

## Re: Bastard spammers

---

*Source:* <http://newsgroups.derkeiler.com/Archive/Uk/uk.legal/2006-01/msg02009.html>

---

- *From:* Mike <mike@xxxxxxxxxxxx>
  - *Date:* Mon, 09 Jan 2006 22:21:13 +0000
- 

On Mon, 09 Jan 2006 12:10:29 +0000, Cynic <cynic\_999@xxxxxxxxxxxx> wrote:

>It would be a bit pointless to set up a DNS server, a mail server, a  
>Telnet server

No—one of any competence sets up a publically accessible telnet server!

>and an FTP server and then deny public access to the  
>computer in question.

I have several services exposed to the Internet that aren't available for public access. Access control isn't difficult.

>Just how do you "watch like a hawk" an FTP  
>server?

By monitoring its log automatically and issuing alerts (via email , SMS, etc) in the event of suspicious activity. There are also various intrusion detection systems that can be employed.

>In my case, the hacker gained entry via an exploit and  
>deleted the log entries in question.

You held the logs locally, then. A more experienced administrator might have chosen to send syslog records to another machine where they couldn't have been altered retrospectively.

>The reason I initially chose Linux for my servers was because I  
>believed it less vulnerable to attack. Boy, was I wrong!

You had one unfortunate experience, perhaps due to inexperience, and this has coloured your opinion. Linux and the various versions of unix are in fact several orders of magnitude less vulnerable to attack. Without knowing the details of your experience, I suspect that a fix to the exploit used to gain access to your system was available at the time but you weren't aware of it.

## Re: Bastard spammers

>After

>replacing it with a Windoze system that does the same thing, I have

>suffered only one relatively minor attack in the past 2 years.

Good, although I wonder what you mean by "attack". My firewall sees typically several thousand attempts per day to exploit known vulnerabilities in Windows.

>ISTM that most Windoze nasties are geared toward infecting computers

>that people are using as a client station (via files that the user

>opens and web pages accessed etc.), whilst Linux nasties are geared

>toward computers used as servers rather than depending on the user's

>actions, and infect via ports that have to be open (DNS, HTTP, POP3

>etc.) by exploiting vulnerabilities in the running service.

None of those ports have to be open. The first rule of computer security is to open only those ports that need to be open. This is a concept that Windows hasn't yet taken on board! There will be no vulnerabilities to exploit if the administrator keeps up to date with security announcements.

If you chose to try again with Linux or perhaps FreeBSD, you might be pleasantly surprised.

Mike.

—

Entia non sunt multiplicanda praeter necessitatem

.

---

### • *Follow-Ups:*

◆ ***Re: Bastard spammers***

◇ *From:* Cynic

### • *References:*

◆ ***Re: Bastard spammers***

◇ *From:* Mike

◆ ***Re: Bastard spammers***

◇ *From:* Cynic

◆ ***Re: Bastard spammers***

◇ *From:* Mike

◆ ***Re: Bastard spammers***

◇ *From:* Cynic

◆ ***Re: Bastard spammers***

◇ *From:* Alec McKenzie

◆ ***Re: Bastard spammers***

◇ *From:* Cynic

◆ ***Re: Bastard spammers***

◇ *From:* Benedict White

Re: Bastard spammers

◆ **Re: Bastard spammers**

◇ From: Cynic

◆ **Re: Bastard spammers**

◇ From: Benedict White

◆ **Re: Bastard spammers**

◇ From: Cynic

- Prev by Date: **Re: slander?**
- Next by Date: **Re: Mortgagae (early settlement charge)**
- Previous by thread: **Re: Bastard spammers**
- Next by thread: **Re: Bastard spammers**
- Index(es):
  - ◆ **Date**
  - ◆ **Thread**