

Sponsored Links			
Redundant servers, virus filtering, spam protection, 30 day free trial	Protect Against Viruses From Email. as Low as \$9.95/mo - Get Info Today	Free Scan, advanced Spyware and Adware removal - Download Now!	4 Side-by-side Comparison: Virus Removers. 100% Free

networking.earthweb.com/netsecur/article.php/3389801

[Back to Article](#)

Virus-Hunting Knoppix Gives Windows Machines the Once Over

By [Carla Schroder](#)

August 3, 2004

[Continued From Page 1](#)

Virus Scanning With Knoppix

Well OK, ranting is fun and cathartic, but it doesn't solve problems. Knoppix, the live Linux on a bootable CD, is proving to be the most innovative, useful Linux distribution there is. Starting with Knoppix 3.4, you can use it as a portable, cross-platform virus scanner. The advantages of this are many:

- You are working from a guaranteed clean operating system, which being on a non-writable disk, is impossible to compromise
- Because you must power down the PC to boot Knoppix, any memory-resident nasties are evicted
- It is free, so you can burn masses of disks, and go on a virus-scanning spree

Scanning a Windows system with Knoppix before you install something like Symantec or MacAfee means you'll be scanning with the latest virus updates. Most commercial AV products can do a pre-installation scan from the installation disks, but they are months or more out-of-date.

How To Do A Virus Scan With Knoppix

Boot up the system with Knoppix 3.4. The default keyboard layout is in German, so English speakers might want to use this boot command:

```
knoppix lang=us
```

Hit F2 or F3 to see all the boot-time command options; Knoppix supports a number of languages, and a large number of boot configurations.

When Knoppix is booted, select KNOPPIX -> utilities -> install software. This brings up a menu; check "f-prot."

After f-prot is installed, select KNOPPIX -> Extra Software -> f-prot. This brings up the f-prot menu; the first thing you want to do is 4. "Online Update."

After the new virus definitions are downloaded, select partitions or directories to scan. Yes, you can select Windows partitions too. Knoppix automatically mounts all partitions on your system, so you can easily select the ones you want. Hit the "scan" button, and

go find something to do, because it can take awhile. When it's finished, you'll see a report showing the results of the scan. This method only runs a scan, it does not remove viruses.

Disinfecting Windows With f-prot

What should you do if f-prot finds infected files on a Windows system? If the filesystem is NTFS, f-prot cannot disinfect the system, because write support for NTFS in Linux is not reliable, so you don't even want to try. You'll need an AV product made for Windows.

You can scan and clean up a Windows FAT16/32 partition, by running f-prot from the command line instead of the graphical menu. First, make sure the partition is mounted read/write; simply right-click on the icon for the drive, which is on your Knoppix desktop, and left-click Actions -> Change read/write mode.

Next, open a command shell and run this command, naming of course the partition you want scanned:

```
$ f-prot -disinf -list /mnt/hda1
```

The **-list** option shows the scan's progress, and the **-disinf** option will disinfect the system. And that's all there is to it. If f-prot encounters something it cannot clean up, it should be able to quarantine it.

f-prot has a Windows edition for \$29, and very liberal licensing terms for home users- it covers all your home computers. There is also a free Linux workstation edition; sure, we can mock and abuse Microsoft all we want to, but all it takes is one evil genius to write a lethal Linux exploit, and hordes of happy script kiddies to distribute it all over the planet in a heartbeat.

Many thanks to Fabian Franz for creating the f-prot installer for Knoppix. Mr. Franz is a Knoppix developer.

Resources

- [f-prot home page](#)
- [Trojan turns victims into DDoS, spam zombies](#)
- [Rise of the Spam Zombies](#)
- [Spam and Viruses: Unholy Matrimony, Part 1](#)
- [Spam and Viruses: Unholy Matrimony, Part 2](#)

JupiterWeb networks:



Search JupiterWeb:



[Jupitermedia Corporation](#) has four divisions:
[JupiterWeb](#), [JupiterResearch](#), [JupiterEvents](#) and [JupiterImages](#)

Copyright 2004 Jupitermedia Corporation All Rights Reserved.
[Legal Notices](#), [Licensing](#), [Reprints](#), & [Permissions](#), [Privacy Policy](#).

[Jupitermedia Corporate Info](#) | [Newsletters](#) | [Tech Jobs](#) | [E-mail Offers](#)

Go to page: [Prev](#) [1](#) [2](#)