

Re: Scanning from a CD

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2007-04/msg00011.html>

- *From:* "David Craig" <dave@xxxxxxxxxxxxxx>
 - *Date:* Sun, 1 Apr 2007 14:27:31 -0700
-

I didn't follow this thread, but I can think of one case.

If you have an infected system and then install a drive into it that contains the OS files for another, the virus can replicate itself onto it. Registry hives can be mounted from any place and modified, plus the simple addition of files containing the virus. Then when that drive is returned to its system, it will start with it active. Resplendent Registrar is a nice utility that shows how to mount registry hives if you haven't seen it done before.

There is always a window where virus and spyware definitions do not contain a new virus. In some ways we are lucky in the U.S. that new viral/spyware attacks are usually seen in Asia or the EU before they appear here. There are some attacks that are targeted and only go after some group of computers, so that the traps may not see them until they infect their targets and get reported. Some older versions of antivirus do not have all the detectors currently shipping with later versions of that product. There seems to be a change coming where the major antivirus companies will update the software as long as the subscription is current. Both the problems and the solutions are constantly evolving trying to evade or control the other.

"Bill Ridgeway" <info@xxxxxxxxxxxxxxxxxxxx> wrote in message news:Opa5ryIdHHA.4344@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

You wrote –

- <<If you drop the HD in your PC, there are two risks:
 - your PC may corrupt an at-risk HD (Autochk, SR/SVI, etc.)
 - a surface exploit could infect your PC>>

Any action has its attendant risks. The trick is to keep to reduce the risk and hope you don't get caught.

Could you please explain how my PC may corrupt another HD (which is installed as a secondary master)?

Similarly, if my computer threat prevention is bank up-to-date, how can my computer be infected – other than the ever present risk from the time lapse between the risk being released to the wild and the update being installed)?

Re: Scanning from a CD

Thanks.

Bill Ridgeway
Computer Solutions