Business

Management

Switch to Linux, stay out of jail

Thursday August 14, 2003 (08:54 AM GMT)

PRINT EMAIL DISCUSS

- By Robin 'Roblimo' Miller -

It's a scary thought, but Windows users may actually risk going to jail if they don't protect themselves well enough from the many worms, viruses and 'Trojans' that can infect their operating system. Don't believe me? Go read this story. Then come back and learn how to protect yourself against this problem.

Let's assume you must use Windows. There's an application you can't live without and you have been unable to find a Linux equivalent for it. You can't run it with Wine or one of the Wine-derived CodeWeavers products that allow many Windows programs to run directly under Linux.

(You *did* try Wine or CodeWeavers' CrossOver software with your favorite Windows program before you decided you simply *had* to keep Windows around, didn't you?)

So, Windows-bound one, you must either stay unconnected to the Internet (as in, stop reading this and pull that phone or network wire out of your computer or turn off your wireless network *right now*) or take strong, ongoing precautions to keep malicious code out of your computer.

This kind of defense takes time and money.

Note the way antivirus software purveyor Sophos displays a version of the "Man arrested for porn on his computer because of virus" story on their own site as an inducement for you to buy their product for your business.

Antivirus companies love to tell you about all the threats you can avoid if you buy their products. Right now, aside from the "get a virus, go to jail" problem, they're giving big play to the W32/Lovsan.worm (AKA W32/Blaster) that has been messing up Windows computers like mad over the last week.

Virus protection isn't something you buy once and forget. There are new viruses and worms all the time, so you need to keep updating that antivirus software (and keep paying for it), usually a step behind the virus writers, but that's how it goes in the virus business.

Then there are Trojans: Programs you unwittingly download along with something you want, like a filesharing utility, that make your computer do things you don't expect it to do. Like download kiddie porn that can get you arrested, for example. Or make your computer dial expensive foreign numbers that run up your phone bill. Or any one of a number of other nasties.

Almost all Trojans currently "in the wild" only affect Windows, and they can be hard to remove from a Windows PC because Windows and most Windows programs are full of closed-source secrets, so no one knows what's supposed to be in every file on a Windows hard drive.

It is *possible* to write a Trojan for Linux, and at least one has been distributed -- very briefly, and without doing any notable harm to anyone -- but since every single file in an open source program can be viewed by you, the user, or by a maintainer from the distribution you have chosen, getting rid of a Trojan on a Linux computer is simple, usually a matter of downloading and installing a simple patch or 'delete' script or else manually deleting a few files.

By downloading all your Linux software through trusted sources (and by sticking to open source software) you may not be 100% safe from all Trojans, but you're far safer than if you are running an operating system that is full of files whose source code is kept secret, even if "security" is supposed to be a big reason for that secrecy.

The "download only from trusted sources" advice holds true for all operating systems, by the way. But with Linux and open source software, even if you don't know how to read all of a program's source code to see if it's worth trusting, chances are that someone out there does -- and will check it, and will tell the rest of the world if it's safe.

Note that the *only* way to install software on a Linux computer that's set up correctly (which it is by default in almost all mainstream Linux distributions) is to log in as root. When you're working under your regular username, even if you download the world's most evil porn-sucking, nasty-dialingest, ad-flashing or system-destroying malicious software, there is no way it can install itself and do bad things to your machine. This is not true with Windows. The current Lovesan/Blaster worm is proof: It installs itself, automatically, without the user doing anything. This sort of worm simply can not infect a Linux computer that isn't run as root, which you never should except while performing admin tasks -- preferably while disconnected from the Internet or other networks.

Of course, one reason *not* to prefer an operating system (like Linux) that won't 'accidently' download kiddie porn when you're not watching is that you are a juvenile pornography fan and want to have a, "The computer did it!" defense ready in case you end up in court, faced with criminal charges.

We're not saying most Windows users are kiddie porn lovers or that more than a tiny fraction of Windows users will get busted unjustly for kiddie porn downloads caused by bad programs they unknowingly downloaded. And we know plenty of Windows users who have run high-bandwidth Internet connections for many years with neither a firewall nor anti-virus protection, and have never been infected with a worm, virus or Trojan.

But why take the risk? Linux has gotten a lot easier to use than it used to be, and you can almost certainly either find Linux software to replace your favorite Windows programs or at least find Windows-based ones that will work adequately under Linux through Wine.

It may take some time to learn Linux, not because it's hard, but because it's different from what you're used to.

Now think: If that learning time saves you from just one nasty virus or worm infection, won't it have been worth it?

And isn't that learning time even *more* worthwhile if it saves you from even the remote possibility of an arrest for a crime your computer might commit behind your back?

Editor's note: The recent crack of the GNU.org ftp server was by a local user; that is, someone who had physical access to the system. In all the talk about "Internet" hacking, cracking, viruses, and worms, it's easy to forget that someone working from behind your firewall can do all kinds of damage even if your system is impervious to outside attacks. This is true of all operating systems.)

