

# Re: [opensuse] Who said Linux doesnot get Virus infections

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/SuSE/2007-08/msg00373.html>

---

- *From:* David Bolt <[bcrafhfr@xxxxxxxxxxx](mailto:bcrafhfr@xxxxxxxxxxx)>
  - *Date:* Wed, 8 Aug 2007 13:17:51 +0100
- 

On Tue, 7 Aug 2007, Michael Letourneau wrote:–

David Bolt wrote:

<Snip>

As more and more file types get linked to more applications I am not so sure that "executing" something has the same meaning it used to. Say you download a new screen saver, you never really execute that, but your window manager utilizes the data in it.

Erm, you can execute a screen saver if you test it. And the window manager will do so when the specified idle time is reached.

As an example, I set the screen saver on my 10.2 system to be BSOD and here's me locating the just where the file is, and what type it is:

```
davjam@donnas:~> grep -i "saver" ~/.kde/share/config/kdesktoprc
[ScreenSaver]
Saver=bsod.desktop
davjam@donnas:~> grep -i "exec" /opt/kde3/share/applnk/System/ScreenSavers/bsod.desktop
Exec=bsod
TryExec=xscreensaver
Exec=kxsconfig bsod
Exec=kxsrn bsod -- -window-id %w
Exec=kxsrn bsod -- -root
davjam@donnas:~> find /usr/ -mount -name bsod 2>/dev/null
/usr/lib64/xscreensaver/bsod
davjam@donnas:~> file /usr/lib64/xscreensaver/bsod
/usr/lib64/xscreensaver/bsod: ELF 64-bit LSB executable, AMD x86-64, version 1 (SYSV), for GNU/Linux
2.6.4, dynamically linked (uses shared
libs), for GNU/Linux 2.6.4, stripped
```

All of which makes for an ideal method of introducing a trojan onto a

Re: [opensuse] Who said Linux doesnot get Virus infections

system[0]. And, just to make sure it works across the widest variety of systems, all that's required is to create a statically linked 32bit binary and it'll run on virtually any x86-32 or x86-64 based system.

Of course, there's also those infections that occur without user intervention, but those tend to come in through security holes in server daemons which are unlikely to be running on a normal users desktop system.

Yup, I would classify those more as worms or exploits rather than virii.

They're under the general "viruses" tag. For my definitions, worms require no assistance to spread, as they actively search for files/systems to infect. Trojans require human assistance to spread and are designed to pretend to be one thing while actually being something completely different. True viruses also require human assistance to spread, but do so completely unknown to the user. Boot sector viruses, and those wonderful macro viruses, are what I'd call a virus. I wouldn't classify any of the recent Windows "viruses" a true virus, I'd call them a trojan instead.

But most of the popular services have had some issues, ftp, mail, http, ssh...

The last Linux worm I saw was one that was spread via infected Apache/PHP systems. It worked by having the exploitable PHP parse a command string and fetch a script from some site, chmod the script, and then call it. That script would then download a couple of ELF executables, one of which turned the server into a zombie controlled via IRC, and configured them to start on boot. Thankfully, it's been a couple of years since I saw that, but I still have the sample I managed to acquire stored in an encrypted archive, along with a large selection of Windows viruses[1][2].

<OT>

Presently, I'm seeing a nice selection of infected systems dumping their "you have a greetings card" crap. Unfortunately, it appears that the trojan behind this is mutating so rapidly that, more often than not, ClamAV doesn't recognise the trojan file when I scan it. The good part of this is that, due to ClamAV.org only allowing two submissions per day, I use virustotal.com to do a multi-anti-virus scan and have them submit the files to the different vendors.

Who'd have thought. A Linux system being used to protect Windows systems. Fun, eh?

Re: [opensuse] Who said Linux doesnot get Virus infections

Re: [opensuse] Who said Linux doesnot get Virus infections

</OT>

[0] Of which I'm absolutely certain there either are some right now, or there will be some in the future.

I totally agree. Windows is the low hanging fruit. People can get the most bang for the least effort there. They want a zombie network that can spam the world, right now its far easier to develop something for Windows than to do the same for Linux.

At the moment, as far as I can tell, this still holds true:

<URL:<http://www.immunitysec.com/downloads/tc0.pdf>>

[0] As shown by the number of .SCR trojans that circulated a few years ago

[1] Yes, I said viruses. However, I'm applying the meaning behind the phrase "When in Rome, do as the Romans do."

[2] Each file is renamed as a .bin file and, every now and again, I'll extract them on a Windows system to check whether the newly-deployed anti-virus system still works as it should. So far, they have all recognised what they've had thrown at them.

Regards,  
David Bolt

--

Member of Team Acorn checking nodes at 100 Mnodes/s: [www.distributed.net](http://www.distributed.net)  
RISC OS 3.11 | SUSE 10.0 32bit | SUSE 10.1 32bit | openSUSE 10.2 32bit  
RISC OS 3.6 | SUSE 10.0 64bit | SUSE 10.1 64bit | openSUSE 10.2 64bit  
TOS 4.02 | SUSE 9.3 32bit | | openSUSE 10.3a6 32bit

--

To unsubscribe, e-mail: [opensuse+unsubscribe@xxxxxxxxxxxxx](mailto:opensuse+unsubscribe@xxxxxxxxxxxxx)  
For additional commands, e-mail: [opensuse+help@xxxxxxxxxxxxx](mailto:opensuse+help@xxxxxxxxxxxxx)