

Re: Write-protect sctors?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2006-08/msg00011.html>

- *From:* scott <redhowlingwolves@xxxxxxxxxxxxxxx>
 - *Date:* Mon, 28 Aug 2006 20:14:02 -0400
-

scott wrote:

Bill Church wrote:

It sounds very crazy. Did you ever actually identify if there was a rootkit installed? Did you try booting to a live CD of another distribution and investigating the disks from that live CD?

Remember that partitioning does modify the existing data on the disk, just the partition table, unless you chose to do a full format that data is still there. However, the chances of it actually being able to effect anything that's not directly referencing that data by executing it seems improbable. I wouldn't think that simply copying a file over that location couldn't spawn a process, of course nothing is impossible.

There is a BIOS function that is supposed to protect the boot sector, it's usually disabled by default on most systems. I imagine it would be possible for someone to modify the CMOS and protect any sectors they wish, but the attacker would undoubtedly need to have advanced knowledge of your system, BIOS, hard disk and geometry to make this attack possible. I highly doubt this is the case.

It sounds like you may have a defective hard disk, I would try a disk diagnostic first, or maybe attempt to install another OS or distribution.

-Bill

----- Original Message -----

From: scott Sent: Mon, 8/28/2006 11:23am

To: focus-linux@xxxxxxxxxxxxxxx

Subject: Write-protect sctors?

I had a probable rootkit in ubuntu dapper that proved to be more persistent than I thought possible. I did rkhunter and showed some anomalies in /dev/... Trying to track those dir's down proved elusive, even with root enabled (in ubuntu, root is disabled by default. You can still sudo, but no su without certain switches,) the dir's effectively hid from my view. So I decided to reinstall a clean slate. This is when I encounter problems that don't make sense.

Re: Write-protect sectors?

As the install progresses to the partitioning of the disc,I opt for the erase whole disc option.It progresses to a certain point and then quits with an error..repeatedly.

I filed a bug report with launchpad,but my question is this:Can any malware you are aware of write-protect certain segments of a HD,without BIOS support?Or is there a BIOS trojan that I'm not aware of in Linux?Is this even possible with a hardened system?

Is this even possible in any system,Windows included?

What I.m asking is : Can any malware write-protect sectors on a HD that survive repartioning?

Sounds really crazy,huh?

Thanks,Scott

It was a problem in ubiquity, in that it never resolved to a mount point when installing.

But my point is that I eventually got the same install cd to actually install.Now if something was trying to protect itself,only after many attempted overwrites did I succeed,that would seem...Almost...logical,..Maybe!?

The hard drive is fine,as far functioning,anyway.

I also know that you have to have (presumably,)BIOS access to write- protect sectors of a HD.

Didn't Joanna Rutkowska demonstrate a BIOS virus,or POC,at one time?Not likely,or probable,that this was my problem,but could it be done....theoretically?Especially in a `nix environment?

I think not.But I have been wrong so many times in my life,that I like to think anything is possible.

If ya want to do it bad enough,at least.

Any other thoughts on this matter?

Regards,Scott

Hi again.

I also know that BIOS is ROM,not RAM.

Therefore,it seems that I would have to do a BIOS flash for this to happen?

Regards...again,and thanks,Scott