Related Links

- **http://winehq.com/**
- **http://codeweavers.com/home/**
- **http://sophos.com/**
- **http://sophos.com/virusinfo/ar ticles/porntrojan.html**
- **http://us.mcafee.com/virusInfo /default.asp?id=description&am p;virus_k=100547**
- **http://slashdot.org/article.pl ?sid=03/08/12/2220246&mode =nested&tid=126&tid=128&tid=185&tid=190& tid=201**
- **crack**
- **http://roblimo.com**
- **http://news.com.com/2100-1029_ 3-5062463.html**
- **More Humor stories**
- **Also by roblimo**

This discussion has been archived. No new comments can be posted.

Comments

Switch to Linux, stay out of jail

Top | **84** comments | Search Discussion |

Threaded Oldest First Change

GNU ftp site hacked (Score:1)

By hatux (178175) on 2003.08.14 4:06 (#64649)

Newsforge is lacking that fde ftp.gnu.org is cracked, hacked since march this year. Lot of damage. Alpha stuff has gone and no adequate backup !

Mr Stallmann shame yourself

- Re:GNU ftp site hacked by Anonymous Reader (Score:0) 2003.08.14 4:46
- Re:GNU ftp site hacked by Anonymous Reader (Score:0) 2003.08.14 4:57
- Re:GNU ftp site hacked by Anonymous Reader (Score:0) 2003.08.14 5:12

- Re:GNU ftp site hacked by Anonymous Reader (Score:0) 2003.08.14 5:12
- Hack to get free software? Its free already. by Anonymous Reader (Score:0) 2003.08.14 7:56
  - Re:Hack to get free software? Its free already. by Anonymous Reader (Score:0) 2003.08.14 12:27
- Re:GNU ftp site hacked by Anonymous Reader (Score:0) 2003.08.15 15:01

Updating needed also in FLOSS world... (Score:0)

By Anonymous Reader on 2003.08.14 4:22 (#64651)

While I agree with most of you wrote, I must point out that even Open Source does not permit you to install and then forget about keeping your installation up-to-date wrt security patches. There may not be viruses, but bugs in programs may permit malicius attacks, even if the programs are Open Source. The recent problems at the FSF ftp site are a timely reminder.

As the Harry Potter character Mad-eye Moody thundered, "Constant vigilance, constant vigilance!!!"

- Re:Updating needed also in FLOSS world... by Peter Robertson (Score:1) 2003.08.14 7:34

No more ... (Score:0)

By Anonymous Reader on 2003.08.14 5:13 (#64657)

I can't quite figure out what's wrong with this article - needlessly alarmist, potentially libelous, or what, but it seems you have descended into "yellow journalism". Is this really the level of discourse you want to stoop to?

It is one incident - not an epidemic. The charge is severe and regardless of his innocence, the damage to his reputation is irreparable. However, despite the severity of this incident, I find it impossible to justify an entire article railing against Microsoft and their browser product as the primary cause of his troubles. You might as well come out and say "Bill Gates eats babies for breakfast" (I've come to expect that from the readers, but not the editors).

Using this man's situation as a political tool in your war against Microsoft is crossing a line that I would have avoided.

You've just lost a reader. Not significant in the greater scheme of things, but a lost reader no less.

So, flame on - I won't be here to read it ever again.

- Re:No more ... by Glanz (Score:1) 2003.08.14 5:33
- Re:No more ... by Anonymous Reader (Score:0) 2003.08.14 5:45
- Gates eats babies for breakfast? by Anonymous Reader (Score:0) 2003.08.14 6:49
- Re:No more ... by Anonymous Reader (Score:0) 2003.08.14 10:34
- Re:No more ... by Anonymous Reader (Score:0) 2003.08.14 12:12
  - Re:No more ... by jmeuser21 (Score:1) 2003.08.14 14:20
  - Re:No more ... by Anonymous Reader (Score:0) 2003.08.15 7:04
    - Re:No more ... by Anonymous Reader (Score:0) 2003.08.19 9:35
- Re:No more ... by Anonymous Reader (Score:0) 2003.08.14 21:10
  - Re:No more ... by Anonymous Reader (Score:0) 2003.08.14 21:16

MS Porn Server (Score:0)

By Anonymous Reader on 2003.08.14 5:22 (#64660)

My previous job had servers co-located with various MS-Windows server maintained by some MS fans. It caused my department problems because, being on the same subnet, the MS-servers cut into our bandwidth. It seemed the MS-Servers couldn't go two weeks without starting to eat up the band width with movies and graphics, mostly porn. Even with the MS-fans vigorously applying "patches" and "updates", if left long enough since a clean install, each on turned into a special little porn serving electronic Chernobyl.

