

Re: Virus in memory? I may be crazy, but....

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-06/0210.html>

From: David H. Lipman (*DLipman~nospam~_at_Verizon.Net*)

Date: 06/16/05

Date: Thu, 16 Jun 2005 16:08:19 -0400

From: "JCB_MCSE_wannabe" <JCBMCSEwannabe@discussions.microsoft.com>

| Recently, a friend's computer (Dell workstation, Win XPPro_sp2 w/Norton AV)
| apparently received a virus which was consuming the memory resources of his
| machine. He suddenly began receiving "insufficient memory" messages in
| response to just about every command.

| Can a virus hijack the memory to deny normal system function?

A virus ? Could be any malware or a combination of malware that can do this.

| This problem prevented him from running an AV scan. Not being an expert in
| these matters, I was limited in my abilities to help. Nothing he or I
| attempted would allow us to reboot the machine normally.

You should have come here and we could have provided several methods including but not limited to slaving the drive on another PC.

| He decided to attempt a reinstall from the XP installation CD. A repair
| attempt and reinstall attempts were not successful. During the initial XP
| install phase while system files are being copied, the process suddenly
| stopped and also yielded an "insufficient memory" message.

Once infected a repair install is NOT the way to go. The system must be cleaned.

| Any one memory stick in his machine had sufficient capacity to meet XP
| install requirements, yet (for lack of any better idea...) we removed the
| memory sticks, cleaned the contacts and reinstalled them.

| After this, the reinstall progressed without incident and the machine has
| been incident-free since.

Then you didn't have malware you had a hardware problem !

| Removing the memory was APPARENTLY the solution, but I lack the knowledge to
| explain why this could be so or to reproduce/test/verify this behavior.

| I theorized the virus was actually installed in memory and by physically

Re: Virus in memory? I may be crazy, but....

microsoft.public.security.virus: Re: Virus in memory? I may be crazy, but....

| removing it, the virus was lost without a power supply. I'm no hardware
| expert, but I thought upon shutdown, the memory was refreshed anyway – is
| this not the case?

Once power is removed from RAM, you would kill any virus and it can not exist in volatile
RAM once power is not present and a CPU is not giving it "life". There is no virus
installed in RAM as you seem to describe.

| So.....

|
| Assuming a virus can be in memory and persistent, did we simply dumb-luck
| ourselves into the correct solution, or was something else the solution, and
| we drew an incorrect conclusion

Faux conclusion...

| If an in-memory virus is possible, could my friend simply have removed the
| physical memory AS A FIRST STEP and avoided the wipe/reinstall?

There was no virus. You had a hardware problem.

| Also, the act of removing the memory suggests the virus is volatile – i.e.,
| no power, no problem. Does in-memory data persist even when the machine is
| powered down (relying on the computer's system battery which powers the
| clock, etc.?)

The act of removing the memory module proves it NOT to be a virus but a hardware problem.

| Any thoughts on this problem are appreciated. My friend thinks I am a
| 'genius' for fixing his machine, yet I feel very dissatisfied in not REALLY
| knowing the reason for my "success" in solving the problem.

|
| Regards,

|
| --
| JCB\1059

--
Dave
<http://www.claymania.com/removal-trojan-adware.html>
<http://www.ik-cs.com/qot-a-virus.htm>