

# RE: [Full-Disclosure] RE: MS SQL WORM IS DESTROYING INTERNET BLOCK PORT 1434!

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-01/0069.html>

---

**From:** hellNbak ([hellnbak@nmrc.org](mailto:hellnbak@nmrc.org))

**Date:** 01/27/03

From: hellNbak <[hellnbak@nmrc.org](mailto:hellnbak@nmrc.org)>  
To: "Schmehl, Paul L" <[pauls@utdallas.edu](mailto:pauls@utdallas.edu)>  
Date: Mon, 27 Jan 2003 01:50:15 -0600 (CST)

> No, with a clue *\*and\** permission. I'd be really surprised to find a  
> single edu that has a "deny all" stance. Worldwide. That is a complete  
> paradigm shift for edu. Fortunately, the med schools are being forced  
> to do that now due to HIPAA, and hopefully it will be true some day in  
> all of edu. For now, very few edus even have firewalls, much less a  
> "deny all" policy.

Wow, if this is truly the case then I can see where you get your argument from.

> It's time some folks got a grasp on reality. I have a deny all policy  
> on every box that I control, but for the entire network? Good luck.  
> Maybe some day, after edus have suffered enough that the upper  
> administration and the faculty get some clues, but not today. Not in  
> edu. I wish it were true.

I guess the problem I have with this is that I have done work for some of the worlds largest cororations and have seen them pull exactly this off. I have two clients who are Canadian Universities and they are doing just fine. I guess my ignorance about the USA .edu situation is that I have never been a part of one.

> I'd be real interested to hear the names of any edus that 1) have a  
> firewall and 2) have a "deny all" policy in place and *\*implemented\**.

I can't/won't name people I have done work for on a public list or to you privately. But I can think of a half dozen — granted that is a drop in the bucket but a start...

> Given your last statement is true, then why should I use MS products for  
> security?

I agree — when I originally read your statement I thought you meant that you shy away from MS products in general.

- > 1) *I don't trust MS products for security related tasks. The idea of*
- > *implementing a firewall based on an MS OS scares the hell out of me. 2)*
- > *Their performance sucks. Compared to \*nix based products, it takes*
- > *twice the box to do the same job – whether it's scanning for*

I agree.

- > *vulnerabilities or using an IDS, setting up a firewall, you name it.*
- > *And then there's the cost. ISS wants 6 figures (for software and the*
- > *necessary equipment) to scan for vulnerabilities. Why should I spend*
- > *the few precious dollars we have for that when I can use nmap and nessus*
- > *and get better results?*

I agree here as well. ISS is shit, we all know it yet organizations pay their high fees. Scary and pathetic. When I am doing IDS work for clients I show them the differences between Snort and ISS RealSecure. Their first reaction is — oh well ISS must charge so much for a reason — then we call the ISS rep get a demo and do an actual comparission and guess what — Snort wins and gets implemented.

Sorry, getting off track there — but I do concede this part of the debate to you as my experiance has been the same. Anyone remember Guantlet firewalls running on NT? hehehe, what a joke those were....

- > *And here I thought we'd progressed into the 21st century. It is \*never\**
- > *the victim's fault, no matter the provocation, for a crime having been*
- > *committed against them. Never. Their behavior might mitigate the*
- > *criminal's punishment, but it does not excuse the crime.*

You are right, a crime is a crime. But, lets say that in your particuliar city there is a huge increase in attacks on women. What is the typical reaction (at least in Canadian cities) droves of women go and take self defense training. No, this is not excusing the crime but it is taking the necessary steps to mitigate the risk and protect yourself.

Why can't that same observed human nature happen in the computing world?

- > *Since software was first written.*

Exactly, so why is it such a hard thing for everyone to understand that boxes need to be patched?

- > *We just got ours in September, 2002.*

I am amazed at how far behind the US .edu system is. I can't remember the Canadian system ever not having a dedicated security guy.

- > *Hell, I've been doing that for four years – long before I got this*
- > *position. I sent the notice on this particular problem in July, when*
- > *the patch was first announced. We still had six boxes hit. Most were*
- > *on desktops in schools, in places we weren't aware of.*

Ahh nothing like running SQL on the desktop. ;-) Seriously though, what if the action you took back in July (I know hindsight is 20/20 and all that) was to not only recommend the patch but also recommend that the firewalls filter this port. Shit, with the amount of boxes you have to deal with — it makes more sense to deal with the outside threat first at that firewall then get to patching internal boxes on a regular (but not as often) schedule. Firewalls are not the silver bullet various scumbag consultants want you to think they are but in cases like this they can help lower the risk.

Why not deal with security risks in a more sensible way? Calculate the risk and determine the best way to mitigate that risk — its not always going to be "just install the patch".