There's not too many reasons to leave Windows on the desktop, but it should never enter the server room. Especially if there's any risk of illegal material being stored there by visitors.

Conversely, no personal data should ever be put on a Windows server. E.g. payroll, financial records, insurance, patient data, etc. on a Windows server would be tantamount to facillitating identity theft though willful negligence.

Not entirely true (Score:0)

By Anonymous Reader on 2003.08.14 5:30 (#64663)

While most of the article is fine, there is one huge innaccuracy. The statement that a worm similar to Blaster could not infect a system not running as root simply is NOT true - all it takes is a buffer overflow in a server daemon running as root. That was, if i don't remember incorrectly, the case with the Ramen worm.
Now, most Linux distros these days, especially the consumer-oriented ones, don't have many services like that turned on by the fault, not to mention that most distros lets the user set up some level of firewalling during the install phase, but the _theoretical_ possibility for a remote-root worm like Blaster certainly still exists, even for linux systems.

- Re:Not entirely true by Anonymous Reader (Score:0) 2003.08.14 7:01

"Trustworthy Computing" (Score:0)

By Anonymous Reader on 2003.08.14 5:36 (#64666)

So this is what M$ calls "Trustworthy Computing" eh?

Yes I do know that Linux requires patches a lot too but they usually come out faster becuase everyone can work on it!

Great article!!! (Score:1)

By Glanz (147002) on 2003.08.14 5:46 (#64670)

I have installed or helped installLinux on at least 200 PCs during the last two years for people. And have encouraged countless others to use Mozilla instead of Interlope Expectorator....
Many of the Windows PCs had been "owned" not by trojans but by sites that change user configuration without the user being aware. There are many sites that do this, and their minimal "software" isn't detected by virus scanners or firewalls, because to IE, there is nothing unusual about them, and to Windows, their operation seems par for the MS course.

I have seen at least a two dozen portables at the university returned by students to the sellers because of Linux incompatibility. Most of them were IBM and Compaq portables. Science departments simply no longer use Windows here. Too slow, too glitchy, and too dangerous on a network where all must operate at the speed of the slowest and glitchest member.

Yet, Windows will remain because many unthinking folks like a OS to "think" for them. They do not want to be in charge of their virtual or real environments. Windows is the ideal OS for all who are incapable of analysis and those devoid of will.

- Re:Great article!!! by Anonymous Reader (Score:0) 2003.08.14 11:12
  - Re:Great article!!! by emk (Score:1) 2003.08.14 13:37
  - Re:Great article!!! by Glanz (Score:1) 2003.08.14 14:48
  - Re:Great article!!! by Anonymous Reader (Score:0) 2003.08.14 15:41
- Re:Great article!!! by Anonymous Reader (Score:0) 2003.08.14 11:37

Great article (Score:0)

By Anonymous Reader on 2003.08.14 7:27 (#64688)

Especially, I like this:

It may take some time to learn Linux, not because it's hard, but because it's different from what you're used to.

Fear, Uncertainty, and Doubt (Score:0)

By Anonymous Reader on 2003.08.14 7:27 (#64689)

This is unfortunate. You appear to be trying to win Linux converts with fear tactics. Trumpeting the lack of Linux viruses is one thing; suggesting that it is anywhere reasonable for people to stop using Windows for fear of child pornography charges is just ridiculous, and level headed advocates shouldn't stoop to it.

I like most of your columns, and almost always agree with you, but this column is flawed. Aside from just using fear tactics, you make a couple of bad assertions.

You suggest Wine could solve Windows necessity. You proddingly ask if we've even tried it. I have tried it. Hopefully it's grown up a bit since I did, but my experience was that it was a silly bungled and barely hanging together solution.

You suggest that Open Source is inherently more secure than proprietary code. I completely agree that it has certain advantages, but it also has its own problems. Obscurity does not secure, but it does create a few barriers to entry. I would say that lack of current popularity is athe major contributing factor to keeping non-Windows systems impervious. It's a matter of marketing. If I'm out to damage systems, for whatever reason, I want to damage as many as possible. The biggest market for systems to damage is Windows.

You mention the endless patching of virus protection programs to be a bad thing. Linux systems get just as many updates. Update turnaround is actually one of its strengths. We shouldn't knock the endless update cycle, we should laud auto-update features, and champion the fact that our Open Source systems are updated much more frequently in order to better keep up with a changing world.

None of my ideas and rebuttals here are new. A thousand people think and say these same things on similar sites every day. Sometimes hundreds of times a day. What's new is that FUD has come to visit our Newsforge, and I find that ours doesn't smell any better than theirs.

