

## Re: Detecting Zombies?

---

*Source:* <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2008-09/msg00090.html>

---

- *From:* David Brown <[david.brown@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:david.brown@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sun, 07 Sep 2008 19:38:05 +0200
- 

DanB wrote:

I am the only person who uses Linux on the desktop at my place of work. Naturally, everyone else has XP except for a couple with new machines and Vista. At any given time half of them are running like they were 286's from all the malware that they are infested with. So they reload the OS, over and over.

I have long since stopped working on problem windows machines for clueless users and have given up on trying to convince anyone that there is a far better platform to surf from. If someone has a genuine interest in Linux I will gladly help, but they must make the first move.

So, back to the virus/trojan/zombie problem. How does a person, who is not a career network administrator, determine if their XP is zombied? Years ago, I used to play with network protocols and stuff, but haven't needed it for years. But the average user is never going to learn Snort or the like. If the problem were on a Linux box, netstat might give an indication, but with current browsers there are so many connections coming and going all the time it isn't as simple as just looking at a snapshot of the current connections.

With Windows what would you use? Bear in mind that there is no network admin here. (Not me! – not my work assignment – besides, I am temporary anyhow). Probably, there is no answer for non-techies.

Dan

Set up the network's Internet gateway/firewall to block all outgoing SMTP traffic that is not from the company mail server to the ISP's mail server, and to alert some competent person on other attempts to send SMTP traffic. That will quickly block the effects of most zombie software, and let you know what's happening.

.