- > *shoes. Until you've been responsible for 10,000 desktops of every size,*
- > *shape and description, you have no idea what you're talking about. Talk*
- > *is cheap.*

Paul, I have — I come from a sys-admin background. I have worked in environments where I know there are way to many desktops to even think about patching let alone deal with the headache of trying to script a SMS package that actually works or a Tivoli distribution that won't blue screen boxes. This is why I look at more creative ways around security problems. This is why in a large environment it makes more sense to work around the patch then apply it when you get the time (which in some cases could be never).

- > *I'm not looking for sympathy. I trying to point the blame for these*
- > *problems at the real culprits.*

I agree that the real culprits hold the blame for releasing the damn thing (a big fuck you to whatever government agency was behind it) but there would be zero initiative to "test" worms like this on the net if people worked with the premise that it will fail because most systems are secure.

- > *Sure it will! You'll fill a few lawyers pockets and leave the admins*
- > *behind with less money now than they had before. Now \*there's\* a*
- > *"solution" that has real merit.*

And hopefully this will only have to happen once to scare the higher ups (government included) to spend the required money on security. All we hear is bitching about cyber-terrorism from the US Government yet it is clear that they do not care as they allow the US .edu system to be in such a state.

> *For those of you smartass know-it-alls that think you've got the tiger  
> by the tail, here's a suggestion for you – volunteer your time to some  
> of the local educational institutions. Pick a non-profit in your local  
> area and help them with their network. Do some fund raising to get them  
> the equipment they need. Or donate the equipment you throw out because  
> it's "out of date". DO something about the problem instead of bitching  
> about it in the lists and blaming the poor admins who have no power to  
> fix it.*

1.) I do not think that I know-it-all. I tried very hard to not be a smart-ass in my previous and this reply. :-)

2.) I do know what I am talking about. I have clients who are ca.edu and I do volunteer my time to smaller schools (my son's private school for example, the local church eventhough I don't attend, my community center etc...).

I have built and given away my share of 300\$ boxes running Linux firewalls. Shit, I am 6000 miles away from my home right now and I still SSH into each box and do some health checking. So what? Do I need a hero cookie? Of course not, but these small organizations on their little T1's do not make as much of a difference as the larger .edu's do. Do you think a large USA .edu would plug in and run a firewall if I sent them one? Probaly not, they would be too busy questioning my motives.....

> *I have no problem with that. Just learn it in a controlled environment  
> that \*you\* own. Learning it at someone else's expense is theft – pure  
> and simple.*

I agree, and I am in no way justifying the actions of whoever released the worm. But with or without the Internet this type of stuff happens.

> *Some people have cried for litigation to "force" networks to "clean up"  
> and get rid of "lazy" admins. How about we ask for legislation to put  
> hackers away for life? Would you like that?*

Actually, depending on our definition of a hacker — yeah that is somethign that would be worthwhile. But, the litigation and laws going the other direction also need to happen. I am not saying that admins are lazy — at least not all of them. But the internet is global and we all need to do our part to police it as there is an absense of authority.

> *networks, stop blaming the networks for the problem. Blame the person  
> responsible.*

And I do. But I also know that it wouldn't be so fun and attractive to these people if they already knew it wouldnt work. I truly believe that this wasn't an accident by some kid either.

> *So we should just give up?*

No, we should adjust our behaviour to deal with this.

- > *Did it ever occur to you that my posts might also be informational and*
- > *educational? That they might influence someone \*not\* to experiment with*
- > *other people's networks?*

Actually, I have learned a lot about the .edu system in the USA from your posts so thank you. On the flip side, I am sure there are others -- less honorable than I who have also learned much, I am sure they will eventually thank you too. :-)

- > *It tells me there's a large gap between utopia and reality.*

I agree. Utopia will never be achieved. But we can all get closer I think.

- > *What's change control? ;-*

Heh, oh that would be the stupid system of testing patches thoroughly before rolling them out because too many organizations have been burned by VENDOR SUPPLIED patches breaking production environments.

Actually, I say that in jest but it is really true -- you would think that the same lessons would be learned about security.

Releasing a worm is bad and you should be punished. I hope that is what you meant with your statement about releasing "bugs". You surely don't mean that vulnerabilities should be kept quiet? Or do you? (\*ducks for cover\*)

--  
-----  
"I don't intend to offend, I offend with my intent"  
[hellnbak@nmrc.org](mailto:hellnbak@nmrc.org)  
<http://www.nmrc.org/~hellnbak>  
-----

---

Full-Disclosure - We believe in it.  
Charter: <http://lists.netsys.com/full-disclosure-charter.html>