-Pedro Picasso (pedro at x dash omega dot com)

- Re:Fear, Uncertainty, and Doubt by roblimo (Score:1) 2003.08.14 8:35
  - Re:Fear, Uncertainty, and Doubt by Anonymous Reader (Score:0) 2003.08.15 9:22
- Only time to reply to one your items by Anonymous Reader (Score:0) 2003.08.14 8:55
  - Re:Only time to reply to one your items by Anonymous Reader (Score:0) 2003.08.14 13:15
    - Re:Only time to reply to one your items by Anonymous Reader (Score:0) 2003.08.15 16:40
- Re:Fear, Uncertainty, and Doubt by Anonymous Reader (Score:0) 2003.08.14 11:12
- Re:Fear, Uncertainty, and Doubt by Mr. Firewall (Score:1) 2003.08.16 1:07

Inaccuracies? (Score:0)

By Anonymous Reader on 2003.08.14 7:32 (#64690)

Trojans could easily be uninstalled - what if it was a rootkit that hijacked bits of the system?

We're always told that if hacked we should just reformat and reinstall from clean media and only keep other stuff that is either non-executable or can be compiled from checked source.

Plus, it's perfectly possible for malware to run as an ordinary user. There's nothing that stops you compiling code as an ordinary user and running it yourself. Sure, it can't damage the *system* or other users' files but it can still behave maliciously.

Bad taste... (Score:0)

By Anonymous Reader on 2003.08.14 8:33 (#64708)

Robin,

I think it is in poor taste to put this article under the topic of "Humor". This guys life was/is a living hell because of what happened to him and you find that humorous?

That's dreadful and very bad taste.

What about cracked software stored on your box? (Score:0)

By Anonymous Reader on 2003.08.14 9:00 (#64722)

MS is so unsecure, that I got a virus that downloaded kiddie porn when I didn't have an internet connection, modem, or lan card. LOL, it's that unsecure!!!

Seriously tho', I'm not all that concerned with my winbox since I reinstall about twice a month, so I know what's on my machine (you say that's too much, but it's the only way I found to quell my fears of MS insecurity).

The truth is, Microsoft is dangerous to use. I have had my computer used by hackers to store cracked software, then be a place where they can upload it to their friends. How did I find out? About 2 years ago, my ISP was one of the firt to institute a bandwidth cap, giving me 10gigs download/5 gigs upload, and every gig past that was $4.95 extra. Since I don't share files, and I mostly only surf the net/email, these parameters are were ok with me. I got my ISP bill at the end of the month, first month of the new billing scheme, and my bill was over $400! I took my computer to a repair place and they showed me what it was, a copy of Adobe Acrobat 5.0, a copy of Maya 4, a copy of Norton Security 2001, Works 2000, Windows serial lists, and much much more. How much do you think it would have cost me had I been caught authorities? $150,000 per violation perhaps? The little trove on my machine could have cost me literally, millions of dollars. That's why I installed winXP the way I wanted it, Norton Ghosted it, and now reinstall every couple of weeks or so. You think kiddie porn is a problem, it's nothing compared to having your computer used as a hacker repository.

- Re:What about cracked software stored on your box? by Anonymous Reader (Score:0) 2003.08.14 9:15
  - Re:What about cracked software stored on your box? by Anonymous Reader (Score:0) 2003.08.14 9:31
    - Re:What about cracked software stored on your box? by Anonymous Reader (Score:0) 2003.08.14 10:12

Of all stupid lusers... (Score:0)

By Anonymous Reader on 2003.08.14 10:33 (#64745)

this guy gets a Â¿worm? that downloads child porn into his computer... hmmm. To me, that sounds like pure crap, I'm happy that the jury bought the guy's version, and he would say martians took control of his computer if he needed to...

Don't get me wrong, I'm a (happy) Linux user and I don't like Windoze the same way you don't, but to me this story smells funny from the start. I mean, you can get a worm or a spyware and it could change your home page or something to an adult site, but downloading child porn... beats me. First of

all, since child pornography is so harshly prosecuted, a worm could not have a permanent address to which make reference in order to download the questionable material, since no child porn sites last long. Also, what kind of person does not know what's in his hardisk? I'm constantly looking at it, looking for things, opening files and stuff, I would notice something like 172 extraneous pictures...

So, my answer to the riddle would be: either the guy is really a perv, or somebody else in his house is (I could buy the "conspiracy theory", maybe his ex- wanted to have custody). Otherwise, the guy's a total moron when it comes to using his box, and should stay away from the internet or any computer, for that matter.

Changing subject, I don't think this is the right way of campaining in behalf of Linux. Security is everybody's problem (Linux and otherwise), and although one of the main concerns is to have a secure OS running, the most important thing to do is to LEARN how to protect yourself. You can accomplish little if, as a Linux user, you log in as root all the time (and I'm sure many people do). That's the thing to stress, I mean.

The problem is that too many people out there use computers without the slightest idea of how to use them safely, and in turn they become a risk for other more acknowledged users, since their stupidity make for easier ground for crackers. I mean, most crackers out there are just script kiddies, that go and use their latest crackware, and in fact are just users themselves! Few of them would have the knowledge or will to sit down and do things by hand.

