

## Re:[fw-wiz] Vulnerability Response (was: BGP TCP RST Attacks)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-06/0026.html>

---

**From:** Marcus J. Ranum ([mjr\\_at\\_ranum.com](mailto:mjr_at_ranum.com))

**Date:** 06/01/04

To: Brian Ford <[brford@cisco.com](mailto:brford@cisco.com)>, [firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)

Date: Tue, 01 Jun 2004 14:33:15 -0400

Brian Ford wrote:

*>We need to raise awareness about what is out there; what is good and what is bad. Not by labelling technology or products but by talking about practices. We can start by just focusing on people on lists like this. What's working well for you and why? I don't see many messages like that here (or at any of the conferences) any more.*

Well, I know a \*lot\* of us have posted various "here's what works" – including me – but it's not what people "want to hear" – that's the problem.

What works is not doing it. What works is understanding your traffic.  
What works is log monitoring and strict enforcement of a tight policy.  
What works is not having business units jump over the chain of command.  
What works is not what people WANT or are ABLE to do.  
Fortunately, that's not my problem. :) I'll let Darwinian evolution take care of it, over time.

*>We need to think about how to grow smarter practitioners. I thought last year it might be via CISSP or some other "certification". I gave that a shot. Before that I thought the SANs direction (again with certifications) was good. I don't know if this will work for as large a portion of the population as is needed.*

If education was going to work, it would have worked by now.

Back in the old days, the population of clueful system administrators was larger, proportionally, than it is now. Largely due to population growth in the Internet population. Was security better? Or proportionally the same? The environment has shifted too much to tell – but I think that if there was a big amount of leverage positive or negative to be achieved by education, we'd be seeing it by now, right? The population would be sharply divided into the clued and the non-clued. But instead it's not happening that way. I don't have to prove a negative: show me how education is helping in the big picture...

*>Patching isn't great. But it is what we have right now*

Eat sh\*t, 50 billion flies can't all be wrong.  
Besides, there's lots of it. Is that what you're

saying?

*>The sad reality is that many user type folks insist on doing stuff that is bad for themselves. They read email they shouldn't read. They surf to sites they shouldn't surf to. They don't use good passwords. They don't backup data.*

Right! That's what I mean. It's too late. It's now a human right to click on attachments in Outlook. Heck, it's a human right to run Outlook, apparently. What a crock of dingoes kidneys that is! It's a public health issue. It's a corporate governance issue. It's a matter of survival – or of bearing the costs of being stupid. I don't care which. But people gotta stop whining about the end results of their being stupid.

"\*sniffle\* I run Windows and no matter what I do, I get HACKED!"

Duh! Here's your sign!

"\*WAAAHH!\* I have a firewall and it didn't help!"

Duh! Here's your sign, go stand over there!

"Boo–HOO! I put my mission critical stuff on a toy O/S and it crashed and burned when some co–worker clicked on an attachment in Outlook!"

Duh! Here's your sign, welcome to the club!

*>If we really want to make the Internet a better place we should solve these problems.*

*>– Create strong, effective, cross country laws and go after spammers and phishers.*

Y'know, I saw one go across my radar screen this morning. I'll quote some of it..

[http://news.com.com/2102–1034\\_3–5218178.html?tag=st.util.print](http://news.com.com/2102–1034_3–5218178.html?tag=st.util.print)

More than 85% of the 800 million email messages sent every day from Comcast networks are spam from zombie computers. One reason for the sheer volume of spam coming from Comcast is that Comcast has a large number of high–speed Internet customers whose connections are most desirable for spammers to hijack. Comcast's marketing department nixed a proposal to block traffic on port 25 because the cost of helping customers reconfigure their mail programs would be quite high.

**DUH! HERE'S YOUR SIGN!**

When marketing weenies are worried that \*other\* people are too dumb to do something, then you KNOW that sound in the distance is the hoofbeats of the four horsemen.

*>– Ditto that with web sites that feed the problem.*

What, and ruin the \$129million/year anti–spam industry?

*>– Push the strong password issue back on the organizations that require them. Don't allow the costs of fraud to be assumed by customers. If financial institutions had to pay damages to their customers or others for info leakage incidents or fraud then financial institutions would work on developing better password technology.*

Firewall-Wizards: Re:[fw-wiz] Vulnerability Response (was: BGP TCP RST Attacks)

Passwords are pointless to worry about for real when the operating systems they are being used on are less secure than your average paper bag. The Orange Book Guys knew all this in the 1970's.

>- *Develop an OS that has backup built into the OS.*

Been done. And that's not counting VMS' file versioning, which was great though annoying to many.

>*There is no easy path here. We're somewhere in an unpleasant swamp and we have to \_continue\_ to try and find a way out.*

It's important to have the sense to sometimes say, "WOW! dead end! time to try a different plan!" If you're lost running around FASTER only gets you tired.

mjr.

---

firewall-wizards mailing list  
firewall-wizards@honor.icsalabs.com  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>