

Re: Constant Hacking Attempts – Pacific Bell DSL customer

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-02/0547.html>

From: sponge (mtubi@python.net)

Date: 02/07/02

From: mtubi@python.net (sponge)

Date: Thu, 07 Feb 2002 02:17:35 GMT

On Wed, 06 Feb 2002 19:28:10 +0100, Tilman Schmidt

<Tilman.Schmidt@ePost.de> wrote:

>*Neko* <Neko@nospam.com> wrote:

>

>>*x-no-archive: yes*

>

>*Why?*

>

>>*I have basic dsl service from Pacific Bell in California with a*

>>*dynamic IP address. I use ZoneAlarm Pro as a for Firewall*

>

>*Why?*

>

>> *and just*

>>*installed Zone Analyser to review my logs. I was recently reviewing*

>>*old ZoneAlarm logs with Zonelog as far back as 2000 (ok, I was bored*

>>*and I had new toy) and found I've been attacked at min.4 times a day*

>>*and up to 10 times daily.*

>

>*Those are not attacks, they are probes, and they are absolutely normal*

>*in today's Internet. You should throw away ZoneAnalyzer, and ZoneAlarm*

>*with it, for scaremongering, and concentrate instead of configuring*

>*your system securely.*

ZA and others are useful for detecting attempts by applications to

connect to the Internet. if nothing else. I do find the idea of

stealthng to be useful, even if all it does is to slow up the probes

and scanners a bit. However, you are correct in the part about needing

to configute your system securely.

>*Nothing at all. ISPs aren't supposed to filter traffic, they are*

>*supposed to provide connectivity. Securing your systems is your own*

>*responsibility.*

Some ISPs do offer minute security. I suspect this will become an increasingly significant selling point. However, it is still no replacement for your taking action to protect yourself. Put another way, if you don't protect yourself in this world, don't expect anybody else to.

>> *Can't they afford Checkpoint? <grin>*

>

>*They can't afford the complaints and lawsuits that might result if they block traffic the customer would have wanted to pass, or vice versa, so they wisely offer just full, unfiltered connectivity.*

An ISP has the right to block any traffic they please, as per the Terms of Service. We block a number of abusive ISPs and spamhouses. It's our network, that's our right.

>*Most of the machines those probes are coming from have been hacked themselves, so if you have spare time on your hands you can do their owners a favor if you alert them to the fact that their machine is issuing probes. Many owners are grateful about that.*

>>*Pacbell only sends an auto-reply to my report.*

>

>*Some just don't care.*

Well, for one, PacBell is a black-hat ISP, in my experience. That aside, most security departments realize that virtually all of these complaints come from easily-scared types who see a message pop up on their firewall. It takes a while to learn what's normal and what's a deliberate scan. And, you touched on many of the reasons why we dislike these reports. If you find your IP being scanned for multiple ports from the same originating IP (a vertical scan), or if you find multiple IPs on your network being scanned for one or a few ports (a horizontal scan), then you have a legitimate concern and should email the sending ISP's security department, attaching your firewall logs. However, most people only get one scan, which may be misdirected traffic or someone with a trojan or bug on their machine. And they never know to send their firewall logs, so we don't have enough to go on anyway.

>>*What is Zone Alarm NOT protecting? At one point I was running Black*

>>*Ice Defender + Zone Alarm.....Is Zone Alarm enough?*

>

>*ZoneAlarm doesn't protect anything. It is just watching and blocking traffic to ports where no program should be listening anyway. On a properly configured system it is completely redundant. The probes which ZoneAlarm is alarming you about wouldn't have gotten anywhere, anyway. On the other hand, well-written trojans just circumvent "personal firewall" software like ZoneAlarm, so again, ZoneAlarm and the like don't protect anything.*

Not entirely. See first comment. Bear in mind that your chances are far, far higher that you now have or will someday get a spyware, trojan, or some nasty on your computer. Compared with the relatively low chance of you being hacked from the outside, this means that personal firewalls — or at least some way of monitoring what programs on your machine are trying to connect to the Internet — will be necessary.

>>*The firewall is stopping these hacking attempt::*
>*[list of frequently probed ports]*
>
>*As I said, none of these ports accept traffic on a properly configured*
>*system in the first place. It would do more good to the security of*
>*your system if you concentrated on making sure that it is, in fact,*
>*properly configured, instead of tracking the normal background noise*
>*of the Internet.*

Well put.
Sponge

- ***Next message:*** [Mark T. Ganzer: "Re: Linksys BEFSR41 V.2 and ftp"](#)
- ***Previous message:*** [Greg Hennessy: "Re: Can't browse on networks behind firewall"](#)
- ***In reply to:*** [Tilman Schmidt: "Re: Constant Hacking Attempts – Pacific Bell DSL customer"](#)
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)