That, in my opinion, also keeps viruses away from Linux, the fact that the Linux user base is usually more literate when it comes to computers and security, and protects itself more effectively.

Knowledge, and not the choice of one system or another, is what makes good security. Of course, having better grounds in which to stand is a lot better, and that's why I have Linux installed (and use it almost all the time, except for a game or two, when I want to relax a little), but you should stress that people should learn to defend themselves against the perils of the internet, instead of telling them Linux will solve all their problems.

- Re:Of all stupid lusers... by Anonymous Reader (Score:0) 2003.08.14 11:03
  - The hidden folder they use is ... "Recycle Bin" by Anonymous Reader (Score:0) 2003.08.18 15:46
- Re:Of all stupid lusers... by Anonymous Reader (Score:0) 2003.08.14 11:12
  - Re:Of all stupid lusers... by Anonymous Reader (Score:0) 2003.08.14 12:42
    - Re:Of all stupid lusers... by Anonymous Reader (Score:0) 2003.08.14 13:04
- Re:Of all stupid lusers... by Anonymous Reader (Score:0) 2003.08.14 11:16
  - Re:Of all stupid lusers... by Anonymous Reader (Score:0) 2003.08.14 12:58
- Re:Of all stupid lusers... by chillin (Score:1) 2003.08.14 13:05
  - Re:Of all stupid lusers... by Anonymous Reader (Score:0) 2003.08.14 13:23
    - Re:Of all stupid lusers... by chillin (Score:1) 2003.08.14 16:01

Windows is a Joke (Score:1)

By chillin (169660) on 2003.08.14 10:40 (#64747)

All Microsoft products are complete trash, and we all know it. They can't keep their software secure, simply because they didn't write it. Here's an old boxing saying for you:

"Don't worry about getting lucky, if they deserve the belt, they can defend it!"

Well, the same thing goes for computer software. If it's really your technology, you can continue to innovate and improve it, as well as maintain it . Since Gates left IBM and Microsoft was started, the "defending of the belt" has yet to happen. The same security exploits, buffer overruns, and open port problems still remain, and resurface to this very day. 20 years has passed, and they still haven't fixed their port system (amongst other things). It is obvious - they truely ripped off OS/2.

Open Source will stay more secure, because it was actually written, as appose to stealing the code, and trying to adapt it to your programs/OS. Say whatever you will, but when you actually code your own stuff, bugs are fixed at a much faster pace, and fewer are introducted in the first place. Rewriting

something from the ground up is only and issue of time, because you wrote it originally anyways. If someone chooses to take their ball and go home, the project still goes on. Quanta Plus and Galeon are good examples of this.

For the poster [newsforge.com] who said this is one incident, not an epidemic: I challenge you to read more. To this very day, people are still using webservers to send denial of service attacsk via a security hole present in IIS 4 and 5. Even furhter, I've personally known people in the past (during my teenage years) who used Microsoft's open port problem to upload trojans, and even run servers off of the infected machines. Just because it doesn't make the front page, doesn't mean it isn't happening. This story proves that.

And another thing: Everyone wants to flame the author acting in poor taste, but no one seems to remember when that Shuttle that used Linux machines crashed, and the anti-Linux commnents came out of the woodworks. These people died, and they used that as ammo against Linux. I dare anyone to tell me how you can be in poorer taste than that. Let's not get amnesia now...

- Re:Windows is a Joke by Anonymous Reader (Score:0) 2003.08.14 13:39
  - Re:Windows is a Joke by chillin (Score:1) 2003.08.14 16:04
    - Re:Windows is a Joke by Anonymous Reader (Score:0) 2003.08.19 11:10
- I must have been living on the moon or something by Anonymous Reader (Score:0) 2003.08.14 21:17

Not a Windows Probelm (Score:0)

By Anonymous Reader on 2003.08.14 10:46 (#64749)

While I do appreciate the security of my Linux system(s) The article that is referred to by this article is not a windows problem. I mean it is eveident the problems "this" man had, seems related because of trojan horses or viruses are only part of the picture. It is apparent that the man was having problems with the relationship with his X wife and custody of the kids. Now as we all know, the legal systems are very fair and just (not)..... about dealing with people. That fact is this article left out much of the dynamics about the relationship.

And before anyone jumps on the fact that this is a stricly technological issue, let me point out that the prosecution of the man was based on a legal moral one. The fact that they are using the computer as a way to accuse him is only a side issue. We've all been there, I mean we have all been to places we did not intend to be (on the internet) and to wrestle with dealing with the issues. But in this case there is much more going on behind the scenes and to use this as a justification to "swith" from Windows to Linux is absurd. There are far better approaches then this to take.

