end.

- > *Also by duuhfault, XP restarts the whole PC whenever the RPC service*
- > *fails. As you prolly know, the RPC service has a famous defect that*
- > *allows malware such as Lovesan etc. to infect directly, requiring no*
- > *more than that you are on the infected network (and the Internet is*
- > *the mother of all infected networks!). Change the setting to restart*
- > *the service instead of the whole PC whenever RPC falls over.*
- >
- > *More on RPC attacks:*
- > *- it is the attack attempt (typically unsuccessfull ones aimed*
- > *at other OS versions) that crashes RPC, and av can't help there*
- > *- the original Junly 2003 patch was found to have further defects,*
- > *fixed in an updated patch in September 2003*
- > *- firewall should block these RPC attacks*
- > *- restarts due to this do have a countdown warning, unlike*
- > *the mileage you report*

Re: Is this a virus? Nasty enough to be...

Once again, method of changing that setting?

> 3) *Do a formal virus scan*

>

> *By "formal" I mean; boot without running ANY code off the HD, and from*

> *that known-uninfected boot, run your av to scan all files. You can*

> *see why that's difficult in NTFS! If FATxx, you have free av from*

> *www.f-prot.com, www.sophos.com or www.nod32.com that will run from a*

> *DOS boot diskette. If NTFS, you have uhhh... you tell me.*

Hmmmm... That is a pickle.

> *In summary, it sounds like something is either killing you whenever it*

> *runs from the "normal" startup axis (e.g. malware) of there's a*

> *hardware issue that blows up as soon as the relevant device driver*

> *code fires up or tries to run the affected hardware at higher*

> *performance levels (e.g. AGP or UIDE modes). The latter could as*

> *easily be corrupted driver code as borderline bad hardware.*

>

> *Good luck, keep us posted in the same thread!*

Well well well. I guess I really should have waited for this reply before taking any action. As per another suggestion or two, I attempted to do a repair installation of XP. Unfortunately, fate is not without a sense of irony. Everything in the installation goes right until the program says 34 minutes remaining, then, hell breaks loose. The system blacks out and instantaneously reboots in the exact same way as before, except for one difference: Half a second before the screen blacks out, I can see the (what you call) "STOP" screen extremely briefly. After watching multiple times, I have discerned an error at the top that says something along the lines of "Page fault in nonpaged area." Then the system restarts and repeats the same thing over and over again: "restarting setup", "34 minutes remaining", "Page fault in nonpaged area", blackness, reboot, "restarting setup", "34 minutes remaining", etc. ad infinitum. Maybe that error was causing the original problem and the error screen was just not showing up? Whatever the case is, I have made the problem worse by attempting to repair it, now the problem at the forefront is fixing this new problem and finishing the repair so I can get into Windows XP to fix the OTHER problem (phew!). Unless fixing that error fixes both problems, in which case there will be much rejoicing. At the moment, I'm quite happy that I decided to make this a tri-boot system with Windows 98 and Linux. I'm forced to post this using Google groups at the moment, since 98 seems to be non-affected. Unfortunately I can't access any NTFS partitions with it. *sadness*

Any new suggestions? I really appreciate your effort put into this so far. Let's get this straightened out!

-T.J.