I am always amazed at the lack of looking at the larger issues (Moral, Spiritual) that the Linux community takes. Apparently "this" (technological) world is the only thing that "Geeks" see. For all the "hiding" that you all do, It's interesting to see that "these" important and very relavent issues come in and invade your little "Geekdom" world. You had better wake up to the larger issues (then technological ones) and begin to deal with these things.

- Lost without a Clue by chillin (Score:1) 2003.08.14 13:14

Windows is Not Ready for the Internet (Score:0)

By Anonymous Reader on 2003.08.14 10:52 (#64752)

It's the truth. Repeat it often. Use it as a tagline.

ptrace and ftpgnu.gnu.org (Score:0)

By Anonymous Reader on 2003.08.14 12:48 (#64781)

Editor's note: The recent crack of the GNU.org ftp server was by a local user; that is, someone who had physical access to the system.

Actually, the attacker could have been (and probably was) remote, i.e., without physical access to the system. To run a local exploit, one only needs to be *logged on* to the system being attacked. My guess is that the attacker first stole a valid account/password combination, or was a former

(disgruntled...?) legitimate user.

Apropos of stealing account names and passwords, it's appalling that some public open source repositories (e.g. Freshmeat) don't use SSL for user logins...

TCP/IP Freely

- Re:ptrace and ftpgnu.gnu.org by Anonymous Reader (Score:0) 2003.08.15 3:09
  - Re:ptrace and ftpgnu.gnu.org by Anonymous Reader (Score:0) 2003.08.15 9:45

PLEASE (Score:0)

By Anonymous Reader on 2003.08.14 12:51 (#64782)

Just go away Roblimo. I don't know about anyone besides me, but I'm getting really tired of reading your stories. They do very little to enlighten or even entertain. Even a tongue-in-cheek "ha-ha" over this story just because it involves something related to Windows insecurity just isn't funny to me.

Murphy's Law and Setting up your PC (Score:0)

By Anonymous Reader on 2003.08.14 14:16 (#64801)

These problems are of zero concern to the end users I service. Why? Because I fully respect "Murphy's Law" which states "If it can screw up, It will screw up at some point". The biggest problem in securing Windows and Linux PC's in the "real world", is the brain dead way they (specifically Windows) are initially installed, putting the whole system on one partition.

To use an automobile analogy, I separate the engine from the luggage. I install just the core operating system on the c: drive (along with any programs that can't be fully trusted "Microsoft") and install everything else on a D: partition. Once the system has been fully installed and all defaults have been set, a (ghost or partimage file of the c: drive is saved to a back up folder on the d: partition. Any time the end user makes changes to the basic system, they just update the ghost file.

My clients don't have to worry about any of this crap. They are five to fifteen minutes away from a fresh new system (plus registry) with all of their defaults set ,minus any viruses, trojans or back door tracking data bases put in there by Microsoft or any one else for that matter. Plus if they follow some other surfing and security guidelines I have set up for them, they get no ("zero!") spam.

I am currently working to split Linux up (properly) in this fashion too.

There are alot of factors to consider when you do this kind of splitting in Windows but over time I have gotten it down to a reliable science.

I can't believe all of the geniuses PC writers haven't figured this out. I have had clients tell me that they saw this or that news story about spam or viruses and they are laughing about how stupid (or corrupt) Branded PC makers are.

Want to fix it ? Ask me how! Zeek....

Humorous for all the wrong reasons (Score:0)

By Anonymous Reader on 2003.08.14 15:30 (#64812)

Usually Roblimo's articles are more grounded but this is just blather. The recommendation for Codeweavers/WineHQ is weak because they only run a few applications and if you need an office suite run Open Office if you need graphics run the GIMP. As for the spirit of the article I think the road to failure is paved with good intentions.

If Pete Townsend only knew... (Score:0)

By Anonymous Reader on 2003.08.14 17:09 (#64835)

I'm sure my Who idol, Pete, would have run his Windows on Win4Lin in Linux and saved himself the grief...

Even Mr. Miller seems to be hopelessly underinformed with his ramblings about WINE... what one-or-two app Windows-requiring L-user would use WINE when they could run all the Windows apps they ever abhorred but favored nonetheless?

Win4Lin rocks, Pete.

Very talented trojans (Score:0)

By Anonymous Reader on 2003.08.14 21:31 (#64859)

Can someone tell me how the virus/trojan that this guy somehow got infected with is able to turn his PC on 'all by itself'? I could be wrong, but doesnt a virus/trojan (software) require an OS to be running or at the very least system power before it can weave its 'magic'?

Confused...

- Re:Very talented trojans by Anonymous Reader (Score:0) 2003.08.14 23:04
- Re:Very talented trojans by Anonymous Reader (Score:0) 2003.08.16 7:39

homogeneity (Score:0)

By Anonymous Reader on 2003.08.15 4:59 (#64890)

beyond windows flaws, it is mainly the fact that it is a huge and homogeneous target that makes this sort of attacks easier.

Linux has got its lot of insecurities, but there is such a diversity of component combination between distros that it would make it harder to make an attack work on a large chunk of the linux install base.

The linux worms that I have heard off targeted well defined machines like web servers, which was facilitated by the fact that Apache is used on a wide majority of Linux servers.

That diversity is contributes a lot to make Linux a more difficult target. That fact that most linux users are also technically litterate helps as well...

All that might change if Linux becomes more widespread and that in the process, fewer distros survive.

Code and the law (Score:0)

By Anonymous Reader on 2003.08.15 9:57 (#64920)

Some have said I have not been humorous enough to see humorous advocacy. Yes, this article is a bit over the top in the direct connection that it makes, but it also points out, very indirectly, a different and very worthwhile set of broader questions for society as a whole to consider as we advance into the next century; can a society that comes to depend on computing to enforce laws ultimately tolerate the use of closed source proprietary solutions?

Consider, all laws are openly published. This allows citizens the ability to know what the laws are and when they might be transgressed. When a closed source system becomes part of this equation, then neither the accuracy or the means that laws are applied are open to public scrutiny. There are many principles to consider, including, how does a closed source system potentially select law breakers. At least in my American constitution, deliberately "selective" enforecement of the law is prohibited. Yet, a closed source system could be programmed to do this, or even do so accidently, and offer no immediate recourse to the falsely prosecuted as a result.

I know somebody who was once a free software advocate that passionately explained how code can become law and the inherent dangers of laws enforced by proprietary software. In this I believe he was fundimentally correct.

Very missleading and partly false (Score:0)

By Anonymous Reader on 2003.08.16 6:57 (#65018)

Worms infect systems by hacking in. They need only a security defect. Using open source dose not save you from this. The risk is less than what you'd have if you run Windows but that is purely becouse Microsoft is lazy. Still most of the worms lately happen AFTER Microsoft patched the defect

the same apathy in open source systems can produce identical results.

It is true Unix and Linux are basicly immune to viruses. Viruses need root access and the downloading of binary files. If instead you download and compile source code or run software in secured accounts this isn't a problem.

Anti-virus software won't work with worms. Anti-virus software works to alert you to an infection BEFORE you install it. Worms install themselfs. Once any malware is running your virus checker is unreliable.

The main story here is this guy who's computer was infected and now downloads child porn on it's own.

It seams highly unlikely this was a trojen, virus or worm. Trojens and viruses were originally made to exact revenge against one person and the morus worm (that took down the Internet) was an accadent. Attempts to control malware have proven misserable failures. It seams highly unlikely such a force would infect only one person.

However one form of malware is easly containned.

Pranks. A friend installs a prank when your back is turnned and laughs as you try and figure it out. Pranks have been around for a very long time.

Not a sereous consern becouse as a rule you don't let people use your computer that you don't trust.

It appears to me someone had access to this guys computer who had a major grudge against him and installed the prank.
This person saw to it the poor guy was fingered as a pedophile then investigaters could find child porn on the computer.

Also there have been far more than just one trojen for Linux. There has been many trojens for Linux and Unix over the years far more than Dos and Windows combined. But trojens have a very short life span. Viruses are prefered to trojens becouse they have long life spans. Most of the original dos viruses are still in the wild. There are no Unix viruses purely becouse they won't work. There has been ONE Linux virus it was to prove it could be done it prayed on the new nieve Linux community and a software defect. Some education and it's dead. I don't think the bug was ever fixed instead the libary in question was disguarded.

Overall this man was framed the hard way.
Knowing his system may be more valuable than picking a secure os becouse he knew something was up if he could have tracked it down and removed the offending code there would be none of this public circus.

- Re:Very missleading and partly false by Anonymous Reader (Score:0) 2003.08.17 11:49

Options vs no options (Score:0)

By Anonymous Reader on 2003.08.17 2:59 (#65133)

At the very least those using gnu/linux and BSD have the option of mounting certain partitions as read only (ie /bin). Thus preventing alteration of many executables unless first cracking root. This option is not available for the home users. Additionally, there are extensive tools available like tripwire, snort, nmap, nessus, etc and documentation to go along. While I agree that linux is not immune to the kinds of security problems plaguing m$ products, there is a much greater emphasis on. It is unfortunate that there is no accountabilty for the security failures in m$ products. At the very least people who buy defective products should return said products for a full and complete refund. Additional punative damages should be provided for lost time and productivity suffered by businesses. These options don't exist.

bullshit! (Score:0)

By Anonymous Reader on 2003.08.17 4:17 (#65138)

linux(and other unix based OSes) can't be infected? rehahally?!
What about all the daemons that must run as root? if they has a security hole, it is possible to make a worm just as the blaster for linux.

I find that article lame advertise for linux.

Happy FreeBSD user,
S7.

Windows vs. Linux - what a waste of breath (Score:0)

By Anonymous Reader on 2003.08.17 23:50 (#65228)

I don't have a problem with the article, but what really surprises me is all the crap people talk about in response to these types of articles. Linux is a piece of software, its not a religion (or am I wrong here?) It just seems that there would be more important things to get upset about, than whether someone uses linux or not!

I have been a user of linux for 7 years now. I have a Windows desktop at home as well as a Linux development and firewall server. I also have a windows desktop at work.

I don't have a choice with my work desktop - but I do for my home one.

I choose windows because it is a simpler solution for what I need.

Linux is excellence for what I use it for:
Firewall on my DIALUP account
PHP / Apache / MySQL development server

However I have not found a better PHP editor than the PHPEdit software (Open source and still in beta, but nice all the same) - and that only runs on windows.

I have not found a better graphics software than Adobe Photoshop 6.0! (I do not like GIMP, even after I purchased the excellent book Grokking the Gimp - but that might be more to with the fact that I already know the Photoshop software, and do not have the time to get over the GIMP learning curve)

I have a Canopus Raptor-RT video editing card, and the software does not run on Linux, nor does the card work under linux.

So a decision of windows vs. linux has to be made based on what is the best solution.

My home windows machine sits behind a linux firewall, which is locked down pretty tight, however I always try to stay up to date with the Service Packs, and even installed the RPC hotfix for that worm mentioned in the article. I have also started having a virus checker installed that is up to date.

In my opinion there will always be a place for Windows - its great for its intended use, which does not include Servers! in my experience.

Something I read... (Score:0)

By Anonymous Reader on 2003.08.18 15:31 (#65340)

I'm not sure, this is coming off the top of my head, but I seem to remember an article I read recently where Disney, ILM, and another company that I forgotten the name of ported Adobe Photoshop 6.0 to Linux using WINE. One more reason to use Linux for everything.

False sense of security (Score:0)

By Anonymous Reader on 2003.08.18 16:31 (#65352)

This article is Pro-Linux FUD.
Is this A Bad Thing?
Well, not necessarly. It's dirty, but it's one of the oldest marketing tricks - heck, politics are ONLY about FUD - so, why not use it pro-Linux for once.

The problem that I have with the article is that it creates a false sense of security : "Install Linux, download only from secure sources and nothing can happen to you."
Yeah, right.
When everyone does this, we will have A LOT of Linux breaches in 6 month from now. Linux has mainly fewer important security breaches than Linux because the guys running it, know what they are doing.

Check the Cisco security problem. Nothing happened. Why? Because the guys running Cisco routers are GOOD. They know what they are doing, they configured the routers to reject all packets directed to the router unless they come form a trusted machine (= the remote administration terminal). Therefor nothing happened.

The problem with Windows is NOT that it has security flaws, but that most of it users have no clue of security, even thoose that are "Microsoft certified server administrators".
Microsoft is even proud of the fact that a Microsoft admin is cheaper than a UNIX-Admin.
However, the MS-Admin only knows HOW to do things, but most of the time not WHAT, and if he knows WHY to do something, well then he is as expensive as a good UNIX-Admin (and he should be!!!)
Being a good admin is hard and it's important to know WHAT to do WHY. Knowing HOW to do things is necessary and may be easier in Windows, but in no way suffisant.

Linux and UNIX have fewer issues, because the people running it are better. However, with Linux becomming more and more popular, we will have the same problems that Windows has now. Unupdated systems are crackable. Period.

The other problem that Microsoft has, is that people dont trust them. This is a HUGE problem.
As a home user is not qualified to maintain security on his computer, somebody else has to do this for them. Microsoft offers the possibility to keep the computer up to date with an automatic update. However, most people dont trust Microsoft and deactivate this feature. And who will blame them with an EULA that says that Microsoft may update your computer without notice nor your consent in order to inforce digital rights management anytime in the future.
But by refusing automated updates, they often forget updates at all and leave their computer open to even more malicious people.

This is a point were Linux is TRUELY superior to Windows. I TRUST Debian and allow them to automaticly update my computer and this reduce most security problems.

However, note that this is in no way a technical problem but a problem of Trust.

Viri are for now not a problem on Linux, but when Linux grows, binary distributions may become more common (for now think Realplayer and Java) and viri will become a greater problem. Of course, they wont get root access to the system, but do you really need root access? You can hide a FTP server running on port 12346 on an user account as well. You can email yourself out from an user account as well too.
Again, for now we dont see these problems because clueless people dont use Linux for now, but when Linux really gets 20% of the desktop, we will see Linux-viri as well.

The good thing about Linux is that it can be remote-administrated. But until we have a distri that is remote-administrated by a trustworthy project by default, claims that Linux is a "install-and-forget" System, like this article implies, do more harm then good, because these claims will increade Linux security issues and therefor harm Linux' reputation later on.

Just me 2 (well perhaps 3;) cents